APPENDIX C

Notes for Catalyst 6500 Series Switches

Revised: April 26, 2013, OL-22192-01

TrustSec Supported Hardware

TrustSec-capable supervisors and Line Cards are listed in tables 3 and 4 of "*Cisco Catalyst 6500 Series with Supervisor Engine 2T: Enabling Cisco TrustSec with Investment Protection,*" at the following URL:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-658388.html

The Catalyst 6500 Series switches that are not TrustSec hardware-capable implement TrustSec Network Device Admission Control (NDAC) without SAP or 802.1AE link encryption.

For a complete table of features, platforms, and IOS images supported, see the latest Product Bulletins at the following URL:

http://www.cisco.com/en/US/netsol/ns1051/index.html

See also, the Matrix of Cisco TrustSec-Enabled Infrastructure at the following URL:

http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html

Flexible NetFlow Support

Release	Feature History
15.1(1)SY1	The following Flexible NetFlow flow exporter configuration subcommand was introduced on the Catalyst 6500 series switches: • **option cts-sgt-table** This option allows Flexible NetFlow to export TrustSec environmental data tables that map Security Group Tags (SGTs) to Security Group Names (SGNs).
12.2(50) SY IP Base LAN Image	The following Flexible NetFlow commands and flow objects were introduced on the Catalyst 6500 series switches: • **cts role-based** {**ip** | **ipv6**} **flow monitor** *monitor_name* **dropped** • **cts source group-tag** • **cts destination group-tag**

Flexible NetFlow can account for packets dropped by SGACL enforcement when SGT and DGT flow objects are configured in the flow record with the standard 5-tuple flow objects

Use the **flow record** and **flow exporter** global configuration commands to configure a flow record, and a flow exporter, then use the **flow monitor** command to add them to a flow monitor. Use the **show flow** show commands to verify your configurations.

To collect only SGACL dropped packets, use the [**no**] **cts role-based** {**ip** | **ipv6**} **flow monitor dropped** global configuration command.

For Flexible NetFlow overview and configuration information, see the following documents:

Flexible NetFlow Configuration Guide, Cisco IOS Release 15S

http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/15-s/fnf-15-s-book.html

Catalyst 6500 Release 15.0SY Software Configuration Guide

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/15_0_sy_swcg.html

Sample Configurations

Configuration Excerpt of an IPV4 Flow Record (5-tuple, direction, SGT, DGT)

```
router(config)# flow record cts-record-ipv4
router(config-flow-record)# match ipv4 protocol
router(config-flow-record)# match ipv4 source address
router(config-flow-record)# match ipv4 destination address
router(config-flow-record)# match transport source-port
router(config-flow-record)# match transport destination-port
router(config-flow-record)# match flow direction
router(config-flow-record)# match flow cts source group-tag
router(config-flow-record)# match flow cts destination group-tag
router(config-flow-record)# collect counter packets
```

Configuration Excerpt of an IPV6 Flow Record (5-tuple, direction, SGT, DGT)

```
router(config)# flow record cts-record-ipv6
router(config-flow-record)# match ipv6 protocol
router(config-flow-record)# match ipv6 source address
router(config-flow-record)# match ipv6 destination address
router(config-flow-record)# match transport source-port
router(config-flow-record)# match transport destination-port
router(config-flow-record)# match flow direction
router(config-flow-record)# match flow cts source group-tag
router(config-flow-record)# match flow cts destination group-tag
router(config-flow-record)# collect counter packets
```

Configuration Excerpt of an IPv4 Flow Monitor

```
router(config)# flow monitor cts-monitor-ipv4
router(config-flow-monitor)# record cts-record-ipv4
```

Configuration Excerpt of an IPv6 Flow Monitor

```
router(config)# flow monitor cts-monitor-ipv6
router(config-flow-monitor)# record cts-record-ipv6
```

Configuration Excerpt of the Global Flow Monitor (IPv4 and IPv6)

The following configuration applies the Flow Monitor to packets dropped by Role-Based Access Control Lists (RBACLs) for all TrustSec interfaces on the router or switch:

```
router(config)# cts role-based ip flow monitor cts-monitor-ipv4 dropped
router(config)# cts role-based ipv6 flow monitor cts-monitor-ipv6 dropped
```

Configuration Excerpt of the Interface Monitor

The Flow Monitor can be attached per interface, configured to filter for combinations of ingress (input), egress (output), multicast, unicast, or Layer2 switched traffic.

