

NIST SPECIAL PUBLICATION 1800-15

Securing Small-Business and Home Internet of Things (IoT) Devices

Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Donna Dodson
Tim Polk
Murugiah Souppaya
NIST

Yemi Fashina
Parisa Grayeli
Joshua Klosterman
Blaine Mulugeta
Mary Raguso
Susan Symington
The MITRE Corporation

Jaideep Singh
Molex

William C. Barker
Dakota Consulting

Dean Coclin
Clint Wilson
DigiCert

Darshak Thakore
Mark Walker
CableLabs

Eliot Lear
Brian Weis
Cisco

Tim Jones
ForeScout

Drew Cohen
MasterPeace

PRELIMINARY DRAFT

This publication is available free of charge from:
<https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos>



Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)

*Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B);
and How-To Guides (C)*

Donna Dodson
Tim Polk
Murugiah Souppaya
NIST

William C. Barker
Dakota Consulting

Eliot Lear
Brian Weis
Cisco

Yemi Fashina
Parisa Grayeli
Joshua Klosterman
Blaine Mulugeta
Mary Raguso
Susan Symington
The MITRE Corporation

Dean Coclin
Clint Wilson
DigiCert

Tim Jones
ForeScout

Jaideep Singh
Molex

Darshak Thakore
Mark Walker
CableLabs

Drew Cohen
MasterPeace

PRELIMINARY DRAFT
April 2019



U.S. Department of Commerce
Wilbur Ross, Secretary

National Institute of Standards and Technology
Walter G. Copan, Undersecretary of Commerce for Standards and Technology and Director

NIST SPECIAL PUBLICATION 1800-15A

Securing Small-Business and Home Internet of Things (IoT) Devices

Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)

Volume A:
Executive Summary

Donna Dodson
Tim Polk
Murugiah Souppaya
NIST

William C. Barker
Dakota Consulting

Parisa Grayeli
Mary Raguso
Susan Symington
The MITRE Corporation

April 2019

PRELIMINARY DRAFT

This publication is available free of charge from
<https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos>



1 Executive Summary

2 The goal of the Internet Engineering Task Force’s [manufacturer usage description \(MUD\)](#) architecture is
3 for Internet of Things (IoT) devices to behave as intended by the manufacturers of the devices. This is
4 done by providing a standard way for manufacturers to identify each device’s type and to indicate the
5 network communications that it requires to perform its intended function. When MUD is used, the
6 network will automatically permit the IoT device to perform as intended, and the network will prohibit
7 all other device behaviors.

- 8 ▪ The National Cybersecurity Center of Excellence (NCCoE) has demonstrated for IoT product
9 developers and implementers the ability to ensure that when an IoT device connects to a home
10 or small-business network, MUD can be used to automatically permit the device to send and
11 receive only the traffic it requires to perform its intended function.
- 12 ▪ A distributed denial of service (DDoS) attack can cause a significant negative impact to an
13 organization that is dependent on the internet to conduct business. A DDoS attack involves
14 multiple computing devices in disparate locations sending repeated requests to a server with
15 the intent to overload it and ultimately render it inaccessible.
- 16 ▪ Recently, IoT devices have been exploited to launch DDoS attacks. IoT devices may have
17 unpatched or easily discoverable software flaws, and many have minimal security, are
18 unprotected, or are difficult to secure.
- 19 ▪ A DDoS attack may result in substantial revenue losses and potential liability exposure that can
20 degrade a company’s reputation and erode customer trust. Victims of a DDoS attack can include
 - 21 • **communications service providers** who may suffer service degradation that affects their
22 customers
 - 23 • **businesses that rely on the internet** who may suffer if their customers are unable to reach
24 them
 - 25 • **IoT device manufacturers** who may suffer reputational damage if their devices are being
26 exploited
 - 27 • **users of IoT devices** who may suffer service degradation and potentially incur extra costs
28 due to increased activity by their captured machines
- 29 ▪ Use of MUD combats these IoT-based DDoS attacks by prohibiting unauthorized traffic to and
30 from IoT devices. Even if an IoT device becomes compromised, MUD prevents it from being used
31 in any attack that would require the device to send traffic to an unauthorized destination. MUD
32 provides a standard method for access control information to be available to network control
33 devices.
- 34 ▪ This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide explains
35 what consumers should expect from IoT device manufacturers and demonstrates how MUD
36 protocols and tools can reduce the potential for harm from exploited IoT devices. It also shows
37 IoT product and system providers how to integrate and use MUD to satisfy IoT users’ security
38 requirements.

39 CHALLENGE

40 The term *IoT* is often applied to the aggregate of single-purpose, internet-connected devices, such as
41 thermostats, security monitors, lighting control systems, and smart televisions. The IoT is experiencing
42 what some might describe as hypergrowth. [Gartner](#) predicts there will be 20.4 billion connected IoT
43 devices by 2020 compared with 8.4 billion in 2017, while [Forbes](#) forecasts the market to be \$457 billion
44 by 2020 (a 28.5 percent compounded annual growth rate).

45 As connected devices become more commonplace in homes and businesses, security concerns are also
46 increasing. Many full-featured devices, such as web servers, personal or business computers, and mobile
47 devices, often have state-of-the-art security software protecting them from most known threats.
48 Conversely, many IoT devices are challenging to secure because they are designed to be inexpensive and
49 to perform a single function—resulting in processing, timing, memory, and power constraints.
50 Nevertheless, the consequences of not addressing security concerns of connected devices can be
51 catastrophic. For instance, in typical networking environments, malicious actors can detect and attack
52 an IoT device within minutes of it being connected and then launch an attack on that same device from
53 any system on the internet, unbeknownst to the user. They can also commandeer a group of
54 compromised devices, called *botnets*, to launch large-scale DDoS and other attacks.

55 SOLUTION

56 This Mitigating IoT-Based DDoS Project demonstrates an approach to significantly strengthen security
57 while deploying IoT devices in home and small-business networks. This approach can help bolster the
58 resiliency of IoT devices and prevent them from being used as a platform to mount DDoS attacks across
59 the internet.

60 The NCCoE sought existing technologies that use the MUD specification to permit an IoT device to signal
61 to the network what sort of access and network functionality it requires to properly operate.
62 Constraining the communication abilities of exploited IoT devices reduces the potential for the devices
63 to be used in attacks—both DDoS attacks that could be launched across the internet and attacks on the
64 IoT device’s local network that could have security consequences. This practice guide explains how to
65 effectively implement the MUD specification for MUD-capable IoT devices, and it envisions methods for
66 preventing non-MUD-capable IoT devices from connecting to potentially malicious entities using threat
67 signaling technology.

68 While the NCCoE used a suite of commercial products to address this challenge, this guide does not
69 endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your
70 organization’s information security experts should identify the products that will best integrate with
71 your existing tools and IT system infrastructure. Your organization can adopt this solution or one that
72 adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and
73 implementing parts of a solution.

74 BENEFITS

75 The NCCoE’s practice guide to Mitigating IoT-Based DDoS can help

- 76 ▪ communications service providers and businesses that rely on the internet understand how
77 wide deployment of MUD can help effectively combat DDoS attacks

- 78 ▪ IoT device manufacturers understand the relatively small steps that are required of them to
79 design and enable their devices to take advantage of MUD
- 80 ▪ users of IoT devices better understand that MUD is a crucial component of overall network
81 security and that they should both deploy the infrastructure required to support MUD and use
82 IoT devices that can take advantage of MUD

83 **SHARE YOUR FEEDBACK**

84 You can view or download the guide at [https://www.nccoe.nist.gov/projects/building-blocks/mitigating-
85 iot-based-ddos](https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos). Help the NCCoE make this guide better by sharing your thoughts with us as you read the
86 guide. If you adopt this solution for your own organization, please share your experience and advice
87 with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so
88 we encourage organizations to share lessons learned and best practices for transforming the processes
89 associated with implementing this guide.

90 To provide comments or to learn more by arranging a demonstration of this example implementation,
91 contact the NCCoE at mitigating-iot-ddos-nccoe@nist.gov.

92

93 **TECHNOLOGY PARTNERS/COLLABORATORS**

94 Organizations participating in this project submitted their capabilities in response to an open call in the
95 Federal Register for all sources of relevant security capabilities from academia and industry (vendors
96 and integrators). The following respondents with relevant capabilities or product components (identified
97 as “Technology Partners/Collaborators” herein) signed a Cooperative Research and Development
98 Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution:



99

100 Certain commercial entities, equipment, products, or materials may be identified by name or company
101 logo or other insignia in order to acknowledge their participation in this collaboration or to describe an
102 experimental procedure or concept adequately. Such identification is not intended to imply special
103 status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it
104 intended to imply that the entities, equipment, products, or materials are necessarily the best available
105 for the purpose.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses’ most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit [https://www.nccoe.nist.gov
nccoe@nist.gov](https://www.nccoe.nist.gov/nccoe@nist.gov)
301-975-0200

NIST SPECIAL PUBLICATION 1800-15B

Securing Small-Business and Home Internet of Things (IoT) Devices

Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)

Volume B:
Approach, Architecture, and Security Characteristics

Tim Polk
Murugiah Souppaya
NIST

Yemi Fashina
Parisa Grayeli
Joshua Klosterman
Blaine Mulugeta
Susan Symington
The MITRE Corporation

Jaideep Singh
Molex

William C. Barker
Dakota Consulting

Dean Coclin
Clint Wilson
DigiCert

Darshak Thakore
Mark Walker
CableLabs

Eliot Lear
Brian Weis
Cisco

Tim Jones
ForeScout

Drew Cohen
MasterPeace

April 2019

PRELIMINARY DRAFT

This publication is available free of charge from
<https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos>



DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-15B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-15B, 196 pages, (April 2019), CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: mitigating-iot-ddos-nccoe@nist.gov.

Public comment period: April 24, 2019 through June 24, 2019

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, Maryland 20899
Email: nccoe@nist.gov

1 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

2 The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards
3 and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and
4 academic institutions work together to address businesses' most pressing cybersecurity issues. This
5 public-private partnership enables the creation of practical cybersecurity solutions for specific
6 industries, as well as for broad, cross-sector technology challenges. Through consortia under
7 Cooperative Research and Development Agreements (CRADAs), including technology partners—from
8 Fortune 50 market leaders to smaller companies specializing in information technology security—the
9 NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity
10 solutions using commercially available technology. The NCCoE documents these example solutions in
11 the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework
12 and details the steps needed for another entity to re-create the example solution. The NCCoE was
13 established in 2012 by NIST in partnership with the State of Maryland and Montgomery County,
14 Maryland.

15 To learn more about the NCCoE, visit <https://www.nccoe.nist.gov/>. To learn more about NIST, visit
16 <https://www.nist.gov/>.

17 **NIST CYBERSECURITY PRACTICE GUIDES**

18 NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity
19 challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the
20 adoption of standards-based approaches to cybersecurity. They show members of the information
21 security community how to implement example solutions that help them align more easily with relevant
22 standards and best practices, and provide users with the materials lists, configuration files, and other
23 information they need to implement a similar approach.

24 The documents in this series describe example implementations of cybersecurity practices that
25 businesses and other organizations may voluntarily adopt. These documents do not describe regulations
26 or mandatory practices, nor do they carry statutory authority.

27 **ABSTRACT**

28 The goal of the Internet Engineering Task Force's [manufacturer usage description \(MUD\)](#) architecture is
29 for Internet of Things (IoT) devices to behave as intended by the manufacturer of the devices. This is
30 done by providing a standard way for manufacturers to identify each device's type and to indicate the
31 network communications that it requires to perform its intended function. When MUD is used, the
32 network will automatically permit the IoT device to send and receive the traffic it requires to perform as
33 intended, and it will prohibit all other communications with the device.

34 The NCCoE has demonstrated for IoT product developers and implementers the ability to ensure that
35 when an IoT device connects to a home or small-business network, MUD can be used to automatically
36 permit the device to send and receive only the traffic it requires to perform its intended function.

37 A distributed denial of service (DDoS) attack can cause significant negative impact to an organization
38 that is dependent on the internet to conduct business. A DDoS attack involves multiple computing
39 devices in disparate locations sending repeated requests to a server with the intent to overload it and
40 ultimately render it inaccessible. Recently, IoT devices have been exploited to launch DDoS attacks. IoT
41 devices may have unpatched or easily discoverable software flaws, and many have minimal security, are
42 unprotected, or are difficult to secure. A DDoS attack may result in substantial revenue losses and
43 potential liability exposure, which can degrade a company's reputation and erode customer trust.
44 Victims of a DDoS attack can include

- 45 ▪ communications service providers who may suffer service degradation that affects their
46 customers
- 47 ▪ businesses that rely on the internet who may suffer if their customers cannot reach them
- 48 ▪ IoT device manufacturers who may suffer reputational damage if their devices are being
49 exploited
- 50 ▪ users of IoT devices who may suffer service degradation and potentially incur extra costs due to
51 increased activity by their captured machines

52 Use of MUD combats these IoT-based DDoS attacks by prohibiting unauthorized traffic to and from IoT
53 devices. Even if an IoT device becomes compromised, MUD prevents it from being used in any attack
54 that would require the device to send traffic to an unauthorized destination. MUD provides a standard
55 method for access control information to be available to network control devices. This NIST
56 Cybersecurity Practice Guide shows IoT product and system providers how to integrate and use MUD to
57 help make home and small-business networks more secure. It also shows what users should expect
58 from IoT device manufacturers.

59 **KEYWORDS**

60 *botnets; internet of things; IoT; manufacturer usage description; MUD; router; server; software update*
61 *server; threat signaling.*

62 **DOCUMENT CONVENTIONS**

63 The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the
64 publication and from which no deviation is permitted.

65 The terms “should” and “should not” indicate that among several possibilities, one is recommended as
66 particularly suitable, without mentioning or excluding others, or that a certain course of action is

67 preferred but not necessarily required, or that (in the negative form) a certain possibility or course of
68 action is discouraged but not prohibited.

69 The terms “may” and “need not” indicate a course of action permissible within the limits of the
70 publication.

71 The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

72 **CALL FOR PATENT CLAIMS**

73 This public review includes a call for information on essential patent claims (claims whose use would be
74 required for compliance with the guidance or requirements in this Information Technology Laboratory
75 [ITL] draft publication). Such guidance and/or requirements may be directly stated in this ITL publication
76 or by reference to another publication. This call also includes disclosure, where known, of the existence
77 of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant
78 unexpired U.S. or foreign patents.

79 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in
80 written or electronic form, either:

- 81 1. assurance in the form of a general disclaimer to the effect that such party does not hold and
82 does not currently intend holding any essential patent claim(s); or
- 83 2. assurance that a license to such essential patent claim(s) will be made available to applicants
84 desiring to utilize the license for the purpose of complying with the guidance or requirements in
85 this ITL draft publication either:
 - 86 a. under reasonable terms and conditions that are demonstrably free of any unfair dis-
87 crimination or
 - 88 b. without compensation and under reasonable terms and conditions that are demonstra-
89 bly free of any unfair discrimination

90 Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its
91 behalf) will include in any documents transferring ownership of patents subject to the assurance,
92 provisions sufficient to ensure that the commitments in the assurance are binding on the transferee,
93 and that the transferee will similarly include appropriate provisions in the event of future transfers with
94 the goal of binding each successor-in-interest.

95 The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of
96 whether such provisions are included in the relevant transfer documents.

97 Such statements should be addressed to mitigating-iot-ddos-nccoe@nist.gov

98 **ACKNOWLEDGMENTS**

99 We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Allaukik Abhishek	ARM
Michael Bartling	ARM
Tao Wan	CableLabs
Russ Gyurek	Cisco
Peter Romness	Cisco
Rob Cantu	CTIA
Katherine Gronberg	ForeScout
Adnan Baykal	Global Cyber Alliance
Nate Lesser	MasterPeace Solutions
Tom Martz	MasterPeace Solutions
Daniel Weller	MasterPeace Solutions
Kevin Yeich	MasterPeace Solutions
Mo Alhroub	Molex
Bill Haag	NIST
Bryan Dubois	Patton Electronics

Name	Organization
Karen Scarfone	Scarfone Cybersecurity
Matt Boucher	Symantec
Bruce McCorkendale	Symantec
Yun Shen	Symantec
Pierre-Antoine Vervier	Symantec
Sarah Kinling	The MITRE Corporation
Mary Raguso	The MITRE Corporation
Allen Tan	The MITRE Corporation
Paul Watrobski	University of Maryland
Russ Housley	Vigilsec

100 The Technology Partners/Collaborators who participated in this build submitted their capabilities in
 101 response to a notice in the Federal Register. Respondents with relevant capabilities or product
 102 components were invited to sign a Cooperative Research and Development Agreement (CRADA) with
 103 NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Arm	Subject Matter Expertise
CableLabs	Micronets Gateway Service Provider Server Partner and Service Provider Server Prototype Medical Devices–Raspberry Pi

Technology Partner/Collaborator	Build Involvement
Cisco	Cisco Catalyst 3850S MUD Manager
CTIA	Subject Matter Expertise
DigiCert	Private Transport Layer Security (TLS) Certificate Premium Certificate
ForeScout	CounterACT Appliance–VCT-R Enterprise Manager–VCEM-05
Global Cyber Alliance	Subject Matter Expertise
MasterPeace Solutions	Yikes! Router Yikes! Cloud Yikes! Mobile Application
Molex	Molex light emitting diode (LED) Light Bar Molex power over ethernet (PoE) Gateway
Patton Electronics	Session Border Controller—SN5301/4B/EUI
Symantec	Subject Matter Expertise

104 **Contents**

105 **1 Summary..... 1**

106 1.1 Challenge..... 1

107 1.2 Solution..... 2

108 1.3 Benefits..... 2

109 **2 How to Use This Guide 3**

110 2.1 Typographic Conventions..... 4

111 **3 Approach..... 5**

112 3.1 Audience..... 6

113 3.2 Scope 6

114 3.3 Assumptions..... 6

115 3.4 Risk Assessment 7

116 3.4.1 Threats 8

117 3.4.2 Vulnerabilities 8

118 3.4.3 Risk..... 9

119 **4 Architecture 10**

120 4.1 Logical Architecture..... 10

121 4.2 Physical Architecture..... 11

122 4.3 Technologies..... 13

123 4.3.1 MUD Manager..... 17

124 4.3.2 MUD File Server 18

125 4.3.3 MUD File 18

126 4.3.4 DHCP Server 19

127 4.3.5 Router/Switch 20

128 4.3.6 Certificates 20

129 4.3.7 IoT Devices 21

130 4.3.8 Update Server 23

131 4.3.9 Unapproved Server 23

132 4.3.10 MQTT Broker Server23

133 4.3.11 IoT Device Discovery23

134 4.4 Build Demonstration 25

135 **5 Security Characteristic Analysis 31**

136 5.1 Assumptions and Limitations 31

137 5.2 Security Control Map..... 31

138 5.3 Scenarios 40

139 5.3.1 Scenario 1: No MUD Protection.....41

140 5.3.2 Scenario 2: MUD Protection from External Threats41

141 5.3.3 Scenario 3: MUD Protection from External and Internal Threats.....42

142 5.4 Build Evaluation..... 43

143 **6 Findings and Recommendations..... 51**

144 6.1 Findings..... 51

145 6.2 Security Considerations..... 55

146 6.3 Recommendations..... 58

147 **7 Future Build Considerations 60**

148 7.1 Extension to Demonstrate the Growing Set of Available Components..... 61

149 7.2 Recommended Demonstration of IPv6 Implementation..... 61

150 **Appendix A Information Provided by Collaborators Related to Phase 2.. 62**

151 A.1 MasterPeace..... 62

152 A.1.1 Yikes!.....62

153 A.1.2 Yikes! Components63

154 A.1.3 Requirements.....64

155 A.1.4 Known Limitations65

156 A.2 CableLabs..... 65

157 A.2.1 CableLabs Micronets.....65

158 **Appendix B List of Acronyms 68**

159 **Appendix C Definitions..... 70**

160 **Appendix D Functional Evaluation Plan 74**

161 D.1 Build 1..... 74

162 D.1.1 Build 1 Requirements.....74

163 D.1.2 Build 1 Test Cases.....96

164 D.1.3 Build 1 MUD Files.....162

165 **Appendix E References..... 182**

166 E.1 Core Standards 182

167 E.2 Ongoing MUD Standards Activities 182

168 E.3 Secure Update Standards..... 182

169 E.4 Industry Best Practices for Software Quality 183

170 E.5 Best Practices for Identification and Authentication 183

171 E.6 Cryptographic Standards and Best Practices 183

172 E.7 Risk, Risk Assessment, and Risk Management Guidance..... 184

173 **List of Figures**

174 **Figure 4-1 Logical Architecture 11**

175 **Figure 4-2 Physical Architecture..... 13**

176 **Figure 4-3 Methods the ForeScout Platform Can Use to Discover and Classify IP-Connected Devices . 24**

177 **Figure 4-4 Classify IoT Devices by Using the ForeScout Platform 25**

178 **Figure 4-5 Logical Architecture–Build 1 26**

179 **Figure 4-6 Physical Architecture–Build 1 28**

180 **Figure 4-7 Process Flow–Build 1..... 29**

181 **Figure 5-1 No MUD Protection Threat Scenario 41**

182 **Figure 5-2 MUD Protection from External Threats Scenario 42**

183 **Figure 5-3 MUD Protection from External and Internal Threats Scenario..... 43**

184 **Figure A-1 Yikes! Architecture 63**

185 **Figure A-2 Micronets Reference Architecture..... 66**

186 **List of Tables**

187 **Table 4-1 Products and Technologies** 14

188 **Table 5-1 Mapping Demonstration Platform Characteristics to NIST Interagency/Internal Report 8228**
189 **Expectations, NIST SP 800-53 Controls, and Cybersecurity Framework Subcategories** 32

190 **Table 5-2 Mapping Project Objectives to the Cybersecurity Framework and Informative Security**
191 **Control References** 36

192 **Table 5-3 Summary of Functional Tests**..... 43

193 **Table D-1: Functional IoT Use Case Requirements** 74

194 **Table D-2: Test Case Fields** 96

195 **Table D-3: Test Case IoT-1-v4**..... 99

196 **Table D-4: Test Case IoT-2-v4**..... 105

197 **Table D-5: Test Case IoT-3-v4**..... 109

198 **Table D-6: Test Case IoT-4-v4**..... 114

199 **Table D-7: Test Case IoT-5-v4**..... 120

200 **Table D-8: Test Case IoT-6-v4**..... 125

201 **Table D-9: Test Case IoT-7-v4**..... 133

202 **Table D-10: Test Case IoT-8-v4**..... 136

203 **Table D-11: Test Case IoT-9-v4**..... 138

204 **Table D-12: Test Case IoT-10-v4**..... 141

205 **Table D-13: Test Case IoT-11-v4** 145

206 **Table D-14: Test Case IoT-12-v4** 146

207 **Table D-15: Test Case IoT-13-v4** 155

208 **Table D-16: Test Case IoT-14-v4**..... 158

209 1 Summary

210 The [Manufacturer Usage Description \(MUD\) Specification \(Request for Comments \[RFC\] 8520\)](#) provides
211 a means for IoT devices to signal to networks what sort of access and network functionality they require
212 to properly function. The objective of this project is to show how IoT product and system manufacturers
213 can use MUD to reduce the vulnerability of Internet of Things (IoT) devices to botnets and other
214 automated distributed threats while limiting the utility of any compromised IoT devices to malicious
215 actors. This volume describes the approach adopted for the project, the laboratory architecture
216 demonstrated by the project, and the security characteristics demonstrated in the laboratory
217 environment. The primary technical elements of this project include MUD-capable network
218 gateways/routers supporting wired and wireless network access, MUD managers, MUD file servers,
219 MUD-capable Dynamic Host Configuration Protocol (DHCP) servers, update servers, and threat signaling
220 servers. We used personal computing devices, business computing devices, and both MUD-capable and
221 non-MUD-capable IoT devices to demonstrate the security benefits provided by MUD. MUD will not
222 provide perfect security, but it will significantly increase the effort required by malicious actors to
223 compromise and exploit IoT devices on a home or small-business network. The scenarios examined by
224 this National Cybersecurity Center of Excellence (NCCoE) project involve IoT devices being onboarded
225 and used on home and small-business networks, where plug-and-play deployment is required. The
226 example solution network includes MUD-capable IoT devices that interact with external systems to
227 access secure updates and various cloud services, in addition to interacting with traditional personal
228 computing devices, as permitted by their MUD files. The IoT devices used include smart lighting
229 controllers, cameras, smartphones, printers, baby monitors, digital video recorders, and smart
230 assistants.

231 1.1 Challenge

232 The term *IoT* is often applied to the aggregate of single-purpose, internet-connected devices, such as
233 thermostats, security monitors, lighting control systems, and smart television sets. The IoT is
234 experiencing what some might describe as hypergrowth. [Gartner](#) predicts there will be 20.4 billion
235 connected IoT devices by 2020 compared with 8.4 billion in 2017, while [Forbes](#) forecasts the market to
236 be \$457 billion by 2020 (a 28.5 percent compounded annual growth rate). As connected devices
237 become more commonplace in homes and businesses, security concerns are also increasing. Many full-
238 featured devices such as web servers, personal or business computers, and mobile devices often have
239 state-of-the-art security software protecting them from most known threats. Conversely, many IoT
240 devices are challenging to secure because they are designed to be inexpensive and to perform a single
241 function—resulting in processing, timing, memory, and power constraints. Nevertheless, the
242 consequences of not addressing security concerns of connected devices can be catastrophic. For
243 instance, in typical networking environments, malicious actors can detect an IoT device within minutes
244 of it being connected and then launch an attack on that same device from any system on the internet,

245 unbeknownst to the user. They can also commandeer a group of compromised devices, called a botnet,
246 to launch large-scale attacks.

247 **1.2 Solution**

248 This project demonstrates an approach to significantly strengthen security while deploying IoT devices
249 in home and small-business networks. This approach can help bolster the resiliency of IoT devices and
250 prevent them from being used as platforms from which to mount DDoS attacks across the internet.

251 The NCCoE sought existing technologies that use the [MUD Specification \(Request for Comments \[RFC\]
252 8520\)](#) to permit an IoT device to signal to the network what sort of access and network functionality it
253 requires to properly operate. Constraining the communication abilities of exploited IoT devices reduces
254 the potential for the devices to be used in attacks—both DDoS attacks that could be launched across
255 the internet and attacks on the IoT device’s local network that could have security consequences. This
256 practice guide explains how to effectively implement the MUD specification for MUD-capable IoT
257 devices and envisions methods for preventing non-MUD-capable IoT devices from connecting to
258 potentially malicious entities that use threat signaling technology.

259 **1.3 Benefits**

260 This project provides benefits to several different types of stakeholders:

- 261 ▪ Communications service providers will benefit from reduction of the set of IoT devices that can
262 be easily used by “bad actors” to participate in DDoS attacks against their networks and
263 thereby degrade service for their customers.
- 264 ▪ Organizations and others who use the internet, including businesses that rely on their
265 customers being able to reach them over the internet, as well as critical infrastructures and
266 other public and private sector institutions, will benefit from improved confidence in internet
267 availability and performance due to reductions in network-based attacks.
- 268 ▪ IoT device manufacturers will benefit by avoiding reputational damage that they might suffer if
269 their devices could be easily exploited to conduct DDoS attacks.
- 270 ▪ Users of IoT devices, including small businesses and homeowners, will benefit from improved
271 understanding of how to find and use the set of tools available to protect their internal
272 networks from being subverted by bad actors and of how to reduce the threats to their
273 businesses that can result from such subversion. By protecting their networks, they also avoid
274 suffering increased costs and bandwidth saturation that could result from having their
275 machines captured and used to launch network-based attacks.

276 2 How to Use This Guide

277 This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a
278 standards-based reference design and provides users with the information they need to replicate
279 deployment of the MUD protocol to mitigate IoT-based DDoS threats. This reference design is modular
280 and can be deployed in whole or in parts.

281 This guide contains three volumes:

- 282 ▪ NIST Special Publication (SP) 1800-15A: *Executive Summary*
- 283 ▪ NIST SP 1800-15B: *Approach, Architecture, and Security Characteristics*—what we built and why
284 **(you are here)**
- 285 ▪ NIST SP 1800-15C: *How-To Guides*—instructions for building the example solution

286 Depending on your role in your organization, you might use this guide in different ways:

287 **Business decision makers, including chief security and technology officers**, will be interested in the
288 *Executive Summary* (NIST SP 1800-15A), which describes the:

- 289 ▪ challenges that enterprises face in mitigating IoT-based DDoS threats
- 290 ▪ example solution built at the NCCoE
- 291 ▪ benefits of adopting the example solution

292 **Technology or security program managers** who are concerned with how to identify, understand, assess,
293 and mitigate risk will be interested in this part of the guide, NIST SP 1800-15B, which describes what we
294 did and why. The following sections will be of particular interest:

- 295 ▪ Section 3.4.3, Risk, provides a description of the risk analysis we performed.
- 296 ▪ Section 5.2, Security Control Map, maps the security characteristics of this example solution to
297 cybersecurity standards and best practices.

298 You might share the *Executive Summary*, NIST SP 1800-15A, with members of your leadership team to
299 help them understand the importance of adopting use of standards-based mitigation of network-based
300 distributed denial of service using MUD protocols.

301 **IT professionals** who want to implement an approach like this will find the whole practice guide useful.
302 You can use the how-to portion of the guide, NIST SP 1800-15C, to replicate all or parts of the build
303 created in our lab. The how-to guide provides specific product installation, configuration, and
304 integration instructions for implementing the example solution. We do not re-create the product
305 manufacturers' documentation, which is generally widely available. Rather, we show how we
306 incorporated the products together in our environment to create an example solution.

307 This guide assumes that information technology (IT) professionals have experience implementing
 308 security products within the enterprise. While we have used a suite of commercial products to address
 309 this challenge, this guide does not endorse these particular products. Your organization can adopt this
 310 solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point
 311 for tailoring and implementing parts of the MUD protocol. Your organization’s security experts should
 312 identify the products that will best integrate with your existing tools and IT system infrastructure. We
 313 hope you will seek products that are congruent with applicable standards and best practices. Section
 314 4.3, Technologies, lists the products we used, and Section 5.2 maps them to the cybersecurity controls
 315 provided by this reference solution.

316 A NIST Cybersecurity Practice Guide does not describe “the” solution, but a possible solution. This is a
 317 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and
 318 success stories will improve subsequent versions of this guide. Please contribute your thoughts to mitigating-iot-ddos-nccoe@nist.gov.
 319

320 2.1 Typographic Conventions

321 The following table presents typographic conventions used in this volume.

Typeface/ Symbol	Meaning	Example
<i>Italics</i>	file names and pathnames; references to documents that are not hyperlinks; new terms; and placeholders	For detailed definitions of terms, see the <i>NCCoE Glossary</i> .
Bold	names of menus, options, command buttons, and fields	Choose File > Edit .
Monospace	command-line input, onscreen computer output, sample code examples, status codes	Mkdir
Monospace Bold	command-line user input contrasted with computer output	service sshd start

Typeface/ Symbol	Meaning	Example
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov .

322 **3 Approach**

323 The NCCoE invited technology providers to participate in demonstrating a proposed approach for
 324 deployment of consumer and commercial IoT devices in home and small-business networks in a manner
 325 that provides significantly higher security than is typically achieved in today's environments. In this
 326 project, current and emerging network standards are applied to home and business networks that are
 327 composed of both IoT and fully featured devices (e.g., personal computers and mobile devices) to
 328 constrain communications-based malware exploits. Network gateway components and security-aware
 329 IoT devices leverage the [MUD Specification \(RFC 8520\)](#) to permit a MUD-capable IoT device to signal to
 330 the network what sort of access and network functionality it requires to properly operate. The resulting
 331 access control capability reduces the potential for exploited MUD-capable IoT devices to be used in a
 332 DDoS attack by constraining their communication abilities. In addition, network components could in
 333 the future implement network-wide access controls based on threat signaling to protect legacy IoT
 334 devices, MUD-capable IoT devices, and fully featured devices (e.g., personal computers). Automatic
 335 secure update controls are implemented on all devices used in this project, and they support secure
 336 administrative access. (Note that software update formats for IoT devices are not currently
 337 standardized. NCCoE experiences with software update strategies will be contributed to emerging
 338 standardization activities.)

339 The NCCoE prepared a *Federal Register* Notice seeking technology providers to provide products and/or
 340 expertise to compose prototypes that include MUD-capable routers or switches; MUD managers; MUD
 341 file servers; MUD-capable DHCP servers; IoT devices capable of both inserting the MUD uniform
 342 resource locator (URL) into DHCP address requests and requesting, verifying, and applying software
 343 updates; update servers; and threat signaling servers. Cooperative Research and Development
 344 Agreements (CRADAs) were established with qualified respondents, and build teams were assembled.
 345 The build teams fleshed out the initial architecture, and the collaborators' components were composed
 346 into example implementations. The build team documented the architecture and design
 347 implementation. As the build progressed, the team documented the steps taken to install and configure
 348 each component of the demonstration environment. The team then conducted functional testing of the
 349 demonstration environment, including demonstrating software update processes and responses to
 350 attempts to perform prohibited communications. The team conducted and documented the results of a
 351 risk assessment and a security characteristics analysis, including mapping the security contributions of

352 the demonstrated capability to the *Framework for Improving Critical Infrastructure Cybersecurity*
353 ([Cybersecurity Framework](#)) and other relevant standards. Finally, the NCCoE worked with industry
354 collaborators to suggest future considerations for mitigating IoT-based DDoS threats.

355 3.1 Audience

356 The focus of this project is on home and small-business deployments. This guide is intended for

- 357 ▪ IoT device manufacturers, sensor manufacturers, networking companies, and industry groups
- 358 ▪ internet service providers (ISPs), venture capitalists, and Smart Cities interests
- 359 ▪ standards development organizations such as the Internet Engineering Task Force
360 (IETF), foreign government organizations, and state/local governments having IoT authority
361 and standards

362 3.2 Scope

363 The objective of this project is to demonstrate a proposed approach for deployment of IoT devices in
364 home and small-business networks in a manner that provides significantly higher security than is
365 typically achieved in today's IoT environments. The scope of this NCCoE project includes both home and
366 small-business applications where plug-and-play deployment is required. The demonstration prototype
367 network includes MUD-capable IoT devices that interact with external systems to access secure updates
368 and various cloud services, in addition to interacting with traditional personal computing devices, as
369 permitted by their MUD files. It employs both MUD-capable and non-MUD-capable IoT devices, such as
370 smart lighting controllers, cameras, smartphones, printers, baby monitors, digital video recorders, and
371 smart assistants.

372 3.3 Assumptions

373 The primary technical elements of a MUD-capable home and small-business IoT system include

- 374 ▪ MUD managers
- 375 ▪ MUD file servers
- 376 ▪ MUD file and corresponding signature file
- 377 ▪ MUD-capable DHCP servers
- 378 ▪ MUD-capable routers or switches supporting wired and wireless network access
- 379 ▪ MUD-capable IoT devices
- 380 ▪ non-MUD-capable (legacy) IoT devices
- 381 ▪ personal computing devices (personal computers, tablets, and phones)
- 382 ▪ business computing devices

- 383 ▪ update servers

384 Cost is a major factor affecting consumer purchasing decisions and consequent product development
385 decisions.

386 MUD-capable IoT devices deployed in environments that incorporate the networking and best practice
387 controls included in this project should be able to only send traffic to and receive traffic from
388 preapproved devices, such as associated cloud-based services or update servers. A malicious actor
389 would need to compromise the professionally operated cloud service or update server to detect or
390 launch an attack, and each compromise would apply only to devices that are designed to communicate
391 with the compromised service or update server. Best practices for administrative access and security
392 updates would reduce the success rate for attempted compromises. Previously long-lived vulnerabilities
393 (global administrative passwords) or short-lived vulnerabilities (known vulnerabilities subject to security
394 updates) would be unavailable. As a result, the malicious actor would be forced to use expensive zero-
395 day attacks or socially engineered administrative passwords, which are not scalable. If an IoT device is
396 compromised despite these controls, virtual network segmentation can prevent lateral movement
397 within the home/enterprise or prevent attacking systems outside the preapproved list; in this situation,
398 control of the IoT device would be of dubious value. Obtaining value from a compromised device would
399 demand the additional step of integrity attacks on the list of approved communicating devices. That is,
400 attacking *www.example.com* with a botnet of thermostats would require modifying the product
401 vendor’s list of approved communicating devices to indicate that thermostats should be allowed to
402 communicate with *www.example.com*.

403 **3.4 Risk Assessment**

404 [NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*](#), states that risk is “a measure of the
405 extent to which an entity is threatened by a potential circumstance or event, and typically a function of:
406 (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of oc-
407 currence.” The guide further defines risk assessment as “the process of identifying, estimating, and pri-
408 oritizing risks to organizational operations (including mission, functions, image, reputation), organiza-
409 tional assets, individuals, other organizations, and the Nation, resulting from the operation of an infor-
410 mation system. Part of risk management incorporates threat and vulnerability analyses, and considers
411 mitigations provided by security controls planned or in place.”

412 The NCCoE recommends that any discussion of risk management, particularly at the enterprise level,
413 begins with a comprehensive review of [NIST SP 800-37 Revision 2, *Risk Management Framework for In-*](#)
414 [formation Systems and Organizations: A System Life Cycle Approach for Security and Privacy](#), material
415 that is available to the public. The [risk management framework \(RMF\)](#) guidance as a whole proved inval-
416 uable in giving us a baseline to assess risks, from which we developed the project, the security charac-
417 teristics of the build, and this guide.

418 According to CNSSI No. 4009, *Committee on National Security Systems (CNSS) Glossary*, risk manage-
419 ment is “the program and supporting processes to manage information security risk to organizational
420 operations (including mission, functions, image, reputation), organizational assets, individuals, other or-
421 ganizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) as-
422 sessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.” *Considerations*
423 *for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, NIST Interagency/Internal Report
424 (NISTIR) 8228, identified security and privacy considerations and expectations that, together with the
425 *Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)* and *Security*
426 *and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53)*, informed our
427 risk assessment and subsequent recommendations from which we developed the security characteris-
428 tics of the build, and this guide.

429 3.4.1 Threats

430 Historically, internet devices have enjoyed full connectivity at the network and transport layers. Any pair
431 of devices with valid internet protocol (IP) addresses was, in general, able to communicate by using
432 transmission control protocol (TCP) for connection-oriented communications or User Datagram Protocol
433 (UDP) for connectionless protocols. Full connectivity was a practical architectural option for fully
434 featured devices (e.g., servers and personal computers) because the identity of communicating hosts
435 depended largely on the needs of inherently unpredictable human users. Requiring a reconfiguration of
436 hosts to permit communications to meet the needs of system users as they evolved was not a scalable
437 solution. However, a combination of whitelisting device capabilities and blacklisting devices or domains
438 that are considered suspicious allowed network administrators to mitigate some threats.

439 With the evolution of internet hosts from multiuser systems to personal devices, this security
440 posture became impractical, and the emergence of the IoT has made it unsustainable. In typical
441 networking environments, a malicious actor can detect an IoT device and launch an attack on that
442 device from any system on the internet. Once compromised, that device can be used to attack any
443 other system on the internet. Anecdotal evidence indicates that a new device will be detected and will
444 experience its first attack within minutes of deployment. Because the devices being deployed often
445 have known security flaws, the success rate for the compromise of detected systems is very high.
446 Typically, malware is designed to compromise a list of specific devices, making such attacks very
447 scalable. Once compromised, an IoT device can be used to compromise other internet-connected
448 devices, launch attacks on any victim device on the internet, or move laterally within the local network
449 hosting the device.

450 3.4.2 Vulnerabilities

451 The vulnerability of IoT devices in this environment is a consequence of full connectivity, exacerbated by
452 the large number of security vulnerabilities in today’s complex software systems. Currently accepted
453 coding practices result in approximately one software bug for every one thousand lines of code, and

454 many of these bugs create security vulnerabilities. Modern systems ship with millions of lines of code,
455 creating a target-rich environment for malicious actors. Although some vendors provide patches for
456 security vulnerabilities and an efficient means for securely updating their products, patches are often
457 unavailable or nearly impossible to install on many other products, including many IoT devices. Poorly
458 implemented default configuration baselines and administrative access controls, such as hard-coded or
459 widely known default passwords, provide a large attack surface for malicious actors. Once again, IoT
460 devices are particularly vulnerable. The Mirai malware relied heavily on hard-coded administrative
461 access to assemble botnets consisting of more than 100,000 devices.

462 3.4.3 Risk

463 The demonstrated capability implements a set of protocols designed to permit users and product
464 support staff to constrain access to IoT devices. Implementation for some but not all IoT components in
465 a system mitigates only the threat based on subversion of those devices. The system as a whole remains
466 vulnerable. A residual risk is that the implementation of the demonstrated capability may be
467 prophylactic only. It does not necessarily permit owners to find, identify, and correct already-
468 compromised systems without replacing or reprogramming existing system components.

469 For example, if a system is compromised so that it emits a new URL referencing a MUD file that permits
470 malicious actors to send traffic to and from the IoT device, MUD may not be able to help owners detect
471 such compromised systems and stop the communications that should be prohibited. However, if a
472 system is compromised but it is still emitting the correct MUD URL, MUD can detect and stop any
473 unauthorized communications that the device attempts. Such attempts would also indicate potential
474 compromises.

475 If a network is set up so that it uses legacy IoT devices that do not emit MUD URLs, these devices could
476 be associated with MUD files by connecting the devices to specific ports and associating each port with
477 a MUD file appropriate to the device. If the device is compromised and attempts unauthorized
478 communication, the attempt should be detected. That is, the device would still be subjected to the
479 constraints specified in its MUD file. Under these circumstances, MUD can permit the owner to find and
480 identify already-compromised systems. Moreover, where threat signaling is employed, a compromised
481 system that reaches back to a known bad internet protocol (IP) address can be detected, and the
482 connection can be refused.

483 **4 Architecture**

484 The project architecture is intended for home and business networks that are composed of both IoT
485 (e.g., single-purpose) and fully featured devices (e.g., personal computers and mobile devices) to
486 constrain communications-based malware exploits. The architecture is designed to provide three forms
487 of protection:

- 488 ▪ use of the MUD specification to permit a MUD-capable IoT device to signal to the network
489 what sort of access and network functionality it requires to properly operate, thereby reducing
490 the potential for the device to be used in a DDoS attack
- 491 ▪ use of network-wide access controls based on threat signaling to protect legacy (non-MUD-
492 capable) IoT devices and fully featured devices in addition to MUD-capable devices
- 493 ▪ automatic secure software updates to all devices to ensure that operating system (OS) patches
494 are installed promptly

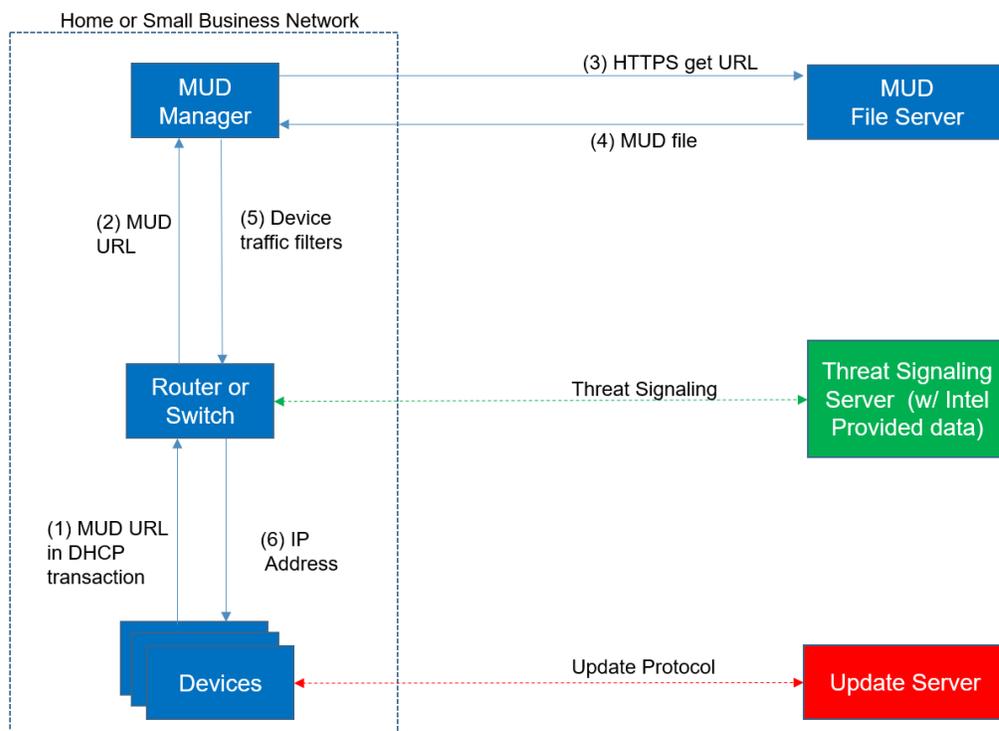
495 **4.1 Logical Architecture**

496 Figure 4-1 depicts the logical architecture. A new functional component, the MUD manager, is
497 introduced into the home or enterprise network to augment the existing networking functionality
498 offered by the router or switch: address assignment and control of access to devices.

499 IoT devices insert the MUD URL into DHCP address requests that they generate when they attach to the
500 network (e.g., when powered on). The MUD URL is passed to the MUD manager, which retrieves a MUD
501 file from the designated website (denoted as the MUD file server) using https. The MUD file describes
502 the communications requirements for this device; the MUD manager converts the requirements into
503 traffic filters (e.g., access control lists—ACLs) that are installed on the router or switch to enforce access
504 controls on the network. This enables the router or switch to deny traffic sent to or from the IoT device
505 that is outside the device’s communications profile.

506 To provide further security, periodic updates are incorporated into the architecture. IoT devices
507 periodically contact the appropriate update server to download and apply security patches. To ensure
508 that such updates are possible, the IoT device’s MUD file must explicitly permit the IoT device to receive
509 traffic from the update server.

510 The router or switch could also periodically receive threat feeds from the threat signaling server to use
511 as a basis for restricting certain types of network traffic. For example, malicious traffic can be denied
512 access to a device by a cloud-based or infrastructure service like domain name system (DNS), with
513 detailed threat information, including type, severity, and mitigation available to the router or switch on
514 demand. (Note that although threat signaling is part of the logical architecture, it is not part of the
515 current build. Threat signaling is planned for inclusion in a later phase of the project.)

516 **Figure 4-1 Logical Architecture**

517

518 Note that communications between the MUD manager and router/switch, between the threat signaling
 519 server and router/switch, and between IoT devices and the corresponding update server are not
 520 standardized.

521 The components of this architecture will not provide perfect security, but they will significantly increase
 522 the effort required by malicious actors to compromise and exploit IoT devices on a home or small-
 523 business network.

524 The components shown in the high-level architecture are described in Section 4.3 below.

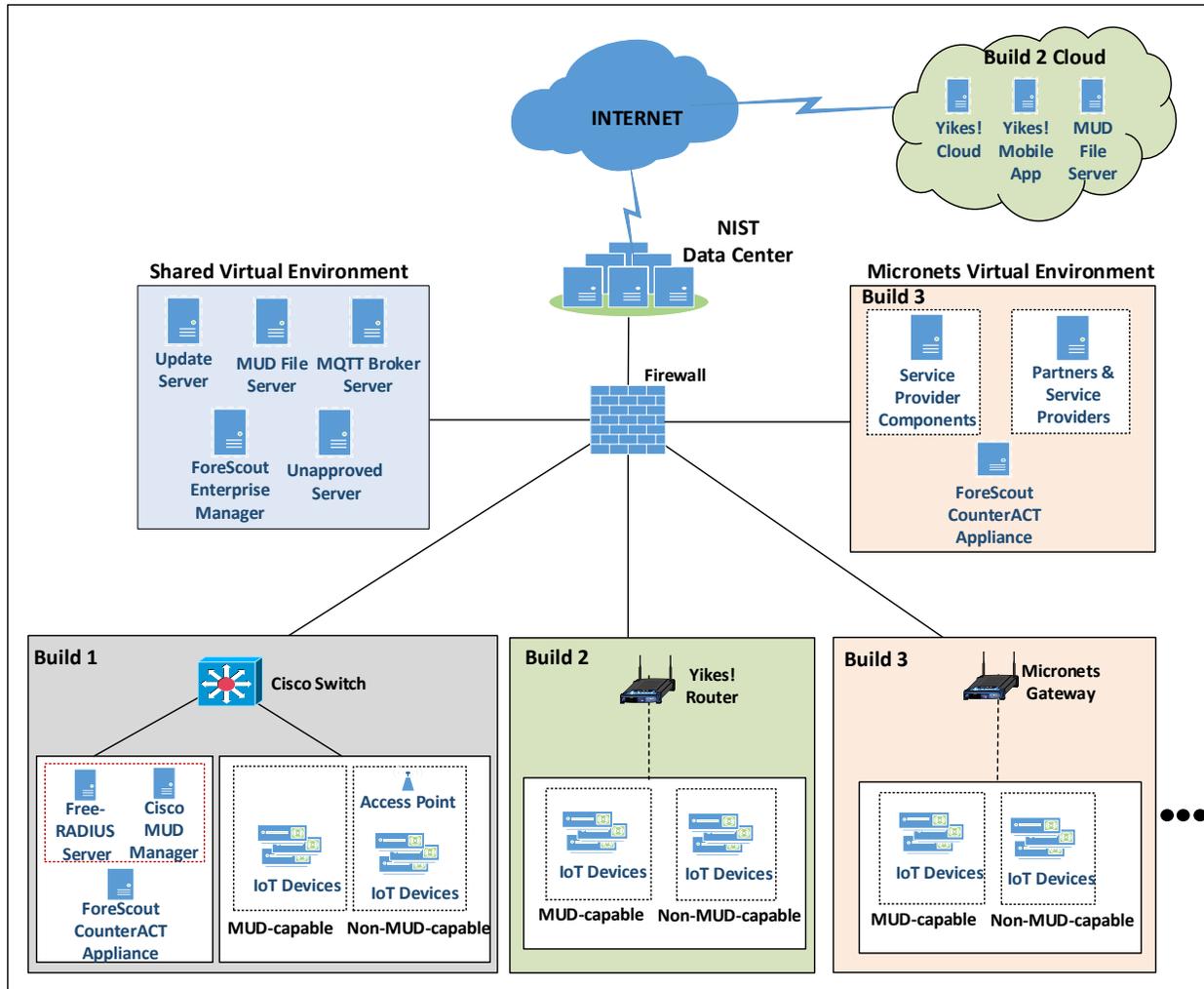
525 4.2 Physical Architecture

526 Figure 4-2 depicts the high-level physical architecture of the NCCoE laboratory implementation. This
 527 implementation supports the flexibility to implement additional builds in the future. As depicted, the
 528 NCCoE laboratory network is connected to the internet via the NIST data center. Access to and from the
 529 NCCoE network is protected by a firewall. The NCCoE network includes a virtual environment that
 530 houses an update server, a MUD file server, an unapproved server (i.e., a server that is not listed as a
 531 permissible communications source or destination in any MUD file), a Message Queuing Telemetry
 532 Transport (MQTT) Broker Server, and ForeScout Enterprise Manager. (Note that although threat

533 signaling is part of the logical architecture, there is currently no threat signaling server included in the
534 laboratory network's virtual environment; threat signaling is planned for inclusion in a later phase of the
535 project.) These components are hosted at NCCoE and will be used across builds. The Transport Layer
536 Security (TLS) certificate and Premium certificate used by the MUD file server are provided by DigiCert.

537 Only Build 1, as depicted in the diagram, has been implemented during this phase of the project. Build 2
538 and Build 3 will be part of the next phase of the project. Build 1 network components consist of a Cisco
539 Catalyst 3850-S switch, a Cisco MUD Manager, a FreeRADIUS Server, and a virtualized ForeScout
540 CounterACT appliance. IoT devices used in this architecture include both MUD-capable and non-MUD-
541 capable IoT devices. The MUD-capable IoT devices for Build 1 include Raspberry Pi, Artik, u-blox, Intel
542 UP Squared, and the Molex Light Engine controlled by Power Over Ethernet (PoE) Gateway. Non-MUD-
543 capable devices chosen for Build 1 include a wireless access point, cameras, a printer, smartphones,
544 lighting devices, a smart assistant device, a baby monitor, and a digital video recorder. Build 1 and the
545 role that each of its components plays in the architecture are explained in more detail in Section 4.3 and
546 Section 4.4.

547 **Figure 4-2 Physical Architecture**



548

549 **4.3 Technologies**

550 Table 4-1 lists all the products and technologies used in this project and provides a mapping among the
 551 generic component term, the specific product used to implement that component, and the security
 552 control(s) that the product provides. Some functional Subcategories are described as being directly
 553 provided by a component. Others are described as Subcategories, the provision of which is supported
 554 by a component but not directly provided by a component. Refer to Table 5-1 for an explanation of the
 555 Cybersecurity Framework’s Subcategory codes.

556 Table 4-1 Products and Technologies

Component	Product	Function	Cybersecurity Framework Subcategories
MUD manager	Cisco MUD Manager (Open Source) and a FreeRADIUS Server	Fetches, verifies, and processes MUD files from the MUD file server; configures router or switch with traffic filters to enforce access control based on the MUD file	Provides: PR.PT-3 Supports: ID.AM-1 ID.AM-2 ID.AM-3 PR.AC-4 PR.AC-5 PR.DS-5 DE.AE-1
MUD file server	NCCoE-hosted Apache server	Hosts MUD files; serves MUD files to the MUD Manager by using https	ID.AM-1 ID.AM-2 ID.AM-3 PR.AC-4 PR.AC-5 PR.DS-5 PR.PT-3 DE.AE-1
MUD file maker	MUD File Maker (https://www.mud-maker.org/)	YANG script GUI used to create MUD files	ID.AM-1
MUD file	A YANG model instance that has been serialized in javascript object notation (JSON) [RFC7951]. The manufacturer of a MUD-capable device creates that device’s MUD file. MUD file maker (see previous row) can be used to create MUD files. Each MUD file is also associated with a separate MUD signature file.	Specifies the communications that are permitted to and from a given device	Provides: PR.PT-3 Supports: ID.AM-1 ID.AM-2 ID.AM-3

Component	Product	Function	Cybersecurity Framework Subcategories
DHCP server	Cisco IOS (Catalyst 3850-S)	Dynamically assigns IP addresses; recognizes MUD URL in DHCP DISCOVER; should notify MUD manager if the device's IP address lease expires or has been released	ID.AM-3 PR.AC-4 PR.AC-5 PR.DS-5 PR.PT-3 DE.AE-1
Link Layer Discovery Protocol (LLDP)	Cisco IOS (Catalyst 3850-S)	Supports capability for devices to advertise their identity and capabilities to neighbors on a local area network (LAN) segment; provides capability to receive MUD URL in IoT device LLDP Type Length Value (TLV) frame as an extension	ID.AM-1
Router or switch	Cisco Catalyst 3850-S (IOS XE software version 16.09.02)	Provides MUD URL to MUD manager; gets configured by the MUD manager to enforce the IoT device's communication profile; performs per-device access control	ID.AM-3 PR.AC-4 PR.AC-5 PR.DS-5 PR.PT-3 DE.AE-1
Certificates	DigiCert Certificates (TLS and Premium)	Authenticates MUD file server and secures TLS connection between MUD manager and MUD file server; used to sign MUD files and generate corresponding signature file	PR.AC-1 PR.AC-3 PR.AC-5 PR.AC-7

Component	Product	Function	Cybersecurity Framework Subcategories
MUD-capable IoT device	Raspberry Pi Model 3B (Devkit) u-blox C027-G35 (Devkit) Samsung ARTIK 520 (Devkit) Intel UP Squared Grove (Devkit) Molex PoE Gateway and Light Engine	Emits a MUD URL as part of its DHCP DISCOVER; requests and applies software updates	ID.AM-1
Non-MUD-capable IoT device	Cameras Smartphones Smart lighting devices Smart assistant Printer Baby monitor Wireless access point Digital video recorder	Acts as typical IoT devices on a network; creates network connections to cloud services	ID.AM-1
Update server	NCCoE-hosted Apache server Molex Update Agent	Provides patches and other software updates	PR.IP-1 PR.IP-3
Unapproved server	NCCoE-hosted Apache server	Acts as an internet host that has not been explicitly approved in a MUD file	DE.DP-3 DE.AM-1

Component	Product	Function	Cybersecurity Framework Subcategories
MQTT Broker Server	NCCoE-hosted MQTT server	Receives and publishes messages to/from clients	ID.AM-3 DE.AE-3
IoT Device Discovery	ForeScout CounterACT Virtual Appliances and Enterprise Manager	Discovers IoT devices on network	ID.AM-1 PR.IP-1 DE.AM-1

557 Each of these components is described more fully in the following sections.

558 4.3.1 MUD Manager

559 The MUD manager is a key component of the architecture. It fetches, verifies, and processes MUD files
560 from the MUD file server. It then configures the router or switch with an access list to control
561 communications based on the contents of the MUD files.

