CISCO VALIDATED PROFILE

Data Center Switching Secure Data Center Using Cisco TrustSec Solution

April 2017

Table of Contents

Profile Introduction 1

- Simplified Security Engineering 1
- Reduced Risk 1
- Reduced Operational Cost 1
- Improved Regulatory Compliance 1
- Consistent and Effective Network Segmentation 1
- Improved Agility and Scalability 2

Network Profile 3

- Topology Diagram 3
- Hardware Profile 4
- Features and Scale 6

Use-Case Scenarios 8

- Test Methodology 8
- Use Cases 8

Profile Introduction

This document focuses on the deployment of a Cisco TrustSec Solution (CTS) in an enterprise network. TrustSec assigns a security group tag (SGT) to the user's or device's traffic at ingress (inbound into the network) and then enforces the access policy based on the tag elsewhere in the infrastructure (for example, in the data center). The CTS in an enterprise/data center simplifies the provisioning and management of network access control through the use of software-defined segmentation to classify network traffic and enforce policies for more flexible access controls.

With CTS, traffic classification is based on endpoint identity, not IP address, enabling policy change without network redesign. A centralized policy management platform gathers advanced contextual data about who and what are accessing your network, uses SGTs to define roles and access rights, and then pushes the associated policy to your TrustSec-enabled network devices, such as switches, routers, and security equipment. This provides better visibility through richer contextual information and allows an organization to be better able to detect threats and accelerate remediation, reducing the impact and costs associated with a potential breach.

SIMPLIFIED SECURITY ENGINEERING

With Software-Defined Segmentation, Cisco TrustSec technology simplifies the provisioning of network access, accelerates security operations, and consistently enforces policy anywhere in the network by using the SGT to define the roles and access rights that push associated policies to TrustSec-enabled network devices.

REDUCED RISK

TrustSec reduces risk and allows segmentation to be introduced gracefully. It helps to limit the impact of data breaches and prevent the lateral movement of threats and compromised devices.

REDUCED OPERATIONAL COST

TrustSec reduces operational costs, with the cost avoidance of an alternative traditional perimeter-based security solution; reduces additional IT operations headcount required; and improves network resilience, with a lower risk of downtime. TrustSec reduces administrative costs for access management, particularly when considering the administration effort required for more traditional solutions, such as VLANs and firewalls. Also, TrustSec reduces the need for costly network re-architecture by automating access rules and access control list (ACL) administration.

IMPROVED REGULATORY COMPLIANCE

CTS helps you easily comply with PCI audits and other compliance requirements using network segmentation.

CONSISTENT AND EFFECTIVE NETWORK SEGMENTATION

CTS defines role-based access using security group tags to segment the network and consistently enforce policies across the Cisco TrustSec-enabled network devices with the use of Cisco Identity Services Engine, a central policy management platform.

IMPROVED AGILITY AND SCALABILITY

Through Identity Services Engine, TrustSec uses ingress tagging and egress filtering to enforce access control policy in a scalable manner.

The following table summarizes key areas on which this profile focuses.

Table 1 *CTS profile summary*

Deployment areas	Features
Security	SGACL policies downloaded from ISE and MACsec
Network services	Controlled access
Mobility	Through ISE, nodes can download policies on the fly
High availability	SSO
Network planning and troubleshooting	NetFlow Wireshark SGACL counter stats SGACL monitoring/logging
Efficient network management	WebUI (for ISE)
Performance and scalability	Scalable policies in ISE matrix

Network Profile

Based on research, customer feedback, and configuration samples, this profile is designed with a deployment topology that is generic and can easily be modified to fit any specific deployment scenario. Both the Fabric Path and the Classical Ethernet-based profiles are covered for the TrustSec deployment. For both the profiles, positioning the platforms, the scale numbers, feature interoperability, and the use cases are covered in the upcoming sections.

TOPOLOGY DIAGRAM

Figures 1 and 2 show the three-tiered design that was used for the validation of this profile.

The topology represents a typical campus deployment with Cisco Catalyst 6500 and Cisco ASR 1000 in the core layer. Based on the size of the campus, its geographical location, and user-scale, there might be more distribution switches connecting to the core layer. Nexus7K devices are positioned in the aggregation level and N5K/N6K at the access layer, with Fex boxes facing the hosts.

