Catalyst 3750X Series 스위치의 802.1x MACsec을 사용하는 TrustSec 클라우드 구성 예

목차

소개

이 문서에서는 두 Catalyst 3750X Series 스위치(3750X) 간에 링크 암호화를 사용하여 Cisco TrustSec(CTS) 클라우드를 구성하는 데 필요한 단계를 설명합니다.

이 문서에서는 SAP(Security Association Protocol)를 사용하는 스위치 간 MACsec(Media Access Control Security) 암호화 프로세스에 대해 설명합니다. 이 프로세스에서는 수동 모드가 아닌 IEEE 802.1x 모드를 사용합니다.

다음은 관련 단계 목록입니다.

- 시드 및 비 시드 디바이스에 대한 PAC(Protected Access Credential) 프로비저닝
- 키 관리를 위한 SAP와의 NDAC(Network Device Admission Control) 인증 및 MACsec 협상
- 환경 및 정책 업데이트
- 클라이언트에 대한 포트 인증
- SGT(Security Group Tag)를 사용한 트래픽 태깅
- SGACL(Security Group ACL)을 통한 정책 시행

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CTS 구성 요소에 대한 기본 지식
- Catalyst 스위치의 CLI 구성에 대한 기본 지식
- ISE(Identity Services Engine) 컨피그레이션 경험

사용되는 구성 요소

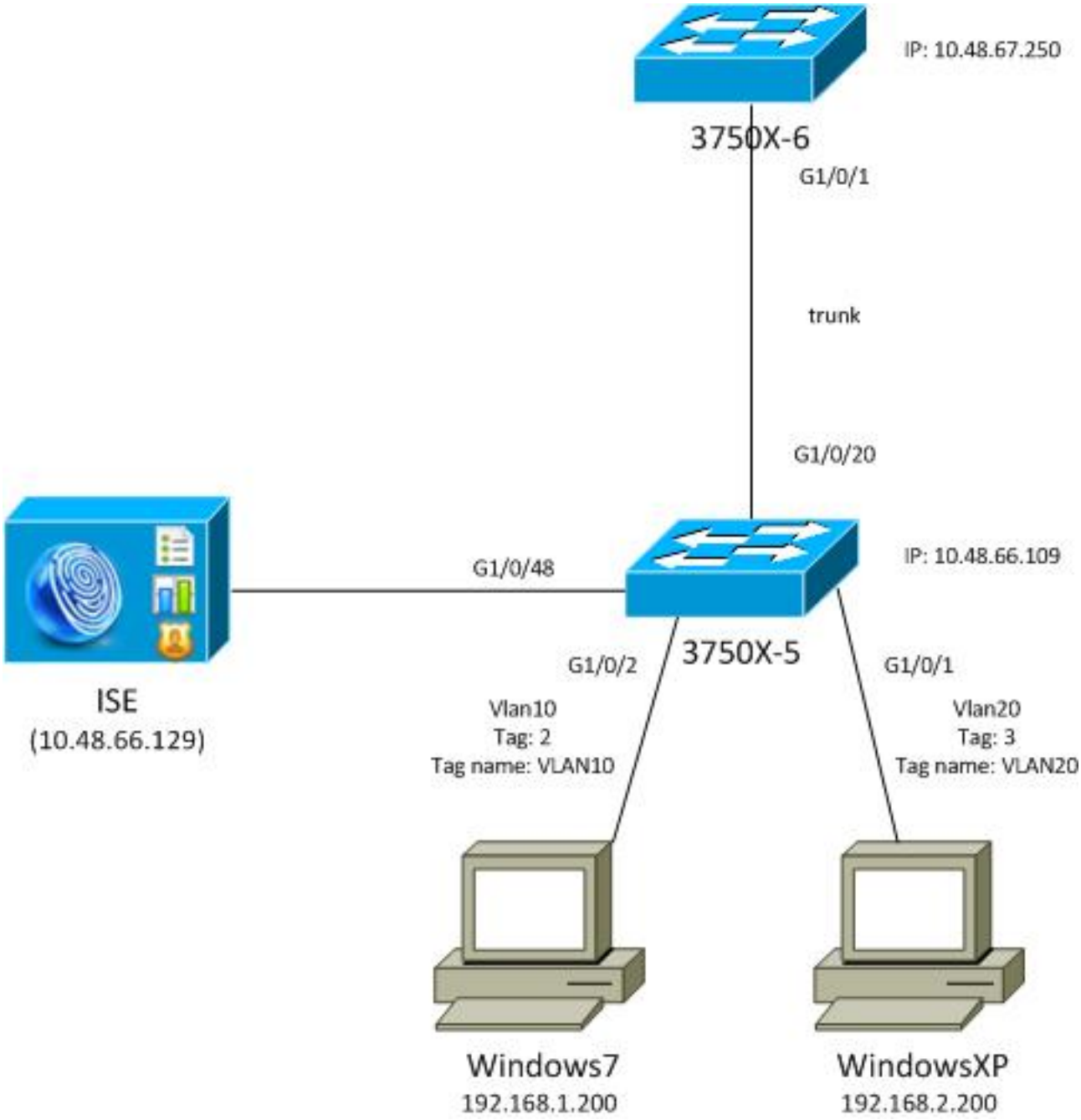
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft(MS) Windows 7 및 MS Windows XP
- 3750X 소프트웨어, 버전 15.0 이상
- ISE 소프트웨어, 버전 1.1.4 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 다이어그램



