ASA versie 9.2 Configuratie-voorbeeld van VPN SGT-classificatie en -handhaving

Inhoud

Inleiding

Dit document beschrijft hoe u een nieuwe functie kunt gebruiken in release 9.2.1 van de adaptieve security applicatie (ASA) en in de classificatie van TrustSec Security Group Tag (SGT) voor VPN-gebruikers. Dit voorbeeld geeft twee VPN-gebruikers weer die een andere SGT en Security Group Firewall (SGFW) hebben toegewezen, waarmee het verkeer tussen de VPN-gebruikers wordt gefilterd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van ASA CLI-configuratie en Secure Socket Layer (SSL) VPN-configuratie
- Basiskennis van de configuratie van VPN voor externe toegang op de ASA
- Basiskennis van Identity Services Engine (ISE) en TrustSec-services

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

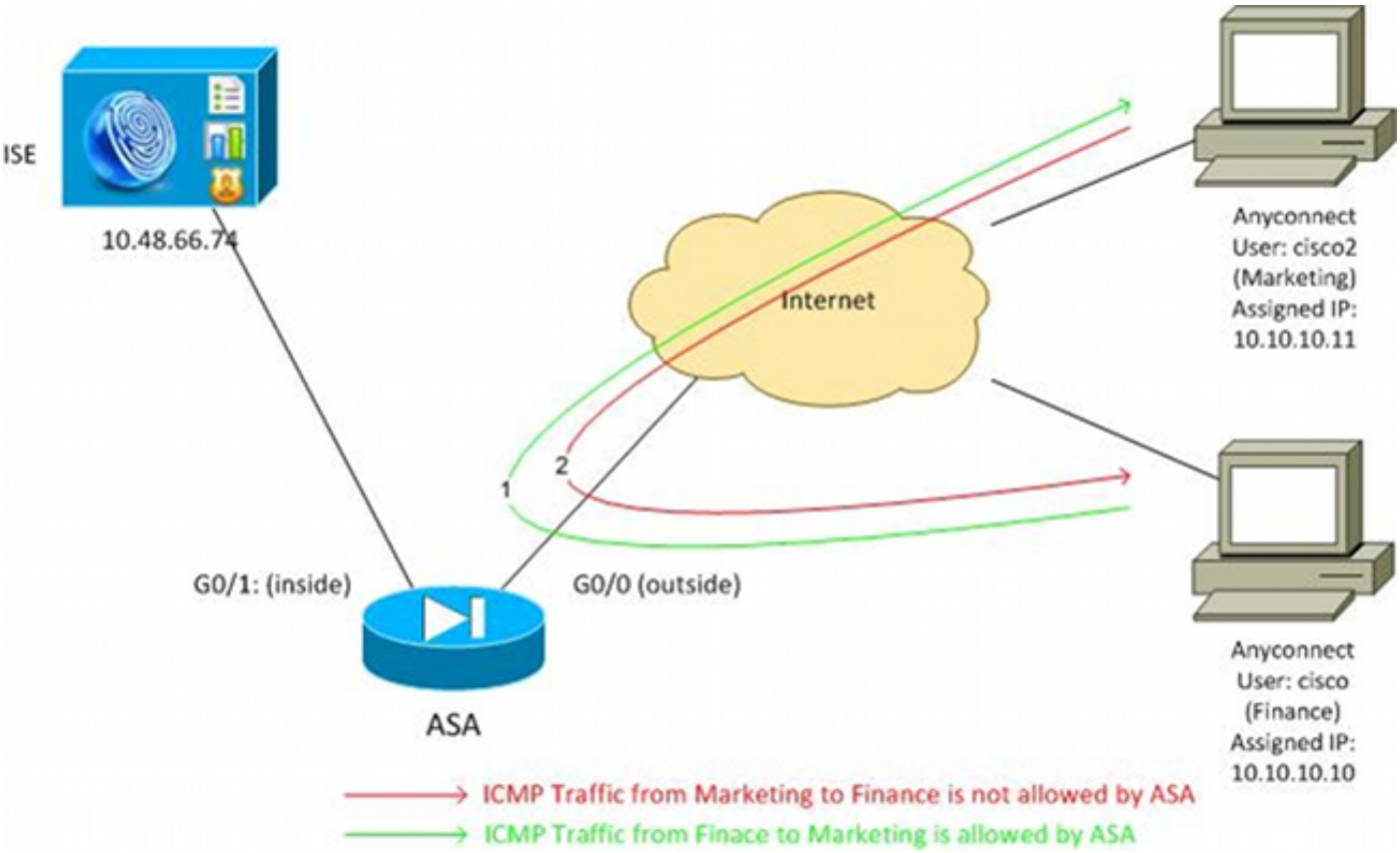
- Cisco ASA-software, versie 9.2 en hoger
- Windows 7 met Cisco AnyConnect Secure Mobility-client, release 3.1
- Cisco ISE, release 1.2 en hoger

