White Paper

Cisco Catalyst 6500 Series with Supervisor Engine 2T: Enabling Cisco TrustSec with Investment Protection

What You Will Learn

This paper describes two new operating modes designed for the Cisco® Catalyst® 6500 Series with Supervisor Engine 2T enabling a Cisco TrustSec® network. The two new operating modes provide investment protection for the wiring closet and the aggregation layer deployments using a mix of different generation line cards.

A basic understanding of the Cisco TrustSec solution is assumed for this paper. Additional information about Cisco TrustSec is available from the http://www.Cisco.com website.

Overview

Cisco TrustSec helps secure access to your networks and networked resources through policy-based access control, identity-aware networking, and data integrity and confidentiality services. Cisco TrustSec also allows you to improve compliance, strengthen security, and increase operational efficiency. As your network expands and adds devices, applications, and users, Cisco TrustSec solutions deliver identity-based business services and applications to anyone, anywhere, any time with confidence, consistency, and efficiency. Cisco and our partners offer smart, personalized professional services to prepare your network to deploy a Cisco TrustSec solution by providing policy review, analysis, and design expertise. Using leading practices, these services help you more quickly and cost-effectively deploy a full authentication and access solution while also providing knowledge transfer for ongoing operational efficiency.

The Cisco Catalyst 6500 with Supervisor Engine 2T and 6900 Series line cards provide complete hardware and software support for implementing a Cisco TrustSec network. Table 1 lists the primary Cisco TrustSec related features available for the first time on the Cisco Catalyst 6500 with the Supervisor Engine 2T and 6900 Series line cards.

Table 1. Cisco TrustSec Features Available in Supervisor Engine 2T and 6900 Series Line Cards

TrustSec Feature	Supervisor Engine 2T 6900 Series Line Cards	Supervisor Engine 720-Based Systems
Policy-Based SGACL Enforcement	Yes	No
IEEE 802.1AE Media Access Control (MAC) Security	Yes	No
Cisco TrustSec Layer 3 Transport Forwarding	Yes	No
Cisco TrustSec Security Group Tag Exchange Protocol (SXP)	Yes	Yes
Network Device Admission Control (NDAC)	Yes	Yes

When a Cisco Catalyst 6500 is configured with the Supervisor Engine 2T and 6900 Series line cards, the system is fully capable without any restrictions of providing Cisco TrustSec services. The forwarding performance of the system with Cisco TrustSec enabled, with or without Security Group Tagging (SGT) imposition, is consistent with a system without any Cisco TrustSec configuration.

Line-Card Compatibility with Supervisor Engine 2T and Cisco TrustSec

The Cisco Catalyst 6500 has traditionally been positioned end to end in enterprise networks, including the wiring closet, WAN edge, data center, and medium to large enterprise distribution and core environments.

Many customers desire to continue using their existing Cisco Catalyst 6500 switches and line cards while migrating to a Cisco TrustSec network using the Supervisor Engine 2T. For this reason Cisco has developed the Supervisor Engine 2T to be compatible with certain existing line cards when deployed in a Cisco TrustSec network.

In order to support new Cisco TrustSec functionality such as SGT and IEEE 802.1AE MACsec link encryption at wire-speed rates, dedicated application-specific integrated circuits (ASICs) are used on the new Supervisor Engine 2T and the new 6900 Series line cards. This functionality also requires changes to the internal forwarding decision processes. Therefore, providing compatibility with existing line cards requires the use of two new operating modes designed just for maintaining compatibility with the existing or previous generation line cards. Before going into the details on how the Cisco Catalyst 6500 provides investment protection in a Cisco TrustSec network deployment, we should start with some definitions that describe line cards and their different levels of Cisco TrustSec support.

With respect to Ethernet LAN line cards, the Supervisor Engine 2T supports the following:

- All WS-X6148 series line cards
- All 6700 Series line cards equipped with a centralized forwarding card (CFC)
- All WS-X6700 series line cards equipped with a distributed forwarding card version 4 (DFC4) (note that a WS-X6800 series line card is essentially a 6700 line card with a DFC4)
- All WS-X6900 series modules

We can describe the Cisco Catalyst 6500 line-card support for Supervisor Engine 2T and Cisco TrustSec using the descriptions in Table 2.

