ASA Version 9.2 VPN SGT Classification and Enforcement Configuration Example

Document ID: 117694

Contributed by Michal Garcarz, Cisco TAC Engineer.
May 21, 2014

Contents

Introduction

This document describes how to use a new feature in the Adaptive Security Appliance (ASA) Release 9.2.1, TrustSec Security Group Tag (SGT) classification for VPN users. This example presents two VPN users which have been assigned a different SGT and Security Group Firewall (SGFW), which filters the traffic between the VPN users.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of ASA CLI configuration and Secure Socket Layer (SSL) VPN configuration
- Basic knowledge of remote access VPN configuration on the ASA
- Basic knowledge of Identity Services Engine (ISE) and TrustSec services

Components Used

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

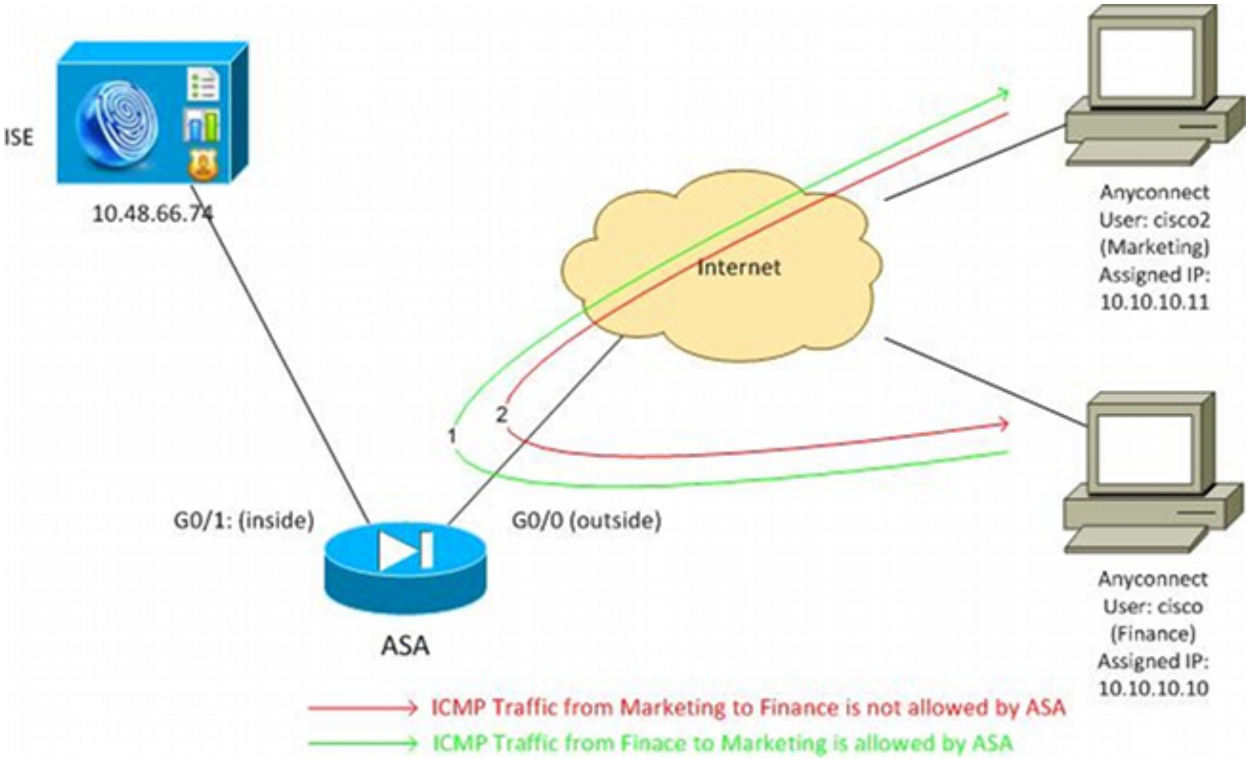
- Cisco ASA software, Version 9.2 and later
- Windows 7 with Cisco AnyConnect Secure Mobility Client, Release 3.1
- Cisco ISE, Release 1.2 and later