562 4.3.1.1 Cisco MUD Manager

563 The Cisco MUD Manager is an open-source implementation. For this project, the Cisco MUD Manager
564 was used to support IoT devices that emit their MUD URLs via DHCP messages and other IoT devices
565 that emit their MUD URLs via the IEEE 802.1AB LLDP. The Cisco MUD Manager is supported by an open-
566 source implementation of an authentication, authorization, and accounting (AAA) server that
567 communicates by using the remote authentication dial-in user service (RADIUS) protocol (i.e., a RADIUS
568 server) called FreeRADIUS. When the MUD URL is emitted via DHCP or LLDP, it is extracted from the
569 corresponding message, and the switch thereafter provides these MUD URLs to the MUD manager via
570 RADIUS messages. The MUD manager then retrieves MUD files associated with those URLs and
571 configures the Catalyst 3850-S switch to enforce the IoT devices' communication profiles based on these
572 MUD files. The switch implements an IP access control list -based policy for src-dnsname, dst-dnsname,
573 my-controller, and controller constructs that are specified in the MUD file, and it uses virtual local area
574 network (VLANs) to enforce same-manufacturer, manufacturer, and local-networks constructs that are
575 specified in the MUD file. The system supports both lateral "east-west" protection and appropriate
576 access to internet sites ("north-south" protection).

577 When supporting MUD URL emission by LLDP TLV, LLDP TLV must be enabled on both the Cisco switch
578 and the IoT device. A policy-map configuration and a corresponding template are used to cause MAC
579 Authentication Bypass (MAB) to happen. This will trigger an access-session attribute that will cause LLDP
580 TLVs (including the MUD URL) to be forwarded in an accounting message to the RADIUS server.

581 Some manual preconfiguration of VLANs on the switch is required. The Cisco MUD Manager supports a
582 default policy for IPv4. It implements a static mapping between domain names and IP addresses inside a
583 configuration file.

584 The version of the Cisco MUD Manager used in this project is a proof-of-concept implementation that is
585 intended to introduce advanced users and engineers to the MUD concept. It is not a fully automated
586 MUD manager implementation, and some protocol features are not present. These are described in
587 Section 6.1, Findings.

588 4.3.2 MUD File Server

589 In the absence of a commercial MUD manager for use in this project, the NCCoE implemented its own
590 MUD file server by using an Apache web server. This file server signs and stores the MUD files along
591 with their corresponding signature files for the IoT devices used in the project. Upon receiving a “GET”
592 request for the MUD files and signatures, it serves the request to the MUD manager by using https.

593 4.3.3 MUD File

594 Using the MUD file maker component referenced above in Table 4-1, it is possible to create a MUD file
595 with the following contents:

- 596 ▪ Internet communication class—access to cloud services and other specific internet hosts:
 - 597 • Host: updateserver (hosted internally at the NCCoE)
 - 598 ○ Protocol: TCP
 - 599 ○ Direction-initiated: from IoT device
 - 600 ○ Source port: any
 - 601 ○ Destination port: 80
- 602 ▪ Controller class—access to **classes** of devices that are known to be controllers (could describe
603 well-known services such as DNS or Network Time Protocol—NTP):
 - 604 • Host: mqttbroker (hosted internally at the NCCoE)
 - 605 ○ Protocol: TCP
 - 606 ○ Direction-initiated: from IoT device
 - 607 ○ Source port: any
 - 608 ○ Destination port: 1883
- 609 ▪ Local-networks class—access to/from **any** local host for specific services (e.g., http or https):
 - 610 • Host: any
 - 611 ○ Protocol: TCP

- 612 ○ Direction-initiated: from IoT device
- 613 ○ Source port: any
- 614 ○ Destination port: 80
- 615 ■ My-controller class—access to controllers specific to this device:
 - 616 ● Controllers: null (to be filled in by the network administrator)
 - 617 ○ Protocol: TCP
 - 618 ○ Direction-initiated: from IoT device
 - 619 ○ Source port: any
 - 620 ○ Destination port: 80
 - 621 ■ Same-manufacturer class—access to devices of the same manufacturer:
 - 622 ● Same-manufacturer: null (to be filled in by the MUD manager)
 - 623 ○ Protocol: TCP
 - 624 ○ Direction-initiated: from IoT device
 - 625 ○ Source port: any
 - 626 ○ Destination port: 80
 - 627 ■ Manufacturer class—access to devices of a specific manufacturer (identified by MUD URL):
 - 628 ● Manufacturer: devicetype (URL decided by the device manufacturer)
 - 629 ○ Protocol: TCP
 - 630 ○ Direction-initiated: from IoT device
 - 631 ○ Source port: any
 - 632 ○ Destination port: 80

633 4.3.3.1 Signature file

634 According to the IETF MUD specification, “a MUD file MUST be signed using CMS as an opaque binary
 635 object.” The MUD file (*ciscopi2.json*) was signed with the OpenSSL tool by using the command described
 636 in the specification (this will be detailed in Volume C of this publication). A Premium certificate,
 637 requested from DigiCert, was leveraged to generate the signature file (*ciscopi2.p7s*). Once created, the
 638 signature file is stored on the MUD file server.

639 4.3.4 DHCP Server

640 The DHCP server in the architecture is MUD-capable. In addition to dynamically assigning IP addresses,
 641 it recognizes the DHCP option (161) and extracts the MUD URL from the IoT device’s DHCP message.

642 The MUD URL is provided to the MUD manager. The DHCP server is typically embedded in a
643 router/switch. This project uses the DHCP server that is embedded in the Cisco Catalyst 3850-S.

644 *4.3.4.1 Cisco DHCP Server*

645 Cisco IOS provides a basic DHCP server that is useful in small-/medium-business and home network
646 environments, where centralized address management is not required. As described in the previous
647 section, the DHCP server in this case is configured to allocate addresses for the test network, provide a
648 default router, and configure a domain name server. It is **not** used to deliver MUD URLs to the MUD
649 manager.

650 *4.3.5 Router/Switch*

651 This project uses the Cisco Catalyst 3850-S switch.

652 *4.3.5.1 Cisco Catalyst 3850-S*

653 The Cisco Catalyst 3850-S is an enterprise-class layer 3 switch capable of Universal PoE for digital
654 building solutions. The optional PoE feature means it can be configured to supply power to capable
655 devices over Ethernet through its ports. In addition to providing DHCP services, the switch also acts as a
656 broker for connected IoT devices for AAA through the FreeRADIUS server. The LLDP is enabled on ports
657 that MUD-capable devices are plugged into to help facilitate recognition of connected IoT device
658 features, capabilities, and neighbor relationships at layer 2. Additionally, an access session policy is
659 configured on the switch to enable port control for multihost authentication and port monitoring. The
660 combined effect of these switch configurations is a dynamic access list, which has been generated by
661 the MUD manager, being active on the switch to permit or deny access to and from MUD-capable IoT
662 devices. The version of the Cisco Catalyst switch used in this project is a proof-of-concept
663 implementation that is intended to introduce advanced users and engineers to the MUD concept. Some
664 protocol features are not present. These are described in Section 6.1, Findings.

665 *4.3.6 Certificates*

666 DigiCert's CertCentral™ web-based platform allows for provisioning and managing publicly trusted X.509
667 certificates for TLS and code signing as well as a variety of other purposes. After establishing an account,
668 clients can log in, request, renew, and revoke certificates using only a browser. Multiple roles can be
669 assigned within an account, and a discovery tool can be used to inventory all certificates within the
670 enterprise. In addition to certificate-specific features, the platform also offers baseline enterprise
671 software as a service (SaaS) capabilities, including role-based access control (RBAC), security assertion
672 markup language (SAML), single sign-on (SSO), and security policy management and enforcement. All
673 account features come with full parity between the web portal and a publicly available application
674 programming interface (API). For this implementation, two certificates were provisioned: a private TLS

675 certificate for the MUD file server to support the https connection from the MUD manager to the MUD
676 file server, and a Premium certificate for signing the MUD files.

677 4.3.7 IoT Devices

678 This section describes the IoT devices used in the laboratory implementation. There are two distinct
679 categories of devices: devices that are capable of emitting a MUD URL in compliance with the MUD
680 specification, i.e., MUD-capable IoT devices; and devices that are not capable of emitting a MUD URL in
681 compliance with the MUD specification, i.e., non-MUD-capable IoT devices.

682 4.3.7.1 MUD-Capable IoT Devices

683 The project used several MUD-capable IoT devices: NCCoE Raspberry Pi (Devkit), u-blox C027-G35
684 (Devkit), Samsung ARTIK 520 (Devkit), Intel UP Squared Grove (Devkit), Molex PoE Gateway, and Molex
685 Light Engine. The devkits were modified by the NCCoE to simulate IoT devices. All of the MUD-capable
686 IoT devices demonstrate the ability to emit a MUD URL as part of a DHCP transaction or LLDP message
687 and to request and apply software updates.

688 4.3.7.1.1 Molex PoE Gateway and Light Engine

689 This set of IoT devices was developed by Molex. The PoE Gateway acts as a network end point and
690 manages lights, sensors, and other devices. One of the devices managed by the PoE Gateway is a light
691 engine that was provided by Molex.

692 4.3.7.1.2 NCCoE Raspberry Pi (Devkit)

693 The Raspberry Pi devkit runs the Raspbian 9 operating system. It is configured to include a MUD URL
694 that it emits during a typical DHCP transaction. The NCCoE developed a Python script that allowed the
695 Raspberry Pi to receive and process on and off commands by using the MQTT protocol, which were sent
696 to the light-emitting diode (LED) bulb connected to the Raspberry Pi.

697 4.3.7.1.3 NCCoE u-blox C027-G35 (Devkit)

698 The u-blox C027-G35 devkit runs the ARM Mbed operating system. The NCCoE modified several of the
699 Mbed-OS libraries to configure the devkit to include a MUD URL that it emits during a typical DHCP
700 transaction. The u-blox devkit is also configured to initiate network connections to test network traffic
701 throughout the MUD process.

702 4.3.7.1.4 NCCoE Samsung ARTIK 520 (Devkit)

703 The Samsung ARTIK 520 devkit runs the Fedora 24 operating system. It is configured to include a MUD
704 URL that it emits during a typical DHCP transaction. The same Python script mentioned earlier was used
705 to simulate a smart lock. This Python script allowed the ARTIK devkit to receive on and off commands by
706 using the MQTT protocol.

707 [4.3.7.1.5 NCCoE Intel UP Squared Grove \(Devkit\)](#)

708 The Intel UP Squared Grove devkit runs the Ubuntu 16.04 LTS operating system. It is configured to
709 include a MUD URL that it emits during a typical DHCP transaction. The same Python script mentioned
710 earlier was used to simulate a smart lighting device. This allowed the UP Squared Grove devkit to
711 receive on and off commands by using the MQTT protocol.

712 [4.3.7.2 Non-MUD-Capable IoT Devices](#)

713 The laboratory implementation also includes a variety of legacy, non-MUD-capable IoT devices that are
714 not capable of emitting a MUD URL. These include cameras, smartphones, lighting, a smart assistant, a
715 printer, a baby monitor, a wireless access point, and a digital video recorder (DVR).

716 [4.3.7.2.1 Cameras](#)

717 The three cameras utilized in the laboratory implementation are produced by two different
718 manufacturers. They stream video and audio either to another device on the network or to a cloud
719 service. These cameras are controlled and managed by a smartphone.

720 [4.3.7.2.2 Smartphones](#)

721 Two types of smartphones are used for setting up, interacting with, and controlling IoT devices.

722 [4.3.7.2.3 Lighting](#)

723 Two types of smart lighting devices are used in the laboratory implementation. These smart lighting
724 components are controlled and managed by a smartphone.

725 [4.3.7.2.4 Smart Assistant](#)

726 A smart assistant is utilized in the laboratory implementation. The device is used to demonstrate and
727 test the wide range of network traffic generated by a smart assistant.

728 [4.3.7.2.5 Printer](#)

729 A smart printer is connected to the laboratory network wirelessly to demonstrate smart printer usage.

730 [4.3.7.2.6 Baby Monitor](#)

731 A baby monitor with remote control plus video and audio capabilities is connected wirelessly to the
732 laboratory network. This baby monitor is controlled and managed by a smartphone.

733 [4.3.7.2.7 Wireless Access Point](#)

734 A smart wireless access point is used in the laboratory implementation to demonstrate the network
735 activity and functionality of this type of device.

736 [4.3.7.2.8 Digital Video Recorder](#)

737 A smart DVR is also connected to the laboratory implementation network. This is also controlled and
738 managed by a smartphone.

739 4.3.8 Update Server

740 The update server provides patches and other software updates to the IoT devices. This project used an
741 NCCoE-hosted update server.

742 4.3.8.1 NCCoE Update Server

743 The NCCoE implemented its own update server by using an Apache web server. This file server hosts
744 software update files to be served as software updates to the IoT device devkits. When the server
745 receives an http request, it sends the corresponding update file.

746 4.3.8.2 Molex Update Agent

747 The process for updating the firmware on a Molex PoE Gateway is currently a manual process, with the
748 firmware update taking place over the CoAP, UDP, and trivial file transfer protocol (TFTP) protocols. The
749 update process is initiated by an update agent on the local network connecting to the PoE Gateway and
750 sending the firmware update information.

751 4.3.9 Unapproved Server

752 The NCCoE implemented its own unapproved server by using an Apache web server. This web server
753 acts as an unapproved internet host, i.e., an internet host that is not explicitly approved in the MUD
754 File. This was created to test the communication between a MUD-enabled IoT device and an internet
755 host that is not included in the MUD file and should thus be denied. To verify that the traffic filters were
756 applied as expected, communication to and from the unapproved server and the MUD-enabled IoT
757 device was tested.

758 4.3.10 MQTT Broker Server

759 The NCCoE implemented an MQTT Broker Server by using the open-source tool Mosquitto. The server
760 communicates messages among multiple clients. For this project, it provides the ability for mobile
761 devices set up with the appropriate application to communicate with the MQTT-enabled IoT devices in
762 the build. The messages exchanged by the devices are on and off messages, which allow the mobile
763 device to control the LED light on the IoT device.

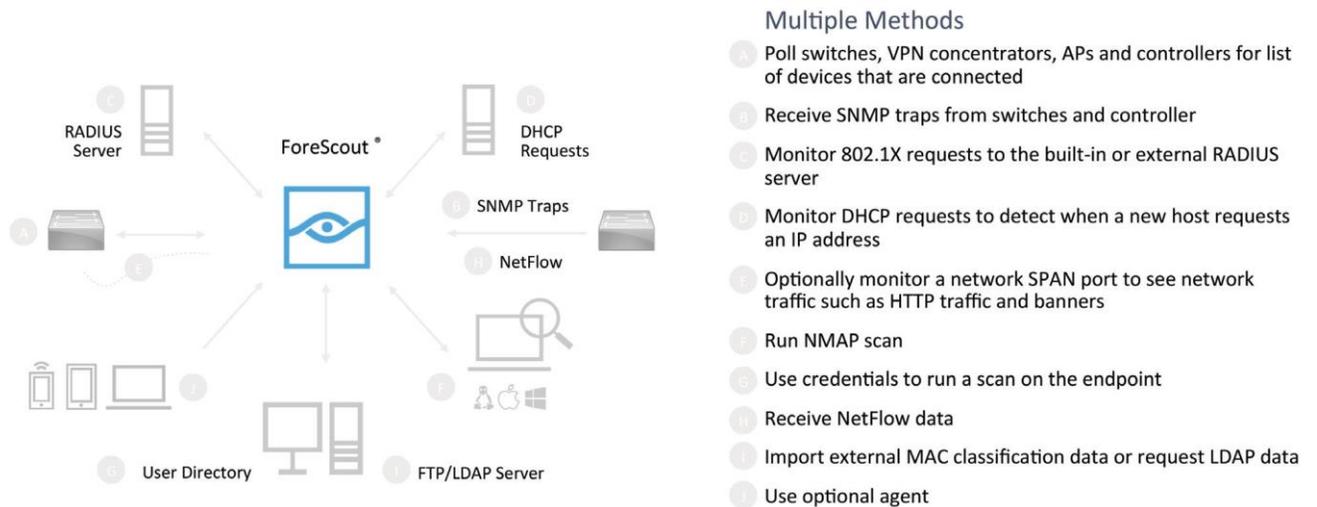
764 4.3.11 IoT Device Discovery

765 This project uses ForeScout CounterACT appliance and Enterprise Manager to provide an IoT device
766 discovery service for the demonstration network. CounterACT is able to discover, inventory, profile, and
767 classify all attached devices to validate that the access that is being granted to each device is consistent
768 with that device's type. ForeScout can also continuously monitor the actions of these assets as they join
769 and leave the network. While ForeScout CounterACT provides a wide range of data collection
770 capabilities, items this project focuses on include

- 771 ▪ Device Information
 - 772 • Device Type
 - 773 • Manufacturer
 - 774 • Connection Type
 - 775 • Hardware Information
 - 776 • MAC and IP Addresses
 - 777 • Operating System
 - 778 ○ Network Services
- 779 ▪ Network Configuration
 - 780 • Wired or Wireless

781 CounterACT detects IoT devices in real time as they connect to the network. It uses both passive
 782 monitoring and integration with the network infrastructure. As a device connects to the network,
 783 CounterACT may learn about that device via a variety of different techniques to discover and classify it
 784 without requiring agents, as shown in Figure 4-3. The methods demonstrated in this project included
 785 the following: CounterACT passive discovery of devices using switch polling, importation of MAC
 786 classification data, and TCP fingerprinting. Due to the passive nature of the device discovery, neither
 787 performance nor reliability of the IoT devices is impacted.

788 **Figure 4-3 Methods the ForeScout Platform Can Use to Discover and Classify IP-Connected Devices**

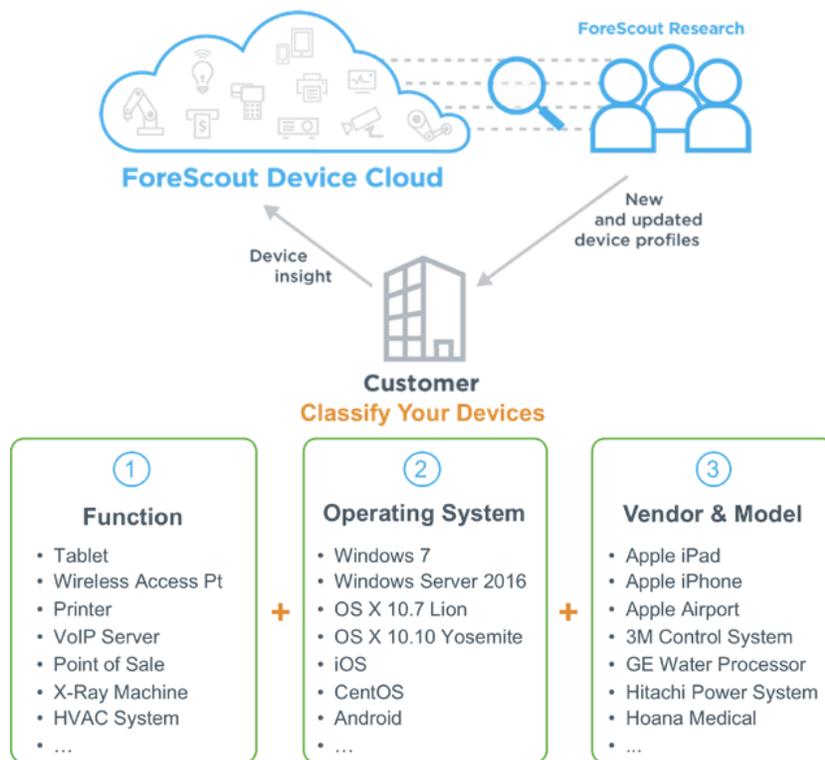


789

790 ForeScout CounterACT is deployed as virtual appliances on the NCCoE laboratory network and managed
 791 by a single Enterprise Manager. After discovering IoT devices and collecting relevant information, classi-
 792 fication is the next step.

793 To automatically classify discovered devices, the ForeScout platform includes ForeScout Device Cloud.
 794 Device Cloud allows users to benefit from crowdsourced device insight to auto-classify their devices, as
 795 shown in Figure 4-4. It also auto-classifies the devices by their type and function, operating system and
 796 version, and manufacturer and model. Users can leverage new and updated auto-classification profiles
 797 published by ForeScout. In addition, they can create custom classification policies to auto-classify
 798 devices unique to their environments. At the time of this writing, the ForeScout CounterACT appliance
 799 did not have the ability to identify whether an IoT device on the network was MUD-enabled.

800 **Figure 4-4 Classify IoT Devices by Using the ForeScout Platform**



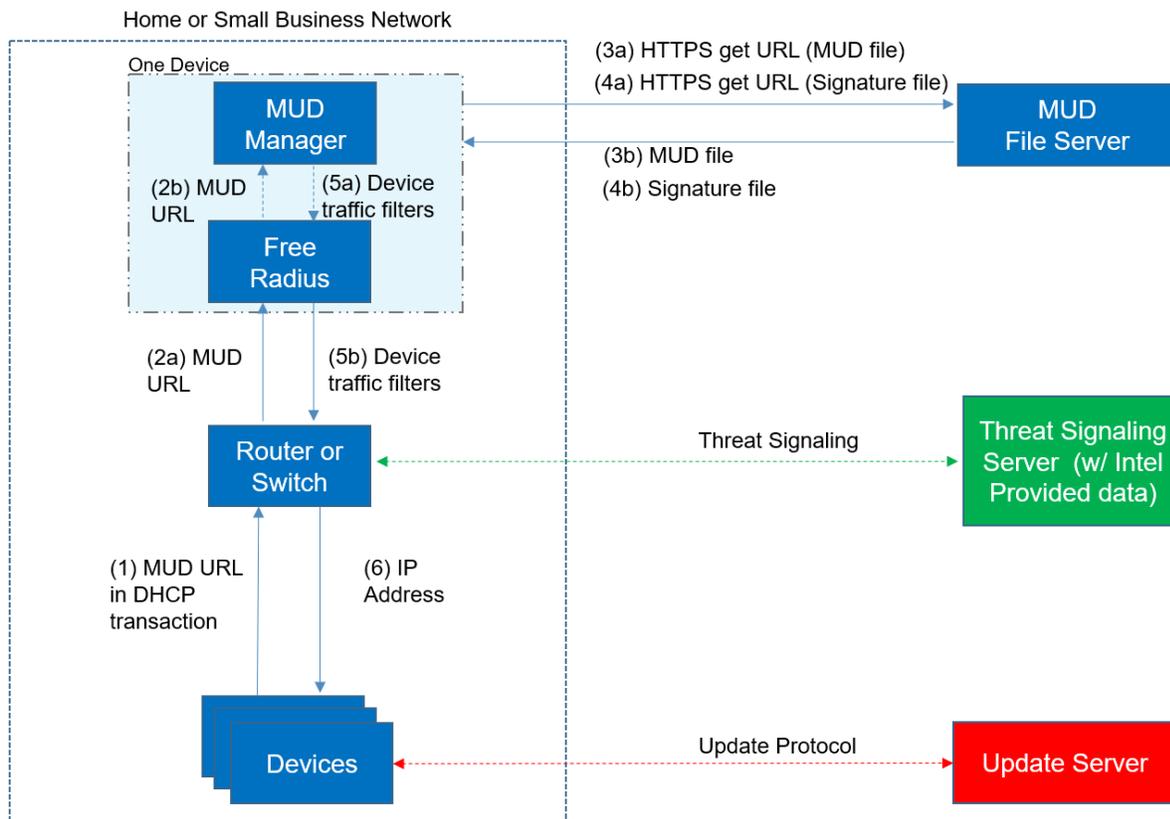
801

802 4.4 Build Demonstration

803 The MUD manager used in the capability demonstration was provided by Cisco. Cisco is a provider of
 804 enterprise, telecommunications, and industrial networking solutions. The work in this project is being
 805 undertaken within Cisco’s Enterprise Central Software Group, with an eye toward improving the
 806 product offering over time. Cisco has provided a proof-of-concept MUD manager as well as a Catalyst
 807 3850-S switch with Power-over-Ethernet.

808 Figure 4-5 describes the logical architecture of the first build. The example implementation is designed
 809 with a single device serving as the MUD manager and FreeRADIUS server that interfaces with the
 810 Catalyst 3850-S switch over TCP/IP. The Catalyst 3850-S switch contains a DHCP server that is configured
 811 to extract MUD URLs from IPv4 DHCP transactions. Upon connecting a MUD-enabled device, the MUD
 812 URL will be emitted in some approved method (LLDP, X.509, or DHCP)—for this example implementation,
 813 DHCP and LLDP were leveraged (step 1). The Catalyst 3850-S switch will send the MUD URL to the
 814 FreeRADIUS server (step 2a); this is passed from the FreeRADIUS server to the MUD manager (step 2b).
 815 Once the MUD URL is received, the MUD manager will fetch the MUD file by using the MUD URL
 816 provided in the previous step (step 3a); if successful, the MUD file server at the specified location will
 817 serve the MUD file (step 3b). Next, the MUD manager will request the signature file associated with the
 818 MUD file (step 4a) and upon receipt (step 4b) will verify the MUD file with the respective signature file.
 819 Once the MUD file has been verified successfully, the MUD manager passes the device’s traffic filters
 820 to the FreeRADIUS server (step 5a), which in turn sends the device’s traffic filters to the router or switch,
 821 where they are applied (step 5b). The device is finally assigned an IP address (step 6).

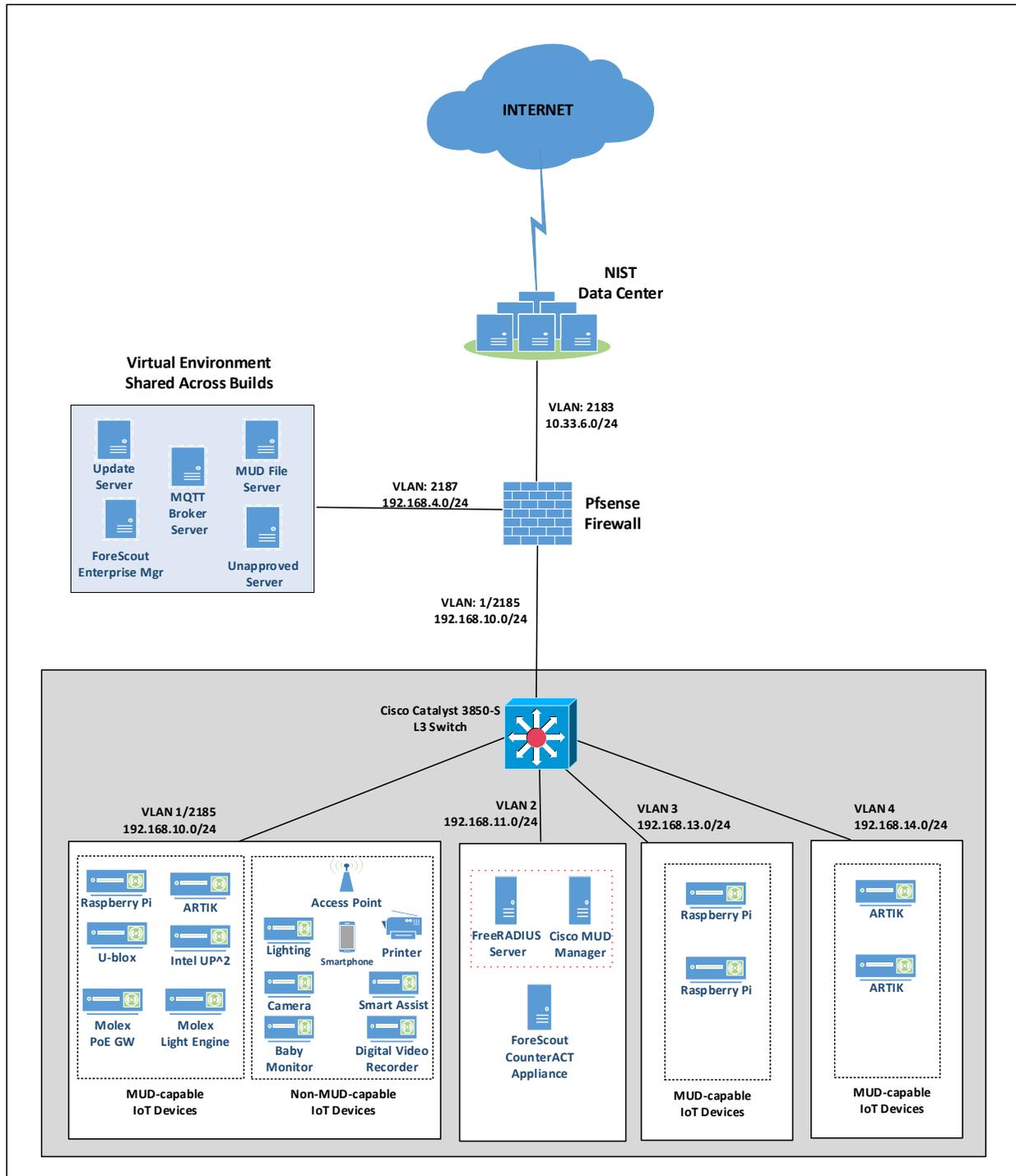
822 **Figure 4-5 Logical Architecture—Build 1**



823

824 Figure 4-6 describes the physical architecture of laboratory build 1. The Catalyst 3850-S switch is
825 configured to host four VLANs. The first VLAN, VLAN 1 hosts a large number of IoT devices. Three
826 separate instances of DHCP servers are configured for VLANs 1, 3, and 4 to dynamically assign IPv4
827 addresses to each IoT device that connects to the switch on each of these VLANs. VLAN 2 is configured
828 on the catalyst switch to host the Cisco MUD Manager, the FreeRADIUS server, and the ForeScout
829 CounterACT appliance. VLAN 3 and VLAN 4 are configured to host IoT devices from the same
830 manufacturer. Specifically, VLAN 3 hosts two Raspberry Pi devices, while VLAN 4 hosts two u-blox
831 devices. The network infrastructure as configured utilizes the IPv4 protocol for communication both
832 internally and to the internet.

833 Figure 4-6 Physical Architecture—Build 1

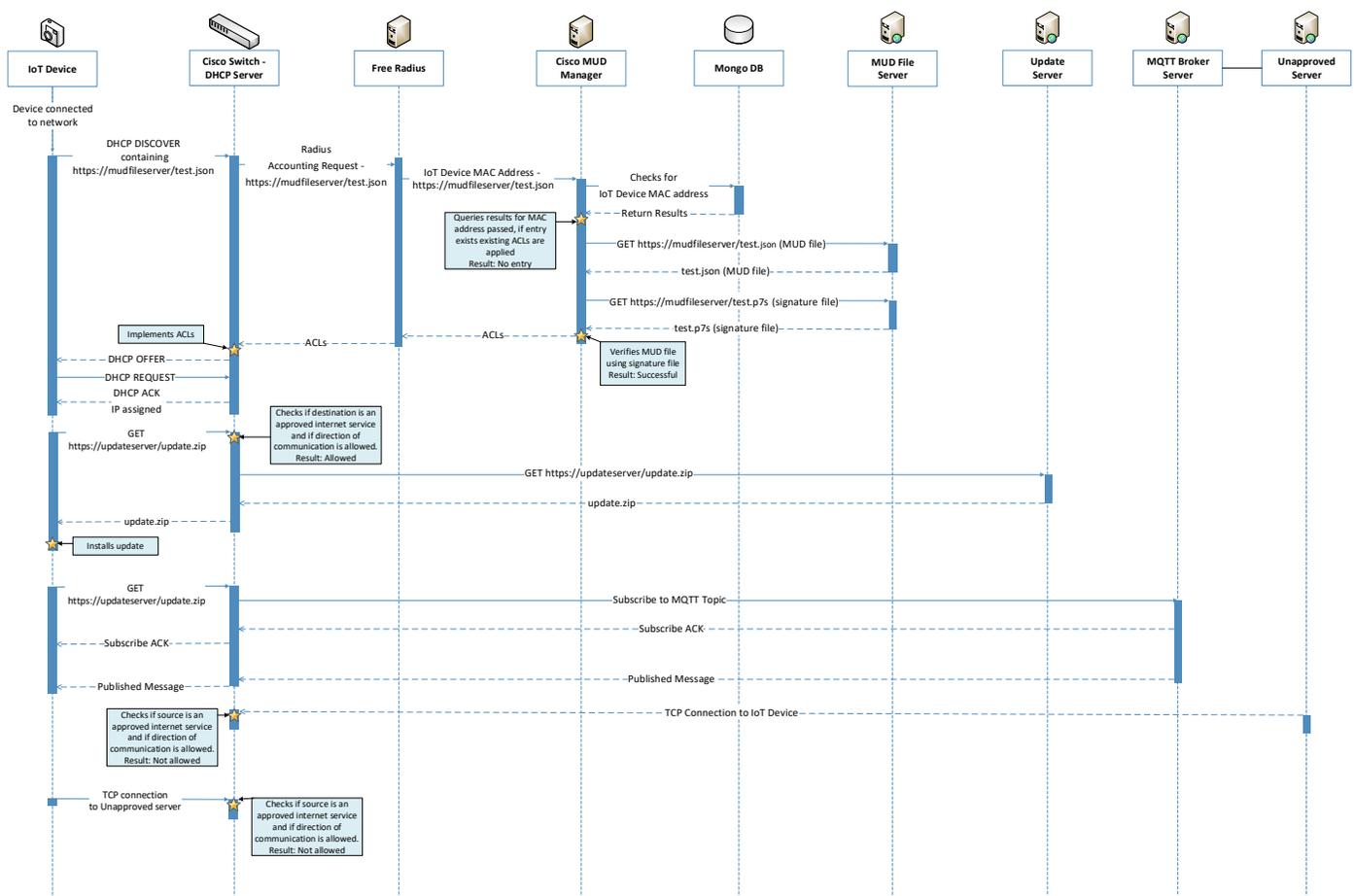


834

835 A full description of Cisco’s proof of concept can be found at [https://github.com/CiscoDevNet/MUD-](https://github.com/CiscoDevNet/MUD-Manager)
 836 [Manager](https://github.com/CiscoDevNet/MUD-Manager). The Cisco MUD Manager is built as a callout from FreeRADIUS and uses MongoDB to store
 837 policy information. The MUD manager is configured from a JSON file that will vary slightly based on the
 838 installation. This configuration file provides a number of static bindings and directives as to whether
 839 both egress and ingress ACLs should be applied, and it identifies the definition of the “local network”
 840 class on the network.

841 Figure 4-7 shows the process flow of onboarding a MUD-enabled IoT device that emits a MUD URL via
 842 DHCPv4.

843 **Figure 4-7 Process Flow–Build 1**



- 844
- 845 As shown in Figure 4-7, the process flow is as follows:
- 846
- A MUD-enabled IoT device is connected to the network.

- 847 ▪ The MUD-enabled IoT device begins a DHCPv4 transaction in which DHCP option 161, the
848 internet assigned numbers authority (IANA)-assigned value for MUD, is transmitted as part of a
849 DHCP request. It is possible to transmit the option in both DISCOVERY and REQUEST messages.
- 850 ▪ The DHCP server on the Cisco switch recognizes that option and extracts the MUD URL from
851 the DHCP message, which is sent from the switch to the FreeRADIUS server in the associated
852 accounting request. From this point, the FreeRADIUS server sends the MAC address and MUD
853 URL for the newly onboarded device to the MUD manager.
- 854 ▪ Next, the MUD manager does a query for the MAC address in its database, searching for any
855 cached MUD files associated with the MAC address and MUD URL. If an entry does not exist, as
856 depicted in the figure, the MUD manager fetches the MUD file and signature file from the
857 MUD file server.
- 858 ▪ The MUD manager verifies the MUD file with the corresponding signature file and translates
859 the contents into ACLs, which are passed through the FreeRADIUS server to the Cisco switch
860 where they are applied.
- 861 ▪ The MUD-enabled IoT device is assigned an IP address and is ready to be used on the network.
- 862 ▪ Finally, when the MUD-enabled IoT device is in use, access of all traffic to and from the IoT
863 device is controlled by the Cisco switch.

864 Communications that are allowed by the MUD file include egress north/south and east/west traffic. At
865 the time of publication, ingress access control was not yet supported. Specifics can be found in Section
866 6.1, Findings. The version of the Cisco MUD Manager implemented in this build leverages a JSON
867 configuration file that is responsible for translating many of the abstractions that are defined by the
868 MUD file. East/west constructs as described in the MUD specification are

- 869 ▪ Controller–class of devices known to be controllers (could describe well-known services such
870 as DNS or NTP)
- 871 ▪ My-controller–class of devices that the local network administrator admits to the particular
872 class
- 873 ▪ Local-networks –class of IP addresses that are scoped within some local administrative
874 boundary
- 875 ▪ Same-manufacturer–class of devices from the same manufacturer as the IoT device in question
- 876 ▪ Manufacturer–class of devices made by a particular manufacturer as identified by the
877 authority component of its MUD URL

878 In addition to the components required for the MUD solution to function as defined, the example
879 implementation also includes the CounterACT appliance. This appliance was leveraged in order to
880 discover IoT devices on network.

881 5 Security Characteristic Analysis

882 The purpose of the security characteristic analysis is to understand the extent to which the project
883 meets its objective of demonstrating the ability to identify IoT components to MUD managers and
884 manage access to those components in a manner that maintains component functionality while limiting
885 unauthorized access to and from the components. In addition, it seeks to understand the security
886 benefits and drawbacks of the example solution.

887 5.1 Assumptions and Limitations

888 The security characteristic analysis has the following limitations:

- 889 ▪ It is not a comprehensive test of all security components, nor is it a red team exercise.
- 890 ▪ It cannot identify all weaknesses.
- 891 ▪ It does not include the lab infrastructure. It is assumed that devices are hardened. Testing
892 these devices would reveal only weaknesses in implementation that would not be relevant to
893 those adopting this reference architecture.

894 5.2 Security Control Map

895 One aspect of the security characteristic analysis involved assessing how well the reference design
896 addresses the security characteristics that it was intended to support. The NIST Cybersecurity
897 Framework Subcategories were used to provide structure to the security assessment. We consulted the
898 specific sections of each standard that are cited in reference to a Subcategory. The cited sections
899 provide validation points that the example implementation would be expected to exhibit. Using the
900 Cybersecurity Framework Subcategories as a basis for organizing our analysis allowed us to
901 systematically consider how well the reference design supports the intended security characteristics.

902 The characteristics analysis was conducted in the context of home network and small-business usage
903 scenarios. Use in large enterprise environments may be included in future project extensions but is not
904 considered in this analysis.

905 The capabilities demonstrated by the architectural elements described in Section 4 and used in the
906 home networks and small-business environments are primarily intended to address requirements, best
907 practices, and capabilities described in the following NIST documents: *Framework for Improving Critical*
908 *Infrastructure Cybersecurity* (Cybersecurity Framework), *Security and Privacy Controls for Federal*
909 *Information Systems and Organizations* (NIST SP 800-53), and *Considerations for Managing Internet of*
910 *Things (IoT) Cybersecurity and Privacy Risks* (NIST Interagency/Internal Report 8228). NIST
911 Interagency/Internal Report 8228 identifies a set of 25 security and privacy expectations for IoT devices
912 and subsystems. These include expectations regarding meeting device protection, data protection, and
913 privacy protection goals. As described in the Mitigating IoT-Based Distributed Denial of Service (DDoS)

914 project description, the example implementation directly addresses the PR.AC-1, PR.AC-2, PR.AC-7, and
 915 PR.PT-3 Cybersecurity Framework Subcategories and supports activities addressing the ID.AM-1, ID.AM-
 916 2, ID-AM-3, ID.RA-2, ID.RA-3, PR.AC-5, PR.AC-4, PR.DS-5, PR.DS-6, PR-IP-1, PR-IP-3, and DE.CM-8
 917 Subcategories. Also, the security platform directly addresses NIST SP 800-53 controls AC-3, AC-18, CM-7,
 918 SC-5, SC-7, SC-28, and SI-2, and it supports activities addressing NIST SP 800-53 controls AC-4, AC-6, AC-
 919 24, CM-8, IA-2, IA-5, IA-8, PA-4, PM-5, RA-5, SC-8, and SI-5. In addition, seven of the NIST
 920 Interagency/Internal Report 8228 expectations are addressed by the example implementation. Table
 921 5-1 describes how example implementation characteristics address NIST Interagency/Internal Report
 922 8228 expectations, NIST SP 800-53 controls, and Cybersecurity Framework Subcategories.

923 **Table 5-1 Mapping Demonstration Platform Characteristics to NIST Interagency/Internal Report 8228**
 924 **Expectations, NIST SP 800-53 Controls, and Cybersecurity Framework Subcategories**

Applicable Project Description Element That Addresses the Expectation	Applicable NISTIR 8228 Expectations	Draft NIST SP 800-53 Rev 5 Controls Supported	Cybersecurity Framework Subcategories Supported
1	IoT devices insert the MUD extension into DHCP address requests when they attach to the network (e.g., power on).	Device has a built-in identifier.	<u>Supports:</u> CM-8 System Component Inventory PM-5 System Inventory <u>Supports:</u> ID.AM-1 Physical devices and systems within the organization are inventoried.
2	The contents of the MUD extension are passed to the MUD manager, which retrieves a MUD file from the designated website (denoted as the MUD file server) by using https. The MUD file describes the communications requirements for this device. The MUD manager converts the requirements into access control information for enforcement by the router or switch.	Device can interface with enterprise asset management systems.	<u>Provides:</u> AC-3 Access Enforcement AC-18 Wireless Access CM-7 Least Functionality SC-5 Denial of Service Protection SC-7 Boundary Protection <u>Provides:</u> PR.PT-3 The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. <u>Supports:</u> ID.AM-1 Physical devices and systems within the organization are inventoried. ID.AM-2 Software platforms and applications within the

			<p><u>Supports:</u> <u>AC-4</u> Information Flow Enforcement <u>AC-6</u> Least Privilege <u>AC-24</u> Access Control Decisions <u>CM-8</u> System Component Inventory <u>PM-5</u> System Inventory</p>	<p>organization are inventoried. <u>ID.AM-3</u> Organizational communication and data flows are mapped. <u>PR.AC-4</u> Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. <u>PR.AC-5</u> Network integrity is protected (e.g., network segregation, network segmentation). <u>PR.DS-5</u> Protections against data leaks are implemented. <u>DE.AE-1</u> A baseline of network operations and expected data flows for users and systems is established and managed.</p>
5	<p>IoT devices periodically contact the appropriate update server to download and apply security patches.</p>	<p>The manufacturer will provide patches or upgrades for all software and firmware throughout each device's life span.</p>	<p><u>Provides:</u> <u>SI-2</u> Flaw Remediation</p>	<p><u>Supports:</u> <u>PR.IP-1</u> A baseline configuration of information technology/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality). <u>PR.IP-3</u></p>

				Configuration change control processes are in place.
7	The router or switch periodically receives threat feeds from the threat signaling server to use as a basis for restricting certain types of network traffic. (Note that although threat signaling is included as part of the reference architecture, it has not yet been implemented in the build.)	The device either supports the use of vulnerability scanners or provides built-in vulnerability identification and reporting capabilities.	<p><u>Supports:</u></p> <p><u>AC-24</u> Access Control Decisions</p> <p><u>RA-5</u> Vulnerability Scanning</p> <p><u>SI-5</u> Security Alerts, Advisories, and Directives</p>	<p><u>Supports:</u></p> <p><u>ID.RA-2</u> Cyber threat intelligence is received from information-sharing forums and sources.</p> <p><u>ID.RA-3</u> Threats, both internal and external, are identified and documented.</p> <p><u>DE.CM-8</u> Vulnerability scans are performed.</p>
11	The contents of the MUD extension are passed to the MUD manager, which retrieves a MUD file from the designated website (denoted as the MUD file server) by using https. The MUD file server must have a valid TLS certificate, and the MUD file itself must have a valid signature. The MUD file describes the communications requirements for this device. The MUD manager converts the requirements into access control information for enforcement by the router or switch.	The device can use existing enterprise authenticators and authentication mechanisms.	<p><u>Supports:</u></p> <p><u>IA-2</u> Identification and Authentication (Organizational Users)</p> <p><u>IA-5</u> Authenticator Management</p> <p><u>IA-8</u> Identification and Authentication (Non-Organizational Users)</p>	<p><u>Provides:</u></p> <p><u>PR.AC-1</u> Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.</p> <p><u>PR.AC-3</u> Remote access is managed.</p> <p><u>PR.AC-7</u> Users, devices, and other assets are authenticated commensurate with the risk of the transaction.</p>
21	IoT devices insert the MUD extension into DHCP address requests when they attach to the network (e.g., power on). The contents of the MUD extension are passed to the MUD manager, which retrieves a MUD file from the designated website (denoted as the MUD file server) by using https. The	Device can prevent unauthorized access to all sensitive	<p><u>Provides:</u></p> <p><u>SC-23</u> Session Authenticity</p> <p><u>Supports:</u></p>	<p><u>Provides:</u></p> <p><u>PR.PT-3</u> The principle of least functionality is incorpo-</p>

	MUD file describes the communications requirements for this device. The MUD manager converts the requirements into access control information for enforcement by the router or switch.	data transmitted from it over networks.	<u>AC-18</u> Wireless Access <u>SC-8</u> Transmission Confidentiality and Integrity	rated by configuring systems to provide only essential capabilities. <u>Supports:</u> <u>PR.DS-5</u> Protections against data leaks are implemented. <u>PR.DS-6</u> Integrity-checking mechanisms are used to verify software, firmware, and information integrity.
24	IoT devices insert the MUD extension into DHCP address requests when they attach to the network (e.g., power on). The contents of the MUD extension are passed to the MUD manager, which retrieves a MUD file from the designated website (denoted as the MUD file server) by using https. The MUD file describes the communications requirements for this device. The MUD manager converts the requirements into access control information for enforcement by the router or switch. The router or switch periodically receives threat feeds from the threat signaling server to use as a basis for restricting certain types of network traffic. (As mentioned earlier, although a part of the logical architecture, threat signaling has not yet been implemented in the build.)	There is sufficient centralized control to apply policy or regulatory requirements to personally identifiable information.	<u>Supports:</u> <u>PA-4</u> Information Sharing with External Parties	None

925 Table 5-2 details Cybersecurity Framework Identify, Protect, and Detect Categories and Subcategories
 926 that the example implementation directly addresses or for which the example implementation may
 927 serve a supporting role. Those Subcategories that are directly addressed are highlighted in green. While
 928 some of the references provide general guidance that informs implementation of referenced
 929 Cybersecurity Framework core functions, the NIST SP and Federal Information Processing Standard
 930 (FIPS) references provide specific recommendations that should be considered when composing and

931 configuring security platforms. (Note that not all of the informative references apply to this example
 932 implementation.)

933 **Table 5-2 Mapping Project Objectives to the Cybersecurity Framework and Informative Security**
 934 **Control References**

Cybersecurity Framework Category	Cybersecurity Framework Subcategory	Informative References
<p>Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.</p>	<p>ID.AM-1: Physical devices and systems within the organization are inventoried.</p>	<p>CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5</p>
	<p>ID.AM-2: Software platforms and applications within the organization are inventoried.</p>	<p>CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5</p>
	<p>ID.AM-3: Organizational communication and data flows are mapped.</p>	<p>CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 SA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8</p>
<p>Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</p>	<p>ID.RA-2: Cyber threat intelligence is received from information-sharing forums and sources.</p>	<p>CIS CSC 4 COBIT 5 BAI08.01 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16</p>

	<p>ID.RA-3: Threats, both internal and external, are identified and documented.</p>	<p>CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16</p>
<p>Identity Management, Authentication, and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.</p>	<p>PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.</p>	<p>COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 CIS CSC 1, 5, 15, 16</p>
	<p>PR.AC-3: Remote access is managed.</p>	<p>CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15</p>
	<p>PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.</p>	<p>CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24</p>

	<p>PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate.</p>	<p>CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7</p>
	<p>PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks).</p>	<p>CIS CSC 1, 12, 15, 16 COBIT 5 DSS05.04, DSS05.10, DSS06.10 ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11</p>
<p>E.g., Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.</p>	<p>PR.DS-5: Protections against data leaks are implemented.</p> <p>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity</p>	<p>CIS CSC 13 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISA 62443-3-3:2013 SR 5.2 ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4</p> <p>ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8</p>

		<p>ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3</p> <p>FIPS 140-2 Sec. 4</p> <p>NIST SP 800-45 Ver. 2 2.4.2, 3, 4.2.3, 4.3, 5.1, 6.1, 7.2.2, 8.2, 9.2</p> <p>NIST SP 800-49 2.2.1, 2.3.2, 3.4</p> <p>NIST SP 800-52 Rev. 1 3, 4, D1.4</p> <p>NIST SP 800-53 Rev. 4 SI-7</p> <p>NIST SP 800-57 Part 1 Rev. 4 5.5, 6.1, 8.1.5.1, B.3.2, B.5</p> <p>NIST SP 800-57 Part 2 1, 3.1.2.1.2, 4.1, 4.2, 4.3, A.2.2, A.3.2, C.2.2</p> <p>NIST SP 800-81-2 All</p> <p>NIST SP 800-130 2.2, 4.3, 6.2.1, 6.3, 6.4, 6.5, 6.6.1</p> <p>NIST SP 800-152 6.1.3, 6.2.1, 8.2.1, 8.2.4, 9.4</p> <p>NIST SP 800-177 2.2, 4.1, 4.4, 4.5, 4.7, 5.2, 5.3</p>
<p>Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p>	<p>PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality).</p>	<p>CIS CSC 1</p> <p>COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05</p> <p>ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3</p> <p>ISA 62443-3-3:2013 SR 7.6</p> <p>ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4</p> <p>NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10</p>
	<p>PR.IP-3: Configuration change control processes are in place.</p>	<p>CIS CSC 3, 11</p> <p>COBIT 5 BAI01.06, BAI06.01</p> <p>ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3</p> <p>ISA 62443-3-3:2013 SR 7.6</p> <p>ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4</p>

		NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10
<p>Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	<p>PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.</p>	<p>CIS CSC 3, 11, 14 COBIT 5 DSS05.02, DSS05.05, DSS06.06 ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 ISO/IEC 27001:2013 A.9.1.2 NIST SP 800-53 Rev. 4 AC-3, CM-7</p>
<p>Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	<p>DE.CM-8: Vulnerability scans are performed.</p>	<p>CIS CSC 4, 20 COBIT 5 BAI03.10, DSS05.01 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-5</p>

935 Additional resources and references required to develop this solution are identified in Appendix E. The
 936 core standards, secure update standards, industry best practices for software quality, and best
 937 practices for identification and authentication are generally stable, well understood, and available in the
 938 commercial off-the-shelf market. Standards associated with the MUD protocol are in an advanced level
 939 of development in the Internet Engineering Task Force.

940 5.3 Scenarios

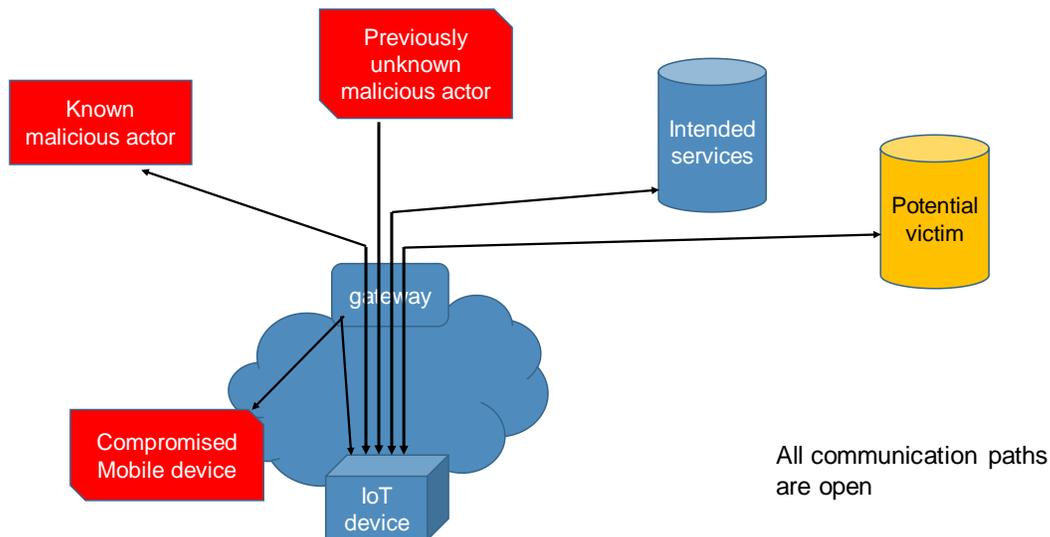
941 This section presents three threat scenarios for home and small-business networks involving increasing
 942 levels of security. In the first scenario, MUD is not deployed on the network, so IoT devices are
 943 vulnerable to being port scanned and are not restricted from exchanging traffic with either external
 944 sites or other devices on the local network. IoT devices in this first scenario are highly vulnerable to
 945 attack.

946 In the second scenario, MUD is deployed on the network, but the MUD files being used only restrict
 947 traffic from being sent between the IoT devices and some external internet domains (i.e., north-south
 948 traffic); IoT devices are still able to send and receive traffic from all other devices on the local network
 949 (i.e., east-west traffic). In the third scenario, the MUD file protections provided in scenario 2 are
 950 enhanced to also restrict traffic between IoT devices and some other devices on the local network,
 951 ensuring that the IoT devices are permitted to exchange traffic with only external domains and internal
 952 devices that are explicitly specified in their MUD file.

953 5.3.1 Scenario 1: No MUD Protection

954 In the *No MUD Protection* scenario, as shown in Figure 5-1, the home/small-business network (depicted
 955 by the blue cloud) does not have MUD deployed to provide security for its IoT devices.

956 **Figure 5-1 No MUD Protection Threat Scenario**



957
 958 All IoT devices on the network can be port scanned (and perhaps hijacked) from anywhere. IoT devices
 959 are permitted access to and from intended services as desired. However, the IoT devices are also
 960 reachable by compromised mobile devices that are on their local network and by malicious external
 961 devices, making them vulnerable to attacks from these compromised and malicious devices. In addition,
 962 if an IoT device becomes compromised, there are no protections in place to stop it from launching an
 963 attack on outside devices, creating additional potential victims.

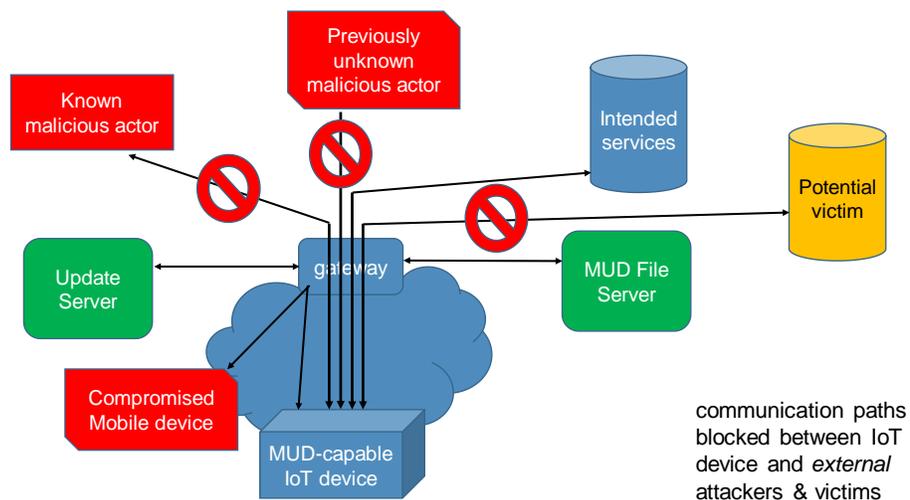
964 5.3.2 Scenario 2: MUD Protection from External Threats

965 In the *MUD Protection from External Threats* scenario, as shown in Figure 5-2, the home/small-business
 966 network (depicted by the blue cloud) has MUD deployed (the components of the MUD deployment are
 967 not depicted). The MUD file for the IoT device lists the domains of all external services with which the

968 device is permitted to exchange traffic. All domains that are not explicitly permitted in the MUD file are
 969 denied. Therefore, the IoT device on the network can freely communicate with its intended external
 970 services, but all other attempted communications between the IoT device and external devices are
 971 blocked. The IoT device cannot be port scanned or receive traffic from external malicious actors, even if
 972 those actors are not known to be malicious. Furthermore, even if the IoT device is compromised in
 973 some way after being onboarded, it will not be permitted to send traffic to any external devices to
 974 attack those devices. One of the external devices with which the IoT device is permitted to
 975 communicate is an update server, from which the device receives regular software updates to ensure
 976 that it installs the most recent security patches as needed.

