ASA und Catalyst Switches der Serie 3750X - TrustSec-Konfigurationsbeispiel und Leitfaden zur Fehlerbehebung

Inhalt

Einleitung

In diesem Artikel wird beschrieben, wie Cisco TrustSec (CTS) auf der Cisco Secure Adaptive Security Appliance (ASA) und einem Cisco Catalyst Switch der Serie 3750X (3750X) konfiguriert wird.

Um die Zuordnung zwischen Sicherheitsgruppentags (SGTs) und IP-Adressen zu erlernen,

verwendet die ASA das SGT Exchange Protocol (SXP). Anschließend werden Zugriffskontrolllisten (ACLs) auf Basis des SGT verwendet, um den Datenverkehr zu filtern. Der 3750X lädt RBACL-Richtlinien (Role-Based Access Control List) von der Cisco Identity Services Engine (ISE) herunter und filtert den Datenverkehr auf Grundlage dieser Richtlinien. In diesem Artikel wird die Paketstufe beschrieben, um den Kommunikationsablauf und die erwarteten Fehlerbehebungen zu beschreiben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in diesen Themen verfügen:

- CTS-Komponenten
- CLI-Konfiguration von ASA und Cisco IOS®

Verwendete Komponenten

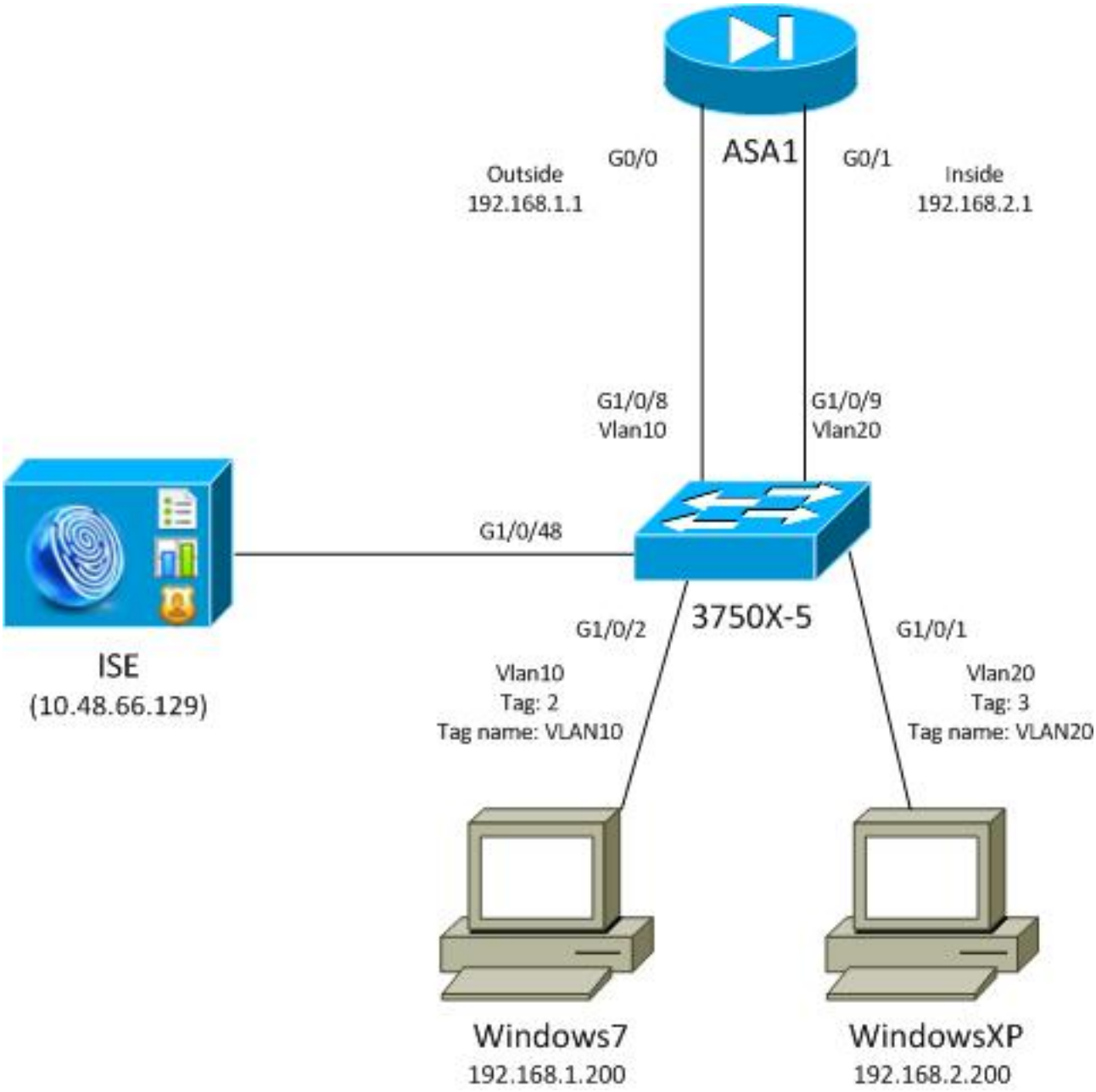
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ASA Software, Version 9.1 und höher
- Microsoft (MS) Windows 7 und MS Windows XP
- Cisco 3750X Software, Versionen 15.0 und höher
- Cisco 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



Datenverkehrsfluss

Der Datenverkehrsfluss:

- Der 3750X wird auf **G1/0/1** und **G1/0/2** für die Port-Authentifizierung konfiguriert.
- Die ISE wird als AAA-Server (Authentication, Authorization und Accounting) verwendet.
- MAC Address Bypass (MAB) wird für die Authentifizierung von MS Windows 7 verwendet.
- IEEE 802.1x wird für MS Windows XP verwendet, um zu zeigen, dass es keine Rolle spielt, welche Authentifizierungsmethode verwendet wird.

Nach erfolgreicher Authentifizierung gibt die ISE das SGT zurück, und der 3750X bindet dieses Tag an die Authentifizierungssitzung. Der Switch erfasst mit dem Befehl **ip device tracking** außerdem die IP-Adressen beider Stationen. Der Switch verwendet dann SXP, um die Zuordnungstabelle zwischen dem SGT und der IP-Adresse an die ASA zu senden. Beide MS Windows-PCs verfügen über ein Standard-Routing, das auf die ASA verweist.

Nachdem die ASA Datenverkehr von der IP-Adresse empfängt, die dem SGT zugeordnet ist, kann sie die ACL auf Basis des SGT verwenden. Wenn Sie den 3750X als Router verwenden

(Standard-Gateway für beide MS Windows-Stationen), kann er den Datenverkehr anhand von Richtlinien filtern, die von der ISE heruntergeladen wurden.

Nachfolgend sind die Schritte zur Konfiguration und Überprüfung aufgeführt, die jeweils in einem Abschnitt weiter unten im Dokument beschrieben werden:

- Port-Authentifizierung mit dem Befehl **ip device tracking** auf dem 3750X
- ISE-Konfiguration für Authentifizierungs-, SGT- und SGACL-Richtlinien (Security Group Access Control List)
- CTS-Konfiguration auf der ASA und dem 3750X
- Bereitstellung von Protected Access Credential (PAC) für den 3750X (automatisch) und die ASA (manuell)
- Umgebungsaktualisierung auf der ASA und dem 3750X
- Port-Authentifizierung, Verifizierung und Durchsetzung auf dem 3750X
- Richtlinienaktualisierung auf dem 3750X
- SXP-Austausch (ASA als Listener und 3750X als Lautsprecher)
- Datenverkehrsfilterung auf der ASA mit SGT ACL
- Datenverkehrsfilterung auf dem 3750X mit Richtlinien, die von der ISE heruntergeladen wurden

Konfigurationen

Port-Authentifizierung mit dem Befehl *ip device tracking* auf dem 3750X

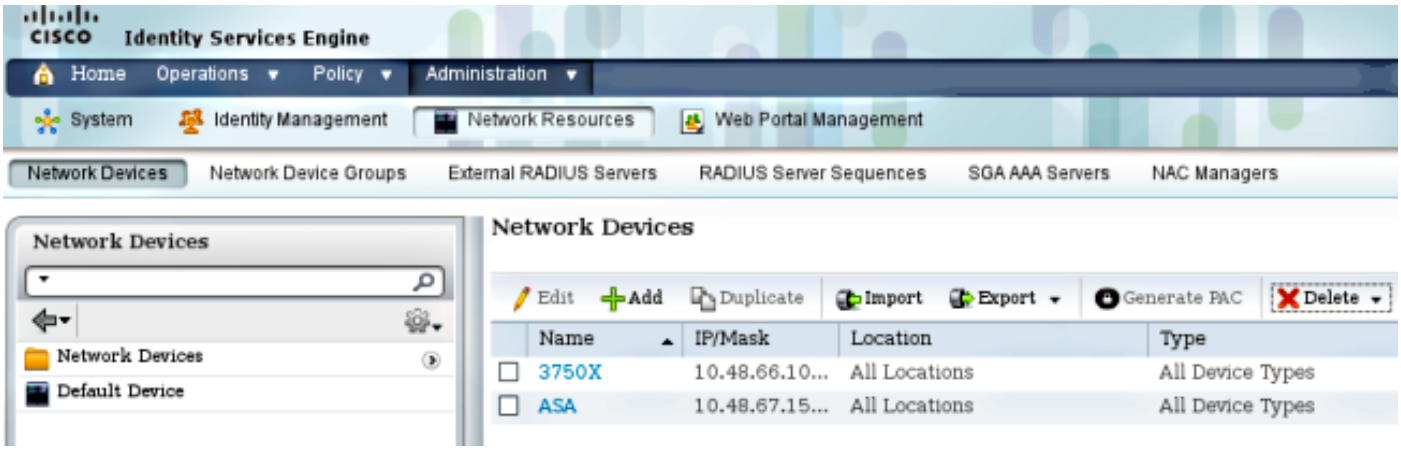
Dies ist die typische Konfiguration für 802.1x oder MAB. RADIUS Change of Authorization (CoA) ist nur erforderlich, wenn Sie eine aktive Benachrichtigung von der ISE verwenden.

```
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

!Radius COA
aaa server radius dynamic-author
 client 10.48.66.129 server-key cisco
 server-key cisco

ip device tracking

interface GigabitEthernet1/0/1
 description windowsxp
 switchport mode access
 authentication order mab dot1x
 authentication port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 description windows7
 switchport mode access
 authentication order mab dot1x
```

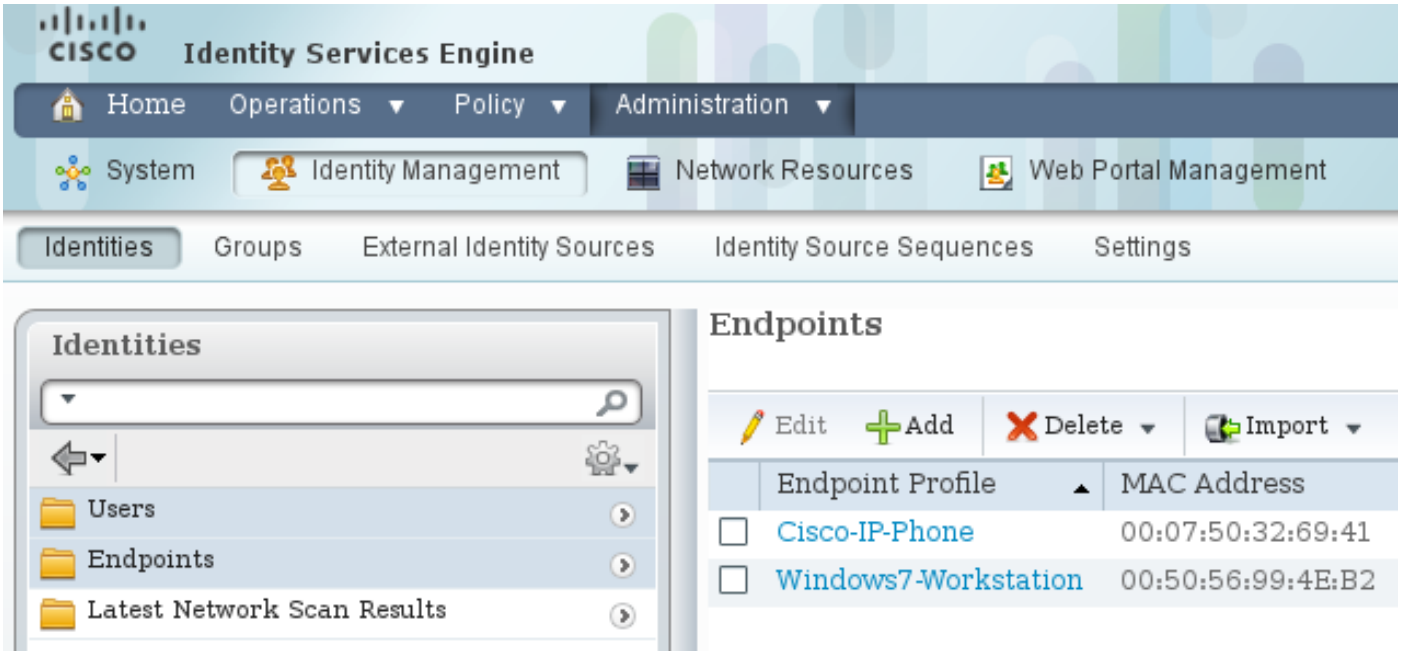
```
 authentication port-control auto
 mab
 dot1x pae authenticator
spanning-tree portfast

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
```

