

ASA 9.3.1 TrustSec-Inline-Tagging konfigurieren

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[ISE - Konfigurationsschritte](#)

[1. SGT für Finanzen und Marketing](#)

[2. Security Group ACL für Datenverkehrsmarketing > Finanzen](#)

[3. Binden der ACL in Matrix](#)

[4. Autorisierungsregel für VPN-Zugriff Zuweisen von SGT = 3 \(Marketing\)](#)

[5. Autorisierungsregel für 802.1x-Zugriff Zuweisung von SGT = 2 \(Finanzierung\)](#)

[6. Hinzufügen von Netzwerkgeräten, Erstellen von PAC für ASA](#)

[7. Netzwerkgerät hinzufügen, "Secret for Switch Automatic PAC Provisioning" konfigurieren](#)

[ASA - Konfigurationsschritte](#)

[1. Einfacher VPN-Zugriff](#)

[2. PAC importieren und CTS aktivieren](#)

[3. SGACL für Verkehrsfinanzierung > Marketing](#)

[4. Aktivieren von cts auf der internen Schnittstelle](#)

[Switch - Konfigurationsschritte](#)

[1. Grundlegendes 802.1x](#)

[2. CTS-Konfiguration und -Bereitstellung](#)

[3. Aktivieren von cts auf Schnittstelle zur ASA](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[SGT-Zuweisung](#)

[Durchsetzung auf ASA](#)

[Switch-Durchsetzung](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument beschreibt die Verwendung der in der Adaptive Security Appliance (ASA) Version 9.3.1 - TrustSec Inline-Tagging implementierten Funktion. Mit dieser Funktion kann ASA TrustSec-Frames empfangen und senden. Auf diese Weise kann ASA problemlos in die TrustSec-Domäne integriert werden, ohne dass TrustSec SGT Exchange Protocol (SXP) verwendet werden muss.

In diesem Beispiel wird ein Remote-VPN-Benutzer dargestellt, dem das Security Group Tag (SGT)-Tag = 3 (Marketing) und der 802.1x-Benutzer zugewiesen wurden und dem SGT-Tag = 2 (Finanzierung) zugewiesen wurde. Die Durchsetzung des Datenverkehrs erfolgt sowohl von der

ASA mithilfe der lokal definierten Sicherheitsgruppen-Zugriffskontrollliste (SGACL) als auch vom Cisco IOS®-Switch mithilfe der RBACL (Role Based Access Control List), die von der Identity Services Engine (ISE) heruntergeladen wurde.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Cisco ASA Software, Version 9.3.1 und höher
- Cisco ASA Hardware 55x5 oder ASAv
- Windows 7 mit Cisco AnyConnect Secure Mobility Client, Version 3.1
- Cisco Catalyst 3750X Switch mit Software 15.0.2 und höher
- Cisco ISE, Version 1.2 und höher

