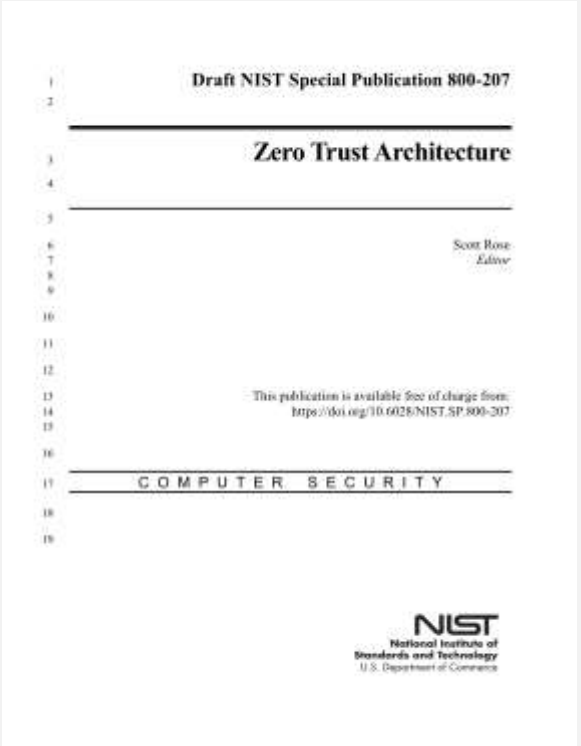
NIST SP 800-207 Draft Status Update

Scott Rose, NIST
scott.rose@nist.gov
11/13/2019

NIST SP 800-207 Zero Trust Architecture

- Released for public comment September 23, 2019
  - https://csrc.nist.gov/News/2019/zero-trust-architecture-draft-sp-800-207
- Comment period ends Nov 22, 2019
  - Comment submission address goes to NIST project team

- **Goal**: to provide a technology neutral conceptual framework for developing zero trust architectures and strategies for enterprises
  - No direct guidance for creating or operating an enterprise ZTA strategy


Draft NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Editor

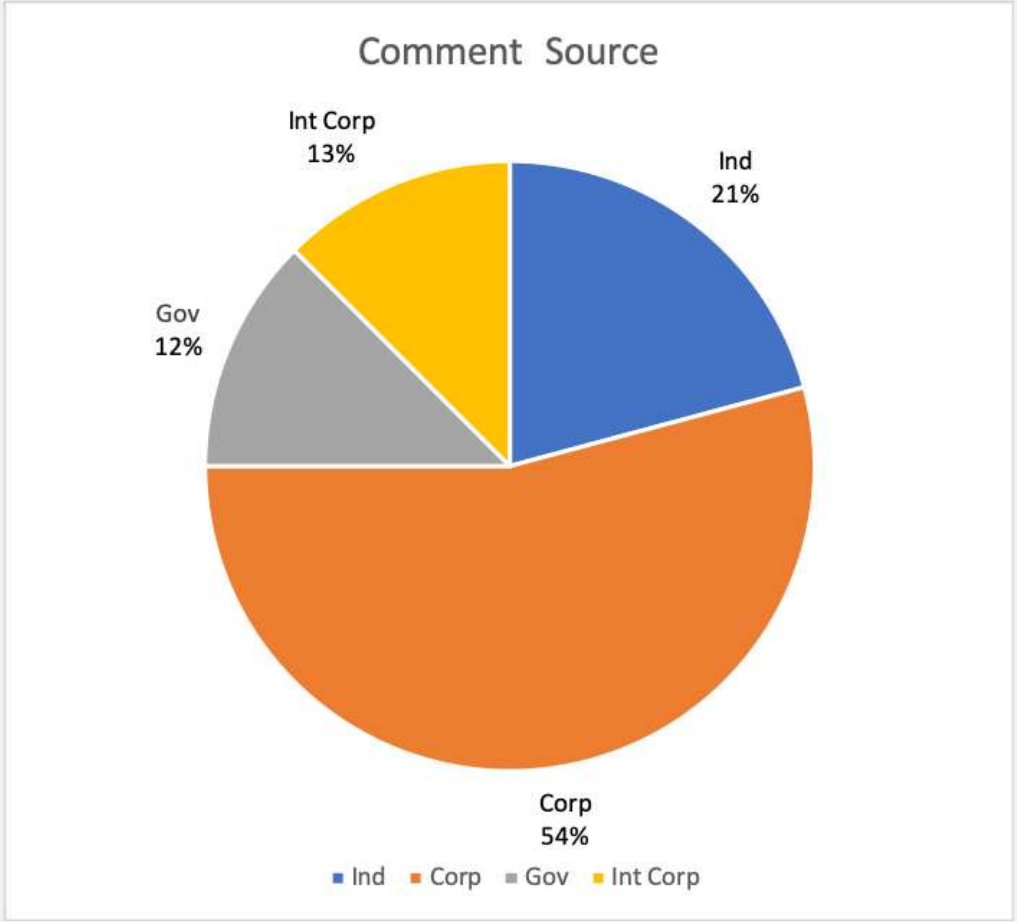
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