ISE-Konfiguration für Authentifizierung, SGT und SGACL-Richtlinien

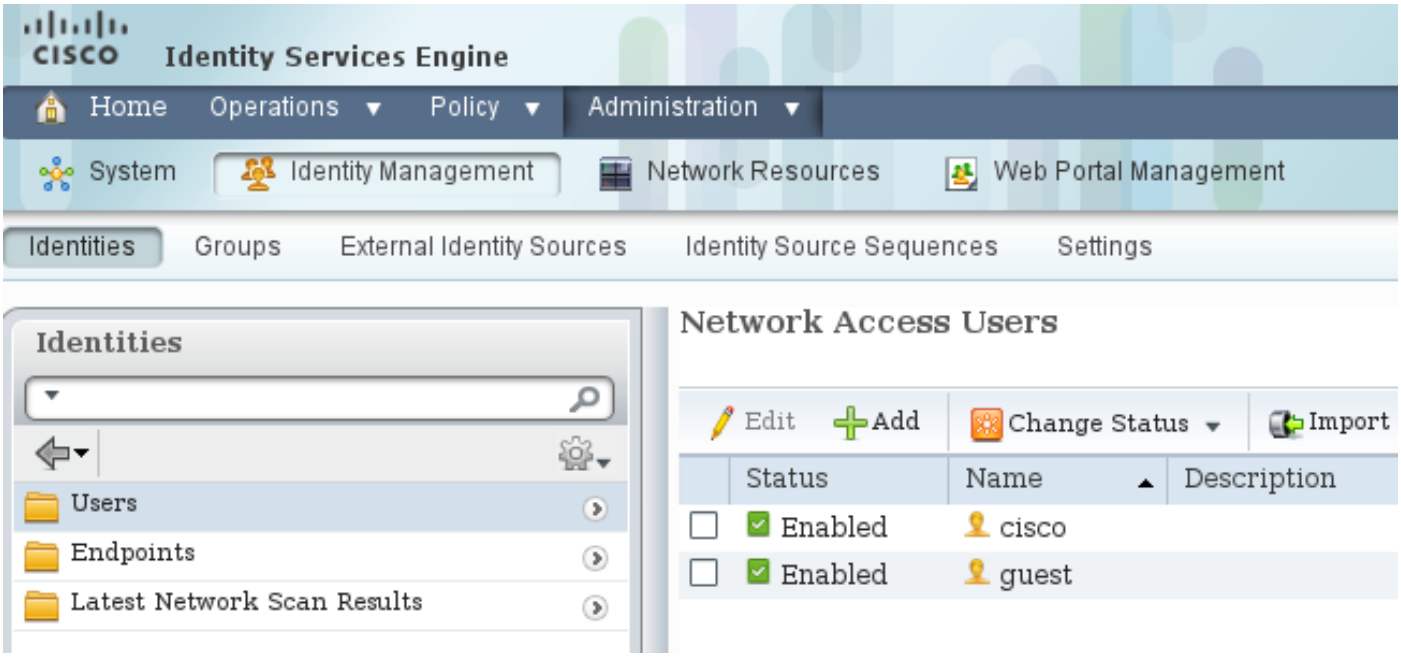
Für die ISE müssen beide Netzwerkgeräte konfiguriert sein unter **Administration > Network Devices**:



Für MS Windows 7, das die MAB-Authentifizierung verwendet, müssen Sie Endpoint Identity (MAC-Adresse) unter **Administration > Identity Management > Identities > Endpoints** erstellen:

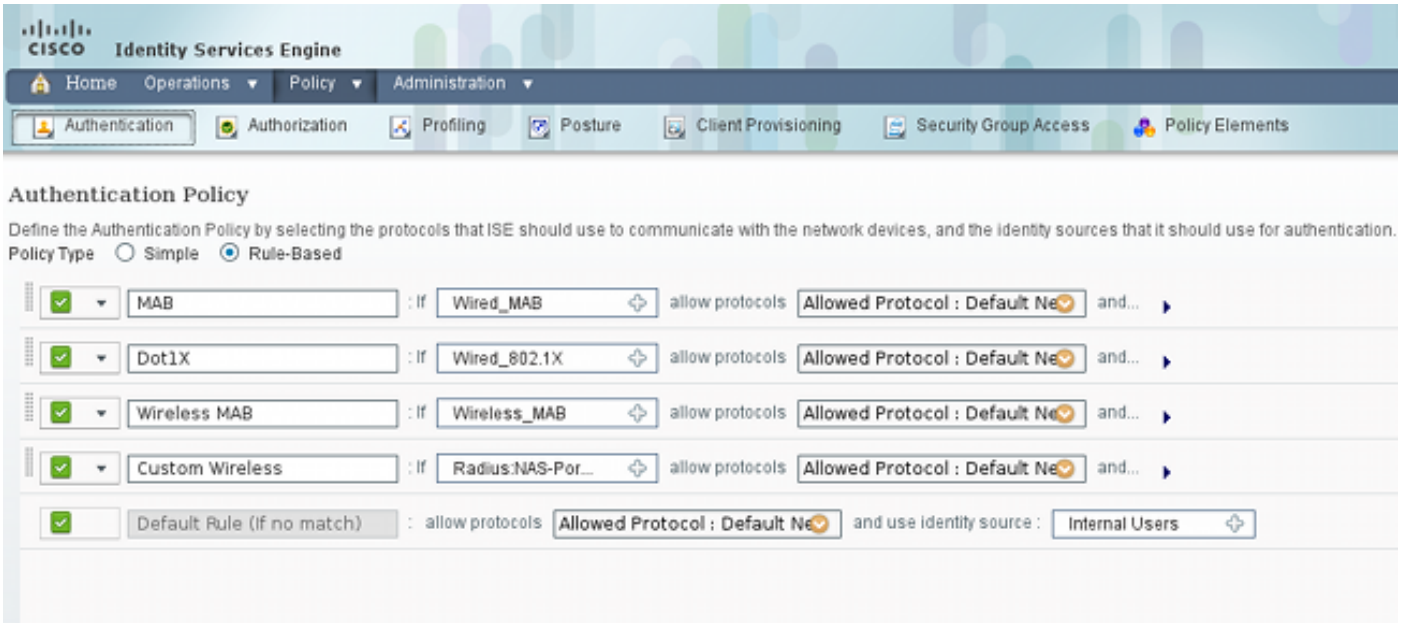


Für MS Windows XP, das die 802.1x-Authentifizierung verwendet, müssen Sie unter **Administration > Identity Management > Identities > Users** eine Benutzeridentität (Benutzername) erstellen:

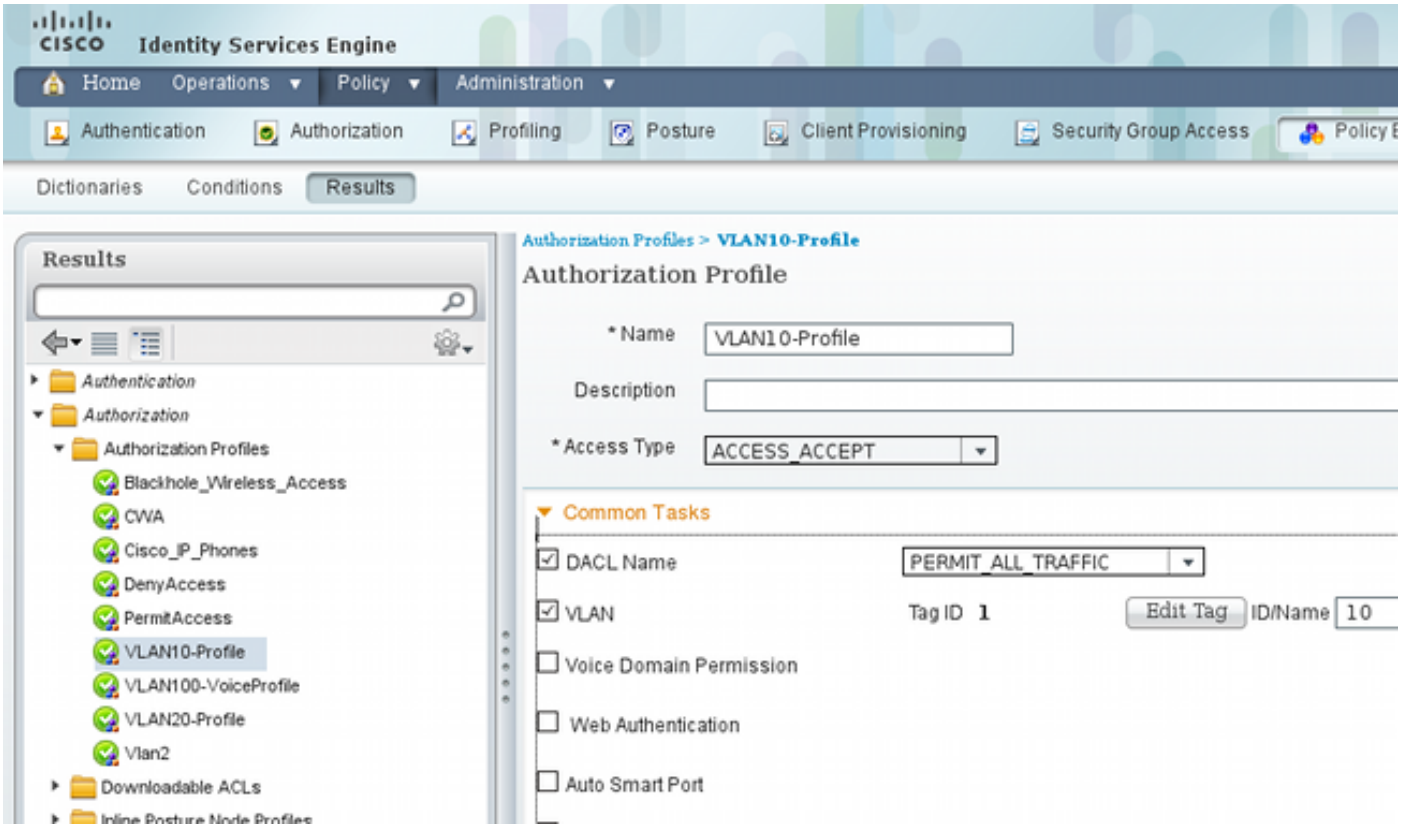


Der Benutzername **cisco** wird verwendet. Konfigurieren Sie MS Windows XP für EAP (Extensible Authentication Protocol-Protected EAP) mit diesen Anmeldeinformationen.

