TrustSec Cloud met 802.1x MACsec op Catalyst 3750X Series Switch-configuratievoorbeeld

Inhoud

Inleiding

In dit artikel worden de stappen beschreven die nodig zijn om een Cisco TrustSec (CTS)-cloud met koppelingscodering tussen twee Catalyst 3750X Series switches (3750X) te configureren.

In dit artikel wordt het MACsec-coderingsproces (switch-to-switch Media Access Control Security) uitgelegd waarbij gebruik wordt gemaakt van Security Association Protocol (SAP). Dit proces gebruikt de IEEE 802.1x-modus in plaats van de handmatige modus.

Hier volgen een aantal stappen:

- Protected Access Credential (PAC) levering voor zaden en niet-zaadtoestellen
- NDAC-verificatie (Network Device Admission Control) en MACsec-onderhandeling met SAP voor sleutelbeheer
- Milieu en beleidsvernieuwing
- Poortverificatie voor clients
- Traffic tagging met de Security Group Tag (SGT)
- Beleidshandhaving met Security Group ACL (SGACL)

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van CTS-componenten
- Basiskennis van de CLI-configuratie van Catalyst switches
- Ervaring met configuratie van Identity Services Engine (ISE)

Gebruikte componenten

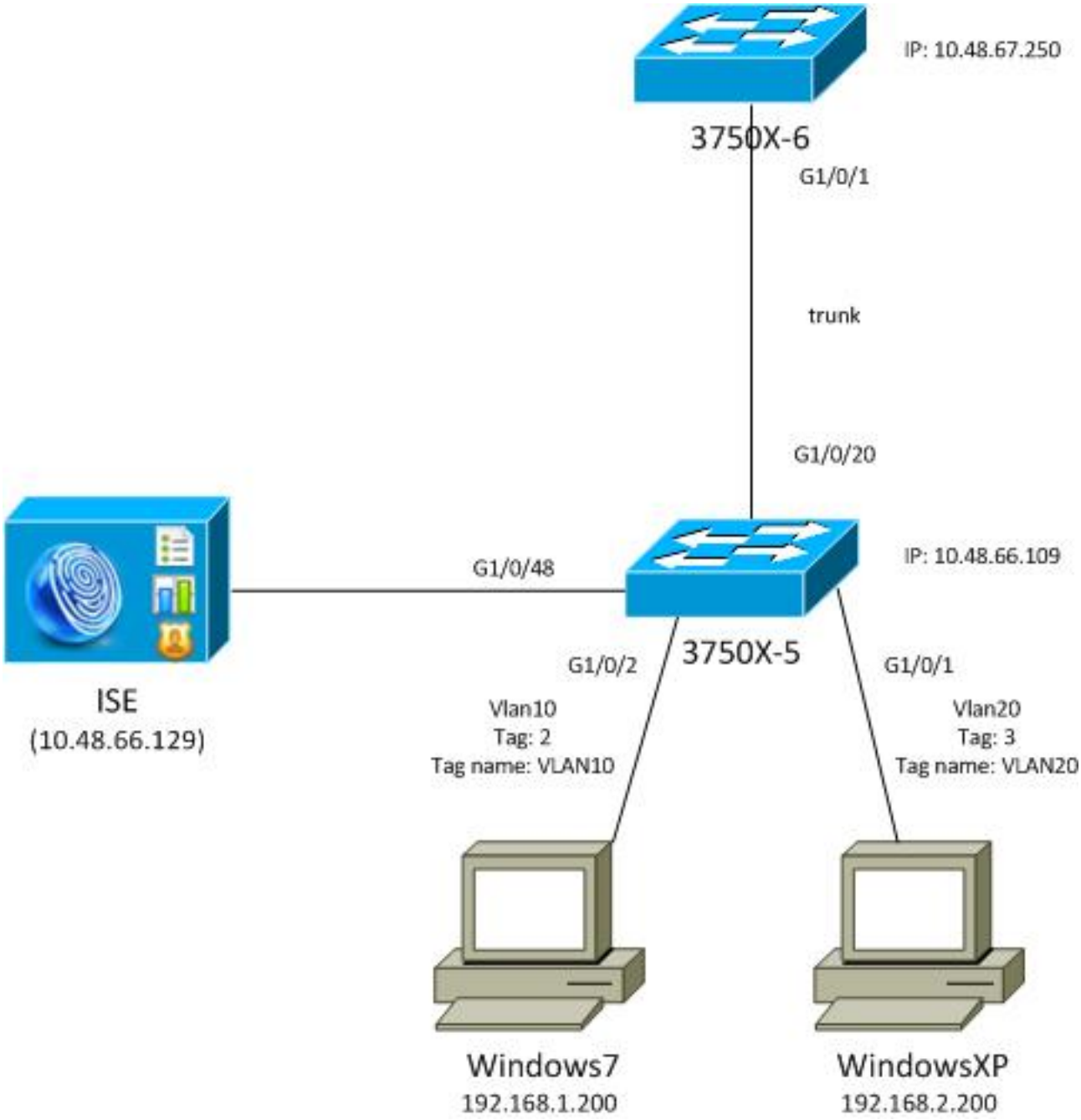
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft (MS) Windows 7 en MS Windows XP
- 3750X software, versies 15.0 en hoger
- ISE-software, versies 1.1.4 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Netwerkdiagram



In dit netwerktopologiediagram is de 3750X-5-switch het zaadapparaat dat het IP-adres van de ISE kent, en het downloadt automatisch de PAC die wordt gebruikt voor verdere verificatie in de CTS-cloud. Het zaadapparaat fungeert als een 802.1x-authenticator voor niet-zaadapparaten. De Cisco Catalyst 3750X-6 Series switch (3750X-6) is het apparaat dat niet van zaad is. Het fungeert als een 802.1x supplicant voor het zaadapparaat. Nadat het niet-zaadapparaat aan de ISE door het zaadapparaat wordt geverifieerd, wordt het toegelaten toegang tot de CTS wolk. Na een succesvolle verificatie wordt de 802.1x-poortstatus op de 3750X-5 switch gewijzigd in **geverifieerd** en wordt de MACsec-encryptie besproken. Het verkeer tussen de switches wordt vervolgens gelabeld met SGT en versleuteld.

Deze lijst vat de verwachte verkeersstroom samen:

- De seed 3750X-5 verbindt met de ISE en downloadt de PAC, die later wordt gebruikt voor een omgeving en beleidsvernieuwing.
- De non-seed 3750X-6 voert 802.1x-verificatie uit met de ondersteunende rol om de PAC te authenticeren/autoriseren en downloaden van de ISE.
- De 3750X-6 voert een tweede 802.1x Extensible Verification Protocol-Flexible Verification via

Secure Protocol (EAP-FAST)-sessie uit om te verifiëren met de beschermde tunnel op basis van de PAC.
- De 3750X-5 downloadt SGA-beleid voor zichzelf en namens 3750X-6.
- Een SAP-sessie vindt plaats tussen de 3750X-5 en 3750X-6, MACsec-algoritmen worden onderhandeld en het beleid wordt uitgewisseld.
- Het verkeer tussen de switches wordt gelabeld en versleuteld.