977 Unfortunately, the MUD file for the IoT device in this scenario also includes a construct that permits the
 978 IoT device to exchange traffic with all devices that are on the local network. If a device on the local
 979 network becomes compromised, that device will be able to attack the IoT device.

980 **Figure 5-2 MUD Protection from External Threats Scenario**



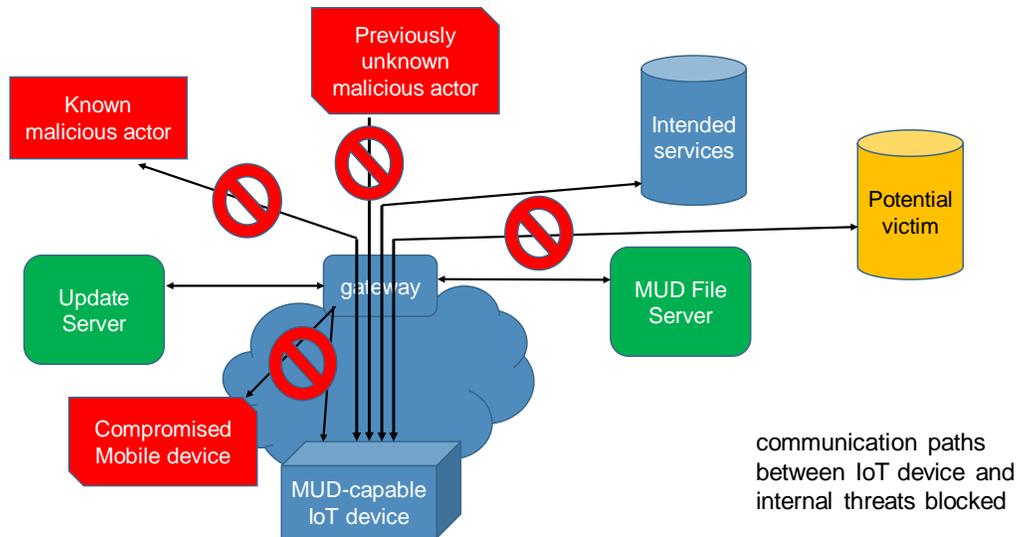
981

982 5.3.3 Scenario 3: MUD Protection from External and Internal Threats

983 In the *MUD Protection from External and Internal Threats* scenario, as shown in Figure 5-3, the
 984 home/small-business network (depicted by the blue cloud) has MUD deployed (the components of the
 985 MUD deployment are not depicted). As in the MUD Protection from External Threats scenario, the MUD
 986 file for the IoT device lists the domains of all external services with which the device is permitted to
 987 exchange traffic, thereby protecting the IoT devices from being attacked by external entities and
 988 protecting external entities from being attacked by the IoT device. In addition, unlike the previous
 989 scenario, the MUD file in this scenario does not include a construct that permits the IoT device to
 990 exchange traffic with all other devices that are on the local network. Instead, the MUD file specifies
 991 specific devices with which the IoT device is permitted to communicate based on, for example, the

992 manufacturer of those other devices. If a local device is not from the specified manufacturer, it will not
 993 be permitted to communicate with the IoT device. So, if a device on the local network becomes
 994 compromised and that device’s manufacturer or model is not one that has been explicitly permitted in
 995 the MUD file, that device will not be permitted to send traffic to attack the IoT device.

996 **Figure 5-3 MUD Protection from External and Internal Threats Scenario**



997

998 5.4 Build Evaluation

999 A functional evaluation of the IoT example implementation was conducted to verify that it meets the
 1000 requirements. Table 5-3 summarizes the tests that were performed, their expected and observed
 1001 outcomes, and the applicable Cybersecurity Framework Subcategories and NIST SP 800-53 controls for
 1002 which each test is designed to verify support. The tests that are listed in the table are described in a
 1003 functional evaluation plan that is provided in 7.2Appendix D. Not all tests defined in the functional
 1004 evaluation plan are listed in Table 5-3 because not all those tests were applicable to this build of the IoT
 1005 example implementation. Boldface text is used in the Test Summary and Expected Outcome columns to
 1006 highlight the gist of the information that is being conveyed.

1007 **Table 5-3 Summary of Functional Tests**

Test	Applicable Cybersecurity Framework Subcategories & NIST SP 800-53 Controls	Test Summary	Expected Outcome	Observed Outcome
IoT-1	ID.AM-1: Physical devices and systems within the organization are inventoried.	A MUD-enabled IoT device is configured to emit a MUD URL. The	Upon connection to the network, the MUD-enabled IoT	Pass

	<p>NIST SP 800-53 Rev. 4 CM-8, PM-5 ID.AM-2: Software platforms and applications within the organization are inventoried.</p> <p>NIST SP 800-53 Rev. 4 CM-8, PM-5 ID.AM-3: Organizational communication and data flows are mapped.</p> <p>NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 PR.DS-5: Protections against data leaks are implemented.</p> <p>NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.</p> <p>PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.</p> <p>NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate.</p> <p>NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7 PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality).</p> <p>NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10</p>	<p>DHCP server extracts the MUD URL, which is sent to the MUD manager. The MUD manager requests the MUD file and signature from the MUD file server, and the MUD file server serves the MUD file to the MUD manager. The MUD file explicitly permits traffic to/from some internet services and hosts and implicitly denies traffic to/from all other internet services. The MUD manager translates the MUD file information into local network configurations that it installs on the router or switch that is serving as the MUD PEP for the IoT device.</p>	<p>device has its MUD policy enforcement point (PEP) router/switch automatically configured according to the MUD file’s route filtering policies.</p>	
--	--	---	--	--

	<p>PR.IP-3: Configuration change control processes are in place. NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10</p> <p>PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. NIST SP 800-53 Rev. 4 AC-3, CM-7</p> <p>PR.DS-2: Data in transit is protected.</p>			
IoT-2	<p>PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks). NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11</p>	<p>A MUD-enabled IoT device is configured to emit a URL for a MUD file, but the MUD file server that is hosting that file does not have a valid TLS certificate. Local policy has been configured to ensure that if the MUD file for an IoT device is located on a server with an invalid certificate, the router/switch will be configured to deny all communication to/from the device.</p>	<p>When the MUD-enabled IoT device is connected to the network, the MUD manager sends locally defined policy to the router/switch that handles whether to allow or block traffic to the MUD-enabled IoT device. Therefore, the MUD PEP router/switch will be configured to block all traffic to and from the IoT device.</p>	Pass
IoT-3	<p>PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity. NIST SP 800-53 Rev. 4 SI-7</p>	<p>A MUD-enabled IoT device is configured to emit a URL for a MUD file, but the certificate that was used to sign the MUD file had already expired at the time of signing. Local policy has been configured to ensure that if the MUD file for a device has a signature that was signed by a</p>	<p>When the MUD-enabled IoT device is connected to the network and the MUD file and signature are fetched, the MUD manager will detect that the MUD file’s signature was created by using a certificate that had already expired</p>	Pass

		certificate that had already expired at the time of signature, the device’s MUD PEP router/switch will be configured to deny all communication to/from the device.	at the time of signing. According to local policy, the MUD PEP will be configured to block all traffic to/from the device.	
IoT-4	PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity. NIST SP 800-53 Rev. 4 SI-7	A MUD-enabled IoT device is configured to emit a URL for a MUD file, but the signature of the MUD file is invalid. Local policy has been configured to ensure that if the MUD file for a device is invalid, the router/switch will be configured to deny all communication to/from the IoT device.	When the MUD-enabled IoT device is connected to the network, the MUD manager sends locally defined policy to the router/switch that handles whether to allow or block traffic to the MUD-enabled IoT device. Therefore, the MUD PEP router/switch will be configured to block all traffic to and from IoT device.	Pass
IoT-5	ID.AM-3: Organizational communication and data flows are mapped. NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 PR.DS-5: Protections against data leaks are implemented. NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality).	Test IoT-1 has run successfully, meaning that the MUD PEP router/switch has been configured based on a MUD file that permits traffic to/from some internet locations and implicitly denies traffic to/from all other internet locations.	When the MUD-enabled IoT device is connected to the network, its MUD PEP router/switch will be configured to enforce the route filtering that is described in the device’s MUD file with respect to traffic being permitted to/from some internet locations; and traffic being implicitly blocked to/from	Pass (for testable procedure –ingress cannot be tested)

	<p>NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10</p> <p>PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.</p> <p>NIST SP 800-53 Rev. 4 AC-3, CM-7</p>		all remaining internet locations.	
IoT-6	<p>ID.AM-3: Organizational communication and data flows are mapped.</p> <p>NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8</p> <p>PR.DS-5: Protections against data leaks are implemented.</p> <p>NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4</p> <p>PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate.</p> <p>NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7</p> <p>PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality).</p> <p>NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10</p> <p>PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.</p> <p>NIST SP 800-53 Rev. 4 AC-3, CM-7</p>	<p>Test IoT-1 has run successfully, meaning that the MUD PEP router/switch has been configured based on a MUD file that permits traffic to/from some lateral hosts and implicitly denies traffic to/from all other lateral hosts. (The MUD file does not explicitly identify the hosts as lateral hosts; it identifies classes of hosts to/from which traffic should be denied, where one or more hosts of this class happen to be lateral hosts.)</p>	<p>When the MUD-enabled IoT device is connected to the network, its MUD PEP router/switch will be configured to enforce the access control information that is described in the device’s MUD file with respect to traffic being permitted to/from some lateral hosts; and traffic being implicitly blocked to/from all remaining lateral hosts.</p>	<p>Pass (for testable procedure –ingress cannot be tested)</p>
IoT-7	<p>PR.IP-3: Configuration change control processes are in place.</p> <p>NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10</p>	<p>Test IoT-1 has run successfully, meaning that the MUD PEP router/switch has</p>	<p>When the MUD-enabled IoT device explicitly releases its IP address lease,</p>	<p>Pass</p>

	<p>PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.</p>	<p>been configured based on the MUD file for a specific MUD-enabled device in question. Next, have the IoT device change DHCP state by explicitly releasing its IP address lease, causing the device’s policy configuration to be removed from the MUD PEP router/switch.</p>	<p>the MUD-related configuration for that IoT device will be removed from its MUD PEP router/switch.</p>	
IoT-8	<p>PR.IP-3: Configuration change control processes are in place. NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10</p> <p>PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.</p>	<p>Test IoT-1 has run successfully, meaning that the MUD PEP router/switch has been configured based on the MUD file for a specific MUD-enabled device in question. Next, have the IoT device change DHCP state by waiting until the IoT device’s address lease expires, causing the device’s policy configuration to be removed from the MUD PEP router/switch.</p>	<p>When the MUD-enabled IoT device’s IP address lease expires, the MUD-related configuration for that IoT device will be removed from its MUD PEP router/switch.</p>	<p>Failed (not supported)</p>
IoT-12	<p>ID.AM-1: Physical devices and systems within the organization are inventoried. NIST SP 800-53 Rev. 4 CM-8, PM-5</p> <p>ID.AM-2: Software platforms and applications within the organization are inventoried. NIST SP 800-53 Rev. 4 CM-8, PM-5</p> <p>ID.AM-3: Organizational communication and data flows are mapped.</p>	<p>A MUD-enabled IoT device is configured to emit a MUD URL. Upon being connected to the network, its MUD file is retrieved, and the PEP is configured to enforce the policies specified in that MUD URL for that device. Within 24 hours (i.e., within</p>	<p>Upon connection of the second IoT device to the network, the MUD manager does not contact the MUD file server. Instead, it uses the cached MUD file. It translates this MUD file’s contents into appropriate route-</p>	<p>Pass</p>

	<p>NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8</p> <p>PR.DS-5: Protections against data leaks are implemented.</p> <p>NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4</p> <p>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.</p> <p>PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.</p> <p>NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24</p> <p>PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate.</p> <p>NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7</p> <p>PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality).</p> <p>NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10</p> <p>PR.IP-3: Configuration change control processes are in place.</p> <p>NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10</p> <p>PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.</p>	<p>the cache-validity period for that MUD file), a second IoT device that has been configured to emit the same MUD URL is connected to the network.</p>	<p>filtering rules and installs these rules onto the PEP for the second IoT device.</p>	
--	--	--	---	--

	<p>NIST SP 800-53 Rev. 4 AC-3, CM-7 PR.DS-2: Data in transit is protected.</p>			
IoT-13	<p>ID.AM-1: Physical devices and systems within the organization are inventoried. NIST SP 800-53 Rev. 4 CM-8, PM-5 ID.AM-2: Software platforms and applications within the organization are inventoried. NIST SP 800-53 Rev. 4 CM-8, PM-5 ID.AM-3: Organizational communication and data flows are mapped. NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed. NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4 DE.CM-1: The network is monitored to detect potential cybersecurity events. NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4</p>	<p>A visibility/monitoring component is connected to the local IoT network. It is configured to detect all devices connected to the network, discover attributes of these devices, categorize the devices, and monitor the devices for any change of status.</p>	<p>Upon being connected to the network, the visibility/monitoring component detects all connected devices, identifies their attributes (e.g., type, IP address, OS), and categorizes them. When an additional device is powered on, it is also detected, and its attributes identified. When a device is powered off, its change of status is detected.</p>	Pass
IoT-14	<p>ID.AM-1: Physical devices and systems within the organization are inventoried.</p>	<p>A MUD-enabled IoT device is capable of emitting a MUD URL. The device should leverage one of the specified manners for emitting a MUD URL.</p>	<p>Upon initialization, the MUD-enabled IoT device broadcasts a DHCP message on the network, including at most one MUD URL, in https scheme, within the DHCP transaction. OR Upon initialization, the MUD-enabled IoT device emits a</p>	Pass

			MUD URL as an LLDP extension.	
--	--	--	--------------------------------------	--

1008 6 Findings and Recommendations

1009 This section introduces findings based on the build implementation and demonstration, as well as
1010 recommendations.

1011 6.1 Findings

- 1012 ▪ It is possible to provide significantly higher security than is typically achieved in today's (non-
1013 MUD-capable) home and small-business networks by deploying and using MUD on those
1014 networks.
- 1015 ▪ The NCCoE example solution demonstrates that by using MUD-capable IoT devices on
1016 networks where support for MUD has been deployed, it is possible to manage access to MUD-
1017 capable IoT devices in a manner that maintains device functionality while
- 1018 • preventing access to the MUD-capable IoT device from other components on the internal
1019 network that are not from authorized manufacturers or authorized device classes
 - 1020 • preventing the MUD-capable IoT device from being used to access unauthorized external
1021 domains
 - 1022 • preventing the MUD-capable IoT device from being used to access other components on
1023 the internal network that are not from authorized manufacturers or that are not
1024 authorized device types
- 1025 ▪ MUD can help prevent MUD-capable IoT devices from being used to launch DDoS and other
1026 attacks that are typically possible by commandeering non-MUD-capable IoT devices on today's
1027 home and small-business networks. To enable MUD to provide this protection, it must be
1028 deployed correctly, networks must use MUD-capable IoT devices, and MUD files must be
1029 written and available for these devices so that the files authorize only the outgoing
1030 communications that each MUD-capable IoT device needs to maintain its intended
1031 functionality.
- 1032 ▪ There are commercially available network visibility/monitoring technologies that are able to
1033 detect connected devices and identify certain device attributes (e.g., type, IP address, OS)
1034 throughout the duration of a device's connection to the network. These technologies are also
1035 able to detect when the devices leave the network or are powered off and to note their change
1036 of status accordingly.
- 1037 ▪ Setup and configuration of the components needed to deploy MUD on a network (MUD-
1038 capable router/switch and MUD manager) should ideally be able to be performed easily, right
1039 out of the box, to enable typical home or small-business users to deploy MUD successfully. It is

- 1040 not clear that the current suite of available products is sufficiently user-friendly to enable the
1041 typical, nontechnical user to easily and seamlessly deploy MUD on their home and small-
1042 business networks. However, improvements in the usability of MUD components are expected
1043 as more manufacturers implement support for MUD and as current manufacturers that
1044 support MUD refine the design of their MUD components to target the home and small-
1045 business user.
- 1046 ■ MUD has the potential to help with the security of even those IoT devices that have been
1047 deprecated and are no longer receiving regular updates. Eventually, most IoT devices will reach
1048 a point at which they will no longer be updated by their manufacturer. This is a dangerous
1049 point in any device’s life cycle because it means that any of its security vulnerabilities that
1050 become known after this point will not be protected against, leaving the device open to attack.
1051 For MUD-capable devices that reach this end-of-life stage, however, the use of MUD provides
1052 additional protection that is not available to non-MUD-capable devices. Even if a MUD-capable
1053 device can no longer be updated, its MUD file will still limit the other devices with which that
1054 MUD-capable device is able to communicate, thereby limiting what other devices could be
1055 used to attack it and what other devices it could be used to attack. In the future, there are
1056 expected to be many IoT devices that are no longer being updated by their manufacturers, yet
1057 that will continue to be used. The ability to leverage MUD to limit the communications profiles
1058 of such unsupported devices will be important for protecting these highly vulnerable devices
1059 from attack by unauthorized end points and for protecting the internet from attack by these
1060 vulnerable devices.
 - 1061 ■ Even when using components that are fully conformant to the MUD specification, there are
1062 still some behaviors that will be determined by local policy. If the default policy that is
1063 provided by a specific product out of the box is not sufficient, user action will be required to
1064 configure the device according to a different and desired policy. User-friendly interfaces will be
1065 needed to enable the typical, nontechnical user of a home or small-business network to
1066 interact with the MUD components to modify their default settings when needed. For
1067 example, the MUD specification does not dictate what action to take (e.g., block or permit
1068 traffic to the IoT device) if the MUD manager is not able to validate the device’s MUD file
1069 server’s TLS certificate or if the MUD manager is not able to validate the device’s MUD file’s
1070 certificate. In either of these cases, if the default behavior that the device is configured to
1071 perform is not acceptable, the user would need to configure the device to perform the desired
1072 behavior. Ideally the device would provide a user-friendly interface through which to do so.
 - 1073 ■ There is a dearth of MUD-capable IoT devices. Users wanting to deploy MUD do not yet have
1074 the option to do so because of a lack of availability of MUD-capable IoT devices. More vendor
1075 buy in is required to encourage IoT device manufacturers to implement support for MUD in
1076 their devices.
 - 1077 ■ Communications between the MUD manager and the router/switch, between the threat
1078 signaling server and the MUD manager/router, and between the IoT devices and their
1079 corresponding update servers are not standardized. This lack of standardization has the
1080 potential to inhibit interoperability of components that are obtained from different

- 1081 manufacturers, thereby limiting the choice that consumers have to mix architectural
1082 components from different vendors in their MUD deployments.
- 1083 ■ Specifically, for Build 1 we observed the following limitations that are informing improvements
1084 to the current proof-of-concept implementation:
- 1085 ● MUD Manager (version 1.0):
- 1086 ○ DNS resolution of internet host names in the MUD file is performed manually and
1087 remains static. The MUD manager does not invoke a DNS resolution service to
1088 automatically resolve the fully qualified domain names (FQDNs) that are referenced in
1089 MUD files dynamically at the time that it reads those MUD files. Instead, DNS
1090 resolution of FQDNs referenced in MUD files is performed manually by a human
1091 operator before beginning execution of the MUD manager service. The operator
1092 inserts this address resolution information into the MUD manager's .JSON
1093 configuration file, where it remains static for the duration of the operation of the MUD
1094 manager service. The MUD manager consults this configuration file, which is passed to
1095 it at the time the MUD manager service is started, to obtain this static DNS resolution
1096 information.
- 1097 Use of the .JSON configuration file as the mechanism to provide the MUD manager
1098 with DNS resolution information means that every FQDN that will be referenced in any
1099 MUD file must be resolved and inserted into the MUD manager's configuration file
1100 manually before beginning execution of the MUD manager service. So, for example, if
1101 a MUD file that will be used on the network permits traffic to be sent to domains
1102 *www.example.com* and *www.company.com*, the MUD manager's .JSON configuration
1103 file must be provided with lines that indicate that the FQDN *www.example.com*
1104 resolves to IP address 128.56.54.3 and the FQDN *www.company.com* resolves to IP
1105 address 128.54.35.2.
- 1106 Use of the .JSON configuration file as the mechanism to provide the MUD manager
1107 with DNS resolution information also means that the operator who is configuring the
1108 .JSON file must have prior knowledge of all FQDNs that will be referenced in all MUD
1109 files that will be used by devices on the network. If a MUD file references an FQDN that
1110 has not been listed and associated with a corresponding IP address in the MUD
1111 manager's .JSON configuration file, the MUD manager will not be able to configure an
1112 ACL to enforce controls related to that FQDN.
- 1113 In addition, because the DNS resolution information is passed to the MUD manager at
1114 execution time, this address resolution information remains static for as long as the
1115 MUD manager service continues to operate. To add new FQDN address resolutions or
1116 change existing ones, the MUD manager's .JSON file would have to be edited and the
1117 MUD manager process killed and restarted by using the new .JSON configuration file.
- 1118 Dynamic resolution of FQDNs is expected to be supported in the future.

- 1119 ○ Translation and implementation of the “model” construct from the MUD file was not
1120 supported at the time of testing. However, this should be addressed in newer versions.
- 1121 ● Catalyst 3850-S Switch (IOS version 16.09.02):
- 1122 ○ The MUD URL cannot be extracted when emitted via DHCPv6. Hence, the switch is only
1123 capable of supporting MUD-capable IoT devices that use DHCPv4 and IPv4. This version
1124 of the switch does not yet support MUD-capable IoT devices when they are configured
1125 to use IPv6. IPv6 functionality is expected to be supported in the future.
- 1126 ○ The DHCP server does not notify the MUD manager of changes in DHCP state for MUD-
1127 enabled IoT devices on the network. According to the MUD specification, the DHCP
1128 server should notify the MUD manager if the MUD-enabled IoT device’s IP address
1129 lease expires or has been released. However, this version of the DHCP server does not
1130 do so at the time of testing. This is expected to be addressed in the future.
- 1131 ○ Ingress Dynamic ACLs (DACLs) (i.e., DAACLs that pertain to traffic that is received from
1132 sources external to the network and directed to local IoT devices) are not supported
1133 with this version. Consequently, even if a MUD-capable IoT device’s MUD file indicates
1134 that the IoT device is not authorized to receive traffic from a particular external
1135 domain, the DAACL that is needed to prohibit that ingress traffic will not be configured
1136 on the switch. As a result, unless there is some other layer of security in place, such as
1137 a firewall that is configured to block this incoming traffic, the IoT device will still be
1138 able to receive incoming packets from that unauthorized external domain, which
1139 means it will still be vulnerable to attacks originating from that domain, despite the
1140 fact that the device’s MUD file makes it clear that the device is not authorized to
1141 receive traffic from that domain. Because egress DAACLs (i.e., DAACLs that pertain to
1142 traffic that is sent from IoT devices to an external domain) are supported, however,
1143 even though packets that are sent from an outside domain are not stopped from being
1144 received at the IoT device, return traffic from the device to the external domain will be
1145 stopped. This means, for example, that if an attacker is able to get packets to an IoT
1146 device from an outside domain, it will not be possible for the attacker to establish a
1147 TCP connection with the device from that outside domain, thereby limiting the range
1148 of attacks that can be launched against the IoT device. This is expected to be addressed
1149 in the future.
- 1150 ■ In working with project collaborators, the NCCoE determined that MUD is only one of several
1151 foundational elements that are important to IoT security. First and foremost, it is imperative
1152 that IoT device manufacturers follow best practices for security when designing, building, and
1153 supporting their devices. Manufacturers should, for example, understand and manage the
1154 security and privacy risks posed by their devices as discussed in [NISTIR 8228](#) (*Considerations for
1155 Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*) as well as the more general
1156 guidelines for identifying, assessing, and managing security risks that are discussed in the
1157 *Framework for Improving Critical Infrastructure Cybersecurity* ([Cybersecurity Framework](#)). In
1158 addition, they should continue to support their devices throughout their full life cycle, from

1159 initial availability through eventual decommissioning, with regular patches and updates. Cisco
1160 has proposed the following four elements as necessary for IoT security:

- 1161 • device security by design: Certifiable device capabilities
- 1162 • device intent: MUD
- 1163 • device network onboarding: Secure, scalable, automated–bootstrapping remote secure
1164 key infrastructure/autonomic networking integrated model approach
- 1165 • life-cycle management: behavior, software patches/updates

1166 The NCCoE recommends additional work with IoT security that builds on the broader set of
1167 security controls.

1168 6.2 Security Considerations

1169 Use of MUD, when implemented correctly, allows manufacturers to constrain communications to and
1170 from IoT devices to only those sources and destinations intended by the device’s manufacturer. By
1171 restricting an IoT device’s communications to only those that it needs to fulfill its intended function,
1172 MUD reduces both the communications vectors that can be used to attack a vulnerable IoT device and
1173 the communications vectors that a compromised IoT device can use to attack other devices. MUD does
1174 not, however, provide any inherent security protections to IoT devices themselves. If a device’s MUD
1175 file permits an IoT device to receive communications from a malicious domain, traffic from that domain
1176 can be used to attack the IoT device. Similarly, if the MUD file permits an IoT device to send
1177 communications to other domains, and if the IoT device is compromised, it can be used to attack those
1178 other domains. Users implementing MUD are advised to keep the following security considerations in
1179 mind.

- 1180 ■ It is important to ensure that the MUD implementation itself is secure and not vulnerable to
1181 attack. If the MUD implementation itself were to be compromised, the compromised MUD
1182 infrastructure would serve as a venue for attack. As stated in the Security Considerations
1183 section of the [MUD Specification \(RFC 8520\)](#), “the basic purpose of MUD is to configure access,
1184 and so by its very nature can be disruptive if used by unauthorized parties.” Protecting the
1185 MUD infrastructure includes ensuring the security of the IoT device MUD URL emission, the
1186 MUD manager, the DHCP server, the MUD file server, the router, and the private key used to
1187 sign the MUD file. If the MUD implementation itself is compromised—e.g., if an IoT device
1188 emits an incorrect MUD file URL; if a different MUD file URL is sent to the MUD manager than
1189 that provided by the IoT device; if a well-formed, signed MUD file is malicious; if a bad actor
1190 creates a compromised MUD manager; or if a router is compromised so that it does not
1191 enforce its ACL rules—then MUD can be used to enable rather than prevent potentially
1192 damaging communications between affected IoT devices and other domains.
- 1193 ■ If a bad actor is able to create a well-formed, signed, malicious MUD file, the undesirable
1194 communications that will be permitted by that MUD file will be readily visible by reading the

- 1195 MUD file. Therefore, for added protection, users implementing MUD should review the MUD
1196 file for their IoT devices to ensure it specifies communications that are appropriate for the
1197 device. Unfortunately, on home and small-business networks, where users are not likely to
1198 have the technical expertise to enable themselves to understand how to read MUD files, users
1199 will be required to trust that the MUD files specify communications appropriate for the device
1200 or rely on a third party to perform this review for them.
- 1201 ■ To protect all IoT devices on a network, both MUD-capable and non-MUD-capable, users may
1202 want to consider investigating mechanisms for supplying MUD files for legacy (non-MUD-
1203 capable) devices.
 - 1204 ■ By emitting a MUD URL, a device reveals information about itself, thereby potentially providing
1205 an attacker with guidance on what vulnerabilities it might have and how it might be attacked.
 - 1206 ■ An attacker could spy on the MUD manager to determine what devices are connected to the
1207 network and then use this information to plan an attack.
 - 1208 ■ If an attacker can gain access to the local network, they may be able to use the MUD manager
1209 in a reflected DoS attack by emitting a large amount of MUD URLs (e.g., from spoofed MAC
1210 addresses) and forcing the MUD manager to make connection attempts to retrieve files from
1211 those MUD URLs. Safeguards to counter this, such as throttling connection attempts of the
1212 MUD manager, should be considered.
 - 1213 ■ MUD users should understand that the main benefit of MUD is its ability to limit an IoT device's
1214 communications profile; it does not necessarily permit owners to find, identify, and correct
1215 already-compromised IoT devices.
 - 1216 ● If a system is compromised but it is still emitting the correct MUD URL, MUD can detect
1217 and stop any unauthorized communications that the device attempts. Such attempts may
1218 also indicate potential compromises.
 - 1219 ● On the other hand, a system could be compromised so that it emits a new URL referencing
1220 a MUD file that a malicious actor has created to enable the compromised device to engage
1221 in communications that should be prohibited. In this case, whether the compromised
1222 system will be detected depends on how the MUD manager is configured to react to such a
1223 change in MUD URL. According to the MUD specification, if a MUD manager determines
1224 that an IoT device is sending a different MUD URL, the MUD manager should not use this
1225 new URL without some additional validation, such as a review by a network administrator.
 - 1226 ○ If the MUD manager requires an administrator to accept the new URL but the
1227 administrator does not accept it, MUD would help owners detect the compromised
1228 system and limit the ability of the compromised system to be used in an attack.
 - 1229 ○ However, if the MUD manager does not require an administrator to accept the new URL
1230 or if it requires an administrator to accept the new URL and the administrator does
1231 accept the new URL, MUD would not help owners detect the compromised system, nor
1232 would it limit the ability of the compromised system to be used in an attack.

- 1233 ○ As a third possibility, a compromised system could be subjected to a more sophisticated
1234 attack that enables it to dynamically change its identity (e.g., its MAC address) along
1235 with emitting a new URL. In this case, the compromised system would not be detected
1236 unless the MUD manager were configured to require the administrator to explicitly add
1237 each new identity to the network.
- 1238 ■ The following security considerations are specific to the MUD deployment and configuration
1239 process:
- 1240 ● When an IoT device emits its MUD URL by using DHCP or LLDP rather than using an X.509
1241 certificate that can be used to provide strong authentication of the device, the device may
1242 be able to lie about its identity and thereby gain network access it should not have. If a
1243 network includes IoT devices that emit their MUD URL by using one of these insecure
1244 mechanisms, as does the MUD build implemented in this project, network administrators
1245 should take additional precautions to try to improve security. For example, the MUD
1246 implementation should be configured to:
- 1247 ○ prevent devices that have not been authenticated from being in the same class as
1248 devices that have been strongly authenticated to prevent the nonauthenticated devices
1249 from getting possibly elevated permissions that are granted to the authenticated
1250 devices
- 1251 ○ prevent devices that have not been authenticated from being able to use the same
1252 MUD URL as devices that have been strongly authenticated
- 1253 ○ whenever possible, bind communications to the authentication that has been used,
1254 e.g., IEEE 802.1X, 802.1AE (MACsec), 802.11i (WPA2), or future authentication types
- 1255 ○ remove state if an unauthenticated method of MUD URL emission is being used and any
1256 form of break in that session is detected
- 1257 ○ not include unauthenticated devices into the manufacturer grouping of any specific
1258 manufacturer without additional validation
- 1259 ○ use additional discovery and classification components that may be on the network to
1260 try to fingerprint devices that have not been authenticated to try to verify that they are
1261 of the type they are asserting to be by their MUD URLs
- 1262 ○ To protect against rogue Certificate Authorities, the MUD implementation should be
1263 configured to raise an alert and require administrator approval if the MUD manager
1264 detects that the signer of a MUD file has changed.
- 1265 ○ To protect compromised IoT devices that seek to be associated with malevolent MUD
1266 files, the MUD implementation should be configured to raise an alert and require
1267 administrator approval if the MUD manager detects that a device's MUD file has
1268 changed.

- 1269 ○ To protect against domain name ownership changes that would permit a bad actor to
 1270 provide MUD files for a device, MUD managers should be configured to cache
 1271 certificates used by the MUD file server. If a new certificate is retrieved, the MUD
 1272 manager should check to see if ownership of the domain has changed and, if so, it
 1273 should raise an alert and require administrator approval.

1274 The above bullets provide only a summary of the security considerations discussed in the [MUD](#)
 1275 [Specification \(RFC 8520\)](#). Users deploying a MUD implementation are encouraged to consult that
 1276 document directly for more detailed discussion.

1277 Additionally, please refer to [NISTIR 8228](#) (*Considerations for Managing Internet of Things (IoT)*
 1278 *Cybersecurity and Privacy Risks*) for more details related to IoT cybersecurity and privacy considerations.

1279 6.3 Recommendations

1280 The following are recommendations for using MUD:

- 1281 ■ Home and small-business network owners should enable MUD on their networks by deploying
 1282 a MUD-capable infrastructure.
- 1283 ■ Home and small-business network owners should select and use MUD-capable IoT devices on
 1284 their networks.
- 1285 ■ ISPs should consider providing and supporting MUD-capable home routers for their customers.
- 1286 ■ IoT device manufacturers should configure their devices to emit a MUD URL by default.
- 1287 ■ IoT device manufacturers should write MUD files for their devices. By doing so, they will be
 1288 able to provide network administrators the confidence to know what sort of access their
 1289 device needs (and what sort of access it does not need), and they will do so in a way that
 1290 someone trained to operate and install the device does not need to understand network
 1291 administration.
- 1292 ■ IoT device manufacturers should ensure that the MUD files for their devices remain
 1293 continuously available by hosting these MUD files at their specified MUD URLs throughout the
 1294 devices' life cycles.
- 1295 ■ IoT device manufacturers should update each of their MUD files over the course of their
 1296 devices' life cycles, as needed, in the event that the communications profiles for their devices
 1297 evolve.
- 1298 ■ Even after an IoT device manufacturer deprecates an IoT device so that it will no longer be
 1299 supported, the manufacturer should continue to make the device's MUD file available so the
 1300 device's communications profile can continue to be enforced. This will be especially important
 1301 for deprecated IoT devices that have unpatched vulnerabilities.
- 1302 ■ IoT device manufacturers should provide regular updates to patch security vulnerabilities and
 1303 other bugs that are discovered throughout the life cycle of their devices, and they should make

- 1304 these updates available at a designated URL that is explicitly named in the device’s MUD file as
1305 being a permissible end point with which the device may communicate.
- 1306 ■ Manufacturers of MUD managers, MUD-capable DHCP servers, and MUD-capable routers that
1307 are targeted for use on home and small-business networks should strive to make deployment
1308 and configuration of these devices as easy to understand and as user-friendly as possible to
1309 increase the probability that they will be deployed and configured correctly and securely, even
1310 when the person performing the deployment has limited understanding of network
1311 administration.
 - 1312 ■ Home and small-business network owners should have visibility into every device on their
1313 network. Any device is a potential attack or reconnaissance point that must be discovered and
1314 secured. In particular, non-MUD-capable devices are inviting targets.
 - 1315 ■ Home and small-business network owners should segment their networks where possible. In
1316 small-business and home environments it may not be possible to apply good segmentation
1317 policies. But at a minimum, where there are IoT devices that are known to have security risks,
1318 e.g., non-MUD-capable devices, keep these on a separate network segment from the everyday
1319 computing devices that are afforded with a higher level of cybersecurity protection via regular
1320 updates and security software. This is an important step to contain any threats that may
1321 emerge from the IoT devices.
 - 1322 ■ Home and small-business network owners should use the information presented in the
1323 Security Considerations section of the [MUD Specification \(RFC 8520\)](#) to enhance protection of
1324 MUD deployments.
 - 1325 ■ Home and small-business network owners should consider their deployment of MUD to be
1326 only one pillar in the overall security of their network and IoT devices. Deployment of MUD is
1327 not a substitute for performing best practices to ensure overall, comprehensive security for
1328 their network as a whole.
 - 1329 ■ Standards development organizations should standardize communications between the MUD
1330 manager and the router, between the threat signaling server and the MUD manager/router,
1331 and between the IoT devices and their corresponding update servers.
 - 1332 ■ Manufacturers of MUD-capable network components and MUD-capable IoT devices should
1333 consider MUD to be only one pillar in helping users secure their networks and IoT devices.
1334 Manufacturers should, for example, understand the security and privacy risks posed by their
1335 devices as discussed in [NISTIR 8228 \(Considerations for Managing Internet of Things \(IoT\)
1336 Cybersecurity and Privacy Risks\)](#) as well as the guidelines for identifying, assessing, and
1337 managing security risks that are discussed in the *Framework for Improving Critical
1338 Infrastructure Cybersecurity (Cybersecurity Framework)*. They should use this information as
1339 they make decisions regarding both how they design their MUD-capable components and the
1340 default configurations with which they provide these components, being mindful of the fact
1341 that home and small-business network users of their components may have only a limited
1342 understanding of network administration and security.

1343 The following recommendations are suggestions for continuing activity with the collaboration team:

- 1344 ▪ Continue work with collaborators to enhance MUD capabilities in their commercial products
1345 (see Section 6.1).
- 1346 ▪ Perform additional work that builds on the broader set of security controls identified in Section
1347 5.2.
- 1348 ▪ Work with collaborators to demonstrate MUD deployments that are configured to address the
1349 security considerations that are raised in the MUD specification, such as
 - 1350 • configuring IoT devices to emit their MUD URLs in a secure fashion by providing the IoT
1351 devices with credentials and binding the device’s MUD URLs with their identities
 - 1352 • restricting the access control permissions of IoT devices that do not emit their MUD URLs
1353 in a secure fashion, so they are not elevated beyond those of devices that do not present a
1354 MUD policy
 - 1355 • configuring the MUD manager to raise an exception and seek administrator approval if the
1356 signer of a MUD file or the MUD file itself changes
 - 1357 • for IoT devices that do not emit their MUD URLs in a secure fashion, if their MUD files
1358 include rules based on the “manufacturer” construct, performing additional validation
1359 measures before admitting the devices to that manufacturer class. For example, look up
1360 each device’s MAC address and verify that the manufacturer associated with that MAC
1361 address is the same as the manufacturer specified in the “manufacturer” construct in that
1362 device’s MUD file.
- 1363 ▪ Explore the possibility of using crowdsourcing and analytics to perform traffic flow analysis and
1364 thereby adapt and evolve traffic profiles of MUD-capable devices over the course of their use.
1365 Instead of simply dropping traffic that is received at the router if that traffic is not within the
1366 IoT device’s profile, this traffic could be quarantined, recorded, and analyzed for further study.
1367 An analytics application that receives such traffic from many sources would be able to analyze
1368 the traffic and determine whether there may be valid reasons to expand the device’s
1369 communications profile.
- 1370 ▪ Work with collaborators to define a blueprint to guide IoT device manufacturers as they build
1371 MUD support into their devices, from initial device availability to eventual decommissioning.
1372 Provide guidance on required and recommended manufacturer activities and considerations.

1373 **7 Future Build Considerations**

1374 As the MUD build proceeded, some emerging components were not included in our initial
1375 demonstration platform. The physical architecture described in Section 4.2 and the technologies
1376 identified in Section 4.3 describe those components that were demonstrated in the course of
1377 developing this preliminary practice guide. The team is working on additional builds that include

1378 additional components that have become available. Findings from the demonstration of components,
1379 including those described in Appendix A will appear in a subsequent version of this draft practice guide.

1380 The number of components that can employ the MUD protocol continues to grow rapidly. It is
1381 recommended that this project be further extended to demonstrate the capabilities of the maturing
1382 offerings of technology providers and to integrate additional related capabilities such as threat
1383 signaling. In addition, IPv6, for which MUD-capable products were unavailable for the initial
1384 demonstration sequences, adds a new dimension to using MUD to help mitigate IoT-based DDoS
1385 threats. As discussed in Section 7.2 below, inclusion of IPv6-capability should be considered for future
1386 builds.

1387 **7.1 Extension to Demonstrate the Growing Set of Available Components**

1388 ARM, CableLabs, Cisco, CTIA, DigiCert, ForeScout, Global Cyber Alliance, MasterPeace Solutions, Molex,
1389 Patton Electronics, and Symantec have signed CRADAs and are collaborating in the project. There is also
1390 strong interest from additional industry collaborators to participate in future builds, particularly if we
1391 expand the project scope to include the enterprise use case. Several of these new potential
1392 collaborators may submit letters of interest leading to CRADAs for participation in tackling the challenge
1393 of integrating MUD and other security features into enterprise or industrial IoT use cases. 7.2Appendix
1394 A describes components scheduled for demonstration in the second phase of this project.

1395 **7.2 Recommended Demonstration of IPv6 Implementation**

1396 Due to product limitations, the initial phase of this project involved support for only IPv4 and did not
1397 include investigation of IPv6 issues. Additionally, due to the absence of NAT in IPv6, all IPv6 devices are
1398 directly addressable. Hence, the potential for DDoS attacks against IPv6 networks could potentially be
1399 worse than it is against IPv4 networks. Consequently, we recommend that demonstration of MUD in an
1400 IPv6 environment be performed as part of follow-on work.

1401 **Appendix A Information Provided by Collaborators Related** 1402 **to Phase 2**

1403 This appendix provides information provided by collaborators regarding potential components to be
1404 used in future builds.

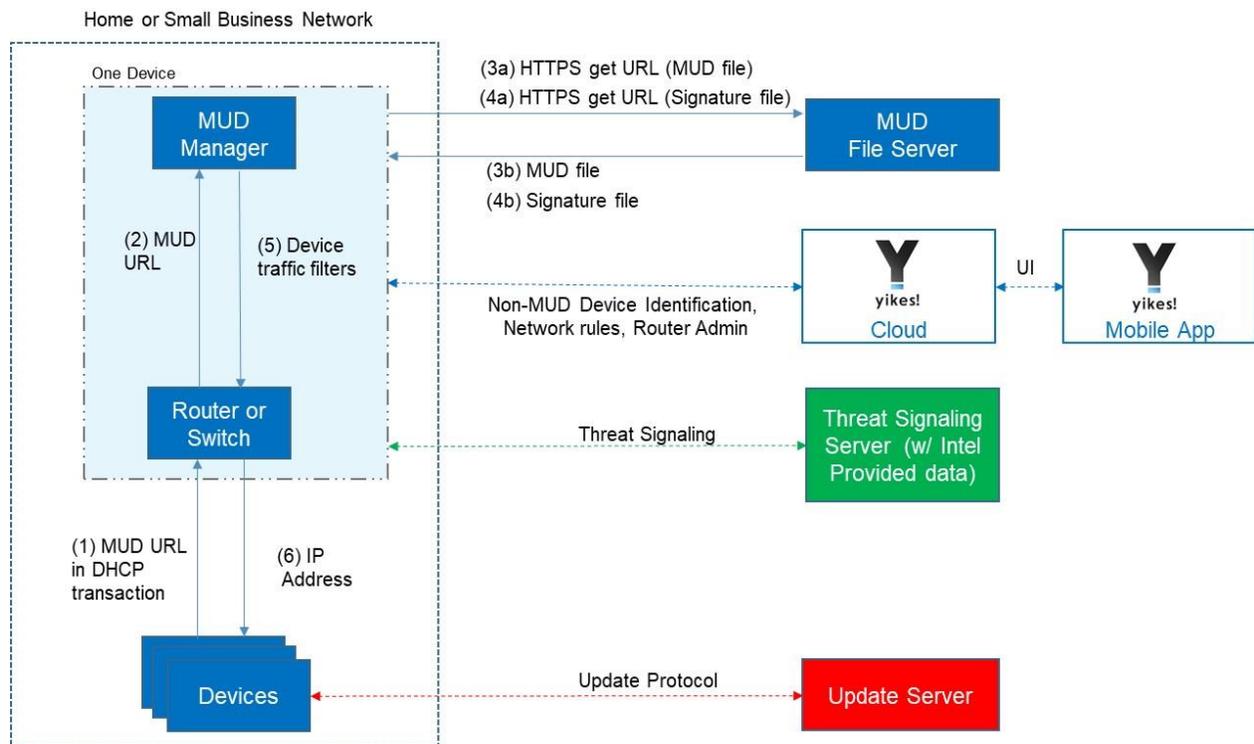
1405 **A.1 MasterPeace**

1406 MasterPeace Solutions Ltd is a cybersecurity company in Columbia, Maryland, that focuses on serving
1407 federal intelligence community agencies. MasterPeace also operates the MasterPeace LaunchPad start-
1408 up studio, chartered with launching cyber-oriented technology product companies. A current
1409 LaunchPad start-up portfolio company, Yikes!, has developed a solution that includes both a MUD
1410 manager and cloud-based support for non-MUD IoT device security. Yikes! was created to bring
1411 automated enterprise-level security to consumer and small-business networks. Those networks are
1412 typically flat (unsegmented), predominantly connected to by Wi-Fi-enabled devices, and managed by
1413 individuals who possess relatively little IT or cyber background compared with enterprise IT and cyber
1414 teams.

1415 **A.1.1 Yikes!**

1416 Yikes! is a commercial router/cloud service solution focused on consumer and small-business markets.
1417 Yikes! starts by thinking about networking differently and isolating every device on the network. As
1418 devices are added to a Yikes! home/small-business network, Yikes! leverages a cloud-based process to
1419 automatically identify and categorize devices and, based on categories, enables specific internet access
1420 (north/south [N/S]) and internal network access to specific devices (east/west [E/W]). Yikes! also
1421 provides a mobile application to allow users further fine-grained device filtering control. Yikes! includes
1422 a MUD manager that is compliant with the IETF MUD Specification. MUD rules for MUD-enabled devices
1423 are enforced automatically.

1424 Figure A-1 depicts a deployment of Yikes! and required related components. Yikes! is designed to run as
1425 a router with a connection to the Yikes! cloud and managed via the Yikes! mobile application.

1426 **Figure A-1 Yikes! Architecture**

1427

1428 **A.1.2 Yikes! Components**1429 **A.1.2.1 Yikes! Router**

1430 The Yikes! router initially isolates all devices connected to the router from all other devices on the
 1431 network. When devices connect to the router, the Yikes! router provides the device's DHCP header,
 1432 MAC address, operating system, and connection characteristics to the Yikes! cloud services. The Yikes!
 1433 router receives from the Yikes! cloud service rules for N/S and E/W filtering based on the Yikes! cloud
 1434 processing (see Yikes! Cloud) and custom user settings (see Yikes! App). The Yikes! router also handles
 1435 IoT devices that emit MUD URLs via DHCP. Yikes! reads these MUD URLs from the device, retrieves MUD
 1436 files associated with those URLs, and configures the traffic filters (access control lists) in the router to
 1437 enforce the communication limitations specified in the MUD file for each device.

1438 **A.1.2.2 Yikes! Cloud**

1439 The Yikes! cloud uses proprietary techniques and machine learning to analyze the DHCP header, MAC
 1440 address, operating system, and connection characteristics provided by the Yikes! router to
 1441 automatically classify the device, including Make, Model, and Yikes! Device category. Yikes! has a
 1442 comprehensive list of categories that includes these examples:

- 1443 ▪ Mobile: Phone, Tablet, eBook, Smart Watch, Wearable, Car
- 1444 ▪ Home & Office: Computer, Laptop, Printer, IP Phone, Scanner
- 1445 ▪ Smart Home: IP Camera, Smart Device, Smart Plug, Light, Voice Assistant, Thermostat,
1446 Doorbell, Baby Monitor
- 1447 ▪ Network: Router, Wi-Fi Extender
- 1448 ▪ Server: NAS, Server
- 1449 ▪ Engineering: Raspberry Pi, Arduino

1450 The Yikes! cloud then uses the Yikes! Category to define specific E/W rules for that device and every
1451 other device on the Yikes! router’s network. It also looks up the device in the Yikes! proprietary IoT
1452 device library, and if available, provides specialized N/S filtering rules for that device. The E/W and N/S
1453 rules are then returned to the Yikes! router for local enforcement.

1454 The Yikes! cloud also provides information about the device, its categorization, and filtering rules to the
1455 Yikes! application (see Yikes! App). This information is presented to the user, and the user can make
1456 specific changes. These changes are also provided to the Yikes! router for enforcement.

1457 **A.1.2.3 Yikes! Application**

1458 The Yikes! application is a mobile application (available from the iPhone App Store). It communicates
1459 with the Yikes! cloud, receiving information about the Yikes! router and all the devices connected to the
1460 router, including Yikes! device identification and categorization information and associated N/S and E/W
1461 network rules. The Yikes! application allows users to override the automated device information and
1462 change the filtering rules. User changes are communicated to the Yikes! cloud and then provided to the
1463 Yikes! router for enforcement.

1464 **A.1.3 Requirements**

1465 The Yikes! router is a self-contained router, Wi-Fi access point, and firewall that communicates locally
1466 with Wi-Fi devices and wired devices. Yikes! requires wide area network (WAN) access to the internet
1467 that allows MQTT access to the Yikes! cloud service.

1468 **A.1.3.1 Hardware**

1469 Yikes! provides a customized original equipment manufacturer (OEM) router.

1470 **A.1.3.2 Supported Network Architecture**

1471 Yikes! currently supports networks that use DHCP. Future work may be done to allow for protocols sup-
1472 porting RADIUS or LLDP compatibility.

1473 A.1.3.3 Required Components Status

1474 Yikes! WAN access to the internet must allow MQTT access to the Yikes! cloud service.

1475 A.1.4 Known Limitations

1476 Here is a list of some important things to be aware of with the current state of Yikes!:

- 1477 ▪ Does not implement MUD via LLDP
- 1478 ▪ Does not implement MUD via protocols supporting X.509 certificates
- 1479 ▪ The Yikes IoT Device Library currently supports automated N/S filtering for only a limited set of
1480 IoT devices.

1481 A.2 CableLabs

1482 As the leading Innovation and R&D lab for the cable industry, CableLabs creates global impact through
1483 its more than 60 cable-network-operator members around the world, representing approximately 180
1484 million subscribers and roughly 500 million individuals.

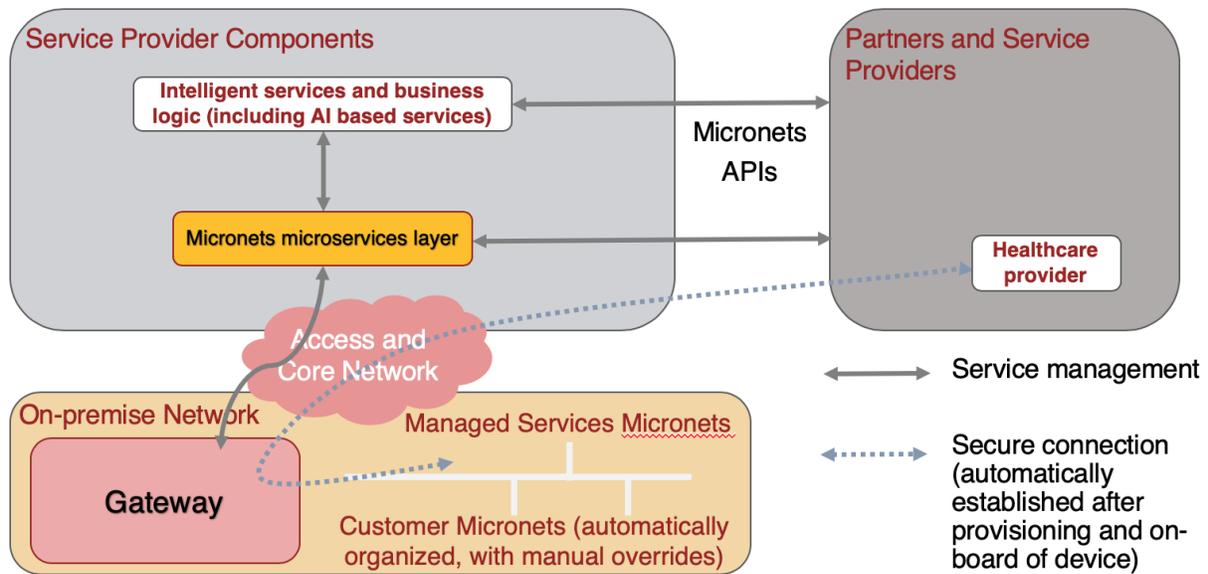
1485 A.2.1 CableLabs Micronets

1486 In [November 2018](#), CableLabs publicly announced [Micronets](#), a next-generation on-premise network
1487 platform focused on providing adaptive security for all devices connecting to a residential or small-
1488 business network through dynamic micro-segmentation and management of connectivity to those
1489 devices. Micronets is designed to provide seamless and transparent security to users without burdening
1490 them with the technical aspects of configuring the network. Micronets incorporates and leverages MUD
1491 as one technology component to help identify and manage the connectivity of devices, in support of the
1492 broader Micronets on-premise network platform. In addition, Micronets can provide enhanced security
1493 for high-value or sensitive devices, further reducing the risk of compromise for these devices and their
1494 applications. More detailed description can be found in CableLabs' [Micronets white paper](#).

1495 In addition to MUD, Micronets incorporates a number of device identity and fingerprinting techniques
1496 to enable real-time detection and quarantining of compromised IoT devices, minimizing the risk to other
1497 devices on the local network and to the broader internet. CableLabs deployed a Micronets instance in
1498 the NCCoE lab based on the open-source reference implementation available on [GitHub](#). CableLabs
1499 plans to continue to develop and add new features and functionality to the open-source reference
1500 implementation.

1501 As illustrated in Figure A-2 and described in more detail below, Micronets consists of the following
1502 architectural components: an intelligent services and business logic layer (e.g., machine learning-based
1503 services), a Micronets microservices layer, the on-premise network that includes the Micronets
1504 gateway, and the Micronets APIs that are exposed by each of these components.

1505 **Figure A-2 Micronets Reference Architecture**



1507 **A.2.1.1 Intelligent Services and Business Logic**

1508 This architectural component is the interface for the Micronets platform to interact with the rest of the
 1509 world. It functions as a receiver of the user’s intent and business rules from the user’s services and
 1510 combines them into operational decisions that are handed over to the Micronets microservices for
 1511 execution. It may receive information from various Micronets’ microservices (such as the software
 1512 defined networking [SDN] controller) and in turn use that information to dynamically update the access
 1513 rules for connected IoT devices. For example, to support devices that do not emit a MUD URL, a
 1514 “synthetic” MUD file generator and MUD server are provided that can host crowdsourced MUD files
 1515 that are provided to the Micronets microservices. Another example is an IoT fingerprinting service that
 1516 allows detection of devices in the network or an artificial intelligence/machine learning-based malware
 1517 detection service that can provide updated MUD files or access policies based on actively detected
 1518 threats in the network.

1519 **A.2.1.2 Micronets Microservices**

1520 This layer hosts a number of network management-related microservices that interact with the on-
 1521 premise gateway to manage the devices and network connectivity. One of the core microservices, the
 1522 Micronets Manager, coordinates the entire state of the Micronets-enabled on-premise network. It
 1523 orchestrates the overall services delivery to the devices and ultimately to the user. Several
 1524 microservices are engaged and managed by the Micronets Manager like the SDN controller, DHCP/DNS
 1525 manager, AAA server, and MUD manager.

1526 *A.2.1.2.1 MUD Manager*

1527 The MUD manager is responsible for retrieving MUD files, processing the MUD files, and generating the
1528 rules/policies that are consumed by the Micronets Manager to enforce SDN-based flow rules on the on-
1529 premise gateway. The MUD manager can get the files from either the MUD server or any other external
1530 location.

1531 **A.2.1.3 Micronets Gateway**

1532 The core networking component of Micronets is the gateway. The gateway implements an SDN-capable
1533 switch that is also integrated with the Wi-Fi access point. The gateway supports connectivity for both
1534 wired and wireless components.

1535 *A.2.1.3.1 Supported Hardware*

1536 The gateway components are implemented on an Ubuntu 16.04-based next unit of computing (NUC)
1537 with the Atheros AR9462 Wi-Fi chipset. A port of the current components on a Linksys WRT1900ACS
1538 based on OpenWRT is in progress.

1539 **A.2.1.4 On-Premise Micronets**

1540 The Micronets gateway is responsible for creation and enforcement of the Micronets. Each Micronet
1541 represents a distinct trust domain and at the minimum represents a distinct IP subnet.

1542 *A.2.1.4.1 MUD-Driven Policies*

1543 The Micronets definition and the device allocation within a given Micronets are governed by the
1544 Micronets manager and are driven by specific policies. A MUD-based policy drives the allocation of
1545 devices into specific Micronets.