Auf der ISE werden die Standardauthentifizierungsrichtlinien verwendet (ändern Sie dies nicht). Die erste Richtlinie betrifft die MAB-Authentifizierung, die zweite 802.1x:



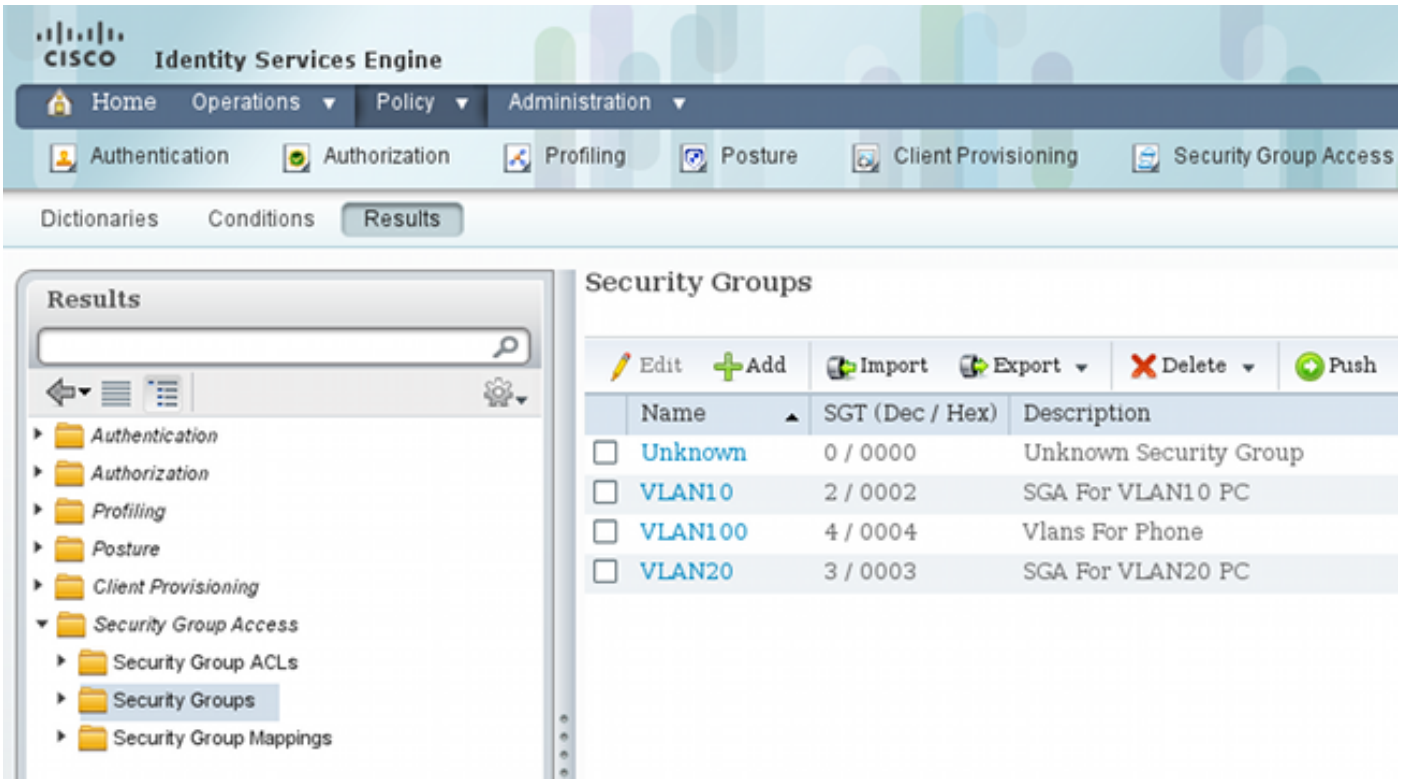
Zum Konfigurieren von Autorisierungsrichtlinien müssen Sie Autorisierungsprofile unter **Richtlinie > Ergebnisse > Autorisierung > Autorisierungsprofile** definieren. Das VLAN10-Profil mit herunterladbarer ACL (DACL), das den gesamten Datenverkehr ermöglicht, wird für das MS Windows 7-Profil verwendet:



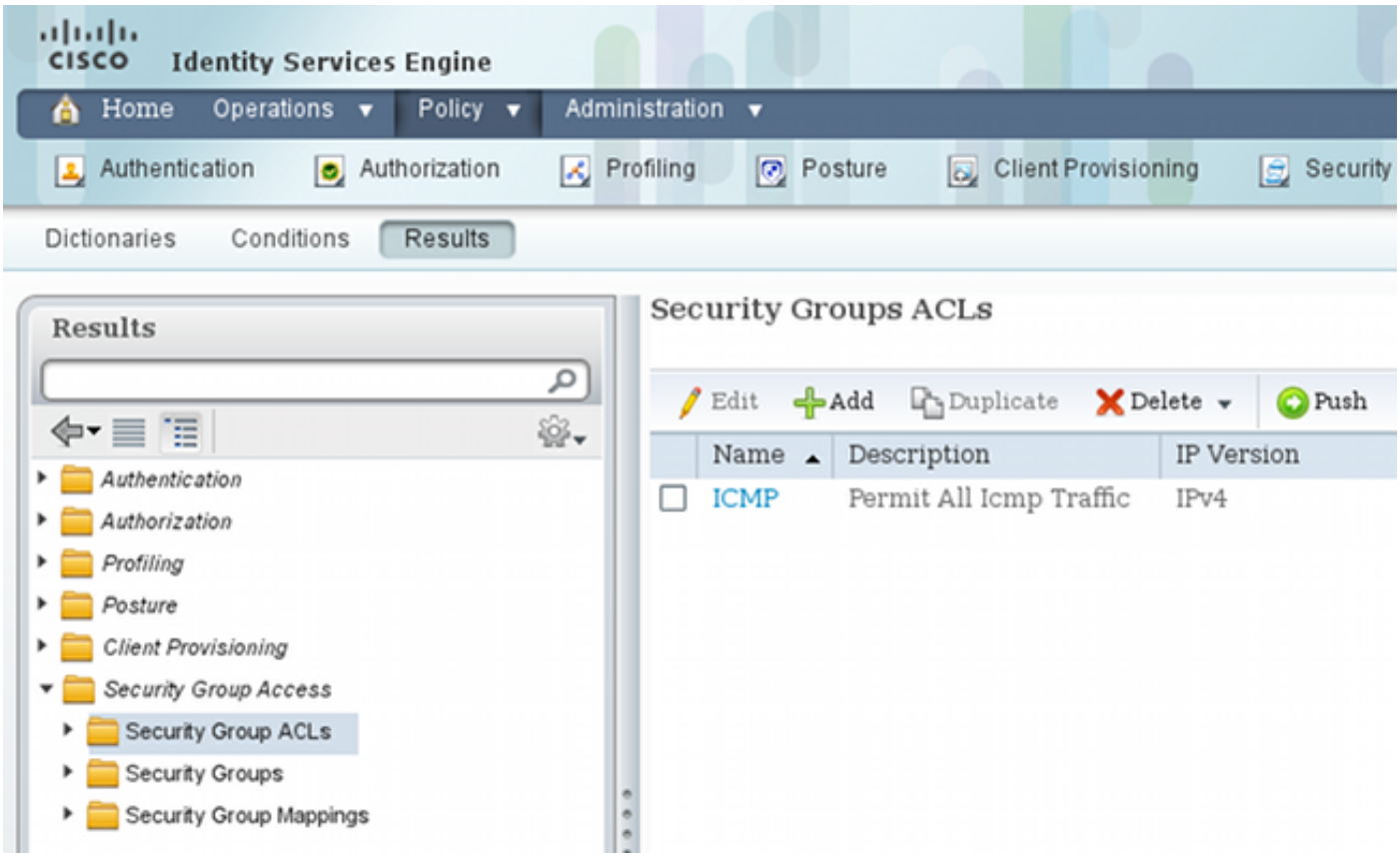
Eine ähnliche Konfiguration, VLAN20-Profile, wird für MS Windows XP verwendet, mit Ausnahme der VLAN-Nummer (20).

Um die SGT-Gruppen (Tags) auf der ISE zu konfigurieren, navigieren Sie zu **Richtlinie > Ergebnisse > Sicherheitsgruppenzugriff > Sicherheitsgruppen**.

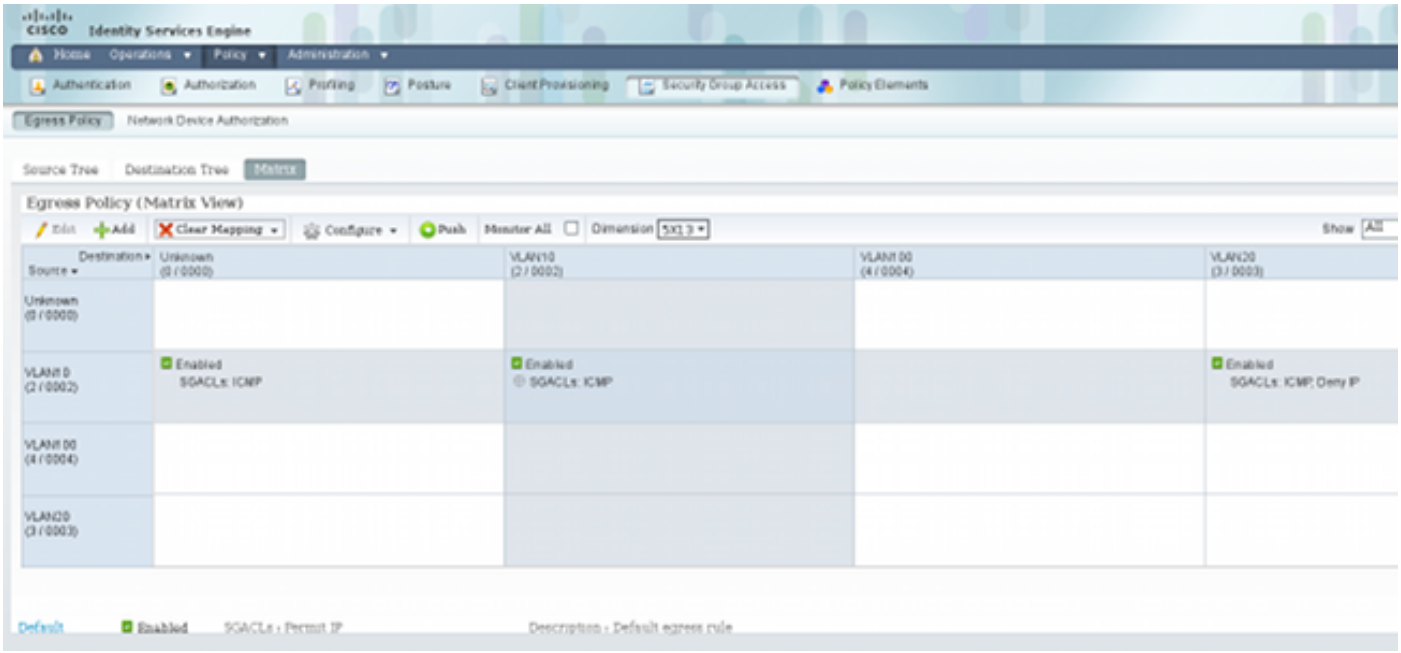
> **Hinweis**: Es ist nicht möglich, eine Tag-Nummer auszuwählen. Sie wird automatisch von der ersten freien Nummer mit Ausnahme von 1 ausgewählt. Sie können nur den SGT-Namen konfigurieren.



Um die SGACL so zu erstellen, dass ICMP-Datenverkehr (Internet Control Message Protocol) zugelassen wird, navigieren Sie zu **Policy > Results > Security Group Access > Security Group ACLs**:

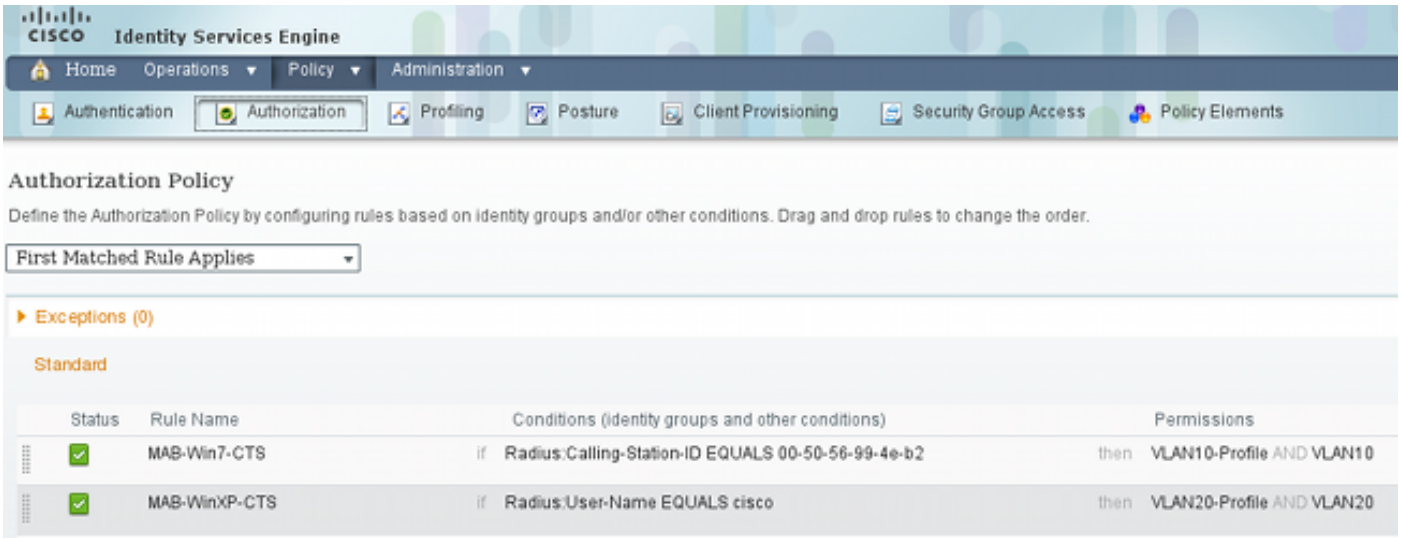


Um Richtlinien zu erstellen, navigieren Sie zu **Policy > Security Group Access > Egress Policy**. Für den Datenverkehr zwischen VLAN10 und dem unbekannten VLAN bzw. VLAN10 oder VLAN20 wird die ICMP-ACL verwendet (**permit icmp**):



Um Autorisierungsregeln festzulegen, navigieren Sie zu **Richtlinie > Autorisierung**. Für MS Windows 7 (spezifische MAC-Adresse) wird **VLAN10-Profile** verwendet, das VLAN10 und DACL zurückgibt, sowie das Sicherheitsprofil VLAN10 mit dem SGT **VLAN10**. Für MS Windows XP (spezieller Benutzername) wird **VLAN20-Profile** verwendet, das VLAN 20 und DACL zurückgibt,

sowie das Sicherheitsprofil VLAN20 mit dem SGT **VLAN20**.