Konfigurieren

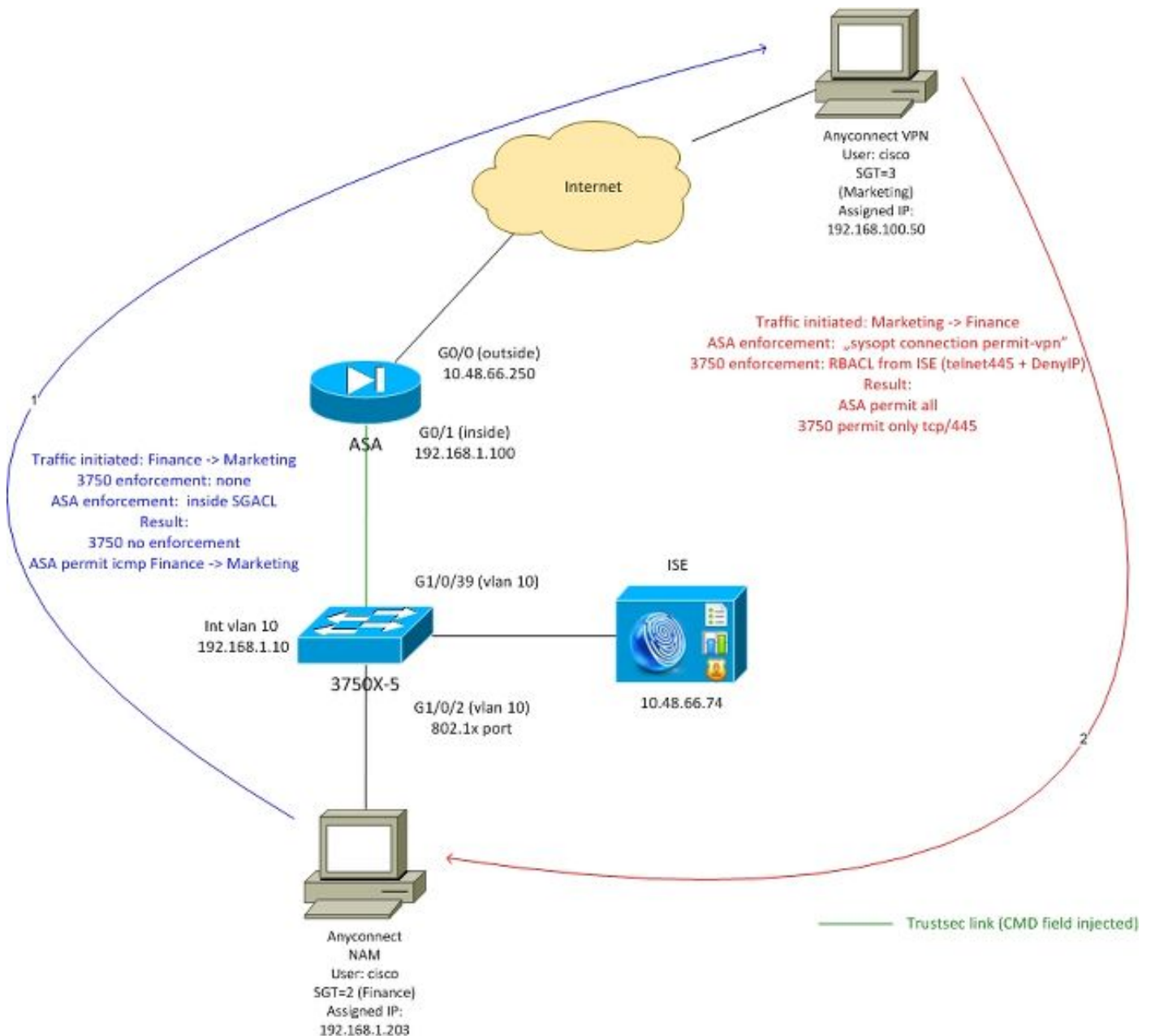
Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

Die Verbindung zwischen ASA und 3750X ist für manuelle CTS konfiguriert. Das bedeutet, dass beide Geräte modifizierte Ethernet-Frames mit Cisco Metadata Field (CMD) senden und empfangen können. Dieses Feld enthält die Security Group Tag (SGT), die die Paketquelle beschreibt.

Der Remote-VPN-Benutzer beendet die SSL-Sitzung auf der ASA und erhält SGT-Tag 3 (Marketing).

802.1x-Benutzer des lokalen Unternehmens nach erfolgreicher Authentifizierung mit SGT-Tag 2 (Finance).



In der ASA ist SGACL auf der internen Schnittstelle konfiguriert, sodass ICMP-Datenverkehr von der Finanzabteilung zum Marketing möglich ist.

ASA lässt den gesamten Datenverkehr zu, der vom entfernten VPN-Benutzer initiiert wurde (aufgrund der Konfiguration "sysopt connection permit-vpn").

SGACL auf ASA ist zustandsorientiert, d. h., dass nach Erstellung des Datenflusses das Rückgabepaket automatisch akzeptiert wird (basierend auf der Überprüfung).

Der Switch 3750 verwendet RBACL, um den Datenverkehr vom Marketing zur Finanzierung zu steuern.

RBACL ist statusfrei, d. h., jedes Paket wird geprüft, aber die TrustSec-Durchsetzung auf der 3750X-Plattform wird am Ziel durchgeführt. Auf diese Weise ist der Switch für die Durchsetzung des Verkehrs von Marketing zu Finanzen verantwortlich.