Figure 1 *Fabric path profile: topology overview*

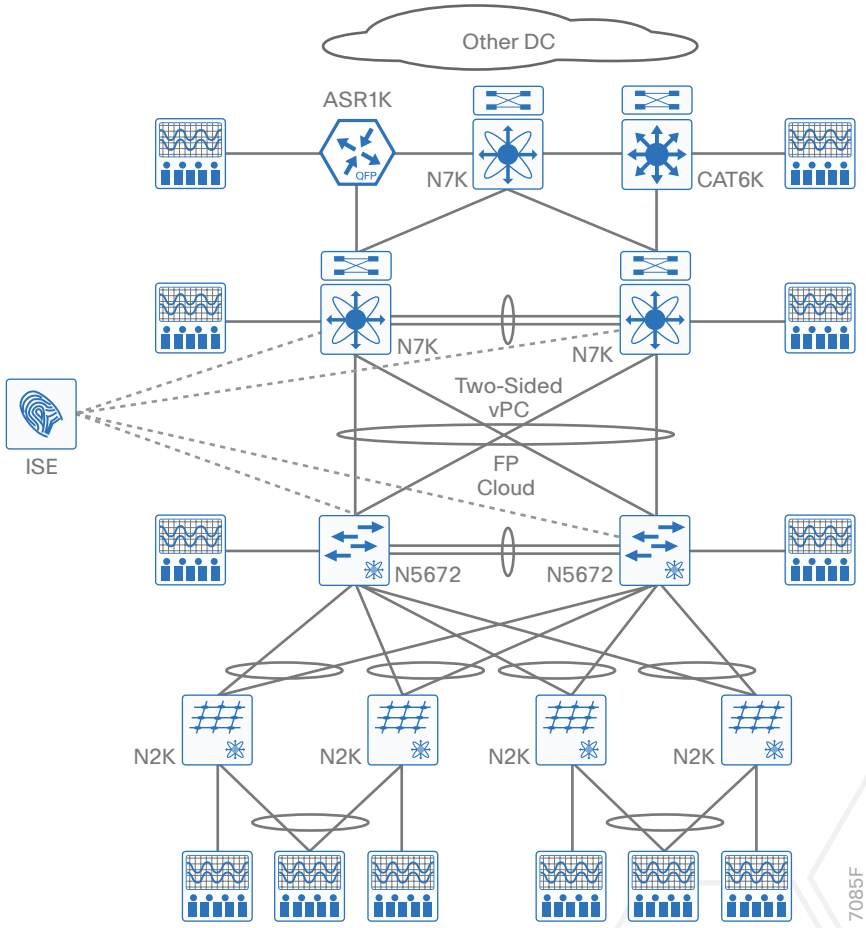
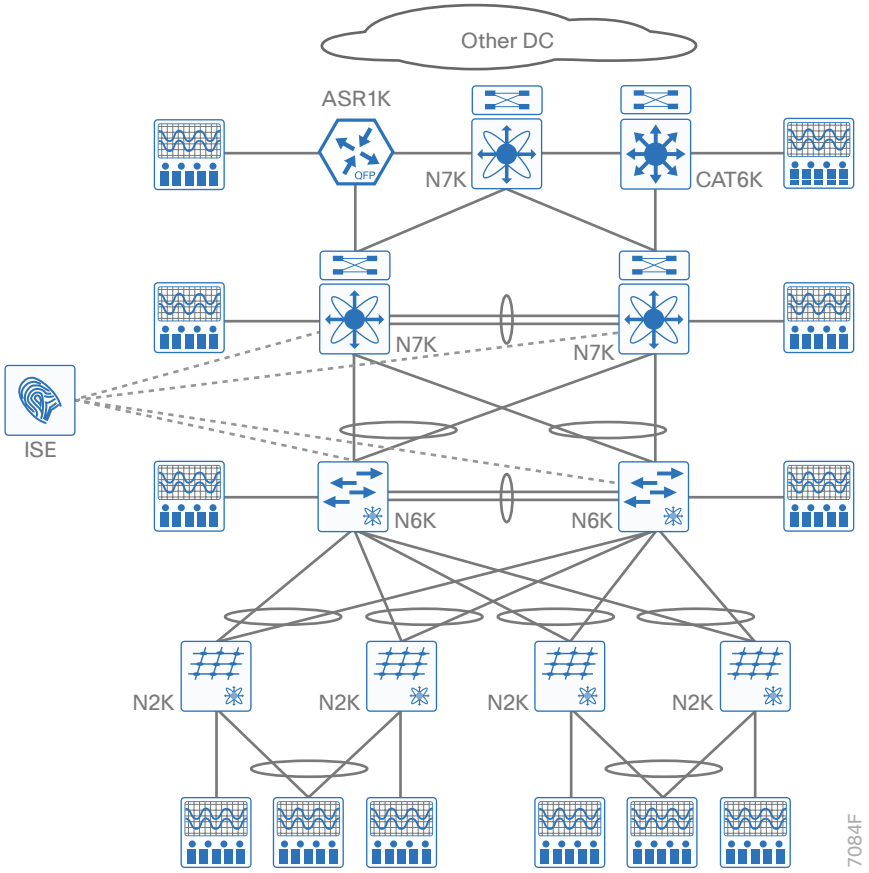


Figure 2 *Classical Ethernet profile: topology overview*



HARDWARE PROFILE

Table 2 defines the set of relevant hardware, servers, test equipment, and endpoints that are used to complete the end-to-end profile deployment.

