Clasificación de ASA versión 9.2 VPN SGT y ejemplo de configuración de aplicación

Contenido

Introducción

Este documento describe cómo utilizar una nueva función en la versión 9.2.1 del Adaptive Security Appliance (ASA), la clasificación de TrustSec Security Group Tag (SGT) para usuarios de VPN. Este ejemplo presenta dos usuarios de VPN a los que se ha asignado una SGT y un firewall de grupo de seguridad (SGFW) diferentes, que filtran el tráfico entre los usuarios de VPN.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos sobre la configuración de ASA CLI y la configuración de VPN con Secure Socket Layer (SSL)
- Conocimiento básico de la configuración de VPN de acceso remoto en ASA
- Conocimientos básicos de los servicios Identity Services Engine (ISE) y TrustSec

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

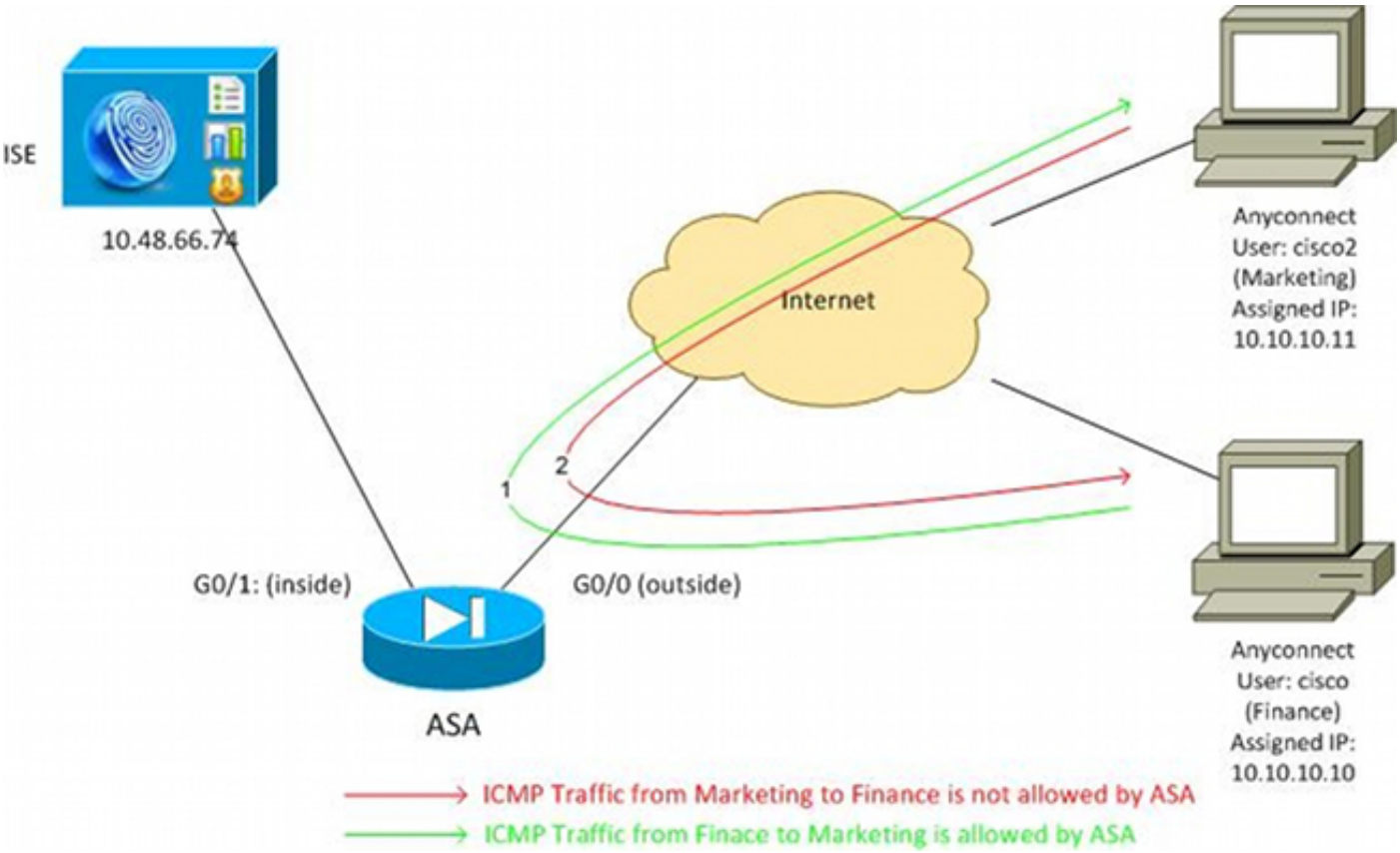
- Software Cisco ASA, versión 9.2 y posteriores
- Windows 7 con Cisco AnyConnect Secure Mobility Client, versión 3.1
- Cisco ISE, versión 1.2 y posteriores