Zaad- en niet-zaadhoudende Switches configureren

Het zaadapparaat (3750X-5) wordt geconfigureerd om de ISE als RADIUS-server voor CTS te gebruiken:

```
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
```

Op rollen gebaseerde toegangscontrolelijsten (RBACL) en op security groepen gebaseerde toegangscontrolelijsten (SGACL) zijn ingeschakeld (worden later gebruikt):

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

Het apparaat zonder zaad (3750X-6) wordt alleen geconfigureerd voor verificatie, autorisatie en accounting (AAA) zonder dat hiervoor RADIUS- of CTS-autorisatie nodig is:

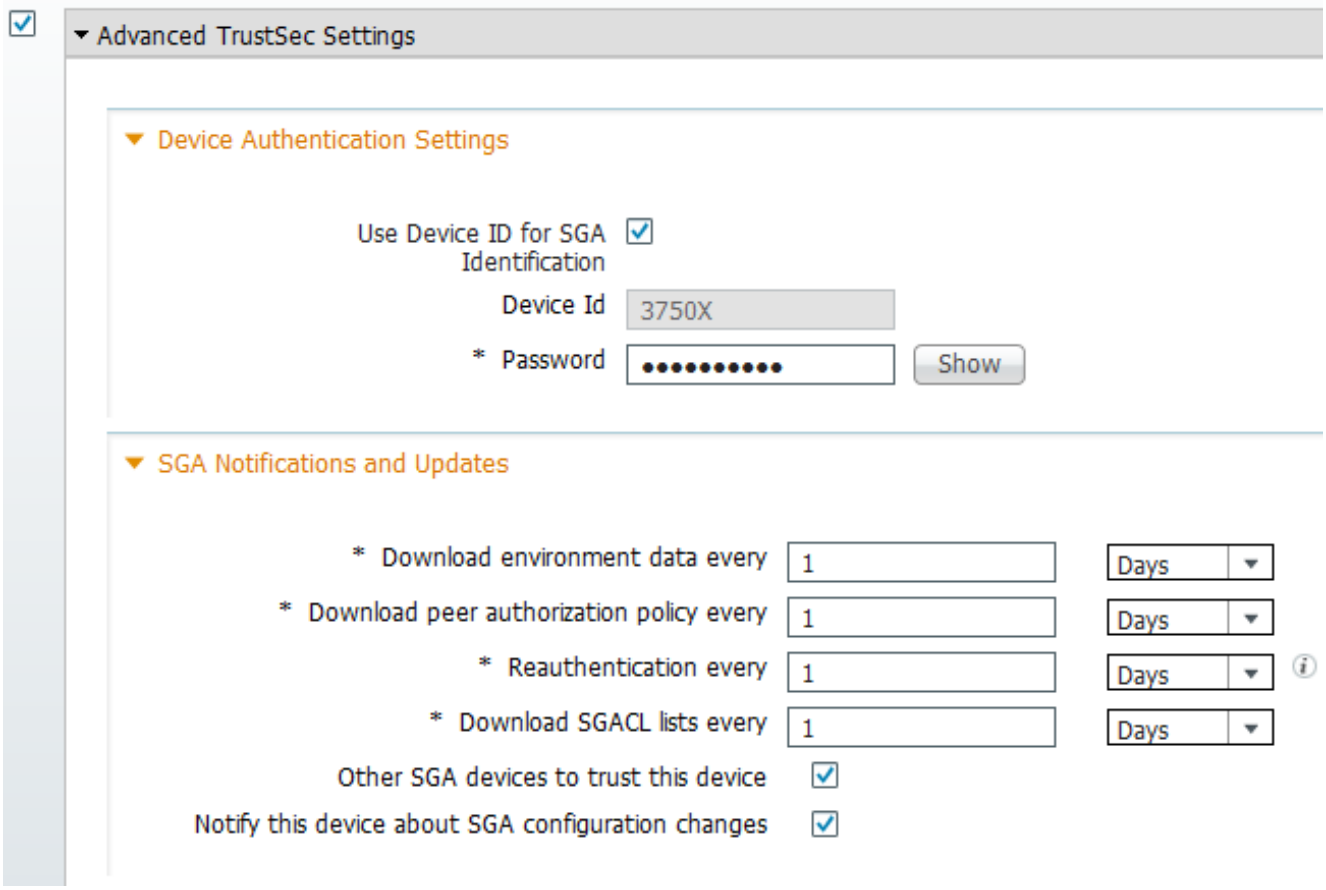
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

Alvorens u 802.1x op de interface toelaat, is het noodzakelijk om ISE te vormen.

