# ASA Version 9.2 VPN SGT-Klassifizierung und -Durchsetzung - Konfigurationsbeispiel

## Inhalt



## Einleitung

In diesem Dokument wird die Verwendung einer neuen Funktion der Adaptive Security Appliance (ASA) Version 9.2.1, TrustSec Security Group Tag (SGT)-Klassifizierung für VPN-Benutzer beschrieben. Dieses Beispiel zeigt zwei VPN-Benutzer, denen ein anderes SGT und eine Security Group Firewall (SGFW) zugewiesen wurde, die den Datenverkehr zwischen den VPN-Benutzern filtert.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der ASA CLI-Konfiguration und der SSL VPN-Konfiguration (Secure Socket Layer)
- Grundkenntnisse der VPN-Konfiguration für Remote-Zugriff auf der ASA
- Grundkenntnisse der Identity Services Engine (ISE) und der TrustSec-Services

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

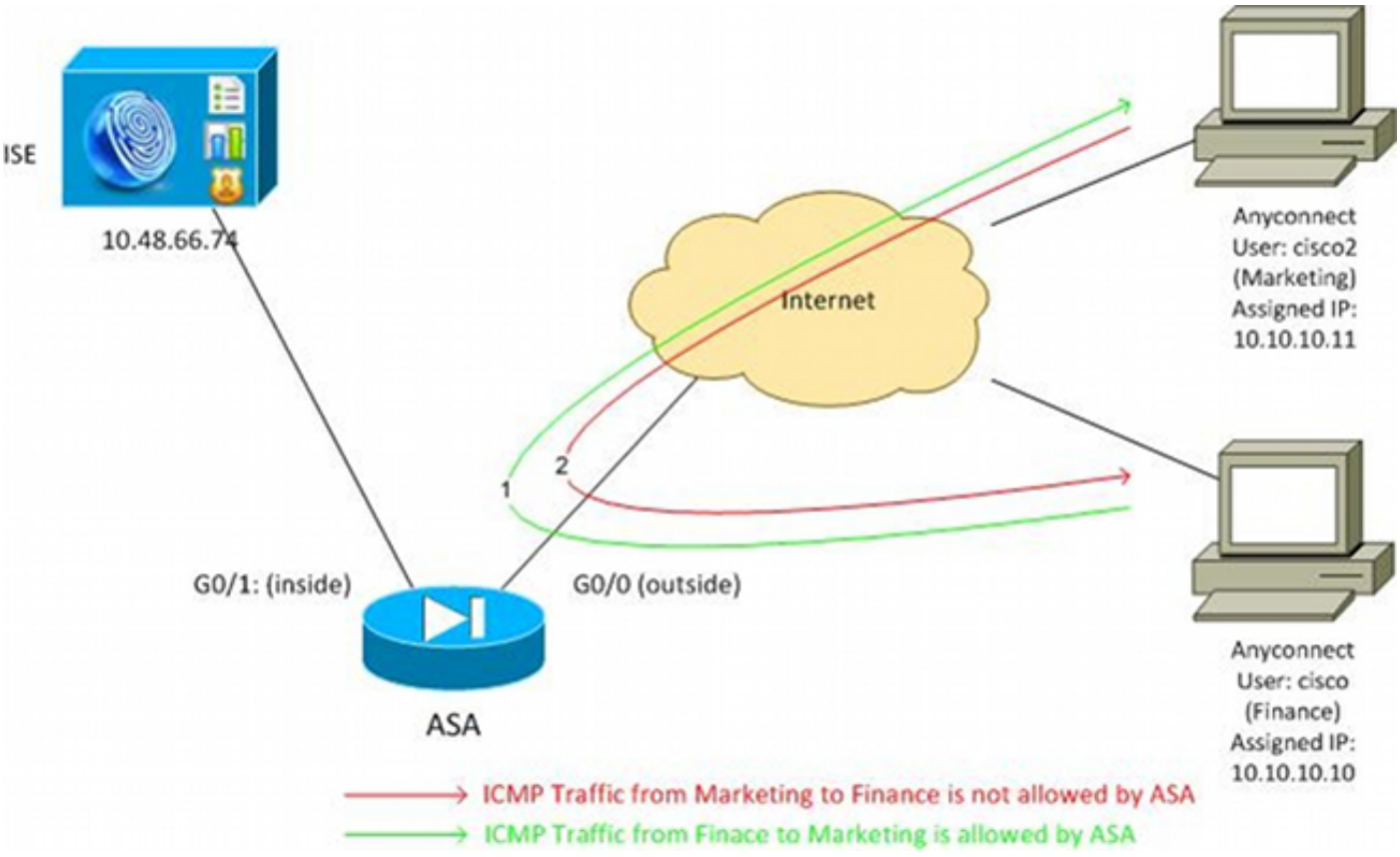
- Cisco ASA Software, Version 9.2 und höher
- Windows 7 mit Cisco AnyConnect Secure Mobility Client, Version 3.1
- Cisco ISE, Version 1.2 und höher