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

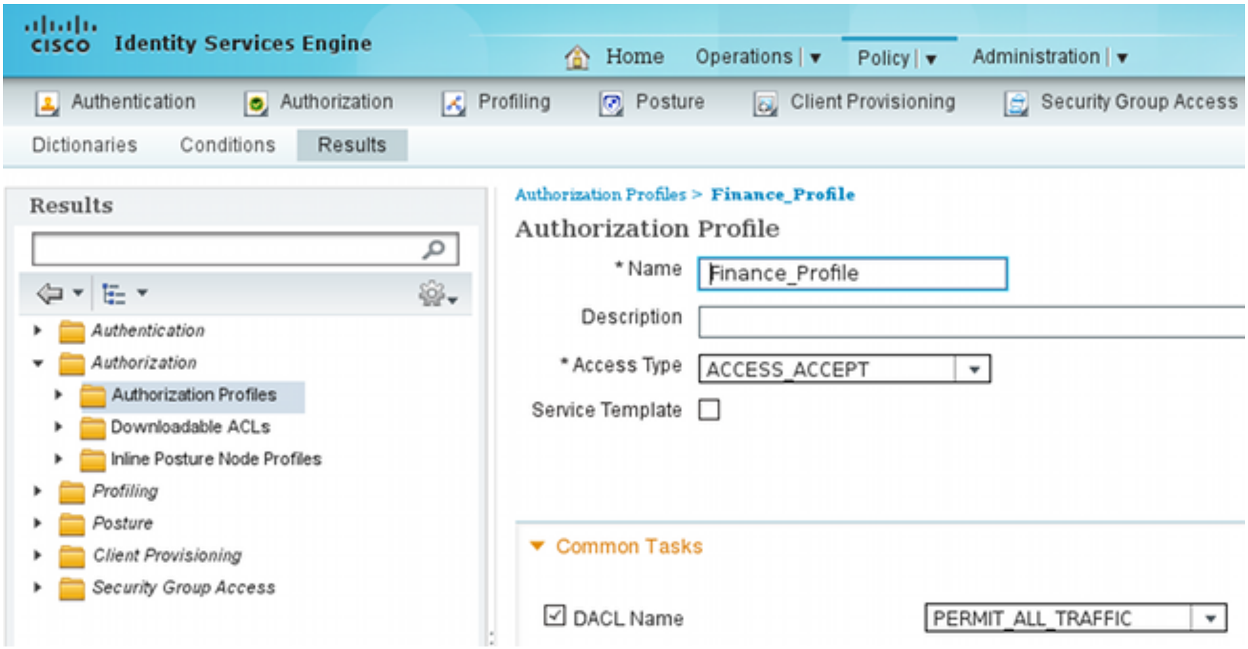
VPN user 'cisco' is assigned to the Finance team, which is allowed to initiate an Internet Control Message Protocol (ICMP) connection to the Marketing team. VPN user 'cisco2' is assigned to the Marketing team, which is not allowed to initiate any connections.



ISE Configuration

1. Choose ***Administration*** > ***Identity Management*** > ***Identities*** in order to add and configure the user 'cisco' (from Finance) and 'cisco2' (from Marketing).
2. Choose ***Administration*** > ***Network Resources*** > ***Network Devices*** in order to add and configure the ASA as a network device.
3. Choose ***Policy*** > ***Results*** > ***Authorization*** > ***Authorization Profiles*** in order to add and configure the Finance and Marketing authorization profiles.

   Both profiles include just one attribute, Downloadable Access Control List (DACL), that permits all traffic. An example for Finance is shown here:



Authorization Profiles > Finance_Profile

Authorization Profile

* Name: Finance_Profile

Description:

* Access Type: ACCESS_ACCEPT

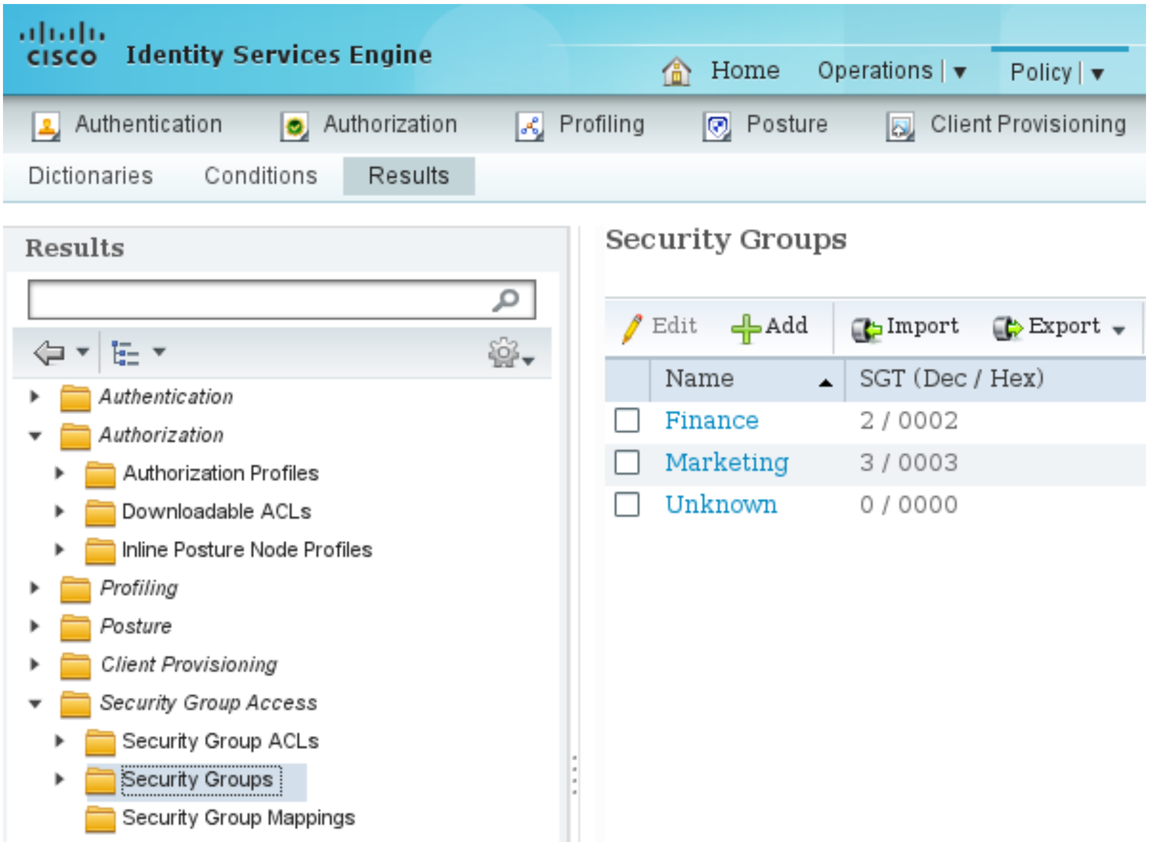
Service Template ☐

Common Tasks

☑ DACL Name: PERMIT_ALL_TRAFFIC

Each profile could have a specific, restrictive DACL, but for this scenario all traffic is allowed. Enforcement is performed by the SGFW, not the DACL assigned to each VPN session. Traffic that is filtered with a SGFW allows for the use of just SGTs instead of IP addresses used by DACL.

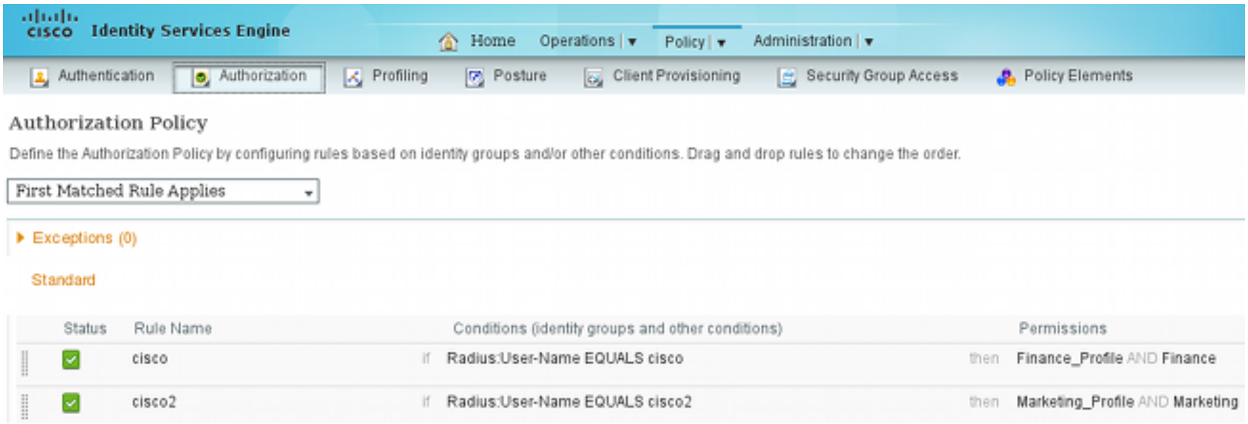
4. Choose ***Policy*** > ***Results*** > ***Security Group Access*** > ***Security Groups*** in order to add and configure the Finance and Marketing SGT groups.