This list of hardware, along with the relevant software versions and the role of these devices, complement the actual physical topology defined in Figures 1 and 2.

Table 2 Hardware profile of servers and endpoints

VM and HW	Software versions	Hardware versions	Description
Nexus 7K	8.0.1	Chassis: N7000, N7700 Supervisor: N7K-SUP2, N77-SUP2E I/O module: N77-F248XP-23E N77-F348XP-23 N77-F324FQ-25 N77-F312CK-26 N77-M348XP-32L N7K-M348XP-25L N77-M312CQ-26L N7K-F248XP-25E N7K-F248XT-25E N7K-M224XP-23L N7K-F312FQ-25	Aggregation deployment (DUT) and MACsec interop
Nexus 5K/6K with Fexes	7.3.1	Supervisor: N5K-C5672UP-16G-SUP I/O module: N5600-72UP16GFC N5600-72UP16GFC-FC N5600-72UP16GFC-M6Q Fabric extender: N2K-C2248PQ-10GE N2K-C2232PP-10GE N2K-C2348UPQ-10GE	Access deployment (DUT)
ISE	2.1, 2.2	ESXi 5.5	For authentication, authorization
Cat6K, ASR1K	15.2	WS-X6904-40G (in 10G mode) ASR1006	As core device
UCS Server	ESXi 5.x	–	To manage and host the virtual machines
Ixia	–	–	Generate traffic streams

FEATURES AND SCALE

This section contains the description of the features covered in Classical Ethernet and Fabric Path base profile deployments, along with CTS coverage in both the areas. The relevant scale numbers for different line cards at which the features are deployed across the physical topology are also captured. Table 3 lists the scale for each respective profile.

Table 3 *CE deployment base profile*

Feature	N7K scale	N5K/6K scale
VLAN	1000	400
Unicast routes	200K	3K
HSRP	800	200
SNMP	SXP MIB walks	n/a
DHCP	8K	8K
Clients	8K	8K
UDLD	Enabled	Enabled
BFD	Enabled	Enabled
LACP	Enabled	Enabled
LLDP	Enabled	Enabled
AAA	Enabled	Enabled
Radius	Enabled	Enabled

Table 4 *FP deployment base profile*

Feature	N7K scale	N5K/6K scale
VLAN	1000	400
Unicast routes	200K	3K
Anycast HSRP	5	5
HSRP	800	200
SNMP	SXP MIB walks	n/a
DHCP	8K	8K
Clients	8K	8K
UDLD	Enabled	Enabled
AAA	Enabled	Enabled
Radius	Enabled	Enabled

Table 5 *CTS feature scale*

Feature	N7K scale	N5K/6K scale
IP-SGTs on M2, M3	200K	n/a
IP-SGTs on F2E	32K	n/a
IP-SGTs on F3	64K	n/a
SXP learnt IP-SGT mappings	200K	2K (speaker)
SGT groups	3K SGT/DGT	n/a
SGACL	3K	2K
CFS sync learnt/VLAN entries	800	n/a
SNMP	SXP MIB walks	n/a

Use-Case Scenarios

TEST METHODOLOGY

The use cases listed in Table 6 will be executed using the topology defined in Figures 1 and 2, along with the test environment already explained.

With respect to the longevity for this profile setup, the CPU and memory usage would be monitored overnight, including weekends, along with mem-check leaks. In order to test robustness, certain negative events would be triggered during the use-case testing.

USE CASES

Table 6 describes the use cases that were executed on the CTS profile. The test coverage is divided into buckets of customer use-case scenarios, as listed below.

The customer use case is composed of system upgrade/bring-up, operational triggers/config changes, steady state/usability, network events/link flaps, and resiliency/error recovery.