Configureren

> **Opmerking**: Gebruik de Command Lookup Tool (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

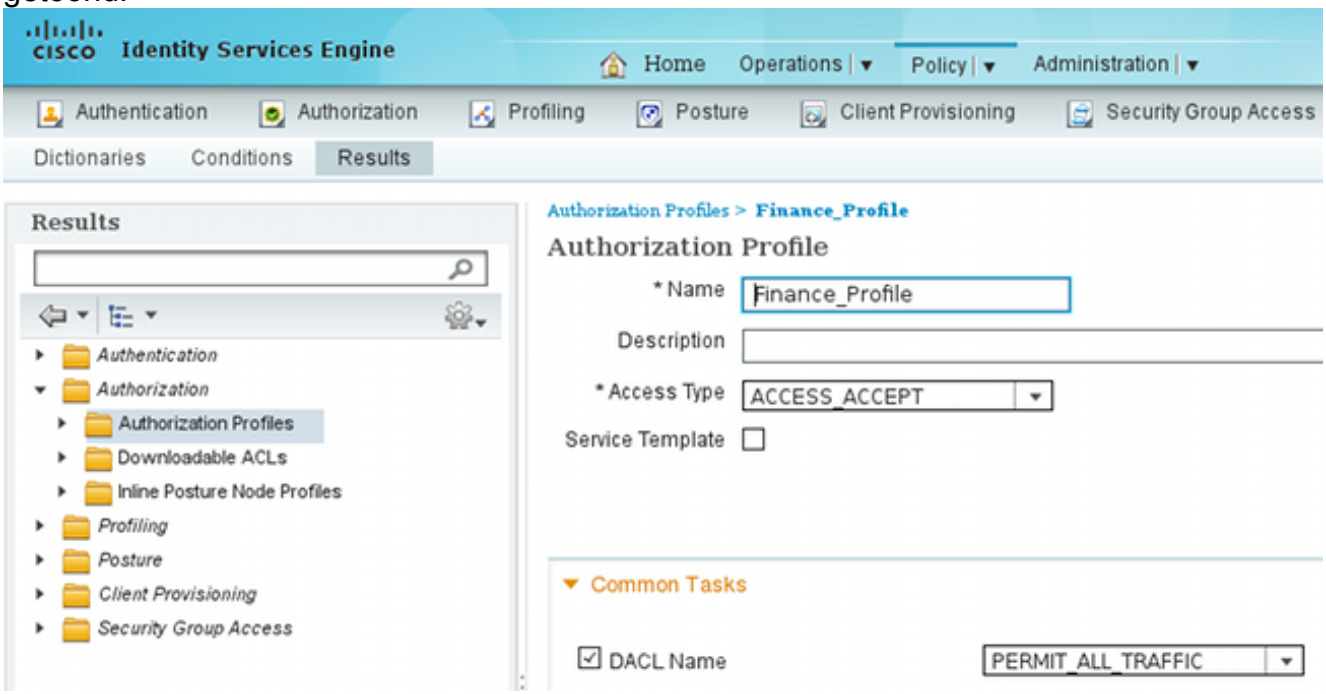
VPN-gebruiker 'cisco' wordt toegewezen aan het Finance-team, dat een ICMP-verbinding (Internet Control Message Protocol) met het marketingteam mag starten. VPN-gebruiker 'cisco2' wordt toegewezen aan het marketingteam, dat geen verbindingen mag initiëren.



