Esempio di configurazione della classificazione e dell'applicazione ASA VPN SGT versione 9.2

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Configurazione](#)
[Esempio di rete](#)
[Configurazione di ISE](#)
[Configurazione ASA](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Riepilogo](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come utilizzare una nuova funzionalità della classificazione Adaptive Security Appliance (ASA) release 9.2.1, TrustSec Security Group Tag (SGT) per gli utenti VPN. In questo esempio vengono presentati due utenti VPN a cui è stato assegnato un SGT diverso e un firewall del gruppo di sicurezza (SGFW) che filtra il traffico tra gli utenti VPN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base della configurazione di ASA CLI e della configurazione VPN SSL (Secure Sockets Layer)
- Conoscenze base della configurazione VPN di accesso remoto sull'appliance ASA
- Conoscenze base dei servizi Identity Services Engine (ISE) e TrustSec

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

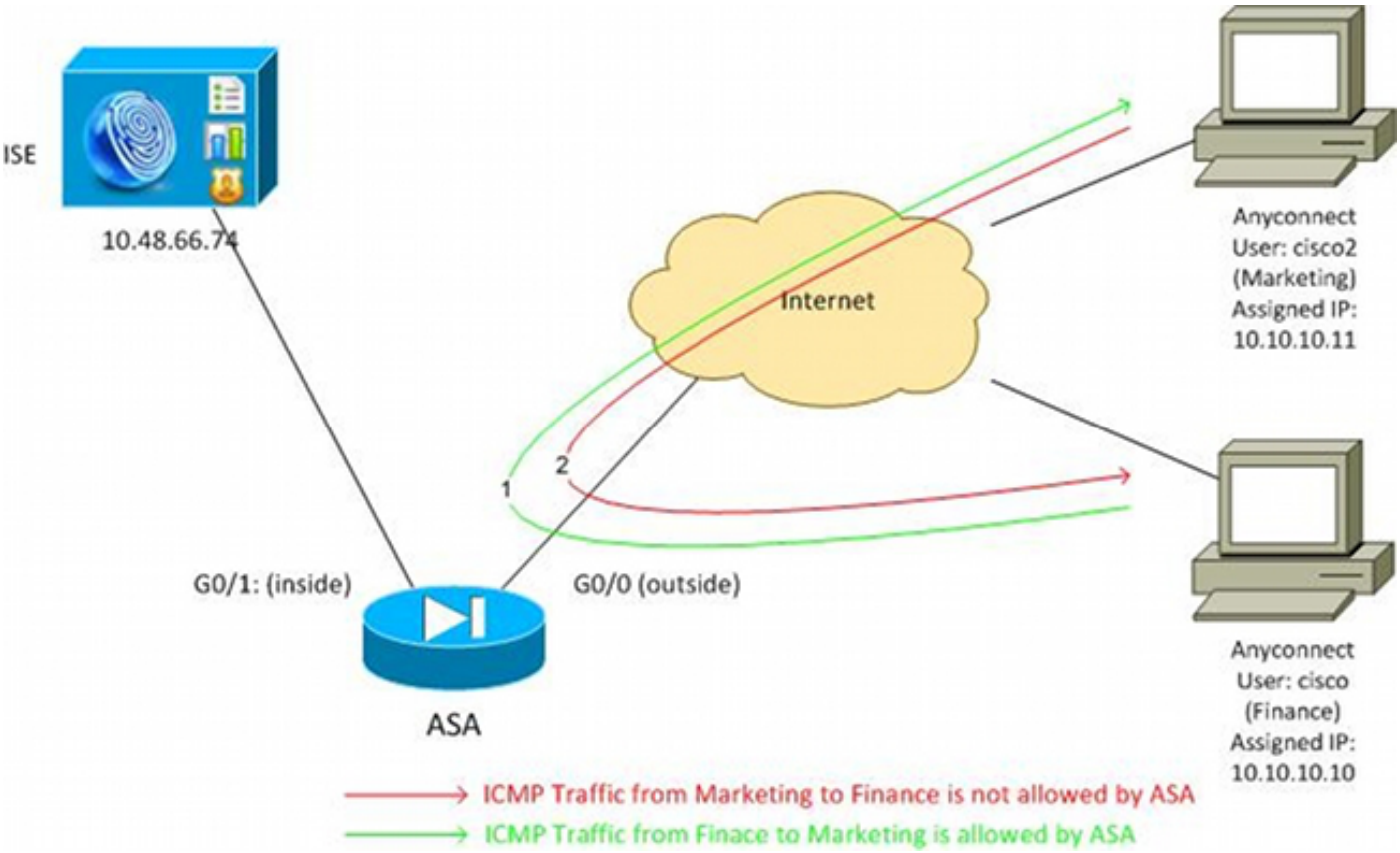
- Software Cisco ASA, versione 9.2 e successive
- Windows 7 con Cisco AnyConnect Secure Mobility Client, versione 3.1
- Cisco ISE versione 1.2 e successive

