

Cisco TrustSec for PCI Scope Reduction—Verizon Assessment and Validation



CONTENTS

Overview	3
Legacy Segmentation Challenges	3
TrustSec Security Group Tagging	3
Benefits of Segmentation with TrustSec	4
Verizon Validation Overview	4
Use Case 1—PCI Scope Reduction with Security Group Tags (Wired Network)	5
Description	5
Use Case 2—PCI Scope Reduction with Security Group Tags (Wireless Network)	6
Description	6
Use Case 3—PCI Scope Reduction with Security Group Tags (Across Networks)	7
Description	7
Verizon Validation Summary	9
Cisco Components to Support TrustSec	12
For More Information	14

Overview

Cisco TrustSec Security Group Tagging (SGT) technology dramatically simplifies PCI compliance. Cisco's innovation transforms segmentation and offers a more intuitive business-level approach on how it is designed, enforced, and managed. The Qualified Security Assessors and Penetration Testers at Verizon have performed an assessment of Cisco Security Group Tagging within Cisco's laboratories; Verizon has validated that Cisco Security Group Tagging can be used to reduce the scope for PCI and simplify the management of segmentation.

Legacy Segmentation Challenges

Network segmentation isolates particular groups of users and computers into logical segments on a network to allow security enforcement points to permit or deny traffic between those groups. Traditionally, this discrete separation uses access controls based on network addressing, VLANs, and firewalls. Companies are then able to apply controls on how traffic flows are permitted between these groups to meet compliance targets. The benefit is that the network area separated from the PCI environment is no longer within the scope of PCI compliance, reducing the cost of managing and sustaining compliance across an environment.

Unfortunately, this method of segmentation can be difficult and time-consuming to manage:

- For some industries such as healthcare and retail, the activity of implementing a separate PCI network from their current "flat" network can be a daunting task because of the scale and complexity of their organizations, and its associated cost.
- Access control lists and firewall rules based on IP addresses tend to grow and become hard to audit as more applications are introduced.
- Management of the segmentation policies is manual, with the risk of rules being misconfigured; each branch office needs to be identified individually because each site has its own addressing scheme, making policy management for those branch offices tedious and sometimes difficult.

TrustSec Security Group Tagging

Organizations frequently have simple business goals that they want their security architecture to facilitate; for example, they may want only traders to access trading systems, or only doctors to access patient records. However, when these policies are implemented, they traditionally need to be translated into network security rules that define users and servers by their IP addresses, subnet, or site. The



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright 2014 Cisco Systems, Inc. All rights reserved

resulting rules are no longer simple to understand and may not clearly correlate with the original business goals. They also do not account for user, device, or server roles, leading to some complexity in how protected assets are classified, and are at risk of misconfiguration.

Cisco TrustSec simplifies the provisioning and management of secure access to network services and applications. Compared to access control mechanisms based on network topology, Cisco TrustSec defines policies using logical policy groupings, so that secure access is consistently maintained even as resources are moved. De-coupling access policy from IP addresses and VLANs simplifies security policy maintenance tasks, lowers operational costs, and allows common access policies to be applied to wired, wireless, and VPN access consistently.

Benefits of Segmentation with TrustSec

Security Group Tagging transforms segmentation by simplifying administration:

- Security group tags allow organizations to segment their networks without having to redesign to accommodate more VLANs and subnets.
- Firewall rules are dramatically streamlined by using an intuitive business-level profile method.
- Policy enforcement is automated, assisting compliance and increasing security efficacy.
- Security auditing becomes much easier, as Qualified Security Assessors can more easily validate that rules are being enforced to meet compliance.

Verizon Validation Overview

Verizon QSA assessors were invited into Cisco’s laboratories to evaluate the effectiveness of TrustSec Security Group Tagging for the purposes of reducing PCI scope. Verizon performed and observed a series of tests, including network penetration testing for evaluating network segmentation. Based on assessment and observations, Verizon concludes that TrustSec Security Group Tagging meets the intent of segmentation, as required by the Payment Card Industry Data Security Standard (PCI DSS), for purposes of PCI scope reduction and restricting access to cardholder data, above and beyond that required by PCI DSS requirements.