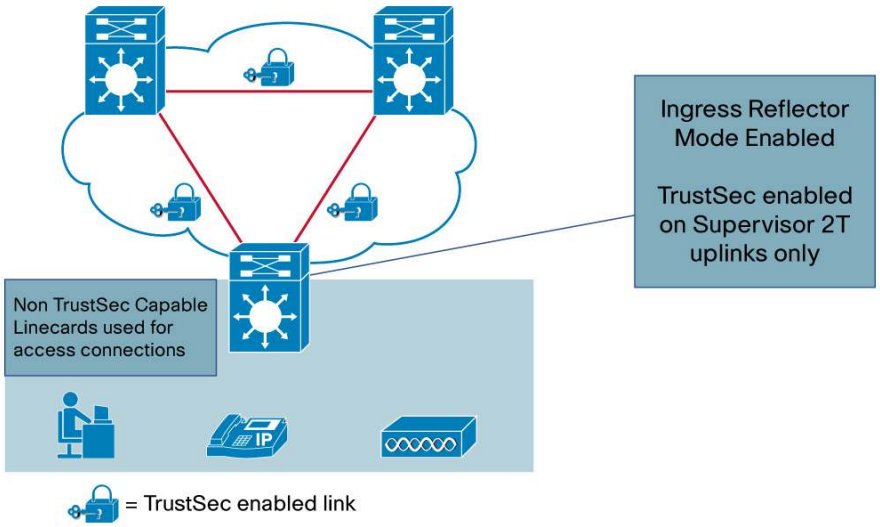
Table 2. Cisco Catalyst 6500 Line-Card Support Levels for Cisco TrustSec

Cisco TrustSec Support Level	Description	Line Card
Cisco TrustSec Capable	Supports full Cisco TrustSec capabilities with hardware acceleration for Security Group Tag imposition and IEEE 802.1AE MACsec	Supervisor Engine 2T, and all 6900 Series line cards
Cisco TrustSec Aware	Does not support Security Group Tag imposition or IEEE 802.1AE MACsec; however, these line cards are capable of understanding forwarding decisions, which include the Security Group Tag information. This allows them to forward traffic to a Cisco TrustSec capable line card for egress.	WS-X6816-10G-4C/XL WS-X6816-10T-4C/XL
Not Capable of Using Cisco TrustSec	Does not support Security Group Tag imposition or IEEE 802.1AE MACsec; also does not interpret forwarding decisions with Security Group Tag information.	WS-X6724-SFP WS-X6748-SFP WS-X6748-GE-TX WS-X6704-10G WS-X6824-SFP WS-X6848-SFP WS-X6848-GETX WS-X6148 series (all)

Ingress Reflector Mode

Ingress reflector mode provides compatibility between line cards not capable of using Cisco TrustSec and the Supervisor Engine 2T uplinks with Cisco TrustSec enabled. The intention is for wiring closet or access layer deployments. With ingress reflector mode only centralized forwarding is supported, meaning all packet forwarding (lookup decisions) will occur on the Supervisor Engine 2T PFC. Only 6148 Series or fabric-enabled CFC line cards such as the 6748-GE-TX line cards are supported. Line cards with a DFC or any 10 Gigabit Ethernet line cards are not supported when ingress reflector mode is enabled. Nonsupported line cards will not power up with ingress reflector mode configured. (See Figure 1)

Figure 1. Ingress Reflector Mode Use Case



Ingress reflector mode is enabled using a global configuration command and requires a system reload.

Figure 2 shows the CLI required. Be sure to save the running configuration to the startup configuration before performing the system reload.

Figure 2. Example CLI Enabling Ingress Reflector Mode

```
6513E.SUP2T.SA.2(config)#platform cts ?
  egress    Platform Hardware CTS egress
  ingress   Platform Hardware CTS ingress

6513E.SUP2T.SA.2(config)#platform cts ingress
CTS Ingress reflector will be active only on next system reboot.
Please reboot the system for CTS Ingress reflector to be active.

6513E.SUP2T.SA.2(config)#
```