For IPv6, flow monitor is supported only for routed traffic in Cisco IOS Release 12.2(50)SY.

```
router(config)# interface TenGigabitEthernet 8/1
router(config-if)# ip address 192.1.1.1 255.255.255.0

;; Ingress IPv4 unicast only and egress unicast only
router(config-if)# ip flow monitor cts-monitor-ipv4 unicast input
router(config-if)# ip flow monitor cts-monitor-ipv4 unicast output

;; Ingress IPV4 L2-switched traffic only
router(config-if)# ip flow monitor cts-monitor-ipv4 layer2-switched input

;; Ingress Ipv4 multicast and egress IPv4 multicast traffic only
router(config-if)# ip flow monitor cts-monitor-ipv4 multicast input
router(config-if)# ip flow monitor cts-monitor-ipv4 multicast output

;; For both Unicast/multicast egress traffic
router(config-if)# ip flow monitor cts-monitor-ipv4 output

;; For both Unicast/multicast ingress traffic
router(config-if)# ip flow monitor cts-monitor-ipv4 input

;; For Ipv6 only the following are supported in Cisco IOS Release 12.2(50)SY
router(config-if)# ipv6 address 2022::22:1:1:11/64
router(config-if)# ipv6 flow monitor cts-monitor-ipv6 input
router(config-if)# ipv6 flow monitor cts-monitor-ipv6 unicast input
router(config-if)# ipv6 flow monitor cts-monitor-ipv6 output
router(config-if)# ipv6 flow monitor cts-monitor-ipv6 unicast output
```

Flexible NetFlow Show Commands

show flow record

show flow monitor

show flow exporter

show flow interface

show cts role-based counters

show flow monitor <monitor_name> cache

show flow monitor <monitor_name> statistics

show platform flow ip

show platform software flow internal fnf

show platform hardware flow table flowmask

show platform hardware flow table profile

show platform hardware acl entry rbacl all

show platform hardware acl entry tcam

show platform software flow internal export

show platform software flow internal export statistics

show platform internal export information

show platform internal export statistics

TrustSec System Error Messages

Cisco TrustSec system error messages are listed in the Cisco Catalyst 6500 Series Switches Error and System Messages guides, found at the following URL:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_system_message_guides_list.html

The Error Message Decoder Tool is at the following URL:
http://www.cisco.com/en/US/support/tsd_most_requested_tools.html

FIPS Support

The Federal Information Processing Standard (FIPS) certification documents for Catalyst 6500 series switch software and hardware combinations are posted on the following website:

http://www.cisco.com/web/strategy/government/security_certification/net_business_benefit_seccert_fips140.html

The Catalyst 6500 Series FIPS certification documents describe the FIPS concepts and implementation per software/hardware combination.

TrustSec Considerations when Configuring FIPS

Perform initial setup, initialization, and configuration procedures of the Catalyst switch per the FIPS certification guide appropriate to your hardware and software configuration.

Licensing Requirements for FIPS

FIPS requires no licence for the Catalyst 6500 series switches.

Prerequisites for FIPS Configuration

- Disable Telnet. Users should log in using Secure Shell (SSH) only.
- Disable SNMPv1 and v2. Any existing user accounts on the device that have been configured for SNMPv3 should be configured only with SHA for authentication and AES/3DES for privacy.
- Delete all SSH server RSA1 key-pairs.

Guidelines and Limitations for FIPS

- The RADIUS keywrap feature works only with Cisco Identity Services Engine 1.1 or Cisco ACS Release 5.2 or later releases.
- HTTPS/TLS access to the module is allowed in FIPS approved mode of operation, using SSLv3.1/TLSv1.0 and a FIPS approved algorithm.
- SSH access to the module is allowed in FIPS approved mode of operation, using SSHv2 and a FIPS approved algorithm. Many SSH clients provide cryptographic libraries that can be set to FIPS Mode, making all cryptographic operations FIPS 140-2 Level 2 compliant.
- Your passwords must have a minimum of eight alphanumeric characters including at least one letter and at least one number character.

Default Settings for FIPS

The default is FIPS mode disabled, RADIUS keywrap disabled.