ISE-configuratie

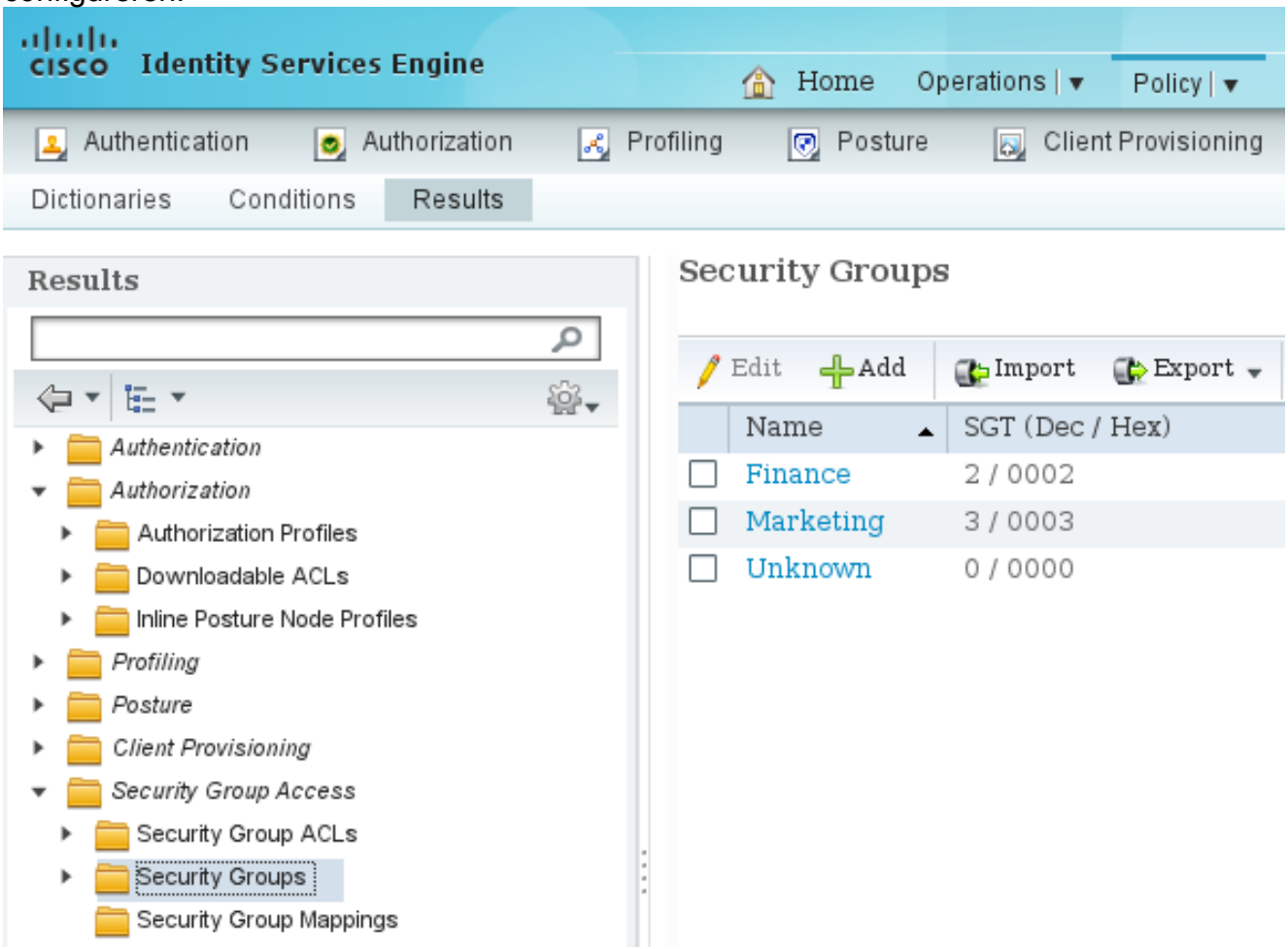
1. Kies **Beheer > Identity Management > Identiteiten** om de gebruiker 'cisco' (van Finance) en 'cisco2' (van Marketing) toe te voegen en te configureren.
2. Kies **Beheer > Netwerkbronnen > Netwerkapparaten** om de ASA als netwerkapparaat toe te voegen en te configureren.
3. Kies **Beleid > Resultaten > Vergunning > Vergunningsprofielen** om de de vergunningsprofielen van Financiën en van de Marketing toe te voegen en te vormen.Beide profielen bevatten slechts één kenmerk, de DACL (Downloadable Access Control List), dat al