# Konfigurieren

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur für registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

## Netzwerkdiagramm

Der VPN-Benutzer "cisco" wird dem Finanzteam zugewiesen, das eine ICMP-Verbindung (Internet Control Message Protocol) mit dem Marketingteam initiieren kann. Der VPN-Benutzer "cisco2" ist dem Marketingteam zugewiesen, das keine Verbindungen initiieren darf.

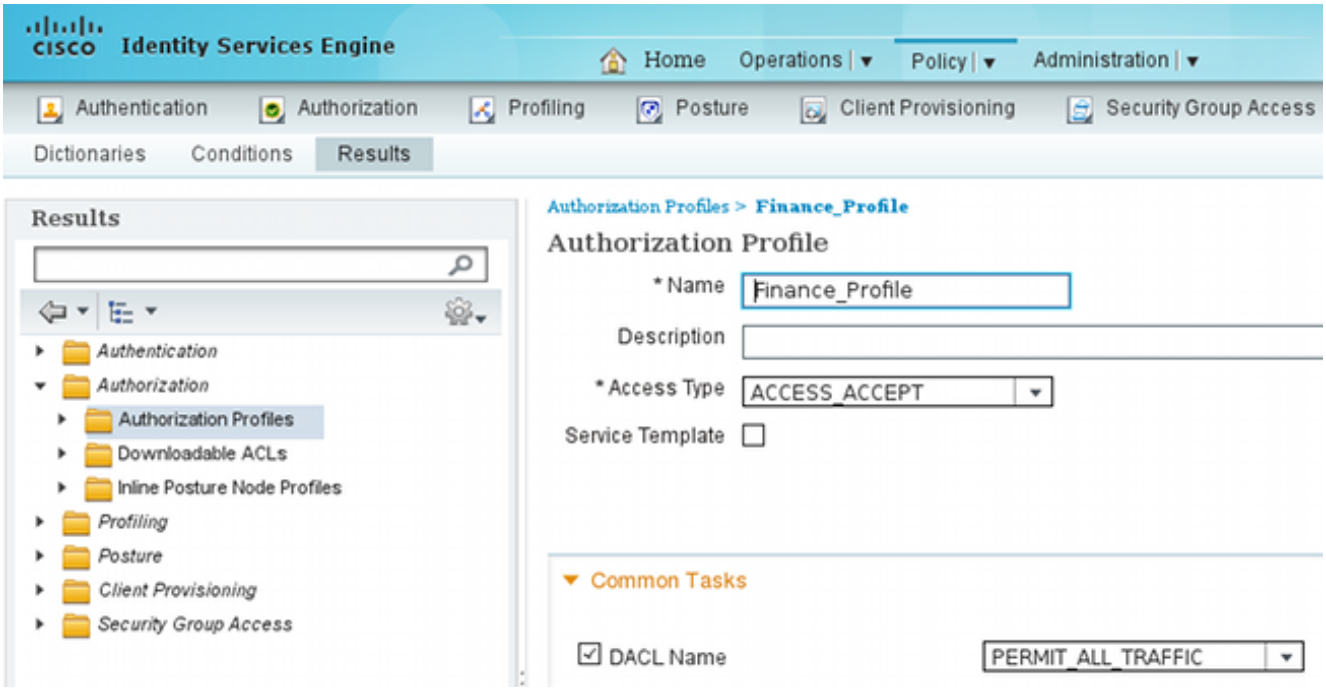



## ISE-Konfiguration

1. Wählen Sie **Administration > Identity Management > Identities,** um den Benutzer "cisco" (aus der Finanzabteilung) und "cisco2" (aus der Marketingabteilung) hinzuzufügen und zu konfigurieren.
2. Wählen Sie **Administration > Network Resources > Network Devices** (Administration > Netzwerkressourcen > Netzwerkgeräte), um die ASA hinzuzufügen und als Netzwerkgerät zu