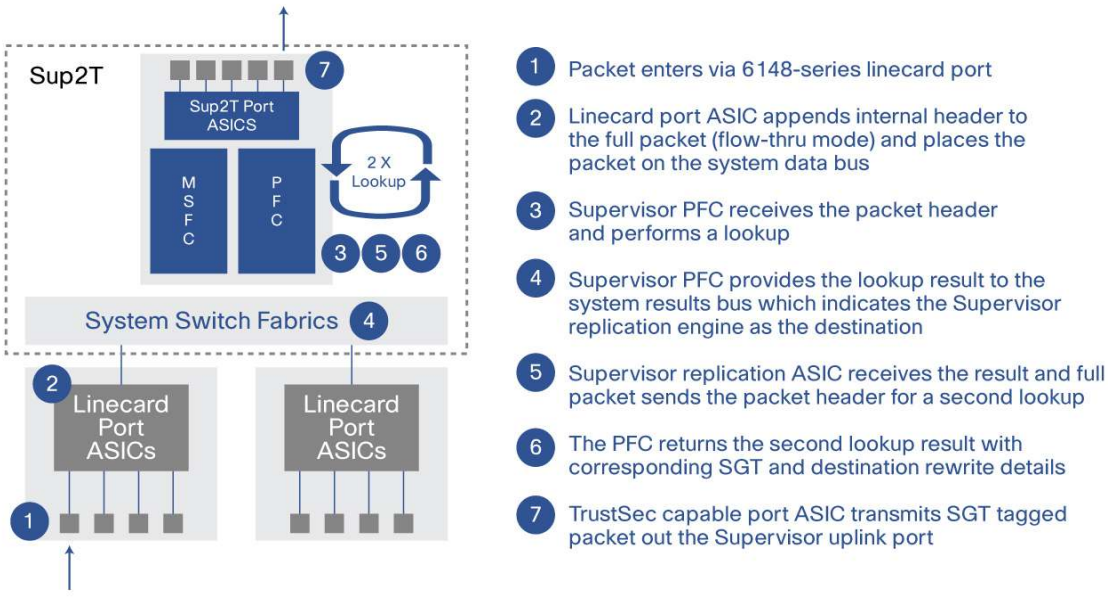
As stated earlier, ingress reflector mode is intended to provide compatibility with line cards built on the classic bus[1] and CEF 720 architecture[2]. The challenge in this case is that these line cards do not have the necessary hardware capable of understanding forwarding results provided with a source SGT. Therefore, when enabling ingress reflector mode, the system uses the packet replication ASIC built into the Supervisor Engine 2T PFC to reflect (replicate) packets for an additional forwarding lookup cycle. The second forwarding result will then be processed by the replication ASIC, which is capable of processing results with SGT information.

Ingress Reflector Mode Operation

While providing compatibility with the most commonly installed access layer line cards is the main benefit, it is also important to understand the performance and restrictions incurred when using ingress reflector mode. To help understand how ingress reflector mode works, Figure 3 provides a high-level packet walk example.

In this example a packet enters the system using the line-card port in step 1, and the line-card port ASIC appends an internal system header to the entire packet and places the packet on the shared system bus for packet forwarding. The PFC in this case provides a forwarding decision directing the packet to the replication ASIC on the supervisor engine. The replication ASIC then initiates a second forwarding decision by sending the packet headers to PFC. Note that this is the second cycle through the PFC forwarding process for this specific frame. With this forwarding decision the SGT tag information as well as any associated packet rewrite information needed will be derived. The replication ASIC in this case is able to process the lookup decision, which includes the SGT tag information, and forward the packet using the supervisor engine uplinks. It should also be noted that traffic statistics are not updated for the first pass through the PFC; statistics are only updated for the second and final pass through the PFC.

Figure 3. Ingress Reflector Mode Packet Forwarding Example



[1] Classic bus line cards are line cards that use the 32-Gbps shared bus switch fabric; the 6148 Series line cards are the only classic bus series line cards supported with the Supervisor Engine 2T.
[2] CEF 720 line cards are line cards that use the cross-fabric switch fabric for intramodule traffic and use the classic bus for centralized forwarding decisions. The line cards do not have distributed forwarding daughter card installed.

The additional forwarding decision cycle does reduce overall system performance, but the forwarding process remains fully hardware accelerated. For systems with 6148 Series line cards, the aggregate forwarding performance will be roughly 7.5 mpps. For systems with all fabric-enabled line cards such as the 6700 Series, performance is approximately 24 mpps.

Table 3 provides a summary of the various traffic direction possibilities and the associated maximum forwarding performance.