Configurazione

> **Nota**: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

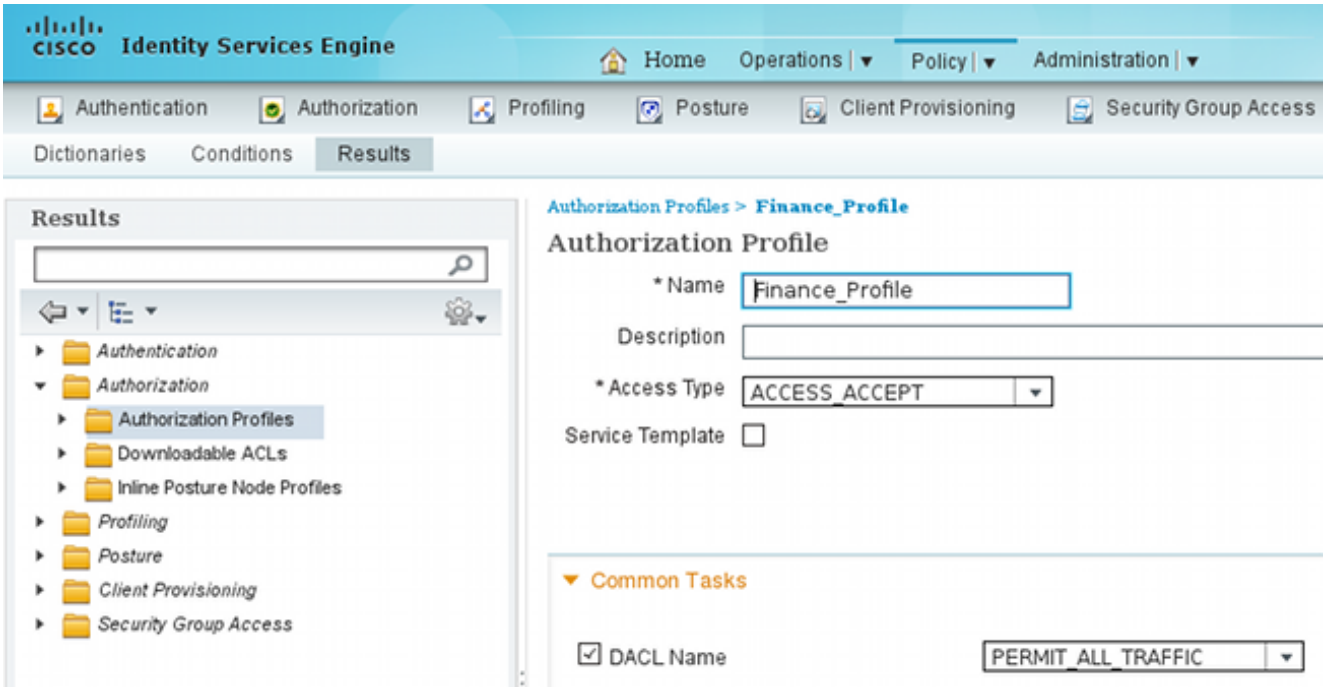
L'utente VPN 'cisco' viene assegnato al team finanziario, che è autorizzato ad avviare una connessione Internet Control Message Protocol (ICMP) al team di marketing. L'utente VPN 'cisco2' è assegnato al team di marketing e non è autorizzato ad avviare connessioni.



