Konfigurationsbeispiel für TrustSec Cloud mit 802.1x MACsec auf Catalyst Switches der Serie 3750X

Inhalt

Einleitung

In diesem Artikel werden die erforderlichen Schritte zur Konfiguration einer Cisco TrustSec (CTS)-Cloud mit Link-Verschlüsselung zwischen zwei Catalyst Switches der Serie 3750X (3750X) beschrieben.

In diesem Artikel wird der Verschlüsselungsprozess für die Switch-to-Switch Media Access Control Security (MACsec) erläutert, der das Security Association Protocol (SAP) verwendet. Bei diesem Prozess wird anstelle des manuellen Modus der IEEE 802.1x-Modus verwendet.

Hier finden Sie eine Liste der erforderlichen Schritte:

- Bereitstellung von Protected Access Credential (PAC) für Seed- und Nicht-Seed-Geräte
- Network Device Admission Control (NDAC)-Authentifizierung und MACsec-Aushandlung mit SAP für die Schlüsselverwaltung
- Umwelt- und Politikaktualisierung

- Port-Authentifizierung für Clients
- Datenverkehr-Tagging mit dem Security Group Tag (SGT)
- Richtliniendurchsetzung mit der Security Group ACL (SGACL)

Voraussetzungen

Anforderungen

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

- Grundkenntnisse der CTS-Komponenten
- Grundkenntnisse der CLI-Konfiguration von Catalyst Switches
- Erfahrung mit der Konfiguration der Identity Services Engine (ISE)

Verwendete Komponenten

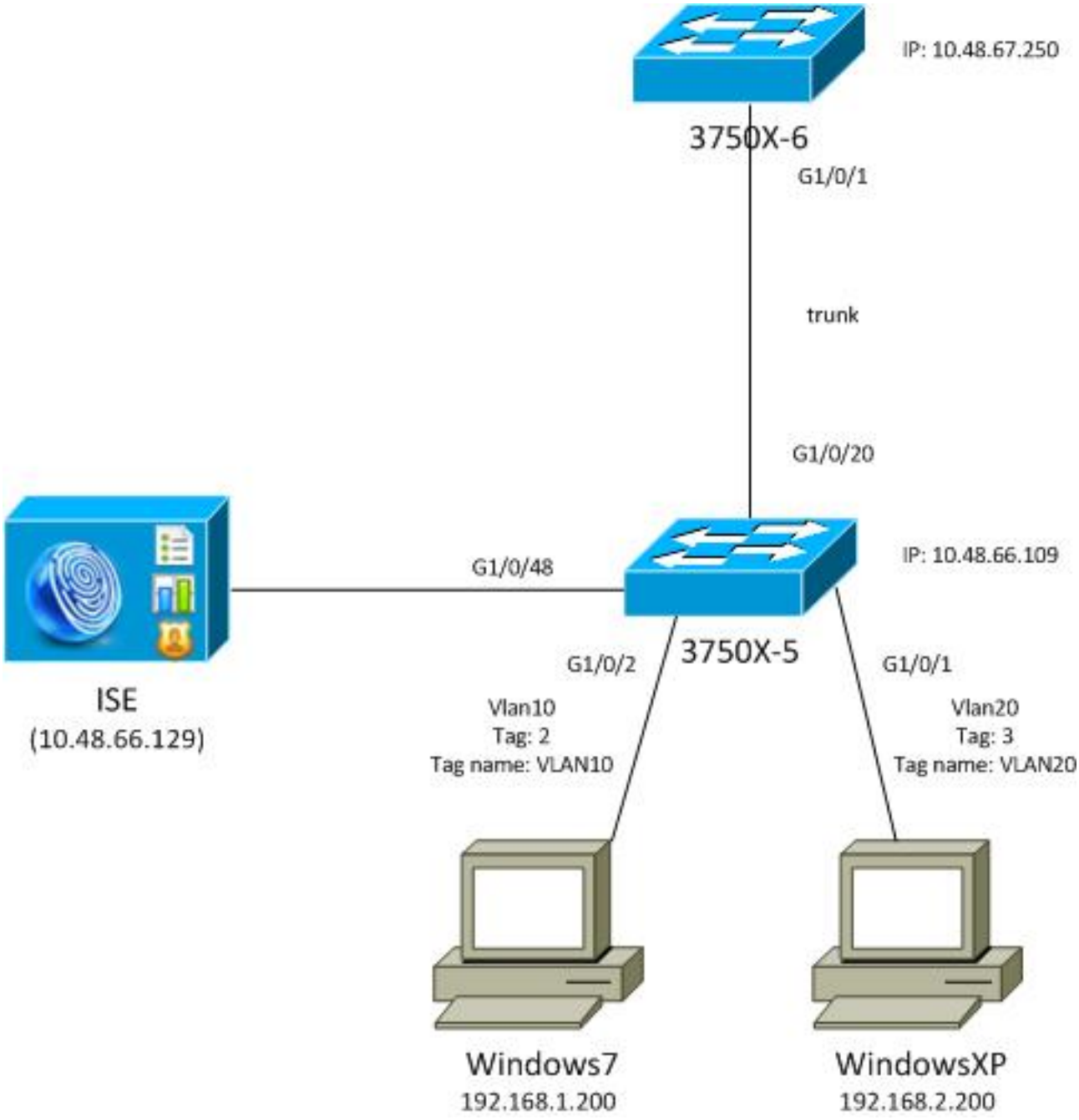
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Microsoft (MS) Windows 7 und MS Windows XP
- 3750X Software, Versionen 15.0 und höher
- ISE Software, Versionen 1.1.4 und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfigurieren

Netzwerkdiagramm



In diesem Netzwerktopologiediagramm ist der 3750X-5-Switch das Seed-Gerät, das die IP-Adresse der ISE kennt, und er lädt automatisch die PAC herunter, die für die nachfolgende Authentifizierung in der CTS-Cloud verwendet wird. Das Seed-Gerät fungiert als 802.1x-Authentifizierer für Nicht-Seed-Geräte. Der Cisco Catalyst Switch der Serie 3750X-6 (3750X-6) ist das Non-Seed-Gerät. Es fungiert als 802.1x-Komponente für das Seed-Gerät. Nachdem sich das Nicht-Seed-Gerät über das Seed-Gerät bei der ISE authentifiziert hat, erhält es Zugriff auf die CTS-Cloud. Nach erfolgreicher Authentifizierung wird der 802.1x-Portstatus auf dem 3750X-5-Switch in "**authentifiziert**" geändert, und die MACsec-Verschlüsselung wird ausgehandelt. Der Datenverkehr zwischen den Switches wird dann mit dem SGT markiert und verschlüsselt.

Diese Liste fasst den erwarteten Datenverkehrsfluss zusammen:

- Der Seed 3750X-5 stellt eine Verbindung zur ISE her und lädt die PAC herunter, die später für eine Aktualisierung der Umgebung und Richtlinien verwendet wird.
- Der Nicht-Seed-Router 3750X-6 führt eine 802.1x-Authentifizierung mit der Supplicant-Rolle durch, um die PAC zu authentifizieren/zu autorisieren und von der ISE herunterzuladen.
- Der 3750X-6 führt eine zweite 802.1x Extensible Authentication Protocol-Flexible

Authentication via Secure Protocol (EAP-FAST)-Sitzung durch, um sich über den geschützten Tunnel basierend auf der PAC zu authentifizieren.
- Der 3750X-5 lädt SGA-Richtlinien für sich und für den 3750X-6 herunter.
- Zwischen dem 3750X-5 und 3750X-6 findet eine SAP-Sitzung statt, MACsec-Verschlüsselungen werden ausgehandelt, und die Richtlinie wird ausgetauscht.
- Der Datenverkehr zwischen den Switches wird markiert und verschlüsselt.