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

Received Comments Summary

- Received from individuals, companies, and members of US government.
  - US based and International
  - Expecting most comments to come in during last week of period
- Overall positive and mostly substantive comments
  - Many included text or wording suggestions



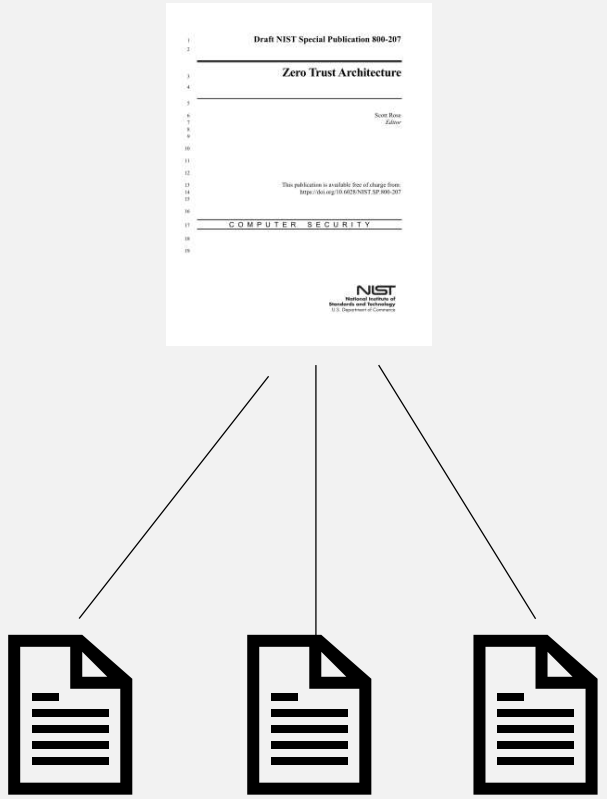
New Material Ideas?

- Approaches to ZTA
  - Enhanced Identity – access privileges tied to ID, network open otherwise.
  - Microsegmentation using Next-Gen Firewalls (NGFW)
  - Network segmentation/SDN/network overlay approach

- Would call for another public comment period
  - Acceptable?
  - Estimate close of 2nd public comment period Jan/Feb, final publication March/April

