Configure ASA 9.3.1 TrustSec Inline Tagging

Contents

Introduction

This document describes how to use the feature implemented in the Adaptive Security Appliance (ASA) Release 9.3.1 - TrustSec Inline Tagging. That feature allows ASA to receive TrustSec frames as well as to send them. This way ASA can be easily integrated within TrustSec domain without the need to use TrustSec SGT Exchange Protocol (SXP).

This example presents remote VPN user which have been assigned Security Group Tag (SGT) tag = 3 (Marketing) and 802.1x user which have been assigned SGT tag = 2 (Finance). Traffic enforcement is performed by both ASA with the use of Security Group Access Control List (SGACL) defined locally and Cisco IOS® switch using Role Based Access Control List (RBACL)

downloaded from Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ASA CLI configuration and Secure Socket Layer (SSL) VPN configuration
- Remote access VPN configuration on the ASA
- ISE and TrustSec services

Components Used

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

- Cisco ASA software, version 9.3.1 and later
- Cisco ASA hardware 55x5 or ASAv
- Windows 7 with Cisco AnyConnect Secure Mobility Client, release 3.1
- Cisco Catalyst 3750X switch with software 15.0.2 and later
- Cisco ISE, release 1.2 and later

Configure

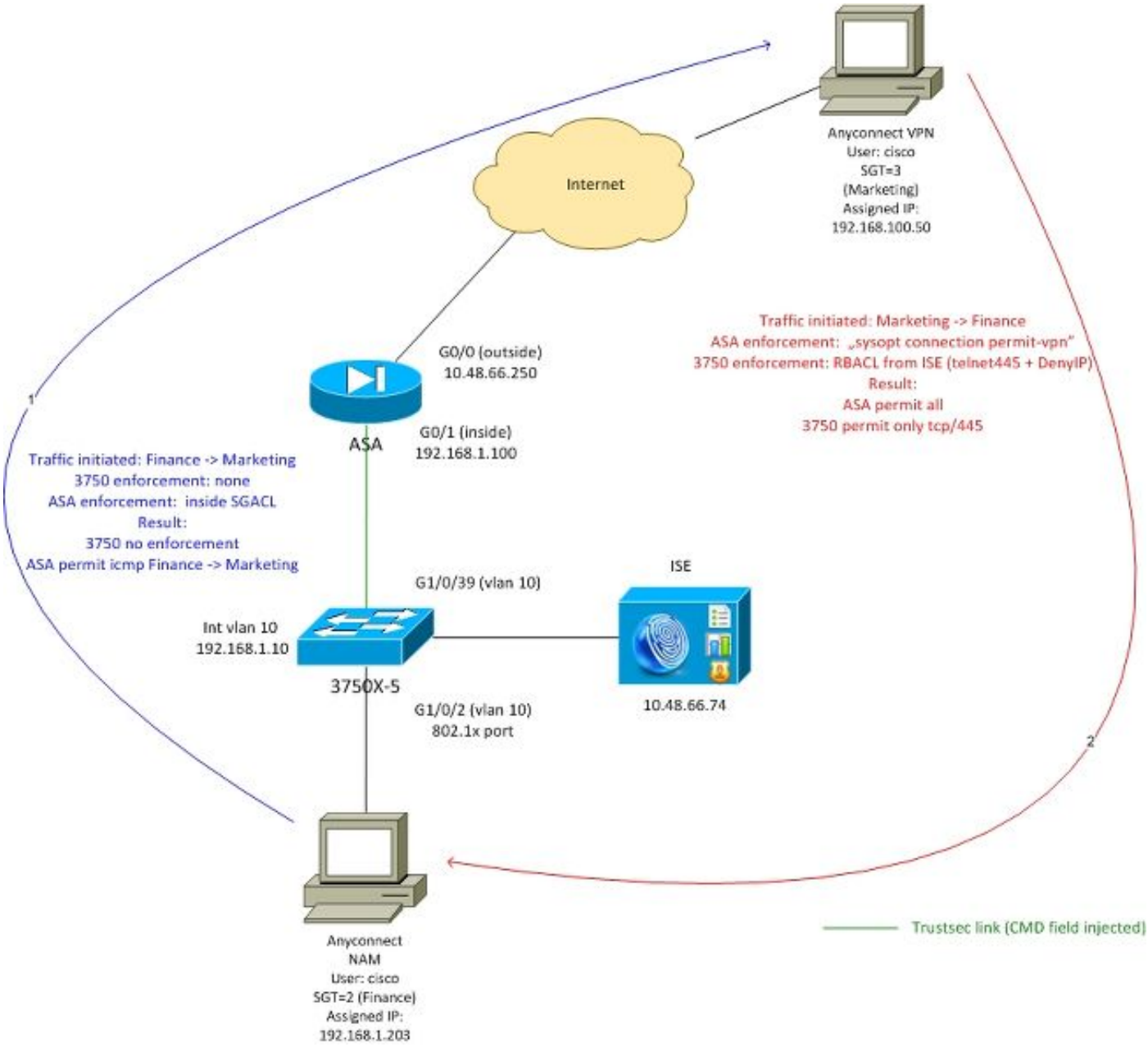
> **Note**: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram

Connection between ASA and 3750X is configured for manual cts. That means both devices can send and receive modified Ethernet frames with Cisco Metadata Field (CMD). That field includes Security Group Tag (SGT) which describes the source of the packet.