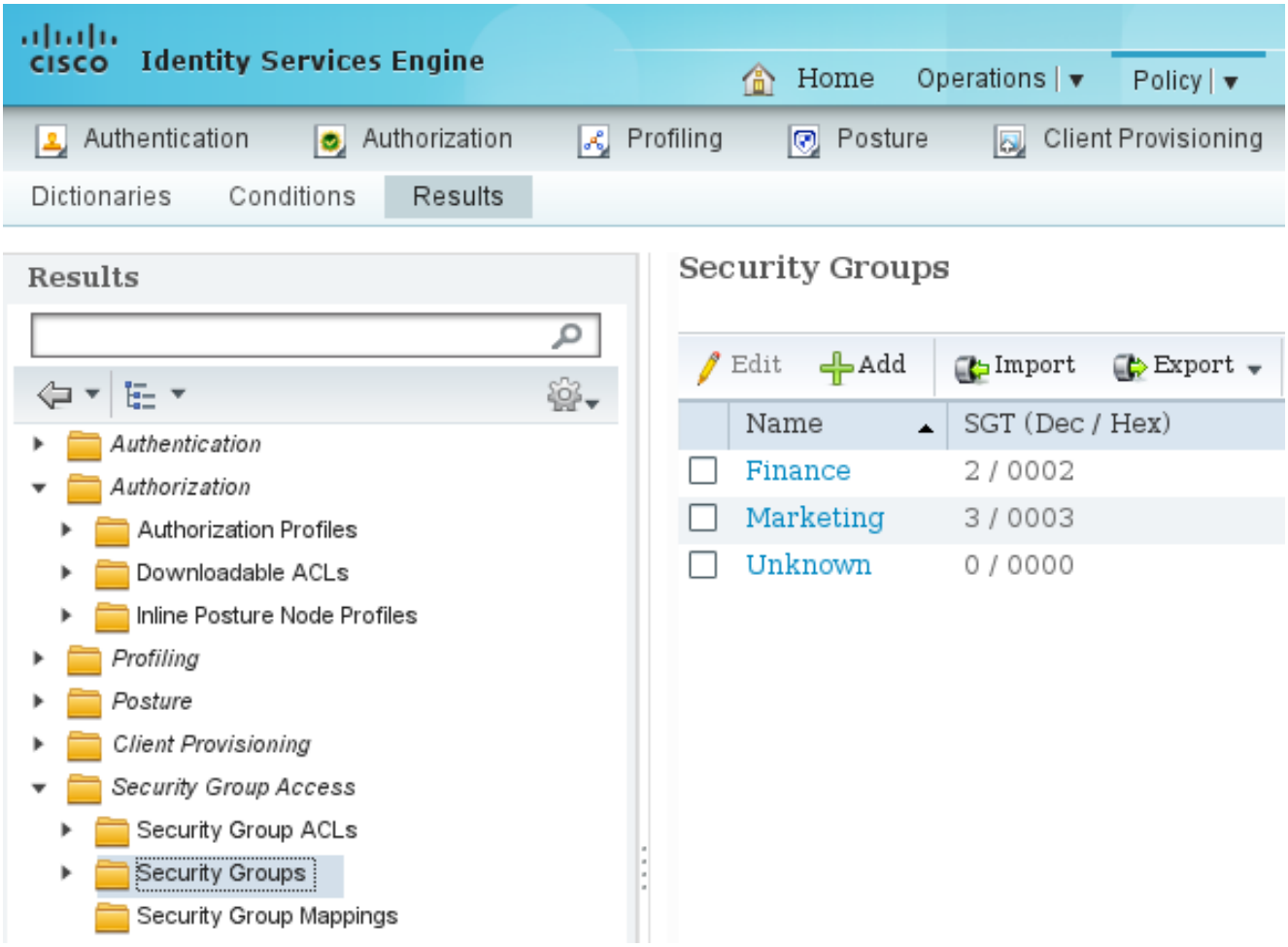
konfigurieren.