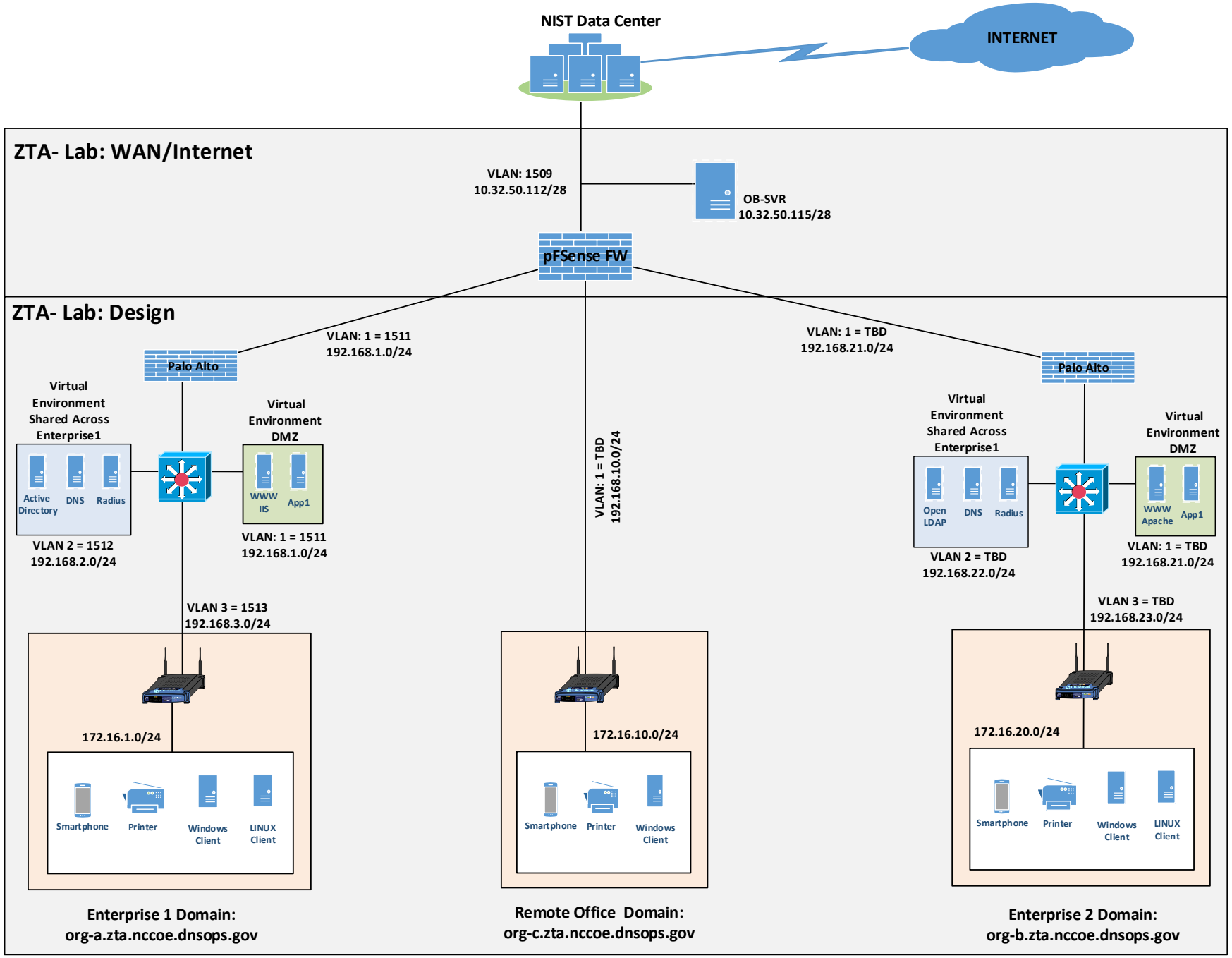
Next Steps Using the Publication

- Use Special Publication in test lab
  - Using use cases from SP to produce test scenarios
  - May produce more material for gap analysis (Appendix A)
- Deeper dive documents
  - Focus on one aspect covered in the SP
  - SP 800-207 could become foundation for several follow on papers.



Zero Trust Gap Analysis

- We invited 17 vendors for technical demos
- Three main areas of gaps identified by vendor survey
  1. Procurement and existing security strategies
     - No current language for procurement and misconception that ZTA conflicts with current security posture
  2. Vendor lock-in / interoperability
     - Too much reliance on vendor APIs and possible need for minimal standardization of technologies through standards bodies such as IETF or others
  3. Evolving threat models and changes business processes caused by ZTA
     - Security compromises and user experience


NIST Data Center
INTERNET
ZTA- Lab: WAN/Internet
VLAN: 1509
10.32.50.112/28
OB-SVR
10.32.50.115/28
pFSense FW
ZTA- Lab: Design
VLAN: 1 = 1511
192.168.1.0/24
VLAN: 1 = TBD
192.168.21.0/24
Palo Alto
Palo Alto
Virtual Environment Shared Across Enterprise1
Active Directory
DNS
Radius
VLAN 2 = 1512
192.168.2.0/24
Virtual Environment DMZ
WWW IIS
App1
VLAN: 1 = 1511
192.168.1.0/24
VLAN: 1 = TBD
192.168.10.0/24
Virtual Environment Shared Across Enterprise1
Open LDAP
DNS
Radius
VLAN 2 = TBD
192.168.22.0/24
Virtual Environment DMZ
WWW Apache
App1
VLAN: 1 = TBD
192.168.21.0/24
VLAN 3 = 1513
192.168.3.0/24
VLAN 3 = TBD
192.168.23.0/24
172.16.1.0/24
172.16.10.0/24
172.16.20.0/24
Smartphone
Printer
Windows Client
LINUX Client
Smartphone
Printer
Windows Client
Smartphone
Printer
Windows Client
LINUX Client
Enterprise 1 Domain:
org-a.zta.nccoe.dnsops.gov
Remote Office Domain:
org-c.zta.nccoe.dnsops.gov
Enterprise 2 Domain:
org-b.zta.nccoe.dnsops.gov

Questions & Feedback