Troubleshoot Trustsec Inline Tagging

Contents

Introduction

This document describes how to configure and verify the Cisco Inline Tagging feature on a Cisco Catalyst Switch 9300.

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Cisco TrustSec (CTS) components
- Basic knowledge of CLI configuration of Catalyst switches
- Experience with Identity Services Engine (ISE) configuration

You must have Cisco ISE deployed in your network, and end users must authenticate to Cisco ISE via 802.1x (or other method) when they connect wired. Cisco ISE assigns a Security Group Tag (SGT) once they authenticate to your wired network.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Services Engine that runs 3.0 P5

- Cisco Catalyst 9300 Switch that runs 17.03.02a
- Cisco Catalyst 9300 Switch that runs 17.07.01

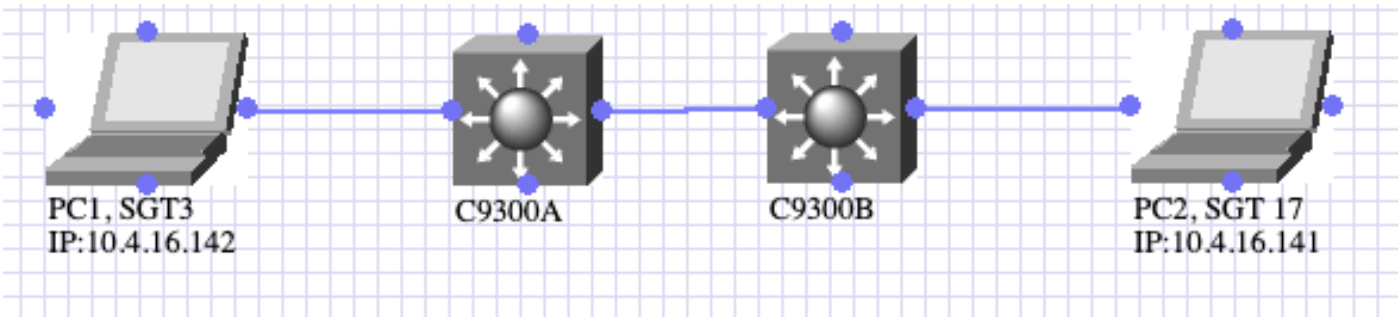
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Inline tagging is implemented at the Access layer because this is the first point of contact of the information. In other words, all your end devices are connected to the Access layer. Once the Access-layer devices does the classification it is necessary to share this information with the devices that do the enforcement. To do this, the NAS can add 20 bytes to the ethernet frame. This is the CMD (Cisco metadata) field of the frame. Inside of this the SGT is included.

Configure

Network Diagram



Topology diagram

- PC1 authenticates and ISE dynamically assigns SGT3.
- C9300A inline tagging with C9300B
- PC2 authenticates and ISE dynamically assigns SGT 17
- C9300B enforces ICMP traffic from SGT3 to SGT17.

Inline Tagging

C9300A

interface TwoGigabitEthernet1/0/4 switchport trunk allowed vlan 761 switchport mode trunk cts manual policy static sgt 2 trusted end

C9300B

interface GigabitEthernet1/0/4 switchport trunk allowed vlan 761 switchport mode trunk cts manual policy static sgt 2 trusted end

You must use the command **cts manual** and then **policy static** to enable inline tagging. The sgt used on the command can be the sgt of the Network device or any other its a placeholder. The function of the **trusted** command is to instruct the switch to honor the SGT, if it receives traffic with CMD header. Without **trusted** command, the switch tags all traffic that flows from that interface with the defined SGT.

Checks

Access Session Downloads SGT

PC1

```
Switch#show authentication session interface Tw1/0/3 details
            Interface:  TwoGigabitEthernet1/0/3
               IIF-ID:  0x1FB0D90E
          MAC Address:  507b.9df0.34bb
         IPv6 Address:  Unknown
         IPv4 Address:  10.4.16.142
            User-Name:  50-7B-9D-F0-34-BB
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  3D781F0A0000000F2AE95F4A
      Acct Session ID:  0x00000005
               Handle:  0x02000004
       Current Policy:  POLICY_Tw1/0/3


Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure

Server Policies:
            SGT Value:  3


Method status list:
       Method           State
          mab           Authc Success
```