Configurazione di ISE

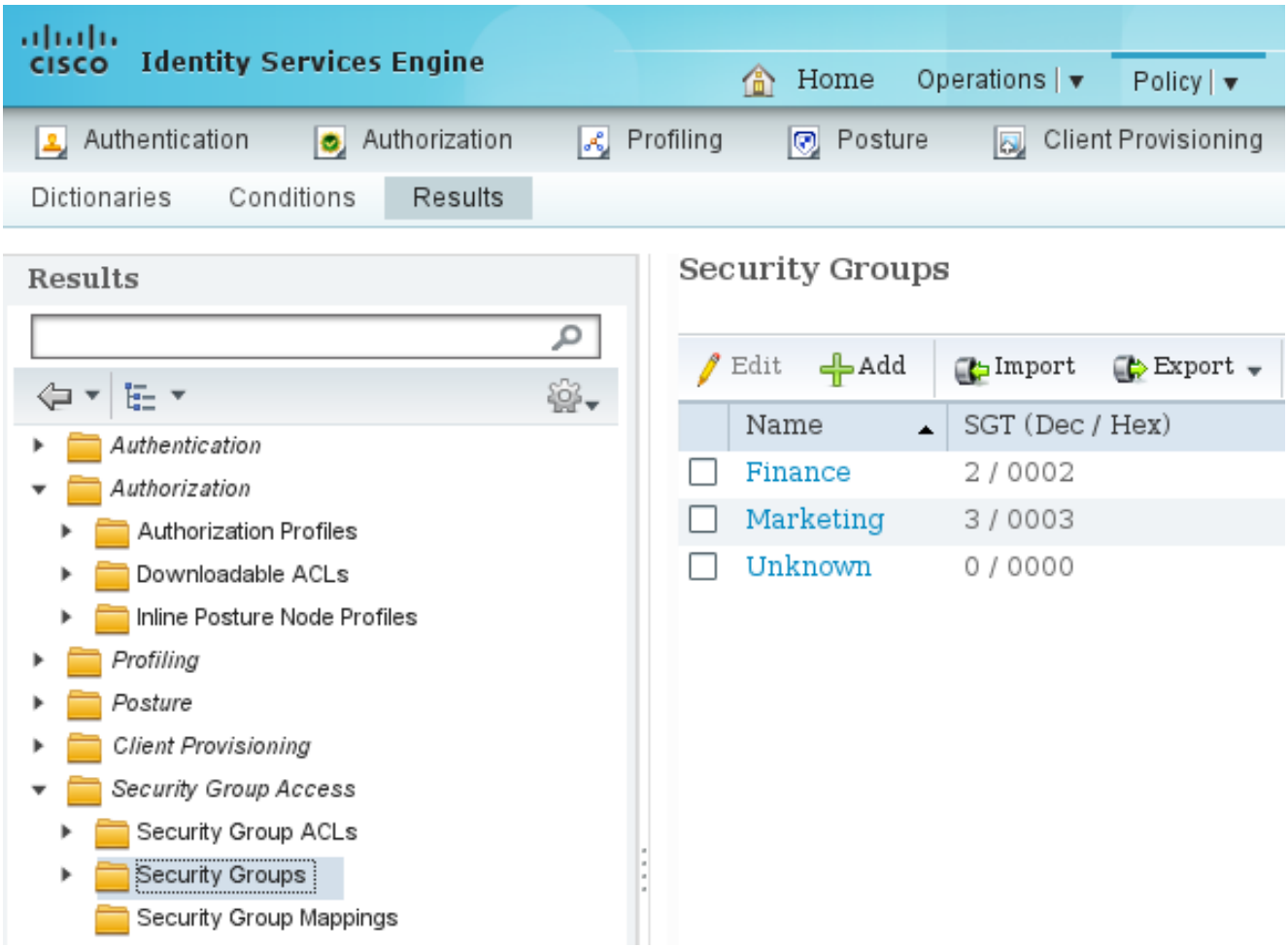
1. Scegliere **Amministrazione > Gestione delle identità > Identità** per aggiungere e configurare l'utente 'cisco' (da Finanza) e 'cisco2' (da Marketing).
2. Per aggiungere e configurare l'ASA come dispositivo di rete, selezionare **Amministrazione > Risorse di rete > Dispositivi di rete**.
3. Per aggiungere e configurare i profili di autorizzazione Finanza e marketing, scegliere **Criteri > Risultati > Autorizzazione** > Profili di autorizzazione.Entrambi i profili includono un solo attributo, DACL (Downloadable Access Control List), che consente tutto il traffico. Di seguito