Beenden Sie die Switch- und ASA-Konfiguration, damit die SGT RADIUS-Attribute akzeptiert werden.

CTS-Konfiguration auf der ASA und dem 3750X

Sie müssen grundlegende CTS-Einstellungen konfigurieren. Auf dem 3750X müssen Sie angeben, von welchem Server Richtlinien heruntergeladen werden sollen:

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

Auf der ASA wird nur der AAA-Server zusammen mit dem CTS benötigt, der auf diesen Server verweist:

```
aaa-server ISE protocol radius
aaa-server ISE (mgmt) host 10.48.66.129
 key *****
cts server-group ISE
```

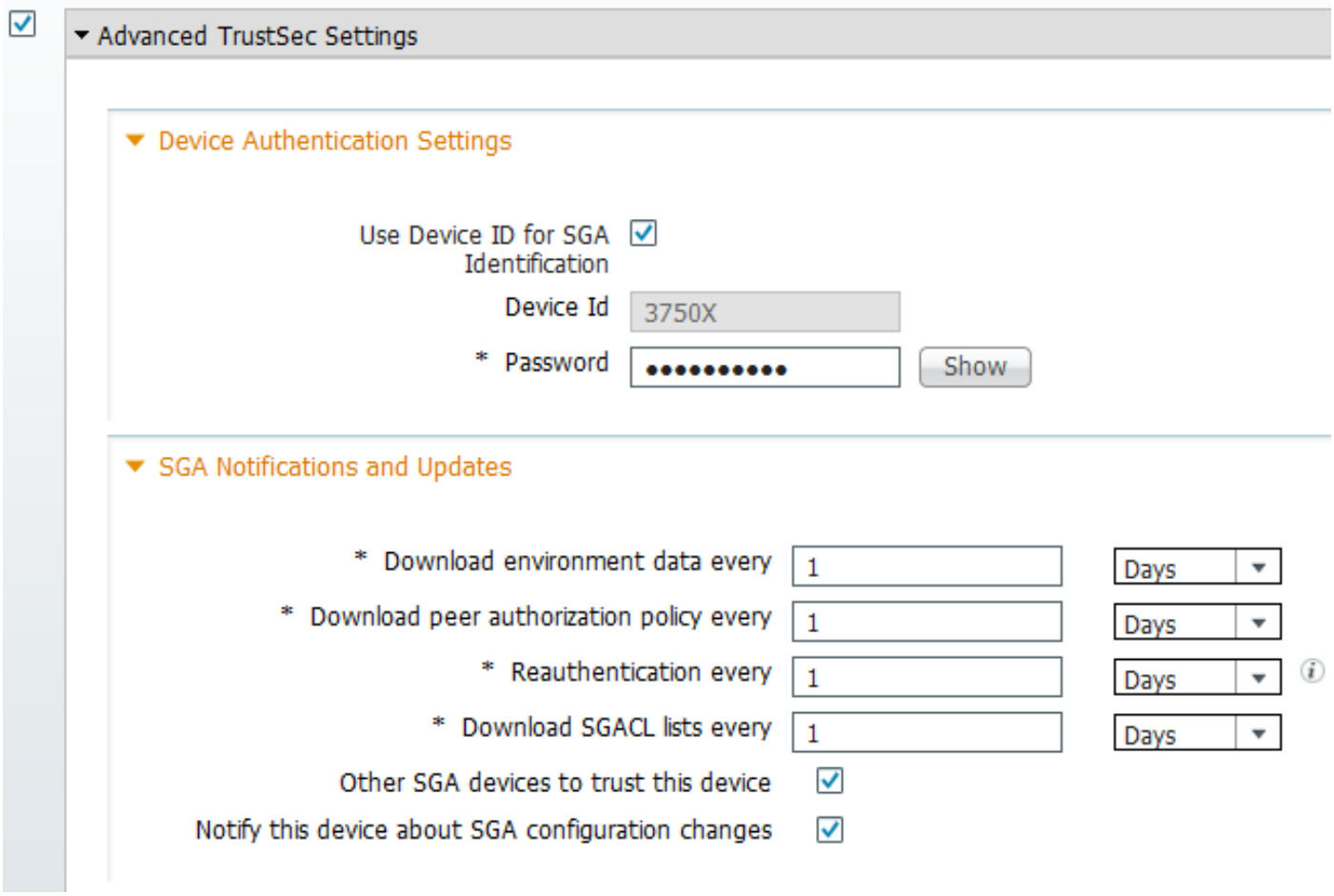
> **Hinweis**: Auf dem 3750X müssen Sie mit dem Befehl **group radius** explizit auf den ISE-Server zeigen. Der Grund hierfür ist, dass der 3750X die automatische PAC-Bereitstellung verwendet.

PAC-Bereitstellung auf dem 3750X (automatisch) und der ASA (manuell)

Jedes Gerät in der CTS-Cloud muss sich beim Authentifizierungsserver (ISE) authentifizieren, um von anderen Geräten als vertrauenswürdig eingestuft zu werden. Hierfür wird die Extensible Authentication Protocol-Flexible Authentication via Secure Protocol (EAP-FAST)-Methode (RFC 4851) verwendet. Für diese Methode muss PAC Out-of-Band bereitgestellt werden. Dieser Prozess wird auch als **phase0** bezeichnet und ist in keinem RFC definiert. PAC für EAP-FAST hat eine ähnliche Rolle wie das Zertifikat für Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). PAC wird verwendet, um einen sicheren Tunnel (Phase1) einzurichten, der für die Authentifizierung in Phase2 benötigt wird.

PAC-Bereitstellung auf dem 3750X

Der 3750X unterstützt die automatische PAC-Bereitstellung. Auf dem Switch und der ISE wird ein gemeinsam genutztes Kennwort verwendet, um PAC herunterzuladen. Dieses Kennwort und diese ID müssen auf der ISE unter **Administration > Network Resources > Network Devices (Administration > Netzwerkressourcen > Netzwerkgeräte)** konfiguriert werden. Wählen Sie den Switch aus, und erweitern Sie den Abschnitt **Erweiterte TrustSec-Einstellungen**, um Folgendes zu konfigurieren:



Damit PAC diese Anmeldeinformationen verwendet, geben Sie die folgenden Befehle ein:

```
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: 08:04:40 UTC Sep 25 2013
 PAC-Opaque: 000200B000030001000400010C40A15A339286CEAC28A50DBBAC59784000600940003
010094F559DAE0C837D7847F2454CAD7E80B0000001351C8235900093A803D7D427BFB5C6F0FBBDF
7EDF0818C58FECF97F8BDECF1B115FB0240260ADA8C96A46AA2A64C9EA2DB51E0E886768CA2D133D
2468D9D33339204BAA7E4CA2DE8E37FF1EB5BCB343408E9847998E301C26DDC6F91711F631A5B4C7
C2CB09EAB028630A3B22901FE3EF44F66FD019D09D2C46D92283
 Refresh timer is set for 2y24w
```

PAC-Bereitstellung auf der ASA

Die ASA unterstützt nur die manuelle PAC-Bereitstellung. Dies bedeutet, dass Sie es manuell auf

der ISE generieren müssen (unter Netzwerkgeräte/ASA):

Dann muss die Datei installiert werden (z.B. mit FTP):

```
bsns-asa5510-17(config)# cts import-pac ftp://ftp:ftp@10.147.25.80/ASA.pac
password ciscocisco
!PAC Imported Successfully

bsns-asa5510-17(config)# show cts pac

 PAC-Info:
   Valid until: Jul 04 2014 13:33:02
   AID:         c40a15a339286ceac28a50dbbac59784
   I-ID:        ASA
   A-ID-Info:   Identity Services Engine
   PAC-type:    Cisco Trustsec
 PAC-Opaque:
   000200a800030001000400010c40a15a339286ceac28a50dbbac597840006008c000301
   0003d64668f2badc76e251683394b3d5690000001351d15dd900093a8044df74b2b71f
   e667d7b908db7aeea3229e61462bdb70f46580bef9425011126bbf6c2f4212ccdacf08
   c01ddbc7608c3a1ddeb996ba9bfbd1b207281e3edc9ff61b9e800f225dc3f82bd5f794
   7e0a86bee8a3d437af93f54e61858bac877c58d3fe0ec6be54b4c75fad23e1fd
```

Umgebungsaktualisierung auf der ASA und dem 3750X

Zu diesem Zeitpunkt ist PAC auf beiden Geräten korrekt installiert und es werden automatisch die ISE-Umgebungsdaten heruntergeladen. Diese Daten sind im Grunde Tagnummern und ihre Namen. Um eine Umgebungsaktualisierung auf der ASA auszulösen, geben Sie den folgenden Befehl ein:

```
bsns-asa5510-17# cts refresh environment-data
```

Geben Sie den folgenden Befehl ein, um die ASA-Konfiguration zu überprüfen (die spezifischen SGT-Tags/-Namen werden leider nicht angezeigt, werden aber später überprüft):

```
bsns-asa5510-17(config)# show cts environment-data
CTS Environment Data
====================
Status:                  Active
Last download attempt:   Successful
Environment Data Lifetime: 86400 secs
Last update time:        05:05:16 UTC Apr 14 2007
Env-data expires in:     0:23:56:15 (dd:hr:mm:sec)
Env-data refreshes in:   0:23:46:15 (dd:hr:mm:sec)
```

Um dies auf dem 3750X zu überprüfen, lösen Sie mit dem folgenden Befehl eine Umgebungsaktualisierung aus:

```
bsns-3750-5#cts refresh environment-data
```

Geben Sie den folgenden Befehl ein, um die Ergebnisse zu überprüfen:

```
bsns-3750-5#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 0-01:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
         Status = ALIVE    flag(0x11)
         auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs
Security Group Name Table:
 0001-60 :
    0-47:Unknown
    2-47:VLAN10
    3-47:VLAN20
    4-47:VLAN100
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 86400 secs
Last update time = 05:33:49 UTC Thu Apr 7 2011
Env-data expires in   0:16:46:50 (dd:hr:mm:sec)
Env-data refreshes in 0:16:46:50 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

Dies zeigt, dass alle Tags und die entsprechenden Namen korrekt heruntergeladen wurden.

Port-Authentifizierungsprüfung und -durchsetzung auf dem 3750X

Wenn der 3750X über die Umgebungsdaten verfügt, müssen Sie überprüfen, ob die SGTs auf authentifizierte Sitzungen angewendet werden.

Geben Sie den folgenden Befehl ein, um zu überprüfen, ob MS Windows 7 richtig authentifiziert ist:

```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.4eb2
          IP Address:  192.168.1.200
            User-Name:  00-50-56-99-4E-B2
               Status:  Authz Success
               Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  10
```

```
            ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
                SGT:  0002-0
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A80001000001002B67334C
     Acct Session ID:  0x00000179
              Handle:  0x94000101

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

Die Ausgabe zeigt, dass VLAN10 zusammen mit dem SGT 0002 und der DACL verwendet wird, die den gesamten Datenverkehr zulassen.