Security Groups

	Name	SGT (Dec / Hex)
☐	Finance	2 / 0002
☐	Marketing	3 / 0003
☐	Unknown	0 / 0000

5. Choose ***Policy*** > ***Authorization*** in order to configure the two authorization rules. The first rule assigns the Finance_profile (DACL that permits whole traffic) along with the SGT group Finance to the 'cisco' user. The second rule assigns the Marketing_profile (DACL that permits whole traffic) along with the SGT group Marketing to the 'cisco2' user.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	cisco	if	Radius:User-Name EQUALS cisco	then	Finance_Profile AND Finance
✓	cisco2	if	Radius:User-Name EQUALS cisco2	then	Marketing_Profile AND Marketing

ASA Configuration

1. Complete the basic VPN configuration.

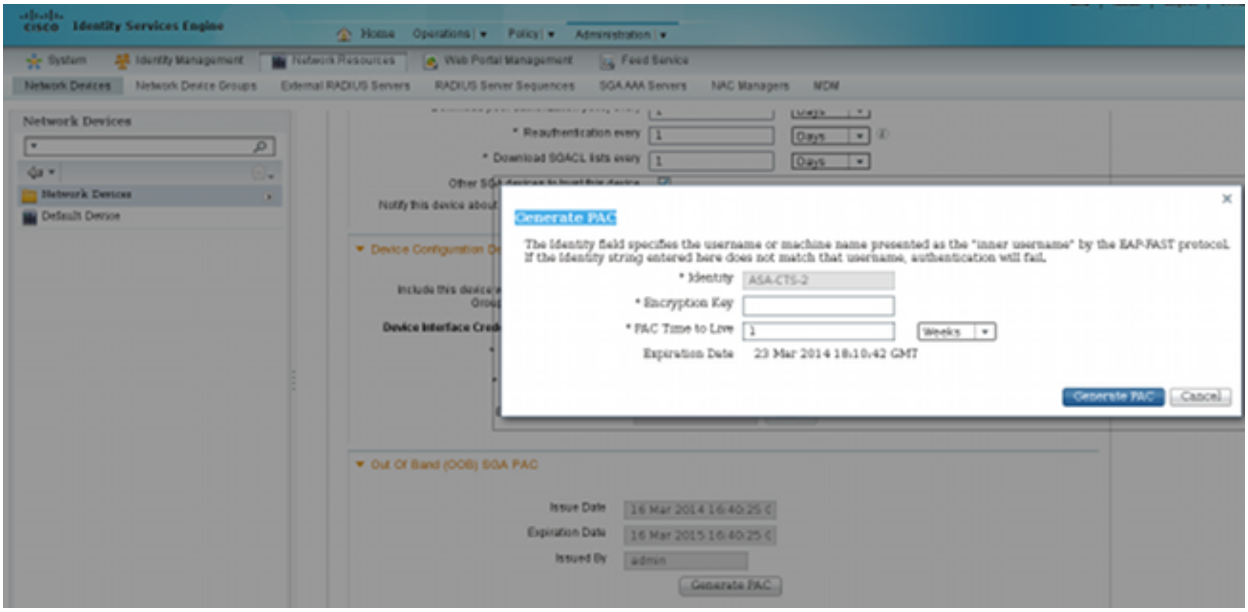
```
webvpn
 enable outside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

group-policy GP-SSL internal
group-policy GP-SSL attributes
 vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group ISE
 accounting-server-group ISE
 default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
 group-alias RA enable

ip local pool POOL 10.10.10.10-10.10.10.100 mask 255.255.255.0
```

2. Complete the ASA AAA and TrustSec configuration.

```
aaa-server ISE protocol radius
aaa-server ISE (outside) host 10.48.66.74
 key *****
cts server-group ISE
```

   In order to join the TrustSec cloud, the ASA needs to authenticate with Protected Access Credential (PAC). The ASA does not support automatic PAC provisioning, which is why that file needs to be manually generated on the ISE and imported to the ASA.