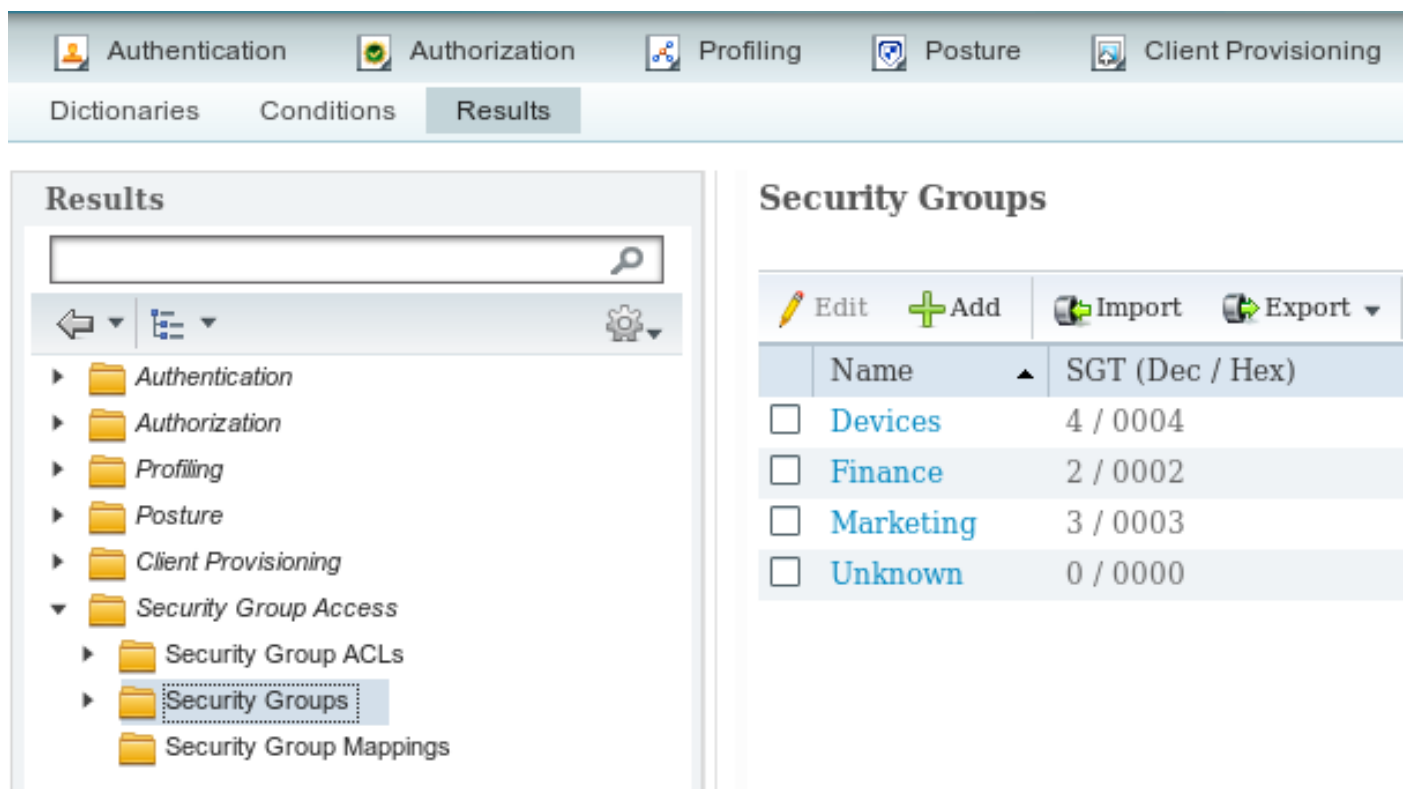
Hinweis: Für TrustSec-sensitive Stateful-Firewall auf Cisco IOS® Zone-basierter Firewall können z. B. folgende Informationen verwendet werden:

Hinweis: ASA kann SGACL-Datenverkehr steuern, der von einem Remote-VPN-Benutzer stammt. Um das Szenario zu vereinfachen, wurde es in diesem Artikel nicht vorgestellt. Beispiel: [Konfigurationsbeispiel für die ASA Version 9.2 VPN-SGT-Klassifizierung und -Durchsetzung](#)

ISE - Konfigurationsschritte

1. SGT für Finanzen und Marketing

Navigieren Sie zu **Richtlinien > Ergebnisse > Security Group Access > Security Groups** und erstellen Sie ein SGT für Finanzen und Marketing, wie in diesem Bild gezeigt.



The screenshot shows the Cisco ISE configuration interface. At the top, there are tabs for Authentication, Authorization, Profiling, Posture, and Client Provisioning. Below these are sub-tabs for Dictionaries, Conditions, and Results. The Results tab is active, and the Security Groups folder is selected in the left-hand navigation pane. The main content area displays the Security Groups configuration page, which includes a table of existing security groups and action buttons (Edit, Add, Import, Export).