het verkeer toestaat. Hier wordt een voorbeeld voor Finance getoond:

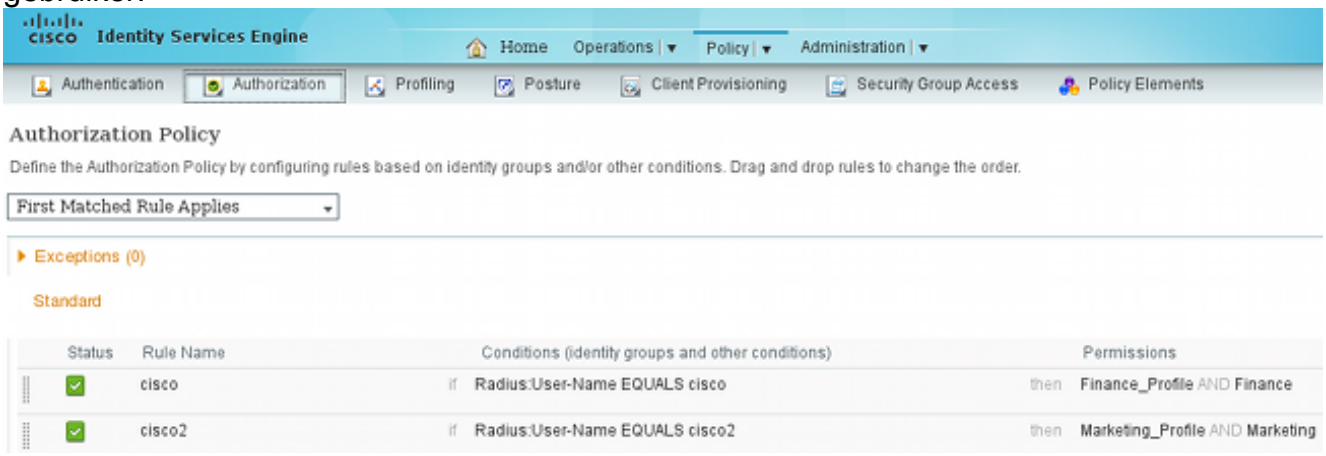


Elk profiel kon een specifieke, beperkende DACL hebben, maar voor dit scenario is al het verkeer toegestaan. Handhaving wordt uitgevoerd door de SGFW en niet door de DACL die aan elke VPN-sessie is toegewezen. Verkeer dat met een SGFW wordt gefilterd, maakt het gebruik van alleen SGT's mogelijk in plaats van IP-adressen die door DACL worden gebruikt.

4. Kies **Beleid > Resultaten > Beveiligingsgroeptoegang > Beveiligingsgroepen** om de Finance and Marketing SGT-groepen toe te voegen en te configureren.