Remote VPN user terminates SSL session on ASA and is assigned SGT tag 3 (Marketing).

Local corporate 802.1x user after successful authentication has been assigned SGT tag 2 (Finance).



ASA has SGACL configured on the inside interface that allows for ICMP traffic initiated from Finance to Marketing.

ASA permits all the traffic initiated from remove VPN user (because of "sysopt connection permit-vpn" configuration).

SGACL on ASA is stateful which means that once the flow is created, return packet is accepted automatically (based on the inspection).

3750 switch uses RBACL in order to control the traffic received from Marketing to Finance.

RBACL is stateless which means that every packet is checked but TrustSec enforcement on 3750X platform is performed at the destination. This way switch is responsible for enforcement of the traffic from Marketing to Finance.

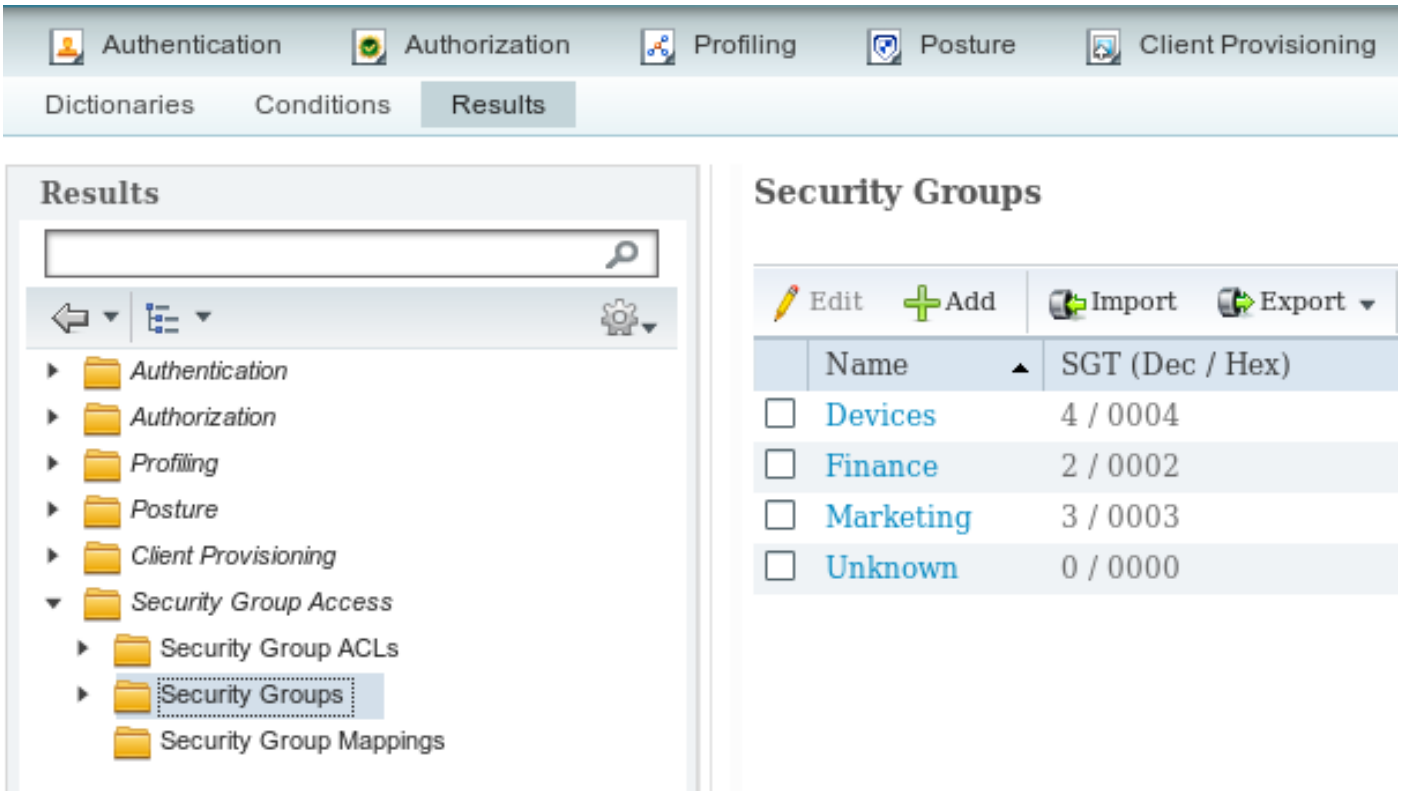
> **Note**: For Trustsec aware stateful firewall on Cisco IOS® Zone Based Firewall can be used, For example, refer:

Note: ASA could have SGACL controlling traffic that comes from remote VPN user. In order to simplify the scenario, it has not been presented in this article. For example refer: ASA Version 9.2 VPN SGT Classification and Enforcement Configuration Example

ISE - Configuration Steps

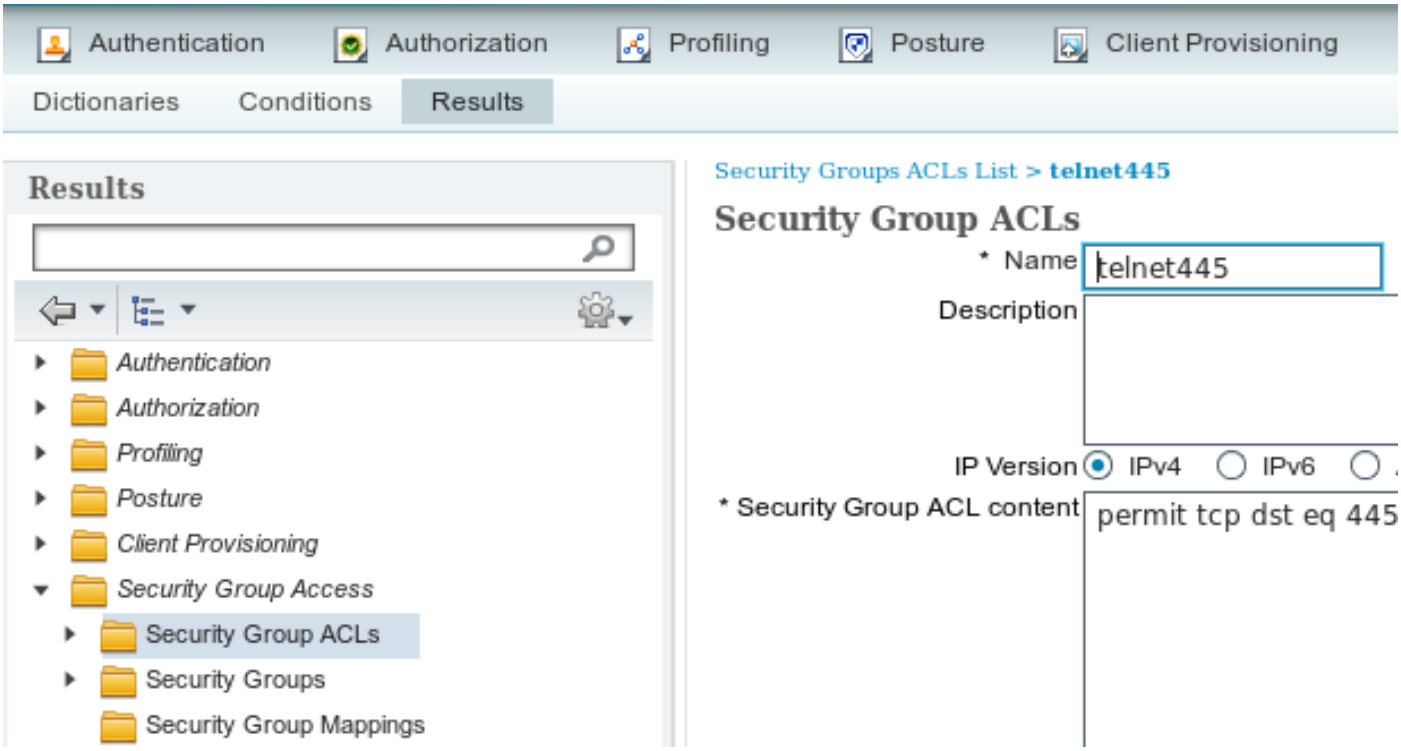
1. SGT for Finance and Marketing

Navigate to **Policy > Results > Security Group Access > Security Groups** and create SGT for Finance and Marketing as shown in this image.