Note

It is important to note that all three use cases described subsequently use the same policy, demonstrating how easily segmentation can be consistently managed.

Figure 1 shows the Cisco TrustSec policy.

Figure 1 Cisco TrustSec Policy

		Destination	
		PCI Devices	Non-PCI Devices
Source	PCI Devices	Permit	DENY
	Non-PCI Devices	DENY	Permit

347915

The following three use cases were used for testing the efficacy of TrustSec security group tags for PCI scope reduction.

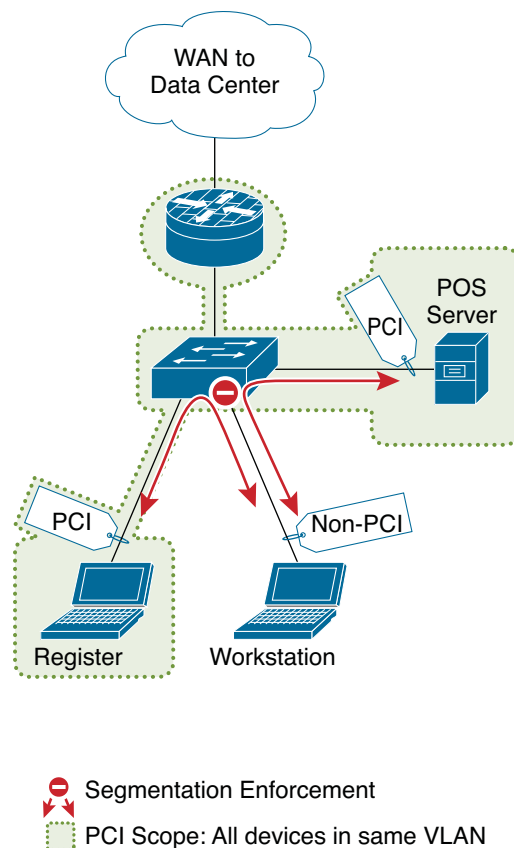
Use Case 1—PCI Scope Reduction with Security Group Tags (Wired Network)

Description

- All devices are connected to the same subnet (VLAN 10).
- The POS register and the POS server are classified into “PCI” security groups and are assigned the relevant security group tags.
- The workstation has no security group tag assigned.
- The register can communicate with the server and the data center but no communication can be established with the workstation.
- The workstation can communicate to the data center but communication is denied with the register or POS server.

Figure 2 shows a diagram of Use Case 1.

Figure 2 Use Case 1—PCI Scope Reduction with Security Group Tags (Wired Network)



347912

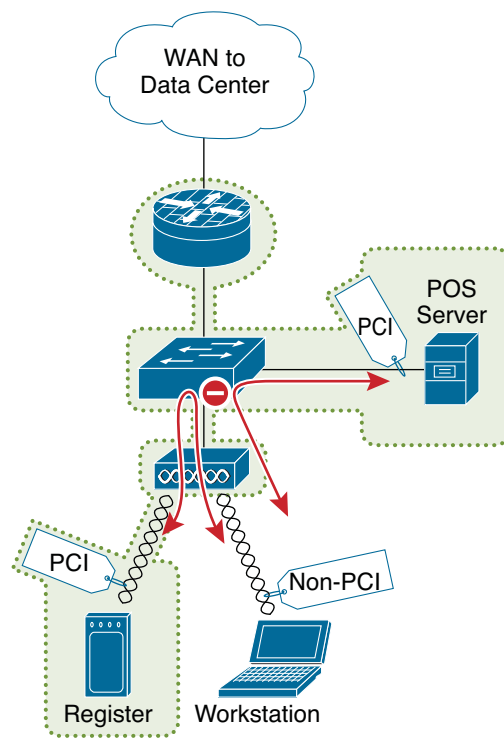
Use Case 2—PCI Scope Reduction with Security Group Tags (Wireless Network)



Description

- All devices are connected to the same subnet (VLAN 10).
- All wireless devices are associated to the same SSID.
- The mobile register and server are classified in “PCI” security groups and assigned relevant security group tags.
- The mobile workstation has no security group tag.
- The mobile register can communicate with the server and the data center.
- The workstation can communicate to the data center but not to the register or the server.