3. Wählen Sie **Policy > Results > Authorization > Authorization Profiles,** um die Finance- und Marketing-Autorisierungsprofile hinzuzufügen und zu konfigurieren.Beide Profile enthalten nur ein Attribut, eine herunterladbare Zugriffskontrollliste (DACL), die den gesamten Datenverkehr zulässt. Hier sehen Sie ein Beispiel für die Finanzbranche:

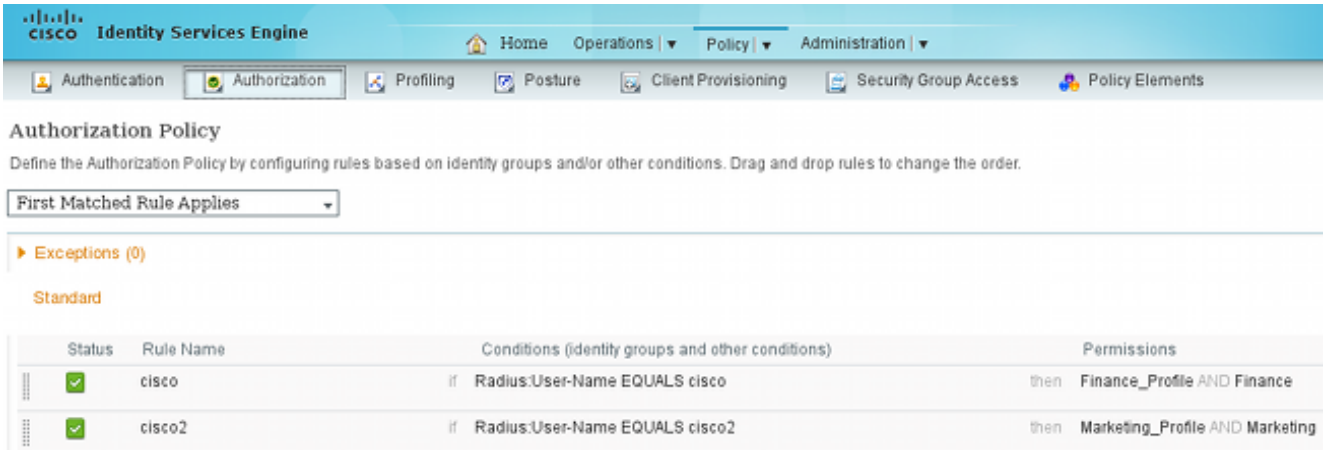



Jedes Profil könnte eine spezifische, restriktive DACL haben, aber in diesem Szenario ist der gesamte Datenverkehr zulässig. Die Durchsetzung erfolgt durch das SGFW, nicht durch die jeder VPN-Sitzung zugewiesene DACL. Mit einer SGFW gefilterter Datenverkehr ermöglicht die Verwendung von SGTs anstelle von IP-Adressen, die von der DACL verwendet werden.

4. Wählen Sie **Policy > Results > Security Group Access > Security Groups**, um die SGT-Gruppen für Marketing und Finanzen hinzuzufügen und zu konfigurieren.




5. Wählen Sie **Policy > Authorization** (Richtlinie > Autorisierung), um die beiden Autorisierungsregeln zu konfigurieren. Die erste Regel weist dem Benutzer "cisco" das Finance_profile-Profil (DACL, die den gesamten Datenverkehr zulässt) zusammen mit der SGT-Gruppe "Finance" zu. Die zweite Regel weist dem Benutzer "cisco2" das "Marketing_profile" (DACL, die den gesamten Datenverkehr zulässt) zusammen mit der SGT-Gruppe "Marketing"
zu.