Geben Sie den folgenden Befehl ein, um zu überprüfen, ob MS Windows XP richtig authentifiziert ist:

```
bsns-3750-5#sh authentication sessions interface 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:  C0A80001000000FE2B67334C
     Acct Session ID:  0x00000177
              Handle:  0x540000FF

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

Die Ausgabe zeigt, dass VLAN 20 zusammen mit dem SGT 0003 und der DACL verwendet wird, die den gesamten Datenverkehr zulassen.

IP-Adressen werden mit der IP-Geräte-Tracking-Funktion erkannt. Der DHCP-Switch muss für DHCP-Snooping konfiguriert werden. Anschließend wird nach der DHCP-Antwort mit dem Snooping die IP-Adresse des Clients ermittelt. Für eine statisch konfigurierte IP-Adresse (wie in diesem Beispiel) wird die ARP-Snooping-Funktion verwendet, und ein PC muss jedes Paket senden, damit der Switch seine IP-Adresse erkennen kann.

Für die Geräteverfolgung kann ein versteckter Befehl erforderlich sein, um sie an den Ports zu aktivieren:

```
bsns-3750-5#ip device tracking interface g1/0/1
bsns-3750-5#ip device tracking interface g1/0/2
```

```
bsns-3750-5#show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
---------------------------------------------------------------------
 IP Address     MAC Address   Vlan  Interface                STATE
---------------------------------------------------------------------
192.168.1.200   0050.5699.4eb2  10   GigabitEthernet1/0/2     ACTIVE
192.168.2.200   0050.5699.4ea1  20   GigabitEthernet1/0/1     ACTIVE

Total number interfaces enabled: 2
Enabled interfaces:
 Gi1/0/1, Gi1/0/2
```

Richtlinienaktualisierung auf dem 3750X

Der 3750X kann (im Gegensatz zur ASA) Richtlinien von der ISE herunterladen. Bevor Sie eine Richtlinie herunterladen und durchsetzen, müssen Sie sie mit den folgenden Befehlen aktivieren:

```
bsns-3750-5(config)#cts role-based enforcement
bsns-3750-5(config)#cts role-based enforcement vlan-list 1-1005,1007-4094
```

Wenn Sie die Richtlinie nicht aktivieren, wird sie heruntergeladen, aber nicht installiert und nicht zur Durchsetzung verwendet.

Um eine Richtlinienaktualisierung auszulösen, geben Sie den folgenden Befehl ein:

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

Geben Sie den folgenden Befehl ein, um zu überprüfen, ob die Richtlinie von der ISE heruntergeladen wurde:

```
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 2:VLAN10:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

Die Ausgabe zeigt, dass nur der erforderliche Teil der Richtlinie heruntergeladen wird.

In der CTS-Cloud enthält das Paket das SGT des Quell-Hosts, und **die Durchsetzung erfolgt auf dem Zielgerät**. Das bedeutet, dass das Paket von der Quelle an das letzte Gerät weitergeleitet wird, das direkt mit dem Ziel-Host verbunden ist. Dieses Gerät stellt den Durchsetzungspunkt dar, da es die SGTs seiner direkt verbundenen Hosts kennt und weiß, ob das eingehende Paket mit einem Quell-SGT für das spezifische Ziel-SGT zugelassen oder abgelehnt werden soll.

Diese Entscheidung basiert auf Richtlinien, die von der ISE heruntergeladen wurden.

In diesem Szenario werden alle Richtlinien heruntergeladen. Wenn Sie jedoch die MS Windows XP-Authentifizierungssitzung (SGT=VLAN20) löschen, muss der Switch keine Richtlinie (Zeile)

herunterladen, die VLAN20 entspricht, da keine weiteren Geräte von diesem SGT mit dem Switch verbunden sind.

Im Abschnitt "Erweitert (Fehlerbehebung)" wird erläutert, wie der 3750X unter Berücksichtigung der Paketstufe entscheidet, welche Richtlinien heruntergeladen werden sollen.

SXP Exchange (ASA als Listener und 3750X als Lautsprecher)

Die ASA unterstützt SGT nicht. Alle Frames mit SGT werden von der ASA verworfen. Aus diesem Grund kann der 3750X keine mit einem SGT gekennzeichneten Frames an die ASA senden. Stattdessen wird SXP verwendet. Dieses Protokoll ermöglicht es der ASA, Informationen über die Zuordnung zwischen den IP-Adressen und dem SGT vom Switch zu empfangen. Anhand dieser Informationen kann die ASA IP-Adressen SGTs zuordnen und auf der Grundlage von SGACL eine Entscheidung treffen.

Um den 3750X als Lautsprecher zu konfigurieren, geben Sie die folgenden Befehle ein:

```
cts sxp enable
cts sxp default source-ip 192.168.1.10
cts sxp default password cisco
cts sxp connection peer 192.168.1.1 password default mode local
```

Um die ASA als Listener zu konfigurieren, geben Sie die folgenden Befehle ein:

```
cts sxp enable
cts sxp default password *****
cts sxp default source-ip 192.168.1.1
cts sxp connection peer 192.168.1.10 password default mode local listener
```

Geben Sie den folgenden Befehl ein, um zu überprüfen, ob die ASA die Zuordnungen erhalten hat:

```
bsns-asa5510-17# show cts sxp sgt-map ipv4 detail
Total number of IP-SGT mappings : 2
Total number of IP-SGT mappings shown: 2

SGT        : 2:VLAN10
IPv4       : 192.168.1.200
Peer IP    : 192.168.1.10
Ins Num    : 1
Status     : Active
Seq Num    : 49

SGT        : 3:VLAN20
IPv4       : 192.168.2.200
Peer IP    : 192.168.1.10
Ins Num    : 1
Status     : Active
Seq Num    : 39
```

Wenn die ASA das eingehende Paket nun mit der Quell-IP-Adresse **192.168.1.200** empfängt, kann sie es wie ein **SGT=2** behandeln. Für die Quell-IP-Adresse **192.168.200.2** kann sie wie von **SGT=3** behandelt werden. Dasselbe gilt für die Ziel-IP-Adresse.

Hinweis: Der 3750X muss die IP-Adresse des verknüpften Hosts kennen. Dies erfolgt über

die IP-Geräteverfolgung. Für eine statisch konfigurierte IP-Adresse auf dem End-Host muss der Switch nach der Authentifizierung ein beliebiges Paket empfangen. Dies löst die IP-Geräteverfolgung aus, um die IP-Adresse zu ermitteln, wodurch ein SXP-Update ausgelöst wird. Wenn nur das SGT bekannt ist, wird es nicht über SXP gesendet.

Datenverkehrsfilterung auf ASA mit SGT ACL

Nachfolgend wird die ASA-Konfiguration geprüft:

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.2.1 255.255.255.0
```

Eine ACL wird erstellt und auf die interne Schnittstelle angewendet. Es ermöglicht den gesamten ICMP-Datenverkehr von **SGT=3** bis **SGT=2 (**auch als **VLAN10** bezeichnet):

```
access-list inside extended permit icmp security-group tag 3 any security-group
name VLAN10 any
access-group inside in interface inside
```

Hinweis: Sie können die Tag-Nummer oder den Tag-Namen verwenden.

Wenn Sie einen Ping von MS Windows XP mit der Quell-IP-Adresse **192.168.2.200** (**SGT=3)** an MS Windows 7 mit der IP-Adresse **192.168.1.200** (**SGT=2) senden, stellt die ASA eine Verbindung her:**

```
%ASA-6-302020: Built outbound ICMP connection for faddr 192.168.1.200/0
(2:VLAN10) gaddr 192.168.2.200/512 laddr 192.168.2.200/512(3:VLAN20)
```

Wenn Sie dasselbe mit Telnet versuchen, wird der Datenverkehr blockiert:

```
Deny tcp src inside:192.168.2.200/2478(3:VLAN20) dst outside:192.168.1.200/23
(2:VLAN10) by access-group "inside"
```

Auf der ASA gibt es weitere Konfigurationsoptionen. Es ist möglich, sowohl ein Sicherheits-Tag als auch eine IP-Adresse für die Quelle und das Ziel zu verwenden. Diese Regel ermöglicht den ICMP-Echo-Datenverkehr vom **SGT-Tag = 3** und der IP-Adresse **192.168.2.200** zum SGT-Tag **VLAN10** und zur Ziel-Host-Adresse **192.168.1.200**:

```
access-list inside extended permit icmp security-group tag 3 host 192.168.2.200
security-group name VLAN10 host 192.168.1.200 echo
```

Dies kann auch mit Objektgruppen erreicht werden:

```
object-group security SGT-VLAN-10
 security-group name VLAN10
```

```
object-group security SGT-VLAN-20
 security-group tag 3
object-group network host1
 network-object host 192.168.1.200
object-group network host2
 network-object host 192.168.2.200
object-group service my-icmp-echo
 service-object icmp echo

access-list inside extended permit object-group my-icmp-echo
object-group-security SGT-VLAN-20 object-group host2 object-group-security
SGT-VLAN-10 object-group host1
```

Datenverkehrsfilterung auf dem 3750X mit von der ISE (RBACL) heruntergeladenen Richtlinien

Es ist auch möglich, lokale Richtlinien auf dem Switch zu definieren. In diesem Beispiel werden jedoch Richtlinien dargestellt, die von der ISE heruntergeladen wurden. Auf der ASA definierte Richtlinien dürfen sowohl IP-Adressen als auch SGTs (und den Benutzernamen aus Active Directory) in einer Regel verwenden. Die auf dem Switch definierten Richtlinien (lokal und von der ISE) lassen nur SGTs zu. Wenn Sie IP-Adressen in Ihren Regeln verwenden müssen, wird die Filterung auf der ASA empfohlen.

Der ICMP-Datenverkehr zwischen MS Windows XP und MS Windows 7 wurde getestet. Hierfür müssen Sie das Standard-Gateway von ASA auf 3750X unter MS Windows ändern. Der 3750X verfügt über Routing-Schnittstellen und kann die Pakete routen:

```
interface Vlan10
 ip address 192.168.1.10 255.255.255.0
!
interface Vlan20
 ip address 192.168.2.10 255.255.255.0
```

Die Richtlinien werden bereits von der ISE heruntergeladen. Geben Sie den folgenden Befehl ein, um diese zu überprüfen:

```
 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 2:VLAN10:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

Der Datenverkehr von VLAN10 (MS Windows 7) zu VLAN20 (MS Windows XP) unterliegt der ICMP-20 ACL, die von der ISE heruntergeladen wird:

```
bsns-3750-5#show ip access-lists ICMP-20
Role-based IP access list ICMP-20 (downloaded)
   10 permit icmp
```

Geben Sie den folgenden Befehl ein, um die ACL zu überprüfen:

```
bsns-3750-5#show cts rbacl
CTS RBACL Policy
================
RBACL IP Version Supported: IPv4
 name   = Deny IP-00
 IP protocol version = IPV4
 refcnt = 2
 flag   = 0x41000000
 stale  = FALSE
 RBACL ACEs:
   deny ip

  name   = ICMP-20
 IP protocol version = IPV4
 refcnt = 6
 flag   = 0x41000000
 stale  = FALSE
 RBACL ACEs:
    permit icmp

 name   = Permit IP-00
 IP protocol version = IPV4
 refcnt = 2
 flag   = 0x41000000
 stale  = FALSE
 RBACL ACEs:
   permit ip
```

Geben Sie den folgenden Befehl ein, um die SGT-Zuordnung zu überprüfen und sicherzustellen, dass der Datenverkehr von beiden Hosts korrekt gekennzeichnet ist:

```
bsns-3750-5#show cts role-based sgt-map all
Active IP-SGT Bindings Information

IP Address              SGT     Source
============================================
192.168.1.200           2       LOCAL
192.168.2.200           3       LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2
```

ICMP von MS Windows 7 (**SGT=2**) zu MS Windows XP (**SGT=3**) funktioniert mit ACL ICMP-20 einwandfrei. Dies wird durch die Überprüfung der Zähler für den Datenverkehr von **2** bis **3 (**15 zulässige Pakete) überprüft:

```
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               1695            224
2       2       0               -               0               -
```

```
*       *       0               0               133258          132921

2       3       0               0               0               15
```

Wenn Sie versuchen, den Telnet-Zähler zu verwenden, nehmen die abgelehnten Pakete zu (dies ist für ICMP-20 ACL nicht zulässig):

```
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               1695            224
2       2       0               -               0               -

*       *       0               0               133281          132969

2       3       0               2               0               15
```

> **Hinweis:** Das in der Ausgabe angezeigte Sternzeichen (*) bezieht sich auf den gesamten Datenverkehr, der nicht gekennzeichnet ist (diese Spalte und Zeile wird in Matrix auf der ISE als **unbekannt** bezeichnet, und Tag-Nummer **0** wird verwendet).

Wenn Sie einen ACL-Eintrag mit dem log-Schlüsselwort (definiert auf der ISE) haben, werden die entsprechenden Paketdetails und durchgeführten Aktionen wie in jeder ACL mit dem log-Schlüsselwort protokolliert.