Table 3. Ingress Reflector Mode Performance

Traffic Direction	Maximum Throughput	Example
From 6100 Series line card not capable of using Cisco TrustSec to Supervisor Engine 2T uplinks	15 mpps	WS-X6148-GETX to Supervisor Engine 2T uplink
From 6100 Series line card not capable of using Cisco TrustSec to other line card not capable of using Cisco TrustSec	7.5 mpps	WS-X6148GETX to WS-X6148-GETX
From 6100 Series line card not capable of using Cisco TrustSec to WS-X6908	7.5 mpps	WS-X6148GETX to WS-X6908-10G
From 6700 Series or 6800 Series line card not capable of using Cisco TrustSec to Supervisor Engine 2T uplink	24 mpps (systemwide centralized forwarding using CFC)	WS-X6748-SFP to Supervisor Engine 2T uplink (CFC) WS-X6848-SFP to Supervisor Engine 2T uplink (DFC)
From 6700 Series or 6800 Series line card not capable of using Cisco TrustSec to other line card not capable of using Cisco TrustSec	7.5 - 15 mpps to WS-X6148 series 24 mpps (systemwide centralized forwarding using CFC) 24 mpps per line card (using DFC4)	WS-X6748 to WS-X6148-GETX WS-X6748 to WS-X6748 (CFC)
From 6700 Series or 6800 Series line card not capable of using Cisco TrustSec to WS-X6908	24 mpps (systemwide centralized forwarding using CFC)	WS-X6748 to WS-X6908 (CFC)
From Cisco TrustSec aware DFC4 line card to Supervisor Engine 2T uplinks	48 mpps per line card	WS-X6716 to Supervisor Engine 2T uplink
From 6900 Series to 6900 Series	60 mpps	WS-X6908 to WS-X6908

Ingress reflector mode summary:

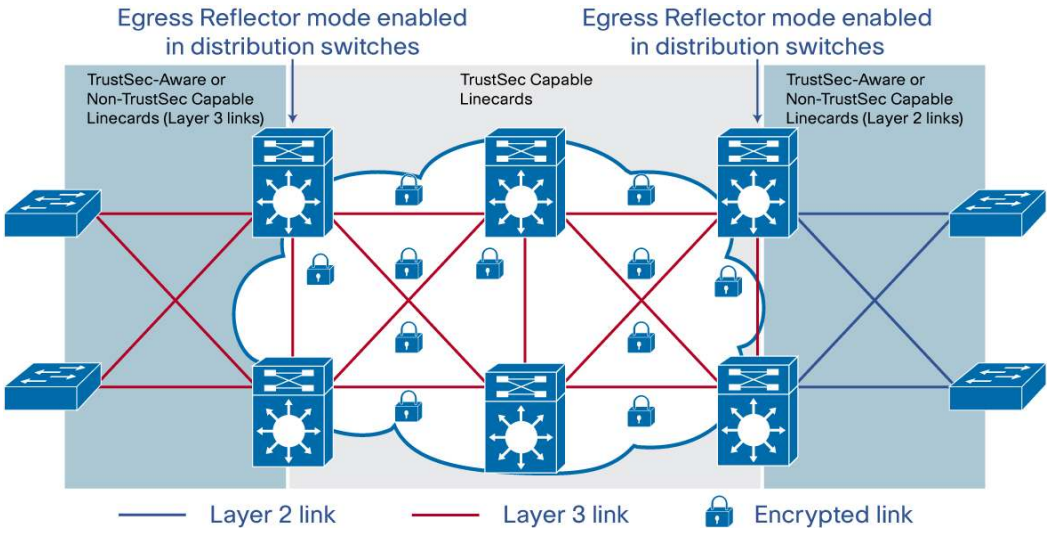
- Intended for wiring closet or access layer deployments
- Provides backward compatibility with 6148 Series and 6700 Series line cardsCisco TrustSec SGT tag propagation enabled only on Supervisor Engine 2T uplink ports (both active and standby uplink supported) or WS-X6908-10G ports
- DFC daughter cards are only supported on the WS-X6908-10G and WS-6816-10G linecards[3] Aggregate forwarding performance in flow-through switching mode is 7.5 mpps (classic line cards)
- Aggregate forwarding performance in compact switching mode is 24 mpps (6700 Series line cards)
- Service modules are not supported with ingress reflector mode

Egress Reflector Mode

Egress reflector mode is a system-level operating mode that allows Cisco TrustSec to be enabled on the Supervisor Engine 2T and 6900 Series line cards while providing backward compatibility with existing line cards. The intention is for aggregation points of the network such as in the distribution layer. With egress reflector mode customers can upgrade a supervisor engine module and DFCs and continue to use their existing line cards. (See Figure 4)

[3] WS-X6816-10G linecard is essentially a WS-X6716-10GE line card with a DFC4 installed.