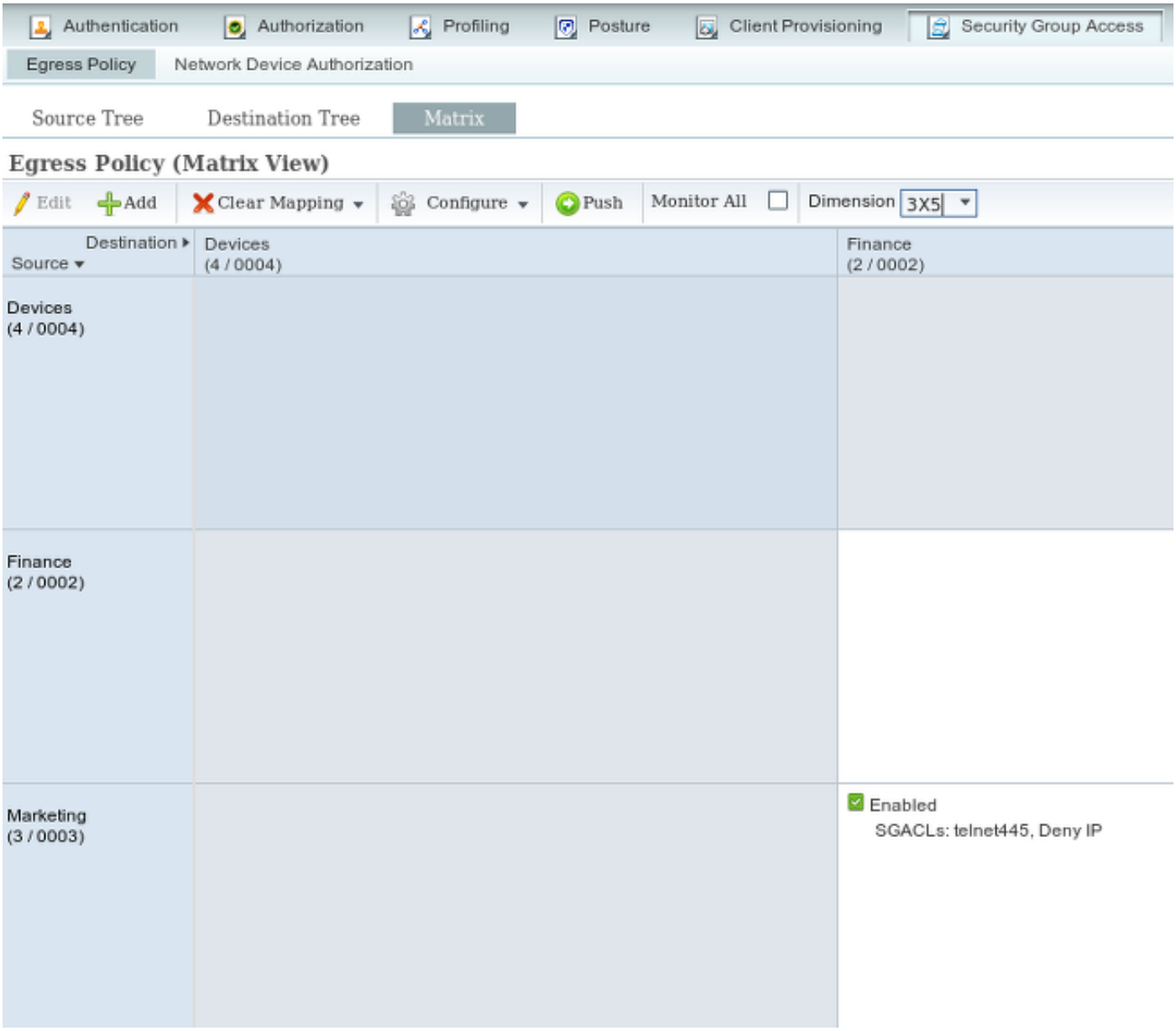
2. Security Group ACL for Traffic Marketing > Finance

Navigate to **Policy > Results > Security Group Access > Security Group ACL** and create ACL which is used to control traffic from Marketing to Finance. Only tcp/445 is allowed as shown in this image.



3. Binding ACL in Matrix

Navigate to **Policy > Egress Policy > Matrix** bind configured ACL for the Source: **Marketing** and Destination: **Finance**. Also attach **Deny IP** as the last ACL to drop all other traffic as shown in the image. (without that default policy will be attached, default is permit any)



4. Authorization Rule for VPN Access Assigning SGT = 3 (Marketing)

Navigate to **Policy > Authorization** and create a rule for remote VPN access. All VPN connections established via AnyConnect 4.x client will get full access (PermitAccess) and will be assigned SGT tag 3 (Marketing). The condition is to use AnyConnect Identity Extentions (ACIDEX):

```
Rule name: VPN
Condition: Cisco:cisco-av-pair CONTAINS mdm-tlv=ac-user-agent=AnyConnect Windows 4
Permissions: PermitAccess AND Marketing
```

5. Authorization Rule for 802.1x Access Assigning SGT = 2 (Finance)

Navigate to **Policy > Authorization** and create a rule for 802.1x access. Supplicant terminating 802.1x session on 3750 switch with username **cisco** will get full access (PermitAccess) and will be assigned SGT tag 2 (Finance).