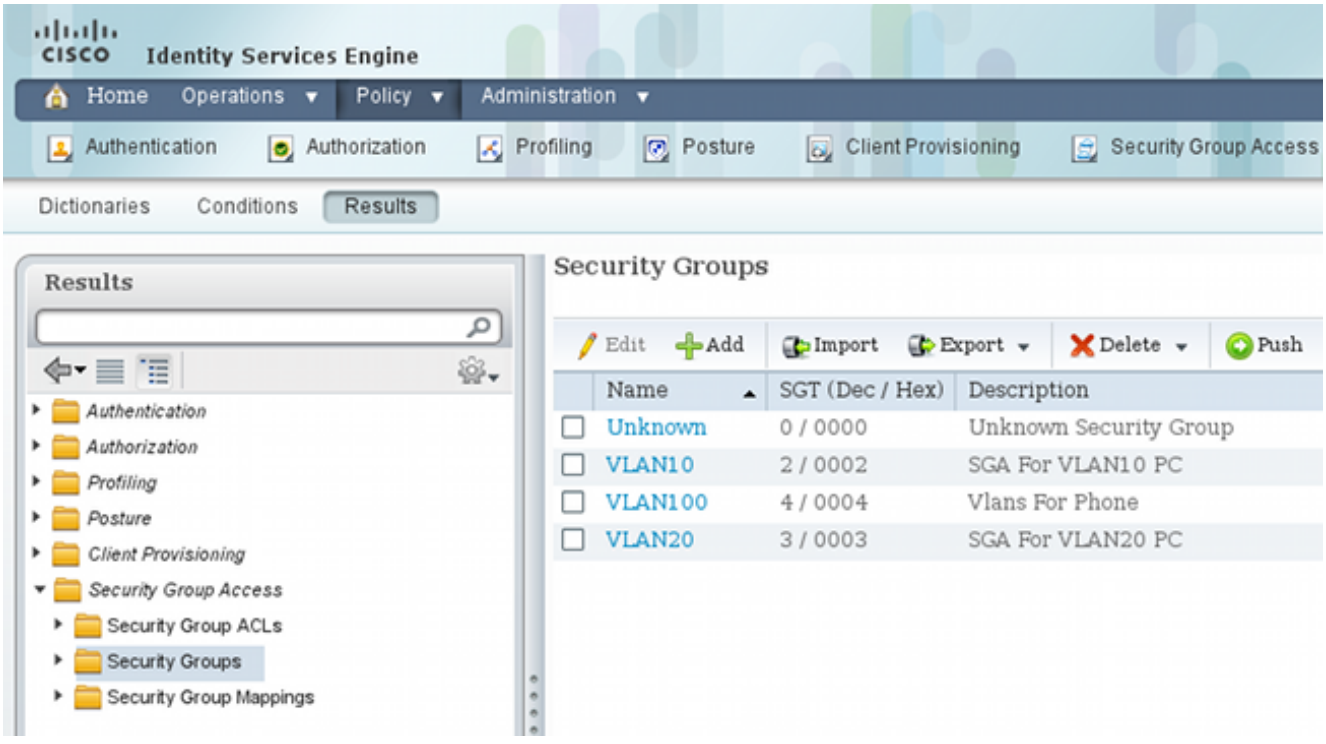
De ISE configureren

Voltooi de volgende stappen om de ISE te configureren:

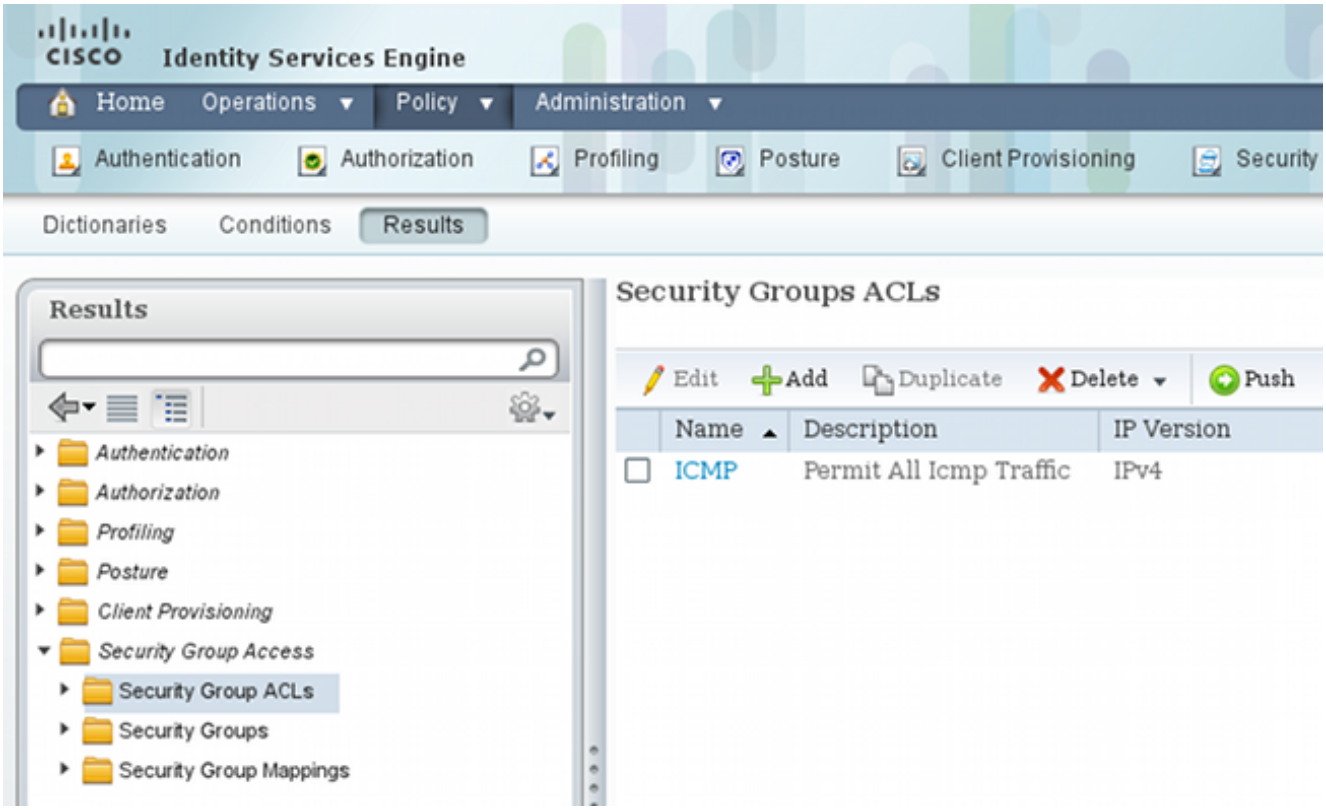
1. Ga naar **Beheer > Netwerkbronnen > Netwerkapparaten** en voeg beide switches toe als Network Access Devices (NAD's). Configureer onder **Advanced TrustSec Settings** een CTS-wachtwoord voor later gebruik op de switch CLI.



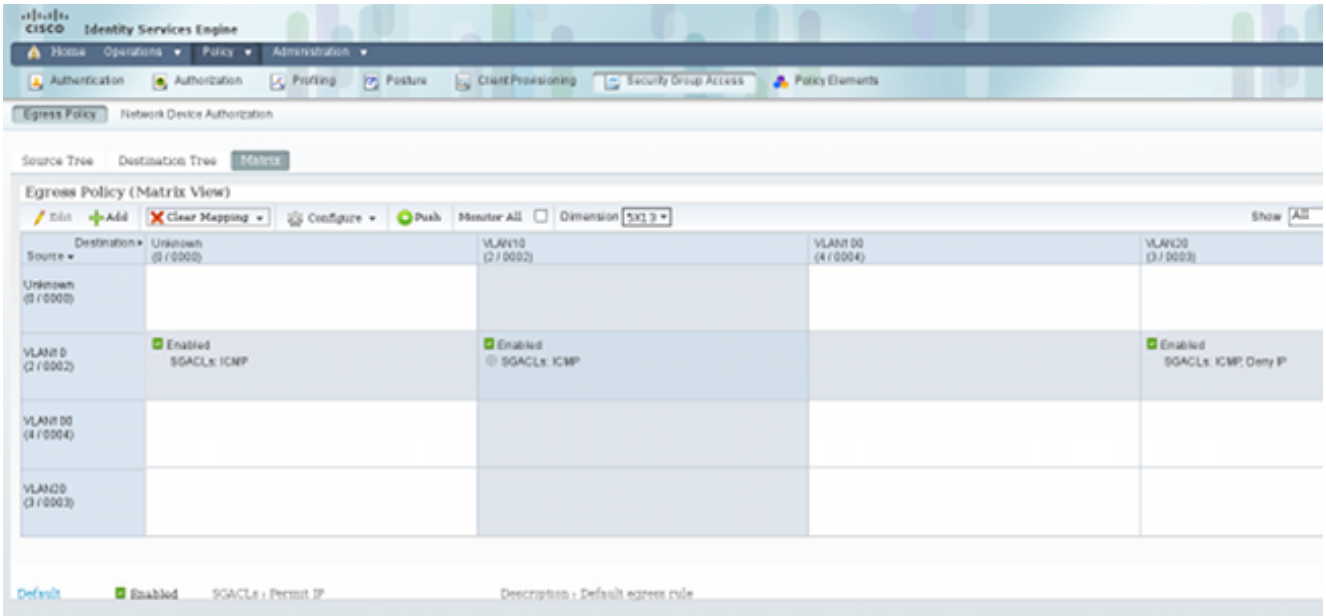
2. Navigeer naar **Policy > Policy Elements > Results > Security Group Access > Security Groups**, en voeg de juiste SGT's toe. Deze tags worden gedownload wanneer switches een verzoek indienen om een omgeving te vernieuwen.