Figure 4. Egress Reflection Mode Use Case



Egress Reflector Mode Operation

Egress reflector mode provides compatibility with legacy line cards by using the forwarding engines built-in packet replication ASICs to initiate a second packet forwarding decision. This second forwarding decision is used to derive the Cisco TrustSec SGT information.

Egress reflector mode is enabled using a global configuration command and requires a system reload.

Figure 5 shows the CLI required. Be sure to save the running configuration to the startup configuration before performing the system reload.

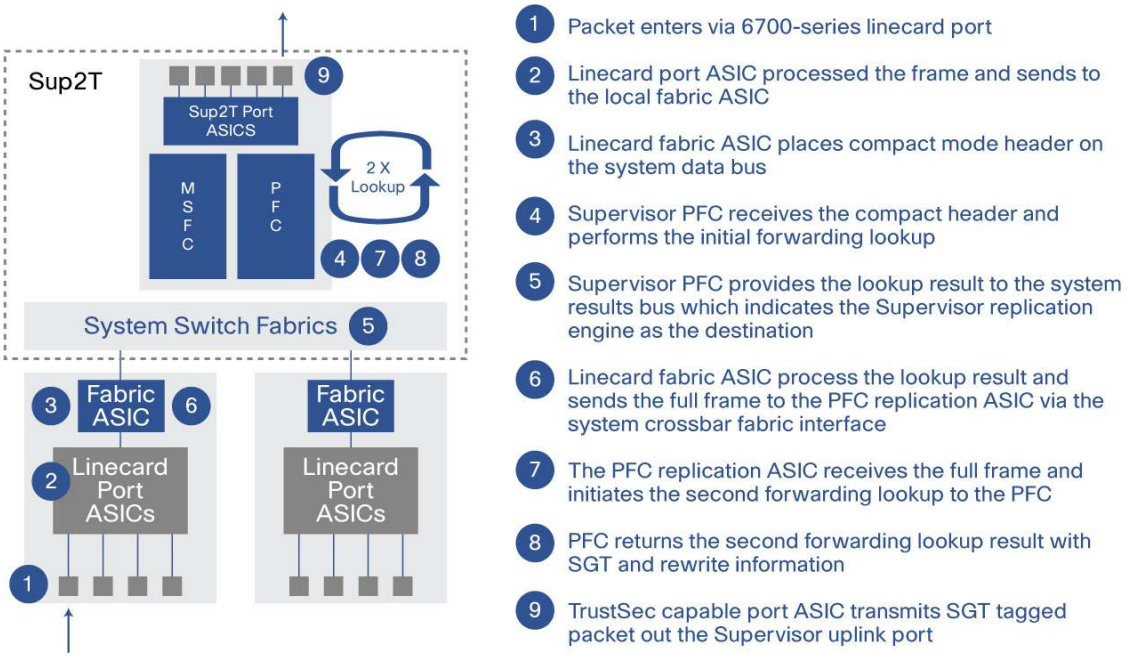
Figure 5. Example CLI Enabling Egress Reflector Mode

```
6513E.SUP2T.SA.2(config)#platform cts ?
  egress   Platform Hardware CTS egress
  ingress  Platform Hardware CTS ingress

6513E.SUP2T.SA.2(config)#platform cts egress
CTS Egress reflector will be active only on next system reboot.
Please reboot the system for CTS Egress reflector to be active.

6513E.SUP2T.SA.2(config)#
```

To help understand how egress reflector mode works, Figure 5 provides a high-level review of a packet forwarding process between a line card not capable of using Cisco TrustSec to the Supervisor Engine 2T uplink port. Even though this example shows the egress interface as an interface of the Supervisor Engine 2T, the egress interface could also be any routed interface on a 6900 Series line card as well. If the egress interface is on a 6900 Series line card, then the replication ASIC on the egress line card is used to reflect the frame instead of the supervisor engine PFC.

In the first step a packet enters the switch through a port on the 6700 Series line card. The line card uses its local port and fabric ASICs to perform the typical Layer 2 and Layer 3 forwarding process. Because egress replication mode is configured, the resulting PFC forwarding lookup decision indicates the destination index for the replication ASIC on the supervisor engine PFC. The line-card fabric then sends the entire frame to the PFC replication ASIC using the cross-bar switch fabric interface. The PFC replication then reflects (replicates) the frame and initiates a second forwarding lookup decision. The result from this second lookup decision will include the SGT information as well as the packet rewrite information. Next the PFC replication engine will forward the entire frame out the supervisor engine uplink port with the appropriate SGT. It should also be noted that traffic statistics are not updated for the first pass through the PFC; statistics are only updated for the second and final pass through the PFC. (See Figure 6.)