	Name	SGT (Dec / Hex)
<input type="checkbox"/>	Devices	4 / 0004
<input type="checkbox"/>	Finance	2 / 0002
<input type="checkbox"/>	Marketing	3 / 0003
<input type="checkbox"/>	Unknown	0 / 0000

2. Security Group ACL für Datenverkehrsmarketing > Finanzen

Navigieren Sie zu **Richtlinien > Ergebnisse > Security Group Access > Security Group ACL (Richtlinien > Ergebnisse > Sicherheitsgruppenzugriff > Sicherheitsgruppen-Zugriffskontrollliste)**, und erstellen Sie eine Zugriffskontrollliste, mit der der Datenverkehr von Marketing zu Finanzen gesteuert wird. Nur tcp/445 ist zulässig, wie in diesem Bild gezeigt.

The screenshot shows a network management interface with a top navigation bar containing icons and labels for Authentication, Authorization, Profiling, Posture, and Client Provisioning. Below this is a secondary bar with 'Dictionaries', 'Conditions', and 'Results' tabs. The 'Results' tab is active, displaying a left-hand navigation tree with folders for Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, Security Group ACLs (highlighted), Security Groups, and Security Group Mappings. The main content area is titled 'Security Groups ACLs List > telnet445' and 'Security Group ACLs'. It features a form with the following fields: 'Name' (text input with 'telnet445'), 'Description' (empty text area), 'IP Version' (radio buttons for IPv4, IPv6, and an unlabeled one, with IPv4 selected), and '* Security Group ACL content' (text area containing 'permit tcp dst eq 445').

3. Binden der ACL in Matrix

Navigieren Sie zu **Richtlinie > Ausgangsrichtlinie > Matrix-Binding** für die konfigurierte ACL für die Quelle: **Marketing** und Ziel: **Finanzen**. Fügen Sie außerdem **Deny IP** als letzte ACL hinzu, um wie im Bild gezeigt den gesamten anderen Datenverkehr zu verwerfen. (Ohne diese Standardrichtlinie wird die Standardrichtlinie angefügt, ist "permit any" festgelegt.)

Authentication Authorization Profiling Posture Client Provisioning Security Group Access

Egress Policy Network Device Authorization

Source Tree Destination Tree **Matrix**

Egress Policy (Matrix View)

Edit Add Clear Mapping Configure Push Monitor All Dimension 3X5

Destination Source	Devices (4 / 0004)	Finance (2 / 0002)
Devices (4 / 0004)		
Finance (2 / 0002)		
Marketing (3 / 0003)		<input checked="" type="checkbox"/> Enabled SGACLs: telnet445, Deny IP

4. Autorisierungsregel für VPN-Zugriff Zuweisen von SGT = 3 (Marketing)

Navigieren Sie zu **Richtlinien > Autorisierung**, und erstellen Sie eine Regel für den Remote-VPN-Zugriff. Alle VPN-Verbindungen, die über den AnyConnect 4.x-Client hergestellt werden, erhalten vollständigen Zugriff (PermitAccess) und erhalten SGT-Tag 3 (Marketing). Die Bedingung hierfür ist die Verwendung von AnyConnect Identity Extensions ([ACIDEX](#)):

Rule name: VPN
 Condition: Cisco:cisco-av-pair CONTAINS mdm-tlv=ac-user-agent=AnyConnect Windows 4
 Permissions: PermitAccess AND **Marketing**

5. Autorisierungsregel für 802.1x-Zugriff Zuweisung von SGT = 2 (Finanzierung)

Navigieren Sie zu **Richtlinien > Autorisierung**, und erstellen Sie eine Regel für den 802.1x-Zugriff. Bei Beendigung der 802.1x-Sitzung auf dem 3750-Switch mit dem Benutzernamen **cisco** erhält der Supplicant vollständigen Zugriff (PermitAccess) und erhält SGT-Tag 2 (Finance).

Rule name: 802.1x

Condition: Radius:User-Name EQUALS cisco AND Radius:NAS-IP-Address EQUALS 192.168.1.10
Permissions: PermitAccess AND Finance

6. Hinzufügen von Netzwerkgeräten, Erstellen von PAC für ASA

Um ASA zur TrustSec-Domäne hinzuzufügen, muss die PAC-Datei manuell generiert werden. Diese Datei wird auf ASA importiert.