Figure 3 shows a diagram of Use Case 2.

Figure 3 Use Case 2—PCI Scope Reduction with Security Group Tags (Wireless Network)



 Segmentation Enforcement
 PCI Scope: All devices in same VLAN and SSID

347913

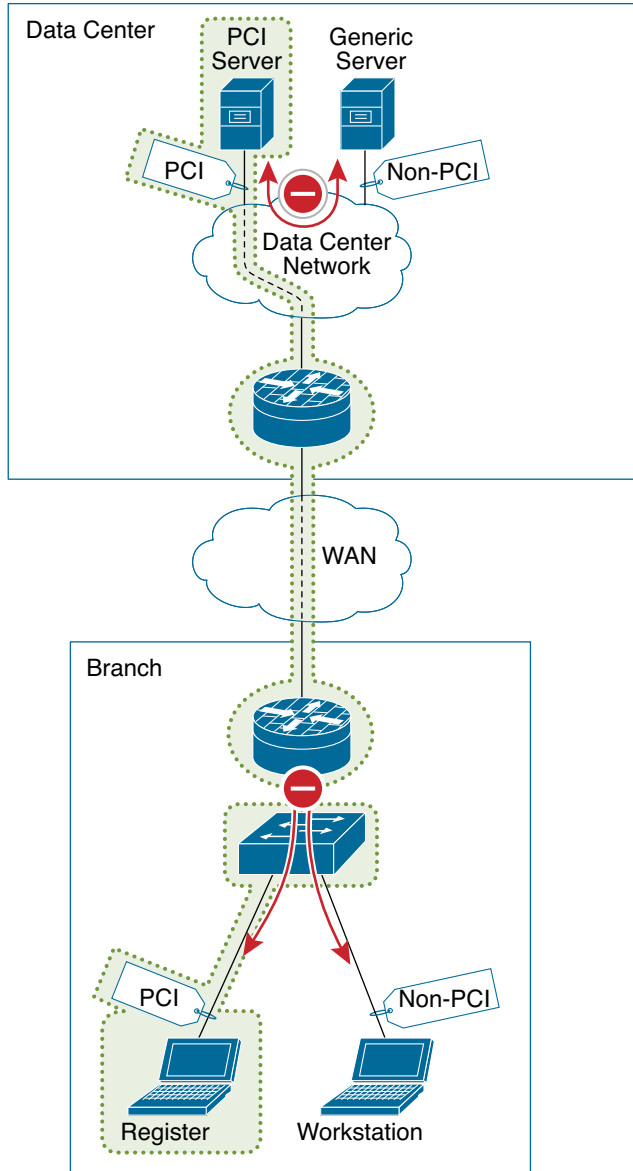
Use Case 3—PCI Scope Reduction with Security Group Tags (Across Networks)



Description

- This use case demonstrates effective segmentation across networks.
- The register in the branch and the PCI server in the data center are both assigned “PCI” security group tags.
- The workstation in the branch and the non-PCI server in the data center do not use security group tags.
- Classification information (security group tags and associated device information) are shared between branch office and data center
- The register and the PCI server can communicate to each other but not to the workstation or the non-PCI server.
- The workstation and the non-PCI server can communicate to each other but not to the register or the PCI server.

[Figure 4](#) shows a diagram of Use Case 3.