Figure 6. Egress Reflection Mode Packet Forwarding Example



The main benefit of egress reflector mode is providing compatibility with previous generation line cards. There are a few restrictions, including the requirement that SGT propagation can only be enabled on L3 routed ports. Cisco TrustSec aware line cards and line cards not capable of using Cisco TrustSec are supported in the system as downlinks using either Layer 2 or Layer 3. The downlink interfaces can still be used in a software-based Cisco TrustSec configuration, for example, when configured to implement network device admission control.

Table 4 provides a summary of the various traffic direction possibilities and the associated maximum forwarding performance.

Table 4. Egress Reflector Mode Performance

Traffic Direction	Maximum Throughput	Example
From 6100 Series line card not capable of using Cisco TrustSec to Supervisor Engine 2T uplink	15 mpps (systemwide centralized forwarding)	WS-X6148-GETX to Supervisor Engine 2T uplink
From 6100 Series line card not capable of using Cisco TrustSec to other line card not capable of using Cisco TrustSec	15Mpps mpps (systemwide centralized forwarding)	WS-X6148GETX to WS-X6148-GETX
From 6100 Series line card not capable of using Cisco TrustSec to WS-X6908	15 mpps (systemwide centralized forwarding)	WS-X6148GETX to WS-X6908-10G
From 6700 Series or 6800 Series line card not capable of using Cisco TrustSec to Supervisor Engine 2T uplink	30 mpps (systemwide centralized forwarding using CFC) 30 mpps per line card (using DFC4)	WS-X6748-SFP to Supervisor Engine 2T uplink (CFC) WS-X6848-SFP to Supervisor Engine 2T uplink (DFC)
From 6700 Series or 6800 Series line card not capable of using Cisco TrustSec to other line card not capable of using Cisco TrustSec	15 mpps to WS-X6148 series 30 mpps (systemwide centralized forwarding using CFC) 30 mpps per line card (using DFC4)	WS-X6748 to WS-X6148-GETX WS-X6748 to WS-X6748 (CFC) WS-X6748 to WS-X6848 (DFC)
From 6700 Series or 6800 Series line card not capable of using Cisco TrustSec to WS-X6908	30 mpps (systemwide centralized forwarding using CFC) 30 mpps per line card (using DFC4)	WS-X6748 to WS-X6908 (CFC) WS-X6748 to WS-X6908 (DFC4)
From Cisco TrustSec-aware DFC4 line card to Supervisor Engine 2T uplink	48 mpps per line card	WS-X6716 to Supervisor Engine 2T uplink
From 6900 Series to 6900 Series	60 mpps	WS-X6908 to WS-X6908

The following restrictions apply to egress reflection mode:

- All ports configured to propagate SGTs must be L3 routed ports or L3 routed EtherChannel interfaces (L2 switchports are not supported)
- An interval system VLAN will be allocated for every port enabled with Cisco TrustSec SGT
- Service modules are not supported with egress reflector mode, although this may change in future software releases

Conclusion

The Cisco Catalyst 6500 continues to evolve with the release of the Supervisor Engine 2T and 6900 Series line cards. The Cisco Catalyst 6500's support for the full suite of Cisco TrustSec is particularly important because of the Cisco Catalyst 6500's large installed base and diverse deployment options. With the Cisco Catalyst 6500's support of Cisco TrustSec, a true end-to-end deployment is possible.

Prepare your network to deploy a Cisco TrustSec solution with smart, personalized professional services from Cisco and our partners that provide policy review, analysis, and design expertise. Using leading practices, these services help you more quickly and cost-effectively deploy a full authentication and access solution while also providing knowledge transfer for ongoing operational efficiency.

Finally, customers who choose to deploy Cisco Catalyst 6500 systems with Supervisor Engine 2T and 6900 Series line cards can take advantage of the full suite of Cisco TrustSec features and benefits. Customers can also choose to use their installed base of existing line cards with a Cisco TrustSec network by utilizing the ingress and

egress reflector modes described in this paper. Customers can therefore choose to migrate to a Cisco TrustSec network as their needs dictate.

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.**

Printed in USA C11-658388-00 07/11