1546 *A.2.1.4.2 Customer Micronets*

1547 Customers will acquire and connect their own devices. They may even integrate entire service-oriented
1548 networks, such as a smart home lighting system. Customer-networked devices may be fingerprinted or
1549 authenticated by using an ecosystem certificate (e.g., an [Open Connectivity Foundation](#) certified device)
1550 and automatically placed into an appropriate Micronet.

1551 **A.2.1.5 Micronets API Framework**

1552 Each component (the microservices as well as the gateway services) exposes a set of APIs that form the
1553 Micronets API framework. Some of the APIs can be exposed to allow partners and service providers to
1554 interface with the customer's Micronets environment to provision and deliver specific services that the
1555 customer has requested.

1556 **Appendix B List of Acronyms**

2FA	Two-factor Authentication
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
COA	Change of Authorization
CoAP	Constrained Application Protocol
CRADA	Cooperative Research and Development Agreement
Cybersecurity Framework	NIST Framework for Improving Critical Infrastructure Cybersecurity
DAACL	Dynamic Access Control List
DB	Database
DDoS	Distributed Denial of Service
Devkit	Development Kit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
IOS	Cisco's Internetwork Operating System
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IT	Information Technology
ITL	NIST's Information Technology Laboratory
LAN	Local Area Network
LED	Light-Emitting Diode
LLDP	Link Layer Discovery Protocol (IEEE 802.1AB)
MAB	MAC Authentication Bypass
MAC	Media Access Control
MQTT	Message Queuing Telemetry Transport
MUD	Manufacturer Usage Description
NAS	Network Address Server
NAT	Network Address Translation
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency/Internal Report
OS	Operating System
PC	Personal Computer

PEP	Policy Enforcement Point
PoE	Power over Ethernet
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RMF	Risk Management Framework
SP	Special Publication
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TLV	Type Length Value
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
WPA2	Wi-Fi Protected Access 2 Security Certificate Protocol (IEEE 802.11i-2004 standard)
WPA3	Wi-Fi Protected Access 3 Security Certificate protocol
YANG	Yet Another Next Generation

1557 **Appendix C** **Definitions**

Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures (National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12 Rev. 1)
Best Practice	A procedure that has been shown by research and experience to produce optimal results and that is established or proposed as a standard suitable for widespread adoption (Merriam-Webster)
Botnet	The word botnet is formed from the words “robot” and “network.” Cyber criminals use special Trojan viruses to breach the security of several users’ computers, take control of each computer, and organize all the infected machines into a network of “bots” that the criminal can remotely manage. (https://usa.kaspersky.com/resource-center/threats/botnet-attacks)
Control	A measure that is modifying risk (Note: Controls include any process, policy, device, practice, or other actions that modify risk.) (NIST Interagency/Internal Report 8053)
Denial of Service	The prevention of authorized access to a system resource or the delaying of system operations and functions (NIST SP 800-82 Rev. 2)
Distributed Denial of Service (DDoS)	A denial of service technique that uses numerous hosts to perform the attack (NIST Interagency/Internal Report 7711)
Managed Devices	Personal computers, laptops, mobile devices, virtual machines, and infrastructure components require management agents, allowing information technology staff to discover, maintain and control them. Those with broken or missing agents cannot be seen or managed by agent-based security products.
Mapping	Depiction of how data from one information source maps to data from another information source
Mitigate	To make less severe or painful or to cause to become less harsh or hostile (Merriam-Webster)

Manufacturer Usage Description (MUD)	A component-based architecture specified in Request for Comments (RFC) 8250 that is designed to provide a means for end devices to signal to the network what sort of access and network functionality they require to properly function
MUD-Capable	An Internet of Things (IoT) device that is capable of emitting a MUD uniform resource locator (URL) in compliance with the MUD specification
Network Address Translation	A function by which internet protocol (IP) addresses within a packet are replaced with different IP addresses. This function is most commonly performed by either routers or firewalls. It enables private IP networks that use unregistered IP addresses to connect to the internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.
Non-MUD-Capable	An IoT device that is not capable of emitting a MUD URL in compliance with the MUD specification (RFC 8250)
Policy	Statements, rules, or assertions that specify the correct or expected behavior of an entity. For example, an authorization policy might specify the correct access control rules for a software component. (NIST SP 800-95 and NIST Interagency/Internal Report 7621 Rev. 1)
Policy enforcement point	A network device on which policy decisions are carried out or enforced
Risk	The net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. (NIST SP 800-30)
Router	A computer that is a gateway between two networks at open system interconnection (OSI) layer 3 and that relays and directs data packets through that internetwork. The most common form of router operates on IP packets. (NIST SP 800-82 Rev. 2)
Server	A computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries). (NIST SP 800-47)

Security Control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements (NIST SP 800-53 Rev. 4)
Shall	A requirement that must be met unless a justification of why it cannot be met is given and accepted (NIST Interagency/Internal Report 5153)
Should	This term is used to indicate an important recommendation. Ignoring the recommendation could result in undesirable results. (NIST SP 800-108)
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability (FIPS 200)
Threat Signaling	Real-time signaling of DDoS-related telemetry and threat-handling requests and data between elements concerned with DDoS attack detection, classification, trace back, and mitigation (https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/cybersecurity-network-and-information-security)
Traffic Filter	An entry in an access control list that is installed on the router or switch to enforce access controls on the network
Uniform Resource Locator (URL)	A reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. A typical URL could have the form <i>http://www.example.com/index.html</i> , which indicates a protocol (http), a host name (<i>www.example.com</i>), and a file name (<i>index.html</i>). Also sometimes referred to as a <i>web address</i> .
Update	New, improved, or fixed software, which replaces older versions of the same software. For example, updating an operating system brings it up-to-date with the latest drivers, system utilities, and security software. Updates are often provided by the software publisher free of charge. (https://www.computerhope.com/jargon/u/update.htm)
Update Server	A server that provides patches and other software updates to IoT devices.

- VLAN** A broadcast domain that is partitioned and isolated within a network at the data link layer. A single physical local area network (LAN) can be logically partitioned into multiple, independent VLANs; a group of devices on one or more physical LANs can be configured to communicate within the same VLAN, as if they were attached to the same physical LAN.
- Vulnerability** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (NIST SP 800-37 Rev. 2)

1558 **Appendix D Functional Evaluation Plan**

1559 The functional evaluation plan describes the test cases conducted.

1560 **D.1 Build 1**

1561 Functional evaluations of the Internet of Things (IoT) example implementations, as constructed in the
1562 Mitigating IoT-Based DDoS lab, were conducted to verify they meet their requirements. Figure 4-6
1563 details the lab environment. Additionally, the architecture shown in Figure 4-1 is used as a guiding
1564 principle for this test plan.

1565 It is assumed that prior to testing the example implementation, all communication paths to the IoT
1566 devices on the network are open and could potentially be used to attack systems on the internet. It is
1567 also assumed that for traffic to be sent to/from one IoT device to another that traffic must pass through
1568 the router/switch.

1569 The MUD Specification defines three methods for an IoT device to emit a MUD URL: DHCP, LLDP, and
1570 X.509 extensions. This functional evaluation plan shows the methods that were leveraged in the
1571 example implementation—emission via DHCP and LLDP.

1572 **D.1.1 Build 1 Requirements**

1573 Each functional test case is designed to verify that the example implementation meets a specific set of
1574 requirements. These requirements are closely aligned to the order of operations in the [Manufacturer
1575 Usage Description \(MUD\) Specification \(RFC 8520\)](#). These requirements are listed in Table D-1. Each of
1576 these requirements contains two separate tests, one using IPv4, and one using IPv6 for devices that
1577 support IPv6. At the time of testing, the IPv6 functionality was not fully supported by the
1578 implementation and was not evaluated. The names of the tests in which each requirement is tested are
1579 listed in the right-most column of Table D-1. Tests that end with the suffix “v4” are those in which IPv4
1580 addressing is used; tests that end with the suffix “v6” are those in which IPv6 addressing is used.

1581 **Table D-1: Functional IoT Use Case Requirements**

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
CR 1	The IoT DDoS example implementation shall include a MUD-enabled IoT device that can emit a MUD URL.			IoT-1-v4, IoT-1-v6, IoT-14-v4, IoT-14-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
CR 1.a		Upon initialization, the MUD-enabled IoT device shall broadcast a DHCP message on the network, including at most one MUD URL, in https scheme, within the DHCP transaction.		IoT-1-v4, IoT-1-v6, IoT-14-v4, IoT-14-v6
CR-1.a.1			The DHCP server shall be able to receive DHCPv4 DISCOVER and/or REQUEST with IANA code 161 (OPTION_MUD_URL_V4) from the MUD-enabled IoT device.	IoT-1-v4, IoT-14-v4
CR-1.a.2			The DHCP server shall be able to receive DHCPv6 Solicit and/or Request with IANA code 112 (OPTION_MUD_URL_V6) from the MUD-enabled IoT device.	IoT-1-v6, IoT-14-v6
CR-1.b		Upon initialization, the MUD-enabled IoT device shall emit the MUD URL as an LLDP extension.		IoT-1-v4, IoT-1-v6, IoT-14-v4, IoT-14-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
CR-1.b.1			The network service shall be able to process the MUD URL that is received as an LLDP extension .	IoT-1-v4, IoT-1-v6, IoT-14-v4, IoT-14-v6
CR 2	The IoT DDoS example implementation shall include the capability for the extracted MUD URL to be forwarded to a MUD manager .			IoT-1-v4, IoT-1-v6
CR-2.a		The DHCP server shall assign an IP address lease to the MUD-enabled IoT device.		IoT-1-v4, IoT-1-v6
CR-2.a.1			The MUD-enabled IoT device shall receive the IP address .	IoT-1-v4, IoT-1-v6
CR-2.b		The DHCP server shall receive the DHCP message and extract the MUD URL, which is then passed to the MUD manager .		IoT-1-v4, IoT-1-v6
CR-2.b.1			The MUD manager shall receive the MUD URL .	IoT-1-v4, IoT-1-v6
CR 3	The IoT DDoS example implementation shall include a			IoT-1-v4, IoT-1-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
	MUD manager that is capable of requesting a MUD file and signature from a MUD file server.			
CR-3.a		The MUD manager shall use the “GET” method (RFC 7231) to request MUD and signature files (per RFC 7230) from the MUD file server and is able to validate the MUD file server’s TLS certificate by using the rules in RFC 2818.		IoT-1-v4, IoT-1-v6
CR-3.a.1			The MUD file server shall receive the https request from the MUD manager.	IoT-1-v4, IoT-1-v6
CR-3.b		The MUD manager shall use the GET method (RFC 7231) to request MUD and signature files (per RFC 7230) from the MUD file server but it is not able to validate the MUD file server’s TLS certificate by using the rules in RFC 2818.		IoT-2-v4, IoT-2-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
CR-3.b.1			The MUD manager shall drop the connection to the MUD file server.	IoT-2-v4, IoT-2-v6
CR-3.b.2			The MUD manager shall send locally defined policy to the router or switch that handles whether to allow or block traffic to/from the MUD-enabled IoT device.	IoT-2-v4, IoT-2-v6
CR 4	The IoT DDoS example implementation shall include a MUD file server that is capable of serving a MUD file and signature to the MUD manager.			IoT-1-v4, IoT-1-v6
CR-4.a		The MUD file server shall serve the file and signature to the MUD manager, and the MUD manager shall check to determine whether the certificate used to sign the MUD file (signed using distinguished encoding rules (DER)-encoded Cryptographic Message Syntax [CMS])		IoT-1-v4, IoT-1-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
		[RFC 5652) was valid at the time of signing, i.e., the certificate had not expired.		
CR-4.b		The MUD file server shall serve the file and signature to the MUD manager, and the MUD manager shall check to determine whether the certificate used to sign the MUD file was valid at the time of signing, i.e., the certificate had already expired when it was used to sign the MUD file.		IoT-3-v4, IoT-3-v6
CR-4.b.1			The MUD manager shall cease to process the MUD file.	IoT-3-v4, IoT-3-v6
CR-4.b.2			The MUD manager shall send locally defined policy to the router or switch that handles whether to allow or block traffic to/from the MUD-enabled IoT device.	IoT-3-v4, IoT-3-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
CR 5	The IoT DDoS example implementation shall include a MUD manager that is capable of translating local network configurations based on the MUD file.			IoT-1-v4, IoT-1-v6
CR-5.a		The MUD manager shall successfully validate the signature of the MUD file.		IoT-1-v4, IoT-1-v6
CR-5.a.1			The MUD manager, after validation of the MUD file signature, shall check for an existing MUD file, compare both files, and translate abstractions in the MUD file to router or switch configurations if the new MUD file is an update.	IoT-1-v4, IoT-1-v6
CR-5.a.2			The MUD manager shall cache this newly received MUD file.	IoT-12-v4, IoT-12-v6
CR-5.b		The MUD manager shall attempt to validate the signature of the MUD file , but the signature validation fails (even though the		IoT-4-v4, IoT-4-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
		certificate that had been used to create the signature had not been expired at the time of signing, i.e., the signature is invalid for a different reason).		
CR-5.b.1			The MUD manager shall cease processing the MUD file.	IoT-4-v4, IoT-4-v6
CR 5.b.2			The MUD manager shall send locally defined policy to the router or switch that handles whether to allow or block traffic to/from the MUD-enabled IoT device.	IoT-4-v4, IoT-4-v6
CR 6	The IoT DDoS example implementation shall include a MUD manager that is capable of configuring the MUD PEP , i.e., the router or switch nearest the MUD-enabled IoT device that emitted the URL.			IoT-1-v4, IoT-1-v6
CR-6.a		The MUD manager shall install a router configuration on the router or switch nearest the MUD-enabled		IoT-1-v4, IoT-1-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
		IoT device that emitted the URL.		
CR-6.a.1			The router or switch shall have been configured to enforce the route filter sent by the MUD manager.	IoT-1-v4, IoT-1-v6
CR 7	The IoT DDoS example implementation shall allow the MUD-enabled IoT device to communicate with approved internet services in the MUD file.			IoT-5-v4, IoT-5-v6
CR-7.a		The MUD-enabled IoT device shall attempt to initiate outbound traffic to approved internet services.		IoT-5-v4, IoT-5-v6
CR-7.a.1			The router or switch shall receive the attempt and shall allow it to pass based on the filters from the MUD file.	IoT-5-v4, IoT-5-v6
CR-7.b		An approved internet service shall attempt		IoT-5-v4, IoT-5-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
		to initiate a connection to the MUD-enabled IoT device.		
CR-7.b.1			The router or switch shall receive the attempt and shall allow it to pass based on the filters from the MUD file.	IoT-5-v4, IoT-5-v6
CR 8	The IoT DDoS example implementation shall deny communications from a MUD-enabled IoT device to unapproved internet services (i.e., services that are denied by virtue of not being explicitly approved).			IoT-5-v4, IoT-5-v6
CR-8.a		The MUD-enabled IoT device shall attempt to initiate outbound traffic to unapproved (implicitly denied) internet services.		IoT-5-v4, IoT-5-v6
CR-8.a.1			The router or switch shall receive the attempt and shall deny it based on the filters from the MUD file.	IoT-5-v4, IoT-5-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
CR-8.b		An unapproved (implicitly denied) internet service shall attempt to initiate a connection to the MUD-enabled IoT device.		IoT-5-v4, IoT-5-v6
CR-8.b.1			The router or switch shall receive the attempt and shall deny it based on the filters from the MUD file.	IoT-5-v4, IoT-5-v6
CR-8.c		The MUD-enabled IoT device shall initiate communications to an internet service that is approved to initiate communication with the MUD-enabled device but not approved to receive communications initiated by the MUD-enabled device.		IoT-5-v4, IoT-5-v6
CR-8.c.1			The router or switch shall receive the attempt and shall deny it based on the filters from the MUD file.	IoT-5-v4, IoT-5-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
CR-8.d		An internet service shall initiate communication to a MUD-enabled device that is approved to initiate communications with the internet service but that is not approved to receive communications initiated by the internet service.		IoT-5-v4, IoT-5-v6
CR-8.d.1			The router or switch shall receive the attempt and shall deny it based on the filters from the MUD file.	IoT-5-v4, IoT-5-v6
CR 9	The IoT DDoS example implementation shall allow the MUD-enabled IoT device to communicate laterally with devices that are approved in the MUD file.			IoT-6-v4, IoT-6-v6
CR-9.a		The MUD-enabled IoT device shall attempt to initiate lateral traffic to approved devices.		IoT-6-v4, IoT-6-v6
CR-9.a.1			The router or switch shall receive the at-	IoT-6-v4, IoT-6-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
			tempt and shall allow it to pass based on the filters from the MUD file.	
CR-9.b		An approved device shall attempt to initiate a lateral connection to the MUD-enabled IoT device.		IoT-6-v4, IoT-6-v6
CR-9.b.1			The router or switch shall receive the attempt and shall allow it to pass based on the filters from the MUD file.	IoT-6-v4, IoT-6-v6
CR 10	The IoT DDoS example implementation shall deny lateral communications from MUD-enabled IoT device to devices that are not approved in the MUD file (i.e., devices that are implicitly denied by virtue of not being explicitly approved).			IoT-6-v4, IoT-6-v6
CR-10.a		The MUD-enabled IoT device shall attempt to initiate lateral traffic to unapproved (implicitly denied) devices.		IoT-6-v4, IoT-6-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
CR-10.a.1			The router or switch shall receive the attempt and shall deny it based on the filters from the MUD file.	IoT-6-v4, IoT-6-v6
CR-10.b		An unapproved (implicitly denied) device shall attempt to initiate a lateral connection to the MUD-enabled IoT device.		IoT-6-v4, IoT-6-v6
CR-10.b.1			The router or switch shall receive the attempt and shall deny it based on the filters from the MUD file.	IoT-6-v4, IoT-6-v6
CR 11	The IoT DDoS example implementation shall remove the implemented policy when the MUD-enabled IoT device changes DHCP state.			IoT-7-v4, IoT-7-v6
CR-11.a		The MUD-enabled IoT device shall explicitly release the IP address lease (i.e., it sends a DHCP release message to the DHCP server).		IoT-7-v4, IoT-7-v6
CR-11.a.1			The DHCP server shall notify the MUD	IoT-7-v4, IoT-7-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
			manager that the device's IP address lease has been released.	
CR-11.a.2			The MUD manager shall remove all policies associated with the disconnected IoT device that had been configured on the MUD PEP router/switch.	IoT-7-v4, IoT-7-v6
CR-11.b		The MUD-enabled IoT device's IP address lease shall expire.		IoT-8-v4, IoT-8-v6
CR-11.b.1			The DHCP server shall notify the MUD manager that the device's IP address lease has expired.	IoT-8-v4, IoT-8-v6
CR-11.b.2			The MUD manager shall remove all policies associated with the affected IoT device that had been configured on the MUD PEP router/switch.	IoT-8-v4, IoT-8-v6
CR 12	The IoT DDoS example implementation shall include a			IoT-9-v4, IoT-9-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
	<p>router or switch that is capable of receiving and implementing threat signaling information from a threat signaling server that includes “blacklisted” URLs and hosts that are not considered to be trusted. The router/switch shall be capable of being configured so it applies threat signaling rules to both MUD-enabled and non-MUD-capable devices, depending on local policy.</p>			
CR-12.a		<p>The router or switch shall receive threat signals from the threat signaling server and translate them into appropriate permit/deny configuration rules that will pertain to all devices (both MUD-enabled and non-MUD-capable).</p>		IoT-9-v4, IoT-9-v6
CR-12.a.1			<p>A non-MUD-capable IoT device shall attempt to initiate outbound traffic to a blacklisted internet URL. The router or switch shall receive</p>	IoT-9-v4, IoT-9-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
			<p>the attempt and shall deny it based on the filters from the threat signaling server.</p>	
CR-12.a.2			<p>There shall be an attempt to initiate a connection from a blacklisted internet URL to a non-MUD-capable IoT device. The router or switch shall receive the attempt and shall deny it based on the filters from the threat signaling server.</p>	IoT-9-v4, IoT-9-v6
CR-12.a.3			<p>The MUD-enabled IoT device shall attempt to initiate outbound traffic to an internet URL that is explicitly permitted in its MUD file but that has been blacklisted by the threat signaling service. The router or switch shall receive the attempts and shall deny it based on the filters from the threat signaling server.</p>	IoT-9-v4, IoT-9-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
CR-12.a.4			<p>A blacklisted internet URL that is explicitly permitted in a MUD-enabled device’s MUD file shall attempt to send traffic to the MUD-enabled device. The router or switch shall receive the attempt and shall deny it based on the filters from the threat signaling server.</p>	IoT-9-v4, IoT-9-v6
CR 13	<p>The IoT DDoS example implementation shall include a router or switch that is capable of receiving and implementing threat signaling information from a threat signaling server that includes “blacklisted” URLs and hosts that are not considered to be trusted. The router/switch shall be capable of being configured so that it applies threat signaling rules only to non-MUD-capable devices, based on local policy.</p>			IoT-10-v4, IoT-10-v6
CR-13.a		<p>The router or switch shall receive threat signals from the threat signaling server</p>		IoT-10-v4, IoT-10-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
		and translate them into appropriate permit/deny configuration rules that will pertain only to non-MUD-capable devices.		
CR-13.a.1			The non-MUD-capable IoT device shall attempt to initiate outbound traffic to blacklisted internet URL. The router or switch shall receive the attempt and shall deny it based on the filters from the threat signaling server.	IoT-10-v4, IoT-10-v6
CR-13.a.2			There shall be an attempt to initiate a connection from a blacklisted internet URL to the non-MUD-capable IoT device. The router or switch shall receive the attempt and shall deny it based on the filters from the threat signaling server.	IoT-10-v4, IoT-10-v6
CR-13.a.3			The MUD-enabled IoT device shall at-	IoT-10-v4, IoT-10-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
			<p>tempt to initiate outbound traffic to an internet URL that is explicitly permitted in its MUD file but that has been black-listed by the threat signaling service. The router or switch shall receive the attempt and shall permit it because the filters from the threat signaling server do not apply to MUD-enabled devices.</p>	
CR-13.a.4			<p>A device from a blacklisted internet URL that is explicitly permitted in a MUD-enabled device’s MUD file shall attempt to send traffic to the MUD-enabled IoT device. The router or switch shall receive the attempt and shall permit it because the filters from the threat signaling server do not apply to MUD-enabled devices.</p>	IoT-10-v4, IoT-10-v6
CR-14	The IoT DDoS example implementation shall include the			IoT-11

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
	capability to handle life-cycle changes, such as decommissioning IoT devices.			
CR-14.a		MUD-enabled IoT device manufacturers should provide a final MUD file for devices no longer being supported.		IoT-11
CR-14.a.1			The MUD manager shall use the final MUD file to configure traffic filters for the IoT device per CR 1-6.	IoT-11
CR-15	The IoT DDoS example implementation shall include a MUD manager that uses a cached MUD file rather than retrieve a new one if the cache-validity time period has not yet elapsed for the MUD file indicated by the MUD URL.			IoT-12-v4, IoT-12-v6
CR-15.a		The MUD manager shall check if the file associated with the MUD URL is present in its cache and shall determine that it is.		IoT-12-v4, IoT-12-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
CR-15.a.1			The MUD manager shall check whether the amount of time that has elapsed since the cached file was retrieved is less than or equal to the number of hours in the cache-validity value for this MUD file . If so, the MUD manager shall apply the contents of the cached MUD file.	IoT-12-v4, IoT-12-v6
CR-15.a.2			The MUD manager shall check whether the amount of time that has elapsed since the cached file was retrieved is greater than the number of hours in the cache-validity value for this MUD file . If so, the MUD manager may (but does not have to) fetch a new file by using the MUD URL received.	IoT-12-v4, IoT-12-v6
CR-16	The IoT DDoS example implementation shall include a visibility component that is able to detect, identify, categorize, and monitor the status			IoT-13-v4, IoT-13-v6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Subrequirement 2	Test Case
	of IoT devices that are on the network.			
CR-16.a		The visibility component shall detect and identify the attributes and category of a newly connected IoT device.		IoT-13-v4, IoT-13-v6
CR-16.a.1			The visibility component shall monitor the status of the IoT device (e.g., notice if the device goes of- fline).	IoT-13-v4, IoT-13-v6

1582

1583 **D.1.2 Build 1 Test Cases**

1584 Each test case consists of multiple fields that collectively identify the goal of the test, the specifics
 1585 required to implement the test, and how to assess the results of the test. Table D-2 describes each field
 1586 in any given test case.

1587 **Table D-2: Test Case Fields**

Test Case Field	Description
Parent Requirement	Identifies the top-level requirement or the series of top-level requirements leading to the testable requirement.
Testable Requirement	Guides the definition of the remainder of the test case fields. Specifies the capability to be evaluated.

Test Case Field	Description
Description	Describes the objective of the test case.
Associated Test Cases	In some instances, a test case may be based on the outcome of (an)other test case(s). For example, analysis-based test cases produce a result that is verifiable through various means (e.g., log entries, reports, and alerts).
Associated Cybersecurity Framework Subcategories	Lists the Cybersecurity Framework Subcategories addressed by the test case.
IoT Device(s) Under Test	Text identifying which IoT device is being connected to the network in this test
MUD File(s) Used	Name of MUD file(s) used
Preconditions	The starting state of the test case. Preconditions indicate various starting state items, such as a specific capability configuration required or specific protocol and content.
Procedure	The step-by-step actions required to implement the test case. A procedure may consist of a single sequence of steps or multiple sequences of steps (with delineation) to indicate variations in the test procedure.
Expected Results	The expected results for each variation in the test procedure
Actual Results	The observed results
Overall Results	The overall result of the test as pass/fail

1588 The remainder of this section contains the test cases that were used to verify that the example
1589 implementations met the requirements listed in Table D-1. Each test case is presented in the format
1590 described in Table D-2. It is assumed that all tests are run on the lab architecture shown in the figure
1591 above. It is further assumed that for all tests, the MUD PEP is the router/switch that is nearest the IoT

1592 device in question. Only the IPv4 versions of each test are listed explicitly below. For each test that has
 1593 both an IPv4 and an IPv6 version, the IPv4 version of the test, IoT-n-v4, is identical to the IPv6 version of
 1594 the test, IoT-n-v6, except

- 1595 ▪ IoT-n-v6 devices are configured to use IPv6, whereas IoT-n-v4 devices are configured to use
 1596 IPv4.
- 1597 ▪ IoT-n-v6 devices are configured to use DHCPv6, whereas IoT-n-v4 devices are configured to use
 1598 DHCPv4.
- 1599 ▪ The IoT-n-v6 DHCPv6 message that is emitted includes the MUD URL option that uses IANA
 1600 code 112, whereas the IoT-n-v4 DHCPv4 message that is emitted includes the MUD URL option
 1601 that uses IANA code 161.

1602 In addition to the lab setup that is depicted in Figure 4-6, the following hosts and web servers must also
 1603 be set up and available to support the tests defined below. On the local network where the MUD man-
 1604 ager and IoT devices are located, hosts with the following names must exist and be reachable from an
 1605 IoT device that is plugged into the local network:

- 1606 ▪ *unnamed-host* (i.e., a local host that is not from the same manufacturer as the IoT device in
 1607 question and whose MUD URL is not explicitly mentioned in the MUD file of the IoT device in
 1608 question as denoting a class of devices with which the IoT device in question is permitted to
 1609 communicate. For example, if device A's MUD file says that it may communicate locally with
 1610 devices that have MUD URLs *www.zzz.com* and *www.xxx.com*, then a local host that has a
 1611 MUD file of *www.qqq.com* could be *unnamed-host*.)
- 1612 ▪ *anyhost-to* (i.e., a local host to which the IoT device in question is permitted to initiate
 1613 communications but not vice versa)
- 1614 ▪ *anyhost-from* (i.e., a local host that is permitted to initiate communications to the IoT device
 1615 but not vice versa)
- 1616 ▪ *same-manufacturer-host* (i.e., a local host that is from the same manufacturer as the IoT
 1617 device in question. For example, if device A's MUD file is found at URL *www.aaa.com* and
 1618 device B's MUD file is also found at URL *www.aaa.com*, then device B could be *same-*
 1619 *manufacturer-host*.)

1620 On the internet (i.e., outside the local network), the following web servers must be set up and reachable
 1621 from an IoT device that is plugged into the local network:

- 1622 ▪ *https://yes-permit-to.com* (i.e., an internet location to which the IoT device in question is
 1623 permitted to initiate communications, but not vice versa)
- 1624 ▪ *https://yes-permit-from.com* (i.e., an internet location that is permitted to initiate
 1625 communications to the IoT device but not vice versa)
- 1626 ▪ *https://unnamed.com* (i.e., an internet location with which the IoT device is not permitted to
 1627 communicate)

1628 Please note all the listed capabilities will be included in a single MUD file in which we will highlight the
 1629 specific capability being evaluated in the respective test.

1630 **D.1.2.1 Test Case IoT-1-v4**

1631 **Table D-3: Test Case IoT-1-v4**

Test Case Field	Description
Parent Requirements	<p>(CR 1) The IoT DDoS example implementation shall include a MUD-enabled IoT device that is capable of emitting a MUD URL.</p> <p>(CR 2) The IoT DDoS example implementation shall include the capability for the extracted MUD URL to be forwarded to a MUD manager.</p> <p>(CR 3) The IoT DDoS example implementation shall include a MUD manager that is capable of requesting a MUD file and signature from the MUD file server.</p> <p>(CR 4) The IoT DDoS example implementation shall include a MUD file server that is capable of serving a MUD file and signature to the MUD manager.</p> <p>(CR 5) The IoT DDoS example implementation shall include a MUD manager that is capable of translating local network configurations based on the MUD file.</p> <p>(CR 6) The IoT DDoS example implementation shall include a MUD manager that is capable of configuring the router or switch nearest the MUD-enabled IoT device that emitted the URL.</p>
Testable Requirements	<p>(CR 1.a) Upon initialization, the MUD-enabled IoT device shall broadcast a DHCP message on the network, including at most one MUD URL, in https scheme, within the DHCP transaction.</p> <p>(CR 1.a.1) DHCP server shall be able to receive DHCPv4 DISCOVER and /or REQUEST with IANA code 161 (OPTION_MUD_URL_V4) from the MUD-enabled IoT device (NOTE: Test IoT-1-v6 does not test this requirement; instead, it tests CR 1.a.2, which pertains to DHCPv6 rather than DHCPv4.)</p> <p>OR</p> <p>(CR 1.b) Upon initialization, the MUD-enabled IoT device shall emit MUD URL as an LLDP extension.</p>

Test Case Field	Description
	<p>(CR 1.b.1) The network service shall be able to process the MUD URL that is received as an LLDP extension.</p> <p>(CR 2.a) The DHCP server shall assign an IP address lease to the MUD-enabled IoT device.</p> <p>(CR 2.a.1) MUD-enabled IoT device shall receive the IP address.</p> <p>(CR 2.b) The DHCP server shall receive the DHCP message and extract the MUD URL, which is then passed to the MUD manager.</p> <p>(CR 2.b.1) The MUD manager shall receive the MUD URL.</p> <p>(CR 3.a) The MUD manager shall use the GET method (RFC 7231) to request MUD and signature files (per RFC 7230) from the MUD file server and is able to validate the MUD file server’s TLS certificate by using the rules in RFC 2818.</p> <p>(CR 3.a.1) MUD file server shall receive the https request from the MUD manager.</p> <p>(CR 4.a) The MUD file server shall serve the file and signature to the MUD manager, and the MUD manager shall check to determine whether the certificate used to sign the MUD file (signed using DER-encoded CMS [RFC 5652]) was valid at the time of signing, i.e., the certificate had not expired.</p> <p>(CR 5.a) The MUD manager shall successfully validate the signature of the MUD file.</p> <p>(CR 5.a.1) The MUD manager, after validation of the MUD file signature, shall check for an existing MUD file, compare both files, and translate abstractions in the MUD file to router or switch configurations if the new MUD file is an update.</p> <p>(CR 6.a) The MUD manager shall install a router configuration on the router or switch nearest the MUD-enabled IoT device that emitted the URL.</p> <p>(CR 6.a.1) The router or switch shall have been configured to enforce the route filter sent by the MUD manager.</p>
Description	Shows that, upon connection to the network, a MUD-enabled IoT device used in the IoT DDoS example implementation has its MUD PEP router/switch automatically configured to enforce the route filtering that is described in the device’s MUD file, assuming the MUD file has a

Test Case Field	Description
	valid signature and is served from a MUD file server that has a valid TLS certificate.
Associated Test Cases	N/A
Associated Cybersecurity Framework Subcategories	ID.AM-1, ID.AM-2, ID.AM-3, PR.DS-5, DE.AE-1, PR.AC-4, PR.AC-5, PR.IP-1, PR.IP-3, PR.PT-3, PR.DS-2
IoT Device(s) Under Test	Raspberry Pi
MUD File(s) Used	ciscopi2.json
Preconditions	<ol style="list-style-type: none"> 1. All devices have been configured to use IPv4, and the IoT device under test has been configured to emit a DHCPv4 message that includes the URL of its MUD file by using the DHCPv4 MUD URL option (IANA code 161). (Note that in the v6 version of this test, IPv6, DHCPv6, and IANA code 112 will be used.) 2. This MUD file is not currently cached at the MUD manager. 3. The device's MUD file has a valid signature that was signed by a certificate that had not yet expired, and it is being hosted on a MUD file server that has a valid TLS certificate. 4. The MUD PEP router/switch does not yet have any configuration settings pertaining to the IoT device being used in the test. 5. The MUD file for the IoT device being used in the test is identical to the MUD file provided in section D.1.3.
Procedure	Verify that the MUD PEP router/switch for the IoT device to be used in the test does not yet have any configuration settings installed with respect to the IoT device being used in the test. Also verify that the MUD file of the IoT device to be used is not currently cached at the MUD manager.

Test Case Field	Description
	<p>Power-on the IoT device and connect it to the test network. This should set in motion the following series of steps, which should occur automatically:</p> <ol style="list-style-type: none"> 1. IoT device automatically emits a MUD URL in one of the following methods: <ol style="list-style-type: none"> a. DHCPv4 message containing the device’s MUD URL (IANA code 161) (Note that in the v6 version of this test, IPv6, DHCPv6, and IANA code 112 will be used.) b. LLDP message containing the device’s MUD URL in its extension 2. Corresponding service is responsible for the following actions: <ol style="list-style-type: none"> a. DHCP server receives the DHCP message containing the IoT device’s MUD URL. b. LLDP server receives LLDP advertisement containing the IoT device’s MUD URL. 3. Respective service (LLDP or DHCP) extracts the MUD URL. 4. The MUD URL is then provided to the MUD manager. 5. The MUD manager automatically contacts the MUD file server that is located using the MUD URL, verifies that it has a valid TLS certificate, requests and receives the MUD file and signature from the MUD file server, validates the MUD file’s signature, and translates the MUD file’s contents into appropriate route filtering rules and installs these rules onto the MUD PEP for the IoT device in question so that this router/switch is now configured to enforce the policies specified in the MUD file. 6. DHCP server offers an IP address lease to the newly connected IoT device. 7. The IoT device requests this IP address lease, which the DHCP server acknowledges.
<p>Expected Results</p>	<p>The MUD PEP router/switch for the IoT device has had its configuration changed, i.e., it has been configured to enforce the policies specified in the IoT device’s MUD file. The expected configuration should resemble the following details:</p> <p>Extended IP access list mud-81726-v4fr.in</p>

Test Case Field	Description
	<pre> 10 permit tcp any host 192.168.4.7 eq www ack syn 20 permit tcp any host 192.168.10.104 eq www 30 permit tcp any host 192.168.10.105 eq www 50 permit tcp any 192.168.10.0 0.0.0.255 eq www 60 permit tcp any 192.168.13.0 0.0.0.255 eq www 70 permit tcp any 192.168.14.0 0.0.0.255 eq www 80 permit tcp any eq 22 any 81 permit udp any eq bootpc any eq bootps 82 permit udp any any eq domain 83 deny ip any any </pre> <p>All protocol exchanges described in steps 1–4 above are expected to occur and can be viewed via Wireshark if desired. If the router/switch does not get configured in accordance with the MUD file, each exchange of DHCP and MUD-related protocol traffic should be viewed on the network via Wireshark to determine which transactions did not proceed as expected, and the observed and absent protocol exchanges should be described here.</p>
Actual Results	<p><u>Dynamic access-session on switch:</u></p> <pre> Build1#sh access-session int g1/0/15 det Interface: GigabitEthernet1/0/15 IIF-ID: 0x1B6BCEA5 MAC Address: b827.ebeb.6c8b IPv6 Address: Unknown IPv4 Address: 192.168.13.9 User-Name: b827ebeb6c8b Status: Authorized Domain: DATA Oper host mode: multi-auth Oper control dir: both Session timeout: N/A Common Session ID: COA80A02000000A6A9828F06 Acct Session ID: 0x0000003b </pre>

Test Case Field	Description				
	<p>Handle: 0x2200009c Current Policy: mud-mab-test</p> <p>Server Policies: ACS ACL: mud-81726-v4fr.in Vlan Group: Vlan: 3</p> <p>Method status list:</p> <table border="0"> <thead> <tr> <th>Method</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>mab</td> <td>Authc Success</td> </tr> </tbody> </table> <p><u>access-list on switch:</u> Build1#sh access-list mud-81726-v4fr.in Extended IP access list mud-81726-v4fr.in 10 permit tcp any host 192.168.4.7 eq www ack syn 20 permit tcp any host 192.168.10.104 eq www 30 permit tcp any host 192.168.10.105 eq www 50 permit tcp any 192.168.10.0 0.0.0.255 eq www 60 permit tcp any 192.168.13.0 0.0.0.255 eq www 70 permit tcp any 192.168.14.0 0.0.0.255 eq www 80 permit tcp any eq 22 any 81 permit udp any eq bootpc any eq bootps 82 permit udp any any eq domain 83 deny ip any any</p>	Method	State	mab	Authc Success
Method	State				
mab	Authc Success				
Overall Results	Pass				

1632 Test Case IoT-1-v6 is identical to test case IoT-1-v4 except that IoT-1-v6 tests requirement CR-1.a.2,
 1633 whereas IoT-1-v4 tests requirement CR-1.a.1. Hence, as explained above, test IoT-1-v6 it uses IPv6,
 1634 DHCPv6, and IANA code 112 instead of using IPv4, DHCPv4, and IANA code 161.

1635 D.1.2.2 Test Case IoT-2-v4

1636 Table D-4: Test Case IoT-2-v4

Test Case Field	Description
Parent Requirement	(CR 3) The IoT DDoS example implementation shall include a MUD manager that is capable of requesting a MUD file and signature from the MUD file server.
Testable Requirement	(CR 3.b) The MUD manager shall use the GET method (RFC 7231) to request MUD and signature files (per RFC 7230) from the MUD file server, but it is not able to validate the MUD file server's TLS certificate using the rules in RFC 2818. (CR 3.b.1) The MUD manager shall drop the connection to the MUD file server. (CR 3.b.2) MUD manager shall send locally defined policy to the router or switch that handles whether to allow or block traffic to/from the MUD-enabled IoT device.
Description	Shows that if a MUD manager is not able to validate the TLS certificate of a MUD file server when trying to retrieve the MUD file for a specific IoT device, the MUD manager will drop the connection to the MUD file server and configure the router/switch according to locally defined policy regarding whether to allow or block traffic to the IoT device in question.
Associated Test Cases	IoT-14-v4 (for the v6 version of this test, IoT-14-v6)
Associated Cybersecurity Framework Subcategories	PR.AC-7
IoT Device(s) Under Test	Raspberry Pi
MUD File(s) Used	ciscopi2.json

Test Case Field	Description
Preconditions	<ol style="list-style-type: none"> 1. All devices have been configured to use IPv4, and the IoT device under test has been configured to emit a DHCPv4 message that includes the URL of its MUD file by using the DHCPv4 MUD URL option (IANA code 161). (Note that in the v6 version of this test, IPv6, DHCPv6, and IANA code 112 will be used.) 2. This MUD file is not currently cached at the MUD Manager. 3. The MUD file server that is hosting the MUD file of the device under test does not have a valid TLS certificate. 4. Local policy has been defined to ensure that if the MUD file for a device is located on a server with an invalid certificate, the router/switch will be configured to deny all communication to/from the device. 5. The MUD PEP router/switch for the IoT device to be used in the test does not yet have any configuration settings with respect to the IoT device being used in the test.
Procedure	<p>Verify that the MUD PEP router/switch for the IoT device to be used in the test does not yet have any configuration settings installed with respect to the IoT device being used in the test.</p> <p>Power-on the IoT device and connect it to the test network. This should set in motion the following series of steps, which should occur automatically:</p> <ol style="list-style-type: none"> 1. IoT device automatically emits a DHCPv4 message containing the device's MUD URL (IANA code 161). (Note that in the v6 version of this test, IPv6, DHCPv6, and IANA code 112 will be used.) 2. DHCP server receives the DHCP message containing the IoT device's MUD URL. 3. DHCP server offers an IP address lease to the newly connected IoT device. 4. The IoT device requests this IP address lease, which the DHCP server acknowledges. 5. DHCP server sends the MUD URL to the MUD manager.

Test Case Field	Description
	<p>6. The MUD manager automatically contacts the MUD file server that is located by using the MUD URL, determines that it does not have a valid TLS certificate, and drops the connection to the MUD file server.</p> <p>7. The MUD manager configures the router/switch that is closest to the IoT device so that it denies all communications to and from the IoT device.</p>
Expected Results	The MUD PEP router/switch for the IoT device has had its configuration changed, i.e., it has been configured to local policy for communication to/from the IoT device.
Actual Results	<pre> ***MUDC [STATUS][send_mudfs_request:2005]--> Request URI <https://mudfileserver/ciscopi2> </home/mudtester/ca.cert.pem> * Trying 192.168.4.5... * TCP_NODELAY set * Connected to mudfileserver (192.168.4.5) port 443 (#0) * found 1 certificate in /home/mudtester/ca.cert.pem * found 400 certificates in /etc/ssl/certs * ALPN, offering http/1.1 * SSL connection using TLS1.2 / EC- DHE_RSA_AES_256_GCM_SHA384 * server certificate verification failed. CAfile: /home/mudtester/ca.cert.pem CRLfile: none * stopped the pause stream! * Closing connection 0 ***MUDC [ERROR][fetch_file:182]--> curl_easy_perform() failed: Peer certificate cannot be authenticated with given CA certificates ***MUDC [INFO][send_mudfs_request:2019]--> Unable to reach MUD fileserver to fetch MUD file. Will try to ap- pend .json * Trying 192.168.4.5... </pre>

Test Case Field	Description
	<pre> * TCP_NODELAY set * Connected to mudfileserver (192.168.4.5) port 443 (#0) * found 1 certificate in /home/mudtester/ca.cert.pem * found 400 certificates in /etc/ssl/certs * ALPN, offering http/1.1 * SSL connection using TLS1.2 / EC- DHE_RSA_AES_256_GCM_SHA384 * server certificate verification failed. CAfile: /home/mudtester/ca.cert.pem CRLfile: none * stopped the pause stream! * Closing connection 0 ***MUDC [ERROR][fetch_file:182]--> curl_easy_perform() failed: Peer certificate cannot be authenticated with given CA certificates ***MUDC [ERROR][send_mudfs_request:2027]--> Unable to reach MUD fileserver to fetch .json file ***MUDC [INFO][mudc_construct_head:135]--> sta- tus_code: 204, content_len: 14, extra_headers: (null) ***MUDC [INFO][mudc_construct_head:152]--> HTTP header: HTTP/1.1 204 No Content Content-Length: 14 ***MUDC [INFO][send_error_result:176]--> error from FS ***MUDC [ERROR][send_mudfs_request:2170]--> mudfs_conn failed </pre> <hr/> <pre> Build1#sho access-session int g1018 det Interface GigabitEthernet1018 IIF-ID 0x181835C2 MAC Address b827.eba7.0533 IPv6 Address Unknown IPv4 Address 192.168.10.106 User-Name b827eba70533 </pre>

Test Case Field	Description
	<pre> Status Authorized Domain DATA Oper host mode multi-auth Oper control dir both Session timeout NA Common Session ID COA80A02000000CCBDB267F8 Acct Session ID 0x00000046 Handle 0x100000c2 Current Policy mud-mab-test Server Policies Method status list Method State mab Authc Success </pre>
Overall Results	Pass

1637 As explained above, test IoT-2-v6 is identical to test IoT-2-v4 except that it uses IPv6, DHCPv6, and IANA
 1638 code 112 instead of using IPv4, DHCPv4, and IANA code 161.

1639 **D.1.2.3 Test Case IoT-3-v4**

1640 **Table D-5: Test Case IoT-3-v4**

Test Case Field	Description
Parent Requirement	(CR 4) The IoT DDoS example implementation shall include a MUD file server that is capable of serving a MUD file and signature to the MUD manager.
Testable Requirement	(CR 4.b) The MUD file server shall serve the file and signature to MUD manager, and the MUD manager shall check to determine whether the certificate used to sign the MUD file was valid at the time of signing, i.e., the certificate had already expired when it was used to sign the MUD file.

Test Case Field	Description
	<p>(CR 4.b.1) The MUD manager shall cease to process the MUD file.</p> <p>(CR 4.b.2) The MUD manager shall send locally defined policy to router or switch that handles whether to allow or block traffic to/from the MUD-enabled IoT device.</p>
Description	Shows that if a MUD file server serves a MUD file with a signature that was created with an expired certificate, the MUD manager will cease processing the MUD file.
Associated Test Cases	IoT-14-v4 (for the v6 version of this test, IoT-14-v6)
Associated Cybersecurity Framework Subcategories	PR.DS-6
IoT Device(s) Under Test	Raspberry Pi
MUD File(s) Used	expiredcerttest.json
Preconditions	<ol style="list-style-type: none"> 1. All devices have been configured to use IPv4, and the IoT device under test has been configured to emit a DHCPv4 message that includes the URL of its MUD file by using the DHCPv4 MUD URL option (IANA code 161). (Note that in the v6 version of this test, IPv6, DHCPv6, and IANA code 112 will be used.) 2. This MUD file is not currently cached at the MUD manager. 3. The IoT device's MUD file is being hosted on a MUD file server that has a valid TLS certificate, but the MUD file signature was signed by a certificate that had already expired at the time of signature. 4. Local policy has been defined to ensure that if the MUD file for a device has a signature that was signed by a certificate that had already expired at the time of signature, the device's MUD PEP router/switch will be configured to deny all communication to/from the device.

Test Case Field	Description
	<p>5. The MUD PEP router/switch for the IoT device to be used in the test does not yet have any configuration settings with respect to the IoT device being used in the test.</p>
Procedure	<p>Verify that the MUD PEP router/switch for the IoT device to be used in the test does not yet have any configuration settings installed with respect to the IoT device being used in the test.</p> <p>Power-on the IoT device and connect it to the test network. This should set in motion the following series of steps, which should occur automatically:</p> <ol style="list-style-type: none"> 1. IoT device automatically emits a DHCPv4 message containing the device's MUD URL (IANA code 161). (Note that in the v6 version of this test, IPv6, DHCPv6, and IANA code 112 will be used.) 2. DHCP server receives the DHCP message containing the IoT device's MUD URL. 3. DHCP server offers an IP address lease to the newly connected IoT device. 4. The IoT device requests this IP address lease, which the DHCP server acknowledges. 5. DHCP server sends the MUD URL to the MUD manager. 6. The MUD manager automatically contacts the MUD file server that is located by using the MUD URL, verifies that it has a valid TLS certificate, and requests the MUD file and signature from the MUD file server. 7. The MUD file server serves the MUD file and signature to MUD manager, and the MUD manager detects that the MUD file's signature was created by using a certificate that had already expired at the time of signing. 8. The MUD manager configures the router/switch that is closest to the IoT device so that it denies all communications to and from the IoT device.

Test Case Field	Description
<p>Expected Results</p>	<p>The MUD PEP router/switch for the IoT device has had its configuration changed, i.e., it has been configured to deny all communication to/from the IoT device. The expected configuration should resemble the following:</p> <p>Expecting a show access session without a MUD file as seen below:</p> <pre> show access-session int g1018 det Interface GigabitEthernet1018 IIF-ID 0x181835C2 MAC Address b827.eba7.0533 IPv6 Address Unknown IPv4 Address 192.168.10.106 User-Name b827eba70533 Status Authorized Domain DATA Oper host mode multi-auth Oper control dir both Session timeout NA Common Session ID COA80A02000000CCBDB267F8 Acct Session ID 0x00000046 Handle 0x100000c2 Current Policy mud-mab-test </pre> <p>Server Policies</p> <pre> Method status list Method State mab Authc Success </pre>
<p>Actual Results</p>	<pre> ***MUDC [INFO][verify_mud_content:1594]--> BIO_reset <1> ***MUDC [ERROR][verify_mud_content:1604]--> Verification Failure </pre>

Test Case Field	Description
	<p>139713269933824:error:2E099064:CMS routines:cms_signerinfo_verify_cert:certificate verify error:../crypto/cms/cms_smime.c:253:Verify error:certificate has expired</p> <p>***MUDC [INFO][send_mudfs_request:2092]--> Verification failed. Manufacturer Index <0></p> <p>***MUDC [INFO][mudc_construct_head:135]--> status_code: 401, content_len: 19, extra_headers: (null)</p> <p>***MUDC [INFO][mudc_construct_head:152]--> HTTP header: HTTP/1.1 401 Unauthorized Content-Length: 19</p> <p>***MUDC [INFO][send_error_result:176]--> Verification failed</p> <p>***MUDC [ERROR][send_mudfs_request:2170]--> mudfs_conn failed</p> <hr/> <pre> Build1#sho access-session int g1018 det Interface GigabitEthernet1018 IIF-ID 0x181835C2 MAC Address b827.eba7.0533 IPv6 Address Unknown IPv4 Address 192.168.10.106 User-Name b827eba70533 Status Authorized Domain DATA Oper host mode multi-auth Oper control dir both Session timeout NA Common Session ID COA80A02000000CCBDB267F8 Acct Session ID 0x00000046 Handle 0x100000c2 Current Policy mud-mab-test </pre>

Test Case Field	Description				
	<p>Server Policies</p> <p>Method status list</p> <table border="1"> <thead> <tr> <th>Method</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>mab</td> <td>Authc Success</td> </tr> </tbody> </table>	Method	State	mab	Authc Success
Method	State				
mab	Authc Success				
Overall Results	Pass				

1641 As explained above, test IoT-3-v6 is identical to test IoT-3-v4 except that it uses IPv6, DHCPv6, and IANA
 1642 code 112 instead of using IPv4, DHCPv4, and IANA code 161.

1643 **D.1.2.4 Test Case IoT-4-v4**

1644 **Table D-6: Test Case IoT-4-v4**

Test Case Field	Description
Parent Requirement	(CR 5) The IoT DDoS example implementation shall include a MUD manager that is capable of translating local network configurations based on the MUD file.
Testable Requirement	<p>(CR-5.b) The MUD manager shall attempt to validate the signature of the MUD file, but the signature validation fails (even though the certificate that had been used to create the signature had not been expired at the time of signing, i.e., the signature is invalid for a different reason).</p> <p>(CR-5.b.1) The MUD manager shall cease processing the MUD file.</p> <p>(CR 5.b.2) MUD manager shall send locally defined policy to router or switch that handles whether to allow or block traffic to/from the MUD-enabled IoT device.</p>
Description	Shows that if the MUD manager determines that the signature on the MUD file it receives from the MUD file server is invalid, it will cease processing the MUD file and configure the

Test Case Field	Description
	router/switch according to locally defined policy regarding whether to allow or block traffic to the IoT device in question.
Associated Test Cases	IoT-14-v4 (for the v6 version of this test, IoT-14-v6)
Associated Cybersecurity Framework Subcategories	PR.DS-6
IoT Device(s) Under Test	Raspberry Pi
MUD File(s) Used	ciscop2.json
Preconditions	<ol style="list-style-type: none"> 1. All devices have been configured to use IPv4, and the IoT device under test has been configured to emit a DHCPv4 message that includes the URL of its MUD file by using the DHCPv4 MUD URL option (IANA code 161). (Note that in the v6 version of this test, IPv6, DHCPv6, and IANA code 112 will be used.) 2. This MUD file is not currently cached at the MUD manager. 3. The MUD file that is served from the MUD file server to the MUD manager has a signature that is invalid, even though it was signed by a certificate that had not expired at the time of signing. 4. Local policy has been defined to ensure that if the MUD file for a device has an invalid signature, the device's MUD PEP router/switch will be configured to deny all communication to/from the device. 5. The MUD PEP router/switch does not yet have any configuration settings with respect to the IoT device being used in the test.

Test Case Field	Description
Procedure	<p>Verify that the MUD PEP router/switch for the IoT device to be used in the test does not yet have any configuration settings installed with respect to the IoT device being used in the test.</p> <p>Power-on the IoT device and connect it to the test network. This should set in motion the following series of steps, which should occur automatically:</p> <ol style="list-style-type: none"> 1. IoT device automatically emits a DHCPv4 message containing the device's MUD URL (IANA code 161). (Note that in the v6 version of this test, IPv6, DHCPv6, and IANA code 112 will be used.) 2. DHCP server receives the DHCP message containing the IoT device's MUD URL. 3. DHCP server offers an IP address lease to the newly connected IoT device. 4. The IoT device requests this IP address lease, which the DHCP server acknowledges. 5. DHCP server sends the MUD URL to the MUD manager. 6. The MUD manager automatically contacts the MUD file server that is located by using the MUD URL, verifies that it has a valid TLS certificate, and requests the MUD file and signature from the MUD file server. 7. The MUD file server sends the MUD file, and the MUD manager detects that the MUD file's signature is invalid. 8. The MUD manager configures the router/switch that is closest to the IoT device so that it denies all communications to and from the IoT device.
Expected Results	<p>The MUD PEP router/switch for the IoT device has had its configuration changed, i.e., it has been configured to deny all communication to/from the IoT device. The expected configuration should resemble the following:</p> <p>Expecting a show access session without a MUD file as seen below:</p>

Test Case Field	Description
	<pre> sho access-session int g1018 det Interface GigabitEthernet1018 IIF-ID 0x181835C2 MAC Address b827.eba7.0533 IPv6 Address Unknown IPv4 Address 192.168.10.106 User-Name b827eba70533 Status Authorized Domain DATA Oper host mode multi-auth Oper control dir both Session timeout NA Common Session ID COA80A02000000CCBDB267F8 Acct Session ID 0x00000046 Handle 0x100000c2 Current Policy mud-mab-test Server Policies Method status list Method State mab Authc Success </pre>
<p>Actual Results</p>	<pre> > GET /ciscopi2.json HTTP/1.1 Host: mudfileserver Accept: */* [omitted for sake of length] ***MUDC [STATUS][send_mudfs_request:2060]--> Request signature URI <https://mudfileserver/ciscopi2.p7s> </home/mudtester/mud-intermediate.pem> * Trying 192.168.4.5... * TCP_NODELAY set </pre>

Test Case Field	Description
	<pre> * Connected to mudfileserv (192.168.4.5) port 443 (#0) * found 1 certificate in /home/mudtester/mud-intermediate.pem * found 400 certificates in /etc/ssl/certs * ALPN, offering http/1.1 * SSL connection using TLS1.2 / EC-DHE_RSA_AES_256_GCM_SHA384 * server certificate verification OK * server certificate status verification SKIPPED * common name: mudfileserv (matched) * server certificate expiration date OK * server certificate activation date OK * certificate public key: RSA * certificate version: #3 * subject: C=US,ST=Maryland,L=Rockville,O=National Cybersecurity Center of Excellence - NIST,CN=mudfileserv * start date: Fri, 05 Oct 2018 00:00:00 GMT * expire date: Wed, 13 Oct 2021 12:00:00 GMT * issuer: C=US,O=DigiCert Inc,CN=DigiCert Test SHA2 Intermediate CA-1 * compression: NULL * ALPN, server did not agree to a protocol > GET /ciscopi2.p7s HTTP/1.1 Host: mudfileserv Accept: */* [omitted for sake of length] ***MUDC [INFO][send_mudfs_request:2080]--> MUD signature file successfully retrieved ***MUDC [DEBUG][verify_mud_content:1543]--> MUD signature file (length 4680) [shortened logs] ***MUDC [INFO][verify_mud_content:1594]--> BIO_reset <1> </pre>

Test Case Field	Description
	<p>***MUDC [ERROR][verify_mud_content:1604]--> Verification Failure</p> <p>140561528563456:error:2E09A09E:CMS routines:CMS_SignerInfo_verify_content:verification failure:../crypto/cms/cms_sd.c:819:</p> <p>140561528563456:error:2E09D06D:CMS routines:CMS_verify:content verify error:../crypto/cms/cms_smime.c:393:</p> <p>***MUDC [INFO][send_mudfs_request:2092]--> Verification failed. Manufacturer Index <0></p> <p>***MUDC [INFO][mudc_construct_head:135]--> status_code: 401, content_len: 19, extra_headers: (null)</p> <p>***MUDC [INFO][mudc_construct_head:152]--> HTTP header: HTTP/1.1 401 Unauthorized</p> <p>Content-Length: 19</p> <p>***MUDC [INFO][send_error_result:176]--> Verification failed</p> <p>***MUDC [ERROR][send_mudfs_request:2170]--> mudfs_conn failed</p> <hr/> <p>Switch access-session:</p> <p>Build1#sho access-session int g1/0/18 det</p> <pre> Interface: GigabitEthernet1/0/18 IIF-ID: 0x11C404C6 MAC Address: b827.eba7.0533 IPv6 Address: Unknown IPv4 Address: 192.168.10.106 User-Name: b827eba70533 Status: Authorized Domain: DATA Oper host mode: multi-auth Oper control dir: both Session timeout: N/A Common Session ID: COA80A02000000CDBDB68A30 </pre>

Test Case Field	Description				
	<p>Acct Session ID: 0x00000047 Handle: 0x690000c3 Current Policy: mud-mab-test</p> <p>Server Policies:</p> <p>Method status list:</p> <table border="0" data-bbox="730 693 1218 777"> <tr> <td>Method</td> <td>State</td> </tr> <tr> <td>mab</td> <td>Authc Success</td> </tr> </table>	Method	State	mab	Authc Success
Method	State				
mab	Authc Success				
Overall Results	Pass				

1645 As explained above, test IoT-4-v6 is identical to test IoT-4-v4 except that it uses IPv6, DHCPv6, and IANA
 1646 code 112 instead of using IPv4, DHCPv4, and IANA code 161.