PC2

```
Switch#show authentication session interface Gi1/0/1 details
            Interface:  GigabitEthernet1/0/1
               IIF-ID:  0x1D1CA5C7
          MAC Address:  507b.9df8.02ed
         IPv6 Address:  fe80::114c:dce1:ffa1:1642
         IPv4 Address:  10.4.16.141
            User-Name:  50-7B-9D-F8-02-ED
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  21781F0A000000242AF41195
      Acct Session ID:  0x00000004
               Handle:  0x4300000f
       Current Policy:  POLICY_Gi1/0/1


Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure
```

```
Server Policies:
            SGT Value:  17


Method status list:
       Method           State
          mab           Authc Success
```

Switch Learns IP-SGT Binding

C9300A

```
Switch#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.4.16.142             3       LOCAL
```

C9300B

```
Switch#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.4.16.141             17      LOCAL
10.31.120.33            2       INTERNAL
```

Authorization status between C9300A and C9300B

C9300A

```
Switch#show cts interface Two 1/0/4
Global Dot1x feature is Disabled
Interface TwoGigabitEthernet1/0/4:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Interface Active for 01:36:44.332
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    SUCCEEDED
        Peer SGT:            2:TrustSec_Devices
        Peer SGT assignment: Trusted
    SAP Status:              NOT APPLICABLE
    Propagate SGT:           Enabled
    Cache Info:
        Expiration            : N/A
        Cache applied to link : NONE

    Statistics:
        authc success:              0
        authc reject:               0
```

```
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                0
        sap fail:                   0
        authz success:              0
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.
```

C9300B

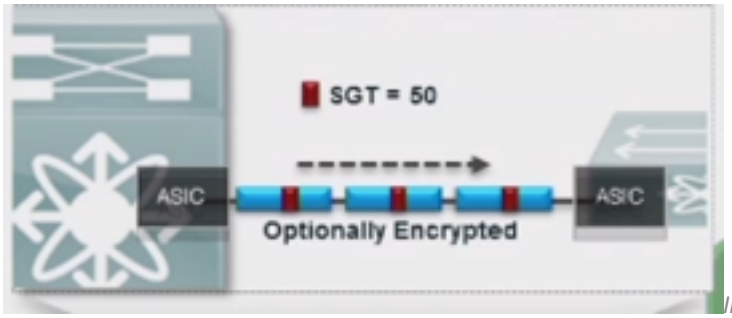
```
Switch#show cts interfac Gig 1/0/4
Global Dot1x feature is Disabled
Interface GigabitEthernet1/0/4:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Interface Active for 01:34:18.433
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    SUCCEEDED
        Peer SGT:            2:TrustSec_Devices
        Peer SGT assignment: Trusted
    SAP Status:              NOT APPLICABLE
    Propagate SGT:           Enabled
    Cache Info:
        Expiration            : N/A
        Cache applied to link : NONE

    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                0
        sap fail:                   0
        authz success:              0
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.
```

Troubleshoot

To troubleshoot any issues, consider:

- Frame is always tagged at ingress port of SGT capable device.
- Tagging process prior to other L2 service such as QoS.
- No impact IP MTU/Fragmentation.
- L2 frame MTU impact: ~ 40 bytes (~1600 bytes with 1552 bytes MTU)
- MACsec is optional for capable hardware.

Packet Capture/EPC



Inline tagging flow

If you want to troubleshoot inline tagging you would need to take a packet capture at the ingress.

> **Tip**: If you take a pcap in the uplink of the SW you do not see the tag since this is included at the interface level so the EPC can be taken before the tag is applied.