Überprüfung

Nachweisverfahren finden Sie in den einzelnen Konfigurationsabschnitten.

Fehlerbehebung

PAC-Bereitstellung

Bei der automatischen PAC-Bereitstellung können Probleme auftreten. Denken Sie daran, das **pac**-Schlüsselwort für den RADIUS-Server zu verwenden. Bei der automatischen PAC-Bereitstellung auf dem 3750X wird die EAP-FAST-Methode mit dem Extensible Authentication Protocol verwendet, wobei die interne Methode die EAP-MSCHAPv2-Authentifizierung (Challenge Handshake Authentication Protocol) von Microsoft verwendet. Beim Debuggen werden mehrere RADIUS-Nachrichten angezeigt, die Teil der EAP-FAST-Aushandlung sind, die zum Erstellen des sicheren Tunnels verwendet wird. Dabei wird EAP-MSCHAPv2 mit der konfigurierten ID und dem konfigurierten Kennwort für die Authentifizierung verwendet.

Die erste RADIUS-Anforderung verwendet AAA **service-type=cts-pac-provisioning,** um die ISE darüber zu informieren, dass es sich um eine PAC-Anforderung handelt.

```
bsns-3750-5#debug cts provisioning events
bsns-3750-5#debug cts provisioning packets
```

```
*Mar  1 09:55:11.997: CTS-provisioning: New session socket: src=
10.48.66.109:57516 dst=10.48.66.129:1645
*Mar  1 09:55:11.997: CTS-provisioning: Sending EAP Response/Identity to
10.48.66.129
*Mar  1 09:55:11.997: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:11.997: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:11.997: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.006: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.006: CTS-provisioning: Sending EAPFAST response to
10.48.66.129
*Mar  1 09:55:12.006: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.106: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.115: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.744: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.744: CTS-provisioning: Sending EAPFAST response to
10.48.66.129
*Mar  1 09:55:12.744: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.844: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.844: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.853: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.853: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.853: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.853: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.861: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.861: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.861: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.861: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.878: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.878: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.886: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.886: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.886: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.895: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.895: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.895: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.895: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.903: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.912: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.912: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.920: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.920: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.920: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.928: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.928: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.970: CTS-pac-refresh: PAC C40A15A339286CEAC28A50DBBAC59784
refresh timer has been set for 20y30w
*Mar  1 09:55:12.970: CTS-provisioning: Ignoring key data.
*Mar  1 09:55:12.979: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.979: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.979: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.995: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.995: CTS-provisioning: Received RADIUS reject from 10.48.66.129.
*Mar  1 09:55:12.995: CTS-provisioning: Successfully obtained PAC for A-ID
c40a15a339286ceac28a50dbbac59784
*Mar  1 09:55:12.995: CTS-provisioning: cts_provi_server_cleanup: 10.48.66.129
```

```
*Mar  1 09:55:12.995: CTS-provisioning: work complete, process terminating.
```

Das **RADIUS-Ablehnen** am Ende der Ausgabe wird erwartet, da Sie PAC bereits empfangen haben und keinen weiteren Authentifizierungsprozess durchgeführt haben.

Beachten Sie, dass PAC für alle anderen Kommunikationen mit der ISE erforderlich ist. Wenn dies jedoch nicht der Fall ist, versucht der Switch dennoch, die Umgebung oder die Richtlinien zu aktualisieren, wenn er konfiguriert ist. Anschließend fügt er **cts-opaqueue (**PAC) nicht an die RADIUS-Anforderungen an, wodurch die Fehler verursacht werden.

Wenn Ihr PAC-Schlüssel falsch ist, wird diese Fehlermeldung auf der ISE angezeigt:

```
The Message-Authenticator RADIUS attribute is invalid
```

Sie sehen auch diese Ausgabe von debugs (**debug cts provisioning + debug radius**) auf dem Switch, wenn Ihr PAC-Schlüssel falsch ist:

```
Apr 20 10:07:11.768: CTS-provisioning: Sending EAP Response/Identity t
Apr 20 10:07:15.325: RADIUS(0000024B): Request timed out!
Apr 20 10:07:15.325: RADIUS: No response from (10.62.84.224:1645,1646) for
id 1645/37
```

Wenn Sie die Konvention des modernen **Radius-Servers** verwenden, wird Folgendes angezeigt:

```
radius server KRK-ISE
 address ipv4 10.62.84.224 auth-port 1645 acct-port 1646
 pac key CISCO
```

> **Hinweis**: Sie müssen für die ISE dasselbe Kennwort verwenden, das Sie in den **Geräteauthentifizierungseinstellungen** verwendet haben.

Nach erfolgreicher PAC-Bereitstellung wird auf der ISE Folgendes angezeigt:

Authentication Summary	
Logged At:	June 26,2013 1:36:32.676 PM
RADIUS Status:	PAC provisioned
NAS Failure:	
Username:	3750
MAC/IP Address:	BC:16:65:25:A5:00
Network Device:	3750X : 10.48.66.109 :
Allowed Protocol:	NDAC_SGT_Service
Identity Store:	Internal CTS Devices
Authorization Profiles:	
SGA Security Group:	
Authentication Protocol :	EAP-FAST(EAP-MSCHAPv2)

Umgebungsaktualisierung

Die Umgebungsaktualisierung wird verwendet, um grundlegende Daten von der ISE zu erhalten,

die die SGT-Nummer und den Namen enthalten. Auf Paketebene werden nur drei RADIUS-Anforderungen und -Antworten mit Attributen angezeigt.

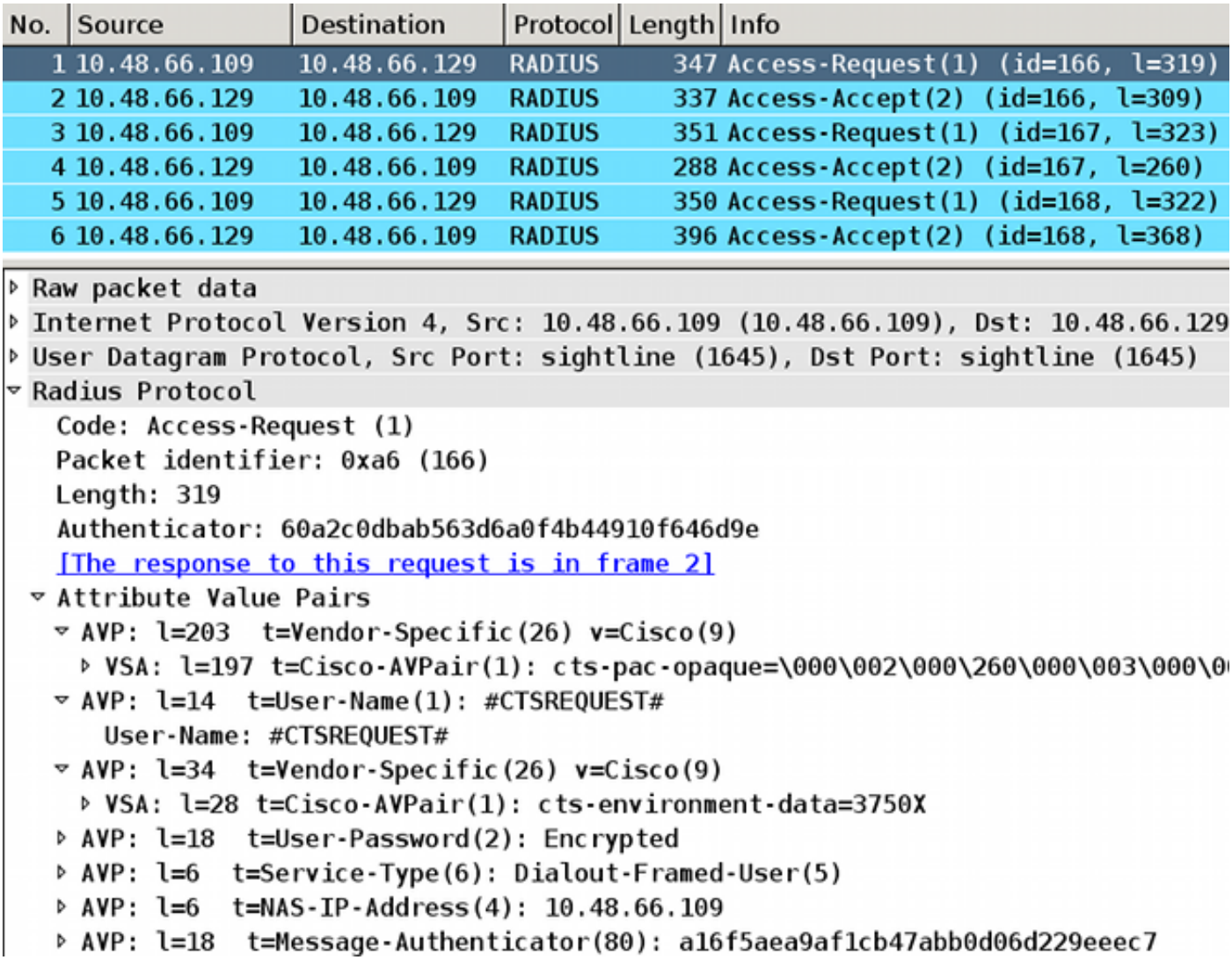
Bei der ersten Anforderung erhält der Switch den Namen der **CTSServerlist**. Für die zweite erhält er die Details für diese Liste, für die letzte alle SGTs mit Tags und Namen:

No.	Source	Destination	Protocol	Length	Info
1	10.48.66.109	10.48.66.129	RADIUS	347	Access-Request(1) (id=166, l=319)
2	10.48.66.129	10.48.66.109	RADIUS	337	Access-Accept(2) (id=166, l=309)
3	10.48.66.109	10.48.66.129	RADIUS	351	Access-Request(1) (id=167, l=323)
4	10.48.66.129	10.48.66.109	RADIUS	288	Access-Accept(2) (id=167, l=260)
5	10.48.66.109	10.48.66.129	RADIUS	350	Access-Request(1) (id=168, l=322)
6	10.48.66.129	10.48.66.109	RADIUS	396	Access-Accept(2) (id=168, l=368)

```
Authenticator: b1672c429de0593417de4315ee0bd40c
[This is a response to a request in frame 5]
[Time from request: 0.008000000 seconds]
▾ Attribute Value Pairs
  ▾ AVP: l=14  t=User-Name(1): #CTSREQUEST#
      User-Name: #CTSREQUEST#
  ▸ AVP: l=40  t=State(24): 526561757468536573736696f6e3a30613330343238313030...
  ▸ AVP: l=50  t=Class(25): 434143533a30613330343238313030303031343033353143...
  ▸ AVP: l=6  t=Termination-Action(29): RADIUS-Request(1)
  ▸ AVP: l=18  t=Message-Authenticator(80): ac8e7b6f0d59da776f0dbf1ffa04baf1
  ▾ AVP: l=39  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=33 t=Cisco-AVPair(1): cts:security-group-table=0001-5
  ▾ AVP: l=46  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=40 t=Cisco-AVPair(1): cts:security-group-info=0-0-00-Unknown
  ▾ AVP: l=45  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=39 t=Cisco-AVPair(1): cts:security-group-info=ffff-0-00-ANY
  ▾ AVP: l=45  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=39 t=Cisco-AVPair(1): cts:security-group-info=2-0-00-VLAN10
  ▾ AVP: l=45  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=39 t=Cisco-AVPair(1): cts:security-group-info=3-0-00-VLAN20
```

Hier sehen Sie das Standard-**SGT 0**, **ffff** sowie zwei benutzerdefinierte Tags: SGT-Tag 2 heißt **VLAN10** und SGT-Tag 3 heißt **VLAN20**.

Hinweis: Alle RADIUS-Anforderungen enthalten **cts-pac-opaque** als Ergebnis der PAC-Bereitstellung.