1647 **D.1.2.5 Test Case IoT-5-v4**

1648 **Table D-7: Test Case IoT-5-v4**

Test Case Field	Description
Parent Requirement	<p>(CR 7) The IoT DDoS example implementation shall allow a MUD-enabled IoT device to communicate with approved internet services in MUD file.</p> <p>(CR 8) The IoT DDoS example implementation shall deny a MUD-enabled IoT device to communicate with unapproved internet services (i.e., services that are implicitly denied by virtue of not being explicitly approved).</p>
Testable Requirement	<p>(CR-7.a) The MUD-enabled IoT device shall attempt to initiate outbound traffic to approved internet services.</p> <p>(CR-7.a.1) The router or switch shall receive the attempt and shall allow it to pass based on the filters from MUD file.</p>

Test Case Field	Description
	<p>(CR-7.b) An approved internet service shall attempt to initiate connection to MUD-enabled IoT device.</p> <p>(CR-7.b.1) The router or switch shall receive the attempt and shall allow it to pass based on the filters from MUD file.</p> <p>(CR-8.a) The MUD-enabled IoT device shall attempt to initiate outbound traffic to unapproved (implicitly denied) internet services.</p> <p>(CR-8.a.1) The router or switch shall receive the attempt and shall deny it based on the filters from MUD file.</p> <p>(CR-8.b) An unapproved (implicitly denied) internet service shall attempt to initiate a connection to the MUD-enabled IoT device.</p> <p>(CR-8.b.1) The router or switch shall receive the attempt and shall deny it based on the filters from the MUD file.</p> <p>(CR-8.c) The MUD-enabled IoT device shall initiate communications to an internet service that is approved to initiate communication with the MUD-enabled device but not approved to receive communications initiated by the MUD-enabled device.</p> <p>(CR-8.c.1) The router or switch shall receive the attempt and shall deny it based on the filters from the MUD file.</p> <p>(CR-8.d) An internet service shall initiate communications to a MUD-enabled device that is approved to initiate communications with the internet service but that is not approved to receive communications initiated by the internet service.</p> <p>(CR-8.d.1) The router or switch shall receive the attempt and shall deny it based on the filters from the MUD file.</p>
Description	Shows that, upon connection to the network, a MUD-enabled IoT device used in the IoT DDoS example implementation has its MUD PEP router/switch automatically configured to enforce the

Test Case Field	Description
	route filtering that is described in the device’s MUD file with respect to communication with internet services. Further shows that the policies that are configured on the MUD PEP router/switch with respect to communication with internet services will be enforced as expected, with communications that are configured as denied being blocked, and communications that are configured as permitted being allowed.
Associated Test Cases	IoT-1-v4 (for the v6 version of this test, IoT-1-v6)
Associated Cybersecurity Framework Subcategories	ID.AM-3, PR.DS-5, PR.IP-1, PR.PT-3
IoT Device(s) Under Test	Raspberry Pi
MUD File(s) Used	ciscopi2.json
Preconditions	<p>Test IoT-1-v4 (or IoT-1-v6) has run successfully, meaning that the MUD PEP router/switch has been configured to enforce the following policies for the IoT device in question (as defined in the MUD file in section D.1.3):</p> <ul style="list-style-type: none"> a) Explicitly permit <i>https://yes-permit-from.com</i> to initiate communication with the IoT device. b) Explicitly permit to the IoT device to initiate communication with <i>https://yes-permit-to.com</i>. c) Implicitly deny all other communications with the internet, including denying <ul style="list-style-type: none"> i) the IoT device to initiate communication with <i>https://yes-permit-from.com</i> ii) <i>https://yes-permit-to.com</i> to initiate communication with the IoT device iii) communication between the IoT device and all other internet locations, such as <i>https://unnamed-</i>

Test Case Field	Description
	<i>to.com</i> (by not mentioning this or any other URLs in the MUD file)
Procedure	<p>Note: Procedure steps with strike-through are not tested in this phase as ingress DACLs are not supported in this implementation.</p> <ol style="list-style-type: none"> 1. As stipulated in the preconditions, right before this test, test IoT-1-v4 (or IoT-1-v6) must have been run successfully. 2. Initiate communications from the IoT device to <i>https://yes-permit-to.com</i> and verify that this traffic is received at <i>https://yes-permit-to.com</i>. (egress) 3. Initiate communications to the IoT device from <i>https://yes-permit-to.com</i> and verify that this traffic is received at the MUD PEP, but it is not forwarded by the MUD PEP, nor is it received at the IoT device. (ingress) 4. Initiate communications to the IoT device from <i>https://yes-permit-from.com</i> and verify that this traffic is received at the IoT device. (ingress) 5. Initiate communications from the IoT device to <i>https://yes-permit-from.com</i> and verify that this traffic is received at the MUD PEP, but it is not forwarded by the MUD PEP, nor is it received at <i>https://yes-permit-from.com</i>. (ingress) 6. Initiate communications from the IoT device to <i>https://unnamed.com</i> and verify that this traffic is received at the MUD PEP, but it is not forwarded by the MUD PEP, nor is it received at <i>https://unnamed.com</i>. (egress) 7. Initiate communications to the IoT device from <i>https://unnamed.com</i> and verify that this traffic is received at the MUD PEP, but it is not forwarded by the MUD PEP, nor is it received at the IoT device. (ingress)
Expected Results	Each of the results that is listed as needing to be verified in procedure steps above occurs as expected.

Test Case Field	Description
Actual Results	<p>Procedure 2– Connection to update server successfully initiated by IoT device:</p> <pre> pi@raspberrypi:~ \$ wget http://www.update-server.com/ --2018-12-13 21:28:00-- http://www.update-server.com/ Resolving www.update-server.com (www.update-server.com)... 192.168.4.7 Connecting to www.update-server.com (www.update-server.com) 192.168.4.7 :80... connected. HTTP request sent, awaiting response... 200 OK Length: 10918 (11K) [text/html] Saving to: 'index.html.2' index.html.2 100%[=====] 10.66K --.-KB/s in 0s 2018-12-13 21:28:00 (30.6 MB/s) - 'index.html.2' saved [10918/10918]</pre> <hr/> <p>Procedure 3– Update server failed to connect to IoT device:</p> <pre> iot@update-server:~\$ wget http://192.168.13.9 --2018-12-13 21:49:36-- http://192.168.13.9/ Connecting to 192.168.13.9:80... failed: Connection timed out. Retrying.</pre> <hr/> <p>Procedure 6– IoT device failed to connect to unapproved server:</p> <pre> pi@raspberrypi:~ \$ wget http://192.168.4.105 --2018-12-14 16:42:36-- http://192.168.4.105/ Connecting to 192.168.4.105:80... failed: Connection timed out. Retrying.</pre>

Test Case Field	Description
	Procedure 7– Unapproved server attempts to connect to IoT device: <pre>[mud@unapprovedserver ~]\$ wget http://192.168.13.14 --2018-12-14 13:03:32-- http://192.168.13.14/ Connecting to 192.168.13.14:80... failed: Connection timed out. Retrying.</pre>
Overall Results	Pass (for testable procedures—as stated, ingress cannot be tested)

1649 As explained above, test IoT-5-v6 is identical to test IoT-5-v4 except that it uses IPv6, DHCPv6, and IANA
 1650 code 112 instead of using IPv4, DHCPv4, and IANA code 161.

1651 **D.1.2.6 Test Case IoT-6-v4**

1652 **Table D-8: Test Case IoT-6-v4**

Test Case Field	Description
Parent Requirement	(CR 9) The IoT DDoS example implementation shall allow MUD-enabled IoT device to communicate laterally with devices that are approved in MUD file. (CR 10) The IoT DDoS example implementation shall deny MUD-enabled IoT device to communicate laterally with devices that are not approved in MUD file (i.e., devices that are implicitly denied by virtue of not being explicitly approved).
Testable Requirement	(CR-9.a) The MUD-enabled IoT device shall attempt to initiate lateral traffic to approved devices. (CR-9.a.1) The router or switch shall receive the attempt and shall allow it to pass based on the filters from MUD file. (CR-9.b) An approved device shall attempt to initiate a lateral connection to the MUD-enabled IoT device.

Test Case Field	Description
	<p>(CR-9.b.1) The router or switch shall receive the attempt and shall allow it to pass based on the filters from MUD file.</p> <p>(CR-10.a) The MUD-enabled IoT device shall attempt to initiate lateral traffic to unapproved (implicitly denied) devices.</p> <p>(CR-10-a.1) The router or switch shall receive the attempt and shall deny it based on the filters from MUD file.</p> <p>(CR-10-b) An unapproved (implicitly denied) device shall attempt to initiate a lateral connection to MUD-enabled IoT device.</p> <p>(CR-10-b.1) The router or switch shall receive the attempt and shall deny it based on the filters from MUD file.</p>
Description	Shows that, upon connection to the network, a MUD-enabled IoT device used in the IoT DDoS example implementation has its MUD PEP router/switch automatically configured to enforce the route filtering that is described in the device's MUD file with respect to communication with lateral devices. Further shows that the policies that are configured on the MUD PEP router/switch with respect to communication with lateral devices will be enforced as expected, with communications that are configured as denied being blocked and communications that are configured as being allowed.
Associated Test Cases	IoT-1-v4 (for the v6 version of this test, IoT-1-v6)
Associated Cybersecurity Framework Subcategories	ID.AM-3, PR.DS-5, PR.AC-5, PR.IP-1, PR.PT-3, PR.IP-3, PR.DS-3
IoT Device(s) Under Test	Raspberry Pi
MUD File(s) Used	ciscopi2.json

Test Case Field	Description
Preconditions	<p>Test IoT-1-v4 (or IoT-1-v6) has run successfully, meaning that the MUD PEP router/switch has been configured to enforce the following policies for the IoT device in question with respect to local communications (as defined in the MUD files in section D.1.3):</p> <ul style="list-style-type: none"> a) Local-network class—Explicitly permit local communication to/from IoT device and any local hosts (including the specific local hosts <i>anyhost-to</i> and <i>anyhost-from</i>) for specific services, as specified in MUD file by source port any, destination port: 80; and protocol: TCP, and which party initiates the connection. b) Manufacturer class—Explicitly permit local communication to/from IoT device and other classes of IoT devices, as identified by their MUD URL (<i>www.device-type.com</i>), and further constrained by source port: any; destination port: 80; and protocol: TCP. c) Same-manufacturer class—Explicitly permit local communication to/from IoT devices of the same manufacturer as the IoT device in question (the domain in the MUD URLs (mudfileservers) of the other IoT devices is the same as the domain in the MUD URL (mudfileservers) of the IoT device in question), and further constrained by source port: any; destination port: 80; and protocol: TCP. d) Implicitly deny all other local communication that is not explicitly permitted in the MUD file, including denying <ul style="list-style-type: none"> i) anyhost-to to initiate communications with the IoT device ii) the IoT device to initiate communications with anyhost-to by using a source port, destination port, or protocol (TCP or UDP) that is not explicitly permitted iii) the IoT device to initiate communications with anyhost-from iv) anyhost-from to initiate communications with the IoT device by using a source port, destination port,

Test Case Field	Description
	<p>or protocol (TCP or UDP) that is not explicitly permitted</p> <ul style="list-style-type: none"> v) communications between the IoT device and all lateral hosts (including <i>unnamed-host</i>) whose MUD URLs are not explicitly mentioned as being permissible in the MUD file vi) communications between the IoT device and all lateral hosts whose MUD URLs are explicitly mentioned as being permissible, but using a source port, destination port, or protocol (TCP or UDP) that is not explicitly permitted vii) communications between the IoT device and all lateral hosts that are not from the same manufacturer as the IoT device in question viii) communications between the IoT device and a lateral host that is from the same manufacturer, but using a source port, destination port, or protocol (TCP or UDP) that is not explicitly permitted
<p>Procedure</p>	<p>Note: Procedure steps with strike-through are not tested in this phase as ingress DACLs are not supported in this implementation.</p> <ol style="list-style-type: none"> 1. As stipulated in the preconditions, right before this test, test IoT-1-v4 (or IoT-1-v6) must have been run successfully. 2. Local-network (ingress): Initiate communications to the IoT device from <i>anyhost-from</i> for specific permitted service, and verify that this traffic is received at the IoT device. 3. Local-network (egress): Initiate communications from the IoT device to <i>anyhost-from</i> for specific permitted service, and verify that this traffic is received at the MUD PEP, but it is not forwarded by the MUD PEP, nor is it received at <i>anyhost-from</i>.

Test Case Field	Description
	<p>4. Local-network, controller, my-controller, manufacturer class (egress): Initiate communications from the IoT device to <i>anyhost-to</i> for specific permitted service, and verify that this traffic is received at <i>anyhost-to</i>.</p> <p>5. Local-network, controller, my-controller, manufacturer-class (ingress): Initiate communications to the IoT device from anyhost-to for specific permitted service, and verify that this traffic is received at the MUD PEP, but it is not forwarded by the MUD PEP, nor is it received at the IoT device.</p> <p>6. No associated class (egress): Initiate communications from the IoT device to <i>unnamed-host</i> (where <i>unnamed-host</i> is a host that is not from the same manufacturer as the IoT device in question and whose MUD URL is not explicitly mentioned in the MUD file as being permitted), and verify that this traffic is received at the MUD PEP, but it is not forwarded by the MUD PEP, nor is it received at <i>unnamed-host</i>.</p> <p>7. No associated class (ingress): Initiate communications to the IoT device from <i>unnamed-host</i> (where <i>unnamed-host</i> is a host that is not from the same manufacturer as the IoT device in question and whose MUD URL is not explicitly mentioned in the MUD file as being permitted), and verify that this traffic is received at the MUD PEP, but it is not forwarded by the MUD PEP, nor is it received at the IoT device.</p> <p>8. Same-manufacturer class (egress): Initiate communications from the IoT device to <i>same-manufacturer-host</i> (where <i>same-manufacturer-host</i> is a host that is from the same manufacturer as the IoT device in question), and verify that this traffic is received at <i>same-manufacturer-host</i>.</p> <p>9. Same-manufacturer class (egress): Initiate communications from the IoT device to <i>same-manufacturer-host</i> (where <i>same-manufacturer-host</i> is a host that is from the same manufacturer as the IoT device in question) but using a port or protocol that is not specified, and verify that this traffic is received at the MUD PEP, but it is not forwarded by the MUD PEP, nor is it received at <i>same-manufacturer-host</i>.</p>

Test Case Field	Description
Expected Results	Each of the results that is listed as needing to be verified in the procedure steps above occurs as expected.
Actual Results	<p>3. Local_network (egress)–blocked:</p> <pre> pi@raspberrypi:~ \$ wget https://192.168.10.106/ --2019-01-31 19:59:23-- https://192.168.10.106/ Connecting to 192.168.10.106:443... failed: Connection timed out. Retrying.</pre> <hr/> <p>4. Local-network, controller, my-controller, manufacturer class (egress)–allowed:</p> <p>Local_Network:</p> <pre> pi@raspberrypi:~ \$ wget http://192.168.10.175 --2018-12-14 15:11:50-- http://192.168.10.175/ Connecting to 192.168.10.175:80... connected. HTTP request sent, awaiting response... 200 OK Length: 10701 (10K) [text/html] Saving to: 'index.html.4'</pre> <pre> index.html.4 100%[=====>] 10.45K --.-KB/s in 0s</pre> <p>2018-12-14 15:11:50 (41.4 MB/s) - 'index.html.4' saved [10701/10701]</p> <hr/> <p>Controller:</p> <pre> pi@raspberrypi:~ \$ wget http://192.168.10.105/ --2019-01-31 21:03:45-- http://192.168.10.105/ Connecting to 192.168.10.105:80... connected. HTTP request sent, awaiting response... 200 OK Length: 277 Saving to: 'index.html.10'</pre>

Test Case Field	Description
	<pre> in- dex.html.10 100%[=====>] 2 77 --.-KB/s in 0s 2019-01-31 21:03:45 (18.8 MB/s) - 'index.html.10' saved [277/277] ----- My-controller: pi@raspberrypi:~ \$ wget http://192.168.10.104/ --2019-01-31 21:06:39-- http://192.168.10.104/ Connecting to 192.168.10.104:80... connected. HTTP request sent, awaiting response... 200 OK Length: 10701 (10K) [text/html] Saving to: 'index.html.11' in- dex.html.11 100%[=====>] 10.4 5K --.-KB/s in 0s 2019-01-31 21:06:39 (32.5 MB/s) - 'index.html.11' saved [10701/10701] Manufacturer: pi@raspberrypi:~ \$ wget http://192.168.14.2/ --2019-01-31 21:13:47-- http://192.168.14.2/ Connecting to 192.168.14.2:80... connected. HTTP request sent, awaiting response... 200 OK Length: 10701 (10K) [text/html] Saving to: 'index.html.12' in- dex.html.12 100%[=====>] 10.4 5K --.-KB/s in 0s </pre>

Test Case Field	Description
	<p>2019-01-31 21:13:47 (39.6 MB/s) - 'index.html.12' saved [10701/10701]</p> <hr/> <p>6. No associated class (egress)–blocked: pi@raspberrypi:~ \$ wget http://192.168.15.105 --2018-12-14 17:15:36-- http://192.168.15.105/ Connecting to 192.168.15.105:80... failed: Connection timed out. Retrying.</p> <hr/> <p>8. Same-manufacturer class (egress)–allowed: pi@raspberrypi:~ \$ wget http://192.168.13.8/ --2019-01-31 21:16:41-- http://192.168.13.8/ Connecting to 192.168.13.8:80... connected. HTTP request sent, awaiting response... 200 OK Length: 10701 (10K) [text/html] Saving to: 'index.html.13'</p> <p>in- dex.html.13 100%[=====>] 10.45K --.-KB/s in 0s</p> <p>2019-01-31 21:16:41 (37.9 MB/s) - 'index.html.13' saved [10701/10701]</p> <hr/> <p>9. Same-manufacturer class (egress)–blocked: pi@raspberrypi:~ \$ wget https://192.168.13.8/ --2019-01-31 21:17:15-- https://192.168.13.8/ Connecting to 192.168.13.8:443... failed: Connection timed out. Retrying.</p>

Test Case Field	Description
Overall Results	Pass (for testable procedures—as stated, ingress cannot be tested)

1653 As explained above, test IoT-6-v6 is identical to test IoT-6-v4 except that it uses IPv6, DHCPv6, and IANA
 1654 code 112 instead of using IPv4, DHCPv4, and IANA code 161.

1655 **D.1.2.7 Test Case IoT-7-v4**

1656 **Table D-9: Test Case IoT-7-v4**

Test Case Field	Description
Parent Requirement	(CR 11) The IoT DDoS example implementation shall remove the implemented policy when the MUD-enabled IoT device changes DHCP state.
Testable Requirement	(CR-11.a) The MUD-enabled IoT device shall explicitly release the IP address lease (i.e., it sends a DHCP release message to the DHCP server). (CR-11.a.1) The DHCP server shall notify MUD manager that the device’s IP address lease has been released. (CR-11.a.2) The MUD manager shall remove all policies associated with the disconnected IoT device that had been configured on the MUD PEP router/switch.
Description	Shows that when a MUD-enabled IoT device explicitly releases its IP address lease, the MUD-related configuration for that IoT device will be removed from its MUD PEP router/switch.
Associated Test Cases	IoT-1-v4 (or IoT-1-v6 when IPv6 addressing is used)
Associated Cybersecurity Framework Subcategories	PR.IP-3, PR.DS-3

Test Case Field	Description
IoT Device(s) Under Test	Raspberry Pi
MUD File(s) Used	ciscopi2.json
Preconditions	Test IoT-1-v4 (or IoT-1-v6) has run successfully, meaning that the MUD PEP router/switch has been configured to enforce the policies defined in the MUD file in section D.1.3 for the IoT device in question.
Procedure	<ol style="list-style-type: none"> 1. As stipulated in the preconditions, right before this test, test IoT-1-v4 (or IoT-1-v6) must have been run successfully. Verify that the MUD PEP router/switch for the IoT device has been configured to enforce the policies listed in the preconditions section above for the IoT device in question. 2. Cause a DHCP release of the IoT device in question. 3. Verify that all the configuration rules listed above have been removed from the MUD PEP router/switch for the IoT device in question.
Expected Results	All of the configuration rules listed above have been removed from the MUD PEP router/switch for the IoT device in question.
Actual Results	<p>Procedure 1–</p> <pre>Build1#sh access-session int g1/0/15 det Interface: GigabitEthernet1/0/15 IIF-ID: 0x1B6BCEA5 MAC Address: b827.ebeb.6c8b IPv6 Address: Unknown IPv4 Address: 192.168.13.17 User-Name: b827ebeb6c8b Status: Authorized Domain: DATA Oper host mode: multi-auth Oper control dir: both</pre>

Test Case Field	Description				
	<p> Session timeout: N/A Common Session ID: COA80A0200000A6A9828F06 Acct Session ID: 0x0000003b Handle: 0x2200009c Current Policy: mud-mab-test </p> <p> Server Policies: ACS ACL: mud-81726-v4fr.in Vlan Group: Vlan: 3 </p> <p> Method status list: <table border="1" data-bbox="649 913 1421 997"> <thead> <tr> <th>Method</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>mab</td> <td>Authc Success</td> </tr> </tbody> </table> </p> <hr/> <p> Procedure 2-- pi@raspberrypi:~ \$ sudo dhclient -v -r </p> <hr/> <p> Build1#sh access-session int g1/0/15 det Interface: GigabitEthernet1/0/15 IIF-ID: 0x1B6BCEA5 MAC Address: b827.ebeb.6c8b IPv6 Address: Unknown IPv4 Address: Unknown User-Name: b827ebeb6c8b Status: Authorized Domain: DATA Oper host mode: multi-auth Oper control dir: both Session timeout: N/A </p>	Method	State	mab	Authc Success
Method	State				
mab	Authc Success				

Test Case Field	Description				
	<p>Common Session ID: COA80A0200000A6A9828F06 Acct Session ID: 0x0000003b Handle: 0x2200009c Current Policy: mud-mab-test</p> <p>Server Policies: ACS ACL: mud-81726-v4fr.in Vlan Group: Vlan: 3</p> <p>Method status list:</p> <table border="1" data-bbox="730 861 1218 945"> <thead> <tr> <th>Method</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>mab</td> <td>Authc Success</td> </tr> </tbody> </table>	Method	State	mab	Authc Success
Method	State				
mab	Authc Success				
Overall Results	Failed				

1657 As explained above, test IoT-7-v6 is identical to test IoT-7-v4 except that it uses IPv6, DHCPv6, and IANA
 1658 code 112 instead of using IPv4, DHCPv4, and IANA code 161.

1659 **D.1.2.8 Test Case IoT-8-v4**

1660 **Table D-10: Test Case IoT-8-v4**

Test Case Field	Description
Parent Requirement	(CR 11) The IoT DDoS example implementation shall remove the implemented policy when the MUD-enabled IoT device changes DHCP state.
Testable Requirement	(CR-11.b) The MUD-enabled IoT device’s IP address lease shall expire.

Test Case Field	Description
	<p>(CR-11.b.1) The DHCP server shall notify the MUD manager that the device's IP address lease has expired.</p> <p>(CR-11.b.2) The MUD manager shall remove all policies associated with the affected IoT device that had been configured on the MUD PEP router/switch.</p>
Description	Shows that when a MUD-enabled IoT device's IP address lease expires, the MUD-related configuration for that IoT device will be removed from its MUD PEP router/switch.
Associated Test Cases	IoT-1-v4 (or IoT-1-v6 when IPv6 addressing is used)
Associated Cybersecurity Framework Subcategories	PR.IP-3, PR.DS-3
IoT Device(s) Under Test	TBD (Not testable in Build 1)
MUD File(s) Used	TBD (Not testable in Build 1)
Preconditions	Test IoT-1-v4 (or IoT-1-v6) has run successfully, meaning that the MUD PEP router/switch has been configured to enforce the policies defined in the MUD file in section D.1.3 for the IoT device in question.
Procedure	<ol style="list-style-type: none"> 1. Configure the DHCP server to have a DHCP lease time of 10 minutes. 2. Run test IoT-1-v4 (or IoT-1-v6). 3. Verify that the MUD PEP router/switch for the IoT device has been configured to enforce the policies listed above for the IoT device in question. 4. Disconnect the IoT device in question from the network. 5. After 10 minutes have elapsed, verify that all of the configuration rules listed above have been removed from the MUD PEP router/switch for the IoT device in question.

Test Case Field	Description
Expected Results	Once 10 minutes have elapsed after disconnecting the IoT device from the network, all of the configuration rules listed above have been removed from the MUD PEP router/switch for the IoT device in question.
Actual Results	TBD (Not testable in Build 1)
Overall Results	TBD (Not testable in Build 1)

1661 As explained above, test IoT-8-v6 is identical to test IoT-8-v4 except that it uses IPv6, DHCPv6, and IANA
 1662 code 112 instead of using IPv4, DHCPv4, and IANA code 161.

1663 **D.1.2.9 Test Case IoT-9-v4**

1664 **Table D-11: Test Case IoT-9-v4**

Test Case Field	Description
Parent Requirement	(CR 12) The IoT DDoS example implementation shall include a router or switch that is capable of receiving and implementing threat signaling information from a threat signaling server that includes “blacklisted” URLs and hosts that are not considered to be trusted. The router/switch can be configured so that it applies threat signaling rules to both MUD-enabled and non-MUD-capable devices, based on local policy.
Testable Requirement	(CR-12.a) The router or switch shall receive threat signals from the threat signaling server and translate them into appropriate permit/deny configuration rules that will pertain to all devices (both MUD-enabled and non-MUD-capable). (CR-12.a.1) A non-MUD-capable IoT device shall attempt to initiate outbound traffic to blacklisted internet URL. The router or switch shall receive the attempt and shall deny it based on the filters from the threat signaling server.

Test Case Field	Description
	<p>(CR-12.a.2) There shall be an attempt to initiate a connection from a blacklisted internet URL to a non-MUD-capable IoT device. The router or switch shall receive the attempt and shall deny it based on the filters from the threat signaling server.</p> <p>(CR-12.a.3) The MUD-enabled IoT device shall attempt to initiate outbound traffic to an internet URL that is explicitly permitted in its MUD file but that has been blacklisted by the threat signaling service. The router or switch shall receive the attempt and shall deny it based on the filters from the threat signaling server.</p> <p>(CR-12.a.4) A blacklisted internet URL that is explicitly permitted in a MUD-enabled device's MUD file shall attempt to send traffic to the MUD-enabled device. The router or switch shall receive the attempt and shall deny it based on the filters from the threat signaling server.</p>
Description	Shows that the devices in the IoT DDoS example implementation can be configured to apply threat signaling to both non-MUD-capable and MUD-enabled devices so that threat-signaling information will override MUD file policy for a MUD-enabled device, denying communication with a blacklisted URL or host even though communication with that URL or host may be explicitly permitted in the device's MUD file.
Associated Test Cases	IoT-1-v4 (or IoT-1-v6)
Associated Cybersecurity Framework Subcategories	TBD (Not testable in Build 1)
IoT Device(s) Under Test	TBD (Not testable in Build 1)
MUD File(s) Used	TBD (Not testable in Build 1)

Test Case Field	Description
Preconditions	<ol style="list-style-type: none"> 1. A threat signaling device is available for use in the IoT DDoS example implementation. 2. The threat signaling device has been configured to generate threat signaling information that blacklists the following host types and internet services, but the threat signaling device has not yet been turned on: <ol style="list-style-type: none"> a. <i>https://yes-permit-to.com</i> b. <i>https://yes-permit-from.com</i> 3. The MUD manager and the device that receives the threat signaling information (if different from the MUD manager) are configured so that threat signaling will be applied to both MUD-enabled and non-MUD-capable devices. 4. Two different types of IoT devices are available for use in this test: one that is MUD-enabled and one that is non-MUD-capable.
Procedure	<ol style="list-style-type: none"> 1. Run test IoT-1-v4 (or IoT-1-v6). Verify that the MUD PEP router/switch for the MUD-enabled IoT device has been configured to enforce the following policies: <ol style="list-style-type: none"> a. Explicitly permit the IoT device to initiate communication with <i>https://yes-permit-to.com</i>. b. Explicitly permit <i>https://yes-permit-from.com</i> to initiate communication with the IoT device. 2. Initiate communication from the MUD-enabled IoT device to <i>https://yes-permit-to.com</i>, and verify that this traffic is received at <i>https://yes-permit-to.com</i>. 3. Initiate communication to the MUD-enabled IoT device from <i>https://yes-permit-from.com</i>, and verify that this traffic is received at the IoT device. 4. Initiate communication from the non-MUD-capable IoT device to <i>https://yes-permit-to.com</i>, and verify that this traffic is received at <i>https://yes-permit-to.com</i>. 5. Initiate communication to the MUD-incapable IoT device from <i>https://yes-permit-from.com</i>, and verify that this traffic is received at the IoT device.

Test Case Field	Description
	<ol style="list-style-type: none"> 6. The above steps verify that both the MUD-enabled and non-MUD-capable devices are operating as expected in the absence of threat signaling information. 7. Turn on the threat signaler and wait sufficient time for it to send threat signaling information. 8. Initiate communication from the MUD-enabled IoT device to <i>https://yes-permit-to.com</i>, and verify that this traffic is neither forwarded to the internet nor received at <i>https://yes-permit-to.com</i>. 9. Initiate communication to the MUD-enabled IoT device from <i>https://yes-permit-from.com</i>, and verify that this traffic is not received at the IoT device. 10. Initiate communication from the non-MUD-capable IoT device to <i>https://yes-permit-to.com</i>, and verify that this traffic is neither forwarded to the internet nor received at <i>https://yes-permit-to.com</i>. 11. Initiate communication to the MUD-incapable IoT device from <i>https://yes-permit-from.com</i>, and verify that this traffic is not received at the IoT device.
Expected Results	All expectations stated in the procedural steps listed above will be verified as described.
Actual Results	TBD (Not testable in Build 1)
Overall Results	TBD (Not testable in Build 1)

1665 As explained above, test IoT-9-v6 is identical to test IoT-9-v4 except that it uses IPv6, DHCPv6, and IANA
 1666 code 112 instead of using IPv4, DHCPv4, and IANA code 161.

1667 **D.1.2.10 Test Case IoT-10-v4**

1668 **Table D-12: Test Case IoT-10-v4**

Test Case Field	Description
Parent Requirement	<p>(CR 13) The IoT DDoS example implementation shall include a router or switch that is capable of receiving and implementing threat signaling information from a threat signaling server that includes “blacklisted” URLs and hosts that are not considered to be trusted. The router/switch can be configured so that it applies threat signaling rules only to non-MUD-capable devices, based on local policy.</p>
Testable Requirement	<p>(CR-13.a) The router or switch shall receive threat signals from the threat signaling server and translate them into appropriate permit/deny configuration rules that will pertain only to non-MUD-capable devices.</p> <p>(CR-13.a.1) The non-MUD-capable IoT device shall attempt to initiate outbound traffic to blacklisted internet URL. The router or switch shall receive the attempt and shall deny it based on the filters from the threat signaling server.</p> <p>(CR-13.a.2) There shall be an attempt to initiate a connection from a blacklisted internet URL to the non-MUD-capable IoT device. The router or switch shall receive the attempt and shall deny it based on the filters from the threat signaling server.</p> <p>CR-13.a.3) The MUD-enabled IoT device shall attempt to initiate outbound traffic to an internet URL that is explicitly permitted in its MUD file but that has been blacklisted by the threat signaling service. The router or switch shall receive the attempt and shall permit it because the filters from the threat signaling server do not apply to MUD-enabled devices.</p> <p>(CR-13.a.4) A device from a blacklisted internet URL that is explicitly permitted in a MUD-enabled device’s MUD file shall attempt to send traffic to the MUD-enabled IoT device. The router or switch shall receive the attempt and shall permit it because the filters from the threat signaling server do not apply to MUD-enabled devices.</p>

Test Case Field	Description
Description	Shows that the devices in the IoT DDoS example implementation can be configured to apply threat signaling only to non-MUD-capable devices and not to MUD-enabled devices, even if the threat-signaling information contradicts the policy in the MUD-enabled device's MUD file.
Associated Test Cases	IoT-1-v4 (or IoT-1-v6)
Associated Cybersecurity Framework Subcategories	TBD (Not testable in Build 1)
IoT Device(s) Under Test	TBD (Not testable in Build 1)
MUD File(s) Used	TBD (Not testable in Build 1)
Preconditions	<ol style="list-style-type: none"> 1. A threat signaling device is available for use in the IoT DDoS example implementation. 2. The threat signaling device has been configured to generate threat signaling information that blacklists the following host types and internet services, but the threat signaling device has not yet been turned on: <ol style="list-style-type: none"> a. https://yes-permit-to.com b. https://yes-permit-from.com 3. The MUD manager and the device that receives the threat signaling information (if different from the MUD manager) are configured so that threat signaling will be applied only to non-MUD-capable devices. 4. Two different types of IoT devices are available for use in this test: one that is MUD-enabled and one that is non-MUD-capable.
Procedure	<ol style="list-style-type: none"> 1. Run test IoT-1-v4 (or IoT-1-v6). Verify that the MUD PEP router/switch for the MUD-enabled IoT device has been configured to enforce the following policies:

Test Case Field	Description
	<ul style="list-style-type: none"> a. Explicitly permit the IoT device to initiate communication with <i>https://yes-permit-to.com</i>. b. Explicitly permit <i>https://yes-permit-from.com</i> to initiate communication with the IoT device. <ol style="list-style-type: none"> 2. Initiate communication from the MUD-enabled IoT device to <i>https://yes-permit-to.com</i>, and verify that this traffic is received at <i>https://yes-permit-to.com</i>. 3. Initiate communication to the MUD-enabled IoT device from <i>https://yes-permit-from.com</i>, and verify that this traffic is received at the IoT device. 4. Initiate communication from the non-MUD-capable IoT device to <i>https://yes-permit-to.com</i>, and verify that this traffic is received at <i>https://yes-permit-to.com</i>. 5. Initiate communication to the MUD-incapable IoT device from <i>https://yes-permit-from.com</i>, and verify that this traffic is received at the IoT device. 6. The above steps verify that both the MUD-enabled and non-MUD-capable devices are operating as expected in the absence of threat signaling information. 7. Turn on the threat signaler and wait sufficient time for it to send threat signaling information. 8. Initiate communication from the MUD-enabled IoT device to <i>https://yes-permit-to.com</i>, and verify that this traffic is received at <i>https://yes-permit-to.com</i>. 9. Initiate communication to the MUD-enabled IoT device from <i>https://yes-permit-from.com</i>, and verify that this traffic is received at the IoT device. 10. Initiate communication from the non-MUD-capable IoT device to <i>https://yes-permit-to.com</i>, and verify that this traffic is neither forwarded to the internet nor received at <i>https://yes-permit-to.com</i>. 11. Initiate communication to the MUD-incapable IoT device from <i>https://yes-permit-from.com</i>, and verify that this traffic is not received at the IoT device.

Test Case Field	Description
Expected Results	TBD (Not testable in Build 1)
Actual Results	TBD (Not testable in Build 1)
Overall Results	TBD (Not testable in Build 1)

1669 As explained above, test IoT-10-v6 is identical to test IoT-10-v4 except that it uses IPv6, DHCPv6, and
 1670 IANA code 112 instead of using IPv4, DHCPv4, and IANA code 161.

1671 **D.1.2.11 Test Case IoT-11-v4**

1672 Table D-13 contains test case requirements, associated test cases, and descriptions of the test scenarios
 1673 for the IoT capabilities of the example implementations. At the time of testing, this test case was not
 1674 evaluated due to not being fully supported by the implementation.

1675 **Table D-13: Test Case IoT-11-v4**

Test Case Field	Description
Parent Requirement	(CR-14) The IoT DDoS example implementation shall include capability to handle life-cycle changes, such as decommissioning, of IoT devices.
Testable Requirement	(CR-14.a) MUD-enabled IoT device manufacturers should provide a final MUD file for devices no longer being supported. (CR-14.a.1) The MUD manager shall use the final MUD file to configure traffic filters for the IoT device per CR 1-6.
Description	Shows that the MUD-enabled IoT device manufacturer and the MUD manager in the IoT DDoS example implementation are able to successfully maintain usage of IoT devices throughout life-cycle changes of the IoT device.
Associated Test Cases	N/A

Test Case Field	Description
Associated Cybersecurity Framework Subcategories	TBD (Not testable in Build 1)
IoT Device(s) Under Test	TBD (Not testable in Build 1)
MUD File(s) Used	TBD (Not testable in Build 1)
Preconditions	TBD (Not testable in Build 1)
Procedure	TBD (Not testable in Build 1)
Expected Results	TBD (Not testable in Build 1)
Actual Results	TBD (Not testable in Build 1)
Overall Results	TBD (Not testable in Build 1)

1676 **D.1.2.12 Test Case IoT-12-v4**

1677 **Table D-14: Test Case IoT-12-v4**

Test Case Field	Description
Parent Requirements	(CR 15) The IoT DDoS example implementation shall include a MUD manager that uses a cached MUD file rather than retrieving a new one if the cache-validity time period has not yet elapsed for the MUD file indicated by the MUD URL.
Testable Requirements	(CR 15.a) The MUD manager shall check if the file associated with the MUD URL is present in its cache and shall determine that it is.

Test Case Field	Description
	<p>(CR 15.a.1) The MUD manager shall check whether the amount of time that has elapsed since the cached file was retrieved is less than or equal to the number of hours in the cache-validity value for this MUD file. If so, the MUD manager shall apply the contents of the cached MUD file.</p> <p>(CR 15.a.2) The MUD manager shall check whether the amount of time that has elapsed since the cached file was retrieved is greater than the number of hours in the cache-validity value for this MUD file. If so, the MUD manager may (but does not have to) fetch a new file by using the MUD URL received.</p>
Description	Shows that, upon connection to the network, a MUD-enabled IoT device used in the IoT DDoS example implementation has its MUD PEP router/switch automatically configured to enforce the route filtering that is described in the cached MUD file for that device's MUD URL, assuming that the amount of time that has elapsed since the cached MUD file was retrieved is less than or equal to the number of hours in the file's cache-validity value. If the cache validity has expired in for the respective file, the MUD manager should fetch a new MUD file from the MUD file server.
Associated Test Cases	N/A
Associated Cybersecurity Framework Subcategories	ID.AM-1, ID.AM-2, ID.AM-3, PR.DS-5, DE.AE-1, PR.AC-4, PR.AC-5, PR.IP-1, PR.IP-3, PR.DS-2
IoT Device(s) Under Test	Raspberry Pi
MUD File(s) Used	ciscopi2.json
Preconditions	<ol style="list-style-type: none"> All devices have been configured to use IPv4, and the IoT device under test has been configured to emit a DHCPv4 message that includes the URL of its MUD file by using the DHCPv4 MUD URL option (IANA code 161). (Note that in the

Test Case Field	Description
	<p>v6 version of this test, IPv6, DHCPv6, and IANA code 112 will be used.)</p> <ol style="list-style-type: none"> 2. The MUD PEP router/switch does not yet have any configuration settings pertaining to the IoT device being used in the test. 3. The MUD file for the IoT device being used in the test is identical to the MUD file provided in section D.1.3.
<p>Procedure</p>	<p>Verify that the MUD PEP router/switch for the IoT device to be used in the test does not yet have any configuration settings installed with respect to the IoT device being used in the test.</p> <ol style="list-style-type: none"> 1. Run test IoT-1-v4 (or IoT-1-v6). 2. Within 24 hours (i.e., within the cache-validity period for the MUD file) of running test IoT-1-v4 (or IoT-1-v6), verify that the IoT device that was connected during test IoT-1-v4 (or IoT-1-v6) is still up and running on the network. Power-on a second IoT device that has been configured to emit the same MUD URL as the device that was connected during test IoT-1-v4 (or IoT-1-v6), and connect it to the test network. This should set in motion the following series of steps, which should occur automatically: <ol style="list-style-type: none"> 3. IoT device automatically emits a DHCPv4 message containing the device’s MUD URL (IANA code 161). (Note that in the v6 version of this test, IPv6, DHCPv6, and IANA code 112 will be used.) 4. DHCP server receives the DHCPv4 message containing the IoT device’s MUD URL. 5. DHCP server offers an IP address lease to the newly connected IoT device. 6. The IoT device requests this IP address lease, which the DHCP server acknowledges. 7. DHCP server sends the MUD URL to the MUD manager. 8. The MUD manager determines that it has this MUD file cached and checks that the amount of time that has elapsed

Test Case Field	Description
	<p>since the cached file was retrieved is less than or equal to the number of hours in the cache-validity value for this MUD file. If the cache validity has been exceeded, the MUD manager will fetch a new MUD file.</p> <p>9. The MUD manager translates the MUD file’s contents into appropriate route filtering rules and installs these rules onto the MUD PEP for the IoT device in question so that this router/switch is now configured to enforce the policies specified in the MUD file.</p>
<p>Expected Results</p>	<p>The MUD PEP router/switch for the IoT device has had its configuration changed, i.e., it has been configured to enforce the policies specified in the IoT device’s MUD file. The expected configuration should resemble the following:</p> <p>Cache is valid (the MUD manager does NOT retrieve the MUD file from the MUD file server):</p> <p>Extended IP access list mud-81726-v4fr.in</p> <pre> 10 permit tcp any host 192.168.4.7 eq www ack syn 20 permit tcp any host 192.168.10.104 eq www 30 permit tcp any host 192.168.10.105 eq www 50 permit tcp any 192.168.10.0 0.0.0.255 eq www 60 permit tcp any 192.168.13.0 0.0.0.255 eq www 70 permit tcp any 192.168.14.0 0.0.0.255 eq www 80 permit tcp any eq 22 any 81 permit udp any eq bootpc any eq bootps 82 permit udp any any eq domain 83 deny ip any any </pre> <p>Cache is valid (the MUD manager does NOT retrieve the MUD file from the MUD file server):</p> <p>Extended IP access list mud-81726-v4fr.in</p> <pre> 10 permit tcp any host 192.168.4.7 eq www ack syn 20 permit tcp any host 192.168.10.104 eq www 30 permit tcp any host 192.168.10.105 eq www </pre>

Test Case Field	Description
	<p>50 permit tcp any 192.168.10.0 0.0.0.255 eq www 60 permit tcp any 192.168.13.0 0.0.0.255 eq www 70 permit tcp any 192.168.14.0 0.0.0.255 eq www 80 permit tcp any eq 22 any 81 permit udp any eq bootpc any eq bootps 82 permit udp any any eq domain 83 deny ip any any</p> <p>Cache is not valid (the MUD manager does not retrieve the MUD file from the MUD file server):</p> <p>Extended IP access list mud-81726-v4fr.in</p> <p>10 permit tcp any host 192.168.4.7 eq www ack syn 20 permit tcp any host 192.168.10.104 eq www 30 permit tcp any host 192.168.10.105 eq www 50 permit tcp any 192.168.10.0 0.0.0.255 eq www 60 permit tcp any 192.168.13.0 0.0.0.255 eq www 70 permit tcp any 192.168.14.0 0.0.0.255 eq www 80 permit tcp any eq 22 any 81 permit udp any eq bootpc any eq bootps 82 permit udp any any eq domain 83 deny ip any any</p> <p>All protocol exchanges described in steps 1–9 above are expected to occur and can be viewed via Wireshark if desired. If the router/switch does not get configured in accordance with the MUD file, each exchange of DHCP and MUD-related protocol traffic should be viewed on the network via Wireshark to determine which transactions did not proceed as expected, and the observed and absent protocol exchanges should be described here.</p>
Actual Results	<p><u>MUD manager logs for valid cache:</u></p> <pre>**MUDC [INFO][mudc_print_request_info:2185]--> print parsed HTTP request header info ***MUDC [INFO][mudc_print_request_info:2186]--> re- quest method: POST</pre>

Test Case Field	Description
	<pre> ***MUDC [INFO][mudc_print_request_info:2187]--> re- quest uri: /getaclname ***MUDC [INFO][mudc_print_request_info:2188]--> local uri: /getaclname ***MUDC [INFO][mudc_print_request_info:2189]--> http version: 1.1 ***MUDC [INFO][mudc_print_request_info:2190]--> query string: (null) ***MUDC [INFO][mudc_print_request_info:2191]--> con- tent_length: 27 ***MUDC [INFO][mudc_print_request_info:2192]--> re- mote ip addr: 0xe7719c38 ***MUDC [INFO][mudc_print_request_info:2193]--> re- mote port: 49344 ***MUDC [INFO][mudc_print_request_info:2194]--> re- mote_user: (null) ***MUDC [INFO][mudc_print_request_info:2195]--> is ssl: 0 ***MUDC [INFO][mudc_print_request_info:2199]--> header(0): name: <Host>, value: <127.0.0.1:8000> ***MUDC [INFO][mudc_print_request_info:2199]--> header(1): name: <User-Agent>, value: <FreeRADIUS 3.0.17> ***MUDC [INFO][mudc_print_request_info:2199]--> header(2): name: <Accept>, value: <*//*> ***MUDC [INFO][mudc_print_request_info:2199]--> header(3): name: <Content-Type>, value: <applica- tion/json> ***MUDC [INFO][mudc_print_request_info:2199]--> header(4): name: <X-FreeRADIUS-Section>, value: <au- thorize> ***MUDC [INFO][mudc_print_request_info:2199]--> header(5): name: <X-FreeRADIUS-Server>, value: <de- fault> ***MUDC [INFO][mudc_print_request_info:2199]--> header(6): name: <Content-Length>, value: <27> ***MUDC [INFO][handle_get_aclname:2506]--> Mac ad- dress <b827eb6c8b> ***MUDC [INFO][fetch_uri_from_macaddr:1702]--> found the fields <{ "_id" : { "\$oid" : "5c182c7edb40218cde918776" }, "URI" : "https://mud- fileserver/ciscopi2" }> ***MUDC [INFO][fetch_uri_from_macaddr:1711]--> ===== Returning URI:https://mud- fileserver/ciscopi2 ***MUDC [INFO][handle_get_aclname:2513]--> Found URI https://mudfileserver/ciscopi2 for MAC address b827eb6c8b </pre>

Test Case Field	Description
	<pre> ***MUDC [INFO][validate_muduri:2373]--> uri: https://mudfileserver/ciscopi2 ***MUDC [INFO][validate_muduri:2399]--> ip: mud- fileserver, filename: ciscopi2 ***MUDC [INFO][handle_get_aclname:2558]--> Got URL from message <https://mudfileserver/ciscopi2> ***MUDC [INFO][query_policies_by_uri:1419]--> found the record <{ "_id" : { "\$oid" : "5c182d9cdb40218cde91884a" }, "DACL_Name" : "ACS:Cis- coSecure-Defined-ACL=mud-81726-v4fr.in", "DACL" : ["ip:inacl#10=permit tcp any host 192.168.4.7 range 80 80 syn ack\", \"ip:inacl#20=permit tcp any host 192.168.10.104 range 80 80\", \"ip:inacl#30=permit tcp any host 192.168.10.105 range 80 80\", \"ip:in- acl#40=permit tcp any host 192.168.10.104 range 80 80\", \"ip:inacl#50=permit tcp any 192.168.10.0 0.0.0.255 range 80 80\", \"ip:inacl#60=permit tcp any 192.168.13.0 0.0.0.255 range 80 80\", \"ip:in- acl#70=permit tcp any 192.168.14.0 0.0.0.255 range 80 80\", \"ip:inacl#80=permit tcp any eq 22 any\", \"ip:inacl#81=permit udp any eq 68 any eq 67\", \"ip:inacl#82=permit udp any any eq 53\", \"ip:in- acl#83=deny ip any any\"}], \"URI\" : \"https://mud- fileserver/ciscopi2\", \"VLAN\" : 3 }> ***MUDC [INFO][query_policies_by_uri:1461]--> Re- sponse <{ \"Cisco-AVPair\": [\"ACS:CiscoSecure-Defined- ACL=mud-81726-v4fr.in\"], \"Tunnel-Type\": \"VLAN\", \"Tunnel-Medium-Type\": \"IEEE-802\", \"Tunnel-Private-Group-Id\": 3 }> ***MUDC [INFO][mudc_construct_head:135]--> sta- tus_code: 200, content_len: 160, extra_headers: Con- tent-Type: application/aclname ***MUDC [INFO][mudc_construct_head:152]--> HTTP header: HTTP/1.1 200 OK Content-Type: application/aclname Content-Length: 160 ***MUDC [INFO][query_policies_by_uri:1464]--> { \"Cisco-AVPair\": [\"ACS:CiscoSecure-Defined- ACL=mud-81726-v4fr.in\"], \"Tunnel-Type\": \"VLAN\", \"Tunnel-Medium-Type\": \"IEEE-802\", \"Tunnel-Private-Group-Id\": 3 } </pre>

Test Case Field	Description
	<pre> ***MUDC [INFO][handle_get_aclname:2568]--> Got ACLs from the MUD URL MUD Manager logs for expired cache: ***MUDC [INFO][mudc_print_request_info:2185]--> print parsed HTTP request header info ***MUDC [INFO][mudc_print_request_info:2186]--> re- quest method: POST ***MUDC [INFO][mudc_print_request_info:2187]--> re- quest uri: /getaclname ***MUDC [INFO][mudc_print_request_info:2188]--> local uri: /getaclname ***MUDC [INFO][mudc_print_request_info:2189]--> http version: 1.1 ***MUDC [INFO][mudc_print_request_info:2190]--> query string: (null) ***MUDC [INFO][handle_get_aclname:2506]--> Mac ad- dress <b827eb6c8b> ***MUDC [INFO][fetch_uri_from_macaddr:1702]--> found the fields <{ "_id" : { "\$oid" : "5c182c7edb40218cde918776" }, "URI" : "https://mud- fileserver/ciscopi2" }> ***MUDC [INFO][fetch_uri_from_macaddr:1711]--> ===== Returning URI:https://mud- fileserver/ciscopi2 ***MUDC [INFO][handle_get_aclname:2513]--> Found URI https://mudfileserver/ciscopi2 for MAC address b827eb6c8b ***MUDC [INFO][validate_muduri:2373]--> uri: https://mudfileserver/ciscopi2 ***MUDC [INFO][validate_muduri:2399]--> ip: mud- fileserver, filename: ciscopi2 ***MUDC [INFO][handle_get_aclname:2558]--> Got URL from message <https://mudfileserver/ciscopi2> ***MUDC [INFO][query_policies_by_uri:1399]--> Cache has expired [omitted for sake of length] ***MUDC [STATUS][send_mudfs_request:2005]--> Request URI <https://mudfileserver/ciscopi2> </home/mudtester/mud-intermediate.pem> </pre>

Test Case Field	Description
	<pre> * Trying 192.168.4.5... * TCP_NODELAY set * Connected to mudfileserver (192.168.4.5) port 443 (#0) * found 1 certificate in /home/mudtester/mud-interme- diate.pem * found 400 certificates in /etc/ssl/certs * ALPN, offering http/1.1 * SSL connection using TLS1.2 / EC- DHE_RSA_AES_256_GCM_SHA384 * server certificate verification OK * server certificate status verification SKIPPED * common name: mudfileserver (matched) * server certificate expiration date OK * server certificate activation date OK * certificate public key: RSA * certificate version: #3 * subject: C=US,ST=Maryland,L=Rockville,O=Na- tional Cybersecurity Center of Excellence - NIST,CN=mudfileserver * start date: Fri, 05 Oct 2018 00:00:00 GMT * expire date: Wed, 13 Oct 2021 12:00:00 GMT * issuer: C=US,O=DigiCert Inc,CN=DigiCert Test SHA2 Intermediate CA-1 * compression: NULL * ALPN, server did not agree to a protocol > GET /ciscopi2 HTTP/1.1 Host: mudfileserver Accept: */* [omitted for sake of length] </pre>
Overall Results	Pass

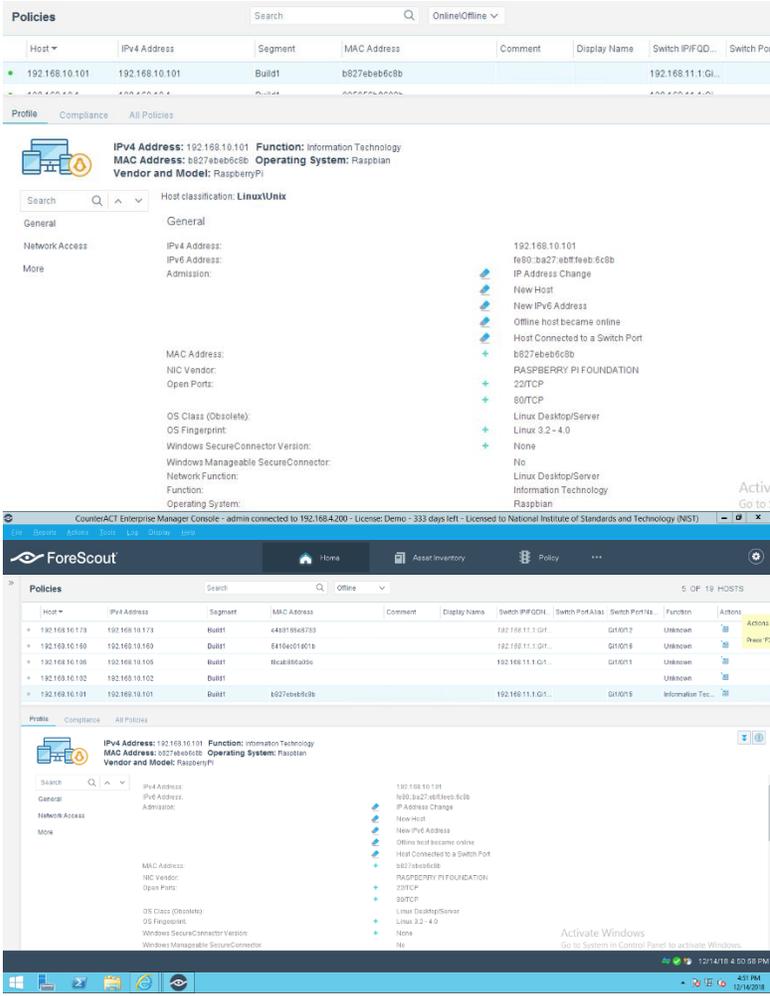
1678 Test Case IoT-12-v6 is identical to test case IoT-12-v4 except that IoT-1-v6 tests requirement CR-1.a.2,
1679 whereas IoT-1-v4 tests requirement CR-1.a.1. Hence, as explained above, test IoT-1-v6 it uses IPv6,
1680 DHCPv6, and IANA code 112 instead of using IPv4, DHCPv4, and IANA code 161.