## ASA-Konfiguration

1. Schließen Sie die grundlegende VPN-Konfiguration ab.

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

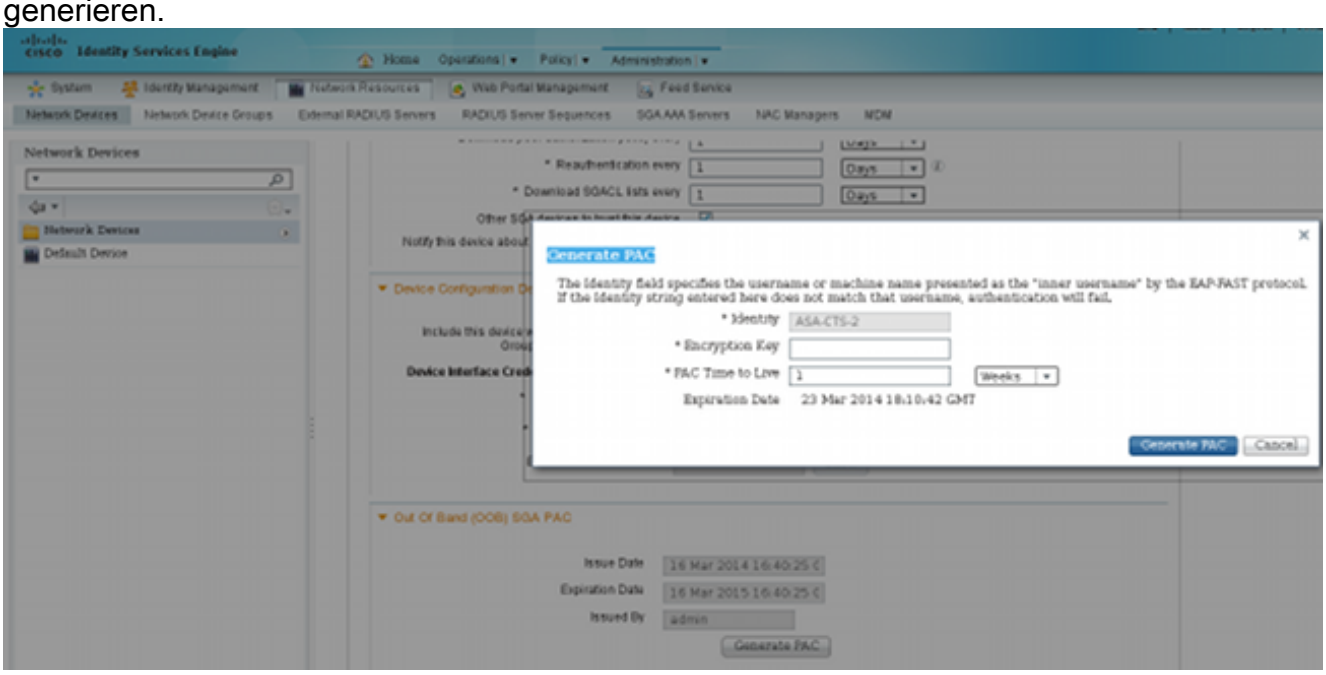
```
 tunnel-group-list enable

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. Schließen Sie die ASA AAA- und TrustSec-Konfiguration ab.

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

Um Teil der TrustSec-Cloud zu werden, muss sich die ASA mit Protected Access Credential (PAC) authentifizieren. Die ASA unterstützt keine automatische PAC-Bereitstellung. Aus diesem Grund muss diese Datei manuell auf der ISE generiert und in die ASA importiert werden.

3. Wählen Sie **Administration > Network Resources > Network Devices > ASA > Advanced TrustSec Settings**, um eine PAC auf der ISE zu generieren. Wählen Sie **Out of Band (OOB) PAC** Provisioning aus, um die Datei zu generieren.




4. Importieren Sie die PAC in die ASA.Die generierte Datei kann auf einem HTTP/FTP-Server abgelegt werden. ASA verwendet diese zum Importieren der Datei.

```
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
```

Wenn Sie über die richtige PAC verfügen, führt die ASA automatisch eine Aktualisierung der Umgebung durch. Dadurch werden Informationen über aktuelle SGT-Gruppen von der ISE heruntergeladen.

```
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. Konfigurieren Sie die SGFW. Der letzte Schritt besteht in der Konfiguration der ACL auf der externen Schnittstelle, die den ICMP-Datenverkehr von der Finanzabteilung zum Marketing zulässt.

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

Anstelle des Tags könnte auch der Sicherheitsgruppenname verwendet werden.

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

Um sicherzustellen, dass die Schnittstelle ACL VPN-Verkehr verarbeitet, muss die Option deaktiviert werden, die standardmäßig VPN-Verkehr ohne Validierung über die Schnittstelle ACL zulässt.

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

Die ASA sollte nun in der Lage sein, VPN-Benutzer zu klassifizieren und die Durchsetzung anhand von SGTs durchzuführen.

# Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

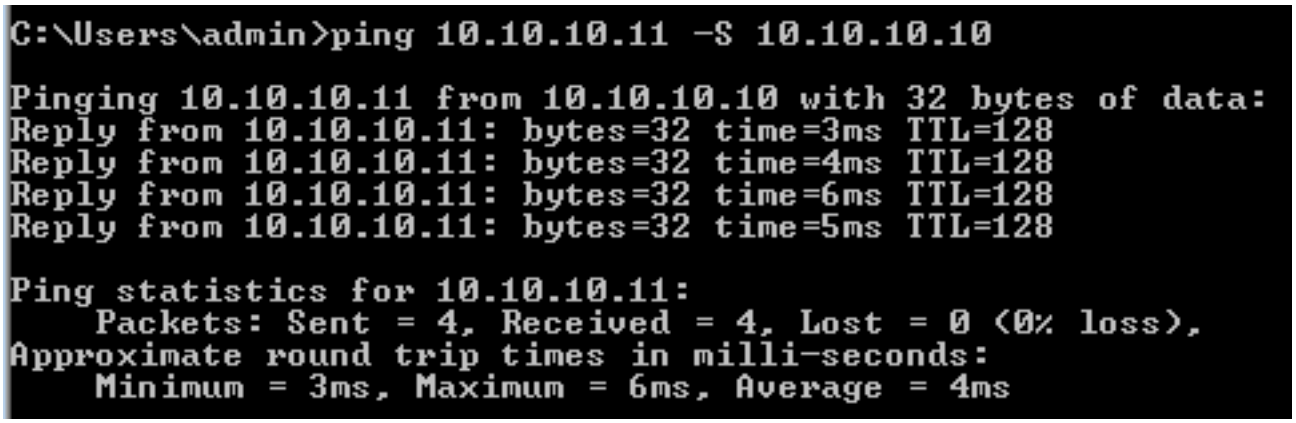
Die Fehlermeldung Output Interpreter Tool (registriert nur Kunden) unterstützt bestimmte **vorführen** -Befehlen. Verwenden Sie das Output Interpreter Tool, um eine Analyse von **vorführen** Befehlsausgabe.

Nachdem das VPN eingerichtet ist, stellt die ASA ein auf jede Sitzung angewendetes SGT dar.

```
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
```

Die SGFW ermöglicht den ICMP-Datenverkehr von der Finanzabteilung (SGT=2) zum Marketing (SGT=3). Aus diesem Grund kann der Benutzer "cisco" den Benutzer "cisco2" pingen.




Die Zähler werden erhöht:

```
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
```

Die Verbindung wurde erstellt:

```
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)
```

Rücksendungen werden automatisch akzeptiert, da die ICMP-Prüfung aktiviert ist.

Wenn Sie versuchen, einen Ping von Marketing (SGT=3) an die Finanzabteilung (SGT=2) zu senden:

```
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-Berichte:

```
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]
```

# Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Weitere Informationen finden Sie in folgenden Dokumenten:

- Konfigurationsbeispiel für TrustSec Cloud mit 802.1x MACsec auf Catalyst Switches der Serie 3750X
- ASA und Catalyst Switches der Serie 3750X - TrustSec-Konfigurationsbeispiel und Leitfaden zur Fehlerbehebung

# Zusammenfassung

In diesem Artikel wird ein einfaches Beispiel für die Klassifizierung von VPN-Benutzern und die Durchführung einer einfachen Durchsetzung vorgestellt. Die SGFW filtert außerdem den Datenverkehr zwischen VPN-Benutzern und dem restlichen Netzwerk. SXP (TrustSec SGT Exchange Protocol) kann auf einem ASA-Gerät verwendet werden, um die Zuordnungsinformationen zwischen IP- und SGT-Geräten abzurufen. So kann eine ASA die Durchsetzung für alle Arten von Sitzungen durchführen, die ordnungsgemäß klassifiziert wurden (VPN oder LAN).

In der ASA-Software Version 9.2 und höher unterstützt die ASA auch RADIUS Change of Authorization (CoA) (RFC 5176). Ein RADIUS-CoA-Paket, das von der ISE nach einem erfolgreichen VPN-Status gesendet wird, kann cisco-av-pair mit einem SGT enthalten, das einen kompatiblen Benutzer einer anderen (sichereren) Gruppe zuweist. Weitere Beispiele finden Sie in den Artikeln im Abschnitt "Verwandte Informationen".

# Zugehörige Informationen

- ASA Version 9.2.1 VPN-Status mit ISE - Konfigurationsbeispiel
- ASA und Catalyst Switches der Serie 3750X - TrustSec-Konfigurationsbeispiel und Leitfaden zur Fehlerbehebung
- Konfigurationsleitfaden für Cisco TrustSec-Switches: Erläuterungen zu Cisco TrustSec
- Konfigurieren eines externen Servers für die Benutzerautorisierung der Sicherheitsappliance
- Konfigurationsleitfaden für die VPN-CLI der Cisco ASA-Serie, 9.1
- Cisco Identity Services Engine Benutzerhandbuch, Version 1.2
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.