5. Kies **Beleid > Autorisatie** om de twee autorisatieregels te configureren. De eerste regel wijst het Finance_profile (DACL die heel verkeer toestaat) samen met de SGT groep Finance toe aan de 'cisco' gebruiker. De tweede regel wijst het Marketing_profile (DACL die heel verkeer toestaat) samen met de SGT groep Marketing toe aan de 'cisco2' gebruiker.



ASA-configuratie

1. Voltooi de basisVPN configuratie.

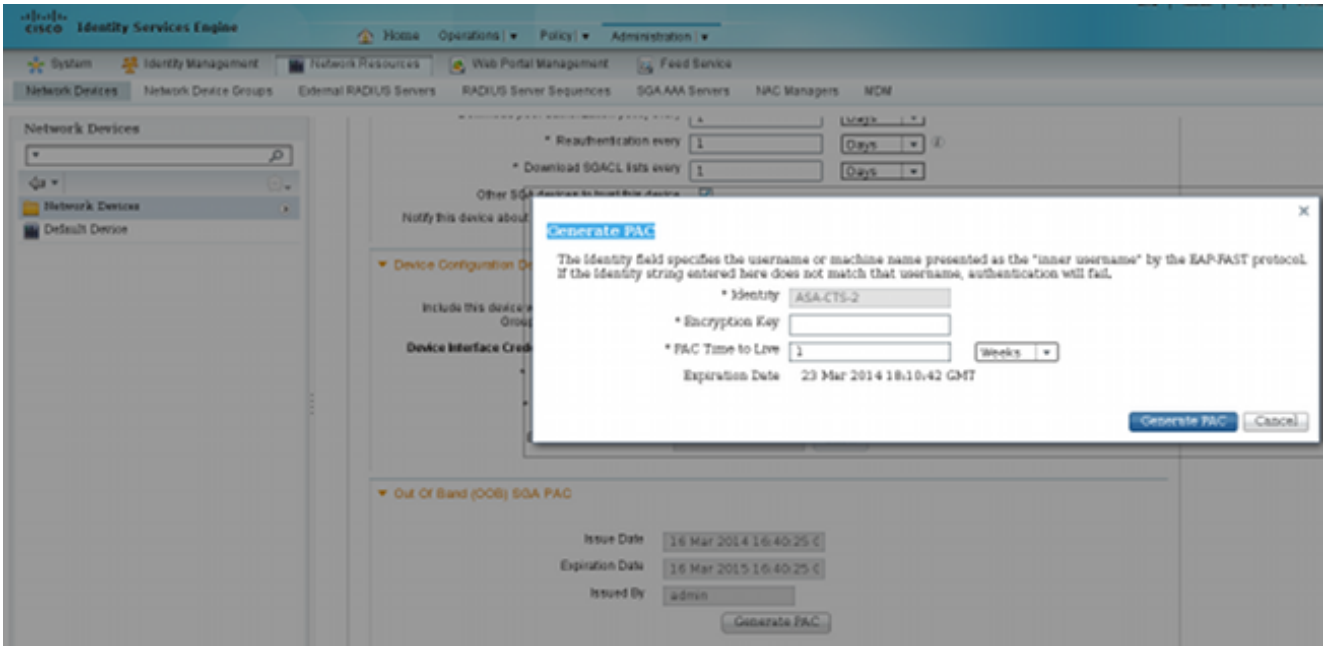
```
webvpn
 enable outside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

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. Voltooi de ASA AAA- en TrustSec-configuratie.

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

Om zich aan te sluiten bij de TrustSec-cloud, moet de ASA authenticeren met Protected Access Credential (PAC). De ASA ondersteunt geen automatische PAC-provisioning, daarom moet dat bestand handmatig op de ISE worden gegenereerd en in de ASA worden geïmporteerd.

3. Kies **Beheer > Netwerkbronnen > Netwerkapparaten > ASA > Geavanceerde TrustSec-instellingen** om een PAC op de ISE te genereren. Kies **uit band (OOB) PAC** levering om het bestand te genereren.



4. Importeer de AKP in de ASA.Het gegenereerde bestand kan op een HTTP-/FTP-server worden gezet. ASA gebruikt dat om het bestand te importeren.