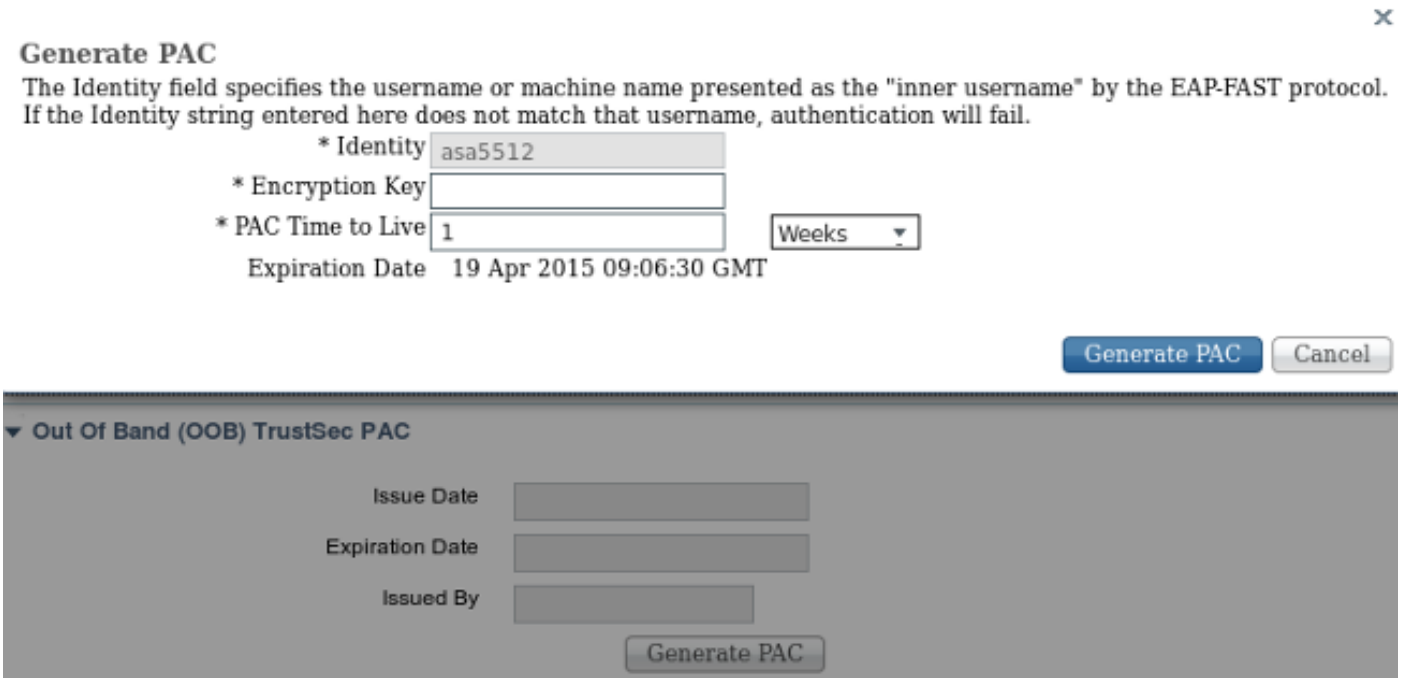
```
Rule name: 802.1x
```

```
Condition: Radius:User-Name EQUALS cisco AND Radius:NAS-IP-Address EQUALS 192.168.1.10
Permissions: PermitAccess AND
```**Finance**

6. Adding Network Device, Generating PAC for ASA

In order to add ASA to TrustSec domain, it's necessary to generate PAC file manually. That file is imported on ASA.

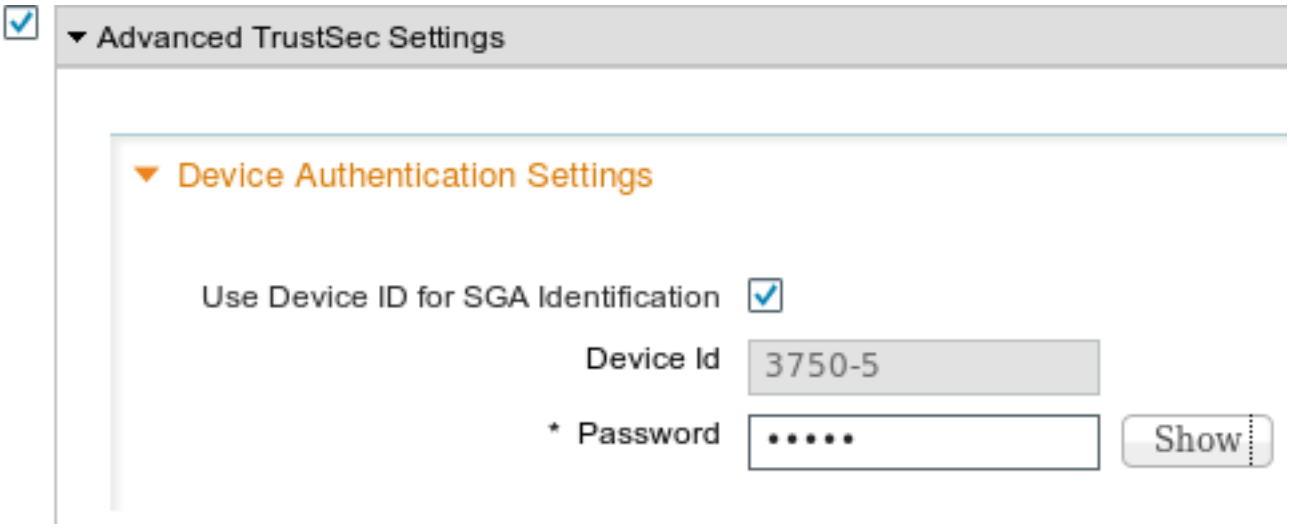
That can be configured from **Administration > Network Devices**. After ASA is added, scroll down to **TrustSec settings** and **Generate PAC** as shown in this image.