> **Caution**: There are some exceptions to this like C4500. Due to the architecture of the C4500, it is not able to detect the CMD header even if you take the pcap at the ingress interface. For this specific cases you can use Netflow, Netflow Trustsec configuration

Take Embedded Packet Capture (EPC) on Ingress Port of the C9300B

```
Switch#monitor capture test interface Gig 1/0/4 both
Switch#monitor capture test match any
Switch#monitor capture test start

<<Generate traffic from PC1 to PC2>>

Switch#monitor capture test stop
```

After you take the EPC you can use **show monitor capture buffer brief** command to check the frame number of the ICMP request.

```
Switch#show monitor capture test buffer
..
..

   44  17.059569  10.4.16.142 b^F^R 10.4.16.141  ICMP 86 Echo (ping) request  id=0x0001,
seq=147/37632, ttl=128
   45  17.061079  10.4.16.141 b^F^R 10.4.16.142  ICMP 74 Echo (ping) reply    id=0x0001,
seq=147/37632, ttl=128 (request in 44)
..
..
```

From the previous output its observed that ICMP packet is in frame 44. With this you can now run: **show monitor capture <name> buffer detailed | begin Frame <number>** to see the content:

.. .. Frame 44: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0 Interface id: 0 (/tmp/epc_ws/wif_to_ts_pipe) Interface name: /tmp/epc_ws/wif_to_ts_pipe Encapsulation type: Ethernet (1) Arrival Time: Jun 3, 2022 19:12:00.140014000 UTC [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1654283520.140014000 seconds [Time delta from previous captured frame: 0.362660000 seconds] [Time delta from previous displayed frame: 0.362660000 seconds] [Time since reference or first frame: 17.059569000 seconds] Frame Number: 44 Frame Length: 86 bytes (688 bits) Capture Length: 86 bytes (688 bits) [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: eth:ethertype:vlan:ethertype:cmd:ethertype:ip:icmp:data] Ethernet II, Src: 50:7b:9d:f0:34:bb (50:7b:9d:f0:34:bb), Dst: 50:7b:9d:f8:02:ed (50:7b:9d:f8:02:ed) Destination: 50:7b:9d:f8:02:ed

(50:7b:9d:f8:02:ed) Address: 50:7b:9d:f8:02:ed (50:7b:9d:f8:02:ed) .... ..0. .... = LG bit: Globally unique address (factory default) ....0 .... = IG bit: Individual address (unicast) Source: 50:7b:9d:f0:34:bb (50:7b:9d:f0:34:bb) Address: 50:7b:9d:f0:34:bb (50:7b:9d:f0:34:bb) .... ..0. .... = LG bit: Globally unique address (factory default) ....0 .... = IG bit: Individual address (unicast) Type: 802.1Q Virtual LAN (0x8100) 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 761 000. .... = Priority: Best Effort (default) (0) ...0 .... = DEI: Ineligible .... 0010 1111 1001 = ID: 761 Type: CiscoMetaData (0x8909) **Cisco MetaData <<<<<<<<<<<<<<<<<<<<<<< CMD header**

```
    Version: 1
    Length: 1
    Options: 0x0001
    SGT: 3    <<<<<<<<<<<<<<<<<<<<<<<<< SGT of PC1
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.4.16.142, Dst: 10.4.16.141
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 60
    Identification: 0x7d1f (32031)
    Flags: 0x0000
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..0. .... .... .... = More fragments: Not set
        ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x887f [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.4.16.142
    Destination: 10.4.16.141
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4cc8 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 147 (0x0093)
    Sequence number (LE): 37632 (0x9300)
    Data (32 bytes)

0000  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70   abcdefghijklmnop
0010  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69   qrstuvwabcdefghi
        Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
        [Length: 32]
..
..
```

SGACL Check

The switch only downloads the SGACLs that match the IP-SGT bindings learned from different methods (local, SXP, inline tagging, and so on). C9300B learns the destination security group dynamically from ISE. How does it learn the source security group? With Inline Tagging. As the command **show cts role-based sgt-map all** does not show the SGTs learned from inline tagging, you can conclude that if the SGACL is downloaded, the switch is aware from both source (inline tagging) and destination (local) security groups.

```
Switch#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit_IP_Log-00
IPv4 Role-based permissions from group 3:DataCenter to group  17:MedicalDevices:
```

```
        denyJonsICMP-06     <<<<
        DENY_PRINTER_80_04-01
        permitJons-01
IPv4 Role-based permissions from group 16:IUH_Office to group 17:MedicalDevices:
        denyJonsICMP-06
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

When you ping from PC1 from PC2, the ICMP is blocked:

```
cisco>ping -S 10.4.16.142 10.4.16.141

Pinging 10.4.16.141 from 10.4.16.142 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.4.16.141:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Related Information

- **Cisco Technical Support & Downloads**