Table 6 *List of use-case scenarios*

No.	Focus area	Use cases
System upgrade/bring-up		
1	System upgrade	Network administrator should be able to perform upgrade and downgrade between releases seamlessly, per the support seen in upgraded or downgraded release. Software upgrade can be performed in a non-disruptive manner on the Nexus 7000/7700, if redundant Supervisor is present. This procedure is called In-Service Software Upgrade (ISSU). The upgrade will be non-disruptive for connected endpoints. For more information, see the Cisco Nexus 7000 Series Software Upgrade and Downgrade Guide. Software upgrade through system reload: ▪ Software upgrade can be performed in a disruptive manner on the Nexus 7000/7700, if the network is built with switch-level redundancy or a short network outage is not of concern (maintenance window). The procedure requires the kickstart- and system-image to be copied into the bootflash, followed by changing the boot variable and a reload of the switch. Graceful insertion and removal: ▪ Nexus 7000/7700 devices can be isolated from the network using system maintenance mode to minimize data traffic impact during system upgrade. After the device is isolated, software can be upgraded using system reload method described above. Software maintenance upgrade (SMU): ▪ Software can be patched for fixing known defects using SMU. Please see the SMU guide in CCO.

Table 6 continued

2	Feature additions	Network admin enables TrustSec features to enable the secure tagging in the retail branch through Port SGT, IP-SGT, VLAN-SGT (using DAI), SXP learnt SGT (bidirectional as well), Subnet SGT, default-route SGT, Cached SGT, per port enforcement and CFS-learned SGT in CE and FP, as applicable. System supports manual and dot1x modes of authentication, encryption and encapsulation through the modelists: gcm-encrypt, gcm-encrypt-256, gmac, no-encap, and null modes with the combination of SGT propagation, as applicable. Support of hashing algorithm HMAC-MD5 and HMAC-SHA-1.
3	Platform additions and interoperability	Addition of Nexus platforms with existing network topology should be possible. Interop with other platforms like Cat6k/ASR1K/ISE as applicable.
4	Reload	All of the configuration should be migrated seamlessly during the reload operation.
5	Traffic forwarding	No loss of permitted traffic across the network topology, if "Permit" policies are configured. In case of "Deny," no traffic should be permitted.
Operational triggers/configuration changes		
6	CTS configuration changes and modifications	Configuration change—adding/deleting/appending/prepending ACEs/CoA and issuing rekey. Change of inline SGT. Support of policy refreshment triggered through CLI and through ISE refresh. Validation of SGACL state changes between Enabled/Monitored/Disabled for CoA/refresh. Support of device SGT changes from ISE for CoA/refresh. System supports adding/deleting/editing IP-SGT bindings. Validation of SGACL priority between CLI configured and ISE. Verify policy caching for ISE connectivity loss.
7	Plug-n-play (topology changes)	Controlling the access through ISE downloaded policies with ingress tagging and egress filtering to enforce access control policy for the nodes located anywhere in the cloud.
8	SNMP polling	SNMP walk for SXP mib objects.
Steady state/usability		
9	Soak	System stability with enabled policies while providing highly flexible operational access management. CTS counters and show CLIs for the matched policies.

Table 6 continued

10	Traffic filtering	Filtering with enforced RBACL to prevent any unauthorized access to the network. Filtering of unknown SGT assignments. Per port enforcement on a trusted port, bypassing all the rules.
11	SGT propagation	Support for propagation of SGT across the CTS cloud
12	Securely exchanging the tags	System support of SGT Exchange Protocol (SXP) to carry the IP-SGT tags from one node to the other Loop-detection/prevention in IPv4 networks. SXP enabled nodes: N7k, N5K/6K (speaker), ISE, Cat6k, ASR1K.
Network events/link flaps		
13	Link flaps	Verify that the system holds good and recovers to working condition after the following events are triggered. ▪ Link flaps, SVI flaps ▪ Clear Counters, Clear ARP, Clear Routes ▪ Deleting VRF/VLAN/SVI & adding them back.
14	Client troubleshooting	Network admin should be able to troubleshoot client connectivity issue.
15	Logging	Use of acllogs used for TrustSec RBACLs with enabled detailed logging.
16	Monitoring	Verification of denied traffic, by enabling monitor-mode, thereby allowing the flow to get recorded.
17	Power off/on	TrustSec ability to resume traffic filtering post outage. If ISE connectivity is lost, then with policy caching, the downloaded policies will be cached and accordingly traffic will be filtered.
18	Reload due to crash	Feature stability after system goes for a reload with unexpected crash.
19	Traffic-based triggers	Validation of different traffic flows/size and streams with Ixia.
Resiliency/error recovery		
20	Negative scenarios	Ensuring MACsec link not coming up with mismatched parameters. Verification of SXP link not coming up with mismatched password/mode/timer values.
21	Triggers during ISSU	System support for process reload, rekeying during ISSU for no traffic loss.
22	Recovery from error state	Network troubleshooting and debugging for IT admins. ▪ Monitor & troubleshoot end-end deployment via topologies ▪ Monitor network for alarms, syslogs and traps Troubleshoot network performance using traffic flow monitoring.
23	SSO	Perform system switchover and ensure all the functionalities hold good.

Please use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.