No.	Source	Destination	Protocol	Length	Info
1	10.48.66.109	10.48.66.129	RADIUS	347	Access-Request(1) (id=166, l=319)
2	10.48.66.129	10.48.66.109	RADIUS	337	Access-Accept(2) (id=166, l=309)
3	10.48.66.109	10.48.66.129	RADIUS	351	Access-Request(1) (id=167, l=323)
4	10.48.66.129	10.48.66.109	RADIUS	288	Access-Accept(2) (id=167, l=260)
5	10.48.66.109	10.48.66.129	RADIUS	350	Access-Request(1) (id=168, l=322)
6	10.48.66.129	10.48.66.109	RADIUS	396	Access-Accept(2) (id=168, l=368)

Auf dem 3750X sollten Debugging-Meldungen für alle drei RADIUS-Antworten sowie die entsprechenden Listen, Listendetails und die spezifische SGT-interne Liste angezeigt werden:

```
bsns-3750-5#debug cts environment-data all

*Mar  1 10:05:07.454: CTS env-data&colon; cleanup mcast SGT table
*Mar  1 10:05:18.057: CTS env-data&colon; Force environment-data refresh
*Mar  1 10:05:18.057: CTS env-data&colon; download transport-type =
CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.057:     cts_env_data START: during state env_data_complete,
got event 0(env_data_request)
*Mar  1 10:05:18.057: @@@ cts_env_data START: env_data_complete ->
env_data_waiting_rsp
*Mar  1 10:05:18.057: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.057: env_data_request_action: state = WAITING_RESPONSE
*Mar  1 10:05:18.057: cts_env_data_is_complete: FALSE, req(x0), rec(x0),
expect(x81), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.057: cts_aaa_req_setup: (CTS env-data)Private group appears DEAD,
attempt public group
*Mar  1 10:05:18.057: cts_aaa_req_setup: (CTS env-data)CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.057: cts_aaa_req_setup: (CTS env-data)AAA req(x7C3DF10)
*Mar  1 10:05:18.057: cts_aaa_attr_add: AAA req(0x7C3DF10)
*Mar  1 10:05:18.057:   username = #CTSREQUEST#
*Mar  1 10:05:18.057:   cts-environment-data = 3750X
*Mar  1 10:05:18.057: cts_aaa_req_send: AAA req(0x7C3DF10) successfully sent to AAA.
*Mar  1 10:05:18.083: cts_aaa_callback: (CTS env-data)AAA req(0x7C3DF10)
response success
```

```
*Mar  1 10:05:18.083:   AAA attr: Unknown type (447).
*Mar  1 10:05:18.083:   AAA attr: Unknown type (220).
*Mar  1 10:05:18.083:   AAA attr: Unknown type (275).
*Mar  1 10:05:18.083:   AAA attr: server-list = CTSServerList1-0001.
*Mar  1 10:05:18.083:   AAA attr: security-group-tag = 0000-00.
*Mar  1 10:05:18.083:   AAA attr: environment-data-expiry = 86400.
*Mar  1 10:05:18.083:   AAA attr: security-group-table = 0001-5.
*Mar  1 10:05:18.083: CTS env-data&colon; Receiving AAA attributes
 CTS_AAA_SLIST
    slist name(CTSServerList1) received in 1st Access-Accept
   slist name(CTSServerList1) created
 CTS_AAA_SECURITY_GROUP_TAG - SGT = unicast-unknown-00
 CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400.
 CTS_AAA_SGT_NAME_LIST
   table(0001) received in 1st Access-Accept
   old name(), gen()
   new name(0001), gen(50)
 CTS_AAA_DATA_END
*Mar  1 10:05:18.083:     cts_env_data WAITING_RESPONSE: during state
env_data_waiting_rsp, got event 1(env_data_received)
*Mar  1 10:05:18.083: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp ->
env_data_assessing
*Mar  1 10:05:18.083: env_data_assessing_enter: state = ASSESSING
*Mar  1 10:05:18.083: env_data_assessing_action: state = ASSESSING
*Mar  1 10:05:18.083: cts_env_data_is_complete: FALSE, req(x1089), rec(xC83),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.083:     cts_env_data ASSESSING: during state env_data_assessing,
got event 3(env_data_incomplete)
*Mar  1 10:05:18.083: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_waiting_rsp
*Mar  1 10:05:18.083: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.083: env_data_request_action: state = WAITING_RESPONSE
*Mar  1 10:05:18.083: cts_env_data_is_complete: FALSE, req(x1089), rec(xC83),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.083: cts_aaa_req_setup: (CTS env-data)Private group appears DEAD,
attempt public group
*Mar  1 10:05:18.083: cts_aaa_req_setup: (CTS env-data)CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.083: cts_aaa_req_setup: (CTS env-data)AAA req(x792FFD0)
*Mar  1 10:05:18.083: cts_aaa_attr_add: AAA req(0x792FFD0)
*Mar  1 10:05:18.091:   username = #CTSREQUEST#
*Mar  1 10:05:18.091:   cts-server-list = CTSServerList1
*Mar  1 10:05:18.091: cts_aaa_req_send: AAA req(0x792FFD0) successfully sent to AAA.
*Mar  1 10:05:18.099: cts_aaa_callback: (CTS env-data)AAA req(0x792FFD0)
response success
*Mar  1 10:05:18.099:   AAA attr: Unknown type (447).
*Mar  1 10:05:18.099:   AAA attr: Unknown type (220).
*Mar  1 10:05:18.099:   AAA attr: Unknown type (275).
*Mar  1 10:05:18.099:   AAA attr: server-list = CTSServerList1-0001.
*Mar  1 10:05:18.099:   AAA attr: server = c40a15a339286ceac28a50dbbac59784:
10.48.66.129:1812.
*Mar  1 10:05:18.099: CTS env-data&colon; Receiving AAA attributes
 CTS_AAA_SLIST
    2nd Access-Accept slist name(CTSServerList1), gen(0001)
 CTS_AAA_SERVERS
   server (c40a15a339286ceac28a50dbbac59784:10.48.66.129:1812) added
 CTS_AAA_DATA_END
*Mar  1 10:05:18.099:     cts_env_data WAITING_RESPONSE: during state
env_data_waiting_rsp, got event 1(env_data_received)
*Mar  1 10:05:18.099: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp ->
env_data_assessing
*Mar  1 10:05:18.099: env_data_assessing_enter: state = ASSESSING
*Mar  1 10:05:18.099: env_data_assessing_action: state = ASSESSING
*Mar  1 10:05:18.099: cts_env_data_is_complete: FALSE, req(x108D), rec(xC87),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
```

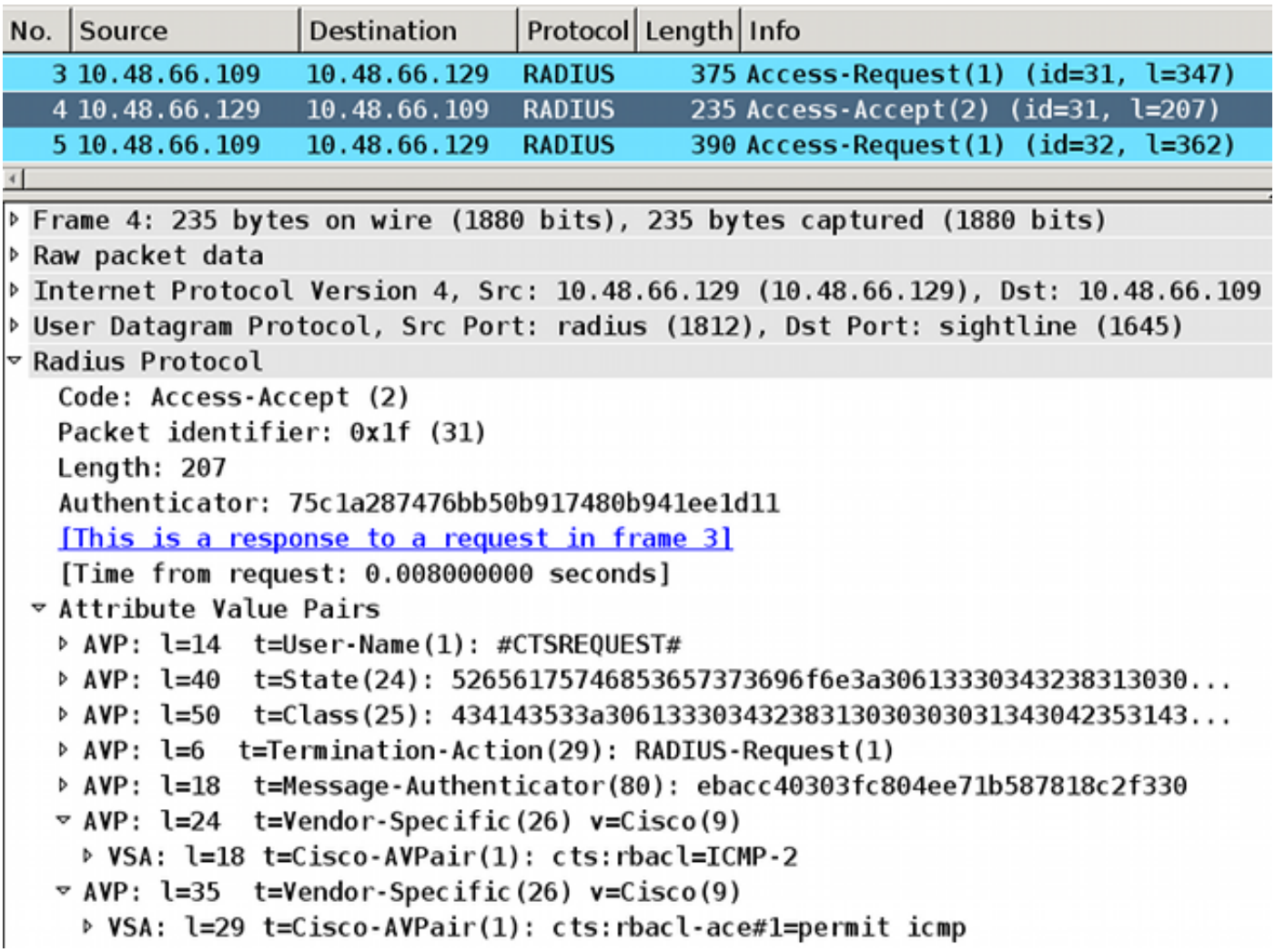
```
*Mar  1 10:05:18.099:     cts_env_data ASSESSING: during state env_data_assessing,
got event 3(env_data_incomplete)
*Mar  1 10:05:18.099: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_waiting_rsp
*Mar  1 10:05:18.099: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.099: env_data_request_action: state = WAITING_RESPONSE
*Mar  1 10:05:18.099: cts_env_data_is_complete: FALSE, req(x108D), rec(xC87),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.099: cts_aaa_req_setup: (CTS env-data)Using private server group
*Mar  1 10:05:18.099: cts_aaa_req_setup: (CTS env-data)CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.099: cts_aaa_req_setup: (CTS env-data)AAA req(x7A6C4AC)
*Mar  1 10:05:18.099: cts_aaa_attr_add: AAA req(0x7A6C4AC)
*Mar  1 10:05:18.099:   username = #CTSREQUEST#
*Mar  1 10:05:18.099:   cts-security-group-table = 0001
*Mar  1 10:05:18.099: cts_aaa_req_send: AAA req(0x7A6C4AC) successfully sent to AAA.
*Mar  1 10:05:18.108: cts_aaa_callback: (CTS env-data)AAA req(0x7A6C4AC)
response success
*Mar  1 10:05:18.108:   AAA attr: Unknown type (447).
*Mar  1 10:05:18.108:   AAA attr: Unknown type (220).
*Mar  1 10:05:18.108:   AAA attr: Unknown type (275).
*Mar  1 10:05:18.108:   AAA attr: security-group-table = 0001-5.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = 0-0-00-Unknown.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = ffff-0-00-ANY.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = 2-0-00-VLAN10.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = 3-0-00-VLAN20.
*Mar  1 10:05:18.108:  CTS env-data&colon; Receiving AAA attributes
 CTS_AAA_SGT_NAME_LIST
   table(0001) received in 2nd Access-Accept
   old name(0001), gen(50)
   new name(0001), gen(50)
 CTS_AAA_SGT_NAME_INBOUND - SGT = unicast-unknown-00
   flag (128) server name (Unknown) added
  name (0001), request (1), receive (1)
  Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
 CTS_AAA_SGT_NAME_INBOUND - SGT = unicast-default-00
   flag (128) server name (ANY) added
  name (0001), request (1), receive (1)
  Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
 CTS_AAA_SGT_NAME_INBOUND - SGT = 2-00
   flag (128) server name (VLAN10) added
  name (0001), request (1), receive (1)
  Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
 CTS_AAA_SGT_NAME_INBOUND - SGT = 3-00
   flag (128) server name (VLAN20) added
  name (0001), request (1), receive (1)
  Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
 CTS_AAA_DATA_END
*Mar  1 10:05:18.108:     cts_env_data WAITING_RESPONSE: during state
env_data_waiting_rsp, got event 1(env_data_received)
*Mar  1 10:05:18.108: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp ->
env_data_assessing
*Mar  1 10:05:18.108: env_data_assessing_enter: state = ASSESSING
*Mar  1 10:05:18.108: env_data_assessing_action: state = ASSESSING
*Mar  1 10:05:18.116: cts_env_data_is_complete: TRUE, req(x2085), rec(x2C87),
expect(x81), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.116:     cts_env_data ASSESSING: during state env_data_assessing,
got event 4(env_data_complete)
*Mar  1 10:05:18.116: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_complete
*Mar  1 10:05:18.116: env_data_complete_enter: state = COMPLETE
*Mar  1 10:05:18.116: env_data_install_action: state = COMPLETE
```

Richtlinienaktualisierung

Die Richtlinienaktualisierung wird nur auf dem Switch unterstützt. Sie ähnelt der Umgebungsaktualisierung. Dies sind lediglich RADIUS-Anforderungen und -Akzepte.