Seed- und Non-Seed-Switches konfigurieren

Das Seed-Gerät (3750X-5) wird konfiguriert, um die ISE als RADIUS-Server für CTS zu verwenden:

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius

cts authorization list ise

radius-server host 10.48.66.129 pac key cisco
radius-server host 10.48.66.129 auth-port 1812
radius-server vsa send accounting
radius-server vsa send authentication
```

Die rollenbasierte Durchsetzung von Zugriffskontrolllisten (RBACL) und SGACL (Security Group Based Access Control List) wird aktiviert (wird später verwendet):

```
cts role-based enforcement
cts role-based enforcement vlan-list 1-1005,1007-4094
```

Das Non-Seed-Gerät (3750X-6) ist nur für Authentication, Authorization und Accounting (AAA) konfiguriert, ohne dass eine RADIUS- oder CTS-Autorisierung erforderlich ist:

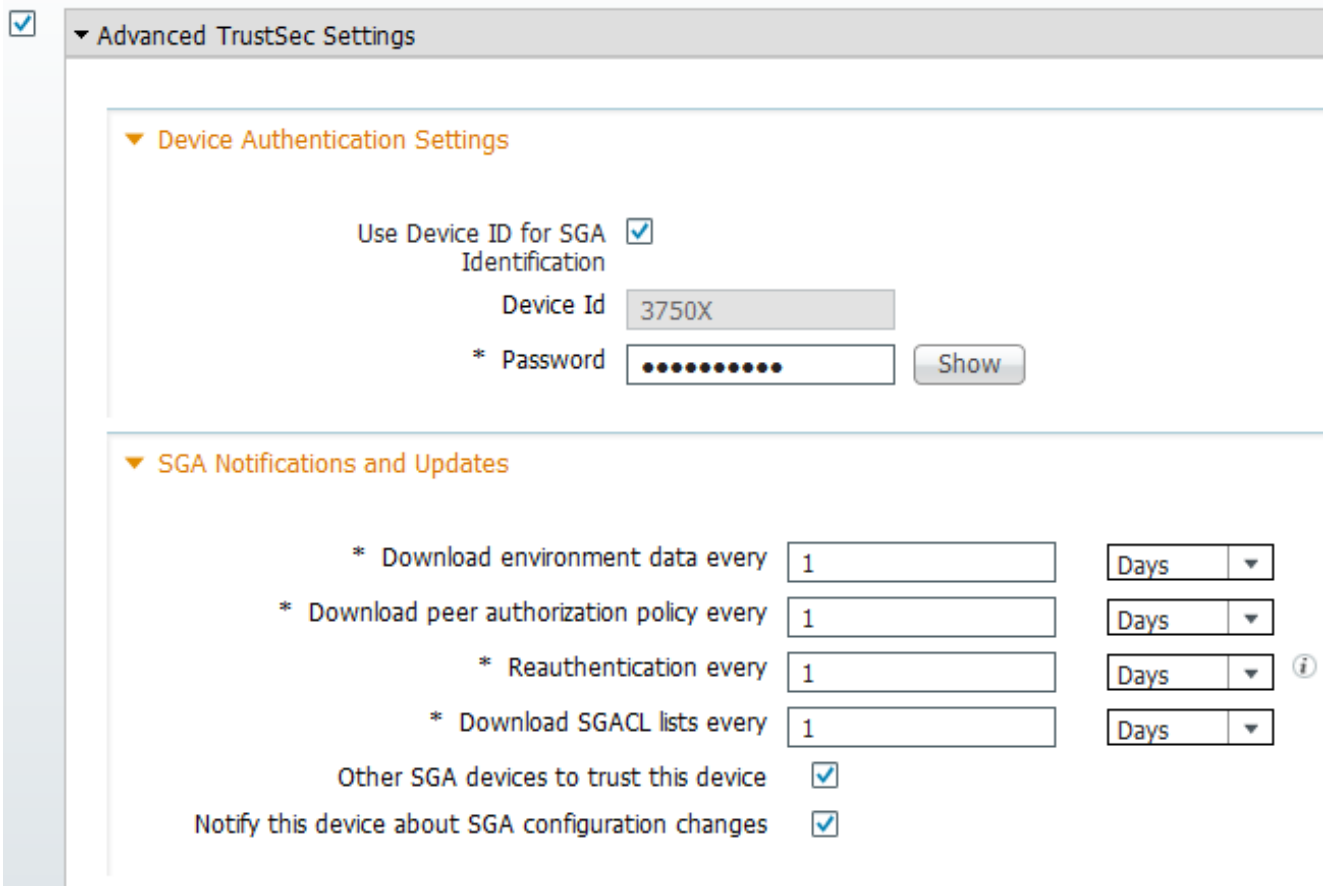
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

Vor der Aktivierung von 802.1x auf der Schnittstelle muss die ISE konfiguriert werden.

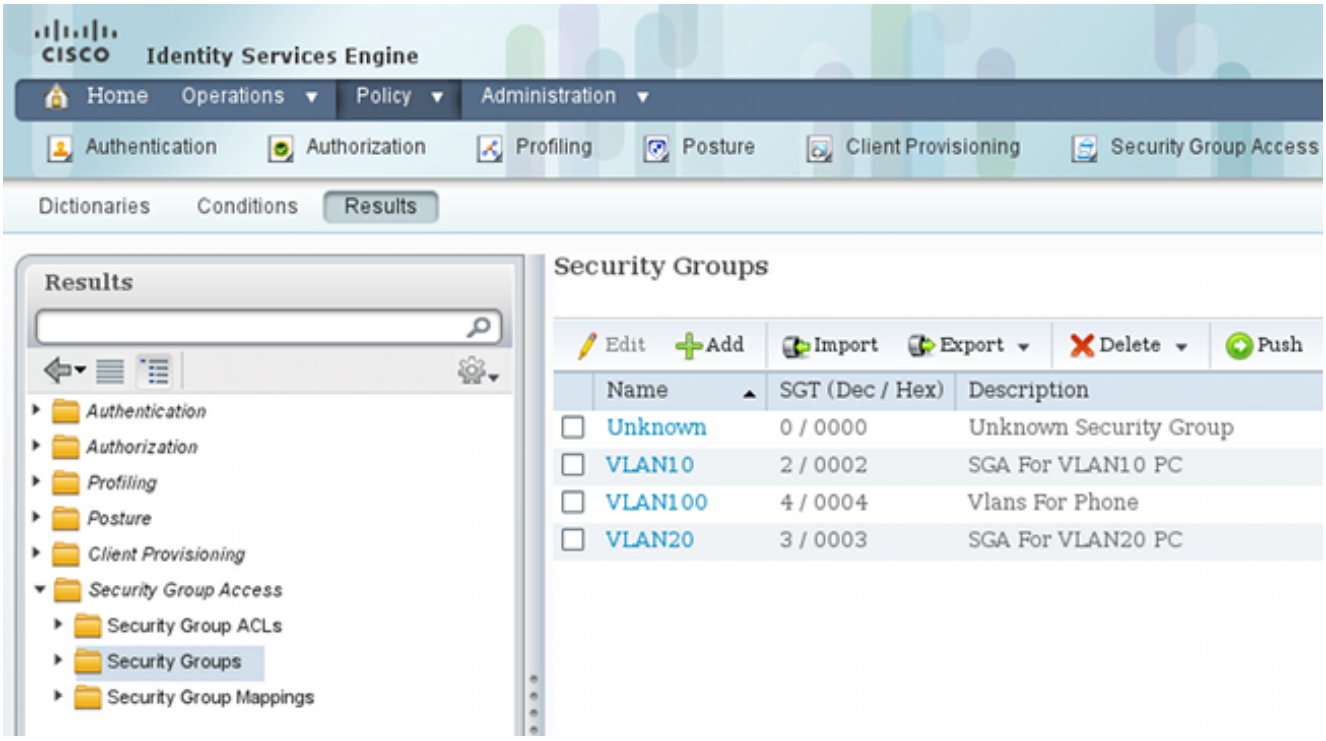
Konfigurieren der ISE

Gehen Sie wie folgt vor, um die ISE zu konfigurieren:

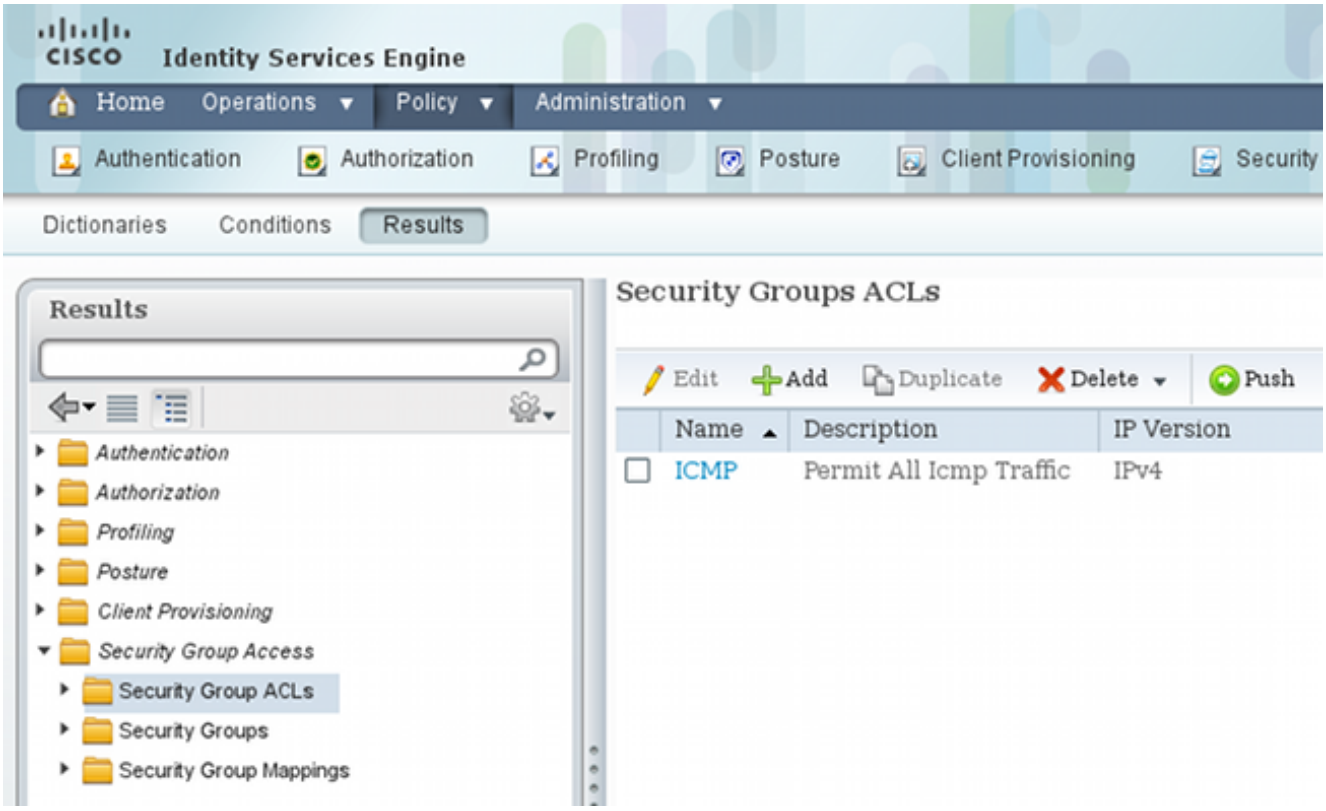
1. Navigieren Sie zu **Administration > Network Resources > Network Devices,** und fügen Sie beide Switches als Network Access Devices (NADs) hinzu. Konfigurieren Sie unter **Erweiterte TrustSec-Einstellungen** ein CTS-Kennwort zur späteren Verwendung auf der Switch-CLI.



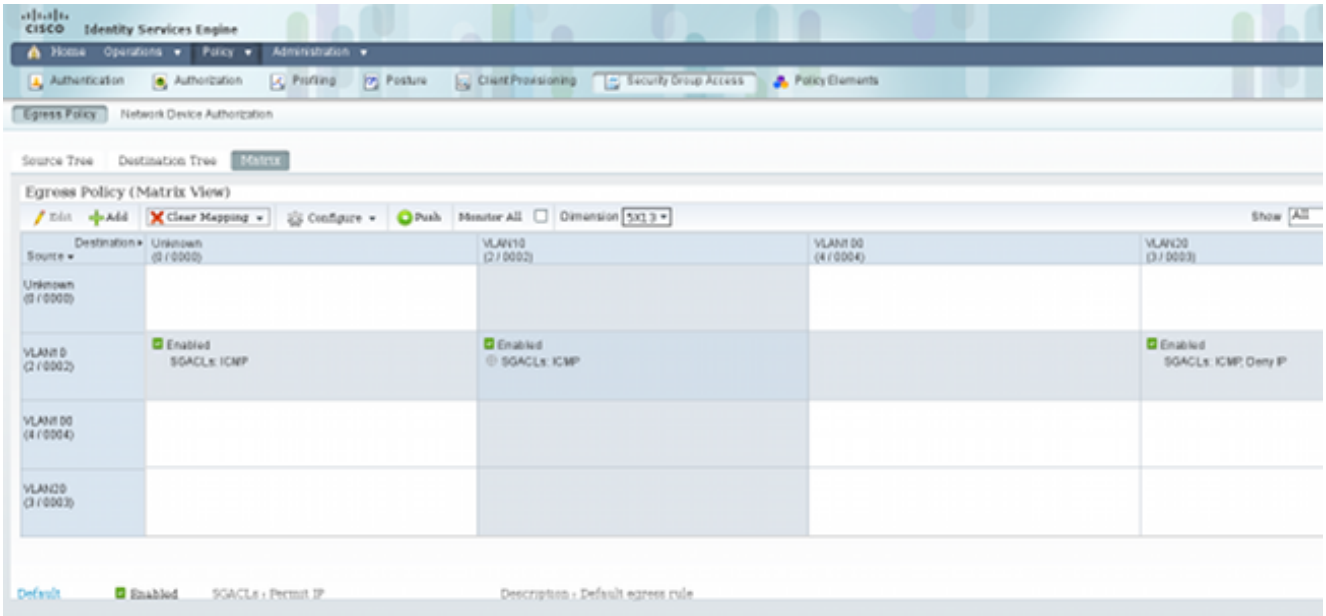
2. Navigieren Sie zu **Richtlinie > Richtlinienelemente > Ergebnisse > Sicherheitsgruppenzugriff > Sicherheitsgruppen,** und fügen Sie die entsprechenden SGTs hinzu. Diese Tags werden heruntergeladen, wenn Switches eine Aktualisierung der Umgebung anfordern.



3. Navigieren Sie zu **Policy > Policy Elements > Results > Security Group Access > Security Group ACLs**, und konfigurieren Sie eine SGACL.



4. Navigieren Sie zu **Policy > Security Group Access**, und definieren Sie eine Richtlinie mit der Matrix.



Hinweis: Sie müssen die Autorisierungsrichtlinie für die MS Windows-Komponente konfigurieren, damit diese das richtige Tag erhält. Eine detaillierte Konfiguration zu diesem Thema finden Sie im Konfigurationsbeispiel und im Leitfaden zur Fehlerbehebung für Switches der Serien ASA und Catalyst 3750X.

PAC-Bereitstellung für 3750X-5

PAC wird für die Authentifizierung in der CTS-Domäne benötigt (als Phase1 für EAP-FAST) und

wird auch verwendet, um Umgebungs- und Richtliniendaten von der ISE abzurufen. Ohne die richtige PAC können diese Daten nicht von der ISE abgerufen werden.

Nachdem Sie auf dem 3750X-5 die richtigen Anmeldeinformationen angegeben haben, wird die PAC heruntergeladen:

```
bsns-3750-5#cts credentials id 3750X password ciscocisco
bsns-3750-5#show cts pacs
 AID: C40A15A339286CEAC28A50DBBAC59784
 PAC-Info:
   PAC-type = Cisco Trustsec
   AID: C40A15A339286CEAC28A50DBBAC59784
   I-ID: 3750X
   A-ID-Info: Identity Services Engine
   Credential Lifetime: 08:31:32 UTC Oct 5 2013
 PAC-Opaque: 000200B000030001000400010C40A15A339286CEAC28A50DBBAC5978400060094
0003010076B969769CB5D45453FDCDEB92271C500000001351D15DD900093A8044DF74B2B71F
E667D7B908DB7AEEA32208B4E069FDB0A31161CE98ABD714C55CA0C4A83E4E16A6E8ACAC1D081
F235123600B91B09C9A909516D0A2B347E46D15178028ABFFD61244B3CD6F332435C867A968CE
A6B09BFA8C181E4399CE498A676543714A74B0C048A97C18684FF49BF0BB872405
 Refresh timer is set for 2y25w
```

Die PAC wird über EAP-FAST mit dem Microsoft Challenge Handshake Authentication Protocol (MSCHAPv2) heruntergeladen, wobei die Anmeldeinformationen in CLI bereitgestellt werden und die gleichen Anmeldeinformationen auf der ISE konfiguriert werden.

Die PAC wird für die Aktualisierung von Umgebung und Richtlinien verwendet. Verwenden Sie für diese Switches RADIUS-Anforderungen mit **cisco av-pair cts-pac-opaque,** das vom PAC-Schlüssel abgeleitet wird und auf der ISE entschlüsselt werden kann.

PAC-Bereitstellung für die 3750X-6- und NDAC-Authentifizierung

Damit ein neues Gerät eine Verbindung zur CTS-Domäne herstellen kann, muss 802.1x auf den entsprechenden Ports aktiviert werden.

Das SAP-Protokoll wird für die Schlüsselverwaltung und die Verhandlung der Verschlüsselungssuite verwendet. Galois Message Authentication Code (GMAC) wird für die Authentifizierung und Galois/Counter Mode (GCM) für die Verschlüsselung verwendet.

Auf dem Seed-Switch:

```
interface GigabitEthernet1/0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
sap mode-list gcm-encrypt
```

Auf dem Switch ohne Seed-Funktion:

```
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
 sap mode-list gcm-encrypt
```

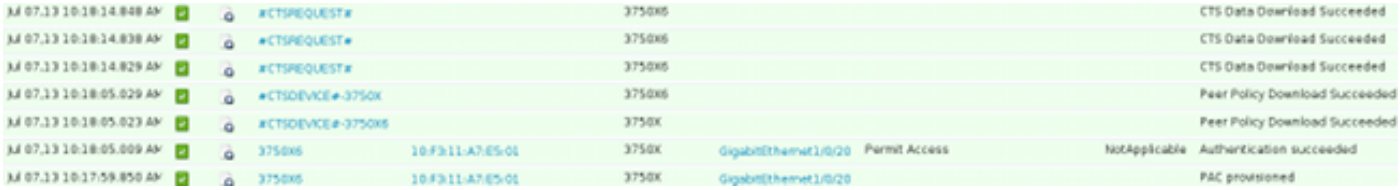
Dies wird nur auf Trunk-Ports (Switch-Switch-MACsec) unterstützt. Informationen zu Switch-Host-MACsec, die anstelle von SAP das MACsec Key Agreement (MKA)-Protokoll verwendet, finden Sie unter Konfigurieren der MACsec-Verschlüsselung.

Unmittelbar nach der Aktivierung von 802.1x an den Ports fungiert der Switch ohne Seed-Konfiguration als Komponente des Seed-Switches, der die Authentifizierung übernimmt.

Dieser Prozess wird als NDAC bezeichnet und hat zum Ziel, ein neues Gerät mit der CTS-Domäne zu verbinden. Die Authentifizierung erfolgt bidirektional. Das neue Gerät verfügt über Anmeldeinformationen, die auf dem Authentifizierungsserver ISE verifiziert werden. Nach der PAC-Bereitstellung ist das Gerät auch sicher, dass es eine Verbindung zur CTS-Domäne herstellt.

> **Hinweis**: PAC wird zum Aufbau eines TLS-Tunnels (Transport Layer Security) für EAP-FAST verwendet. Der 3750X-6 vertraut den PAC-Anmeldeinformationen, die vom Server bereitgestellt werden, ähnlich wie das Zertifikat, das der Server für den TLS-Tunnel für die EAP-TLS-Methode bereitstellt.

Mehrere RADIUS-Nachrichten werden ausgetauscht:



Die erste Sitzung des 3750X (Seed-Switch) wird für die PAC-Bereitstellung verwendet. EAP-FAST wird ohne PAC verwendet (ein anonymer Tunnel für die MSCHAPv2-Authentifizierung wird erstellt).

```
12131  EAP-FAST built anonymous tunnel for purpose of PAC provisioning
22037  Authentication Passed
11814  Inner EAP-MSCHAP authentication succeeded
12173  Successfully finished EAP-FAST CTS PAC provisioning/update
11003  Returned RADIUS Access-Reject
```

Es werden der MSCHAPv2-Benutzername und das Kennwort verwendet, die mit dem Befehl **cts** dentials konfiguriert wurden. Außerdem wird am Ende eine RADIUS Access-Reject zurückgegeben, da nach der PAC-Bereitstellung keine weitere Authentifizierung erforderlich ist.

Der zweite Eintrag im Protokoll bezieht sich auf die 802.1x-Authentifizierung. EAP-FAST wird mit der zuvor bereitgestellten PAC verwendet.

```
12168  Received CTS PAC
12132  EAP-FAST built PAC-based tunnel for purpose of authentication
11814  Inner EAP-MSCHAP authentication succeeded
15016  Selected Authorization Profile - Permit Access
11002  Returned RADIUS Access-Accept
```

Diesmal ist der Tunnel nicht anonym, sondern durch PAC geschützt. Auch hier werden die gleichen Anmeldeinformationen für die MSCHAPv2-Sitzung verwendet. Anschließend wird er anhand der Authentifizierungs- und Autorisierungsregeln auf der ISE überprüft, und es wird ein RADIUS Access-Accept zurückgegeben. Anschließend wendet der Authentifikator-Switch die zurückgegebenen Attribute an, und die 802.1x-Sitzung für diesen Port wechselt in den autorisierten Status.

Wie sieht der Prozess für die ersten beiden 802.1x-Sitzungen vom Seed-Switch aus?

Hier sind die wichtigsten Debugs aus dem Seed. Der Seed erkennt, dass der Port aktiv ist, und versucht zu bestimmen, welche Rolle für 802.1x verwendet werden soll - der Supplicant oder der Authentifikator:

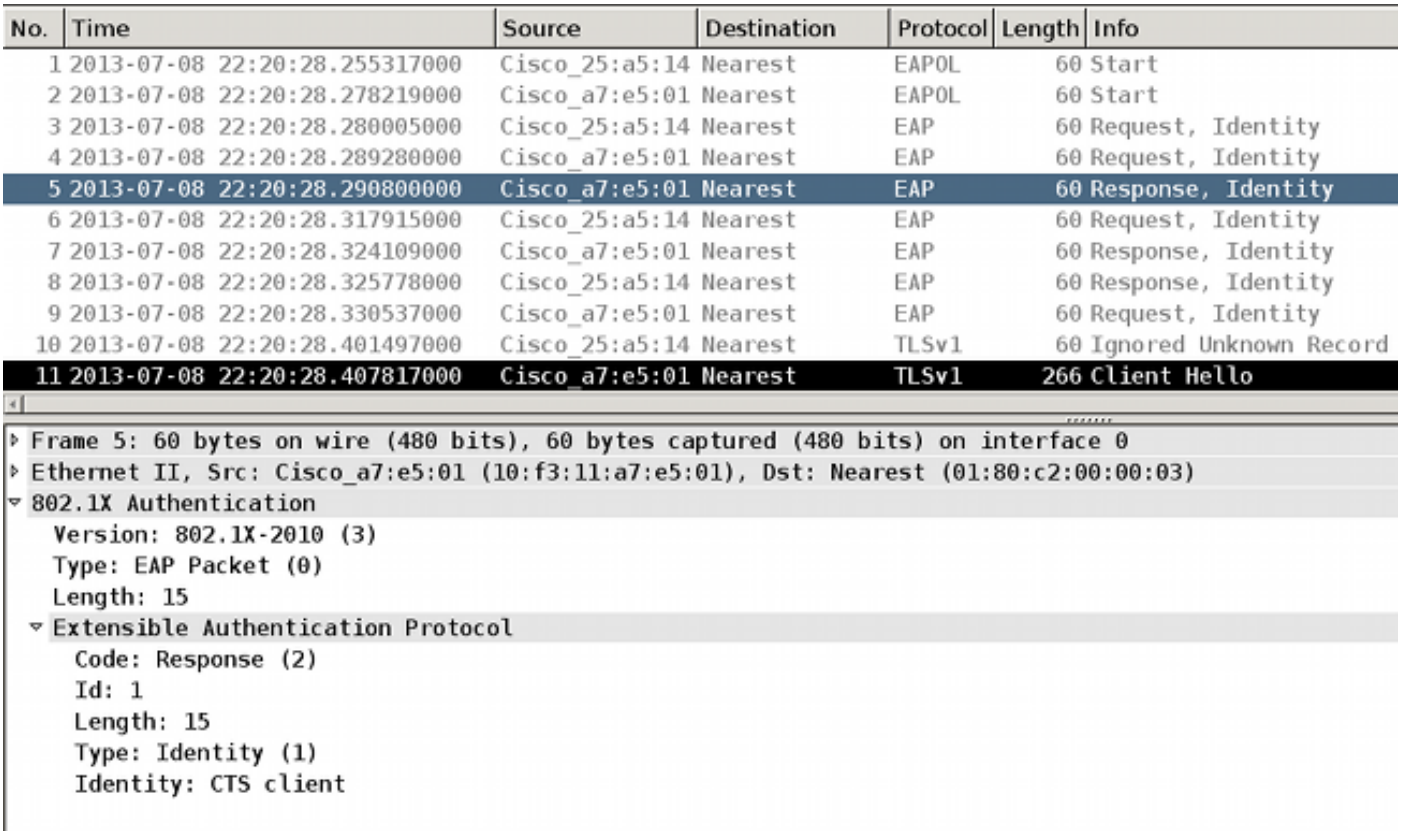
```
debug cts all
debug dot1x all
debug radius verbose
debug radius authentication

Apr 9 11:28:35.347: CTS-ifc-ev: CTS process: received msg_id CTS_IFC_MSG_LINK_UP
Apr 9 11:28:35.347: @@@ cts_ifc GigabitEthernet1/0/20, INIT: ifc_init ->
ifc_authenticating
Apr 9 11:28:35.356: CTS-ifc-ev: Request to start dot1x Both PAE(s) for
GigabitEthernet1/0/20
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created authenticator subblock
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created supplicant subblock

Apr 9 11:28:35.364: dot1x-ev:dot1x_supp_start: Not starting default supplicant
on GigabitEthernet1/0/20
Apr 9 11:28:35.381: dot1x-sm:Posting SUPP_ABORT on Client=7C24F2C