Configurar

> **Nota: Use el Command Lookup Tool (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.**

Diagrama de la red

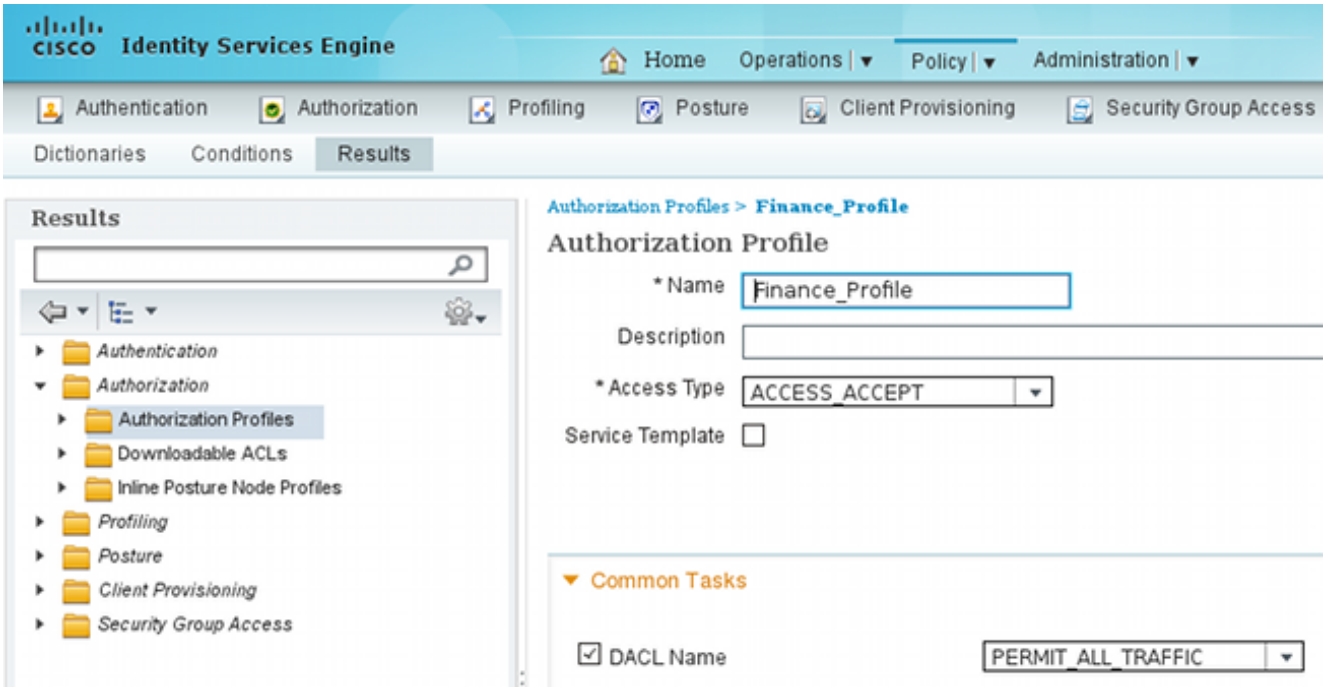
El usuario de VPN 'cisco' está asignado al equipo financiero, que puede iniciar una conexión ICMP (Internet Control Message Protocol) al equipo de marketing. El usuario VPN 'cisco2' está asignado al equipo de marketing, que no puede iniciar ninguna conexión.