3. Choose ***Administration*** > ***Network Resources*** > ***Network Devices*** > ***ASA*** > ***Advanced TrustSec Settings*** in order to generate a PAC on the ISE. Choose ***Out of Band (OOB) PAC*** provisioning in order to generate the file.



* Reauthentication every: 1 Days
* Download SGACL lists every: 1 Days
Other SGA devices to trust this device
Notify this device about

Generate PAC

The Identity field specifies the username or machine name presented as the "inner username" by the EAP-FAST protocol. If the Identity string entered here does not match that username, authentication will fail.

* Identity: ASA-CTS-2
* Encryption Key:
* PAC Time to Live: 1 Weeks
Expiration Date: 23 Mar 2014 18:10:42 GMT

Out Of Band (OOB) SGA PAC

Issue Date: 16 Mar 2014 16:40:25 C
Expiration Date: 16 Mar 2015 16:40:25 C
Issued By: admin

4. Import the PAC to the ASA.

   The generated file could be put on an HTTP/FTP server. The ASA uses that to import the file.

```
ASA# cts import-pac http://192.168.111.1/ASA-CTS-2.pac password 12345678
!PAC Imported Successfully
ASA#
ASA# show cts pac

  PAC-Info:
    Valid until: Mar 16 2015 17:40:25
    AID:         ea48096688d96ef7b94c679a17bdad6f
    I-ID:        ASA-CTS-2
    A-ID-Info:   Identity Services Engine
    PAC-type:    Cisco Trustsec
  PAC-Opaque:
    000200b80003000100040010ea48096688d96ef7b94c679a17bdad6f0006009c000301
    0015e3473e728ae73cc905887bdc8d3cee00000013532150cc00093a8064f7ec374555
    e7b1fd5abccb17de31b9049066f1a791e87275b9dd10602a9cb4f841f2a7d98486b2cb
    2b5dc3449f67c17f64d12d481be6627e4076a2a63d642323b759234ab747735a03e01b
    99be241bb1f38a9a47a466ea64ea334bf51917bd9aa9ee3cf8d401dc39135919396223
    11d8378829cc007b91ced9117a
```

   When you have the correct PAC, the ASA automatically performs an environment refresh. This downloads information from the ISE about current SGT groups.

```
ASA# show cts environment-data sg-table

Security Group Table:
Valid until: 17:48:12 CET Mar 17 2014
Showing 4 of 4 entries

SG Name                          SG Tag     Type
--------                         ------     -------------
ANY                               65535     unicast
Unknown                               0     unicast
Finance                               2     unicast
Marketing                             3     unicast
```

5. Configure the SGFW. The last step is to configure the ACL on the outside interface which allows for the ICMP traffic from Finance to Marketing.

```
access-list outside extended permit icmp security-group tag 2 any security-group
 tag 3 any
```

```
access-group outside in interface outside
```

Also, the Security Group name could be used instead of the tag.

```
access-list outside extended permit icmp security-group name Finance any
 security-group name Marketing any
```

In order to ensure that the interface ACL processes VPN traffic, it is necessary to disable the option that by default permits VPN traffic without validation via the interface ACL.

```
no sysopt connection permit-vpn
```

Now the ASA should be ready to classify VPN users and perform enforcement based on SGTs .

Verify

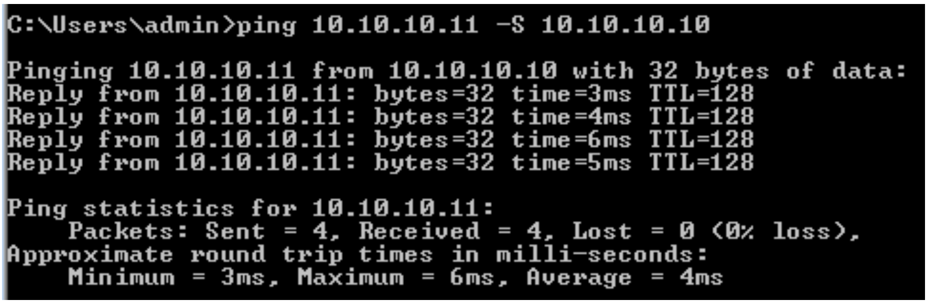
Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) supports certain ***show*** commands. Use the Output Interpreter Tool in order to view an analysis of ***show*** command output.