Apr 9 11:28:35.397: %AUTHMGR-5-START: Starting 'dot1x' for client (10f3.11a7.e501) on
Interface Gi1/0/20 AuditSessionID C0A800010000054135A5E32
```

Schließlich wird die Authentifizierungsrolle verwendet, da der Switch Zugriff auf die ISE hat. Auf dem 3750X-6 wird die Supplicant-Rolle ausgewählt.

Details zur 802.1x-Rollenauswahl

> **Hinweis:** Nachdem der Supplicant Switch die PAC bezieht und 802.1x-authentifiziert ist, lädt er die Umgebungsdaten herunter (später beschrieben) und ruft die IP-Adresse des AAA-Servers ab. In diesem Beispiel verfügen beide Switches über eine dedizierte (Backbone-) Verbindung für die ISE. Später können die Rollen unterschiedlich sein. Der erste Switch, der eine Antwort vom AAA-Server erhält, wird zum Authentifizierer und der zweite Switch zum Supplicant.

Dies ist möglich, da beide Switches, deren AAA-Server als ALIVE markiert ist, eine EAP-Anforderungsidentität (Extensible Authentication Protocol) senden. Diejenige, die zuerst die EAP-Identitätsantwort empfängt, wird zum Authentifizierer und verwirft nachfolgende Identitätsanforderungen.



Nach der Auswahl der 802.1x-Rolle (in diesem Szenario ist 3750X-6 die Komponente, da diese noch keinen Zugriff auf den AAA-Server hat) wird für die nächsten Pakete der EAP-FAST-Austausch zur PAC-Bereitstellung verwendet. Der Benutzername **CTS-Client** wird für den RADIUS-Anforderungsbenutzernamen und als EAP-Identität verwendet:

```
Apr  9 11:28:36.647: RADIUS:  User-Name           [1]   12  "CTS client"
Apr  9 11:28:35.481: RADIUS:  EAP-Message         [79]  17
Apr  9 11:28:35.481: RADIUS:   02 01 00 0F 01 43 54 53 20 63 6C 69 65 6E 74        [ CTS client]
```

Nachdem der anonyme EAP-FAST-Tunnel erstellt wurde, findet eine MSCHAPv2-Sitzung für den Benutzernamen **3750X6** (**CTS-Anmeldeinformationen**) statt. Dies ist auf dem Switch nicht sichtbar, da es sich um einen TLS-Tunnel (verschlüsselt) handelt. Detaillierte Protokolle auf der ISE für die PAC-Bereitstellung belegen dies jedoch. Der **CTS-Client** wird für den RADIUS-Benutzernamen und als EAP-Identitätsantwort angezeigt. Für die innere Methode (MSCHAP) wird jedoch der **3750X6**-Benutzername verwendet:

EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	EAP-FAST
Username:	3750X6
RADIUS Username :	CTS client
Calling Station ID:	10:F3:11:A7:E5:01

Die zweite EAP-FAST-Authentifizierung wird durchgeführt. Diesmal wird die zuvor bereitgestellte PAC verwendet. Auch hier wird der **CTS-Client** als RADIUS-Benutzername und äußere Identität verwendet, aber **3750X6** wird für die innere Identität (MSCHAP) verwendet. Authentifizierung erfolgreich:

RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	3750X6
MAC/IP Address:	10:F3:11:A7:E5:01
Network Device:	3750X : 10.48.66.109 : GigabitEthernet1/0/20
Allowed Protocol:	NDAC_SGT_Service
Identity Store:	Internal CTS Devices
Authorization Profiles:	Permit Access
SGA Security Group:	Unknown
Authentication Protocol :	EAP-FAST(EAP-MSCHAPv2)

Diesmal gibt die ISE jedoch mehrere Attribute im RADIUS Accept-Paket zurück:

Authentication Result

```
User-Name=3750X6
 State=ReauthSession:C0A800010000053A33FD79AF
 Class=CACS:C0A800010000053A33FD79AF:ise/162314118/3616
 Session-Timeout=86400
 Termination-Action=RADIUS-Request
 EAP-Key-Name=2b:54:e8:37:14:10:f0:3c:1b:90:f1:d7:ad:1c:0b:cc:62:e5:03:4c:6b
 cisco-av-pair=cts:security-group-tag=0000-01
 cisco-av-pair=cts:supplicant-cts-capabilities=sap
 MS-MPPE-Send-Key=ce:d6:28:6f:b4:c0:2a:96:69:93:fe:41:0d:1e:80:9d:31:e2:b8:c
 MS-MPPE-Recv-Key=d4:8c:13:cd:d7:18:c7:1f:57:21:0d:de:39:fa:cd:68:aa:ca:1b:4f
```

Hier wechselt der Authentifizierungs-Switch den Port in den autorisierten Status:

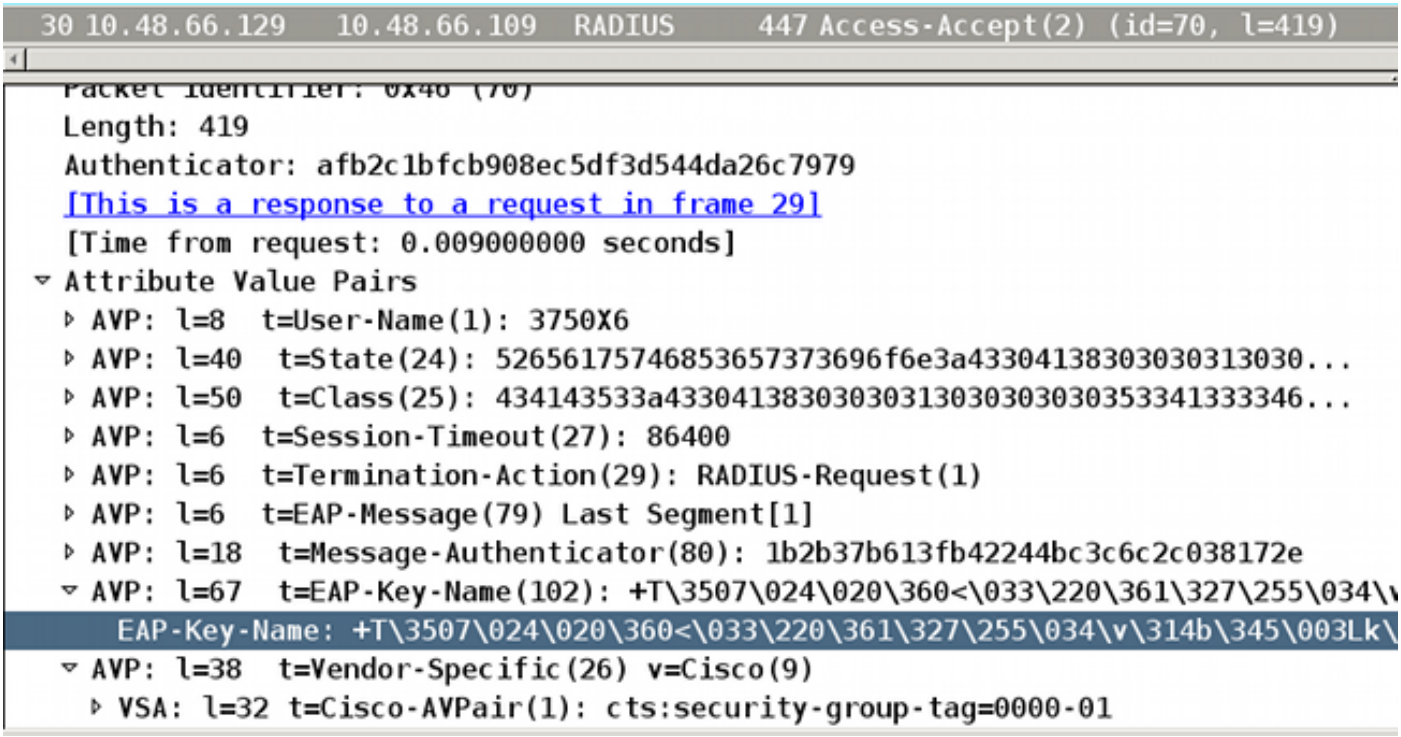
```
bsns-3750-5#show authentication sessions int g1/0/20
            Interface:  GigabitEthernet1/0/20
          MAC Address:  10f3.11a7.e501
           IP Address:  Unknown
             User-Name:  3750X6
                Status:  Authz Success
               Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
     Session timeout:  86400s (local), Remaining: 81311s
      Timeout action:  Reauthenticate
        Idle timeout:  N/A
   Common Session ID:  C0A800010000054135A5E321
     Acct Session ID:  0x0000068E
              Handle:  0x09000542