```
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
```

Wanneer u de juiste PAC hebt, voert de ASA automatisch een omgevingsvernieuwing uit. Dit downloadt informatie van de ISE over de huidige SGT-groepen.

```
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. Configureer de SGFW. De laatste stap is het configureren van de ACL op de buiteninterface die het ICMP-verkeer van Financiën naar Marketing mogelijk maakt.

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

Ook kan de naam Security Group worden gebruikt in plaats van de tag.

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

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

Om ervoor te zorgen dat de interface-ACL VPN-verkeer verwerkt, is het nodig om de optie uit te schakelen die standaard VPN-verkeer zonder validatie via de interface-ACL toestaat.

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

Nu zou ASA bereid moeten zijn om VPN-gebruikers te classificeren en handhaving uit te voeren op basis van SGT's .

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Het Uitvoer-tolk (ingeschreven klanten) ondersteunt bepaalde **tonen** opdrachten. Gebruik het Hulpmiddel van de Tolk van de Output om een analyse van te bekijken **tonen** opdrachtoutput.

Nadat VPN is opgezet, stelt de ASA een SGT voor die op elke sessie wordt toegepast.

```
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
```

SGFW staat voor verkeer ICMP van Financiën (SGT=2) aan Marketing (SGT=3) toe. Dat is de reden dat gebruiker 'cisco' gebruiker 'cisco2' kan pingen.

```
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
```

De tellers stijgen:

```
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
```

De verbinding is tot stand gebracht:

```
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)
```

Het verkeer van de terugkeer wordt automatisch goedgekeurd, omdat de inspectie ICMP wordt toegelaten.

Wanneer u probeert te pingen van Marketing (SGT=3) naar 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 meldt:

```
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]
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Zie deze documenten:

- TrustSec Cloud met 802.1x MACsec op Catalyst 3750X Series Switch-configuratievoorbeeld
- ASA en Catalyst 3750X Series Switch TrustSec-configuratievoorbeeld en gids voor probleemoplossing

Samenvatting

Dit artikel geeft een eenvoudig voorbeeld van hoe VPN-gebruikers te classificeren en het uitvoeren van eenvoudige handhaving. SGFW filtert ook verkeer tussen VPN-gebruikers en de rest van het netwerk. SXP (TrustSec SGT Exchange Protocol) kan op een ASA worden gebruikt om de mapping-informatie tussen IP en SGT's te verkrijgen. Hiermee kan een ASA handhaving uitvoeren voor alle typen sessies die correct zijn geclassificeerd (VPN of LAN).

In ASA-software, versie 9.2 en hoger, ondersteunt de ASA ook RADIUS-wijziging van autorisatie (CoA) (RFC 5176). Een RADIUS CoA-pakket dat van ISE wordt verzonden na een succesvolle VPN-houding kan cisco-av-paar bevatten met een SGT die een conforme gebruiker aan een andere (veiligere) groep toewijst. Zie de artikelen in het gedeelte Verwante informatie voor meer voorbeelden.

Gerelateerde informatie

- ASA versie 9.2.1 VPN-houding met ISE-configuratievoorbeeld
- ASA en Catalyst 3750X Series Switch TrustSec-configuratievoorbeeld en gids voor probleemoplossing
- Cisco TrustSec Switch-configuratiehandleiding: begrip van Cisco TrustSec
- Gebruikersautorisatie voor een externe server voor security applicatie configureren
- Configuratiehandleiding voor Cisco ASA Series VPN CLI, 9.1
- Gebruikershandleiding voor Cisco Identity Services Engine, release 1.2
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.