è riportato un esempio di
Finance:

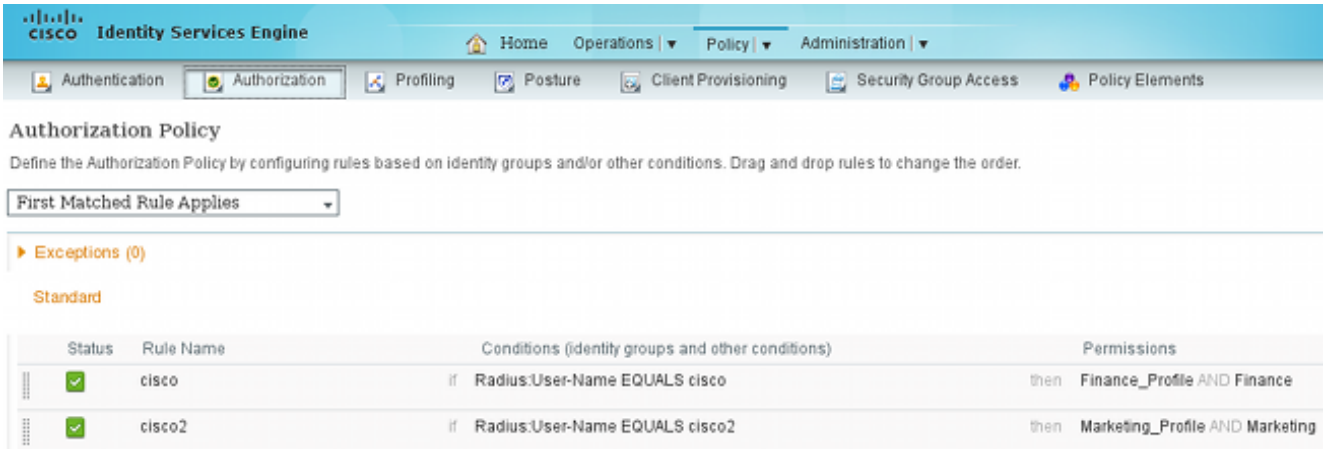


Ogni profilo può avere un DACL specifico e restrittivo, ma per questo scenario tutto il traffico è consentito. L'imposizione viene eseguita dall'SGFW, non dal DACL assegnato a ciascuna sessione VPN. Il traffico filtrato con un SGFW consente l'uso solo di SGT anziché degli indirizzi IP utilizzati da DACL.

4. Per aggiungere e configurare i gruppi SGT per il reparto finanziario e marketing, scegliere **Criteri > Risultati > Accesso al gruppo di sicurezza > Gruppi di sicurezza**.