3. Navigeer naar **Policy > Policy Elements > Results > Security Group Access > Security Group ACL's** en configureer een SGACL.



4. Navigeer naar **Policy > Security Group Access** en definieer een beleid met de matrix.



Opmerking: u moet het autorisatiebeleid voor de MS Windows-aanvrager configureren, zodat deze de juiste tag ontvangt. Raadpleeg [ASA en Catalyst 3750X Series Switch TrustSec Configuration Voorbeeld en de handleiding](#) voor [probleemoplossing](#) voor een gedetailleerde configuratie hiervan.

PAC-provisioning voor de 3750X-5

PAC is nodig voor verificatie in het CTS-domein (als fase 1 voor EAP-FAST) en wordt ook gebruikt om milieu- en beleidsgegevens van de ISE te verkrijgen. Zonder de juiste PAC is het niet mogelijk

die gegevens van de ISE te verkrijgen.

Nadat u de juiste referenties op de 3750X-5 verstrekt, downloadt het de PAC:

```
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
```

De PAC wordt gedownload via EAP-FAST met Microsoft's Challenge Handshake Verification Protocol (MSCHAPv2), waarbij de referenties in CLI worden geleverd en dezelfde referenties op de ISE worden geconfigureerd.

De PAC wordt gebruikt voor de omgeving en beleidsvernieuwing. Voor deze switches kunt u RADIUS-aanvragen gebruiken met **cisco av-pair cts-pac-opaque**, die is afgeleid van de PAC-toets en kan worden gedecodeerd op de ISE.

PAC-provisioning voor de 3750X-6 en NDAC-verificatie

Om een nieuw apparaat te kunnen verbinden met het CTS-domein, is het nodig om 802.1x in te schakelen op de bijbehorende poorten.

SAP-protocol wordt gebruikt voor sleutelbeheer en onderhandeling van een algoritme. De Galois Code van de Berichtverificatie (GMAC) wordt gebruikt voor authentificatie en Galois/Counter Mode (GCM) voor encryptie.

Op de switch:

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

Op de switch zonder zaad:

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

Dit wordt alleen ondersteund op trunkpoorten (switch-switch MACsec). Raadpleeg voor switch-

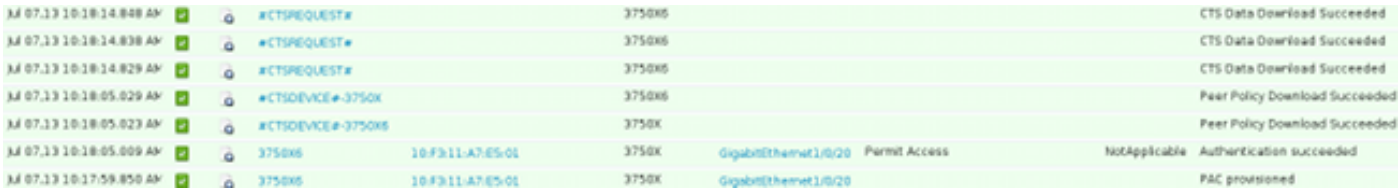
host MACsec, dat in plaats van SAP gebruik maakt van het MACsec Key Agreement (MKA)-protocol, MACsec-encryptie configureren.

Direct nadat u 802.1x op poorten inschakelt, werkt de niet-zaaddragende switch als een supplicant voor de zaaddragende switch, die de authenticator is.

Dit proces wordt NDAC genoemd, en het doel is om een nieuw apparaat te verbinden met het CTS domein. Verificatie is tweerichtings; het nieuwe apparaat heeft referenties die worden geverifieerd op de verificatieserver ISE. Na de levering van PAC, is het apparaat ook zeker dat het met het domein CTS verbindt.

> **Opmerking**: PAC wordt gebruikt om een TLS-tunnel (Transport Layer Security) voor EAP-FAST te bouwen. De 3750X-6 vertrouwt op de PAC-referenties die door de server worden verstrekt, vergelijkbaar met de manier waarop een client het certificaat vertrouwt dat door de server wordt verstrekt voor de TLS-tunnel voor de EAP-TLS-methode.

Er worden meerdere RADIUS-berichten uitgewisseld:



De eerste sessie van de 3750X (seed switch) wordt gebruikt voor PAC-levering. EAP-FAST wordt gebruikt zonder PAC (er wordt een anonieme tunnel voor MSCHAPv2-verificatie gebouwd).

```
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
```

De gebruikersnaam en het wachtwoord voor MSCHAPv2 die zijn geconfigureerd via de opdracht **Cts-referenties** worden gebruikt. Ook wordt een RADIUS access-reject aan het einde teruggestuurd, omdat nadat PAC al een voorziening heeft gemaakt, er geen verdere authenticatie nodig is.

De tweede vermelding in het logbestand verwijst naar 802.1x-verificatie. EAP-FAST wordt gebruikt voor de PAC die eerder was geleverd.

```
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
```

Deze keer is de tunnel niet anoniem, maar beschermd door PAC. Opnieuw worden dezelfde referenties voor de MSCHAPv2-sessie gebruikt. Vervolgens wordt het geverifieerd aan de hand van de authenticatie- en autorisatieregels op de ISE en wordt een RADIUS-toegangsgoedkeuring geretourneerd. Vervolgens past de authenticator switch de geretourneerde kenmerken toe en beweegt de 802.1x-sessie voor die poort naar een geautoriseerde status.

Hoe ziet het proces voor de eerste twee 802.1x sessies eruit vanuit de switch?