Switches (3750X) support automatic PAC provisioning, so that steps needs to be executed only for ASA which supports only manual PAC provisioning.

7. Add Network Device, Configure Secret for Switch Automatic PAC Provisioning

For switch that uses automatic PAC provisioning, a correct secret must be set, as shown in this image.



Note: PAC is used to authenticate ISE and download environment data (eg. SGT) along with

policy (ACL). ASA supports only environment data, policies needs to be manually configured on ASA. Cisco IOS® supports both, so the policies can be downloaded from ISE.

ASA - Configuration Steps

1. Basic VPN Access

Configure basic SSL VPN access for AnyConnect using ISE for authentication.

```
Rule name: 802.1x
Condition: Radius:User-Name EQUALS cisco AND Radius:NAS-IP-Address EQUALS 192.168.1.10
Permissions: PermitAccess AND Finance
```

2. Import PAC and Enable cts

Import PAC generated for ASA (from Step 6 of ISE configuration). Use the same encryption key:

```
BSNS-ASA5512-4# cts import-pac http://10.229.20.86/asa5512.pac password ciscocisco
PAC Imported Successfully
```

In order to verify:

```
BSNS-ASA5512-4# show cts pac

 PAC-Info:
   Valid until: Apr 11 2016 10:16:41
   AID:         c2dcb10f6e5474529815aed11ed981bc
   I-ID:        asa5512
   A-ID-Info:   Identity Services Engine
   PAC-type:    Cisco Trustsec
 PAC-Opaque:
   000200b00003000100040010c2dcb10f6e5474529815aed11ed981bc00060094000301
   007915dcb81032f2fdf04bfe938547fad2000000135523ecb300093a8089ee0193bb2c
   8bc5cfabf8bc7b9543161e6886ac27e5ba1208ce445018a6b07cc17688baf379d2f1f3
   25301fffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
   4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
   4d4013e8fe
```

Enable cts:

```
BSNS-ASA5512-4# show cts pac

 PAC-Info:
   Valid until: Apr 11 2016 10:16:41
   AID:         c2dcb10f6e5474529815aed11ed981bc
   I-ID:        asa5512
   A-ID-Info:   Identity Services Engine
   PAC-type:    Cisco Trustsec
 PAC-Opaque:
   000200b00003000100040010c2dcb10f6e5474529815aed11ed981bc00060094000301
   007915dcb81032f2fdf04bfe938547fad2000000135523ecb300093a8089ee0193bb2c
   8bc5cfabf8bc7b9543161e6886ac27e5ba1208ce445018a6b07cc17688baf379d2f1f3
   25301fffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
   4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
   4d4013e8fe
```

After you enable cts, ASA must download environment data from ISE:

```
BSNS-ASA5512-4# show cts environment-data
CTS Environment Data
====================
Status:                    Active
Last download attempt:     Successful
Environment Data Lifetime: 86400 secs
Last update time:          10:21:41 UTC Apr 11 2015
Env-data expires in:       0:00:37:31 (dd:hr:mm:sec)
Env-data refreshes in:     0:00:27:31 (dd:hr:mm:sec)
```

3. SGACL for Traffic Finance > Marketing

Configure SGACL on the inside interface. The ACL allows to initiate only ICMP traffic from Finance to Marketing.

```
access-list inside extended permit icmp security-group name Finance any security-group name
Marketing any
access-group inside in interface inside
```

ASA must expand the name of the tag to number:

```
BSNS-ASA5512-4(config)# show access-list inside
access-list inside line 1 extended permit icmp security-group name Finance(tag=2) any security-
group name Marketing(tag=3) any (hitcnt=47) 0x5633b153
```

4. Enable cts on Inside Interface

After you enable cts on the inside interface of ASA:

```
interface GigabitEthernet0/1
 nameif inside
cts manual
  policy static sgt 100 trusted
 security-level 100
 ip address 192.168.1.100 255.255.255.0
```

ASA is able to send and receive TrustSec frames (ethernet frames with CMD field). ASA assumes that all ingress frames without a tag must be treated as with the tag 100. All the ingress frames which already include the tag will be trusted.