Dies kann über **Administration > Network Devices** konfiguriert werden. Scrollen Sie nach dem Hinzufügen von ASA nach unten zu **TrustSec-Einstellungen** und **Generieren von PAC**, wie in diesem Bild gezeigt.

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

* Encryption Key

* PAC Time to Live

Expiration Date 19 Apr 2015 09:06:30 GMT

▼ **Out Of Band (OOB) TrustSec PAC**

Issue Date

Expiration Date

Issued By

Switches (3750X) unterstützen die automatische PAC-Bereitstellung, sodass Schritte nur für ASA ausgeführt werden müssen, die nur die manuelle PAC-Bereitstellung unterstützt.

7. Netzwerkgerät hinzufügen, "Secret for Switch Automatic PAC Provisioning" konfigurieren

Für Switches, die automatische PAC-Bereitstellung verwenden, muss ein korrekter geheimer Schlüssel festgelegt werden, wie in diesem Bild gezeigt.

Advanced TrustSec Settings

▼ **Device Authentication Settings**

Use Device ID for SGA Identification

Device Id

* Password

Hinweis: PAC dient zur Authentifizierung der ISE und zum Herunterladen von Umgebungsdaten (z. B. SGT) zusammen mit der Richtlinie (ACL). ASA unterstützt nur Umgebungsdaten, Richtlinien müssen auf ASA manuell konfiguriert werden. Cisco IOS® unterstützt beides, sodass die Richtlinien von der ISE heruntergeladen werden können.

ASA - Konfigurationsschritte

1. Einfacher VPN-Zugriff

Konfigurieren des grundlegenden SSL VPN-Zugriffs für AnyConnect mithilfe der ISE für die Authentifizierung

```
aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.62.145.41
  key cisco

webvpn
  enable outside
  anyconnect-essentials
  anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
  anyconnect enable
  tunnel-group-list enable
  error-recovery disable

tunnel-group TAC type remote-access
tunnel-group TAC general-attributes
  address-pool (outside) POOL
  authentication-server-group ISE
  default-group-policy TAC
tunnel-group TAC webvpn-attributes
  group-alias TAC enable

ip local pool POOL 192.168.100.50-192.168.100.60 mask 255.255.255.0
```

2. PAC importieren und CTS aktivieren

Für ASA generierte PAC importieren (ab Schritt 6 der ISE-Konfiguration). Verwenden Sie denselben Verschlüsselungsschlüssel:

```
BSNS-ASA5512-4# cts import-pac http://10.229.20.86/asa5512.pac password ciscocisco
PAC Imported Successfully
```

So überprüfen Sie:

```
BSNS-ASA5512-4# show cts pac
```

PAC-Info:

```
Valid until: Apr 11 2016 10:16:41
AID:         c2dcb10f6e5474529815aed11ed981bc
I-ID:        asa5512
A-ID-Info:   Identity Services Engine
PAC-type:    Cisco Trustsec
```

PAC-Opaque:

```
000200b00003000100040010c2dcb10f6e5474529815aed11ed981bc00060094000301
007915dcb81032f2fdf04bfe938547fad2000000135523ecb300093a8089ee0193bb2c
8bc5cfabf8bc7b9543161e6886ac27e5ba1208ce445018a6b07cc17688baf379d2f1f3
```



```
25301fffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
4d4013e8fe
```

cts aktivieren:

```
cts server-group ISE
```

Nachdem Sie cts aktiviert haben, muss ASA Umgebungsdaten von der ISE herunterladen:

```
BSNS-ASA5512-4# show cts environment-data
CTS Environment Data
=====
Status:                Active
Last download attempt: Successful
Environment Data Lifetime: 86400 secs
Last update time:      10:21:41 UTC Apr 11 2015
Env-data expires in:   0:00:37:31 (dd:hr:mm:sec)
Env-data refreshes in: 0:00:27:31 (dd:hr:mm:sec)
```

3. SGACL für Verkehrsfinanzierung > Marketing

Konfigurieren Sie SGACL auf der internen Schnittstelle. Mit der ACL kann nur ICMP-Datenverkehr von der Finanzabteilung zum Marketing initiiert werden.

```
access-list inside extended permit icmp security-group name Finance any security-group name
Marketing any
access-group inside in interface inside
```

ASA muss den Namen des Tags auf Nummer erweitern:

```
BSNS-ASA5512-4(config)# show access-list inside
access-list inside line 1 extended permit icmp security-group name Finance(tag=2) any security-
group name Marketing(tag=3) any (hitcnt=47) 0x5633b153
```

4. Aktivieren von cts auf der internen Schnittstelle

Nachdem Sie die cts für die interne ASA-Schnittstelle aktiviert haben:

```
interface GigabitEthernet0/1
 nameif inside
 cts manual
  policy static sgt 100 trusted
 security-level 100
 ip address 192.168.1.100 255.255.255.0
```

ASA kann TrustSec-Frames senden und empfangen (Ethernet-Frames mit CMD-Feld). ASA geht davon aus, dass alle eingehenden Frames ohne Tag wie mit dem Tag 100 behandelt werden müssen. Alle eingehenden Frames, die bereits das Tag enthalten, werden als vertrauenswürdig eingestuft.