Hier zijn de belangrijkste debugs van het zaad. Het zaad detecteert dat de poort omhoog is en probeert te bepalen welke rol moet worden gebruikt voor 802.1x - de aanvrager of de authenticator:

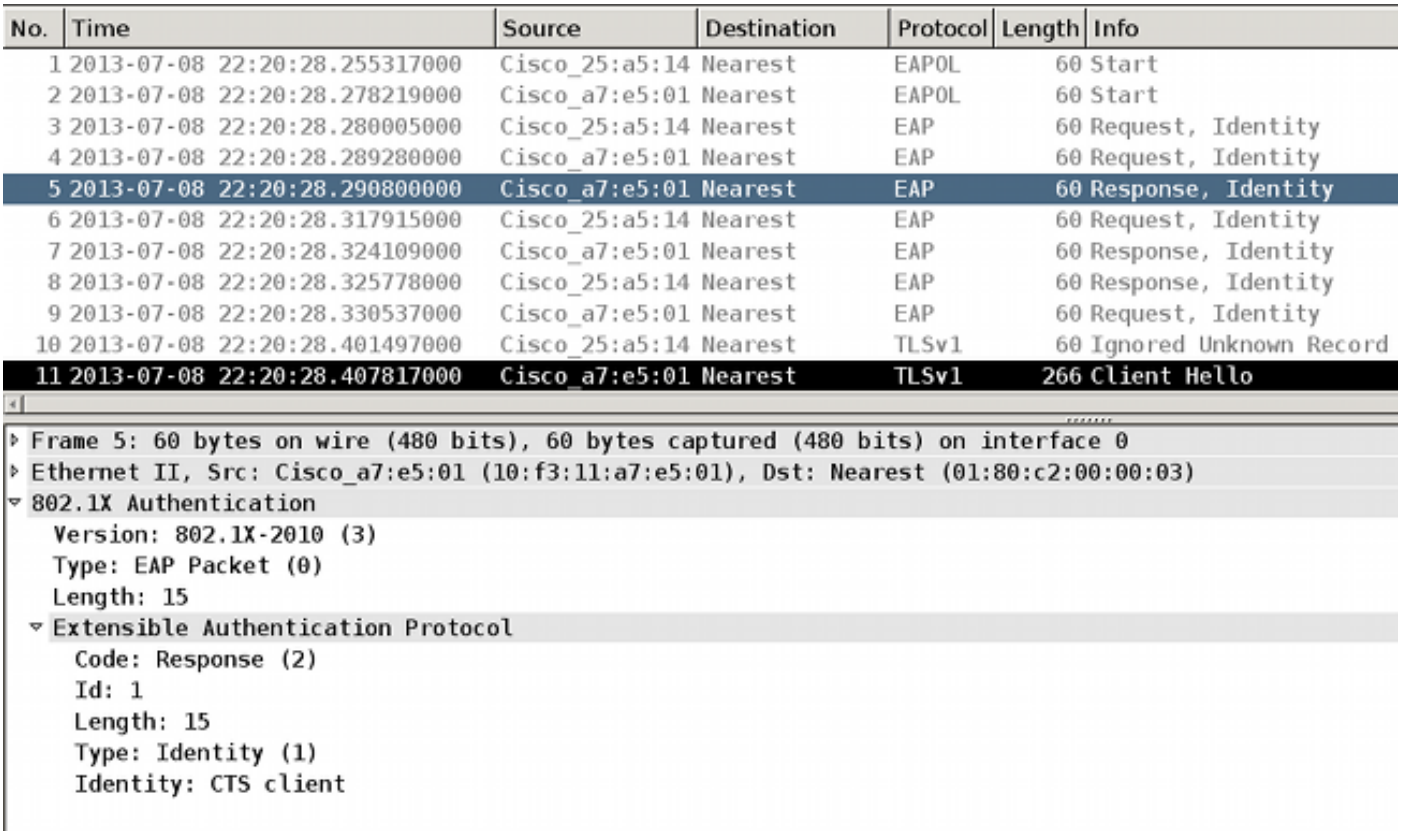
```
debug cts all
debug dot1x all
debug radius verbose
debug radius authentication

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
```

Tot slot wordt de authenticatorrol gebruikt, omdat de switch toegang tot de ISE heeft. Op de 3750X-6 wordt de ondersteunende rol gekozen.

Details over de rolselectie van 802.1x

> **Opmerking**: nadat de switch die het verzoek indient de PAC heeft verkregen en 802.1x-geauthenticeerd is, worden de omgevingsgegevens gedownload (zoals later beschreven) en leert het IP-adres van de AAA-server. In dit voorbeeld hebben beide switches een speciale (backbone) verbinding voor de ISE. Later kunnen de rollen verschillend zijn; de eerste switch die een reactie van de AAA server ontvangt wordt de authenticator, en de tweede wordt de aanvrager.

Dit is mogelijk omdat beide switches met de AAA-server die gemarkeerd is als ALIVE, een EAP-identiteit (Extensible Verification Protocol) aanvragen. Degene die als eerste de EAP Identity Response ontvangt, wordt de verificator en laat latere identiteitsaanvragen vallen.



Nadat de rol 802.1x is geselecteerd (in dit scenario is de 3750X-6 de aanvrager, omdat deze nog geen toegang heeft tot de AAA-server), hebben de volgende pakketten betrekking op de EAP-FAST-uitwisseling voor PAC-levering. De gebruikersnaam **CTS-client** wordt gebruikt voor de gebruikersnaam voor RADIUS-aanvragen en als de EAP-identiteit:

```
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]
```

Nadat de anonieme EAP-FAST-tunnel is gebouwd, vindt een MSCHAPv2-sessie plaats voor de gebruikersnaam **3750X6** (**cts referenties**). Het is niet mogelijk om dat op de switch te zien, omdat het een TLS-tunnel is (versleuteld), maar de ISE voor PAC-levering wordt bewezen door gedetailleerde logboeken. U kunt **CTS-client** zien voor de RADIUS-gebruikersnaam en als de EAP-identiteitsrespons. Voor de innerlijke methode (MSCHAP) wordt echter de **3750X6**-gebruikersnaam gebruikt:

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

De tweede EAP-FAST-verificatie vindt plaats. In dit geval wordt de eerder geleverde PAC gebruikt. Opnieuw wordt de **CTS-client** gebruikt als de RADIUS-gebruikersnaam en buitenidentiteit, maar **3750X6** wordt gebruikt voor de binnenidentiteit (MSCHAP). Verificatie mislukt:

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)

Ditmaal geeft de ISE echter verschillende kenmerken in het RADIUS-acceptpakket terug:

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 wijzigt de switch voor de verificator de poort in de geautoriseerde staat:

```
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
```

Hoe leert de authenticator switch dat de gebruikersnaam **3750X6** is? Voor de RADIUS-gebruikersnaam en de externe EAP-identiteit wordt **CTS-client** gebruikt en wordt de interne

identiteit versleuteld en niet zichtbaar voor de verificator. De gebruikersnaam wordt aangeleerd door de ISE. Het laatste RADIUS-pakket (Access-Accept) bevat **gebruikersnaam=3750X6**, terwijl alle andere pakketten **gebruikersnaam = CTS-client** bevatten. Daarom herkent de switch van de aanvrager de echte gebruikersnaam. Dit gedrag is RFC-conform. Uit afdeling 3.0 van RFC3579:

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

In het laatste pakket van de 802.1x-verificatiesessie retourneert de ISE een RADIUS-bericht accepteren als **cisco-av-paar** met de **EAP-Key-naam**:

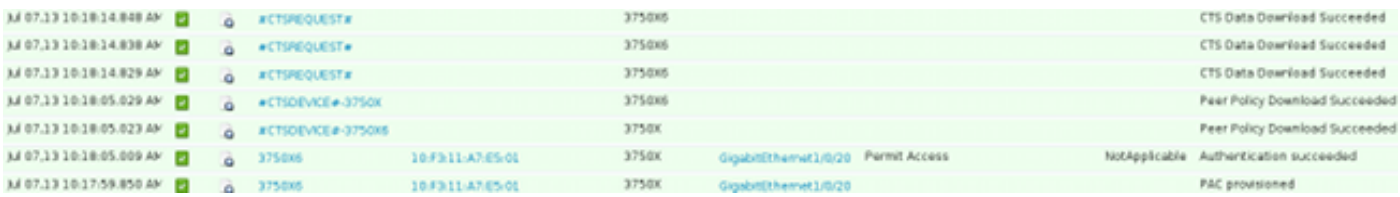
```
30 10.48.66.129   10.48.66.109   RADIUS     447 Access-Accept(2) (id=70, l=419)
  Packet Identifier: 0x46 (70)
  Length: 419
  Authenticator: afb2c1bfcb908ec5df3d544da26c7979
  [This is a response to a request in frame 29]
  [Time from request: 0.009000000 seconds]
▾ Attribute Value Pairs
  ▸ AVP: l=8  t=User-Name(1): 3750X6
  ▸ AVP: l=40  t=State(24): 52656175746853657373696f6e3a43304138303030313030...
  ▸ AVP: l=50  t=Class(25): 434143533a43304138303030313030303030353341333346...
  ▸ AVP: l=6  t=Session-Timeout(27): 86400
  ▸ AVP: l=6  t=Termination-Action(29): RADIUS-Request(1)
  ▸ AVP: l=6  t=EAP-Message(79) Last Segment[1]
  ▸ AVP: l=18  t=Message-Authenticator(80): 1b2b37b613fb42244bc3c6c2c038172e
  ▾ AVP: l=67  t=EAP-Key-Name(102): +T\3507\024\020\360<\033\220\361\327\255\034\v
      EAP-Key-Name: +T\3507\024\020\360<\033\220\361\327\255\034\v\314b\345\003Lk\
  ▾ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
    ▸ VSA: l=32 t=Cisco-AVPair(1): cts:security-group-tag=0000-01
```

Dit wordt gebruikt als sleutelmateriaal voor SAP-onderhandeling.

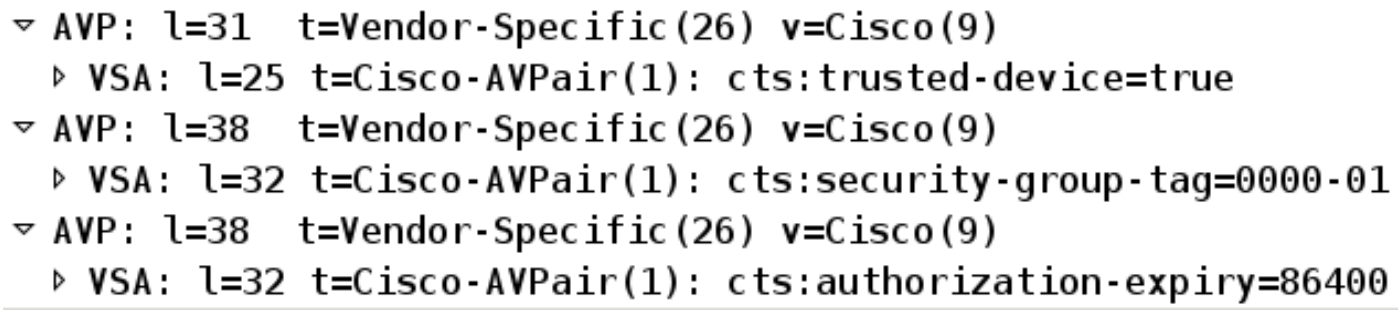
Ook het SGT wordt doorgegeven. Dit betekent dat de authenticator switch verkeer van de aanvrager met een **standaardwaarde = 0** etiketteert. U kunt een specifieke waarde op de ISE configureren om een andere waarde te retourneren. Dit is alleen van toepassing op verkeer zonder tags; het gelabelde verkeer wordt niet herschreven omdat de authenticator switch standaard het verkeer vertrouwt op de geverifieerde aanvrager (maar dit kan ook worden gewijzigd op de ISE).

SGA-beleidsdownload

Er zijn extra RADIUS-uitwisselingen (zonder EAP) anders dan de eerste twee 802.1x EAP-FAST-sessies (de eerste voor PAC-provisioning en de tweede voor verificatie). Hier zijn de ISE-logboeken weer:



Het derde log (**Peer Policy Download**) geeft een eenvoudige RADIUS-uitwisseling aan: RADIUS-verzoek en RADIUS-acceptatie voor de **3760X6-**gebruiker. Dit is nodig om beleid voor verkeer van de aanvrager te downloaden. De twee belangrijkste eigenschappen zijn:



Daarom vertrouwt de authenticator switch op verkeer dat SGT-getagd is door de aanvrager (**cts:usted-device=true**), en ook tags untagged verkeer met **tag=0**.

Het vierde log geeft dezelfde RADIUS-uitwisseling aan. Dit keer is het echter voor de **3750X5** gebruiker (authenticator). Dit komt doordat beide leeftijdsgenoten een beleid voor elkaar moeten hebben. Het is interessant om op te merken dat de aanvrager nog steeds het IP-adres van de AAA-server niet kent. Daarom downloadt de authenticator switch het beleid namens de aanvrager. Deze informatie gaat later door naar de aanvrager (samen met het ISE IP-adres) in SAP-onderhandeling.