5. Per configurare le due regole di autorizzazione, scegliere **Criterio > Autorizzazione**. La prima regola assegna il profilo_finanziario (DACL che consente l'intero traffico) insieme al gruppo SGT Finance all'utente 'cisco'. La seconda regola assegna il profilo_marketing (DACL che consente l'intero traffico) insieme al marketing del gruppo SGT all'utente 'cisco2'.



Configurazione ASA

1. Completare la configurazione VPN di base.

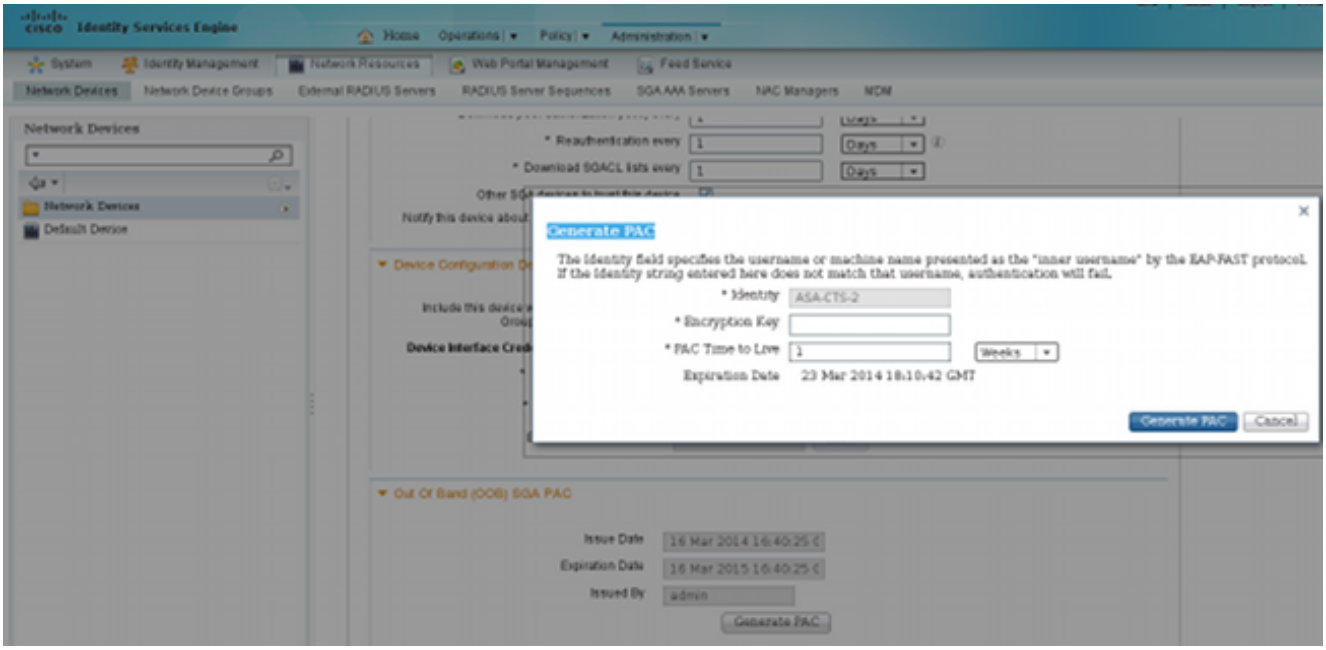
```
webvpn
 enable outside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

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. Completare la configurazione di ASA AAA e TrustSec.

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

Per poter essere aggiunta al cloud TrustSec, l'ASA deve eseguire l'autenticazione con le credenziali di accesso protetto (PAC). L'ASA non supporta la preparazione automatica della PAC, e per questo motivo il file deve essere generato manualmente sull'ISE e importato nell'ASA.

3. Per generare una PAC sull'ISE, scegliere **Amministrazione > Risorse di rete > Dispositivi di rete > ASA > Impostazioni** avanzate TrustSec. Per generare il file, scegliere la preparazione **della PAC fuori banda (OOB)**.



4. Importare la PAC nell'appliance ASA.Il file generato può essere collocato su un server HTTP/FTP. L'appliance ASA lo utilizza per importare il 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
```