Runnable methods list:
      Method   State
      dot1x    Authc Success
```

Wie erkennt der Authentifikator-Switch, dass der Benutzername **3750X6** ist? Für den RADIUS-Benutzernamen und die äußere EAP-Identität wird der **CTS-Client** verwendet, und die innere

Identität wird verschlüsselt und für die Authentifizierung nicht sichtbar. Der Benutzername wird von der ISE übernommen. Das letzte RADIUS-Paket (Access-Accept) enthält **username=3750X6**, während alle anderen **username = CTS-Client** enthielten. Aus diesem Grund erkennt der Supplicant Switch den tatsächlichen Benutzernamen. Dieses Verhalten ist RFC-konform. Aus RFC3579 Abschnitt 3.0:

```
The User-Name attribute within the Access- Accept packet need not be the same
as the User-Name attribute in the Access-Request.
```

Im letzten Paket der 802.1x-Authentifizierungssitzung gibt die ISE die RADIUS Accept-Nachricht **cisco-av-pair** mit dem **EAP-Key-Name zurück**:

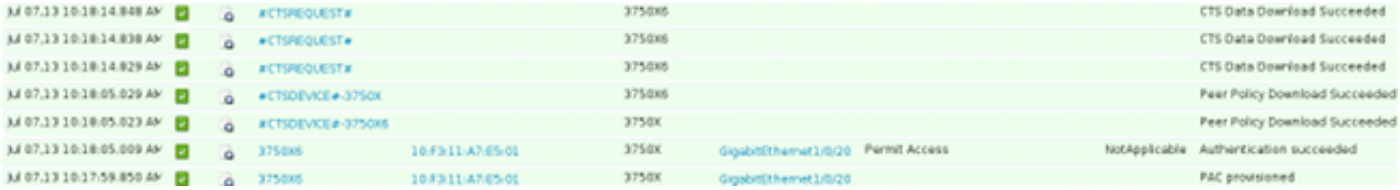


Dies wird als Schlüsselmaterial für die SAP-Verhandlung verwendet.

Außerdem wird das SGT erfolgreich ausgeführt. Das bedeutet, dass der Authentifikator-Switch den Datenverkehr des Supplikanten mit einem **Standardwert = 0** kennzeichnet. Sie können einen bestimmten Wert auf der ISE so konfigurieren, dass jeder andere Wert zurückgegeben wird. Dies gilt nur für nicht gekennzeichneten Datenverkehr. Der gekennzeichnete Datenverkehr wird nicht umgeschrieben, da der Authentifizierungs-Switch standardmäßig dem Datenverkehr der authentifizierten Komponente vertraut (dies kann jedoch auch auf der ISE geändert werden).

SGA-Richtlinien-Download

Neben den ersten beiden 802.1x EAP-FAST-Sitzungen (die erste für die PAC-Bereitstellung und die zweite für die Authentifizierung) sind weitere RADIUS-Austauschvorgänge (ohne EAP) verfügbar. Hier noch einmal die ISE-Protokolle:



Das dritte Protokoll (**Peer Policy Download)** gibt einen einfachen RADIUS-Austausch an: RADIUS Request und RADIUS Accept für den **3760X6-**Benutzer. Dies ist erforderlich, um Richtlinien für den Datenverkehr von der Komponente herunterzuladen. Die beiden wichtigsten Eigenschaften sind:

```
▾ AVP: l=31  t=Vendor-Specific(26) v=Cisco(9)
  ▸ VSA: l=25 t=Cisco-AVPair(1): cts:trusted-device=true
▾ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  ▸ VSA: l=32 t=Cisco-AVPair(1): cts:security-group-tag=0000-01
▾ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  ▸ VSA: l=32 t=Cisco-AVPair(1): cts:authorization-expiry=86400
```

Daher vertraut der Authentifikator-Switch Datenverkehr, der von der Komponente mit einem SGT markiert wurde (**cts:trusted-device=true)**, und kennzeichnet nicht gekennzeichneten Datenverkehr mit dem **Tag=0**.

Das vierte Protokoll gibt denselben RADIUS-Austausch an. Diesmal jedoch für den **3750X5-**Benutzer (Authentifikator). Dies liegt daran, dass beide Peers über eine Richtlinie für einander verfügen müssen. Interessant ist, dass der Supplicant immer noch nicht die IP-Adresse des AAA-Servers kennt. Aus diesem Grund lädt der Authentifizierungs-Switch die Richtlinie für die Komponente herunter. Diese Informationen werden später an den Supplicant (zusammen mit der ISE-IP-Adresse) in der SAP-Verhandlung weitergeleitet.

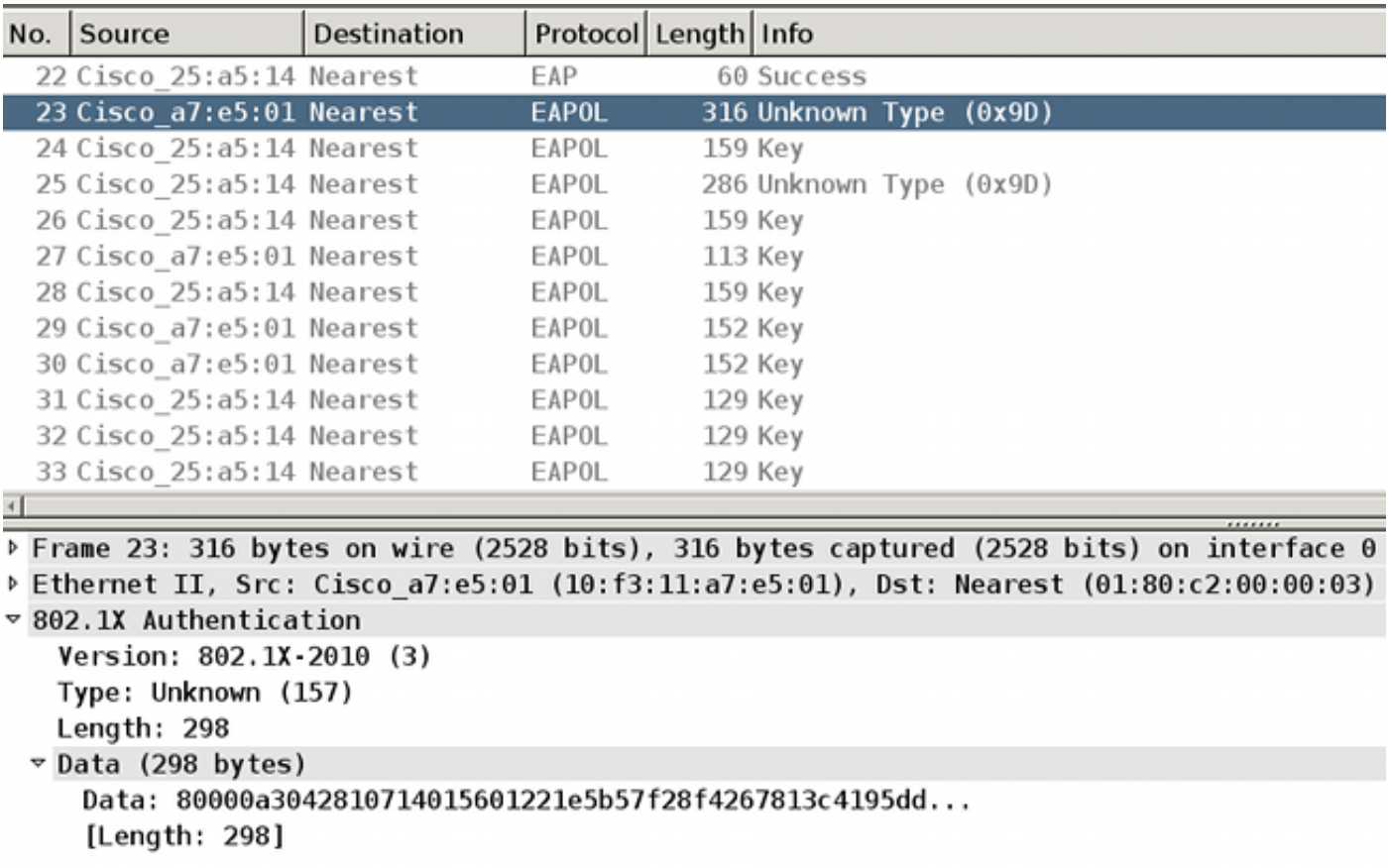
SAP-Verhandlung

Unmittelbar nach Abschluss der 802.1x-Authentifizierungssitzung findet die SAP-Aushandlung statt. Diese Verhandlung ist erforderlich, um:

- Aushandeln von Verschlüsselungsebenen (mit dem Befehl **sap mode-list gcm-encrypt**) und Verschlüsselungssuiten
- Ableitung von Sitzungsschlüsseln für Datenverkehr
- Neueingabe
- Führen Sie zusätzliche Sicherheitsüberprüfungen durch, und stellen Sie sicher, dass die vorherigen Schritte geschützt sind.

SAP ist ein Protokoll, das von Cisco Systems auf der Grundlage eines Entwurfs von 802.11i/D6.0 entwickelt wurde. Um weitere Informationen zu erhalten, fordern Sie den Zugriff auf das Cisco TrustSec Security Association Protocol an, das Cisco Trusted Security für die Cisco Nexus 7000-Seite unterstützt.

SAP Exchange ist 802.1AE-konform. Ein Extensible Authentication Protocol over LAN (EAPOL)-Schlüsselaustausch findet zwischen dem Supplicant und dem Authentifikator statt, um eine Verschlüsselungssuite auszuhandeln, Sicherheitsparameter auszutauschen und Schlüssel zu verwalten. Leider verfügt Wireshark nicht über einen Decoder für alle erforderlichen EAP-Typen:



No.	Source	Destination	Protocol	Length	Info
22	Cisco_25:a5:14	Nearest	EAP	60	Success
23	Cisco_a7:e5:01	Nearest	EAPOL	316	Unknown Type (0x9D)
24	Cisco_25:a5:14	Nearest	EAPOL	159	Key
25	Cisco_25:a5:14	Nearest	EAPOL	286	Unknown Type (0x9D)
26	Cisco_25:a5:14	Nearest	EAPOL	159	Key
27	Cisco_a7:e5:01	Nearest	EAPOL	113	Key
28	Cisco_25:a5:14	Nearest	EAPOL	159	Key
29	Cisco_a7:e5:01	Nearest	EAPOL	152	Key
30	Cisco_a7:e5:01	Nearest	EAPOL	152	Key
31	Cisco_25:a5:14	Nearest	EAPOL	129	Key
32	Cisco_25:a5:14	Nearest	EAPOL	129	Key
33	Cisco_25:a5:14	Nearest	EAPOL	129	Key

Der erfolgreiche Abschluss dieser Aufgaben führt zur Gründung einer Sicherheitszuordnung (SA).

Auf dem Supplicant Switch:

```
bsns-3750-6#show cts interface g1/0/1
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/1:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
    Authentication Status:   SUCCEEDED
       Peer identity:       "3750X"
       Peer's advertised capabilities: "sap"
       802.1X role:         Supplicant
       Reauth period applied to link:  Not applicable to Supplicant role
   Authorization Status:    SUCCEEDED
       Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
   SAP Status:              SUCCEEDED
       Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

       Replay protection:      enabled
       Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE

   Statistics:
       authc success:              12
```

```
       authc reject:              1556
       authc failure:             0
       authc no response:         0
       authc logoff:              0
       sap success:               12
       sap fail:                  0
       authz success:             12
       authz fail:                0
       port auth fail:            0

   L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/1
-----------------------------------
PAE                       = SUPPLICANT
StartPeriod               = 30
AuthPeriod                = 30
HeldPeriod                = 60
MaxStart                  = 3
Credentials profile       = CTS-ID-profile
EAP profile               = CTS-EAP-profile
```

Für den Authentifikator:

```
bsns-3750-5#show cts interface g1/0/20
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Interface Active for 00:29:22.069
   Authentication Status:   SUCCEEDED
        Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
        802.1X role:         Authenticator
       Reauth period configured:       86400 (default)
       Reauth period per policy:       86400 (server configured)
       Reauth period applied to link:  86400 (server configured)
       Reauth starts in approx. 0:23:30:37 (dd:hr:mm:sec)
       Peer MAC address is 10f3.11a7.e501
       Dot1X is initialized
   Authorization Status:    ALL-POLICY SUCCEEDED
        Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
       Version:             2
       Configured pairwise ciphers:
            gcm-encrypt
           {3, 0, 0, 0} checksum 2

       Replay protection:      enabled
       Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE
       Data loaded from NVRAM: F
       NV restoration pending: F
       Cache file name       : GigabitEthernet1_0_20_d
       Cache valid           : F
       Cache is dirty        : T
       Peer ID               : unknown
```

```
        Peer mac              : 0000.0000.0000
        Dot1X role            : unknown
        PMK                   :
             00000000 00000000 00000000 00000000
             00000000 00000000 00000000 00000000

    Statistics:
        authc success:              12
        authc reject:               1542
        authc failure:              0
        authc no response:          0
        authc logoff:               2
        sap success:                12
        sap fail:                   0
        authz success:              13
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/20
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

Hier verwenden die Ports den Modus **gcm-encrypt**, was bedeutet, dass der Datenverkehr sowohl authentifiziert und verschlüsselt als auch korrekt mit SGT markiert ist. Keines der Geräte verwendet eine bestimmte Netzwerkgeräte-Autorisierungsrichtlinie auf der ISE, d. h. der gesamte vom Gerät initiierte Datenverkehr verwendet den Standardtag **0**. Beide Switches vertrauen außerdem den vom Peer empfangenen SGTs (aufgrund von RADIUS-Attributen aus der Peer-Richtliniendownload-Phase).

Aktualisierung von Umgebung und Richtlinien

Wenn beide Geräte mit der CTS-Cloud verbunden sind, werden die Umgebung und die Richtlinien aktualisiert. Die Umgebung muss aktualisiert werden, um die SGTs und Namen abzurufen, und eine Richtlinienaktualisierung ist erforderlich, um die auf der ISE definierte SGACL herunterzuladen.

Zu diesem Zeitpunkt kennt der Supplicant bereits die IP-Adresse des AAA-Servers und kann dies somit selbst tun.

Weitere Informationen zur Umgebung und zur Aktualisierung von Richtlinien finden Sie im Konfigurationsbeispiel und im Leitfaden zur Fehlerbehebung für Switches der Serien ASA und Catalyst 3750X.

Der Supplicant Switch speichert die IP-Adresse des RADIUS-Servers, selbst wenn kein RADIUS-Server konfiguriert ist und die CTS-Verbindung ausfällt (zum Authentifikator-Switch hin). Es ist jedoch möglich, den Switch dazu zu zwingen, diesen Vorgang zu vergessen:

```
bsns-3750-6#show run | i radius
aaa authentication dot1x default group radius
```

```
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius
radius-server vsa send authentication

bsns-3750-6#show cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
         Status = ALIVE
         auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
         Status = ALIVE
         auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
    Server(10.48.66.129:1812,1646) Successful Transactions:
   Authen: 8   Author: 16      Acct: 0
   Server_auto_test_enabled: TRUE
   Keywrap enabled: FALSE

bsns-3750-6#clear cts server 10.48.66.129

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
```

Geben Sie die folgenden Befehle ein, um die Umgebung und die Richtlinien für den entsprechenden Switch zu überprüfen:

```
bsns-3750-6#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 0-01:Unknown
Server List Info:
Security Group Name Table:
    0-00:Unknown
    2-00:VLAN10
    3-00:VLAN20
    4-00:VLAN100
Environment Data Lifetime = 86400 secs
Last update time = 03:23:51 UTC Thu Mar 31 2011
Env-data expires in   0:13:09:52 (dd:hr:mm:sec)
Env-data refreshes in 0:13:09:52 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

```
bsns-3750-6#show cts role-based permissions
```

Warum werden keine Richtlinien angezeigt? Es werden keine Richtlinien angezeigt, da Sie die **Durchsetzung von Richtlinien** aktivieren müssen, um sie anzuwenden:

```
bsns-3750-6(config)#cts role-based enforcement
bsns-3750-6(config)#cts role-based enforcement vlan-list all
bsns-3750-6#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
        ICMP-20
```

Warum hat der Supplicant nur eine Richtlinie, um **Unbekannt** zu **gruppieren**, während der Authentifikator mehr hat?

