National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SECURE INTER-DOMAIN ROUTING

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenges surrounding the safe exchange of internet traffic through collaborative efforts with industry and the information technology (IT) community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide Special Publication 1800-14, *Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation*, and includes background, challenges, goals, and potential benefits. As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this Practice Guide, or would like to schedule a demonstration, please email sidr-nccoe@nist.gov.

BACKGROUND

If information traveling on the internet is rerouted due to either a malicious or accidental act, traffic will: 1) take inefficient paths through the internet, 2) arrive at malicious sites masquerading as legitimate destinations, or 3) never arrive at its intended destination. The consequences of malicious or accidental rerouting are the potential for financial losses, fraud, and erosion of trust, and a strong possibility that future events will repeat with the same results.

This project uses commercially available technologies to demonstrate a cybersecurity reference design that uses security protocols to protect the integrity of internet routing functions that use Border Gateway Protocol (BGP).

BGP has been the default routing protocol for traffic flowing through the internet between autonomous systems. Due to the absence of built-in security controls with BGP, traffic may either divert to malicious sites masquerading as legitimate destinations or not arrive at all.

CHALLENGE

Although commercial implementation of the BGP origin validation technology is available to ensure the safe delivery of internet traffic, to date, the adoption rate in the United States has been slow. Instead, many organizations are relying on preexisting legacy systems to move traffic. The reasons for not adopting resource public key Infrastructure (RPKI)-based BGP route origin validation (ROV) technology are varied, but associated costs, staff time, and lack of familiarity are factors, coupled with some usability and technical questions.

GOALS

The goal of this project is to demonstrate how implementing technology using BGP ROV and RPKI can deliver internet traffic safely to its intended destination.

This project resulted in a publicly available NIST cybersecurity practice guide containing detailed, practical steps to implement a cybersecurity reference design that addresses the secure inter-domain routing challenge.

BENEFITS

If widely implemented, the adoption of BGP security technologies would:

- improve the security and stability of the global internet by allowing network operators to verify the validity of BGP advertisements
- strengthen the security and stability of traffic flowing across the global internet—benefitting all organizations and individuals that use and rely on it.

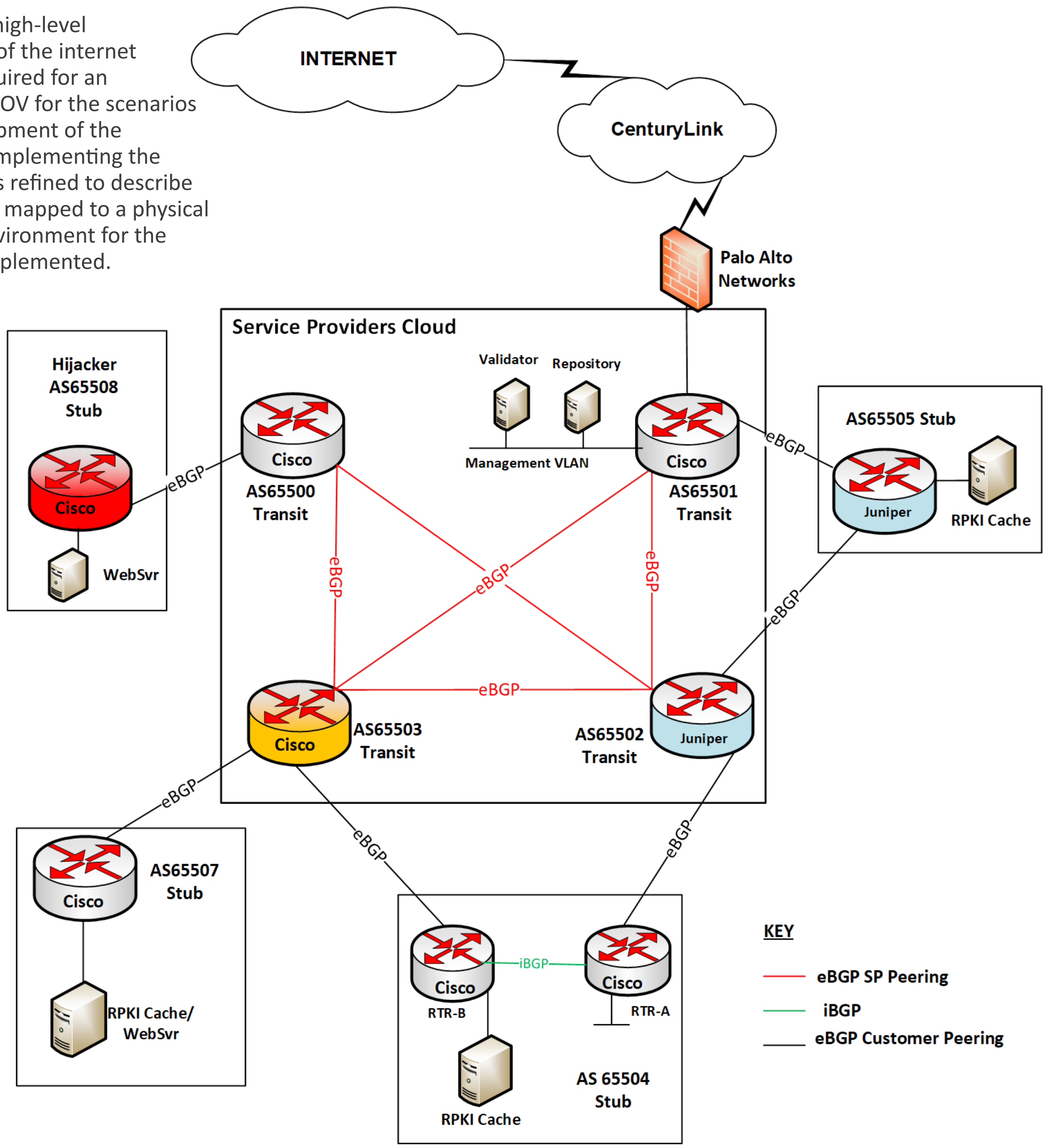
The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. 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 ABOUT NCCOE
Visit https://www.nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE

This diagram identifies a high-level architecture of the areas of the internet technologies that are required for an organization to perform ROV for the scenarios above. During the development of the laboratory environment implementing the use case, the diagram was refined to describe detailed components and mapped to a physical architecture in the lab environment for the specific scenario being implemented.



TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project include:

AT&T CenturyLink CISCO COMCAST JUNIPer NETWORKS paloalto NETWORKS THE GEORGE WASHINGTON UNIVERSITY WASHINGTON, DC

Certain commercial entities, equipment, products, or materials may be identified 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.

DOWNLOAD THE PRACTICE GUIDE

For more information about this project, visit: https://nccoe.nist.gov/projects/building-blocks/secure-inter-domain-routing.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have questions about this project or would like to join the Secure Inter-Domain Routing Community of Interest, please send an email to sidr-nccoe@nist.gov.

February 2019