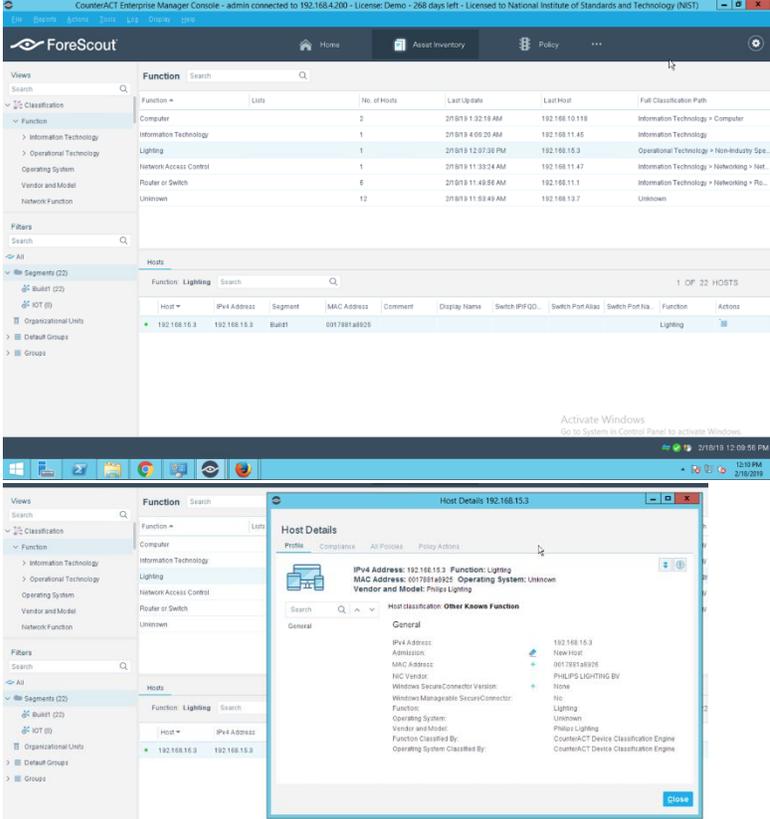
1681 D.1.2.13 Test Case IoT-13-v4

1682 Table D-15: Test Case IoT-13-v4

Test Case Field	Description
Parent Requirements	(CR 16) The IoT DDoS example implementation shall include visibility component that is able to detect, identify, categorize, and monitor the status of IoT devices that are on the network.
Testable Requirements	(CR 16.a) The visibility component shall detect and identify the attributes and category of a newly connected IoT device. (CR 16.a.1) The visibility component shall monitor the status of the IoT device (e.g., notice if the device goes offline).
Description	Shows that the IoT DDoS example implementation includes a visibility component that is capable of performing the following: upon connection of a live IoT device to the network, the device will be detected; identified in terms of attributes such as its IP address, operating system, device type, etc.; and continuously monitored as long as it remains live on the network. If the device becomes disconnected or turns off, this change of status will also be detected.
Associated Test Cases	N/A
Associated Cybersecurity Framework Subcategories	ID.AM-1, ID.AM-2, ID.AM-3, DE.AE-1, DE.CM-1
IoT Device(s) Under Test	Raspberry Pi
MUD File(s) Used	Not applicable for this test
Preconditions	1. The visibility component is up and running and attached to the network.

Test Case Field	Description
Procedure	<ol style="list-style-type: none"> 1. Power on a device and connect it to the network. 2. Verify that the device was detected by the visibility component and that its type, address, operating system (OS), and other features were identified, and device was categorized correctly. 3. Turn off the device. 4. Verify that its absence from the network is detected. 5. Power the device back on. 6. Verify that its presence is detected and its features are identified correctly. 7. Disconnect the device from the network. 8. Verify that its absence from the network is detected.
Expected Results	All expectations as enumerated in items 2, 4, 6, and 8 above are observed.
Actual Results	<p>At Power-On: pi@raspberrypi:~ \$ ifconfig eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 192.168.10.101 netmask 255.255.255.0 broadcast 192.168.10.255 ether b8:27:eb:eb:6c:8b txqueuelen 1000 (Ethernet) RX packets 9193 bytes 8208593 (7.8 MiB) RX errors 0 dropped 5 overruns 0 frame 0 TX packets 7210 bytes 822414 (803.1 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0</p> <p>lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536 inet 127.0.0.1 netmask 255.0.0.0 inet6 ::1 prefixlen 128 scopeid 0x10<host> loop txqueuelen 1000 (Local Loopback) RX packets 16 bytes 1467 (1.4 KiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 16 bytes 1467 (1.4 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0</p>

Test Case Field	Description
	<p>Screenshot from ForeScout: IoT device status is indicated by green or gray light shown in the screen capture.</p>  <p>Categorizing IoT device: We tested this function with a smart light bulb. See the example screenshots below.</p>

Test Case Field	Description
	 <p>The screenshot shows the ForeScout Enterprise Manager Console interface. The main view displays a table of hosts classified under the 'Lighting' function. The table includes columns for Function, Lists, No. of Hosts, Last Update, Last Host, and Full Classification Path. A 'Hosts' table below shows details for host 192.168.15.3, including its IP address, segment, MAC address, and comment. A 'Host Details' window is open for this host, showing its IP address (192.168.15.3), MAC address (0077814925), and classification as 'Lighting' and 'Other Known Function'.</p>
Overall Results	Pass

1683 D.1.2.14 Test Case IoT-14-v4

1684 Table D-16: Test Case IoT-14-v4

Test Case Field	Description
Parent Requirements	(CR 1) The IoT DDoS example implementation shall include a MUD-enabled IoT device that can emit a MUD URL.

Test Case Field	Description
Testable Requirements	<p>(CR 1.a) Upon initialization, the MUD-enabled IoT device shall broadcast a DHCP message on the network, including at most one MUD URL, in https scheme, within the DHCP transaction.</p> <p>(CR 1.a.1) The DHCP server shall be able to receive DHCPv4 DISCOVER and/or REQUEST with IANA code 161 (OPTION_MUD_URL_V4) from the MUD-enabled IoT device</p> <p>OR</p> <p>(CR 1.b) Upon initialization, the MUD-enabled IoT device shall emit the MUD URL as an LLDP extension.</p> <p>(CR 1.b.1) The network service shall be able to process the MUD URL that is received as an LLDP extension.</p>
Description	Shows that the IoT DDoS example implementation includes IoT devices that are capable of emitting a MUD URL via DHCP or LLDP.
Associated Test Cases	N/A
Associated Cybersecurity Framework Subcategories	ID.AM-1
IoT Device(s) Under Test	Raspberry Pi, Molex light engine, u-blox C027-G35
MUD File(s) Used	Ciscopi2.json, molex.json, ublox.json
Preconditions	<ol style="list-style-type: none"> 1. Device has been developed to emit MUD URL in DHCP transaction.

1685 **D.1.3 Build 1 MUD Files**1686 **D.1.3.1 Ciscopi2.json**

```

1687 {
1688   "ietf-mud:mud": {
1689     "mud-version": 1,
1690     "mud-url": "https://mudfilesserver/ciscopi2",
1691     "last-update": "2018-12-05T19:42:01+00:00",
1692     "cache-validity": 24,
1693     "is-supported": true,
1694     "systeminfo": "ingress/egress ",
1695     "from-device-policy": {
1696       "access-lists": {
1697         "access-list": [{
1698           "name": "mud-81726-v4fr"
1699         }]
1700       }
1701     },
1702     "to-device-policy": {
1703       "access-lists": {
1704         "access-list": [{
1705           "name": "mud-81726-v4to"
1706         }]
1707       }
1708     }
1709   },
1710   "ietf-access-control-list:acls": {
1711     "acl": [{
1712       "name": "mud-81726-v4to",
1713       "type": "ipv4-acl-type",
1714       "aces": {
1715         "ace": [{
1716           "name": "cl0-todev",
1717           "matches": {
1718             "ipv4": {
1719               "ietf-acldns:src-dnsname": "www.update-server.com",
1720               "protocol": 6
1721             },
1722             "tcp": {
1723               "ietf-mud:direction-initiated": "from-device",
1724               "source-port": {
1725                 "operator": "eq",
1726                 "port": 80
1727               }
1728             }
1729           },
1730           "actions": {
1731             "forwarding": "accept"
1732           }
1733         }],
1734       }

```

```

1735     "name": "ent0-todev",
1736     "matches": {
1737         "ietf-mud:mud": {
1738             "controller": "http://lightcontroller.example.com"
1739         },
1740         "ipv4": {
1741             "protocol": 6
1742         },
1743         "tcp": {
1744             "source-port": {
1745                 "operator": "eq",
1746                 "port": 80
1747             }
1748         }
1749     },
1750     "actions": {
1751         "forwarding": "accept"
1752     }
1753 },
1754 {
1755     "name": "ent1-todev",
1756     "matches": {
1757         "ietf-mud:mud": {
1758             "controller": "http://lightcontroller.example2.com"
1759         },
1760         "ipv4": {
1761             "protocol": 6
1762         },
1763         "tcp": {
1764             "source-port": {
1765                 "operator": "eq",
1766                 "port": 80
1767             }
1768         }
1769     },
1770     "actions": {
1771         "forwarding": "accept"
1772     }
1773 },
1774 {
1775     "name": "myctl0-todev",
1776     "matches": {
1777         "ietf-mud:mud": {
1778             "my-controller": [
1779                 null
1780             ]
1781         },
1782         "ipv4": {
1783             "protocol": 6
1784         },
1785         "tcp": {
1786             "source-port": {

```

```
1787         "operator": "eq",
1788         "port": 80
1789     }
1790 }
1791 },
1792 "actions": {
1793     "forwarding": "accept"
1794 }
1795 },
1796 {
1797     "name": "loc0-todev",
1798     "matches": {
1799         "ietf-mud:mud": {
1800             "local-networks": [
1801                 null
1802             ]
1803         },
1804         "ipv4": {
1805             "protocol": 6
1806         },
1807         "tcp": {
1808             "source-port": {
1809                 "operator": "eq",
1810                 "port": 80
1811             }
1812         }
1813     },
1814     "actions": {
1815         "forwarding": "accept"
1816     }
1817 },
1818 {
1819     "name": "myman0-todev",
1820     "matches": {
1821         "ietf-mud:mud": {
1822             "same-manufacturer": [
1823                 null
1824             ]
1825         },
1826         "ipv4": {
1827             "protocol": 6
1828         },
1829         "tcp": {
1830             "source-port": {
1831                 "operator": "eq",
1832                 "port": 80
1833             }
1834         }
1835     },
1836     "actions": {
1837         "forwarding": "accept"
1838     }
```

```

1839     },
1840     {
1841         "name": "man0-todev",
1842         "matches": {
1843             "ietf-mud:mud": {
1844                 "manufacturer": "www.devicetype.com"
1845             },
1846             "ipv4": {
1847                 "protocol": 6
1848             },
1849             "tcp": {
1850                 "source-port": {
1851                     "operator": "eq",
1852                     "port": 80
1853                 }
1854             }
1855         },
1856         "actions": {
1857             "forwarding": "accept"
1858         }
1859     }
1860 ]
1861 }
1862 },
1863 {
1864     "name": "mud-81726-v4fr",
1865     "type": "ipv4-acl-type",
1866     "aces": {
1867         "ace": [{
1868             "name": "cl0-frdev",
1869             "matches": {
1870                 "ipv4": {
1871                     "ietf-acldns:dst-dnsname": "www.update-server.com",
1872                     "protocol": 6
1873                 },
1874                 "tcp": {
1875                     "ietf-mud:direction-initiated": "from-device",
1876                     "destination-port": {
1877                         "operator": "eq",
1878                         "port": 80
1879                     }
1880                 }
1881             },
1882             "actions": {
1883                 "forwarding": "accept"
1884             }
1885         }
1886     },
1887     {
1888         "name": "ent0-frdev",
1889         "matches": {
1890             "ietf-mud:mud": {

```

```

1891         "controller": "http://lightcontroller.example.com"
1892     },
1893     "ipv4": {
1894         "protocol": 6
1895     },
1896     "tcp": {
1897         "destination-port": {
1898             "operator": "eq",
1899             "port": 80
1900         }
1901     }
1902 },
1903 "actions": {
1904     "forwarding": "accept"
1905 }
1906 },
1907 {
1908     "name": "ent1-frdev",
1909     "matches": {
1910         "ietf-mud:mud": {
1911             "controller": "http://lightcontroller.example2.com"
1912         },
1913         "ipv4": {
1914             "protocol": 6
1915         },
1916         "tcp": {
1917             "destination-port": {
1918                 "operator": "eq",
1919                 "port": 80
1920             }
1921         }
1922     },
1923     "actions": {
1924         "forwarding": "accept"
1925     }
1926 },
1927 {
1928     "name": "myctl0-frdev",
1929     "matches": {
1930         "ietf-mud:mud": {
1931             "my-controller": [
1932                 null
1933             ]
1934         },
1935         "ipv4": {
1936             "protocol": 6
1937         },
1938         "tcp": {
1939             "destination-port": {
1940                 "operator": "eq",
1941                 "port": 80
1942             }

```

```

1943     }
1944     },
1945     "actions": {
1946         "forwarding": "accept"
1947     }
1948 },
1949 {
1950     "name": "loc0-frdev",
1951     "matches": {
1952         "ietf-mud:mud": {
1953             "local-networks": [
1954                 null
1955             ]
1956         },
1957         "ipv4": {
1958             "protocol": 6
1959         },
1960         "tcp": {
1961             "destination-port": {
1962                 "operator": "eq",
1963                 "port": 80
1964             }
1965         }
1966     },
1967     "actions": {
1968         "forwarding": "accept"
1969     }
1970 },
1971 {
1972     "name": "myman0-frdev",
1973     "matches": {
1974         "ietf-mud:mud": {
1975             "same-manufacturer": [
1976                 null
1977             ]
1978         },
1979         "ipv4": {
1980             "protocol": 6
1981         },
1982         "tcp": {
1983             "destination-port": {
1984                 "operator": "eq",
1985                 "port": 80
1986             }
1987         }
1988     },
1989     "actions": {
1990         "forwarding": "accept"
1991     }
1992 },
1993 {
1994     "name": "man0-frdev",

```

```

1995         "matches": {
1996             "ietf-mud:mud": {
1997                 "manufacturer": "www.devicetype.com"
1998             },
1999             "ipv4": {
2000                 "protocol": 6
2001             },
2002             "tcp": {
2003                 "destination-port": {
2004                     "operator": "eq",
2005                     "port": 80
2006                 }
2007             }
2008         },
2009         "actions": {
2010             "forwarding": "accept"
2011         }
2012     }
2013 ]
2014 }
2015 ]
2016 ]
2017 }
2018 }

```

2019 D.1.3.2 expiredcerttest.json

```

2020 {
2021     "ietf-mud:mud": {
2022         "mud-version": 1,
2023         "mud-url": "https://mudfileserver/expiredcerttest.json",
2024         "last-update": "2018-12-05T19:42:01+00:00",
2025         "cache-validity": 24,
2026         "is-supported": true,
2027         "systeminfo": "ingress/egress ",
2028         "from-device-policy": {
2029             "access-lists": {
2030                 "access-list": [{
2031                     "name": "mud-81726-v4fr"
2032                 }]
2033             }
2034         },
2035         "to-device-policy": {
2036             "access-lists": {
2037                 "access-list": [{
2038                     "name": "mud-81726-v4to"
2039                 }]
2040             }
2041         }
2042     },
2043     "ietf-access-control-list:acls": {
2044         "acl": [{

```

```

2045     "name": "mud-81726-v4to",
2046     "type": "ipv4-acl-type",
2047     "aces": {
2048         "ace": [{
2049             "name": "cl0-todev",
2050             "matches": {
2051                 "ipv4": {
2052                     "ietf-acldns:src-dnsname": "www.update-server.com",
2053                     "protocol": 6
2054                 },
2055                 "tcp": {
2056                     "ietf-mud:direction-initiated": "from-device",
2057                     "source-port": {
2058                         "operator": "eq",
2059                         "port": 80
2060                     }
2061                 }
2062             },
2063             "actions": {
2064                 "forwarding": "accept"
2065             }
2066         },
2067         {
2068             "name": "ent0-todev",
2069             "matches": {
2070                 "ietf-mud:mud": {
2071                     "controller": "http://lightcontroller.example.com"
2072                 },
2073                 "ipv4": {
2074                     "protocol": 6
2075                 },
2076                 "tcp": {
2077                     "source-port": {
2078                         "operator": "eq",
2079                         "port": 80
2080                     }
2081                 }
2082             },
2083             "actions": {
2084                 "forwarding": "accept"
2085             }
2086         },
2087         {
2088             "name": "ent1-todev",
2089             "matches": {
2090                 "ietf-mud:mud": {
2091                     "controller": "http://lightcontroller.example2.com"
2092                 },
2093                 "ipv4": {
2094                     "protocol": 6
2095                 },
2096                 "tcp": {

```

```
2097         "source-port": {
2098             "operator": "eq",
2099             "port": 80
2100         }
2101     }
2102 },
2103     "actions": {
2104         "forwarding": "accept"
2105     }
2106 },
2107 {
2108     "name": "myctl0-todev",
2109     "matches": {
2110         "ietf-mud:mud": {
2111             "my-controller": [
2112                 null
2113             ]
2114         },
2115         "ipv4": {
2116             "protocol": 6
2117         },
2118         "tcp": {
2119             "source-port": {
2120                 "operator": "eq",
2121                 "port": 80
2122             }
2123         }
2124     },
2125     "actions": {
2126         "forwarding": "accept"
2127     }
2128 },
2129 {
2130     "name": "loc0-todev",
2131     "matches": {
2132         "ietf-mud:mud": {
2133             "local-networks": [
2134                 null
2135             ]
2136         },
2137         "ipv4": {
2138             "protocol": 6
2139         },
2140         "tcp": {
2141             "source-port": {
2142                 "operator": "eq",
2143                 "port": 80
2144             }
2145         }
2146     },
2147     "actions": {
2148         "forwarding": "accept"
```

```

2149     }
2150   },
2151   {
2152     "name": "myman0-todev",
2153     "matches": {
2154       "ietf-mud:mud": {
2155         "same-manufacturer": [
2156           null
2157         ]
2158       },
2159       "ipv4": {
2160         "protocol": 6
2161       },
2162       "tcp": {
2163         "source-port": {
2164           "operator": "eq",
2165           "port": 80
2166         }
2167       }
2168     },
2169     "actions": {
2170       "forwarding": "accept"
2171     }
2172   },
2173   {
2174     "name": "man0-todev",
2175     "matches": {
2176       "ietf-mud:mud": {
2177         "manufacturer": "www.devicetype.com"
2178       },
2179       "ipv4": {
2180         "protocol": 6
2181       },
2182       "tcp": {
2183         "source-port": {
2184           "operator": "eq",
2185           "port": 80
2186         }
2187       }
2188     },
2189     "actions": {
2190       "forwarding": "accept"
2191     }
2192   }
2193 ]
2194 }
2195 },
2196 {
2197   "name": "mud-81726-v4fr",
2198   "type": "ipv4-acl-type",
2199   "aces": {
2200

```

```

2201     "ace": [{
2202         "name": "cl0-frdev",
2203         "matches": {
2204             "ipv4": {
2205                 "ietf-acldns:dst-dnsname": "www.update-server.com",
2206                 "protocol": 6
2207             },
2208             "tcp": {
2209                 "ietf-mud:direction-initiated": "from-device",
2210                 "destination-port": {
2211                     "operator": "eq",
2212                     "port": 80
2213                 }
2214             }
2215         },
2216         "actions": {
2217             "forwarding": "accept"
2218         }
2219     },
2220     {
2221         "name": "ent0-frdev",
2222         "matches": {
2223             "ietf-mud:mud": {
2224                 "controller": "http://lightcontroller.example.com"
2225             },
2226             "ipv4": {
2227                 "protocol": 6
2228             },
2229             "tcp": {
2230                 "destination-port": {
2231                     "operator": "eq",
2232                     "port": 80
2233                 }
2234             }
2235         },
2236         "actions": {
2237             "forwarding": "accept"
2238         }
2239     },
2240     {
2241         "name": "ent1-frdev",
2242         "matches": {
2243             "ietf-mud:mud": {
2244                 "controller": "http://lightcontroller.example2.com"
2245             },
2246             "ipv4": {
2247                 "protocol": 6
2248             },
2249             "tcp": {
2250                 "destination-port": {
2251                     "operator": "eq",
2252                     "port": 80

```

```
2253         }
2254     }
2255     },
2256     "actions": {
2257         "forwarding": "accept"
2258     }
2259 },
2260 {
2261     "name": "myctl0-frdev",
2262     "matches": {
2263         "ietf-mud:mud": {
2264             "my-controller": [
2265                 null
2266             ]
2267         },
2268         "ipv4": {
2269             "protocol": 6
2270         },
2271         "tcp": {
2272             "destination-port": {
2273                 "operator": "eq",
2274                 "port": 80
2275             }
2276         }
2277     },
2278     "actions": {
2279         "forwarding": "accept"
2280     }
2281 },
2282 {
2283     "name": "loc0-frdev",
2284     "matches": {
2285         "ietf-mud:mud": {
2286             "local-networks": [
2287                 null
2288             ]
2289         },
2290         "ipv4": {
2291             "protocol": 6
2292         },
2293         "tcp": {
2294             "destination-port": {
2295                 "operator": "eq",
2296                 "port": 80
2297             }
2298         }
2299     },
2300     "actions": {
2301         "forwarding": "accept"
2302     }
2303 },
2304 {
```

```

2305         "name": "myman0-frdev",
2306         "matches": {
2307             "ietf-mud:mud": {
2308                 "same-manufacturer": [
2309                     null
2310                 ]
2311             },
2312             "ipv4": {
2313                 "protocol": 6
2314             },
2315             "tcp": {
2316                 "destination-port": {
2317                     "operator": "eq",
2318                     "port": 80
2319                 }
2320             }
2321         },
2322         "actions": {
2323             "forwarding": "accept"
2324         }
2325     },
2326     {
2327         "name": "man0-frdev",
2328         "matches": {
2329             "ietf-mud:mud": {
2330                 "manufacturer": "www.devicetype.com"
2331             },
2332             "ipv4": {
2333                 "protocol": 6
2334             },
2335             "tcp": {
2336                 "destination-port": {
2337                     "operator": "eq",
2338                     "port": 80
2339                 }
2340             }
2341         },
2342         "actions": {
2343             "forwarding": "accept"
2344         }
2345     }
2346 ]
2347 }
2348 }
2349 ]
2350 }
2351 }

```

2352 D.1.3.3 Molex.json

```
2353 {
```

```
2354     "ietf-mud:mud": {
2355         "mud-version": 1,
2356         "mud-url": "https://mudfileservers/molex",
2357         "last-update": "2019-02-05T13:18:04+00:00",
2358         "cache-validity": 48,
2359         "is-supported": true,
2360         "systeminfo": "Molex Coresync POE Gateway",
2361         "mfg-name": "Molex",
2362         "documentation": "https://www.molex.com/coresync/documentation/gateway",
2363         "model-name": "coresync",
2364         "from-device-policy": {
2365             "access-lists": {
2366                 "access-list": [{
2367                     "name": "mud-10436-v4fr"
2368                 }]
2369             }
2370         },
2371         "to-device-policy": {
2372             "access-lists": {
2373                 "access-list": [{
2374                     "name": "mud-10436-v4to"
2375                 }]
2376             }
2377         }
2378     },
2379     "ietf-access-control-list:acls": {
2380         "acl": [{
2381             "name": "mud-10436-v4to",
2382             "type": "ipv4-acl-type",
2383             "aces": {
```

```
2384         "ace": [{
2385             "name": "myctl0-todev",
2386             "matches": {
2387                 "ietf-mud:mud": {
2388                     "my-controller": [
2389                         null
2390                     ]
2391                 }
2392             },
2393             "actions": {
2394                 "forwarding": "accept"
2395             }
2396         },
2397         {
2398             "name": "loc0-todev",
2399             "matches": {
2400                 "ietf-mud:mud": {
2401                     "local-networks": [
2402                         null
2403                     ]
2404                 }
2405             },
2406             "actions": {
2407                 "forwarding": "accept"
2408             }
2409         }
2410     ]
2411 }
2412 },
2413 {
```

```
2414     "name": "mud-10436-v4fr",
2415     "type": "ipv4-acl-type",
2416     "aces": {
2417         "ace": [{
2418             "name": "myctl0-frdev",
2419             "matches": {
2420                 "ietf-mud:mud": {
2421                     "my-controller": [
2422                         null
2423                     ]
2424                 }
2425             },
2426             "actions": {
2427                 "forwarding": "accept"
2428             }
2429         },
2430         {
2431             "name": "loc0-frdev",
2432             "matches": {
2433                 "ietf-mud:mud": {
2434                     "local-networks": [
2435                         null
2436                     ]
2437                 }
2438             },
2439             "actions": {
2440                 "forwarding": "accept"
2441             }
2442         }
2443     ]
}
```

```
2444         }
2445     }
2446 ]
2447 }
2448 }
2449 D.1.3.4    u-blox.json
2450 {
2451     "ietf-mud:mud": {
2452         "mud-version": 1,
2453         "mud-url": "https://mudfileserver/ublox",
2454         "last-update": "2018-10-31T16:23:26+00:00",
2455         "cache-validity": 48,
2456         "is-supported": true,
2457         "systeminfo": "configurations for ipv4 pi connected to cisco switch",
2458         "from-device-policy": {
2459             "access-lists": {
2460                 "access-list": [{
2461                     "name": "mud-65989-v4fr"
2462                 }]
2463             }
2464         },
2465         "to-device-policy": {
2466             "access-lists": {
2467                 "access-list": [{
2468                     "name": "mud-65989-v4to"
2469                 }]
2470             }
2471         }
2472     },
2473     "ietf-access-control-list:acls": {
```

```
2474     "acl": [{
2475         "name": "mud-65989-v4to",
2476         "type": "ipv4-acl-type",
2477         "aces": {
2478             "ace": [{
2479                 "name": "cl0-todev",
2480                 "matches": {
2481                     "ipv4": {
2482                         "ietf-acldns:src-dnsname":
2483 "www.updatesterver.com",
2484                         "protocol": 6
2485                     },
2486                     "tcp": {
2487                         "ietf-mud:direction-
2488 initiated": "from-device"
2489                     }
2490                 },
2491                 "actions": {
2492                     "forwarding": "accept"
2493                 }
2494             },
2495             {
2496                 "name": "cl1-todev",
2497                 "matches": {
2498                     "ipv4": {
2499                         "ietf-acldns:src-dnsname":
2500 "www.nossl.net",
2501                         "protocol": 6
2502                     }
2503                 },
2504                 "actions": {
2505                     "forwarding": "accept"
```

```

2506                                     }
2507                                     }
2508                                 ]
2509                             }
2510                         },
2511                     {
2512                         "name": "mud-65989-v4fr",
2513                         "type": "ipv4-acl-type",
2514                         "aces": {
2515                             "ace": [{
2516                                 "name": "c10-frdev",
2517                                 "matches": {
2518                                     "ipv4": {
2519                                         "ietf-acldns:dst-dnsname":
2520 "www.update-server.com",
2521                                         "protocol": 6
2522                                     },
2523                                     "tcp": {
2524                                         "ietf-mud:direction-
2525 initiated": "from-device"
2526                                     }
2527                                 },
2528                                 "actions": {
2529                                     "forwarding": "accept"
2530                                 }
2531                             },
2532                             {
2533                                 "name": "c11-frdev",
2534                                 "matches": {
2535                                     "ipv4": {
2536                                         "ietf-acldns:dst-dnsname":
2537 "www.nossl.net",

```

```
2538                                     "protocol": 6
2539                                     }
2540                                 },
2541                                 "actions": {
2542                                     "forwarding": "accept"
2543                                 }
2544                             }
2545                         ]
2546                     }
2547                 }
2548             ]
2549         }
2550     }
```

2551 **Appendix E** **References**

2552 **E.1 Core Standards**

2553 “Dynamic Host Configuration Protocol,” Request for Comments (RFC) 2131, Mar. 1997. See
2554 <http://www.rfc-editor.org/info/rfc2131>

2555 “HTTP Over TLS,” RFC 2818, May 2000. See <http://www.rfc-editor.org/info/rfc2818>

2556 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Pro-
2557 file,” RFC 5280, May 2008. See <http://www.rfc-editor.org/info/rfc5280>

2558 “Cryptographic Message Syntax (CMS),” RFC 5652, Sept. 2009. See <http://www.rfc-editor.org/info/rfc5652>
2559

2560 “YANG—A Data Modeling Language for the Network Configuration Protocol (NETCONF),” RFC
2561 6020, Oct. 2010. See <http://www.rfc-editor.org/info/rfc6020>

2562 “Manufacturer Usage Description Specification,” RFC 8520, ISSN: 2070-1721, Mar. 2019. See
2563 <https://datatracker.ietf.org/doc/rfc8520/>

2564 IEEE802.1AB Link Layer Discovery Protocol (LLDP)

2565 **E.2 Ongoing MUD Standards Activities**

2566 K. Boeckl et al., “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy
2567 Risks,” Draft, National Institute of Standards and Technology (NIST) Interagency/Internal Re-
2568 port 8228, Sept. 2018. See <https://csrc.nist.gov/publications/detail/nistir/8228/draft>

2569 S. Rich and T. Dahm, “MUD Lifecycle: A Network Operator's Perspective,” Mar. 12, 2017. See
2570 <https://tools.ietf.org/html/draft-srich-opsawg-mud-net-lifecycle-01>

2571 S. Rich and T. Dahm, “MUD Lifecycle: A Manufacturer's Perspective,” Mar. 27, 2017.
2572 See <https://tools.ietf.org/html/draft-srich-opsawg-mud-manu-lifecycle-01>

2573 **E.3 Secure Update Standards**

2574 NIST Special Publication (SP) 800-40, *Guide to Enterprise Patch Management Technologies*. See
2575 <https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final>

2576 NIST SP 800-147, *BIOS Protection Guidelines*, and NIST SP 800-147B, *BIOS Protection Guidelines*
2577 *for Servers*. See <https://csrc.nist.gov/publications/detail/sp/800-147/final> and [https://nvl-](https://nvl-pubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-147B.pdf)
2578 [pubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-147B.pdf](https://nvl-pubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-147B.pdf)

2579 NIST Interagency/Internal Report 7823, *Advanced Metering Infrastructure Smart Meter Up-*
2580 *gradeability Test Framework*. See [http://csrc.nist.gov/publications/drafts/nistir-](http://csrc.nist.gov/publications/drafts/nistir-7823/draft_nistir-7823.pdf)
2581 [7823/draft_nistir-7823.pdf](http://csrc.nist.gov/publications/drafts/nistir-7823/draft_nistir-7823.pdf)

2582 NIST SP 800-193, *Platform Firmware Resiliency Guidelines*. See
2583 <https://csrc.nist.gov/publications/detail/sp/800-193/draft>

2584 Multi-stakeholder Working Group for Secure Update of IoT devices (ongoing and established by
2585 the National Telecommunications Information Administration as part of its Internet Policy Task
2586 Force). See <https://www.ntia.doc.gov/category/internet-things>

2587 **E.4 Industry Best Practices for Software Quality**

2588 SANS TOP 25 Most Dangerous Software Errors, SANS Institute. See
2589 <https://www.sans.org/top25-software-errors/>

2590 **E.5 Best Practices for Identification and Authentication**

2591 NIST SP 800-63-3, *Digital Identity Guidelines*. See [https://csrc.nist.gov/publications/de-](https://csrc.nist.gov/publications/detail/sp/800-63/3/final)
2592 [tail/sp/800-63/3/final](https://csrc.nist.gov/publications/detail/sp/800-63/3/final)

2593 NIST SP 800-63-B, *Digital Identity Guidelines: Authentication and Lifecycle Management*. See
2594 <https://csrc.nist.gov/publications/detail/sp/800-63b/final>

2595 FIDO Alliance specifications. See <https://fidoalliance.org/specifications/overview/>

2596 **E.6 Cryptographic Standards and Best Practices**

2597 OMB Circular A-130, Executive Office of the President, Office of Management and Budget,
2598 *Managing Federal Information as a Strategic Resource*, July 28, 2016. See
2599 https://obamawhitehouse.archives.gov/omb/circulars_a130_a130trans4/

2600 NIST SP 800-57 Part 1 Revision 4, *Recommendation for Key Management*. See
2601 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdfh>

2602

2603 NIST SP 800-52 Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport*
2604 *Layer Security (TLS) Implementations*. See
2605 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf>

2606 **E.7 Risk, Risk Assessment, and Risk Management Guidance**

2607 NIST SP 800-30, *Risk Management Guide for Information Technology Systems*. See
2608 <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800>
2609 [-30.pdf](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf)

2610 NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*. See
2611 <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>

2612 NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and*
2613 *Organizations*. See <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>

2614 NIST Computer Security Resource Center Risk Management Framework guidance. See
2615 [https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-](https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides)
2616 [guides](https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides)

2617 NIST Interagency/Internal Report 8228, *Considerations for Managing Internet of Things (IoT)*
2618 *Cybersecurity and Privacy Risks* (Draft). See
2619 <https://csrc.nist.gov/publications/detail/nistir/8228/draft>

2620 NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*
2621 (Draft). See <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft>

2622 NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018.
2623 See <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

NIST SPECIAL PUBLICATION 1800-15C

Securing Small-Business and Home Internet of Things (IoT) Devices

Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)

Volume C:
How-To Guides

Murugiah Souppaya
NIST

Eliot Lear
Cisco

Yemi Fashina
Parisa Grayeli
Joshua Klosterman
Blaine Mulugeta
The MITRE Corporation

William C. Barker
Dakota Consulting

April 2019

PRELIMINARY DRAFT

This publication is available free of charge from
<https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos>



DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-15C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-15C, 78 pages, (April 2019), CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: mitigating-iot-ddos-nccoe@nist.gov.

Public comment period: August 24, 2019 through June 24, 2019

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, Maryland 20899
Email: nccoe@nist.gov

1 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

2 The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards
3 and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and
4 academic institutions work together to address businesses' most pressing cybersecurity issues. This
5 public-private partnership enables the creation of practical cybersecurity solutions for specific
6 industries, as well as for broad, cross-sector technology challenges. Through consortia under
7 Cooperative Research and Development Agreements (CRADAs), including technology partners—from
8 Fortune 50 market leaders to smaller companies specializing in information technology security—the
9 NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity
10 solutions using commercially available technology. The NCCoE documents these example solutions in
11 the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework
12 and details the steps needed for another entity to re-create the example solution. The NCCoE was
13 established in 2012 by NIST in partnership with the State of Maryland and Montgomery County,
14 Maryland.

15 To learn more about the NCCoE, visit <https://www.nccoe.nist.gov/>. To learn more about NIST, visit
16 <https://www.nist.gov>.

17 **NIST CYBERSECURITY PRACTICE GUIDES**

18 NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity
19 challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the
20 adoption of standards-based approaches to cybersecurity. They show members of the information
21 security community how to implement example solutions that help them align more easily with relevant
22 standards and best practices, and provide users with the materials lists, configuration files, and other
23 information they need to implement a similar approach.

24 The documents in this series describe example implementations of cybersecurity practices that
25 businesses and other organizations may voluntarily adopt. These documents do not describe regulations
26 or mandatory practices, nor do they carry statutory authority.

27 **ABSTRACT**

28 The goal of the Internet Engineering Task Force's [manufacturer usage description \(MUD\)](#) architecture is
29 for Internet of Things (IoT) devices to behave as intended by the manufacturer of the devices. This is
30 done by providing a standard way for manufacturers to identify each device's type and to indicate the
31 network communications that it requires to perform its intended function. When MUD is used, the
32 network will automatically permit the IoT device to send and receive the traffic it requires to perform as
33 intended, and it will prohibit all other communications with the device.

34 The NCCoE has demonstrated for IoT product developers and implementers the ability to ensure that
35 when an IoT device connects to a home or small-business network, MUD can be used to automatically
36 permit the device to send and receive only the traffic it requires to perform its intended function.

37 A distributed denial of service (DDoS) attack can cause significant negative impact to an organization
38 that is dependent on the internet to conduct business. A DDoS attack involves multiple computing
39 devices in disparate locations sending repeated requests to a server with the intent to overload it and
40 ultimately render it inaccessible. Recently, IoT devices have been exploited to launch DDoS attacks. IoT
41 devices may have unpatched or easily discoverable software flaws, and many have minimal security, are
42 unprotected, or are difficult to secure. A DDoS attack may result in substantial revenue losses and
43 potential liability exposure, which can degrade a company's reputation and erode customer trust.
44 Victims of a DDoS attack can include

- 45 ▪ communications service providers who may suffer service degradation that affects their
46 customers
- 47 ▪ businesses that rely on the internet who may suffer if their customers cannot reach them
- 48 ▪ IoT device manufacturers who may suffer reputational damage if their devices are being
49 exploited
- 50 ▪ users of IoT devices who may suffer service degradation and potentially incur extra costs due to
51 increased activity by their captured machines

52 Use of MUD combats these IoT-based DDoS attacks by prohibiting unauthorized traffic to and from IoT
53 devices. Even if an IoT device becomes compromised, MUD prevents it from being used in any attack
54 that would require the device to send traffic to an unauthorized destination. MUD provides a standard
55 method for access control information to be available to network control devices. This NIST
56 Cybersecurity Practice Guide shows IoT product and system providers how to integrate and use MUD to
57 help make home and small-business networks more secure. It also shows what users should expect from
58 IoT device providers.

59 **KEYWORDS**

60 *botnets; internet of things; IoT; manufacturer usage description; MUD; router; server; software update*
61 *server; threat signaling.*

62 **DOCUMENT CONVENTIONS**

63 The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the
64 publication and from which no deviation is permitted.

65 The terms “should” and “should not” indicate that among several possibilities, one is recommended as
66 particularly suitable, without mentioning or excluding others, or that a certain course of action is

67 preferred but not necessarily required, or that (in the negative form) a certain possibility or course of
68 action is discouraged but not prohibited.

69 The terms “may” and “need not” indicate a course of action permissible within the limits of the
70 publication.

71 The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

72 **CALL FOR PATENT CLAIMS**

73 This public review includes a call for information on essential patent claims (claims whose use would be
74 required for compliance with the guidance or requirements in this Information Technology Laboratory
75 [ITL] draft publication). Such guidance and/or requirements may be directly stated in this ITL publication
76 or by reference to another publication. This call also includes disclosure, where known, of the existence
77 of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant
78 unexpired U.S. or foreign patents.

79 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in
80 written or electronic form, either:

- 81 1. assurance in the form of a general disclaimer to the effect that such party does not hold and
82 does not currently intend holding any essential patent claim(s); or
- 83 2. assurance that a license to such essential patent claim(s) will be made available to applicants
84 desiring to utilize the license for the purpose of complying with the guidance or requirements in
85 this ITL draft publication either:
 - 86 a. under reasonable terms and conditions that are demonstrably free of any unfair
87 discrimination or
 - 88 b. without compensation and under reasonable terms and conditions that are
89 demonstrably free of any unfair discrimination.

90 Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its
91 behalf) will include in any documents transferring ownership of patents subject to the assurance,
92 provisions sufficient to ensure that the commitments in the assurance are binding on the transferee,
93 and that the transferee will similarly include appropriate provisions in the event of future transfers with
94 the goal of binding each successor-in-interest.

95 The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of
96 whether such provisions are included in the relevant transfer documents.

97 Such statements should be addressed to mitigating-iot-ddos-nccoe@nist.gov

98 **ACKNOWLEDGMENTS**

99 We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Allaukik Abhishek	Arm
Michael Bartling	Arm
Darshak Thakore	CableLabs
Mark Walker	CableLabs
Tao Wan	CableLabs
Russ Gyurek	Cisco
Peter Romness	Cisco
Brian Weis	Cisco
Rob Cantu	CTIA
Dean Coclin	DigiCert
Clint Wilson	DigiCert
Katherine Gronberg	ForeScout
Tim Jones	ForeScout
Adnan Baykal	Global Cyber Alliance
Drew Cohen	MasterPeace Solutions

Name	Organization
Nate Lesser	MasterPeace Solutions
Tom Martz	MasterPeace Solutions
Daniel Weller	MasterPeace Solutions
Kevin Yeich	MasterPeace Solutions
Mo Alhroub	Molex
Jaideep Singh	Molex
Bill Haag	NIST
Bryan Dubois	Patton Electronics
Karen Scarfone	Scarfone Cybersecurity
Matt Boucher	Symantec
Bruce McCorkendale	Symantec
Yun Shen	Symantec
Pierre-Antoine Vervier	Symantec
Sarah Kinling	The MITRE Corporation
Mary Raguso	The MITRE Corporation
Allen Tan	The MITRE Corporation

Name	Organization
Paul Watrobski	University of Maryland
Russ Housley	Vigilsec

100 The Technology Partners/Collaborators who participated in this build submitted their capabilities in
 101 response to a notice in the Federal Register. Respondents with relevant capabilities or product
 102 components were invited to sign a Cooperative Research and Development Agreement (CRADA) with
 103 NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Arm	Subject Matter Expertise
CableLabs	Micronets Gateway Service Provider Server Partner and Service Provider Server Prototype Medical Devices–Raspberry Pi
Cisco	Cisco Catalyst 3850S MUD Manager
CTIA	Subject Matter Expertise
DigiCert	Private Transport Layer Security (TLS) Certificate Premium Certificate
ForeScout	CounterACT Appliance–VCT-R Enterprise Manager–VCEM-05
Global Cyber Alliance	Subject Matter Expertise
MasterPeace Solutions	Yikes! Router Yikes! Cloud Yikes! Mobile Application
Molex	Molex light emitting diode (LED) Light Bar Molex power over ethernet (PoE) Gateway

Technology Partner/Collaborator	Build Involvement
Patton Electronics	Session Border Controller—SN5301/4B/EUI
Symantec	Subject Matter Expertise

104 **Contents**

105 **1 Introduction1**

106 1.1 Practice Guide Structure 1

107 1.2 Build Overview 2

108 1.2.1 Usage Scenarios..... 3

109 1.2.2 Architectural Overview..... 3

110 1.3 Build 1 Architecture Summary 5

111 1.4 Typographic Conventions..... 8

112 **2 Product Installation Guides.....8**

113 2.1 Cisco MUD Manager..... 8

114 2.1.1 Cisco MUD Manager Overview..... 8

115 2.1.2 Cisco MUD Manager Configurations 9

116 2.1.3 Preinstallation..... 10

117 2.1.4 MUD Manager Installation 14

118 2.1.5 MUD Manager Configuration 16

119 2.1.6 FreeRADIUS Installation..... 18

120 2.1.7 FreeRADIUS Configuration 21

121 2.1.8 Start MUD Manager and FreeRADIUS Server..... 23

122 2.2 MUD File Server..... 25

123 2.2.1 MUD File Server Overview..... 25

124 2.2.2 Configuration Overview..... 25

125 2.2.3 Setup..... 25

126 2.3 Cisco Switch–Catalyst 3850-S..... 32

127 2.3.1 Cisco 3850-S Catalyst Switch Overview 32

128 2.3.2 Configuration Overview..... 33

129 2.3.3 Setup..... 35

130 2.4 DigiCert Certificates..... 40

131 2.4.1 DigiCert CertCentral Overview 40

132 2.4.2 Configuration Overview..... 41

133	2.4.3	Setup.....	41
134	2.5	IoT Devices.....	41
135	2.5.1	Moxel PoE Gateway and Light Engine	41
136	2.5.2	IoT Development Kits–Linux-Based	42
137	2.5.3	IoT Development Kit–u-blox C027-G35	47
138	2.5.4	IoT Devices–Non-MUD Capable	53
139	2.6	Update Server.....	54
140	2.6.1	Update Server Overview.....	54
141	2.6.2	Configuration Overview.....	54
142	2.6.3	Setup.....	55
143	2.7	Unapproved Server	55
144	2.7.1	Unapproved Server Overview	56
145	2.7.2	Configuration Overview.....	56
146	2.7.3	Setup.....	56
147	2.8	MQTT Broker Server.....	56
148	2.8.1	MQTT Broker Server Overview.....	56
149	2.8.2	Configuration Overview.....	57
150	2.8.3	Setup.....	57
151	2.9	ForeScout–IoT Device Discovery	58
152	2.9.1	ForeScout Overview	58
153	2.9.2	Configuration Overview.....	58
154	2.9.3	Setup.....	59
155	Appendix A	List of Acronyms	60
156	Appendix B	Glossary	62
157	Appendix C	References	65
158	List of Figures		
159	Figure 1-1:	Generic MUD Logical Architecture	4
160	Figure 1-2:	Build 1 Logical Architecture	6

161 **Figure 1-3: Build 1 NCCoE Laboratory Architecture7**

162 **Figure 2-1: Physical Architecture–Build 134**

163 **List of Tables**

164 **Table 2-1 Cisco 3850-S Switch Running Configuration.....35**

165

166 **1 Introduction**

167 This guide shows information technology (IT) professionals and security engineers how we implemented
168 the example Manufacturer Usage Description (MUD)-based solution for mitigating Internet of Things
169 (IoT)-based attacks by securing home and small-business IoT devices. We cover all of the products
170 employed in this reference design. We do not re-create the product manufacturers' documentation,
171 which is presumed to be widely available. Rather, these volumes show how we incorporated the
172 products together in our environment.

173 *Note: This is not a comprehensive tutorial. There are many possible service and security configurations*
174 *for these products that are out of scope for this reference design.*

175 **1.1 Practice Guide Structure**

176 This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a
177 standards-based reference design and provides users with the information they need to replicate the
178 MUD-based solution for mitigating network-based attacks by securing home and small-business IoT
179 devices. This reference design is modular and can be deployed in whole or in part.

180 This guide contains three volumes:

- 181 ▪ NIST Special Publication (SP) 1800-15A: *Executive Summary*
- 182 ▪ NIST SP 1800-15B: *Approach, Architecture, and Security Characteristics*—what we built and why
- 183 ▪ NIST SP 1800-15C: *How-To Guides*—instructions for building the example solution (**you are here**)

184 Depending on your role in your organization, you might use this guide in different ways:

185 **Business decision makers, including chief security and technology officers,** will be interested in the
186 *Executive Summary*, NIST SP 1800-15A, which describes the following topics:

- 187 ▪ challenges enterprises face in trying to mitigate network-based attacks by securing home and
188 small-business IoT devices
- 189 ▪ example solution built at the NCCoE
- 190 ▪ benefits of adopting the example solution

191 **Technology or security program managers** who are concerned with how to identify, understand, assess,
192 and mitigate risk will be interested in NIST SP 1800-15B, which describes what we did and why. The
193 following sections will be of particular interest:

- 194 ▪ Section 3.4, Risk Assessment, provides a description of the risk analysis we performed.
- 195 ▪ Section 5.2, Security Control Map, maps the security characteristics of this example solution to
196 cybersecurity standards and best practices.

197 You might share the *Executive Summary*, NIST SP 1800-15A, with your leadership team members to help
198 them understand the importance of adopting a standards-based solution for mitigating network-based
199 attacks by securing home and small-business IoT devices.

200 **IT professionals** who want to implement an approach like this will find this whole practice guide useful.
201 You can use this how-to portion of the guide, NIST SP 1800-15C, to replicate all or parts of the build
202 created in our lab. This how-to portion of the guide provides specific product installation, configuration,
203 and integration instructions for implementing the example solution. We do not re-create the product
204 manufacturers' documentation, which is generally widely available. Rather, we show how we
205 incorporated the products together in our environment to create an example solution.

206 This guide assumes that IT professionals have experience implementing security products within the
207 enterprise. While we have used a suite of commercial products to address this challenge, this guide does
208 not endorse these particular products. Your organization can adopt this solution or one that adheres to
209 these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
210 parts of the MUD-based solution. Your organization's security experts should identify the products that
211 will best integrate with your existing tools and IT system infrastructure. We hope that you will seek
212 products that are congruent with applicable standards and best practices. Section 4.3, Technologies, of
213 NIST SP 1800-15B lists the products that we used and maps them to the cybersecurity controls provided
214 by this reference solution.

215 A NIST Cybersecurity Practice Guide does not describe "the" solution but a possible solution. This is a
216 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and
217 success stories will improve subsequent versions of this guide. Please contribute your thoughts to
218 mitigating-iot-ddos-nccoe@nist.gov.

219 **1.2 Build Overview**

220 This NIST Cybersecurity Practice Guide addresses the challenge of using standards-based protocols and
221 available technologies to mitigate network-based attacks by securing home and small-business IoT
222 devices. It uses products that support the IETF MUD protocol to enable each MUD-capable IoT device
223 that connects to the network to provide a uniform resource locator (URL) for a MUD file. The provided
224 MUD file lists the domains of all external services with which the device is permitted to exchange traffic.
225 The network router is then configured according to the information in the MUD file, thereby protecting
226 the IoT device from being attacked by external entities and protecting external entities from being
227 attacked by the IoT device. In addition, the MUD file specifies devices with which the IoT device is
228 permitted to communicate based on, for example, the manufacturer or class of those other devices. If a
229 local device does not have the specified manufacturer or is not a member of the specified class, the
230 router will not permit it to communicate with the IoT device. So if a device on the local network
231 becomes compromised and that device's manufacturer or class is not one that has been explicitly

232 permitted in a given IoT device's MUD file, the compromised device will not be permitted to send traffic
233 to attack the given IoT device.

234 In addition to the protections provided by use of the MUD protocol, this build further secures IoT
235 devices through update servers. Each IoT device on the build network periodically contacts its update
236 server to download and apply security patches, ensuring that it is running the most up-to-date and
237 secure code available. Last, the build uses IoT device discovery technology to discover, inventory,
238 profile, and classify all attached devices. Such classification can be used to validate that the access that is
239 being granted to each device is consistent with that device's type. Threat signaling has not been
240 incorporated into the current build. However, in the future, the build network could be enhanced to
241 periodically receive threat feeds from a threat signaling server to use as a basis for restricting certain
242 types of network traffic.

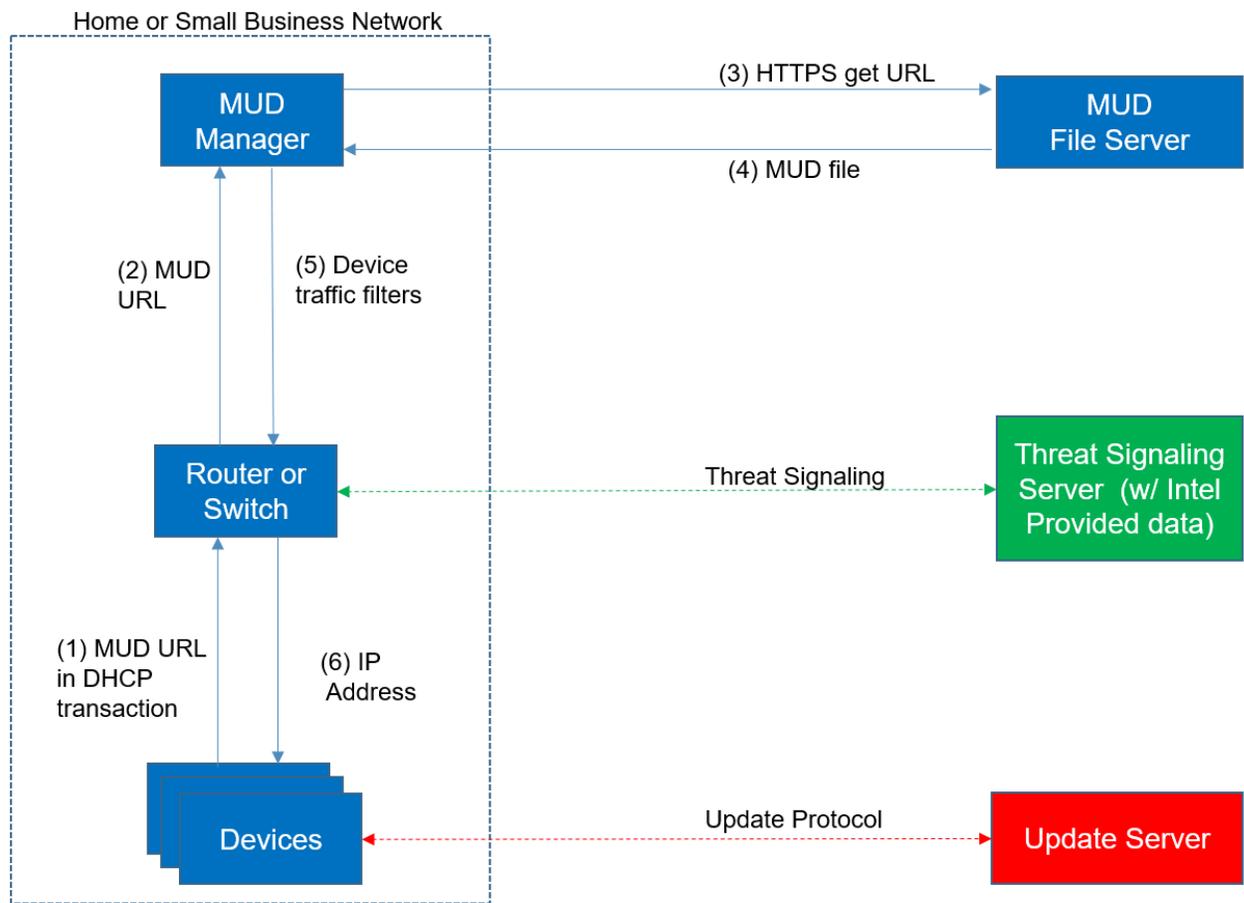
243 1.2.1 Usage Scenarios

244 The example implementation fulfills the use cases of a MUD-capable IoT device being onboarded and
245 used on home and small-business networks, where plug-and-play deployment is required. The example
246 implementation includes both MUD-capable and non-MUD-capable IoT devices. MUD-capable IoT
247 devices include the Molex PoE Gateway and Light Engine as well as four development kits (devkits) that
248 the NCCoE configured to perform actions such as power a LED bulb on and off, start network
249 connections, and power a smart lighting device on and off. These MUD-capable IoT devices interact with
250 external systems to access secure updates and various cloud services, in addition to interacting with
251 traditional personal computing devices, as permitted by their MUD files. Non-MUD-capable IoT devices
252 deployed on the example implementation network include three cameras, two smartphones, two smart
253 lighting devices, a smart assistant, a smart printer, a baby monitor with remote control and video and
254 audio capabilities, a smart wireless access point, and a smart digital video recorder. The cameras, smart
255 lighting devices, baby monitor, and digital video recorder are all controlled and managed by a
256 smartphone. In combination, these devices are capable of generating a wide range of network traffic
257 that could reasonably be expected on a home or small-business network.

258 1.2.2 Architectural Overview

259 Figure 1-1 depicts the logical architecture of this project. A new functional component, the MUD
260 manager, is introduced into the home or small-business network to augment the existing networking
261 functionality offered by the router or switch: address assignment and control of access to devices.

262 **Figure 1-1: Generic MUD Logical Architecture**



263

264 A MUD-capable IoT device inserts its MUD URL into the dynamic host configuration protocol (DHCP)
 265 address request that it generates when it attaches to the network (e.g., when it powers on).
 266 Alternatively, it may include the MUD URL in a Link Layer Discovery Protocol (LLDP) message. The MUD
 267 URL is passed to the MUD manager, which retrieves a MUD file from the designated website (denoted as
 268 the MUD file server) by using hypertext transfer protocol secure (https). The MUD file describes the
 269 communications requirements for the IoT device; the MUD manager converts the requirements into
 270 traffic filters that are installed on the router or switch to enforce access controls on the network. This
 271 enables the router or switch to deny traffic sent to or from the IoT device if that traffic is outside the
 272 device’s communications profile.