이 네트워크 토폴로지 다이어그램에서 3750X-5 스위치는 ISE의 IP 주소를 알고 있는 시드 디바이스이며, CTS 클라우드의 후속 인증에 사용되는 PAC를 자동으로 다운로드합니다. 시드 디바이스는 비시드 디바이스에 대한 802.1x 인증자 역할을 합니다. Cisco Catalyst 3750X-6 Series 스위치(3750X-6)는 비 시드 디바이스입니다. 시드 디바이스에 대한 802.1x 서플리컨트 역할을 합니다. 비시드 디바이스가 시드 디바이스를 통해 ISE에 인증하면 CTS 클라우드에 대한 액세스가 허용됩니다. 인증에 성공하면 3750X-5 스위치의 802.1x 포트 상태가 **authenticated**로 변경되고 MACsec 암호화가 협상됩니다. 스위치 간 트래픽은 SGT로 태그가 지정되고 암호화됩니다.

이 목록에는 예상 트래픽 흐름이 요약되어 있습니다.

- 시드 3750X-5는 ISE에 연결하고 PAC를 다운로드하며, 이는 나중에 환경 및 정책 새로 고침에 사용됩니다.
- 비시드 3750X-6은 ISE에서 PAC를 인증/권한 부여하고 다운로드하기 위해 신청자 역할로 802.1x 인증을 수행합니다.
- 3750X-6은 PAC를 기반으로 보호 터널로 인증하기 위해 두 번째 802.1x EAP-FAST(Extensible Authentication Protocol-Flexible Authentication via Secure Protocol) 세션을 수행합니다.
- 3750X-5는 자신을 위해 그리고 3750X-6을 대신하여 SGA 정책을 다운로드합니다.

- 3750X-5와 3750X-6 간에 SAP 세션이 발생하고 MACsec 암호가 협상되며 정책이 교환됩니다.
- 스위치 간 트래픽은 태그가 지정되고 암호화됩니다.

Seed 및 Non-Seed 스위치 구성

시드 디바이스(3750X-5)는 ISE를 CTS용 RADIUS 서버로 사용하도록 구성됩니다.

```
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
```

RBACL(Role-Based Access Control List) 및 SGACL(Security Group Based Access Control List) 시행이 활성화됩니다(나중에 사용됨).

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

비시드 디바이스(3750X-6)는 RADIUS 또는 CTS 권한 부여 없이 AAA(Authentication, Authorization, and Accounting)에만 구성됩니다.

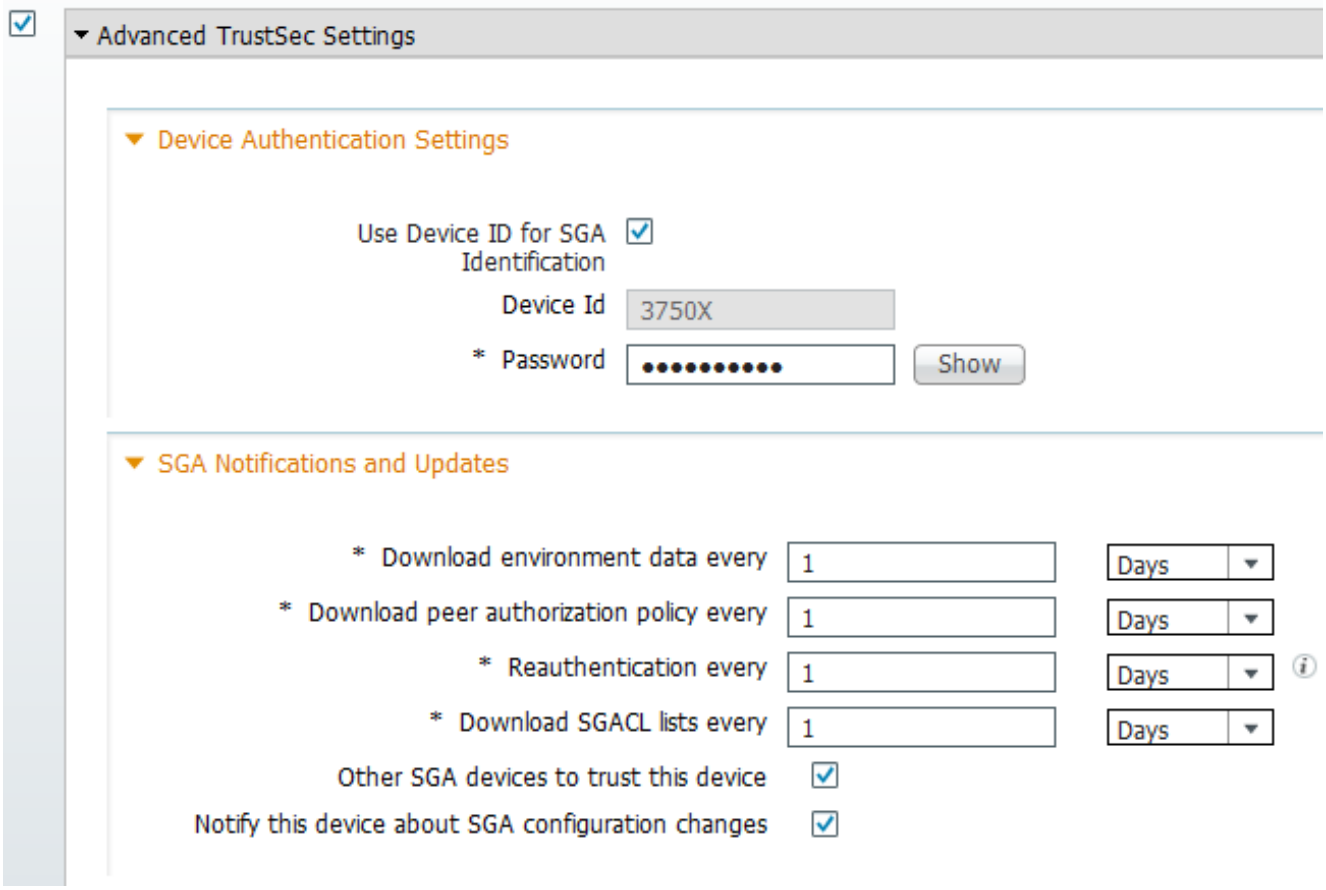
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