Figure 4 Use Case 3—PCI Scope Reduction with Security Group Tags (Across Networks)



-  Segmentation Enforcement
-  PCI Scope: Segmentation Across Company

347914

Verizon Validation Summary



Validation Summary

Regarding the network segmentation testing performed by Verizon on the Cisco TrustSec solution.

prepared for
Cisco Systems, Inc.



www.verizon.com

Verizon Enterprise Solutions
22001 Loudoun County Parkway
Ashburn, VA 20147
Phone: +1.866.507.5004
Fax: +1.703.886.0622

©Verizon 2013. All Rights Reserved.



Cisco TrustSec Validation / Testing Summary

Cisco Systems, Inc engaged Verizon to performed PCI validation and Penetration Testing to assess the effectiveness of Cisco's TrustSec solution, for purposes of Payment Card Industry (PCI) scope reduction (via network segmentation). The validation and testing consisted of two distinct phases, as follows:

PCI Validation:

Verizon performed an assessment of the segmentation capabilities of the Security Group Tagging technology. A Verizon Qualified Security Assessor (QSA) performed the following validation through several conference calls and WebEx sessions, from Sept 13, 2013 through November 6, 2013:

- Reviewed supporting architecture components (documentation and on console) - Cisco Identity Services Engine (authentication / authorization policies, profiling configuration, and Security Group Access policies), Cisco IOS configurations (router, switch, ASA), and ASDM policies.
- Observed online attempts and captured log output (ASDM Realtime Log Viewer) for ingress and egress access attempts, originating from untrusted and trusted sources
- Network-based penetration testing to test access controls for ingress and egress traffic to validate effectiveness of TrustSec to block unwanted traffic and allow trusted traffic (see detailed testing under Use Case #1 - #3)
- Observed Wireshark (pcap) packet captures for ingress and egress access attempts, originating from untrusted and trusted sources

Penetration Testing:

Verizon performed a PCI Internal Network Penetration Test that consisted of testing the Cisco TrustSec solution in a lab environment. The Penetration Test was performed, in addition to PCI-QSA validation, by an independent Threat & Vulnerability practice, within Verizon's Professional Services organization. The Penetration Testing was conducted from November 18, 2013 to November 21, 2013 in a Cisco lab environment. The scenarios undertaken during the PCI Internal Network Penetration Test were:

- Perform Internal Penetration Test: Verizon was given connectivity to a lab environment where network segmentation was implemented via TrustSec. Cisco also provided Verizon with details and documentation of the lab environment. The Verizon consultants then sought to bypass the network segmentation controls.

Verizon conducted network segmentation testing from three perspectives:

- A VLAN specific to PCI hosts
- A VLAN specific to non-PCI hosts
- A mixed VLAN consisting of PCI and non-PCI hosts

Verizon Opinion and Recommendations

Based on the results of the PCI validation and PCI Internal Network Penetration and Segmentation Test, it is Verizon's opinion that Cisco TrustSec can successfully perform network segmentation, for purposes of PCI scope reduction. In order to ensure effective enforcement across the environment in which TrustSec is deployed, it is important to note that proper configuration of the supporting infrastructure and TrustSec policies is essential.



Verizon Disclaimer: The services performed by Verizon were intended to assess and describe the current state at the time of assessment. Verizon makes this document available for informational purposes only. It may not reflect the most current legal developments, and Verizon does not represent, warrant or guarantee that it is complete, accurate or up-to-date nor does Verizon offer any certification or guarantee with respect to the opinions expressed herein. Changing circumstances may change the accuracy of the content herein. The information contained herein is not intended to constitute legal advice nor should it be used as a substitute for specific legal advice from a licensed attorney. This report makes no representations or warranties of any kind regarding the security of Cisco services or its products, or forward-looking statements regarding the effects of future events. You should not act (or refrain from acting) based upon information herein without obtaining professional advice regarding your particular facts and circumstances.