273 To provide further security, periodic updates are incorporated into the architecture. IoT devices
 274 periodically contact the appropriate update server to download and apply security patches. To ensure

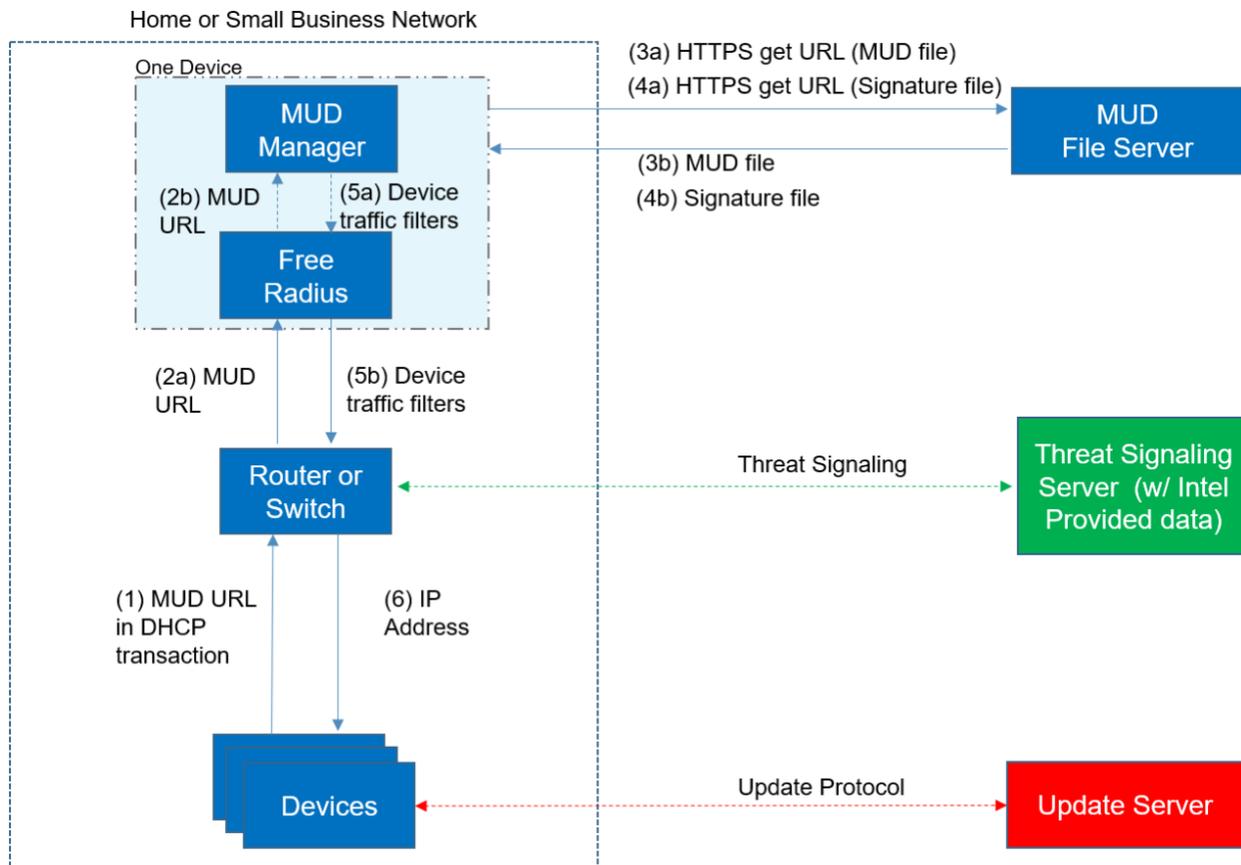
275 that such updates are possible, the IoT device’s MUD file must explicitly permit the IoT device to receive
276 traffic from the update server.

277 In the future, threat signaling could also be incorporated into the architecture, as shown in Figure 1-1.
278 The router or switch would periodically receive threat feeds from the threat signaling server to use as a
279 basis for restricting certain types of network traffic. For example, malicious traffic could be denied
280 access to a device by a cloud-based or infrastructure service like domain name system (DNS), with
281 detailed threat information, including type, severity, and mitigation, available to the router or switch on
282 demand. The example implementation includes all of the architectural elements shown in Figure 1-1
283 except for threat signaling. Incorporation of threat signaling is planned for a future build of the example
284 implementation.

285 **1.3 Build 1 Architecture Summary**

286 Figure 1-2 below describes the logical architecture of the first build of a MUD example implementation,
287 referred to as Build 1. Build 1 is designed with a single device serving as the MUD manager and
288 FreeRADIUS server that interfaces with the Catalyst 3850-S switch over transmission control
289 protocol/internet protocol (TCP/IP). The Catalyst 3850-S switch contains a DHCP server that is
290 configured to extract MUD URLs from IPv4 DHCP transactions. Upon connecting a MUD-enabled device,
291 the device will emit its MUD URL in some approved method (LLDP, X.509, or DHCP). For this example
292 implementation, only DHCP and LLDP were leveraged.

293 **Figure 1-2: Build 1 Logical Architecture**



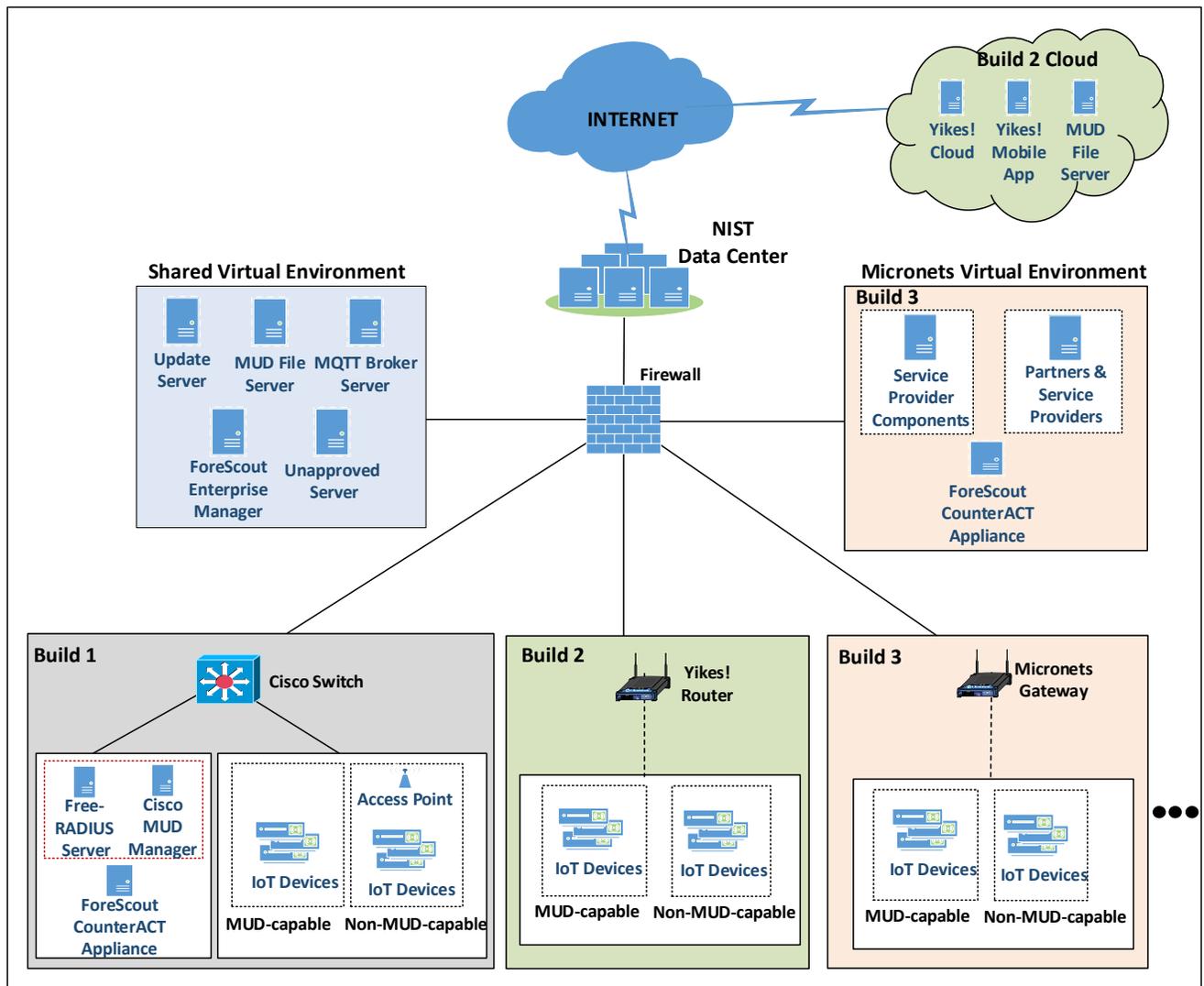
294

295 Figure 1-3 depicts the Build 1 architecture within the context of the NCCoE laboratory. Internet access is
 296 available for connection to external hosts, while software components were installed as virtual servers
 297 within the vSphere environment. This implementation provides flexibility to implement additional builds
 298 in the future. As depicted, the NCCoE laboratory network is connected to the internet via the NIST data
 299 center. Access to and from the NCCoE network is protected by a firewall. The NCCoE network includes a
 300 virtual environment that houses an update server, a MUD file server, an unapproved server (i.e., a
 301 server that is not listed as an approved communications end point in any MUD file), a Message Queuing
 302 Telemetry Transport (MQTT) broker server, and a ForeScout Enterprise Manager. These components are
 303 hosted at the NCCoE and will be used across builds. The TLS certificate and code signing certificates used
 304 by the MUD file server are provided by DigiCert.

305 Only Build 1, as depicted in Figure 1-3, has been implemented during this phase of the project, so that is
 306 what this document describes. Build 1 network components consist of a Cisco Catalyst 3850-S switch
 307 and virtual instances of Cisco MUD Manager, FreeRADIUS server, and the ForeScout CounterACT
 308 appliance. IoT devices used in this architecture comprise MUD-capable and non-MUD-capable devices.

309 The MUD-capable IoT devices for Build 1 include Raspberry Pi, ARTIK, u-blox, Intel UP Squared Devkits,
 310 and the Molex Light Engine controlled by PoE Gateway. Non-MUD-capable devices chosen for Build 1
 311 include three cameras, two smartphones, two smart lighting devices, a smart assistant, a smart printer,
 312 a baby monitor with remote control and video and audio capabilities, a smart wireless access point, and
 313 a smart digital video recorder. The remainder of this document describes installation and configuration
 314 of the various components that are depicted in Figure 1-2.

315 **Figure 1-3: Build 1 NCCoE Laboratory Architecture**



316

317 1.4 Typographic Conventions

318 The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
<i>Italics</i>	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For detailed definitions of terms, see the <i>NCCoE Glossary</i> .
Bold	names of menus, options, command buttons, and fields	Choose File > Edit .
Monospace	command-line input, onscreen computer output, sample code examples, and status codes	Mkdir
Monospace Bold	command-line user input contrasted with computer output	service sshd start
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST’s NCCoE are available at https://www.nccoe.nist.gov .

319 2 Product Installation Guides

320 This section of the practice guide contains detailed instructions for installing and configuring all of the
321 products used to build an instance of the example solution.

322 2.1 Cisco MUD Manager

323 This section describes how to deploy Cisco’s MUD Manager version 1.0, which uses a MUD-based
324 authorization system in the network, by Cisco Catalyst switches, FreeRADIUS, and Cisco MUD Manager.

325 2.1.1 Cisco MUD Manager Overview

326 The Cisco MUD Manager is an open-source implementation that works with IoT devices that emit their
327 MUD URLs. In this implementation we tested two MUD URL emission methods: DHCP and LLDP. The
328 MUD manager is supported by a FreeRADIUS server that receives MUD URLs from the switch. The MUD
329 URLs are extracted by the DHCP server and are sent to the MUD manager via RADIUS messages. The
330 MUD manager is responsible for retrieving the MUD file and corresponding signature file associated
331 with the MUD URL. The MUD manager verifies the legitimacy of the file and then translates the contents
332 to an internet protocol (IP) access control list (ACL)-based policy that is specified in the MUD file.

333 The version of the Cisco MUD Manager used in this project is a proof-of-concept implementation that is
334 intended to introduce advanced users and engineers to the MUD concept. It is not a fully automated
335 MUD manager implementation, and some protocol features are not present. At the time of
336 implementation, the “model” construct was not yet implemented. In addition, if a DNS-based system
337 changes its address, this will not be noticed. Also, IPv6 access has not been fully supported.

338 2.1.2 Cisco MUD Manager Configurations

339 The following subsections document the software, hardware, and network configurations for the Cisco
340 MUD Manager.

341 2.1.2.1 Hardware Configuration

342 Cisco requires installing the MUD manager and FreeRADIUS on a single server with at least 2 gigabytes
343 of random access memory. This server must integrate with at least one switch or router on the network.
344 For this example implementation we used a Catalyst 3850-S switch.

345 2.1.2.2 Network Configuration

346 The MUD manager and FreeRADIUS server instances were installed and configured on a dedicated
347 machine leveraged for hosting virtual machines in the Build 1 lab environment. This machine was then
348 connected to virtual local area network (VLAN) 2 on the Catalyst 3850-S and assigned a static IP address.

349 2.1.2.3 Software Configuration

350 For this build, the Cisco MUD Manager was installed on an Ubuntu 18.04.01 64-bit server. However,
351 there are many approaches for implementation. After completion of this implementation, the MUD
352 manager can be built via Docker containers provided by Cisco.

353 The Cisco MUD Manager can operate on Linux operating systems, such as

- 354 ▪ Ubuntu 18.04.01
- 355 ▪ Amazon Linux

356 The Cisco MUD Manager requires the following installations and components:

- 357 ▪ OpenSSL
- 358 ▪ cJSON
- 359 ▪ MongoDB
- 360 ▪ Mongo C Driver
- 361 ▪ Libcurl
- 362 ▪ FreeRADIUS server

363 At a high level, the following software configurations and integrations are required:

- 364 ▪ The Cisco MUD Manager requires integration with a switch (such as a Catalyst 3850-S) that
365 connects to an authentication, authorization, and accounting (AAA) server that communicates
366 by using the RADIUS protocol (i.e., a RADIUS server).
- 367 ▪ The RADIUS server must be configured to identify a MUD URL received in an accounting request
368 message from a device it has authenticated.
- 369 ▪ The MUD manager must be configured to process a MUD URL received from a RADIUS server
370 and return access control policy to the RADIUS server, which is then forwarded to the switch.

371 2.1.3 Preinstallation

372 Cisco's DevNet GitHub page provides documentation that we followed to complete this section:

373 <https://github.com/CiscoDevNet/MUD-Manager/tree/1.0#dependancies>

- 374 1. Open a terminal window, and enter the following command to log in as root:

375 `sudo su`



```
nccoe — iot@cisco-mud-manager: ~ — ssh iot@192.168.11.45 — 80x24
iot@cisco-mud-manager:~$ sudo su
```

- 376 2. Change to the root directory:

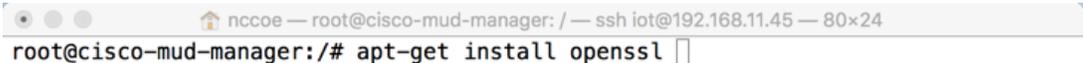
377 `cd /`



```
nccoe — root@cisco-mud-manager: /home/iot — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/home/iot# cd /
```

- 378 3. To install OpenSSL from the terminal, enter the following command:

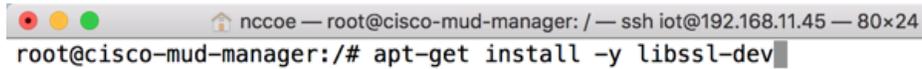
379 `apt-get install openssl`



```
nccoe — root@cisco-mud-manager: / — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/# apt-get install openssl
```

- a. If unable to link to OpenSSL, install the following by entering this command:

381 `apt-get install -y libssl-dev`



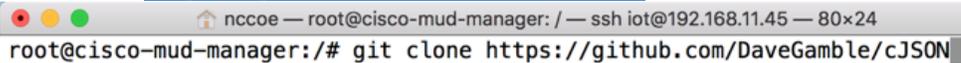
```

nccoe — root@cisco-mud-manager: / — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/# apt-get install -y libssl-dev

```

- 382 4. To install cJSON, download it from GitHub by entering the following command:

383 `git clone https://github.com/DaveGamble/cJSON`



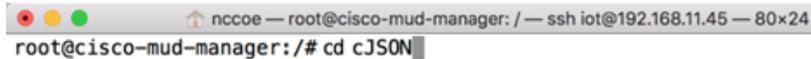
```

nccoe — root@cisco-mud-manager: / — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/# git clone https://github.com/DaveGamble/cJSON

```

- 384 a. Change directories to the cJSON folder by entering the following command:

385 `cd cJSON`



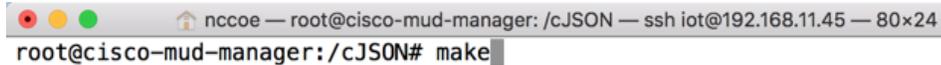
```

nccoe — root@cisco-mud-manager: / — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/# cd cJSON

```

- 386 b. Build cJSON by entering the following commands:

387 `make`

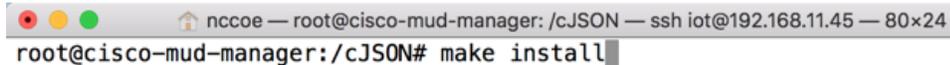


```

nccoe — root@cisco-mud-manager: /cJSON — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/cJSON# make

```

388 `make install`



```

nccoe — root@cisco-mud-manager: /cJSON — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/cJSON# make install

```

- 389 5. Change directories back a folder by entering the following command:

390 `cd ..`

```

nccoe — root@cisco-mud-manager: /cJSON — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/cJSON# cd ..

```

391 6. To install MongoDB, enter the following commands:

392 a. Import the public key:

393 `sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv`
394 `9DA31620334BD75D9DCB49F368818C72E52529D4`

```

nccoe — root@cisco-mud-manager: / — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/# apt-key adv --keyserver hkp://keyserver.ubuntu.com:80
--recv 9DA31620334BD75D9DCB49F368818C72E52529D4

```

I

395 b. Create a list file for MongoDB:

396 `echo "deb [arch=amd64] https://repo.mongodb.org/apt/ubuntu`
397 `trusty/mongodb-org/4.0 multiverse" | sudo tee`
398 `/etc/apt/sources.list.d/mongodb-org-4.0.list`

```

nccoe — root@cisco-mud-manager: / — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/# echo "deb [ arch=amd64 ] https://repo.mongodb.org/apt/
ubuntu trusty/mongodb-org/4.0 multiverse" | sudo tee /etc/apt/sources.list.d/mon
godb-org-4.0.list

```

399 c. Reload the local package database:

400 `sudo apt-get update`

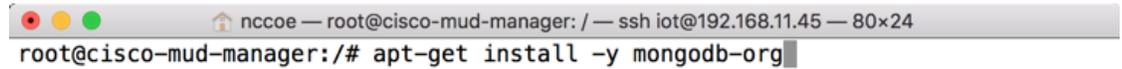
```

nccoe — root@cisco-mud-manager: / — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/# apt-get update

```

401 d. Install the MongoDB packages:

402 `sudo apt-get install -y mongodb-org`



```

nccoe — root@cisco-mud-manager: / — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/# apt-get install -y mongodb-org

```

403 7. To install the Mongo C driver, enter the following command:

404 `wget https://github.com/mongodb/mongo-c-driver/releases/download/1.7.0/mongo-c-`
 405 `driver-1.7.0.tar.gz`



```

nccoe — root@cisco-mud-manager: / — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/# wget https://github.com/mongodb/mongo-c-driver/release
s/download/1.7.0/mongo-c-driver-1.7.0.tar.gz

```

406 a. Untar the file by entering the following command:

407 `untar -xzf mongo-c-driver-1.7.0.tar.gz`



```

nccoe — root@cisco-mud-manager: / — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/# untar -xzf mongo-c-driver-1.7.0.tar.gz

```

408 b. Change into the mongo-c-driver-1.7.0 directory by entering the following command:

409 `cd mongo-c-driver-1.7.0/`



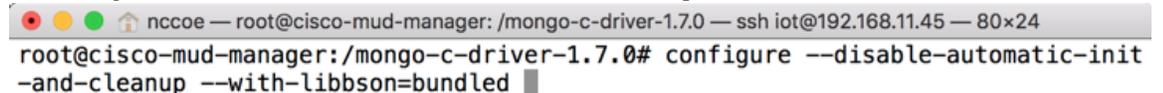
```

nccoe — root@cisco-mud-manager: / — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/# cd mongo-c-driver-1.7.0

```

410 c. Build the Mongo C driver by entering the following commands:

411 `./configure --disable-automatic-init-and-cleanup --with-libbson=bundled`



```

nccoe — root@cisco-mud-manager: /mongo-c-driver-1.7.0 — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/mongo-c-driver-1.7.0# configure --disable-automatic-init
-and-cleanup --with-libbson=bundled

```

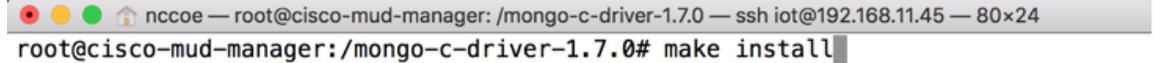
412 `make`



```
root@cisco-mud-manager:/mongo-c-driver-1.7.0# make
```

413

```
make install
```



```
root@cisco-mud-manager:/mongo-c-driver-1.7.0# make install
```

414 8. Change directories back a folder by entering the following command:

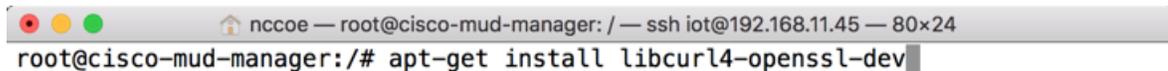
415 `cd ..`



```
root@cisco-mud-manager:/mongo-c-driver-1.7.0# cd ..
```

416 9. To install libcurl, enter the following command:

417 `sudo apt-get install libcurl4-openssl-dev`



```
root@cisco-mud-manager:/# apt-get install libcurl4-openssl-dev
```

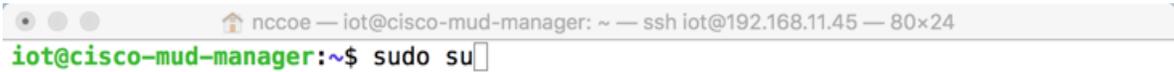
418 2.1.4 MUD Manager Installation

419 A portion of the steps in this section are documented on Cisco's DevNet GitHub page:

420 <https://github.com/CiscoDevNet/MUD-Manager/tree/1.0#building-the-mud-manager>

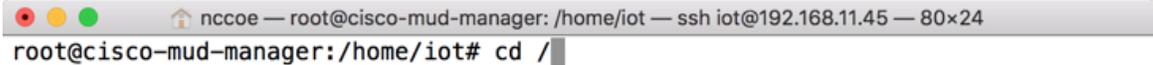
421 1. Open a terminal window, and enter the following command to log in as root:

422 `sudo su`



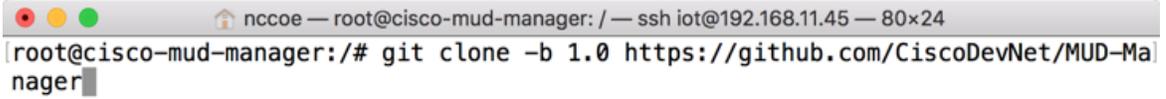
423 2. Change to the root directory by entering the following command:

424 `cd /`



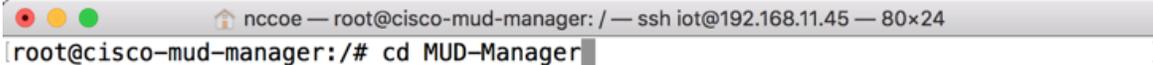
425 3. To install the MUD manager, download it from Cisco's GitHub by entering the following
426 command:

427 `git clone -br 1.0 https://github.com/CiscoDevNet/MUD-Manager.git`



428 4. Change into the MUD manager directory:

429 `cd MUD-Manager`

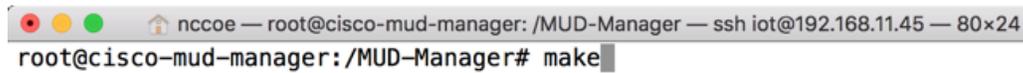


430 5. Build the MUD manager by entering the following commands:

431 `./configure`



432 `make`



```

root@cisco-mud-manager: /MUD-Manager# make

```

433 make install



```

root@cisco-mud-manager: /MUD-Manager# make install

```

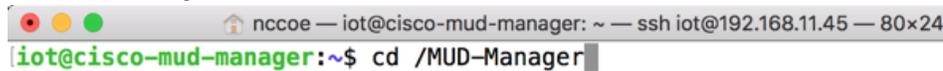
434 2.1.5 MUD Manager Configuration

435 This section describes configuring the MUD manager to communicate with the NCCoE MUD file server
 436 and defining the attributes used for translating the fetched MUD files. Details about the configuration
 437 file and additional fields that could be set within this file can be accessed here:

438 <https://github.com/CiscoDevNet/MUD-Manager#editing-the-configuration-file>.

- 439 1. In the terminal, change to the MUD manager directory:

440 cd /MUD-Manager



```

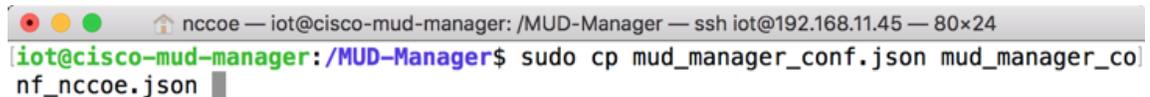
iot@cisco-mud-manager:~$ cd /MUD-Manager

```

- 441 2. Copy the contents of the sample mud_manager_conf.json file to a different file:

442 sudo cp mud_manager_conf.json mud_manager_conf_nccoe.json

443



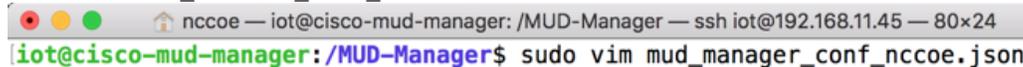
```

iot@cisco-mud-manager: /MUD-Manager$ sudo cp mud_manager_conf.json mud_manager_conf_nccoe.json

```

- 444 3. Modify the contents of the new MUD manager configuration file:

445 sudo vim mud_manager_conf_nccoe.json



```

iot@cisco-mud-manager: /MUD-Manager$ sudo vim mud_manager_conf_nccoe.json

```

446

```

{
  "MUDManagerAPIProtocol" : "http",
  "ACL_Prefix" : "ACS:",
  "ACL_Type" : "dACL-ingress-only",
  "COA_Password" : "cisco",
  "Manufacturers" : {
    { "authority" : "mudfileserver",
      "cert" : "/home/mudtester/digicertca-chain.crt",
      "web_cert" : "/home/mudtester/mud-intermediate.pem",
      "my_controller_v4" : "192.168.10.104",
      "my_controller_v6" : "2610:20:60CE:630:8000::7",
      "local_networks_v4" : "192.168.10.0 0.0.0.255",
      "local_networks_v6" : "2610:20:60CE:630:8000::",
      "vlan_mw_v4" : "192.168.13.0 0.0.0.255",
      "vlan" : 3
    },
    { "authority" : "www.devicetype.com",
      "cert" : "/home/mudtester/digicertca-chain.crt",
      "web_cert" : "/home/mudtester/mud-intermediate.pem",
      "vlan_mw_v4" : "192.168.14.0 0.0.0.255",
      "vlan" : 4
    }
  },
  "DNSMapping" : {
    "www.dominiontea.com" : "192.200.178.19",
    "www.update-server.com" : "192.168.4.7",
    "www.mqttbroker.com" : "192.168.4.6"
  },
  "DNSMapping_v6" : {
    "www.mqttbroker.com" : "2610:20:60CE:630:8000::6",
    "www.update-server.com" : "2610:20:60CE:630:8000::7",
    "www.dominiontea.com" : "2a03:2880:f10c:83:face:b00c:0:25de"
  },
  "ControllerMapping" : {
    "http://lightcontroller.example.com" : "192.168.10.104",
    "http://lightcontroller.example2.com" : "192.168.10.105"
  },
  "ControllerMapping_v6" : {
    "http://lightcontroller.example.com" : "ffff:2343:4444::"
  },
  "DefaultACL" : ["permit tcp any eq 22 any", "permit udp any eq 68 any eq 67",
  "DefaultACL_v6" : ["permit udp any any eq 53", "deny ip any any"],
  "DefaultACL_v6" : ["permit udp any any eq 53", "deny ipv6 any any"]
}
"mud_manager_conf_nccoe.json" 46L, 1612C

```

447
448
449

Details about the contents of the configuration file can be found at the link provided at the start of this section.

450

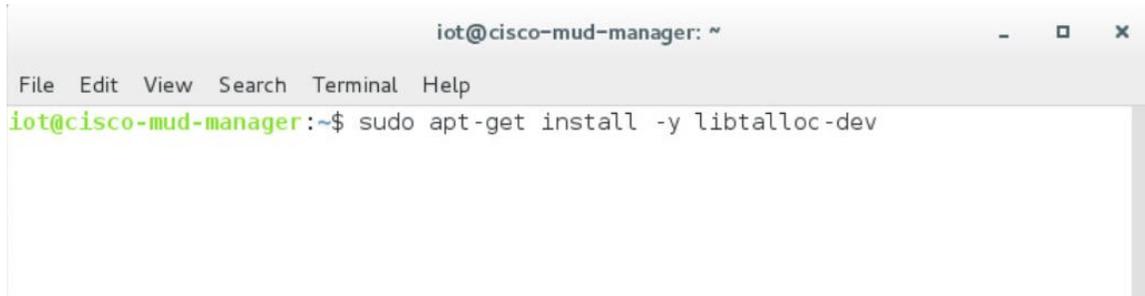
2.1.6 FreeRADIUS Installation

451

1. Install the dependencies for FreeRADIUS:

452

- a. `sudo apt-get install -y libtalloc-dev`

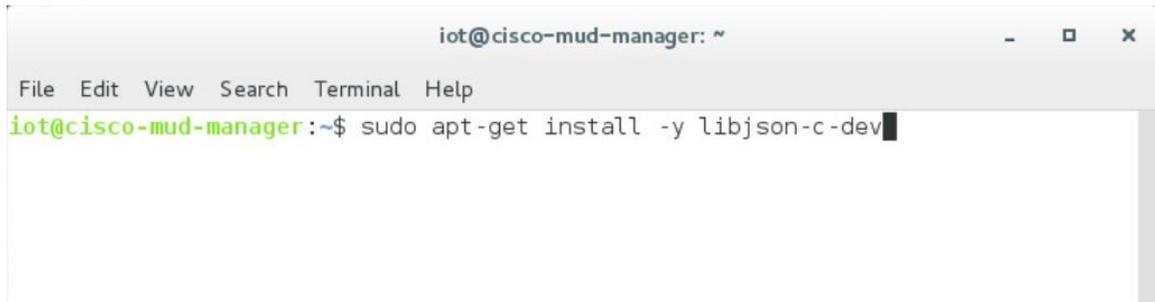


```
iot@cisco-mud-manager: ~  
File Edit View Search Terminal Help  
iot@cisco-mud-manager:~$ sudo apt-get install -y libtalloc-dev
```

453

454

- b. `sudo apt-get install -y libjson-c-dev`

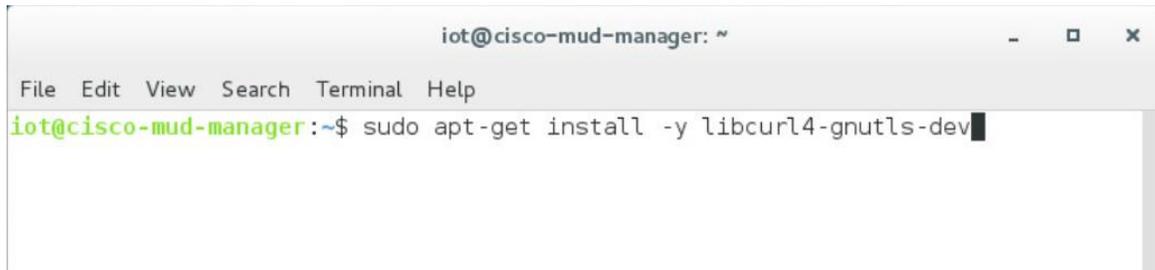


```
iot@cisco-mud-manager: ~  
File Edit View Search Terminal Help  
iot@cisco-mud-manager:~$ sudo apt-get install -y libjson-c-dev
```

455

456

- c. `sudo apt-get install -y libcurl4-gnutls-dev`

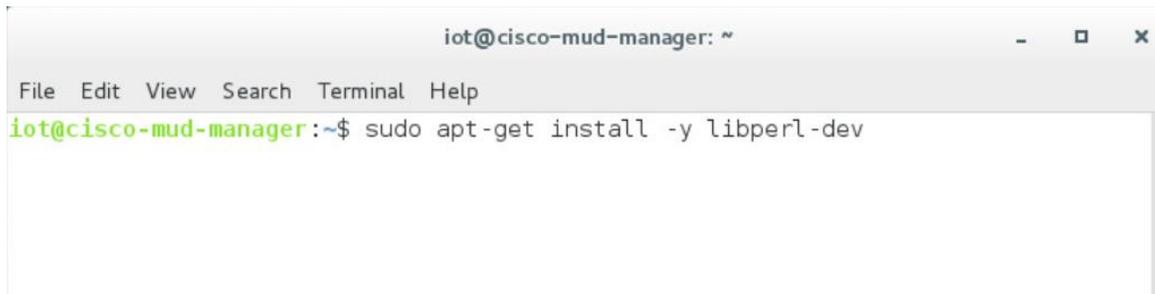


```
iot@cisco-mud-manager: ~  
File Edit View Search Terminal Help  
iot@cisco-mud-manager:~$ sudo apt-get install -y libcurl4-gnutls-dev
```

457

458

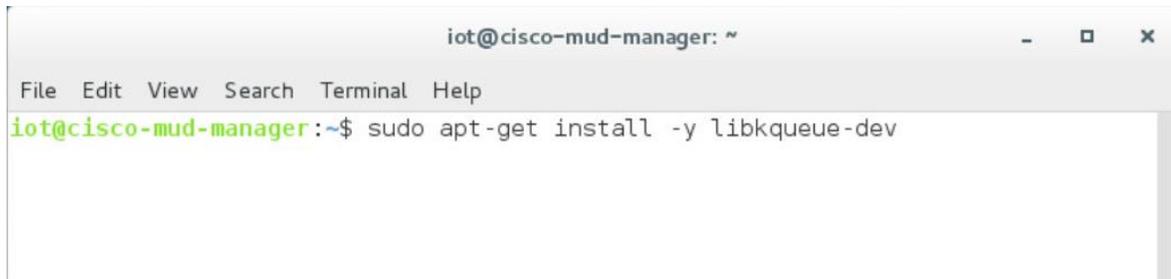
- d. `sudo apt-get install -y libperl-dev`



```
iot@cisco-mud-manager: ~  
File Edit View Search Terminal Help  
iot@cisco-mud-manager:~$ sudo apt-get install -y libperl-dev
```

459

460 e. `sudo apt-get install -y libkqueue-dev`



```
iot@cisco-mud-manager: ~  
File Edit View Search Terminal Help  
iot@cisco-mud-manager:~$ sudo apt-get install -y libkqueue-dev
```

461

462 f. `sudo apt-get install -y libssl-dev`



```
iot@cisco-mud-manager: ~  
File Edit View Search Terminal Help  
iot@cisco-mud-manager:~$ sudo apt-get install -y libssl-dev
```

463 2. Download the source by entering the following command (Note: Version 3.0.17 and later are
464 recommended):

465 `wget ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-3.0.17.tar.gz`

466



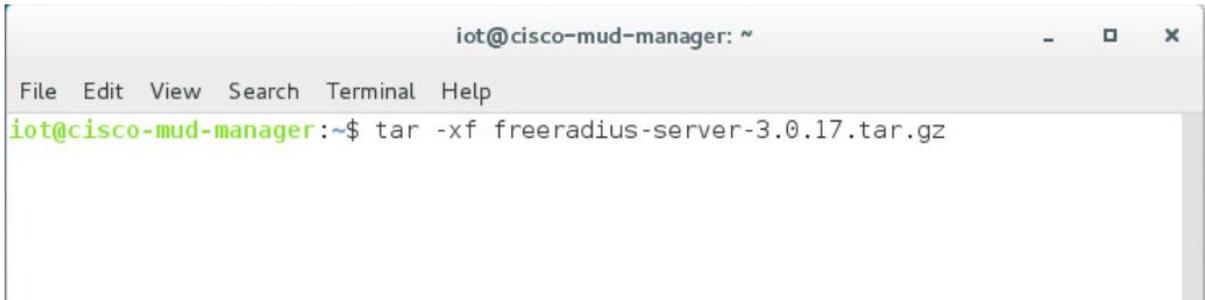
```
iot@cisco-mud-manager: ~  
File Edit View Search Terminal Help  
iot@cisco-mud-manager:~$ wget ftp://ftp.freeradius.org/pub/freeradius  
-server-3.0.17.tar.gz
```

467

468 3. Untar the file pulled by entering the following command:

469 `tar -xf freeradius-server-3.0.17.tar.gz`

470

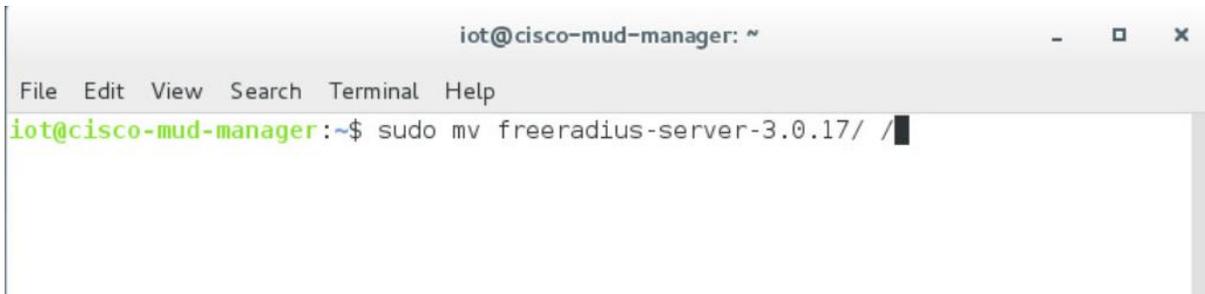


```
iot@cisco-mud-manager: ~  
File Edit View Search Terminal Help  
iot@cisco-mud-manager:~$ tar -xf freeradius-server-3.0.17.tar.gz
```

471 4. Move the FreeRADIUS directory to the root directory:

472 `sudo mv freeradius-server-3.0.17/ /`

473



```
iot@cisco-mud-manager: ~  
File Edit View Search Terminal Help  
iot@cisco-mud-manager:~$ sudo mv freeradius-server-3.0.17/ /
```

474 5. Change to the FreeRADIUS directory:

475 `cd /freeradius-server-3.0.17/`

476



```
iot@cisco-mud-manager: /  
File Edit View Search Terminal Help  
iot@cisco-mud-manager:/$ cd /freeradius-server-3.0.17/
```

477 6. Make and install the source by entering the following:

478 a. `sudo ./configure --with-rest --with-json-c --with-perl`

479



```
iot@cisco-mud-manager: /freeradius-server-3.0.17
File Edit View Search Terminal Help
iot@cisco-mud-manager: /freeradius-server-3.0.17$ sudo ./configure --with-rest --with-json-c --with-perl
```

480

b. sudo make

481



```
iot@cisco-mud-manager: /freeradius-server-3.0.17
File Edit View Search Terminal Help
iot@cisco-mud-manager: /freeradius-server-3.0.17$ sudo make
```

482

c. sudo make install



```
iot@cisco-mud-manager: /freeradius-server-3.0.17
File Edit View Search Terminal Help
iot@cisco-mud-manager: /freeradius-server-3.0.17$ sudo make install
```

483 2.1.7 FreeRADIUS Configuration

484 1. Change to the FreeRADIUS subdirectory in the MUD manager directory:

485 `cd /MUD-Manager/examples/AAA-LLDP-DHCP/`

```

iot@cisco-mud-manager: /freeradius-server-3.0.17
File Edit View Search Terminal Help
iot@cisco-mud-manager: /freeradius-server-3.0.17$ cd /MUD-Manager/examples/AAA-LL
DP-DHCP/

```

- 486
487 2. Run the setup script:

488 `sudo ./FR-setup.sh`

```

iot@cisco-mud-manager: /MUD-Manager/examples/AAA-LLDP-DHCP
File Edit View Search Terminal Help
iot@cisco-mud-manager: /MUD-Manager/examples/AAA-LLDP-DHCP$ sudo ./FR-setup.sh

```

- 489
490 3. Enter the following command to log in as root:

491 `sudo su`

```

nccoe — iot@cisco-mud-manager: /MUD-Manager/examples/AAA-LLDP-DHCP — ssh iot@192.168.11.45...
iot@cisco-mud-manager: /MUD-Manager/examples/AAA-LLDP-DHCP$ sudo su

```

- 492 4. Change to the radius directory:

493 `cd /usr/local/etc/raddb/`

```

nccoe — root@cisco-mud-manager: /MUD-Manager/examples/AAA-LLDP-DHCP — ssh iot@192.168.11.45...
root@cisco-mud-manager: /MUD-Manager/examples/AAA-LLDP-DHCP# cd /usr/local/etc/ra
ddb/

```

- 494 5. Open the *clients.conf* file:

495 `vim clients.conf`

```

nccoe — root@cisco-mud-manager: /usr/local/etc/raddb — ssh iot@192.168.11.45 — 80x24
root@cisco-mud-manager:/usr/local/etc/raddb# vim clients.conf

```

- 496 6. Add the network address server (NAS) as an authorized client in the configuration file on the
 497 server by adding an entry for the NAS in the *client.conf* file opened (Note: Replace the IP address
 498 below with the IP address of the NAS and use the “secret” configured on the NAS to talk to
 499 RADIUS servers):

```

500 client 192.168.10.2 {
501     ipaddr = 192.168.10.2
502     secret = cisco
503 }

```

```

nccoe — root@cisco-mud-manager: /usr/local/etc/raddb — ssh iot@192.168.11.45 — 80x24

```

```

client 192.168.10.2 {
    ipaddr      = 192.168.10.2
    secret      = cisco
}

```

- 504
 505 7. Save and close the file.

506 2.1.8 Start MUD Manager and FreeRADIUS Server

- 507 1. Start and enable the database by executing the following commands:

508 `sudo systemctl start mongod`

```

nccoe — iot@cisco-mud-manager: ~ — ssh iot@192.168.11.45 — 80x24
iot@cisco-mud-manager:~$ sudo systemctl start mongod

```

509 `sudo systemctl enable mongod`

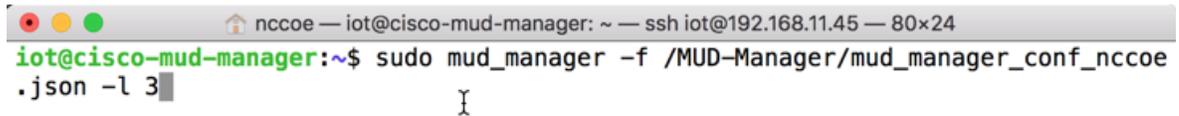
```

nccoe — iot@cisco-mud-manager: ~ — ssh iot@192.168.11.45 — 80x24
iot@cisco-mud-manager:~$ sudo systemctl enable mongod

```

- 510 2. Start the MUD manager in the foreground with logging enabled by entering the following
511 command:

512 `sudo mud_manager -f /MUD-Manager/mud_manager_conf_nccoe.json -l 3`

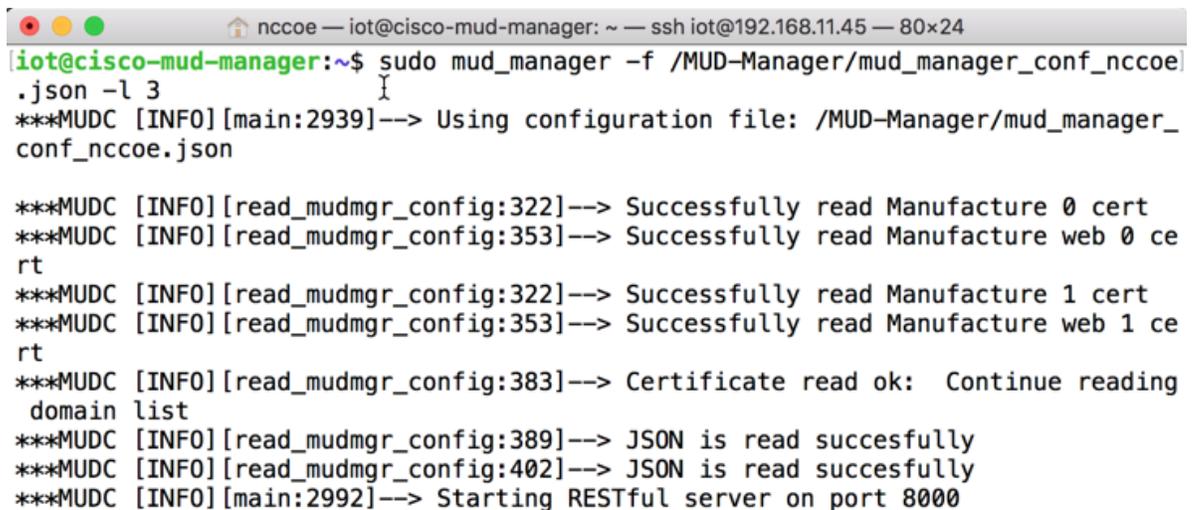


```

nccoe — iot@cisco-mud-manager: ~ — ssh iot@192.168.11.45 — 80x24
iot@cisco-mud-manager:~$ sudo mud_manager -f /MUD-Manager/mud_manager_conf_nccoe
.json -l 3

```

- 513 The following output should appear if the service started successfully:



```

nccoe — iot@cisco-mud-manager: ~ — ssh iot@192.168.11.45 — 80x24
iot@cisco-mud-manager:~$ sudo mud_manager -f /MUD-Manager/mud_manager_conf_nccoe
.json -l 3
***MUDC [INFO][main:2939]--> Using configuration file: /MUD-Manager/mud_manager_
conf_nccoe.json

***MUDC [INFO][read_mudmgr_config:322]--> Successfully read Manufacture 0 cert
***MUDC [INFO][read_mudmgr_config:353]--> Successfully read Manufacture web 0 ce
rt
***MUDC [INFO][read_mudmgr_config:322]--> Successfully read Manufacture 1 cert
***MUDC [INFO][read_mudmgr_config:353]--> Successfully read Manufacture web 1 ce
rt
***MUDC [INFO][read_mudmgr_config:383]--> Certificate read ok: Continue reading
domain list
***MUDC [INFO][read_mudmgr_config:389]--> JSON is read succesfully
***MUDC [INFO][read_mudmgr_config:402]--> JSON is read succesfully
***MUDC [INFO][main:2992]--> Starting RESTful server on port 8000

```

- 514
515 3. Start the FreeRADIUS service in the foreground with logging enabled by entering the following
516 command:

517 `sudo radiusd -Xxx`



```

nccoe — iot@cisco-mud-manager: ~ — ssh iot@192.168.11.45 — 80x24
iot@cisco-mud-manager:~$ sudo radiusd -Xxx

```

- 518 At this point all the necessary processes are up and running from the server side and it is time to move
519 on to configuring the switch. Any DHCP activity on the network should appear here once the switch is
520 configured accordingly.

521 2.2 MUD File Server

522 2.2.1 MUD File Server Overview

523 For this example implementation, the NCCoE built a MUD file server hosted within the lab
524 infrastructure. This file server signs and stores the MUD files along with their corresponding signature
525 files for the MUD-capable IoT devices used in the build. The MUD file server is also responsible for
526 serving the MUD file and the corresponding signature file upon request from the MUD manager.

527 2.2.2 Configuration Overview

528 The following subsections document the software and network configurations for the MUD file server.

529 2.2.2.1 Network Configuration

530 This server was hosted in the NCCoE's virtual environment, functioning as a cloud service. The IP address
531 was statically assigned.

532 2.2.2.2 Software Configuration

533 For this example implementation, the server ran on the CentOS 7 operating system. The MUD files and
534 signatures were hosted by an Apache web server and configured to use secure sockets layer/ transport
535 layer security (SSL/TLS) encryption.

536 2.2.2.3 Hardware Configuration

537 The MUD file server was hosted in the NCCoE's virtual environment, functioning as a cloud service.

538 2.2.3 Setup

539 The following subsections describe the setup process for configuring the MUD file server.

540 2.2.3.1 Apache Web Server

541 The Apache web server was set up by using the official Apache documentation at
542 <https://httpd.apache.org/docs/current/install.html>. After that, SSL/TLS encryption was set up by using
543 the digital certificate and key obtained from DigiCert. This was set up by using the official Apache
544 documentation, found at https://httpd.apache.org/docs/current/ssl/ssl_howto.html.

545 2.2.3.2 MUD File Creation and Signing

546 This section details creating and signing a MUD file on the MUD file server. It is not mandated by the
547 MUD specification that this signing process be performed on the MUD file server itself.

548 **2.2.3.2.1 MUD File Creation**

549 In this implementation, MUD Maker was used to build MUD files. Once the permitted communications
550 have been defined for the IoT device, proceed to www.mudmaker.org to leverage the online tool. There
551 is also a list of sample MUD files on the site, which can be used as a reference. Upon navigating to
552 www.mudmaker.org, complete the following steps to create a MUD file:

- 553 1. Specify the host that will be serving the MUD file and the model name of the device in the
554 following text fields (Note: This will result in the MUD URL for this device):

555 Sample input: mudfileserver, testmudfile

Welcome to MUD File Maker!

This page will help you create a Manufacturer Usage Description (MUD) file for your web site. MUD files can be used by local page that you have designed your product to have. For more information, see [draft-ietf-opsawg-mud](#).

Some resources you might find interesting (apart from this page):

- [The MUD specification](#)
- [The Cisco POC MUD Manager](#)
- [The OSmud.org MUD Manager](#)

Some Samples

A device that just needs to talk to a single cloud service
A device that just needs to talk to its local controllers
A device that just needs to talk to devices from the same manufacturer

If you use the samples, you will need to modify some of the fields, and of course sign them.

Make Your Own!

Please enter host and model the intended MUD-URL for this device: 

/ (model name here->)

Manufacturer Name

Please provide a URL to documentation about this device:

Please enter a short description for this device:

556

- 557 2. Specify the Manufacturer Name of the device in the following text field:

Make Your Own!

Please enter host and model the intended MUD-URL for this device: 

https:// / (model name here->

Manufacturer Name

Please provide a URL to documentation about this device:

Please enter a short description for this device:

×

How will this device communicate on the network?

Internet communication

Access to cloud services and other specific Internet hosts. 

558

559

3. Include a URL to documentation about this device in the following text field:

Make Your Own!

Please enter host and model the intended MUD-URL for this device: 

https:// / (model name here->)

Manufacturer Name

Please provide a URL to documentation about this device:

Please enter a short description for this device:



How will this device communicate on the network?

Internet communication

Access to cloud services and other specific Internet hosts. 

560

561

4. Include a short description of the device in the following text field:

Make Your Own!

Please enter host and model the intended MUD-URL for this device: 

https:// / (model name here->)

Manufacturer Name

Please provide a URL to documentation about this device:

Please enter a short description for this device:

x

How will this device communicate on the network?

Internet communication 

Access to cloud services and other specific Internet hosts.

562
563
564

5. Check the boxes for the types of network communication that are allowed for the device:

How will this device communicate on the network?

	Allow?
Internet communication  Access to cloud services and other specific Internet hosts.	<input checked="" type="checkbox"/>
Access to controllers specific to this device (no need to name a class). 	<input type="checkbox"/>
Controller access  Access to classes of devices that are known to be controllers	<input type="checkbox"/>
Local communication  Access to/from any local host for specific services (like COAP or HTTP)	<input type="checkbox"/>
Specific types of devices  Access to classes of devices that are identified by their MUD URL	<input type="checkbox"/>
Access to devices to/from the same manufacturer 	<input type="checkbox"/>

565

- 566 6. Specify the internet protocol version that the device leverages:

Access to devices to/from the same manufacturer 

This device speaks

Create rules below

Internet Hosts

Protocol

- 567 7. Specify the fields (Internet Hosts, Protocol, Local Port, Remote Port, and Initiated by) that this
568 device will be communicating with:

This device speaks

Create rules below

Internet Hosts

Protocol

Local Port Remote Port Initiated by

- 569 8. Click **Submit** to generate the MUD file:

This device speaks ▾

Create rules below

Internet Hosts

Protocol ▾
Local Port Remote Port Initiated by ▾

570 9. Once completed, the page will redirect to the following page that outputs the MUD file on the
571 screen. Click **Download** to download the MUD file, which is a .JSON file:

572

Your MUD file is ready!

Congratulations! You've just created a MUD file. Simply Cut and paste between the lines and stick into a file. Your next steps are to sign the file and place it in the location that its c

- Get a certificate with which to sign documents/email.
- Use OpenSSL as follows:
openssl cms -sign -signer YourCertificate.pem -inkey YourKey.pem -in YourMUDfile.json -binary -outform DER -certfile intermediate-certs.pem -out YourSignature.p7s
- Place the signature file and the MUD file on your web server (it should match the MUD-URL)

Would you like to download this file?

```
{  
  "ietf-mud:mud": {  
    "mud-version": 1,  
    "mud-url": "https://mudfileserver/testmudfile",  
    "last-update": "2019-02-27T20:51:19+00:00",  
    "cache-validity": 48,  
    "is-supported": true,  
    "systeminfo": "Test MUD file",  
    "mfq-name": "NCCoE",  
  }  
}
```

573

574 10. Click **Save** to store a copy of the MUD file:

575

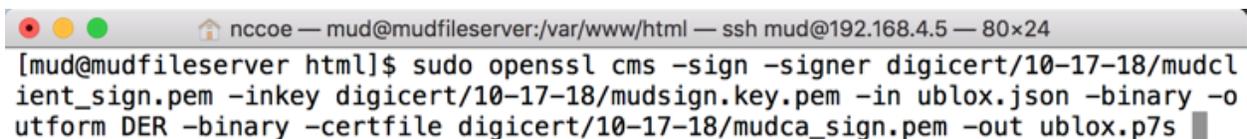
Do you want to open or save **mudfile.json** (2.13 KB) from **mudmaker.org**? ▾ ×

576 2.2.3.2.2 MUD File Signature Creation and Verification

577 In this implementation, OpenSSL is used to sign and verify MUD files. This example uses the MUD file
 578 created in the previous section. To start this process, start with a MUD file (in our example, this file is
 579 named *ublox.json*), the Signing Certificate, the Private Key for the Signing Certificate, the Intermediate
 580 Certificate for the Signing Certificate, and the Certificate of the Trusted Root Certificate Authority for the
 581 Signing Certificate.

582 1. Sign the MUD file by using the following command:

```
583 sudo openssl cms -sign -signer <Signing Certificate> -inkey <Private Key for Signing
584 Certificate> -in <Name of MUD File> -binary -outform DER -binary -certfile
585 <Intermediate Certificate for Signing Certificate> -out <Name of MUD File without the
586 .json file extension>.p7s
```



A terminal window screenshot showing the command to sign a MUD file. The terminal title is 'nccoe — mud@mudfileserverserver:/var/www/html — ssh mud@192.168.4.5 — 80x24'. The command entered is: `[mud@mudfileserverserver html]$ sudo openssl cms -sign -signer digicert/10-17-18/mudclient_sign.pem -inkey digicert/10-17-18/mudsign.key.pem -in ublox.json -binary -outform DER -binary -certfile digicert/10-17-18/mudca_sign.pem -out ublox.p7s`

587 This will create a signature file for the MUD file that has the same name as the MUD file but ends with
 588 the .p7s file extension, i.e., in our case *ublox.p7s*.

589 2. Manually verify the MUD File Signature by using the following command:

```
590 sudo openssl cms -verify -in <Name of MUD File>.p7s -inform DER -content <Name of MUD
591 File>.json -CAfile <Certificate of Trusted Root Certificate Authority for Signing
592 Certificate>
```



A terminal window screenshot showing the command to verify a MUD file signature. The terminal title is 'nccoe — mud@mudfileserverserver:/var/www/html — ssh mud@192.168.4.5 — 80x24'. The command entered is: `[mud@mudfileserverserver html]$ sudo openssl cms -verify -in ublox.p7s -inform DER -content ublox.json -CAfile digicert/10-17-18/mudca_sign.pem`

593 If a valid file signature was created successfully, a corresponding message should appear. Both the MUD
 594 file and MUD File Signature should be placed on the MUD file server in the Apache server directory.

595 2.3 Cisco Switch—Catalyst 3850-S

596 2.3.1 Cisco 3850-S Catalyst Switch Overview

597 The switch used in this build is an enterprise class, Layer 3 switch, the Cisco Catalyst 3850-S that had
 598 been modified to support MUD functionality as a proof-of-concept implementation. In addition to
 599 providing DHCP services, the switch also acts as a broker for connected IoT devices for authentication,

600 authorization, and accounting through a FreeRADIUS server. The LLDP is enabled on ports that MUD-
601 capable devices are plugged into to help facilitate recognition of connected IoT device features,
602 capabilities, and neighbor relationships at layer 2. Additionally, an access session policy is configured on
603 the switch to enable port control for multihost authentication and port monitoring. The combined effect
604 of these switch configurations is a dynamic access list, which has been generated by the MUD manager,
605 being active on the switch to permit or deny access to and from MUD-capable IoT devices.