Switch - Konfigurationsschritte

1. Grundlegendes 802.1x

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius
```

```
dot1x system-auth-control
```

```
interface GigabitEthernet1/0/2
description windows7
switchport access vlan 10
switchport mode access
authentication host-mode multi-domain
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast
```

```
radius-server host 10.48.66.74 pac key cisco
```

Bei dieser Konfiguration muss dem Benutzer (autorisiert über ISE) nach erfolgreicher 802.1x-Autorisierung der Tag 2 (Finanzierung) zugewiesen werden.

2. CTS-Konfiguration und -Bereitstellung

Ebenso wie für ASA wird cts konfiguriert, und es wird auf ISE verwiesen:

```
aaa authorization network ise group radius
cts authorization list ise
```

Außerdem ist die Durchsetzung sowohl für Layer 3 als auch für Layer 2 (alle VLANs) aktiviert:

```
cts role-based enforcement
cts role-based enforcement vlan-list 1-1005,1008-4094
```

So stellen Sie PAC automatisch bereit:

```
bsns-3750-5#cts credentials id 3750-5 password ciscocisco
```

Auch hier muss das Kennwort mit der entsprechenden Konfiguration auf der ISE übereinstimmen (**Netzwerkgerät > Switch > TrustSec**). Derzeit initiiert Cisco IOS® eine EAP-FAST-Sitzung mit der ISE, um die PAC zu erhalten. Weitere Einzelheiten zu diesem Prozess finden Sie hier:

[ASA und Catalyst Switch der Serie 3750X - TrustSec-Konfigurationsbeispiel und Leitfaden zur Fehlerbehebung](#)

So überprüfen Sie, ob PAC installiert ist:

```
bsns-3750-5#show cts pacs
```

```
AID: EA48096688D96EF7B94C679A17BDAD6F
```

```
PAC-Info:
```

```
PAC-type = Cisco Trustsec
```

```
AID: EA48096688D96EF7B94C679A17BDAD6F
```

```
I-ID: 3750-5
```

```
A-ID-Info: Identity Services Engine
```

```
Credential Lifetime: 14:41:24 CEST Jul 10 2015
```

```
PAC-Opaque:
```

```
000200B00003000100040010EA48096688D96EF7B94C679A17BDAD6F0006009400030100365AB3133998C86C1BA1B418
```

```
968C60690000001355261CCC00093A808F8A81F3F8C99A7CB83A8C3BFC4D573212C61CDCEB37ED279D683EE0DA60D86D
5904C41701ACF07BE98B3B73C4275C98C19A1DD7E1D65E679F3E9D40662B409E58A9F139BAA3BA3818553152F28AE04B
089E5B7CBB22A0D4BCEEF80F826A180B5227EAACBD07709DBDCD3CB42AA9F996829AE46F
```

Refresh timer is set for 4y14w

3. Aktivieren von cts auf Schnittstelle zur ASA

```
interface GigabitEthernet1/0/39
 switchport access vlan 10
 switchport mode access
 cts manual
 policy static sgt 101 trusted
```

Der Switch muss von nun an darauf vorbereitet sein, TrustSec-Frames zu verarbeiten und zu senden und die von der ISE heruntergeladenen Richtlinien durchzusetzen.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Die Überprüfung wird in den einzelnen Abschnitten dieses Dokuments behandelt.

Fehlerbehebung

SGT-Zuweisung

Nach Einrichtung einer VPN-Sitzung mit der ASA muss die richtige SGT-Zuweisung bestätigt werden:

```
BSNS-ASA5512-4# show vpn-sessiondb anyconnect
```

Session Type: AnyConnect

```
Username      : cisco                               Index      : 13
Assigned IP   : 192.168.100.50                     Public IP   : 10.229.20.86
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Essentials
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES256 DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 10308                               Bytes Rx    : 10772
Group Policy  : TAC                                 Tunnel Group : TAC
Login Time    : 15:00:13 UTC Mon Apr 13 2015
Duration      : 0h:00m:25s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                                VLAN        : none
Audt Sess ID  : c0a801640000d000552bd9fd
Security Grp : 3:Marketing
```

Gemäß den Autorisierungsregeln für die ISE wurden alle AnyConnect4-Benutzer dem Marketing-Tag zugewiesen.

Gleiches gilt für die 802.1x-Sitzung auf dem Switch. Nachdem das AnyConnect Network Analysis Module (NAM) abgeschlossen ist, wendet der Authentifizierungs-Switch das von der ISE zurückgegebene Tag an:

```
bsns-3750-5#show authentication sessions interface g1/0/2 details
```

```
Interface: GigabitEthernet1/0/2
MAC Address: 0050.5699.36ce
IPv6 Address: Unknown
IPv4 Address: 192.168.1.203
User-Name: cisco
Status: Authorized
Domain: DATA
Oper host mode: multi-domain
Oper control dir: both
Session timeout: N/A
Common Session ID: 0A30426D000000130001B278
Acct Session ID: Unknown
Handle: 0x53000002
Current Policy: POLICY_Gi1/0/2
```

```
Local Policies:
```

```
Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure
Security Status: Link Unsecure
```

```
Server Policies:
```

```
SGT Value: 2
```

```
Method status list:
```

Method	State
dot1x	Authc Success
mab	Stopped

Gemäß den Autorisierungsregeln für die ISE müssen alle mit diesem Switch verbundenen Benutzer SGT = 2 (Finanzierung) zugewiesen werden.

Durchsetzung auf ASA

Wenn Sie versuchen, einen Datenverkehr von Finance (192.168.1.203) an Marketing (192.168.100.50) zu senden, trifft er auf die interne Schnittstelle von ASA. Für die ICMP-Echoanforderung wird die Sitzung erstellt:

```
Built outbound ICMP connection for faddr 192.168.100.50/0(LOCAL\cisco, 3:Marketing) gaddr 192.168.1.203/1 laddr 192.168.1.203/1(2)
```

und erhöht die ACL-Zähler:

```
BSNS-ASA5512-4(config)# sh access-list
```

```
access-list inside line 1 extended permit icmp security-group name Finance(tag=2) any security-group name Marketing(tag=3) any (hitcnt=138)
```

Dies kann auch durch die Paketerfassung bestätigt werden. Beachten Sie, dass die richtigen Tags angezeigt werden:

```
BSNS-ASA5512-4(config)# capture CAP interface inside
```

```
BSNS-ASA5512-4(config)# show capture CAP
```

```
1: 15:13:05.736793      INLINE-TAG 2 192.168.1.203 > 192.168.100.50: icmp: echo request
2: 15:13:05.772237      INLINE-TAG 3 192.168.100.50 > 192.168.1.203: icmp: echo reply
3: 15:13:10.737236      INLINE-TAG 2 192.168.1.203 > 192.168.100.50: icmp: echo request
4: 15:13:10.772726      INLINE-TAG 3 192.168.100.50 > 192.168.1.203: icmp: echo reply
```

Es gibt eine eingehende ICMP-Echoanfrage, die mit SGT = 2 (Finanzen) markiert ist, und eine Antwort von VPN-Benutzern, die von ASA mit SGT = 3 (Marketing) markiert wird. Ein weiteres Tool zur Fehlerbehebung, Packet-Tracer ist ebenfalls TrustSec-fähig.

Leider sieht der 802.1x-PC diese Antwort nicht, da er von der Stateless-RBACL auf dem Switch blockiert wird (Erläuterung im nächsten Abschnitt).

Ein weiteres Tool zur Fehlerbehebung, Packet-Tracer ist ebenfalls TrustSec-fähig. Lassen Sie uns bestätigen, dass eingehende ICMP-Pakete von der Finanzabteilung akzeptiert werden:

```
BSNS-ASA5512-4# packet-tracer input inside icmp inline-tag 2 192.168.1.203 8 0 192.168.100.50
Mapping security-group 3:Marketing to IP address 192.168.100.50
```

```
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
```

```
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.48.66.1 using egress ifc outside
```

```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group inside in interface inside
access-list inside extended permit icmp security-group name Finance any security-group name Marketing any
Additional Information:
```

<some output omitted for clarity>