Switch - Configuration Steps

1. Basic 802.1x

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius

dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
```

```
 switchport access vlan 10
 switchport mode access
 authentication host-mode multi-domain
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast

radius-server host 10.48.66.74 pac key cisco
```

With that configuration, after successful 802.1x authorization the user (authorized via ISE) must be assigned tag 2 (Finance).

2. CTS Configuration and Provisioning

Similarly, as for ASA, cts is configured and point to ISE:

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius

dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
 switchport access vlan 10
 switchport mode access
 authentication host-mode multi-domain
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast

radius-server host 10.48.66.74 pac key cisco
```

Also, enforcement is enabled both for Layer3 and Layer2 (all vlans):

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius

dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
 switchport access vlan 10
 switchport mode access
 authentication host-mode multi-domain
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast

radius-server host 10.48.66.74 pac key cisco
```

In order to provision PAC automatically:

```
bsns-3750-5#cts credentials id 3750-5 password ciscocisco
```

Again, password must match with the corresponding configuration on ISE (**Network Device > Switch > TrustSec**). Right now, Cisco IOS® initiates EAP-FAST session with ISE in order to get

the PAC. More detail on that process can be found here:

ASA and Catalyst 3750X Series Switch TrustSec Configuration Example and Troubleshoot Guide

In order to verify if PAC is installed:

```
bsns-3750-5#show cts pacs
 AID: EA48096688D96EF7B94C679A17BDAD6F
 PAC-Info:
   PAC-type = Cisco Trustsec
   AID: EA48096688D96EF7B94C679A17BDAD6F
   I-ID: 3750-5
   A-ID-Info: Identity Services Engine
   Credential Lifetime: 14:41:24 CEST Jul 10 2015
 PAC-Opaque:
000200B000030001000400010EA48096688D96EF7B94C679A17BDAD6F000600940003010036 5AB3133998C86C1BA1B418
968C6069000000135526 1CCC00093A808F8A81F3F8C99A7CB83A8C3BFC4D573212C61CDCEB37ED279D683EE0DA60D86D
5904C41701ACF07BE98B3B73C4275C98C19A1DD7E1D65E679F3E9D40662B409E58A9F139BAA3BA3818553152F28AE04B
089E5B7CBB22A0D4BCEEF80F826A180B5227EAACBD07709DBDCD3CB42AA9F996829AE46F
 Refresh timer is set for 4y14w
```

3. Enable cts on Interface to ASA

```
interface GigabitEthernet1/0/39
 switchport access vlan 10
 switchport mode access
 cts manual
  policy static sgt 101 trusted
```

From now on, the switch must be ready to process and send TrustSec frames and enforce the policies downloaded from ISE.

Verify

Use this section in order to confirm that your configuration works properly.

Verification is covered in individual sections of this document.

Troubleshoot

SGT Assignment

After VPN session to ASA is established, the correct SGT assignment must be confirmed:

```
BSNS-ASA5512-4# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 13
Assigned IP  : 192.168.100.50         Public IP    : 10.229.20.86
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SHA1
```

```
Bytes Tx     : 10308                  Bytes Rx     : 10772
Group Policy : TAC                    Tunnel Group : TAC
Login Time   : 15:00:13 UTC Mon Apr 13 2015
Duration     : 0h:00m:25s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a801640000d000552bd9fd
Security Grp : 3:Marketing
```

As per authorization rules on ISE, all AnyConnect4 users has been assigned to the Marketing tag.

The same with 802.1x session on the switch. After AnyConnect Network Analysis Module (NAM) finishes, authentication switch will apply the correct tag returned from ISE:

```
bsns-3750-5#show authentication sessions interface g1/0/2 details
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
        IPv6 Address:  Unknown
        IPv4 Address:  192.168.1.203
           User-Name:  cisco
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  multi-domain
    Oper control dir:  both
     Session timeout:  N/A
   Common Session ID:  0A30426D000000130001B278
     Acct Session ID:  Unknown
              Handle:  0x53000002
      Current Policy:  POLICY_Gi1/0/2

Local Policies:
       Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
     Security Policy:  Should Secure
     Security Status:  Link Unsecure

Server Policies:
           SGT Value:  2

Method status list:
      Method           State
      dot1x            Authc Success
      mab              Stopped
```

As per authorization rules on ISE, all users connected to that switch must be assigned to SGT = 2 (Finance).

Enforcement on ASA

When you try to send a traffic from Finance (192.168.1.203) to Marketing (192.168.100.50), it hits inside interface of ASA. For ICMP echo request, it creates the session:

```
Built outbound ICMP connection for faddr 192.168.100.50/0(LOCAL\cisco, 3:Marketing) gaddr
192.168.1.203/1 laddr 192.168.1.203/1(2)
```

and increases the ACL counters:

```
BSNS-ASA5512-4(config)# sh access-list

access-list inside line 1 extended permit icmp security-group name Finance(tag=2) any security-
```

```
group name Marketing(tag=3) any (hitcnt=138)
```

That can be also confirmed looking at packet captures. Note that the correct tags are displayed:

```
BSNS-ASA5512-4(config)# capture CAP interface inside
BSNS-ASA5512-4(config)# show capture CAP

  1: 15:13:05.736793       INLINE-TAG 2 192.168.1.203 > 192.168.100.50: icmp: echo request
  2: 15:13:05.772237       INLINE-TAG 3 192.168.100.50 > 192.168.1.203: icmp: echo reply
  3: 15:13:10.737236       INLINE-TAG 2 192.168.1.203 > 192.168.100.50: icmp: echo request
  4: 15:13:10.772726       INLINE-TAG 3 192.168.100.50 > 192.168.1.203: icmp: echo reply
```

There is incoming ICMP echo request tagged with SGT = 2 (Finance) and then a response from VPN user which is tagged by ASA with SGT = 3 (Marketing). Another troubleshooting tool, packet-tracer is also TrustSec ready.

Unfortunately, 802.1x PC does not see that answer because it's blocked by stateless RBACL on the switch (explanation in the next section).

Another troubleshooting tool, packet-tracer is also TrustSec ready. Let's confirm if incoming ICMP packet from Finance will be accepted:

```
BSNS-ASA5512-4# packet-tracer input inside icmp inline-tag 2 192.168.1.203 8 0 192.168.100.50
Mapping security-group 3:Marketing to IP address 192.168.100.50

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.48.66.1 using egress ifc  outside

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group inside in interface inside
access-list inside extended permit icmp security-group name Finance any security-group name
Marketing any
Additional Information:

<some output omitted for clarity>
```

```
Phase: 13
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 4830, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: allow
```

Let's also try to initiate any TCP connection from Finance to Marketing, that must be blocked by the ASA:

```
Deny tcp src inside:192.168.1.203/49236 dst outside:192.168.100.50/445(LOCAL\cisco, 3:Marketing)
by access-group "inside" [0x0, 0x0]
```

Switch Enforcement

Let's verify if the switch has downloaded policies from ISE correctly:

```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:Finance to group Unknown:
       test_deny-30
IPv4 Role-based permissions from group 8 to group Unknown:
       permit_icmp-10
IPv4 Role-based permissions from group Unknown to group 2:Finance:
       test_deny-30
       Permit IP-00
IPv4 Role-based permissions from group 3:Marketing to group 2:Finance:
        telnet445-60
        Deny IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Policy that controlls the traffic from Marketing to Finance is installed correctly. Only tcp/445 is allowed as per RBACL:

```
bsns-3750-5#show cts rbacl telnet445
CTS RBACL Policy
================
RBACL IP Version Supported: IPv4
 name   = telnet445-60
 IP protocol version = IPV4
 refcnt = 2
 flag   = 0x41000000
 stale  = FALSE
 RBACL ACEs:
   permit tcp dst eq 445
```

That is the reason why ICMP echo response that comes from Marketing to Finance has been dropped. That can be confirmed by checking the counters for traffic from SGT 3 to SGT 2:

```
bsns-3750-5#show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical policies
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted

*       *       0               0               223613          3645233

0       2       0               0               0               122

3       2       0               65              0               0

2       0       0               0               179             0

8       0       0               0               0               0
```

Packets has been dropped by hardware (current counter is 65 and increasing every 1 second).

What if tcp/445 connection is initiated from Marketing?

ASA allows that (accepts all VPN traffic because of "sysopt connection permit-vpn"):

```
Built inbound TCP connection 4773 for outside:192.168.100.50/49181
(192.168.100.50/49181)(LOCAL\cisco, 3:Marketing) to inside:192.168.1.203/445 (192.168.1.203/445)
(cisco)
```

The correct session is created:

```
BSNS-ASA5512-4(config)#  show conn all | i 192.168.100.50
TCP outside  192.168.100.50:49181 inside  192.168.1.203:445, idle 0:00:51, bytes 0, flags UB
```

And, Cisco IOS® accepts it since it matches telnet445 RBACL. The correct counters increases:

```
bsns-3750-5#show cts role-based counters from 3 to 2
3       2       0               65              0               3
```

(last column is traffic permitted by the hardware). The session is permitted.

This example is presented on purpose in order to show the difference in TrustSec policies configuration and enforcement on ASA and Cisco IOS®. Be aware of the differences of Cisco IOS® policies downloaded from ISE (stateless RBACL) and TrustSec aware stateful Zone Based Firewall.

Related Information

- **ASA Version 9.2.1 VPN Posture with ISE Configuration Example**
- **ASA and Catalyst 3750X Series Switch TrustSec Configuration Example and Troubleshoot Guide**
- **Cisco TrustSec Switch Configuration Guide: Understanding Cisco TrustSec**
- **Configuring an External Server for Security Appliance User Authorization**
- **Cisco ASA Series VPN CLI Configuration Guide, 9.1**
- **Cisco Identity Services Engine User Guide, Release 1.2**
- **Technical Support & Documentation - Cisco Systems**