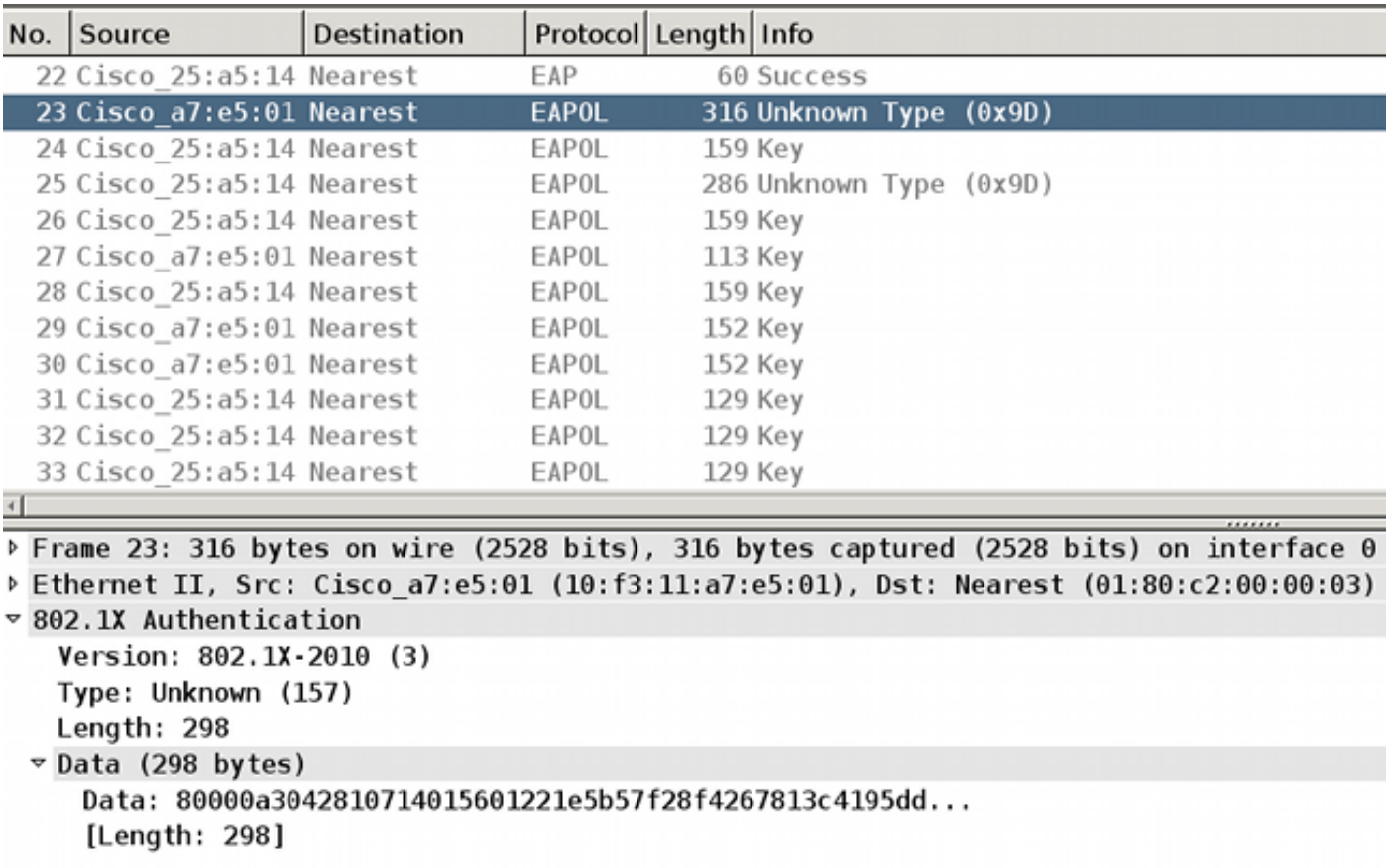
SAP-onderhandeling

Onmiddellijk nadat de 802.1x-verificatiesessie is voltooid, vindt SAP-onderhandeling plaats. Deze onderhandeling is vereist om:

- Bespreek coderingsniveaus (met de **sap mode-list gcm-encrypt** opdracht) en algoritme suites
- Sessietoetsen voor gegevensverkeer afleiden
- Het reparatieproces ondergaan
- Voer aanvullende beveiligingscontroles uit en controleer of de vorige stappen zijn beveiligd

SAP is een protocol dat is ontworpen door Cisco Systems op basis van een conceptversie van 802.11i/D6.0. Voor meer informatie kunt u toegang aanvragen tot het Cisco TrustSec Security Association Protocol - protocol dat Cisco Trusted Security ondersteunt voor de Cisco Nexus 7000-pagina.

SAP exchange is 802.1AE-conform. Er vindt een Extensible Verification Protocol over LAN (EAPOL)-toetsuitwisseling plaats tussen de aanvrager en de verificator om te onderhandelen over een cijferreeks, beveiligingsparameters uit te wisselen en sleutels te beheren. Helaas heeft Wireshark geen decoder voor alle vereiste 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

De succesvolle uitvoering van deze taken resulteert in de oprichting van een veiligheidsvereniging (SA).

Op de switch van de aanvrager:

```
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
```

Op de verificator:

```
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 gebruiken de poorten de modus **gcm-encrypt**, wat betekent dat verkeer zowel wordt geverifieerd en versleuteld als correct SGT-getagd. Geen van beide apparaten maakt gebruik van een specifiek beleid voor de autorisatie van netwerkapparaten op de ISE, wat betekent dat al het verkeer dat vanaf het apparaat wordt geïnitieerd, de standaardtag **0** gebruikt. Ook vertrouwen beide switches op SGT's die van de peer worden ontvangen (vanwege RADIUS-kenmerken uit de downloadfase van het peer-beleid).

Milieu en beleidsvernieuwing

Nadat beide apparaten zijn aangesloten op de CTS-cloud, wordt een omgeving- en beleidsvernieuwing gestart. De omgeving verfrissen is nodig om de SGT's en namen te verkrijgen, en een beleid verfrissen is nodig om de SGACL te downloaden die op de ISE is gedefinieerd.

In dit stadium kent de aanvrager het IP-adres van de AAA-server al, zodat hij dit voor zichzelf kan doen.

Raadpleeg ASA en Catalyst 3750X Series Switch TrustSec Configuration Voorbeeld en de handleiding voor probleemoplossing voor meer informatie over de omgeving en beleidsvernieuwing.

De switch van de aanvrager herinnert zich het IP-adres van de RADIUS-server, zelfs wanneer er geen RADIUS-server is geconfigureerd en wanneer de CTS-koppeling naar beneden gaat (naar de switch van de verificator). Je kunt de switch echter dwingen om het te vergeten:

```
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
```

Voer deze opdrachten in om de omgeving en het beleid op de switch van de aanvrager te controleren:

```
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
```

Waarom wordt er geen beleid weergegeven? Geen beleid weergegeven, omdat u **cts-handhaving** moet inschakelen om ze toe te passen:

```
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
```

Waarom heeft de aanvrager slechts één beleid om **Onbekend** te **groeperen** terwijl de authenticator meer heeft?

```
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
```

Poortverificatie voor clients

De MS Windows-client is aangesloten op en geverifieerd naar de **g1/0/1-**poort van de 3750-5 switch:

```
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, de switch 3750-5 weet dat verkeer van die host moet worden getagd met **SGT=3** wanneer

verzonden naar de CTS cloud.

Traffic tagging met de SGT

Hoe controleert u het verkeer?