```
Phase: 13
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 4830, packet dispatched to next module
```

```
Result:
input-interface: inside
```

```
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
```

Action: allow

Lassen Sie uns auch versuchen, eine TCP-Verbindung von Finance zu Marketing zu initiieren, die von der ASA blockiert werden muss:

```
Deny tcp src inside:192.168.1.203/49236 dst outside:192.168.100.50/445(LOCAL\cisco, 3:Marketing)
by access-group "inside" [0x0, 0x0]
```

Switch-Durchsetzung

Überprüfen wir, ob der Switch Richtlinien richtig von der ISE heruntergeladen hat:

```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
  Permit IP-00
IPv4 Role-based permissions from group 2:Finance to group Unknown:
  test_deny-30
IPv4 Role-based permissions from group 8 to group Unknown:
  permit_icmp-10
IPv4 Role-based permissions from group Unknown to group 2:Finance:
  test_deny-30
  Permit IP-00
IPv4 Role-based permissions from group 3:Marketing to group 2:Finance:
  telnet445-60
  Deny IP-00
```

```
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Richtlinien zur Kontrolle des Datenverkehrs von Marketing zu Finanzen werden korrekt installiert. Gemäß RBACL ist nur tcp/445 zulässig:

```
bsns-3750-5#show cts rbacl telnet445
CTS RBACL Policy
=====
RBACL IP Version Supported: IPv4
  name      = telnet445-60
  IP protocol version = IPV4
  refcnt    = 2
  flag      = 0x41000000
  stale     = FALSE
RBACL ACEs:
  permit tcp dst eq 445
```

Aus diesem Grund wurde die ICMP-Echo-Antwort von Marketing zu Finance verworfen. Dies kann durch Überprüfung der Zähler für Datenverkehr von SGT 3 nach SGT 2 bestätigt werden:

```
bsns-3750-5#show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical policies
From    To      SW-Denied    HW-Denied    SW-Permitted    HW-Permitted

*      *      0            0            223613          3645233

0      2      0            0            0               122
```

3	2	0	65	0	0
2	0	0	0	179	0
8	0	0	0	0	0

Pakete wurden von der Hardware verworfen (der aktuelle Zähler beträgt 65 und erhöht sich alle 1 Sekunde).

Was geschieht, wenn die Verbindung tcp/445 von Marketing initiiert wird?

ASA lässt Folgendes zu (akzeptiert den gesamten VPN-Datenverkehr aufgrund von "sysopt connection permit-vpn"):

```
Built inbound TCP connection 4773 for outside:192.168.100.50/49181
(192.168.100.50/49181) (LOCAL\cisco, 3:Marketing) to inside:192.168.1.203/445 (192.168.1.203/445)
(cisco)
```

Die richtige Sitzung wird erstellt:

```
BSNS-ASA5512-4(config)# show conn all | i 192.168.100.50
TCP outside 192.168.100.50:49181 inside 192.168.1.203:445, idle 0:00:51, bytes 0, flags UB
```

Cisco IOS® akzeptiert diese Einstellung, da sie mit der telnet445 RBACL übereinstimmt. Die korrekten Zähler werden erhöht:

```
bsns-3750-5#show cts role-based counters from 3 to 2
3      2      0      65      0      3
```

(letzte Spalte ist der von der Hardware zugelassene Datenverkehr). Die Sitzung ist zulässig.

Dieses Beispiel dient der Veranschaulichung der Unterschiede bei der Konfiguration und Durchsetzung von TrustSec-Richtlinien auf ASA und Cisco IOS®. Beachten Sie die Unterschiede zwischen Cisco IOS®-Richtlinien, die von der ISE (Stateless RBACL) und der TrustSec-basierten Stateful Zone-Firewall heruntergeladen wurden.

Zugehörige Informationen

- [ASA Version 9.2.1 VPN-Status mit ISE-Konfigurationsbeispiel](#)
- [ASA und Catalyst Switch der Serie 3750X - TrustSec-Konfigurationsbeispiel und Leitfaden zur Fehlerbehebung](#)
- [Konfigurationsanleitung für Cisco TrustSec-Switches: Cisco TrustSec im Überblick](#)
- [Konfigurieren eines externen Servers für die Benutzerautorisierung der Sicherheitsappliance](#)
- [Konfigurationsleitfaden für die CLI der Cisco ASA-Serie 9.1](#)
- [Cisco Identity Services Engine-Benutzerhandbuch, Version 1.2](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)