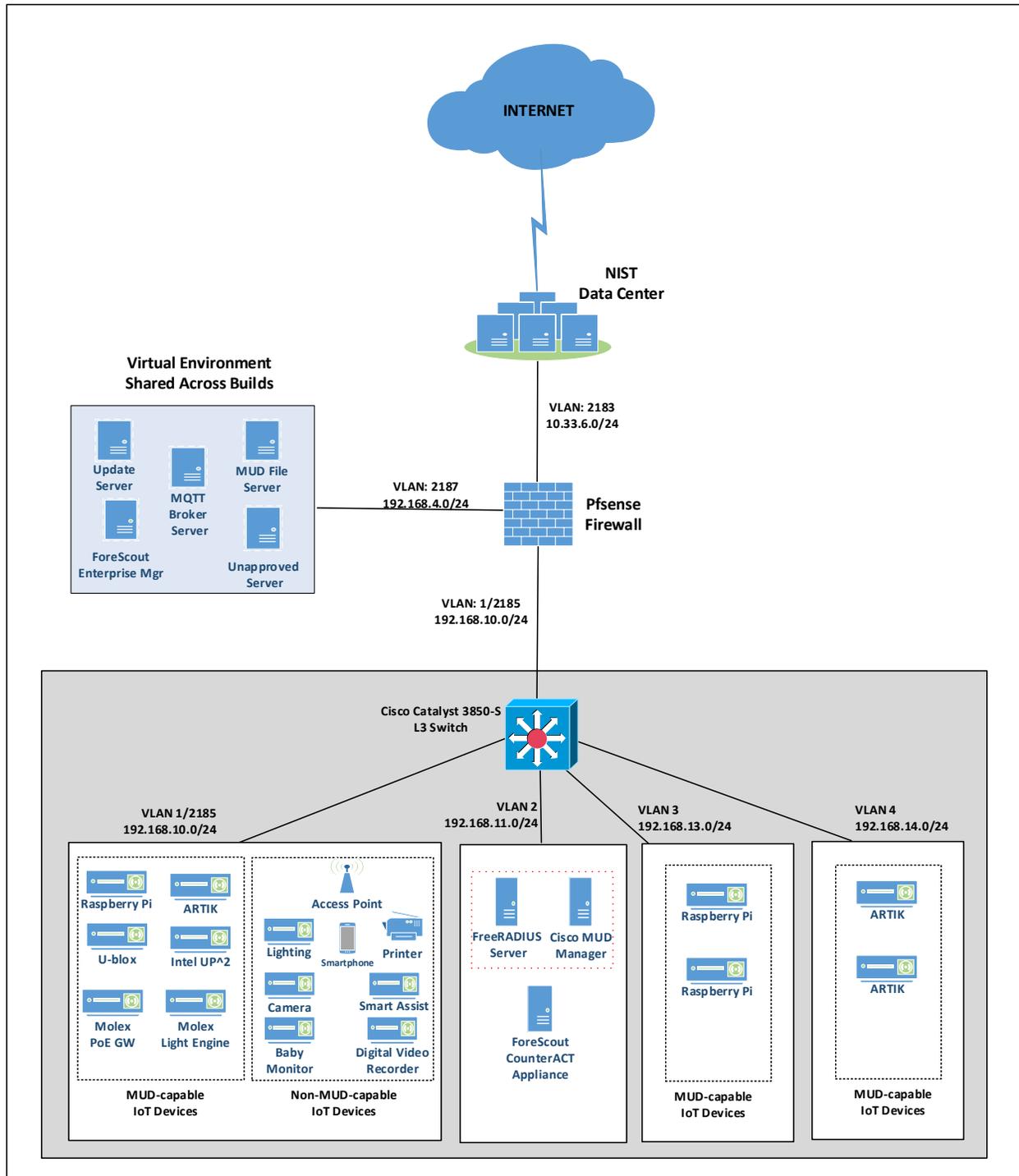
606 2.3.2 Configuration Overview

607 The following subsections document the network, software, and hardware configurations for the Cisco
608 Catalyst 3850-S switch.

609 2.3.2.1 Network Configuration

610 This section describes how to configure the required Cisco Catalyst 3850-S switch to support the
611 example implementation. A special image for the Catalyst 3850-S was provided by Cisco to support
612 MUD-specific functionality. In our example implementation, the switch is integrated with a DHCP server
613 and a FreeRADIUS server, which together support delivery of the MUD URL to the MUD manager via
614 either DHCP or LLDP. The MUD manager is also able to generate and send a dynamic access list to the
615 switch, via the RADIUS server, to permit or deny access to and from the IoT devices. In addition to
616 hosting directly connected IoT devices on VLANs 1, 3, and 4, the switch also hosts both the MUD
617 manager and the FreeRADIUS servers on VLAN 2. As illustrated in Figure 2-1, each locally configured
618 VLAN is protected by a firewall that connects the lab environment to the NIST data center, which
619 provides internet access for all connected devices.

620 Figure 2-1: Physical Architecture—Build 1



621

622 **2.3.2.2 Software Configuration**

623 The prototype, MUD-capable Cisco 3850-S used in this build is running internetwork operating system
624 (IOS) version 16.09.02.

625 **2.3.2.3 Hardware Configuration**

626 The Catalyst 3850-S switch configured in the lab consists of 24 one-gigabit Ethernet ports with two
627 optional 10-gigabit Ethernet uplink ports. A customized version of Cat-OS is installed on the switch. The
628 versions of the operating system are as follows:

- 629 ▪ Cat3k_caa-guestshell.16
- 630 ▪ Cat3k_caa-rpbase.16.06.
- 631 ▪ Cat3k_caa-rpcore.16.06.
- 632 ▪ Cat3k_caa-srdriver.16.06.0
- 633 ▪ Cat3k_caa-webui.16.06.0

634 **2.3.3 Setup**

635 The table below lists the Cisco 3850-S switch running configuration used for the lab environment. In
636 addition to the IOS version and a few generic configuration items, configuration items specifically
637 relating to integration with the MUD manager and IoT devices are highlighted in bold fonts; these
638 include DHCP, LLDP, AAA, RADIUS, and policies regarding access session. The table also provides a
639 description of each configuration item for ease of understanding.

640 **Table 2-1 Cisco 3850-S Switch Running Configuration**

Configuration Item	Description
version 16.9 no service pad service timestamps debug datetime msec service timestamps log datetime msec service call-home no platform punt-keepalive disable-kernel-core ! hostname Build1 ! aaa new-model ! aaa authentication dot1x default group radius	General overview of configuration information needed to configure AAA to use RADIUS and configure the RADIUS server itself. Note that the FreeRADIUS and AAA passwords must match. Enables AAA Creates an 802.1X AAA authentication method list

Configuration Item	Description
<pre> aaa authorization network default group radius aaa accounting identity default start-stop group radius aaa accounting network default start-stop group radius ! aaa server radius dynamic-author client 192.168.11.45 server-key cisco server-key cisco ! aaa session-id common radius server AAA address ipv4 192.168.11.45 auth-port 1812 acct-port 1813 key cisco </pre>	<p>Configures network authorization via RADIUS, including network-related services such as VLAN assignment</p> <p>Enables accounting method list for Session Aware Networking subscriber services</p> <p>Enables accounting for all network-related service requests</p> <p>Enables dynamic authorization local server configuration mode and specifies a RADIUS client/key from which a device accepts Change of Authorization (CoA) and disconnect requests</p> <p>Enables AAA server from the list of multiple AAA servers configured</p> <p>Uses the IP address and ports on which the FreeRADIUS server is listening</p>
<pre> ip routing ! ip dhcp excluded-address 192.168.10.1 192.168.10.100 ! ip dhcp pool NCCOE-V3 network 192.168.13.0 255.255.255.0 default-router 192.168.13.1 dns-server 8.8.8.8 lease 0 12 ! ip dhcp pool NCCOE-V4 network 192.168.14.0 255.255.255.0 default-router 192.168.14.1 dns-server 8.8.8.8 ! </pre>	<p><u>Define a DHCP pool for IoT devices</u></p> <p>Note To reserve a static address, use the hardware-address command as opposed to client address.</p> <p>DHCP server configuration to exclude selected addresses from pool</p> <p>DHCP server configuration to assign IP address to devices on VLAN 3</p> <p>DHCP server configuration to assign IP address to devices on VLAN 4</p>

Configuration Item	Description
<pre> ip dhcp pool NCCOE network 192.168.10.0 255.255.255.0 default-router 192.168.10.2 dns-server 8.8.8.8 lease 0 12 ! ! ip dhcp snooping ip dhcp snooping vlan 1,3 </pre>	<p>DHCP server configuration to assign IP address to devices on VLAN 1</p> <p>Enables DHCP snooping globally Specifically enables DHCP snooping on VLANs 1 and 3</p>
<pre> ! access-session attributes filter-list list mudtest lldp dhcp access-session accounting attributes filter-spec include list mudtest access-session monitor </pre>	<p>Configures access-session attributes to cause LLDP TLVs (including the MUD URL) to be forwarded in an accounting message to the AAA server</p>
<pre> ! dot1x logging verbose </pre>	<p>Global configuration command to filter 802.1x authentication verbose messages</p>
<pre> ldp run ! </pre>	<p>Enables LLDP, a discovery protocol that runs over Layer 2 (the data link layer) to gather information on non-Cisco-manufactured devices</p>
<pre> policy-map type control subscriber mud-mab-test event session-started match-all 10 class always do-until-failure 10 authenticate using mab ! template mud-mab-test switchport mode access mab access-session port-control auto service-policy type control subscriber mud-mab-test ! </pre>	<p>Configures identity control policies that define the actions that Session Aware Networking takes in response to specified conditions and subscriber events</p> <p>Enables policy-map (mud-mab-test) and template to cause Media Access Control (MAC) Address Bypass (MAB) to happen</p> <p>Dynamically applies an interface template to a target</p> <p>Sets the authorization state of a port. The default value is force-authorized.</p>

Configuration Item	Description
<pre>interface GigabitEthernet1/0/15 source template mud-mab-test !</pre>	<p>Statically applies an interface template to a target, i.e., an IoT device</p>
<pre>interface GigabitEthernet1/0/16 source template mud-mab-test !</pre>	<p>Statically applies an interface template to a target, i.e., an IoT device</p>
<pre>interface GigabitEthernet1/0/17 source template mud-mab-test !</pre>	<p>Statically applies an interface template to a target, i.e., an IoT device</p>
<pre>interface GigabitEthernet1/0/18 source template mud-mab-test !</pre>	<p>Statically applies an interface template to a target, i.e., an IoT device</p>
<pre>interface GigabitEthernet1/0/19 source template mud-mab-test !</pre>	<p>Statically applies an interface template to a target, i.e., an IoT device</p>
<pre>interface GigabitEthernet1/0/20 source template mud-mab-test !</pre>	<p>Statically applies an interface template to a target, i.e., an IoT device</p>
<pre>interface GigabitEthernet1/0/21</pre>	
<pre>interface GigabitEthernet1/0/22</pre>	
<pre>interface GigabitEthernet1/0/23 switchport access vlan 2</pre>	
<pre>interface GigabitEthernet1/0/24 switchport access vlan 2</pre>	
<pre>interface GigabitEthernet1/1/1</pre>	
<pre>interface GigabitEthernet1/1/2</pre>	
<pre>interface GigabitEthernet1/1/3</pre>	
<pre>interface GigabitEthernet1/1/4</pre>	
<pre>interface TenGigabitEthernet1/1/1</pre>	
<pre>interface TenGigabitEthernet1/1/2</pre>	
<pre>interface TenGigabitEthernet1/1/3</pre>	

Configuration Item	Description
<pre> ! interface TenGigabitEthernet1/1/4 ! interface Vlan1 ip address 192.168.10.2 255.255.255.0 ! interface Vlan2 ip address 192.168.11.1 255.255.255.0 ! interface Vlan3 ip address 192.168.13.1 255.255.255.0 ! interface Vlan4 ip address 192.168.14.1 255.255.255.0 ! interface Vlan5 ip address 192.168.15.1 255.255.255.0 ! </pre>	<p>Configure and address VLAN1 interface for inter-VLAN routing</p> <p>Configure and address VLAN2 interface for inter-VLAN routing</p> <p>Configure and address VLAN3 interface for inter-VLAN routing</p> <p>Configure and address VLAN4 interface for inter-VLAN routing</p> <p>Configure and address VLAN5 interface for inter-VLAN routing</p>
<pre> ! ip default-gateway 192.168.10.1 ip forward-protocol nd ip http server ip http authentication local ip http secure-server ip route 0.0.0.0 0.0.0.0 192.168.10.1 ip route 192.168.12.0 255.255.255.0 192.168.5.1 ! </pre>	

641 **2.4 DigiCert Certificates**

642 **2.4.1 DigiCert CertCentral Overview**

643 DigiCert’s CertCentral web-based platform allows for provisioning and management of publicly trusted
644 X.509 certificates for a variety of purposes. After establishing an account, clients can log in, request,
645 renew, and revoke certificates by using only a browser. For this implementation, two certificates were
646 provisioned: a private TLS certificate for the MUD file server to support the https connection from the
647 MUD manager to the MUD file server, and a Premium certificate for signing the MUD files.

648 2.4.2 Configuration Overview

649 This section typically documents the network, software, and hardware configurations, but that is not
650 necessary for this component.

651 2.4.3 Setup

652 DigiCert allows certificates to be requested through their web-based platform, CertCentral. A user
653 account is needed to access CertCentral. For details on creating a user account and getting set up with
654 an account, follow the steps described here:

655 <https://www.digicert.com/certcentral-support/digicert-getting-started-guide.pdf>

656 2.4.3.1 TLS Certificate

657 For this example implementation, we leveraged DigiCert's Private TLS certificate because the MUD file
658 server is hosted internally. This certificate supports https connections to the MUD file server, which are
659 required by the MUD manager. Additional information about the TLS certificates offered by DigiCert can
660 be found at <https://www.digicert.com/security-certificate-support/>.

661 For instructions on how to request a certificate, proceed to the DigiCert documentation found here and
662 follow the process for the specific certificate being requested: [https://www.digicert.com/certcentral-
663 support/basic-certcentral-getting-started-guide-v1.4_2018-12-10_opt.pdf](https://www.digicert.com/certcentral-support/basic-certcentral-getting-started-guide-v1.4_2018-12-10_opt.pdf)

664 Once requested, integrate the certificate onto the MUD file server as described in Section 2.2.3.1.

665 2.4.3.2 Premium Certificate

666 To sign MUD files according to the MUD specification, a client certificate is required. For this
667 implementation, we leveraged DigiCert's Premium certificate to sign MUD files. This certificate supports
668 signing or encrypting secure/multipurpose internet mail extensions (S/MIME) messages, which is
669 required by the specification.

670 For detailed instructions on how to request and implement a Premium certificate, proceed to the
671 DigiCert documentation found here: [https://www.digicert.com/certcentral-support/client-certificate-
672 guide.pdf](https://www.digicert.com/certcentral-support/client-certificate-guide.pdf)

673 Once requested, sign MUD files as described in Section 2.2.3.2.2.

674 2.5 IoT Devices

675 2.5.1 Moxel PoE Gateway and Light Engine

676 This section provides configuration details of the MUD-capable Moxel PoE Gateway and Light Engine
677 used in the example implementation, which emits a MUD URL that uses LLDP.

678 **2.5.1.1 Configuration Overview**

679 The Moxel PoE Gateway runs firmware created and provided by Moxel. This firmware was modified by
680 Moxel to emit a MUD URL that uses an LLDP message.

681 **2.5.1.1.1 Network Configuration**

682 The Moxel PoE Gateway is connected to the network over a wired Ethernet connection. The IP address
683 is assigned dynamically by using DHCP.

684 **2.5.1.1.2 Software Configuration**

685 For this example implementation, the Moxel PoE Gateway is configured with Moxel’s PoE Gateway
686 firmware, version 1.6.1.8.4.

687 **2.5.1.1.3 Hardware Configuration**

688 The Moxel PoE Gateway used in this build was Model Number 180993-0001, dated 03/2017.

689 **2.5.1.2 Setup**

690 The Moxel PoE Gateway is controlled via the Constrained Application Protocol (CoAP), and CoAP
691 commands were used to ensure that device functionality was maintained during the MUD process.

692 **2.5.1.2.1 DHCP Client Configuration**

693 The device uses the default DHCP client included in the Moxel PoE Gateway firmware.

694 **2.5.2 IoT Development Kits—Linux-Based**

695 This section provides configuration details for the Linux-based IoT development kits used in the example
696 implementation, which emit MUD URLs by using DHCP. It also provides information regarding a basic IoT
697 application used to test the MUD process.

698 **2.5.2.1 Configuration Overview**

699 The devkits run various flavors of Linux-based operating systems and are configured to emit a MUD URL
700 during a typical DHCP transaction. They also run a Python script that allows the devkits to receive and
701 process commands by using the MQTT protocol, which can be sent to peripherals connected to the
702 devkits.

703 **2.5.2.1.1 Network Configuration**

704 The devkits are connected to the network over a wired Ethernet connection. The IP address is assigned
705 dynamically by using DHCP.

706 **2.5.2.1.2 Software Configuration**

707 For this example implementation, the Raspberry Pi is configured on Raspbian 9, the Samsung ARTIK 520
708 is configured on Fedora 24, and the Intel UP Squared Grove is configured on Ubuntu 16.04 LTS. The

709 devkits also utilized dhclient as the default DHCP client. This DHCP client is installed natively on many
710 Linux distributions and can be installed using a preferred package manager if not currently present.

711 2.5.2.1.3 Hardware Configuration

712 The hardware used for these devkits included the Raspberry Pi 3 Model B, Samsung ARTIK 520, and Intel
713 UP Squared Grove.

714 2.5.2.2 Setup

715 The following subsection describes setting up the devkits to send a MUD URL during the DHCP
716 transaction and to act as a smart device by leveraging an MQTT broker server (we describe setting up
717 the MQTT broker server in Section 2.8).

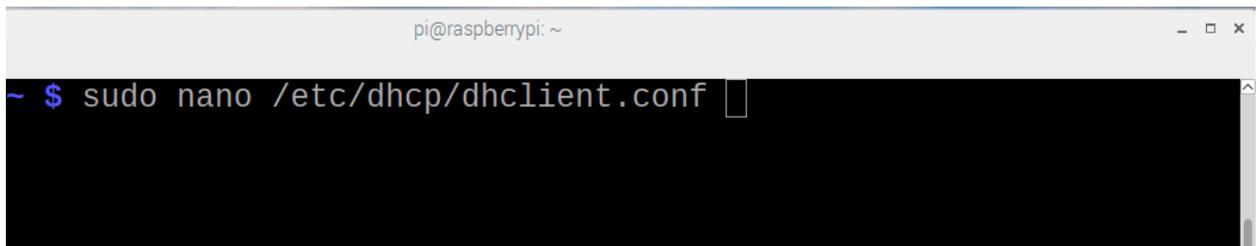
718 2.5.2.2.1 DHCP Client Configuration

719 We leveraged dhclient as the default DHCP client for these devices due to the availability of the DHCP
720 client on different Linux platforms and the ease of emitting MUD URLs via DHCP.

721 To set up the dhclient configuration:

- 722 1. Open a terminal on the device.
- 723 2. Ensure that any other conflicting DHCP clients are disabled or removed.
- 724 3. Install the dhclient package (if needed).
- 725 4. Edit the *dhclient.conf* file by entering the following command:

726 `sudo nano /etc/dhcp/dhclient.conf`
727

A terminal window screenshot with a title bar that reads "pi@raspberrypi: ~". The terminal shows a prompt character "~" followed by a dollar sign "\$" and the command "sudo nano /etc/dhcp/dhclient.conf". A cursor is visible at the end of the command line. The terminal background is black, and the text is white.

728
729

- 730 5. Add the following lines:

731 `option mud-url code 161 = text;`
732 `send mud-url = "<insert URL for MUD File here>";`

```

GNU nano 2.7.4      File: /etc/dhcp/dhclient.conf      Modified
#lease {
# interface "eth0";
# fixed-address 192.33.137.200;
# medium "link0 link1";
# option host-name "andare.swiftmedia.com";
# option subnet-mask 255.255.255.0;
# option broadcast-address 192.33.137.255;
# option routers 192.33.137.250;
# option domain-name-servers 127.0.0.1;
# renew 2 2000/1/12 00:00:01;
# rebind 2 2000/1/12 00:00:01;
# expire 2 2000/1/12 00:00:01;
#}

#DHCP MUD Option
option mud-url code 161 = text;
send mud-url = "https://mudfileserver/pi4";

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line

```

733
734 6. Save and close the file.

735 7. Reboot the device:

736 `reboot`



```

pi@raspberrypi: ~
File Edit Tabs Help
pi@raspberrypi:~ $ reboot

```

737
738 8. Open a terminal.

739 9. Execute the dhclient:

740 `sudo dhclient -v`

741



```

pi@raspberrypi: ~
File Edit Tabs Help
pi@raspberrypi:~ $ sudo dhclient -v

```

742

743 2.5.2.2.2 IoT Application for Testing

744 The following Python application was created by the NCCoE to enable the devkits to act as basic IoT
745 devices:

746 #Program: IoTapp.

747 #Version: 1.0

PRELIMINARY DRAFT

```
748 #Purpose:           Provide IoT capabilities to devkit.
749 #Protocols:        MQTT.
750 #Functionality:    Allow remote control of LEDs on connected breadboard.
751
752 #Libraries
753 import paho.mqtt.client as mqttClient
754 import time
755 import RPi.GPIO as GPIO
756
757 #Global Variables
758 BrokerAddress = "192.168.1.87" #IP address of Broker(Server), change as needed. Best
759 practice would be a registered domain name that can be queried for appropriate server
760 address.
761 BrokerPort = "1883" #Default port used by most MQTT Brokers. Would be 1883 if
762 using Transport Encryption with TLS.
763 ConnectionStatus = "Disconnected" #Status of connection to Broker. Should be either
764 "Connected" or "Disconnected".
765 LED = 26
766
767 #Supporting Functions
768 def on_connect(client, userdata, flags, rc): #Function for connection status to
769 Broker.
770     if rc == 0:
771         ConnectionStatus = "Connected to Broker!"
772         print(ConnectionStatus)
773     else:
774         ConnectionStatus = "Connection Failed!"
775         print(ConnectionStatus)
776
777 def on_message(client, userdata, msg): #Function for parsing message data.
778     if "ON" in msg.payload:
779         print("ON!")
```

PRELIMINARY DRAFT

```
780         GPIO.output(LED, 1)
781
782     if "OFF" in msg.payload:
783         print("OFF!")
784         GPIO.output(LED, 0)
785
786 def MQTTapp():
787     client = mqttClient.Client()      #New instance.
788     client.on_connect = on_connect
789     client.on_message = on_message
790     client.connect(BrokerAddress, BrokerPort)
791     client.loop_start()
792     client.subscribe("test")
793     try:
794         while True:
795             time.sleep(1)
796     except KeyboardInterrupt:
797         print("8")
798         client.disconnect()
799         client.loop_stop()
800
801 #Main Function
802 def main():
803
804     GPIO.setmode(GPIO.BCM)
805     GPIO.setup(LED, GPIO.OUT)
806
807     print("Main function has been executed!")
808     MQTTapp()
809
```

```

810 if __name__ == "__main__":
811     main()

```

812 2.5.3 IoT Development Kit–u-blox C027-G35

813 This section details configuration of a u-blox C027-G35, which emits a MUD URL by using DHCP, and a
814 basic IoT application used to test MUD rules.

815 2.5.3.1 Configuration Overview

816 This devkit runs the ARM Mbed-OS operating system and is configured to emit a MUD URL during a
817 typical DHCP transaction. It also runs a basic IoT application to test MUD rules.

818 2.5.3.1.1 Network Configuration

819 The u-blox C027 is connected to the network over a wired Ethernet connection. The IP address is
820 assigned dynamically by using DHCP.

821 2.5.3.1.2 Software Configuration

822 For this example implementation, the u-blox C027-G35 was configured on the Mbed-OS 5.10.4
823 operating system.

824 2.5.3.1.3 Hardware Configuration

825 The hardware used for this devkit is the u-blox C027-G35.

826 2.5.3.2 Setup

827 The following subsection describes setting up the u-blox C027-G35 to send a MUD URL in the DHCP
828 transaction and act as a smart device by establishing network connections to the update server and
829 other destinations.

830 2.5.3.2.1 DHCP Client Configuration

831 To add MUD functionality to the Mbed-OS DHCP client, the following two files inside Mbed-OS require
832 modification:

- 833 • *mbed-os/features/lwipstack/lwip/src/include/lwip/prot/dhcp.h*
- 834 ○ **NOT:** *mbed-os/features/lwipstack/lwip/src/include/lwip/dhcp.h*
- 835 • *mbed-os/features/lwipstack/lwip/src/core/ipv4/lwip_dhcp.c*

836 Changes to *include/lwip/prot/dhcp.h*:

- 837 1. Add the following line below the greatest DHCP option number (67) on Line 170:

```
#define DHCP_OPTION_MUD_URL_V4 161 /*MUD: RFC-ietf-opsawg-mud-25 draft-ietf-opsawg-mud-08,
Manufacturer Usage Description*/
```

838

839 **Changes to core/ipv4/lwip_dhcp.c:**

840 1. Change within container around Line 141:

841 To `enum dhcp_option_idx` (at Line 141) before the first `#if`, add

```
DHCP_OPTION_IDX_MUD_URL_V4, /*MUD: DHCP MUD URL Option*/
```

842

843 It should now look like the screenshot below:

```
enum dhcp_option_idx {
    DHCP_OPTION_IDX_OVERLOAD = 0,
    DHCP_OPTION_IDX_MSG_TYPE,
    DHCP_OPTION_IDX_SERVER_ID,
    DHCP_OPTION_IDX_LEASE_TIME,
    DHCP_OPTION_IDX_T1,
    DHCP_OPTION_IDX_T2,
    DHCP_OPTION_IDX_SUBNET_MASK,
    DHCP_OPTION_IDX_ROUTER,
    DHCP_OPTION_IDX_MUD_URL_V4, /*MUD: DHCP MUD URL Option*/
#ifdef LWIP_DHCP_PROVIDE_DNS_SERVERS
    DHCP_OPTION_IDX_DNS_SERVER,
    DHCP_OPTION_IDX_DNS_SERVER_LAST = DHCP_OPTION_IDX_DNS_SERVER +
    LWIP_DHCP_PROVIDE_DNS_SERVERS - 1,
#endif /* LWIP_DHCP_PROVIDE_DNS_SERVERS */
#ifdef LWIP_DHCP_GET_NTP_SRV
    DHCP_OPTION_IDX_NTP_SERVER,
    DHCP_OPTION_IDX_NTP_SERVER_LAST = DHCP_OPTION_IDX_NTP_SERVER +
    LWIP_DHCP_MAX_NTP_SERVERS - 1,
#endif /* LWIP_DHCP_GET_NTP_SRV */
    DHCP_OPTION_IDX_MAX
};
```

844

845 2. Change within the function around Line 975:

846 a. To list of local variables for static `err_t dhcp_discover(struct netif *netif)`, add the
847 desired MUD URL (`www.example.com` used here):

```
char* mud_url = "https://www.example.com"; /*MUD: MUD URL*/
```

848

849 NOTE: The MUD URL must be less than 255 octets/bytes/characters long.

850 b. Within `if (result == ERR_OK)` after

```

dhcp_option(dhcp, DHCP_OPTION_PARAMETER_REQUEST_LIST,
LWIP_ARRAYSIZE(dhcp_discover_request_options));
for (i = 0; i < LWIP_ARRAYSIZE(dhcp_discover_request_options); i++) {
  dhcp_option_byte(dhcp, dhcp_discover_request_options[i]);
}

```

851

852 and before:

```
dhcp_option_trailer(dhcp);
```

853

854 add:

```

/*MUD: Begin - Add Option and URL to DISCOVER/REQUEST*/
#if (DHCP_DEBUG != LWIP_DBG_OFF)
  if (strlen(mud_url) > 255)
    LWIP_DEBUGF(DHCP_DEBUG | LWIP_DBG_TRACE, ("dhcp_discover: MUD URL is too large (>255)\n"));
#endif /* DHCP_DEBUG != LWIP_DBG_OFF */

  u8_t mud_url_len = (strlen(mud_url) < 255)? strlen(mud_url) : 255; //Ignores any URL greater than 255
  bytes/octets
  dhcp_option(dhcp, DHCP_OPTION_MUD_URL_V4, mud_url_len);
  for (i = 0; i < mud_url_len; i++) {
    dhcp_option_byte(dhcp, mud_url[i]);
  }
/*MUD: END - Add Option and URL to DISCOVER/REQUEST */

```

855

856 3. Change within the function around Line 1486:

857 Within the following function:

```

static err_t
dhcp_parse_reply(struct dhcp *dhcp, struct pbuf *p)

```

858

859 Within `switch(op)` before default, add the following case (around line 1606):

```

case(DHCP_OPTION_MUD_URL_V4): /* MUD Testing */
  LWIP_ERROR("len == 0", len == 0, return ERR_VAL);
  decode_idx = DHCP_OPTION_IDX_MUD_URL_V4;
  break;

```

860

861 4. Compile by using the following command:

```
mbed compile -m ublox_c027 -t gcc_arm
```

862

863 [2.5.3.2.2 IoT Application for Testing](#)

864 The following application was created by the NCCoE to enable the devkit to test the example
865 implementation as a MUD-capable device:

```
866 #include "mbed.h"
867 #include "EthernetInterface.h"
868
869 //DigitalOut led1(LED1);
870 PwmOut led2(LED2);
871 Serial pc(USBTX, USBRX);
872
873 float brightness = 0.0;
874
875 // Network interface
876 EthernetInterface net;
877
878 // Socket demo
879 int main() {
880     int led1 = true;
881
882     for (int i = 0; i < 4; i++) {
883
884         led2 = (led1)? 0.5 : 0.0;
885
886         led1 = !led1;
887         wait(0.5);
888     }
889
890     for (int i = 0; i < 8; i++) {
891
892         led2 = (led1)? 0.5 : 0.0;
893
```

PRELIMINARY DRAFT

```
894     led1 = !led1;
895     wait(0.25);
896 }
897
898 for (int i = 0; i < 8; i++) {
899
900     led2 = (led1)? 0.5 : 0.0;
901
902     led1 = !led1;
903     wait(0.125);
904 }
905 TCPSocket socket;
906 char sbuffer[] = "GET / HTTP/1.1\r\nHost: www.update-server.com\r\n\r\n";
907 char bbuffer[] = "GET / HTTP/1.1\r\nHost: www.unapproved-server.com\r\n\r\n";
908 int scout, bcount;
909 char rbuffer[64];
910 char brbuffer[64];
911 int rcount, brcount;
912
913 /* By default grab an IP address*/
914 // Bring up the ethernet interface
915 pc.printf("Ethernet socket example\r\n");
916 net.connect();
917 // Show the network address
918 const char *ip = net.get_ip_address();
919 pc.printf("IP address is: %s\r\n", ip ? ip : "No IP");
920 socket.open(&net);
921 /* End of default IP address */
922
923 pc.printf("Press U to turn LED1 brightness up, D to turn it down, G to get IP, R to
924 release IP, H for HTTP request, B for blocked HTTP request\r\n");
```

```
925
926 while(1) {
927     char c = pc.getc();
928     if((c == 'u') && (brightness < 0.5)) {
929         brightness += 0.01;
930         led2 = brightness;
931     }
932     if((c == 'd') && (brightness > 0.0)) {
933         brightness -= 0.01;
934         led2 = brightness;
935     }
936     if(c == 'g'){
937         // Bring up the ethernet interface
938         pc.printf("Sending DHCP Request...\r\n");
939         net.connect();
940         // Show the network address
941         const char *ip = net.get_ip_address();
942         pc.printf("IP address is: %s\r\n", ip ? ip : "No IP");
943     }
944     if(c == 'r'){
945         socket.close();
946         net.disconnect();
947         pc.printf("IP Address Released\r\n");
948     }
949     if(c == 'h'){
950
951         pc.printf("Sending HTTP Request...\r\n");
952         // Open a socket on the network interface, and create a TCP connection
953         socket.open(&net);
954         socket.connect("www.updateserver.com", 80);
```

```

955     // Send a simple http request
956     scount = socket.send(sbuffer, sizeof sbuffer);
957     pc.printf("sent %d [%.*s]\r\n", scount, strstr(sbuffer, "\r\n")-sbuffer, sbuffer);
958     // Receive a simple http response and print out the response line
959     rcount = socket.recv(rbuffer, sizeof rbuffer);
960     pc.printf("recv %d [%.*s]\r\n", rcount, strstr(rbuffer, "\r\n")-rbuffer, rbuffer);
961     socket.close();
962 }
963 if(c == 'b'){
964     pc.printf("Sending Blocked HTTP Request...\r\n");
965     // Open a socket on the network interface, and create a TCP connection
966     socket.open(&net);
967     socket.connect("www.unapprovedserver.com", 80);
968     // Send a simple http request
969     bcount = socket.send(bbuffer, sizeof bbuffer);
970     pc.printf("sent %d [%.*s]\r\n", bcount, strstr(bbuffer, "\r\n")-bbuffer, bbuffer);
971
972     // Receive a simple http response and print out the response line
973     brcount = socket.recv(brbuffer, sizeof brbuffer);
974     pc.printf("recv %d [%.*s]\r\n", brcount, strstr(brbuffer, "\r\n")-brbuffer,
975 brbuffer);
976     socket.close();
977 }
978 }
979 }

```

980 2.5.4 IoT Devices–Non-MUD Capable

981 This section details configuration of non-MUD-capable IoT devices attached to the implementation
982 network. These include several types of devices, such as cameras, smartphones, lighting, a smart
983 assistant, a printer, a baby monitor, a wireless access point, and a digital video recorder. These devices
984 did not emit a MUD URL or have MUD capabilities of any kind.

985 **2.5.4.1 Configuration Overview**

986 These non-MUD-capable IoT devices are unmodified and still retain the default manufacturer
987 configurations.

988 **2.5.4.1.1 Network Configuration**

989 These IoT devices are configured to obtain an IP address via DHCP.

990 **2.5.4.1.2 Software Configuration**

991 The software on these devices is configured according to standard manufacturer instructions.

992 **2.5.4.1.3 Hardware Configuration**

993 The hardware used in these devices is unmodified from manufacturer specifications.

994 **2.5.4.2 Setup**

995 These devices were set up according to the manufacturer instructions and connected to the Cisco switch
996 via Ethernet cable or connected wirelessly through the wireless access point.

997 **2.5.4.2.1 DHCP Client Configuration**

998 These IoT devices used the default DHCP clients provided by the original manufacturer and were not
999 modified in any way.

1000 **2.6 Update Server**

1001 This section describes how to implement a server that will act as an update server. It will attempt to
1002 access and be accessed by the IoT device, in this case one of the development kits we built in the lab.

1003 **2.6.1 Update Server Overview**

1004 The update server is an Apache web server that hosts mock software update files to be served as
1005 software updates to our IoT device devkits. When the server receives an http request, it sends the
1006 corresponding update file.

1007 **2.6.2 Configuration Overview**

1008 The following subsections document the software, hardware, and network requirements for the update
1009 server.

1010 **2.6.2.1 Network Configuration**

1011 The IP address was statically assigned.

1012 [2.6.2.2 Software Configuration](#)

1013 For this example implementation, the update server was configured on the Ubuntu 18.04 LTS operating
1014 system.

1015 [2.6.2.3 Hardware Configuration](#)

1016 The update server was hosted in the NCCoE's virtual environment, functioning as a cloud service.

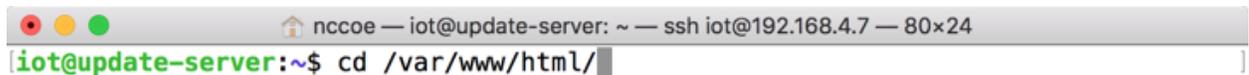
1017 [2.6.3 Setup](#)

1018 The Apache web server was set up by using the official Apache documentation at
1019 <https://httpd.apache.org/docs/current/install.html>. After this, SSL/TLS encryption was set up by using
1020 the digital certificate and key obtained from DigiCert. This was set up by using the official Apache
1021 documentation, found at https://httpd.apache.org/docs/current/ssl/ssl_howto.html.

1022 The following configurations were made to the server to host the update file:

- 1023 1. Open a terminal.
- 1024 2. Change directories to the Hypertext Markup Language (HTML) folder:

1025 `cd /var/www/html`



```

nccoe — iot@update-server: ~ — ssh iot@192.168.4.7 — 80x24
iot@update-server:~$ cd /var/www/html/

```

- 1026 3. Create the update file (Note: this is a mock update file):

1027 `touch IoTsoftwareV2.tar.gz`



```

nccoe — iot@update-server: /var/www/html — ssh iot@192.168.4.7 — 80x24
iot@update-server:/var/www/html$ touch IoTsoftwareV2.tar.gz

```

1028 [2.7 Unapproved Server](#)

1029 This section describes how to implement a server that will act as an unapproved server. It will attempt
1030 to access and to be accessed by an IoT device, in this case one of the MUD-capable devices on the
1031 implementation network.

1032 2.7.1 Unapproved Server Overview

1033 The unapproved server is an internet host that is not explicitly authorized in the MUD file to
1034 communicate with the IoT device. When the IoT device attempts to connect to this server, the router or
1035 switch should not allow this traffic because it is not an approved internet service per the corresponding
1036 MUD file. Likewise, when the server attempts to connect to the IoT device, this traffic should be denied
1037 at the router or switch.

1038 2.7.2 Configuration Overview

1039 The following subsections document the software, hardware, and network configurations for the
1040 unapproved server.

1041 2.7.2.1 Network Configuration

1042 The unapproved server hosts a web server that is accessed via TCP port 80. Any applications that
1043 request access to this server need to be able to connect on this port. Use firewall-cmd, iptables, or any
1044 other system utility for manipulating the firewall to open this port.

1045 2.7.2.2 Software Configuration

1046 For this example implementation, the CentOS 7 operating system was leveraged with an Apache web
1047 server.

1048 2.7.2.3 Hardware Configuration

1049 The unapproved server was hosted in the NCCoE's virtual environment, functioning as a cloud service.
1050 The IP address was statically assigned.

1051 2.7.3 Setup

1052 The following subsection describes the setup process for configuring the unapproved server.

1053 2.7.3.1 Apache Web Server

1054 The Apache web server was set up by using the official Apache documentation at
1055 <https://httpd.apache.org/docs/current/install.html>. SSL/TLS encryption was not used for this server.

1056 2.8 MQTT Broker Server

1057 2.8.1 MQTT Broker Server Overview

1058 For this example implementation, the open-source tool Mosquitto was used as the MQTT broker server.
1059 The server communicates publish and subscribe messages between multiple clients. For our
1060 implementation, this server provides the ability for mobile devices set up with the appropriate

1061 application to communicate with the MQTT-enabled IoT devices in the build. The messages exchanged
1062 by the devices are on and off messages, which allow the mobile device to control the LED light on the
1063 MQTT-enabled IoT device.

1064 2.8.2 Configuration Overview

1065 The following subsections document the software, hardware, and network requirements for the MQTT
1066 broker server.

1067 2.8.2.1 Network Configuration

1068 The MQTT broker server was hosted in the NCCoE's virtual environment, functioning as a cloud service.
1069 The IP address was statically assigned.

1070 The server is accessed via TCP port 1883. Any clients that require access to this server need to be able to
1071 connect on this port. Use firewall-cmd, iptables, or any other system utility for manipulating the firewall
1072 to open this port.

1073 2.8.2.2 Software Configuration

1074 For this example implementation, the MQTT broker server was configured on an Ubuntu 18.04 LTS
1075 operating system.

1076 2.8.2.3 Hardware Configuration

1077 This server was hosted in the NCCoE's virtual environment, functioning as a cloud service. The IP address
1078 was statically assigned.

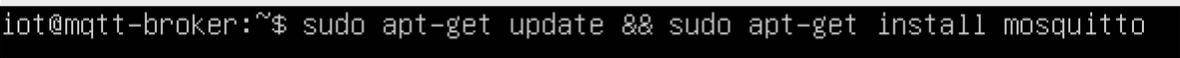
1079 2.8.3 Setup

1080 In this section we describe setting up the MQTT broker server to communicate messages to and from
1081 the controlling application and the IoT device.

1082 2.8.3.1 Mosquitto Setup

1083 1. Install the open-source MQTT broker server, Mosquitto, by entering the following command:

1084 `sudo apt-get update && sudo apt-get install mosquitto`

1085 

1086 Following the installation, this implementation leveraged the default configuration of the Mosquitto
1087 server. The MQTT broker server was set up by using the official Mosquitto documentation at
1088 <https://mosquitto.org/man/>.

1089 **2.9 ForeScout–IoT Device Discovery**

1090 This section describes how to implement ForeScout’s CounterACT appliance and Enterprise Manager to
1091 provide device discovery on the network.

1092 **2.9.1 ForeScout Overview**

1093 The CounterACT appliance discovers, catalogs, profiles, and classifies the devices that are connected to
1094 the demonstration network. When a device is added to or removed from the network, the CounterACT
1095 appliance is updated and actively monitors these devices on the network. The administrator will be able
1096 to manage multiple CounterACT appliances from a central point by integrating the CounterACT
1097 appliance with the Enterprise Manager.

1098 **2.9.2 Configuration Overview**

1099 The following subsections document the software, hardware, and network requirements for the
1100 CounterACT appliance and Enterprise Manager.

1101 **2.9.2.1 Network Configuration**

1102 The virtual CounterACT appliance was hosted on VLAN 2 of the Cisco switch. It was set up with just the
1103 monitor interface. The network configuration for the CounterACT appliance was completed by using the
1104 official ForeScout documentation at [https://www.forescout.com/wp-](https://www.forescout.com/wp-content/uploads/2018/10/CounterACT_Installation_Guide_8.0.1.pdf)
1105 [content/uploads/2018/10/CounterACT_Installation_Guide_8.0.1.pdf](https://www.forescout.com/wp-content/uploads/2018/10/CounterACT_Installation_Guide_8.0.1.pdf) (see Chapters 2 and 8).

1106 The virtual Enterprise Manager was hosted in the virtual environment that is shared across each build.

1107 **2.9.2.2 Software Configuration**

1108 The example implementation leveraged a virtual CounterACT appliance VCT-R version 8.0.1 along with a
1109 virtual Enterprise Manager VCEM-05 version 8.0.1. Both of the virtual appliances were built on a Linux
1110 operating system supported by ForeScout.

1111 ForeScout provides software for managing the appliances on the network. The CounterACT Console is
1112 software that allows management of the CounterACT appliance/Enterprise Manager and visualization of
1113 the data gathered by the appliances.

1114 **2.9.2.3 Hardware Configuration**

1115 The example implementation leveraged a virtual CounterACT appliance, which was set up in the lab
1116 environment on a dedicated machine hosting the local virtual machines in Build 1.

1117 The virtual Enterprise Manager was hosted in the NCCoE’s virtual environment with a static IP
1118 assignment.

1119 2.9.3 Setup

1120 In this section we describe setting up the virtual CounterACT appliance and the virtual Enterprise
1121 Manager.

1122 2.9.3.1 CounterACT Appliance Setup

1123 The virtual CounterACT appliance was set up by using the official ForeScout documentation at
1124 https://www.forescout.com/wp-content/uploads/2018/10/CounterACT_Installation_Guide_8.0.1.pdf
1125 (see Chapters 3 and 8).

1126 2.9.3.2 Enterprise Manager Setup

1127 The Enterprise Manager was set up by using the official ForeScout documentation at
1128 https://www.forescout.com/wp-content/uploads/2018/10/CounterACT_Installation_Guide_8.0.1.pdf
1129 (see Chapters 4 and 8).

1130 Using the Enterprise Manager, we configured the following modules:

- 1131 ▪ Endpoint
- 1132 ▪ Network
- 1133 ▪ Authentication
- 1134 ▪ Core Extension
- 1135 ▪ Device Profile Library—[https://www.forescout.com/wp-](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_Device_Profile_Library.pdf)
1136 [content/uploads/2018/04/CounterACT_Device_Profile_Library.pdf](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_Device_Profile_Library.pdf)
- 1137 ▪ IoT Posture Assessment Library—[https://www.forescout.com/wp-](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_IoT_Posture_Assessment_Library-1.pdf)
1138 [content/uploads/2018/04/CounterACT_IoT_Posture_Assessment_Library-1.pdf](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_IoT_Posture_Assessment_Library-1.pdf)
- 1139 ▪ network interface card (NIC) Vendor DB—[https://www.forescout.com/wp-](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_NIC_Vendor_DB_17.0.12.pdf)
1140 [content/uploads/2018/04/CounterACT_NIC_Vendor_DB_17.0.12.pdf](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_NIC_Vendor_DB_17.0.12.pdf)
- 1141 ▪ Windows Applications—[https://www.forescout.com/wp-](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_Windows_Applications.pdf)
1142 [content/uploads/2018/04/CounterACT_Windows_Applications.pdf](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_Windows_Applications.pdf)
- 1143 ▪ Windows Vulnerability database (DB)—[https://www.forescout.com/wp-](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_Windows_Vulnerability_DB_18.0.2.pdf)
1144 [content/uploads/2018/04/CounterACT_Windows_Vulnerability_DB_18.0.2.pdf](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_Windows_Vulnerability_DB_18.0.2.pdf)
- 1145 ▪ Open Integration Module—[https://www.forescout.com/wp-](https://www.forescout.com/wp-content/uploads/2018/08/CounterACT_Open_Integration_Module_Overview_1.1.pdf)
1146 [content/uploads/2018/08/CounterACT_Open_Integration_Module_Overview_1.1.pdf](https://www.forescout.com/wp-content/uploads/2018/08/CounterACT_Open_Integration_Module_Overview_1.1.pdf)

Appendix A List of Acronyms

2FA	Two-factor Authentication
AAA	Authentication, Authorization, and Accounting
CoA	Change of Authorization
CoAP	Constrained Application Protocol
CRADA	Cooperative Research and Development Agreement
Cybersecurity Framework	National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity
DAACL	Dynamic Access Control List
DB	Database
DDoS	Distributed Denial of Service
Devkit	Development Kit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
IOS	Cisco's Internetwork Operating System
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IT	Information Technology
ITL	NIST's Information Technology Laboratory
LAN	Local Area Network
LED	Light-Emitting Diode
LLDP	Link Layer Discovery Protocol
MAB	MAC Address Bypass
MAC	Media Access Control
MQTT	Message Queuing Telemetry Transport
MUD	Manufacturer Usage Description
NAS	Network Address Server
NAT	Network Address Translation
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OS	Operating System
PC	Personal Computer
PEP	Policy Enforcement Point

PoE	Power over Ethernet
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments (IETF Standard)
RMF	Risk Management Framework
SP	Special Publication
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TLV	Type Length Value
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
WPA2	Wi-Fi Protected Access 2 Security Certificate Protocol (Institute of Electrical and Electronics Engineers (IEEE) 802.11i-2004 standard)
WPA3	Wi-Fi Protected Access 3 Security Certificate Protocol
YANG	Yet Another Next Generation

1148

Appendix B Glossary

Audit	Independent review and examination of records and activities to assess the adequacy of system controls to ensure compliance with established policies and operational procedures (National Institute of Standards and Technology [NIST] Special Publication [SP] 800-12 Rev. 1)
Best Practice	A procedure that has been shown by research and experience to produce optimal results and that is established or proposed as a standard suitable for widespread adoption (Merriam-Webster)
Botnet	The word botnet is formed from the words robot and network. Cybercriminals use special Trojan viruses to breach the security of several users' computers, take control of each computer, and organize all the infected machines into a network of bots that the criminal can remotely manage. https://usa.kaspersky.com/resource-center/threats/botnet-attacks
Control	A measure that is modifying risk (Note: Controls include any process, policy, device, practice, or other actions that modify risk.) (NIST Interagency/Internal Report 8053)
Denial of Service	The prevention of authorized access to a system resource or the delaying of system operations and functions (NIST SP 800-82 Rev. 2)
Distributed Denial of Service (DDoS)	A denial of service technique that uses numerous hosts to perform the attack (NIST Interagency/Internal Report 7711)
Managed Devices	Personal computers, laptops, mobile devices, virtual machines, and infrastructure components require management agents, allowing information technology staff to discover, maintain, and control these devices. Those with broken or missing agents cannot be seen or managed by agent-based security products.
Mapping	Depiction of how data from one information source maps to data from another information source
Mitigate	To make less severe or painful or to cause to become less harsh or hostile (Merriam-Webster)
Manufacturer Usage Description (MUD)	A component-based architecture specified in Request for Comments (RFC) 8250 that is designed to provide a means for end devices to signal to the network what sort of access and network functionality they require to properly function

MUD-capable	An IoT device that is capable of emitting a MUD uniform resource locator (URL) in compliance with the MUD specification
Network Address Translation (NAT)	A function by which internet protocol (IP) addresses within a packet are replaced with different IP addresses. This function is most commonly performed by either routers or firewalls. It enables private IP networks that use unregistered IP addresses to connect to the internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses before packets are forwarded to another network.
Non-MUD-capable	An IoT device that is not capable of emitting a MUD URL in compliance with the MUD specification (RFC 8250)
Policy	Statements, rules, or assertions that specify the correct or expected behavior of an entity. For example, an authorization policy might specify the correct access control rules for a software component. (NIST SP 800-95 and NIST Interagency/Internal Report 7621 Rev. 1)
Policy Enforcement Point	A network device on which policy decisions are carried out or enforced
Risk	The net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. (NIST SP 800-30)
Router	A computer that is a gateway between two networks at open systems interconnection (OSI) layer 3 and that relays and directs data packets through that internetwork. The most common form of router operates on IP packets. (NIST SP 800-82 Rev. 2)
Security Control	A safeguard or countermeasure prescribed for an information system or an organization, which is designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements (NIST SP 800-53 Rev. 4)
Server	A computer or device on a network that manages network resources. Examples are file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries). (NIST SP 800-47)
Shall	A requirement that must be met unless a justification of why it cannot be met is given and accepted (NIST Interagency/Internal Report 5153)

Should	This term is used to indicate an important recommendation. Ignoring the recommendation could result in undesirable results. (NIST SP 800-108)
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat source to successfully exploit a particular information system vulnerability (Federal Information Processing Standard (FIPS) 200)
Threat Signaling	Real-time signaling of DDoS-related telemetry and threat-handling requests and data between elements concerned with DDoS attack detection, classification, traceback, and mitigation https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/cybersecurity-network-and-information-security
Traffic Filter	An entry in an access control list that is installed on the router or switch to enforce access controls on the network
Uniform Resource Locator (URL)	A reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. A typical URL could have the form http://www.example.com/index.html , which indicates a protocol (hypertext transfer protocol (http)), a host name (www.example.com), and a file name (index.html). Also sometimes referred to as a <i>web address</i>
Update	New, improved, or fixed software, which replaces older versions of the same software. For example, updating an operating system brings it up-to-date with the latest drivers, system utilities, and security software. Updates are often provided by the software publisher free of charge. https://www.computerhope.com/jargon/u/update.htm
Update Server	A server that provides patches and other software updates to Internet of Things devices.
Virtual Local Area Network (VLAN)	A broadcast domain that is partitioned and isolated within a network at the data link layer. A single physical local area network (LAN) can be logically partitioned into multiple, independent VLANs; a group of devices on one or more physical LANs can be configured to communicate within the same VLAN as if they were attached to the same physical LAN.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (NIST SP 800-37 Rev. 2)

1151 Appendix C References

- 1152 [1] “Manufacturer Usage Description Specification,” Request for Comments (RFC) 8520, Mar.
1153 2019. Available: <https://tools.ietf.org/html/rfc8520>.
- 1154 [2] Cisco’s developer MUD Manager GitHub page. Available:
1155 <https://github.com/CiscoDevNet/MUD-Manager/tree/1.0#dependencies>.
- 1156 [3] Apache HTTP Server Project documentation, Version 2.4, Compiling and installing Apache
1157 [Website], <https://httpd.apache.org/docs/current/install.html> [accessed 3/5/19].
- 1158 [4] Apache HTTP Server Project documentation, Version 2.4, Apache SSL/TLS Encryption [Website],
1159 https://httpd.apache.org/docs/current/ssl/ssl_howto.html [accessed 3/5/19].
- 1160 [5] Welcome to MUD File maker! [Website], www.mudmaker.org [accessed 3/5/19].
- 1161 [6] Advanced CertCentral™ Getting Started Guide, Version 9.2, DigiCert [Website],
1162 <https://www.digicert.com/certcentral-support/digicert-getting-started-guide.pdf> [accessed
1163 3/5/19].
- 1164 [7] SSL Certificate Support, DigiCert [Website], [https://www.digicert.com/security-certificate-
1165 support/](https://www.digicert.com/security-certificate-support/) [accessed 3/5/19].
- 1166 [8] Basic CertCentral™ Getting Started Guide, Version 1.4, DigiCert [Website],
1167 [https://www.digicert.com/certcentral-support/basic-certcentral-getting-started-guide-
1168 v1.4_2018-12-10_opt.pdf](https://www.digicert.com/certcentral-support/basic-certcentral-getting-started-guide-v1.4_2018-12-10_opt.pdf) [accessed 3/19/19].
- 1169 [9] CertCentral™ Client Certificate Guide, Version 1.9, DigiCert [Website],
1170 <https://www.digicert.com/certcentral-support/client-certificate-guide.pdf> [accessed 3/5/19].
- 1171 [10] ForeScout CounterAct® Installation Guide, Version 8.0.1, ForeScout [Website],
1172 [https://www.forescout.com/wp-
1173 content/uploads/2018/10/CounterACT_Installation_Guide_8.0.1.pdf](https://www.forescout.com/wp-content/uploads/2018/10/CounterACT_Installation_Guide_8.0.1.pdf) [accessed 3/5/19].
- 1174 [11] ForeScout CounterAct Device Profile Library Configuration Guide, Updated February 2018
1175 [Website], [https://www.forescout.com/wp-
1176 content/uploads/2018/04/CounterACT_Device_Profile_Library.pdf](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_Device_Profile_Library.pdf) [accessed 3/5/19].
- 1177 [12] ForeScout CounterAct IoT Posture Assessment Library Configuration Guide, Updated February
1178 2018 [Website], [https://www.forescout.com/wp-
1179 content/uploads/2018/04/CounterACT_IoT_Posture_Assessment_Library-1.pdf](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_IoT_Posture_Assessment_Library-1.pdf) [accessed
1180 3/5/19].

- 1181 [13] ForeScout CounterAct Open Integration Module Overview Guide, Version 1.1 [Website],_
1182 [https://www.forescout.com/wp-](https://www.forescout.com/wp-content/uploads/2018/08/CounterACT_Open_Integration_Module_Overview_1.1.pdf)
1183 [content/uploads/2018/08/CounterACT_Open_Integration_Module_Overview_1.1.pdf](https://www.forescout.com/wp-content/uploads/2018/08/CounterACT_Open_Integration_Module_Overview_1.1.pdf) [accessed
1184 3/5/19].
- 1185 [14] ForeScout CounterAct Windows Applications Configuration Guide, Updated February 2018
1186 [Website], [https://www.forescout.com/wp-](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_Windows_Applications.pdf)
1187 [content/uploads/2018/04/CounterACT_Windows_Applications.pdf](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_Windows_Applications.pdf) [accessed 3/5/19].
- 1188 [15] ForeScout CounterAct Windows Vulnerability DB Configuration Guide, Updated February 2018
1189 [Website], [https://www.forescout.com/wp-](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_Windows_Vulnerability_DB_18.0.2.pdf)
1190 [content/uploads/2018/04/CounterACT_Windows_Vulnerability_DB_18.0.2.pdf](https://www.forescout.com/wp-content/uploads/2018/04/CounterACT_Windows_Vulnerability_DB_18.0.2.pdf) [accessed
1191 3/5/19].
- 1192 [16] ForeScout HPS NIC Vendor DB Configuration Guide, Version 1.2.4 [Website],
1193 https://www.forescout.com/wp-content/uploads/2018/04/HPS_NIC_Vendor_DB_1.2.4.pdf
1194 [accessed 3/5/19].