Quando la PAC è corretta, l'ASA esegue automaticamente un aggiornamento dell'ambiente. In questo modo vengono scaricate dall'ISE le informazioni sui gruppi SGT correnti.

```
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. Configurare il file SGFW. L'ultimo passaggio consiste nel configurare l'ACL sull'interfaccia esterna, che consente il traffico ICMP tra il reparto finanziario e il reparto marketing.

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

Inoltre, è possibile utilizzare il nome del gruppo di sicurezza al posto del tag.

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

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

Per garantire che l'ACL di interfaccia elabori il traffico VPN, è necessario disabilitare l'opzione che per impostazione predefinita permette il traffico VPN senza convalida tramite l'ACL di interfaccia.

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

A questo punto, l'ASA deve essere pronta per classificare gli utenti VPN ed eseguire l'applicazione sulla base delle SGT.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

OSPF (Open Shortest Path First) Strumento Output Interpreter (registrato solo clienti) supporta determinati **mostrare** comandi. Usare lo strumento Output Interpreter per visualizzare un'analisi **mostrare** output del comando.

Dopo aver stabilito la VPN, l'ASA presenta un SGT applicato a ciascuna sessione.

```
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
```

Il protocollo SGFW consente il traffico ICMP dalla finanza (SGT=2) al marketing (SGT=3). Ecco perché l'utente 'cisco' può eseguire il ping con l'utente '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
```

Aumento contatori:

```
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
```

La connessione è stata creata:

```
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)
```

Il traffico di ritorno viene accettato automaticamente perché è abilitata l'ispezione ICMP.

Quando si tenta di eseguire il ping tra Marketing (SGT=3) e Finanza (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),
```

L'ASA riporta:

```
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]
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Vedere i seguenti documenti:

- Esempio di configurazione di TrustSec Cloud con 802.1x MACsec sugli switch Catalyst serie 3750X
- Esempio di configurazione di ASA e Catalyst serie 3750X Switch TrustSec e guida alla risoluzione dei problemi

Riepilogo

In questo articolo viene illustrato un semplice esempio su come classificare gli utenti VPN ed eseguire l'imposizione di base. L'SGFW filtra anche il traffico tra gli utenti VPN e il resto della rete. SXP (TrustSec SGT Exchange Protocol) può essere utilizzato su un'ASA per ottenere le informazioni di mapping tra IP e SGT. Ciò consente all'ASA di eseguire l'imposizione per tutti i tipi di sessioni correttamente classificate (VPN o LAN).

Nel software ASA versione 9.2 e successive, l'appliance ASA supporta anche la funzionalità RADIUS Change of Authorization (CoA) (RFC 5176). Un pacchetto RADIUS CoA inviato da ISE dopo una postura VPN riuscita può includere cisco-av-pair con un SGT che assegna un utente conforme a un gruppo diverso (più sicuro). Per ulteriori esempi, vedere gli articoli della sezione Informazioni correlate.

Informazioni correlate

- Esempio di postura di VPN con ISE versione 9.2.1 di ASA
- Esempio di configurazione di ASA e Catalyst serie 3750X Switch TrustSec e guida alla risoluzione dei problemi
- Guida alla configurazione dello switch Cisco TrustSec: informazioni su Cisco TrustSec
- Configurazione di un server esterno per l'autorizzazione utente di Security Appliance
- Guida alla configurazione di Cisco ASA VPN CLI, 9.1
- Guida dell'utente di Cisco Identity Services Engine, versione 1.2
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).