Reproduction guidelines: You may use this document in accordance with the provisions related to Ownership and Intellectual Property in the Master Service Agreement. If you quote or reference this document, you must appropriately attribute the contents and authorship to Verizon. Verizon and the Verizon logo are trademarks or registered trademarks, in the United States and certain other countries, of Verizon, Inc. Additional company and product names may be trademarks or registered trademarks of the individual companies and are respectfully acknowledged.

Cisco Components to Support TrustSec

Table 1 lists the Cisco components that have TrustSec capabilities.

Table 1 Cisco Components with TrustSec Capabilities

Type	Platform	Function	Version
Policy server	Cisco ISE 3315, 3395, 3415, 3495, and VMware	Policy server for TrustSec classification and policy creation/provisioning	Version 1.2 Patch 1
Campus switches	Cisco Catalyst 2960-S, 2960-X/XR	Classification, propagation (SXP only)	IOS 15.0(2)SE or IOS 15.0(2)EX4
	Cisco Catalyst 3560-E&C/3750-E	Classification, propagation (SXP only)	IOS 15.0(2)SE5
	Cisco Catalyst 3560-X/3750-X	Classification, propagation (SXP, inline SGT), enforcement (SG-ACL)	IOS15.2(1)E
	Cisco Catalyst 3650/3850	Classification, propagation (SXP, inline SGT), enforcement (SG-ACL)	IOS-XE 3.3.0SE
	Cisco Catalyst 4500 Sup7-E/7L-E	Classification, propagation (SXP, inline SGT), enforcement (SG-ACL)	IOS-XE 3.4.2SG
	Cisco Catalyst 4500 Sup6-E /6L-E	Classification, propagation (SXP only)	IOS 15.2(1)E
	Cisco Catalyst 6500 Sup2T	Classification, propagation (SXP, inline SGT), enforcement (SG-ACL)	IOS 15.1(2)SY
	Cisco Catalyst 6500 Sup720/Sup32	Classification, propagation (SXP only)	12.2(33)SXJ6
Data center switches	Cisco Nexus 5500/Nexus 2000	Classification (port, port profile), propagation (inline SGT), enforcement (SG-ACL)	NX-OS 5.1(3)N2(1c)
	Cisco Nexus 7000/Nexus 2000	Classification, propagation (SXP, inline SGT), enforcement (SG-ACL)	NX-OS 6.2(2)
	Cisco Nexus 1000v for VMware ESXi	Classification (port profile), propagation (SXP only)	NX-OS 4.2(1)SV2(1.1)

Table 1 Cisco Components with TrustSec Capabilities (continued)

Routers	Cisco ISRG2 C800, C1900, C2900, C3900	Classification (static IP-SGT), propagation (SXPv4), enforcement (zone-based SG firewall)	IOS 15.4(1)T
	Cisco ISR 4451X	Classification (static IP-SGT), propagation (SXPv4), enforcement (zone-based SG firewall)	IOS-XE 3.11S
	Cisco ASR1000	Classification (static IP-SGT), propagation (SXPv4, SGT over GETVPN), enforcement (zone-based SG firewall)	IOS-XE 3.11S
Wireless	Cisco WLC 5500, 2500, WiSM2, WLCM2	Classification, propagation (SXP only)	AireOS 7.4
	Cisco WLC 5760	Classification, propagation (SXP, inline SGT), enforcement (SG-ACL)	IOS-XE 3.3.0SE
Firewall	Cisco ASA5500	Propagation (SXP only), enforcement (SG firewall)	Version 9.1
Cisco Connected Grid devices	Cisco CGR2010	Classification (static IP-SGT), transport (SXPv4), enforcement (zone-based SG firewall)	IOS 15.3(2)T
Management	Cisco Security Manager	ASA SG-FW management	CSM4.4

For More Information

- For more Cisco PCI compliance information, see the following URL: www.cisco.com/go/pci.
- For more Cisco TrustSec information, see the following URL: www.cisco.com/go/trustsec.