```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
        ICMP-20
        Deny IP-00
```

Port-Authentifizierung für Clients

Der MS Windows-Client ist mit dem **g1/0/1-**Port des 3750-5-Switches verbunden und authentifiziert:

```
bsns-3750-5#show authentication sessions int g1/0/1
       Interface:  GigabitEthernet1/0/1
         MAC Address:  0050.5699.4ea1
           IP Address:  192.168.2.200
            User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
          Vlan Policy:  20
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
                  SGT:  0003-0
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A80001000001BD336EC4D6
     Acct Session ID:  0x000002F9
              Handle:  0xF80001BE


Runnable methods list:
      Method   State
      dot1x    Authc Success
      mab      Not run
```

Hier weiß der Switch 3750-5, dass der Datenverkehr von diesem Host mit **SGT=3** markiert werden

muss, wenn er an die CTS-Cloud gesendet wird.

Datenverkehr-Tagging mit dem SGT

Wie wird Datenverkehr ermittelt und verifiziert?

Dies ist aus folgenden Gründen schwierig:

- Embedded Packet Capture wird nur für IP-Datenverkehr unterstützt (dies ist ein modifizierter Ethernet-Frame mit SGTs und MACsec-Payload).
- Switched Port Analyzer (SPAN)-Port mit dem **Replikations-**Schlüsselwort - dies könnte funktionieren, aber das Problem ist, dass jeder PC mit Wireshark, der mit dem Ziel-Port einer Überwachungssitzung verbunden ist, die Frames aufgrund der fehlenden Unterstützung von 802.1ae verwirft, was auf Hardware-Ebene geschehen kann.
- Der SPAN-Port ohne das **Replikations**-Schlüsselwort entfernt den **cts**-Header, bevor er auf einen Zielport gesetzt wird.

Richtliniendurchsetzung mit der SGACL

Die Richtliniendurchsetzung in der CTS-Cloud erfolgt immer am Zielport. Dies liegt daran, dass nur das letzte Gerät das Ziel-SGT des Endgeräts kennt, das direkt mit diesem Switch verbunden ist. Das Paket überträgt nur die Quell-SGT. Für eine Entscheidung sind sowohl das Quell- als auch das Ziel-SGT erforderlich.

Aus diesem Grund müssen die Geräte nicht alle Richtlinien von der ISE herunterladen. Stattdessen benötigen sie nur den Teil der Richtlinie, der sich auf das SGT bezieht, mit dem das Gerät direkt verbundene Geräte hat.

Dies ist der 3750-6, der als Supplicant-Switch fungiert:

```
bsns-3750-6#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
```

Hier gibt es zwei Richtlinien. Die erste ist die Standardeinstellung für nicht gekennzeichneten Datenverkehr (von/an). Der zweite Befehl wechselt von **SGT=2** zu dem nicht gekennzeichneten SGT, das **0** ist. Diese Richtlinie ist vorhanden, da das Gerät selbst die SGA-Richtlinie der ISE verwendet und zu **SGT=0** gehört. **SGT=0** ist außerdem ein Standardtag. Daher müssen Sie alle Richtlinien herunterladen, die Regeln für den Datenverkehr **zu/von SGT=0** enthalten. Wenn Sie sich die Matrix ansehen, sehen Sie nur eine solche Richtlinie: **von 2 bis 0**.

Dies ist der 3750-5, der als Authentifizierungs-Switch dient:

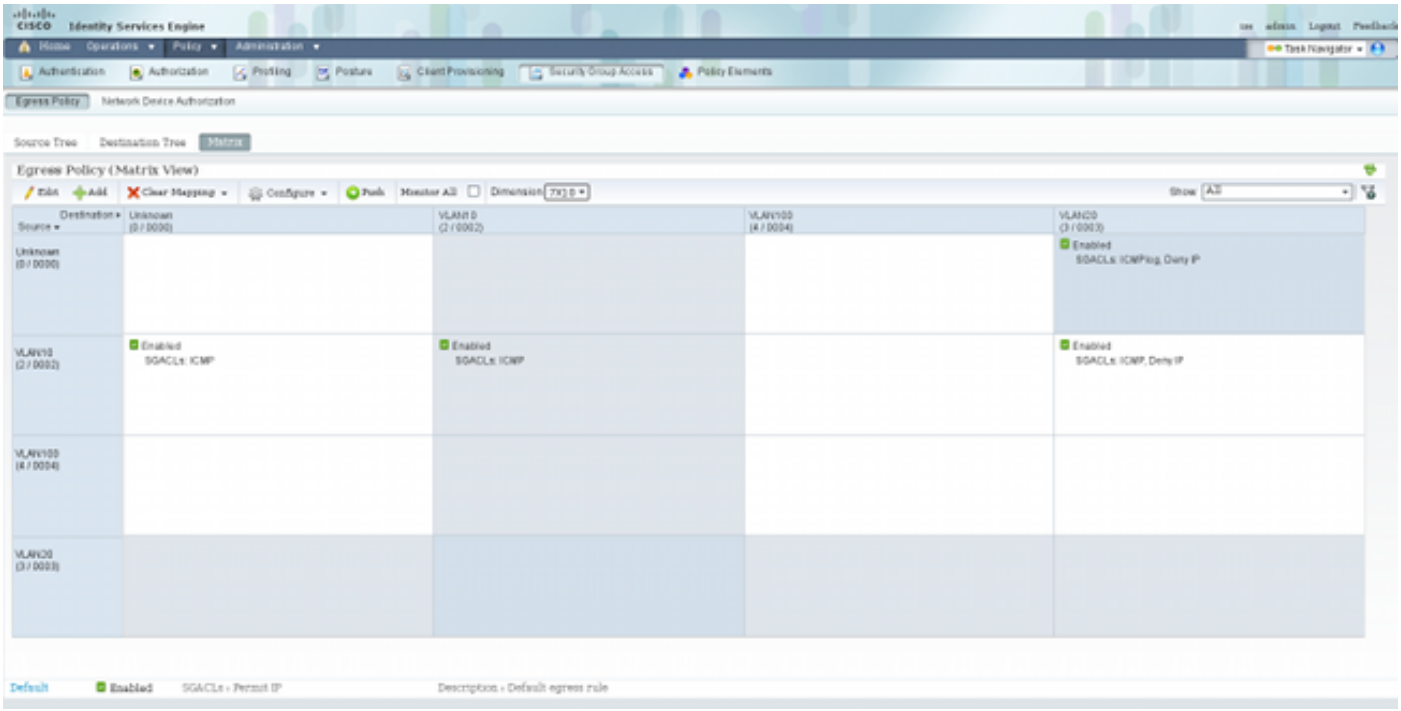
```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
```

```
        ICMP-20
        Deny IP-00
```

Hier gibt es noch eine Richtlinie: **von 2 bis 3**. Der Grund hierfür ist, dass der 802.1x-Client (MS Windows) mit **g1/0/1** verbunden und mit **SGT=3** gekennzeichnet ist. Aus diesem Grund müssen Sie alle Richtlinien **auf SGT=3** herunterladen.

Versuchen Sie, einen Ping von 3750X-6 (**SGT=0)** an MS Windows XP (**SGT=3)** zu senden. Der 3750X-5 ist das Durchsetzungsgerät.

Zuvor müssen Sie auf der ISE eine Richtlinie für den Datenverkehr von **SGT=0 bis SGT=3** konfigurieren. In diesem Beispiel wurde ein SGACL Internet Control Message Protocol (ICMP)-Protokoll erstellt, das nur die Zeile enthält, das **icmp-Protokoll zulässt** und in der Matrix für Datenverkehr von **SGT=0 bis SGT=3** verwendet:



Nachfolgend finden Sie eine Aktualisierung der Richtlinie auf dem durchsetzenden Switch und eine Überprüfung der neuen Richtlinie:

```
bsns-3750-5#cts refresh policy
Policy refresh in progress

bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group Unknown to group 3:VLAN20:
        ICMPlog-10
        Deny IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

Geben Sie den folgenden Befehl ein, um zu überprüfen, ob die Zugriffskontrollliste (ACL) von der ISE heruntergeladen wurde:

```
bsns-3750-5#show ip access-lists ICMPlog-10
Role-based IP access list ICMPlog-10 (downloaded)
   10 permit icmp log
```

Geben Sie den folgenden Befehl ein, um zu überprüfen, ob die ACL angewendet wird (Hardware-Support):

```
bsns-3750-5#show cts rbacl | b ICMPlog-10
 name   = ICMPlog-10
 IP protocol version = IPV4
 refcnt = 2
 flag   = 0x41000000
   POLICY_PROGRAM_SUCCESS
   POLICY_RBACL_IPV4
 stale  = FALSE
 ref_q:
   acl_infop(74009FC), name(ICMPlog-10)
 sessions installed:
   session hld(460000F8)
 RBACL ACEs:
 Num ACEs: 1
    permit icmp log
```

Hier sind die Zähler vor ICMP:

```
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

2       0       0               0               4099            224

*       *       0               0               321810          340989

0       3       0               0               0               0

2       3       0               0               0               0
```

Es folgt ein Ping von **SGT=0 (**Switch 3750-6) an MS Windows XP (**SGT=3**) und die Zähler:

```
bsns-3750-6#ping 192.168.2.200
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.200, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

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

2       0       0               0               4099            224

*       *       0               0               322074          341126

0       3       0               0               0               5

2       3       0               0               0               0
```

Hier sind die ACL-Zähler:

```
bsns-3750-5#show ip access-lists ICMPlog-10
Role-based IP access list ICMPlog-10 (downloaded)
    10 permit icmp log (5 matches)
```

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Cisco TrustSec-Konfigurationsleitfaden für 3750
- Cisco TrustSec-Konfigurationsleitfaden für ASA 9.1
- Cisco TrustSec-Bereitstellung und Roadmap
- 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.