Configuración de ISE

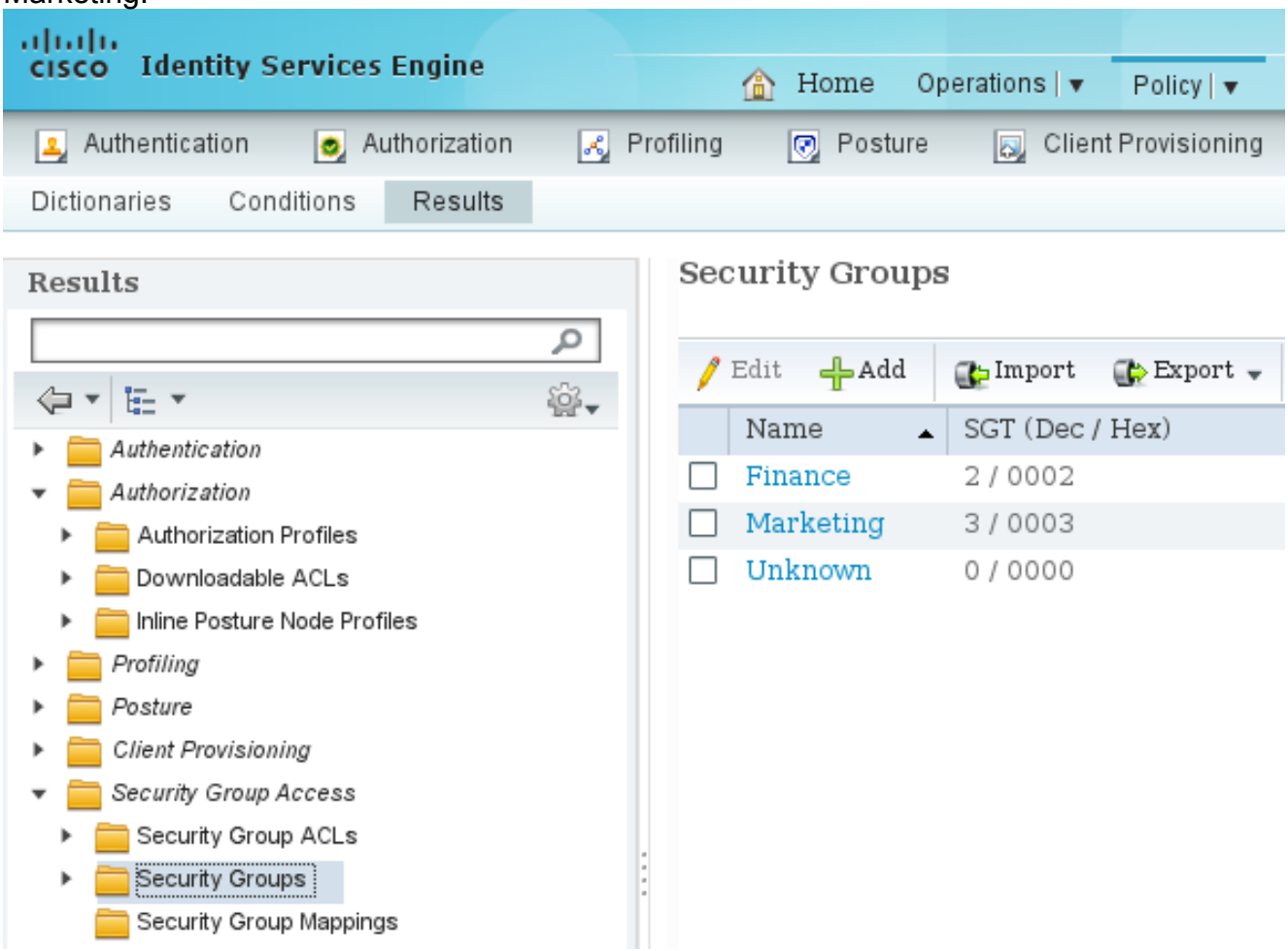
1. Elija **Administration > Identity Management > Identities** para agregar y configurar el usuario 'cisco' (de Finanzas) y 'cisco2' (de Marketing).
2. Elija **Administration > Network Resources > Network Devices** para agregar y configurar el ASA como un dispositivo de red.
3. Elija **Policy > Results > Authorization > Authorization Profiles** para agregar y configurar los perfiles de autorización de Finance and Marketing.Ambos perfiles incluyen un solo atributo, Lista de control de acceso descargable (DACL), que permite todo el tráfico. Aquí se muestra

un ejemplo para
Finance:

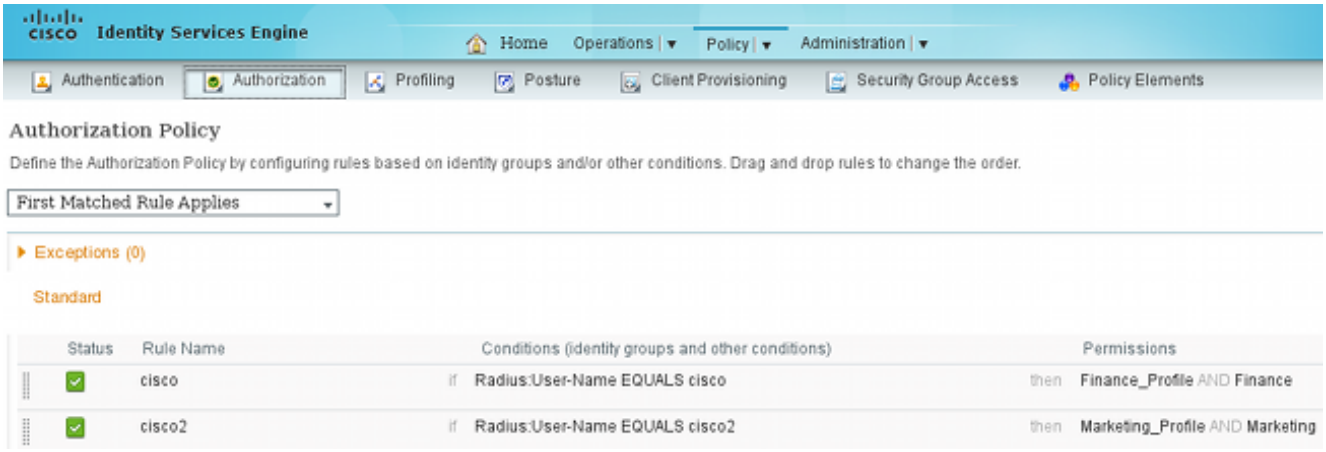


Cada perfil podría tener una DACL específica y restrictiva, pero para este escenario se permite todo el tráfico. La aplicación la realiza el SGFW, no la DACL asignada a cada sesión VPN. El tráfico que se filtra con un SGFW permite el uso de solo SGT en lugar de direcciones IP utilizadas por DACL.

4. Elija **Policy > Results > Security Group Access > Security Groups** para agregar y configurar los grupos SGT de Finanzas y
Marketing.



5. Elija **Policy > Authorization** para configurar las dos reglas de autorización. La primera regla asigna el perfil Finance_Profile (DACL que permite el tráfico completo) junto con el grupo SGT Finance al usuario 'cisco'. La segunda regla asigna el perfil Marketing_Profile (DACL que permite el tráfico completo) junto con el grupo SGT Marketing al usuario 'cisco2'.



Configuración de ASA

1. Complete la configuración básica de VPN.

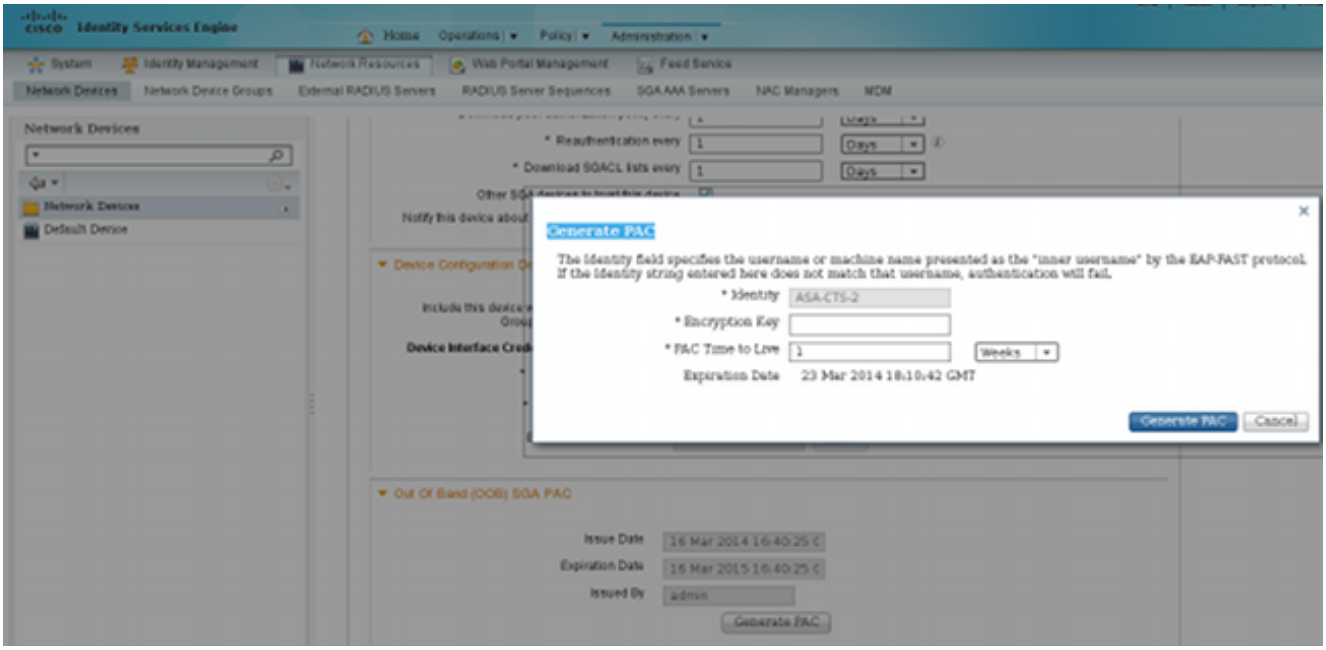
```
webvpn
 enable outside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

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 la configuración de ASA AAA y TrustSec.

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

Para unirse a la nube de TrustSec, ASA debe autenticarse con una credencial de acceso protegido (PAC). El ASA no admite el aprovisionamiento automático de PAC, por lo que ese archivo debe generarse manualmente en el ISE e importarse al ASA.

3. Elija **Administration > Network Resources > Network Devices > ASA > Advanced TrustSec Settings** para generar una PAC en ISE. Elija **Out of Band (OOB) PAC** provisioning para generar el
archivo.



4. Importe la PAC al ASA.El archivo generado se puede colocar en un servidor HTTP/FTP. El ASA utiliza eso para importar el archivo.