Der Switch fordert alle ACLs in der Standardliste an. Anschließend wird für jede nicht aktuelle (oder nicht vorhandene) ACL eine weitere Anforderung gesendet, um die Details abzurufen.

Wenn Sie ICMP-20 ACL anfordern, sehen Sie folgendes Beispiel:



Denken Sie daran, dass Sie **CTS-rollenbasierte Durchsetzung** konfigurieren müssen, um diese ACL durchzusetzen.

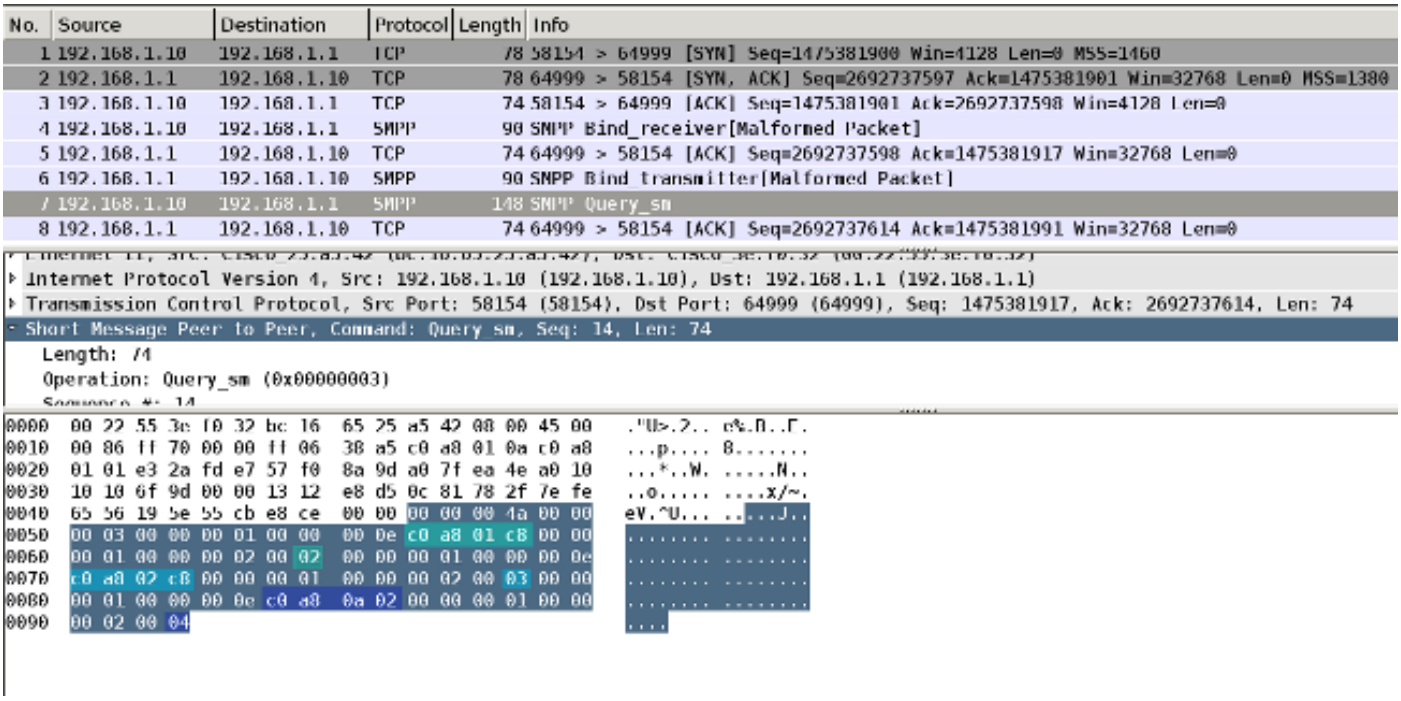
Debugs geben an, ob Änderungen (basierend auf der Generierung-ID) vorgenommen werden. In diesem Fall können Sie die alte Richtlinie bei Bedarf deinstallieren und eine neue installieren. Dazu gehört auch die ASIC-Programmierung (Hardware-Unterstützung).

```
bsns-3750-5#debug cts all

Mar 30 02:39:37.151:  CTS authz entry: peer(Unknown-2) Receiving AAA attributes
   rcv rbacl list: flags: req(81)rcv(0)wait(80)prev(0)install(880)
    - SGT = 2-01:VLAN10
    - SGT = 2-01:VLAN10
   current arg_cnt=8, expected_num_args=11
   3rd Access-Accept rbacl received name(ICMP), gen(20)
   received_policyp->sgt(2-01:VLAN10)
   existing sgt_policy(73FFDB4) sgt(2-01:VLAN10)
   RBACL name(ICMP-20)flag(40000000) already exists
```

```
  acl_listp(740266C) old_acl_infop(0),exist_rbacl_type(0)
 CTS_AAA_AUTHORIZATION_EXPIRY = 86400.
 CTS_AAA_DATA_END

Mar 30 02:39:37.176: cts_authz_entry_complete_action: Policy download complete -
peer(Unknown-2) SGT(2-01:VLAN10) status(RBACL-POLICY SUCCEEDED)
Mar 30 02:39:37.176: cts_authz_rbacl_uninstall_cb:
Mar 30 02:39:37.176: uninstall cb_ctx:
Mar 30 02:39:37.176:   session_hdl = F1000003
Mar 30 02:39:37.176:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.176:   ip_version  = IPV6
Mar 30 02:39:37.176:   src-or-dst  = BOTH
Mar 30 02:39:37.176:   wait_rbm_install_ip_ver(0)
Mar 30 02:39:37.176:   wait_rbm_uninstall_ip_ver(C0000000)
Mar 30 02:39:37.176: cts_authz_rbacl_uninstall_cb:
Mar 30 02:39:37.176: uninstall cb_ctx:
Mar 30 02:39:37.176:   session_hdl = F1000003
Mar 30 02:39:37.176:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.176:   ip_version  = IPV4
Mar 30 02:39:37.176:   src-or-dst  = BOTH
Mar 30 02:39:37.176:   wait_rbm_install_ip_ver(0)
Mar 30 02:39:37.176:   wait_rbm_uninstall_ip_ver(40000000)

Mar 30 02:39:37.210: install cb_ctx:
Mar 30 02:39:37.210:   session_hdl = F1000003
Mar 30 02:39:37.210:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.210:   ip_version  = IPV6
Mar 30 02:39:37.210:   src-or-dst  = SRC
Mar 30 02:39:37.210:   wait_rbm_install_ip_ver(C0000000)
Mar 30 02:39:37.210:   wait_rbm_uninstall_ip_ver(0)
Mar 30 02:39:37.210: cts_authz_rbacl_install_cb: Waiting for more RBM callback
for remaining IP version(40000000) RBACL policy(73FFDB4) for SGT(2-01:VLAN10)
flag(41400001)
Mar 30 02:39:37.210: cts_authz_rbacl_install_cb:
Mar 30 02:39:37.210: install cb_ctx:
Mar 30 02:39:37.210:   session_hdl = F1000003
Mar 30 02:39:37.210:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.210:   ip_version  = IPV4
Mar 30 02:39:37.210:   src-or-dst  = SRC
Mar 30 02:39:37.210:   wait_rbm_install_ip_ver(40000000)
Mar 30 02:39:37.210:   wait_rbm_uninstall_ip_ver(0)
Mar 30 02:39:37.210: cts_authz_rbacl_install_cb: Program RBACL policy(73FFDB4)
for SGT(2-01:VLAN10) flag(41400001) success
```

SXP-Exchange

Das SXP-Update wird durch den IP-Geräte-Tracking-Code ausgelöst, der die IP-Adresse des Geräts ermittelt. Anschließend wird das Short Message Peer-to-Peer (SMPP)-Protokoll verwendet, um die Updates zu senden. Die **TCP-Option 19** für die Authentifizierung entspricht Border Gateway Protocol (BGP). Die SMPP-Nutzlast ist nicht verschlüsselt. Wireshark hat keinen richtigen Decoder für die SMPP-Nutzlast, aber es ist einfach, darin Daten zu finden:



- Die erste, **c0 a8 01 c8**, ist **192.168.1.200** und hat das **Tag 2**.
- Die zweite, **c0 a8 02 c8**, ist **192.168.2.200** und hat das **Tag 3**.
- Die dritte, **c0 a8 0a 02,** ist **192.168.10.2** und hat das **Tag 4 (**dieses wurde verwendet, um das Telefon **SGT=4** zu testen)

Hier sind einige Fehlerbehebungen auf dem 3750X, nachdem die IP-Geräteverfolgung die IP-Adresse von MS Windows 7 findet:

```
bsns-3750-5#debug cts sxp message
bsns-3750-5#debug cts sxp internal
bsns-3750-5#debug cts sxp conn
bsns-3750-5#debug cts sxp mdb
bsns-3750-5#debug cts sxp error

Apr  7 00:39:06.874: CTS-SXP-CONN:sxp_process_message_event = CTS_SXPMSG_REQUEST
Apr  7 00:39:06.874: CTS-SXP-CONN:sxp_process_request  CTS_SXPMSG_REQ_CONN_NVGEN
Apr  7 00:39:06.874: CTS-SXP-CONN:cts_get_next_sxpconn_cli
Apr  7 00:39:06.874: CTS-SXP-CONN:cts_get_next_sxpconn_cli
Apr  7 00:39:06.874: CTS-SXP-INTNL:sxp_process_request boolean set
Apr  7 00:39:06.874: CTS-SXP-INTNL:sxp_send_request set boolean after
Apr  7 00:40:05.418: CTS-SXP-CONN:is_cts_sxp_rf_active
Apr  7 00:40:05.418: CTS-SXP-MDB:sxp_export_ipsgt_change 192.168.1.200/32 add 1
```

Nachfolgend finden Sie die entsprechenden Fehlerbehebungen auf der ASA:

```
bsns-asa5510-17# debug cts sxp all

%ASA-7-776018: CTS SXP: Binding 192.168.1.200->2:VLAN10 from peer 192.168.1.10
(instance 1) added in SXP database.
%ASA-7-776019: CTS SXP: Binding 192.168.1.200->2:VLAN10 added. Update binding
manager.
%ASA-6-776251: CTS SGT-MAP: Binding 192.168.1.200->2:VLAN10 from SXP added to
binding manager.
%ASA-7-776014: CTS SXP: SXP received binding forwarding request (add) binding
192.168.1.200->2:VLAN10.
```

Um mehr Debugging-Meldungen auf dem ASA-Gerät anzuzeigen, können Sie die Debugging-Ausführlichkeitsstufe aktivieren:

```
bsns-asa5510-17# debug cts condition level detail
debug cts condition level detail is enable
```

SGACL auf der ASA

Nachdem die ASA die von SXP empfangenen SGT-Zuordnungen korrekt installiert hat, sollte die ACL der Sicherheitsgruppen einwandfrei funktionieren. Wenn Probleme mit der Zuordnung auftreten, geben Sie Folgendes ein:

```
bsns-asa5510-17# debug cts sgt-map
```

Die ACL für die Sicherheitsgruppe funktioniert genauso wie für die IP-Adresse oder die Benutzeridentität. Die Protokolle enthüllen Probleme und den genauen Eintrag der Zugriffskontrollliste, die getroffen wurde.

Hier ist ein Ping von MS Windows XP zu MS Windows 7, der anzeigt, dass der Packet Tracer richtig funktioniert:

```
bsns-asa5510-17# packet-tracer input inside icmp 192.168.2.200 8 0 192.168.1.200
detailed
<output ommitted>

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group inside in interface inside
access-list inside extended permit icmp security-group tag 3 any security-group
name VLAN10 any
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0xaaf2ae80, priority=13, domain=permit, deny=false
       hits=185, user_data=0xaa2f5040, cs_id=0x0, use_real_addr, flags=0x0,
protocol=1
       src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0, tag=3:VLAN20
       dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, tag=2:VLAN10, dscp=0x0
       input_ifc=inside, output_ifc=any

<output ommitted>
```

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.