After the VPN is established, the ASA presents an SGT applied to each session.

```
ASA(config)# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 1
Assigned IP  : 10.10.10.10            Public IP    : 192.168.10.68
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 35934                  Bytes Rx     : 79714
Group Policy : GP-SSL                 Tunnel Group : RA
Login Time   : 17:49:15 CET Sun Mar 16 2014
Duration     : 0h:22m:57s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a8700a000010005325d60b
Security Grp : 2:Finance

Username     : cisco2                 Index        : 2
Assigned IP  : 10.10.10.11            Public IP    : 192.168.10.80
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 86171                  Bytes Rx     : 122480
Group Policy : GP-SSL                 Tunnel Group : RA
Login Time   : 17:52:27 CET Sun Mar 16 2014
Duration     : 0h:19m:45s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a8700a000020005325d6cb
Security Grp : 3:Marketing
```

The SGFW allows for ICMP traffic from Finance (SGT=2) to Marketing (SGT=3). That is why user 'cisco' can ping user 'cisco2'.



```
C:\Users\admin>ping 10.10.10.11 -S 10.10.10.10

Pinging 10.10.10.11 from 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.11: bytes=32 time=3ms TTL=128
Reply from 10.10.10.11: bytes=32 time=4ms TTL=128
Reply from 10.10.10.11: bytes=32 time=6ms TTL=128
Reply from 10.10.10.11: bytes=32 time=5ms TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 4ms
```

The counters increase:

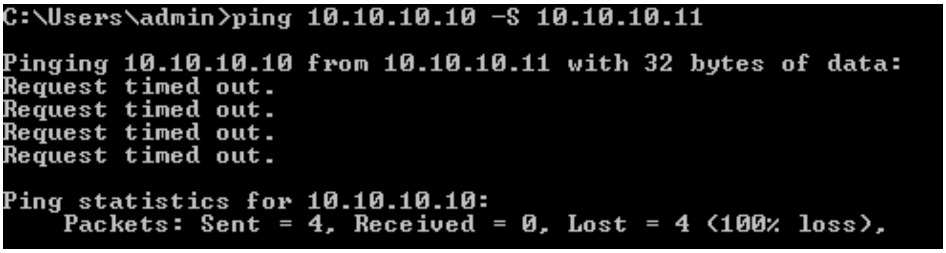
```
ASA(config)# show access-list outside
access-list outside; 1 elements; name hash: 0x1a47dec4
access-list outside line 1 extended permit icmp security-group
 tag 2(name="Finance") any security-group tag 3(name="Marketing")
 any (hitcnt=4) 0x071f07fc
```

The connection has been created:

```
Mar 16 2014 18:24:26: %ASA-6-302020: Built inbound ICMP connection for
 faddr 10.10.10.10/1(LOCAL\cisco, 2:Finance) gaddr 10.10.10.11/0
 laddr 10.10.10.11/0(LOCAL\cisco2, 3:Marketing) (cisco)
```

Return traffic is automatically accepted, because ICMP inspection is enabled.

When you try to ping from Marketing (SGT=3) to Finance (SGT=2):



```
C:\Users\admin>ping 10.10.10.10 -S 10.10.10.11

Pinging 10.10.10.10 from 10.10.10.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

ASA reports:

```
Mar 16 2014 18:06:36: %ASA-4-106023: Deny icmp src outside:10.10.10.11(LOCAL\cisco2,
 3:Marketing) dst outside:10.10.10.10(LOCAL\cisco, 2:Finance) (type 8, code 0) by
 access-group "outside" [0x0, 0x0]
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

See these documents:

- TrustSec Cloud with 802.1x MACsec on Catalyst 3750X Series Switch Configuration Example
- ASA and Catalyst 3750X Series Switch TrustSec Configuration Example and Troubleshoot Guide

Summary

This article presents a simple example on how to classify VPN users and perform basic enforcement. The SGFW also filters traffic between VPN users and the rest of network. SXP (TrustSec SGT Exchange Protocol) can be used on an ASA to obtain the mapping information between IP and SGTs. That allows an

ASA to perform enforcement for all types of sessions which has been properly classified (VPN or LAN).

In ASA software, Version 9.2 and later, the ASA also supports RADIUS Change of Authorization (CoA) (RFC 5176). A RADIUS CoA packet sent from ISE after a successful VPN posture can include cisco−av−pair with a SGT that assigns a compliant user to a different (more secure) group. For more examples, see the articles in the Related Information section.

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***

Updated: May 21, 2014	Document ID: 117694