Dit is moeilijk omdat:

- Ingesloten pakketvastlegging wordt alleen ondersteund voor IP-verkeer (en dit is een aangepast Ethernet-frame met SGT's en MACsec-payload).
- Switched Port Analyzer (SPAN) poort met het **replicatie** sleutelwoord - dit kan werken, maar het probleem is dat elke PC met Wireshark verbonden met de doelpoort van een controlesessie de frames laat vallen vanwege het gebrek aan ondersteuning van 802.1ae, wat kan gebeuren op het hardware niveau.
- De haven van SPAN zonder het **replicatiesleutelwoord** verwijdert de **cts** kopbal alvorens het op een bestemmingshaven zet.

Beleidshandhaving met SGACL

Beleidshandhaving in de CTS-cloud gebeurt altijd in de bestemmingshaven. Dit komt doordat alleen het laatste toestel het bestemmings-SGT kent van het eindpuntapparaat dat rechtstreeks met die switch is verbonden. Het pakket draagt alleen de bron SGT. Voor het nemen van een beslissing is zowel de SGT van herkomst als de SGT van bestemming vereist.

Dit is de reden waarom apparaten niet hoeft te downloaden van alle beleid van de ISE. In plaats daarvan hebben ze alleen het deel van het beleid nodig dat gerelateerd is aan de SGT waarvoor het apparaat rechtstreeks verbonden apparaten heeft.

Hier is de 3750-6, die de switch van de verzoeker is:

```
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
```

Er zijn hier twee beleidsterreinen. De eerste is de standaardinstelling voor verkeer zonder tags (van/naar). De tweede is van **SGT=2** aan untagged SGT, die **0** is. Dit beleid bestaat omdat het apparaat zelf het SGA-beleid van de ISE gebruikt en tot **SGT=0** behoort. Ook is **SGT=0** een standaard tag. Daarom moet u al het beleid downloaden dat de regels heeft voor verkeer **naar/van SGT=0**. Als je naar de matrix kijkt, zie je maar één dergelijk beleid: **van 2 tot 0**.

Hier is de 3750-5, de authenticator switch:

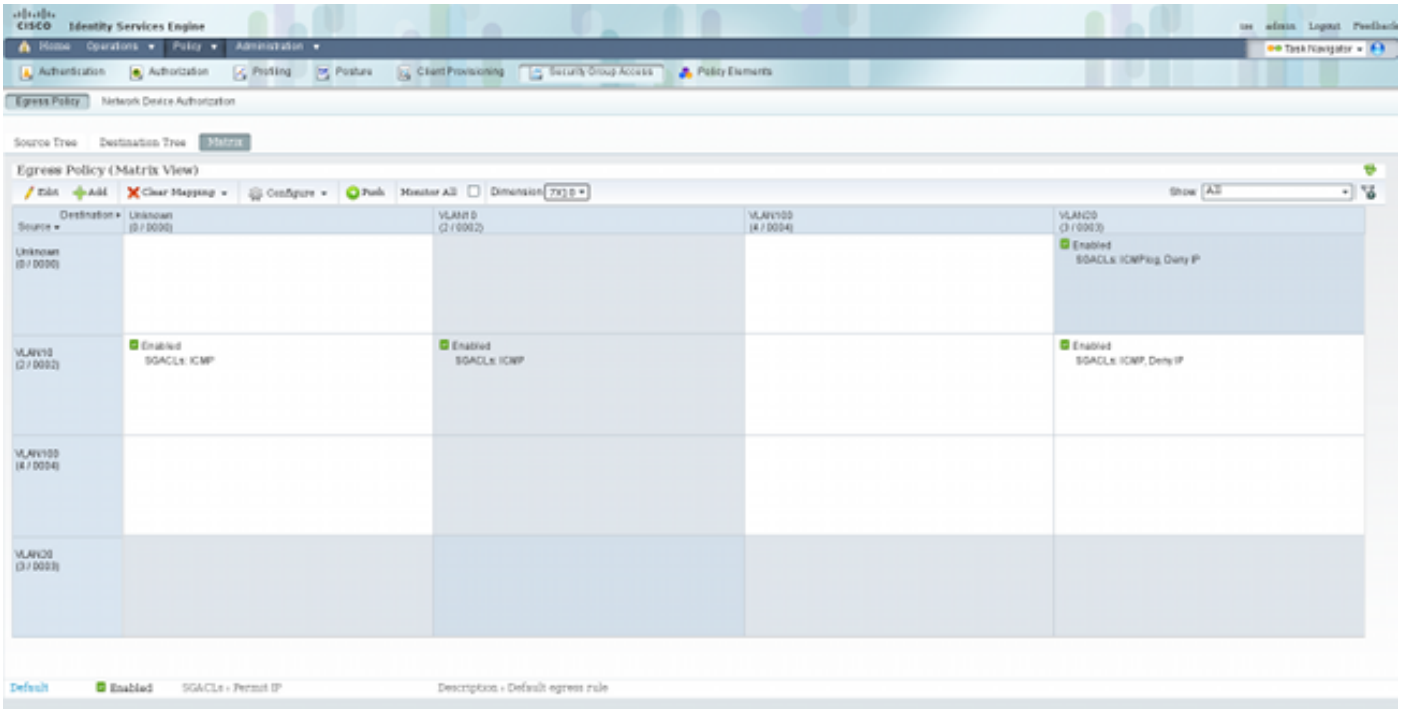
```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
```

```
        Deny IP-00
```

Er is hier nog een beleid: **van 2 tot 3**. Dit komt doordat de 802.1x-client (MS Windows) is verbonden met **g1/0/1** en is gelabeld met **SGT=3**. Daarom moet u alle beleid downloaden **naar SGT=3**.

Probeer te pingen van 3750X-6 (**SGT=0**) naar MS Windows XP (**SGT=3**). De 3750X-5 is het afdwingingsapparaat.

Hiervoor moet u een beleid op de ISE configureren voor verkeer van **SGT=0 naar SGT=3**. In dit voorbeeld is een ICMP-logbestand (SGACL Internet Control Message Protocol) gemaakt met alleen de regel, **laat u een ICMP-logbestand toe** en gebruikt u dit in de matrix voor verkeer van **SGT=0 naar SGT=3**:



Hier is een vernieuwing van het beleid over de afdwingende switch, en een verificatie van het nieuwe beleid:

```
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
```

Om te verifiëren dat de toegangscontrolelijst (ACL) van de ISE wordt gedownload, voert u deze opdracht in:

```
bsns-3750-5#show ip access-lists ICMPlog-10
```

```
Role-based IP access list ICMPlog-10 (downloaded)
   10 permit icmp log
```

Om te verifiëren dat ACL wordt toegepast (hardwaresupport), voert u deze opdracht in:

```
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 zijn de tellers vóór 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
```

Hier is een ping van **SGT=0** (3750-6 switch) naar MS Windows XP (**SGT=3**) en de tellers:

```
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 zijn de ACL-tellers:

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

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Cisco TrustSec-configuratiehandleiding voor 3750
- Cisco TrustSec-configuratiehandleiding voor ASA 9.1
- Cisco TrustSec-implementatie en routekaart
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

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