```
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
```

Cuando tiene la PAC correcta, ASA realiza automáticamente una actualización del entorno. Esto descarga información de ISE sobre los grupos SGT actuales.

```
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. Configuración del SGFW. El último paso es configurar la ACL en la interfaz externa que permite el tráfico ICMP de Finanzas a Marketing.

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

Además, se podría utilizar el nombre del grupo de seguridad en lugar de la etiqueta.

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

```
security-group name Marketing any
```

Para asegurarse de que la ACL de interfaz procesa el tráfico VPN, es necesario inhabilitar la opción que permite de forma predeterminada el tráfico VPN sin validación a través de la ACL de interfaz.

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

Ahora el ASA debe estar listo para clasificar a los usuarios de VPN y realizar la aplicación basada en SGT .

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Herramienta Output Interpreter (registrado solo para clientes) admite determinados **show** comandos. Utilice la herramienta Output Interpreter Tool para ver un análisis de **show** resultado del comando.

Una vez establecida la VPN, el ASA presenta una SGT aplicada a cada sesión.

```
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
```

El SGFW permite el tráfico ICMP desde Finanzas (SGT=2) hasta Marketing (SGT=3). Es por eso que el usuario 'cisco' puede hacer ping al usuario '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
```

Los contadores aumentan:

```
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
```

Se ha creado la conexión:

```
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)
```

El tráfico de retorno se acepta automáticamente, porque la inspección ICMP está habilitada.

Cuando intenta hacer ping desde Marketing (SGT=3) a Finanzas (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),
```

Informes de ASA:

```
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

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Consulte estos documentos:

- Ejemplo de Configuración de TrustSec Cloud con 802.1x MACsec en Catalyst 3750X Series Switch
- Ejemplo de configuración TrustSec de ASA y el Switch Catalyst Serie 3750X y guía de solución de problemas

Summary

En este artículo se presenta un ejemplo sencillo de cómo clasificar a los usuarios de VPN y realizar la aplicación básica. El SGFW también filtra el tráfico entre los usuarios de VPN y el resto de la red. SXP (protocolo de intercambio de SGT de TrustSec) se puede utilizar en un ASA para obtener la información de asignación entre IP y SGT. Esto permite que un ASA realice la aplicación para todos los tipos de sesiones que se han clasificado correctamente (VPN o LAN).

En el software ASA, versión 9.2 y posterior, ASA también admite cambio de autorización (CoA) RADIUS (RFC 5176). Un paquete RADIUS CoA enviado desde ISE después de una postura VPN exitosa puede incluir un par cisco-av con una SGT que asigna un usuario compatible a un grupo diferente (más seguro). Para obtener más ejemplos, vea los artículos de la sección Información relacionada.

Información Relacionada

- Ejemplo de Configuración de la Postura VPN de ASA Versión 9.2.1 con ISE
- Ejemplo de configuración TrustSec de ASA y el Switch Catalyst Serie 3750X y guía de solución de problemas
- Guía de configuración del switch Cisco TrustSec: Descripción de Cisco TrustSec
- Configuración de un servidor externo para la autorización de usuario de dispositivo de seguridad
- Guía de configuración CLI VPN Cisco Serie ASA, 9.1
- Guía de usuario de Cisco Identity Services Engine, versión 1.2
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).