인터페이스에서 802.1x를 활성화하기 전에 ISE를 구성해야 합니다.

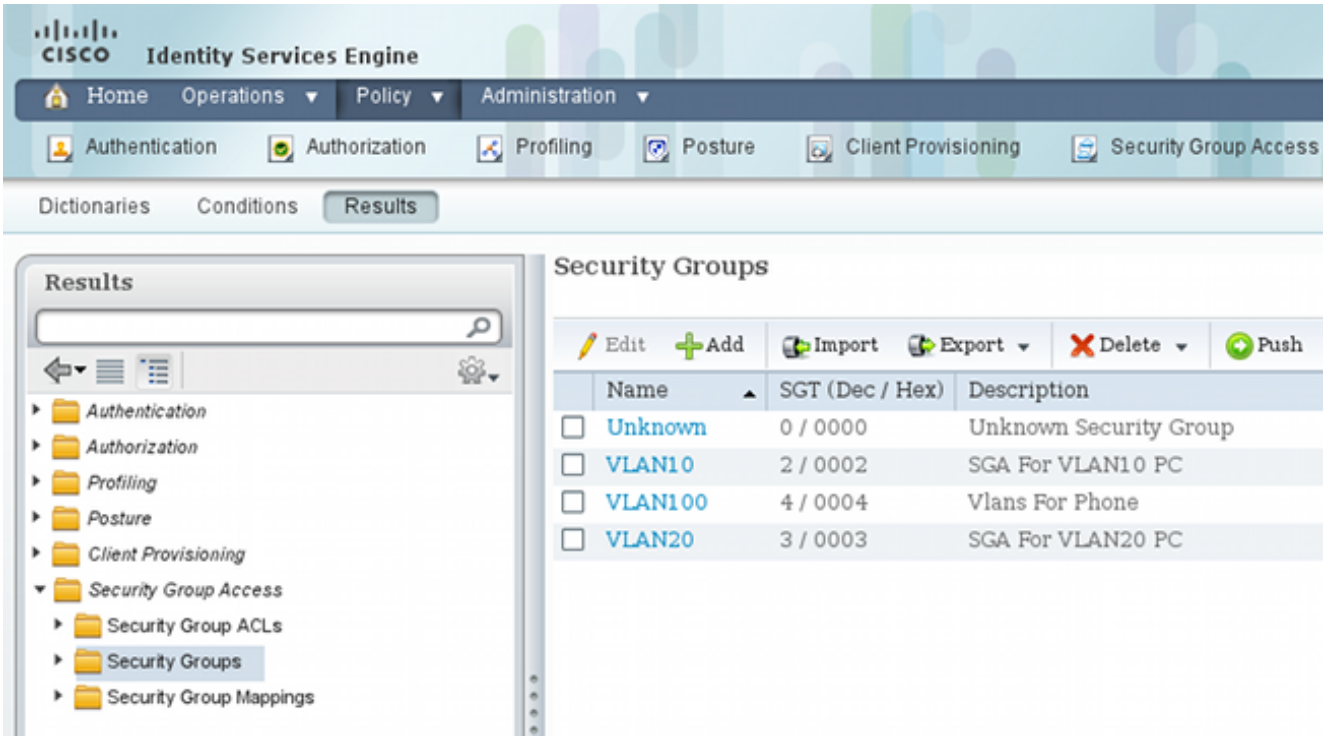
ISE 구성

ISE를 구성하려면 다음 단계를 완료하십시오.

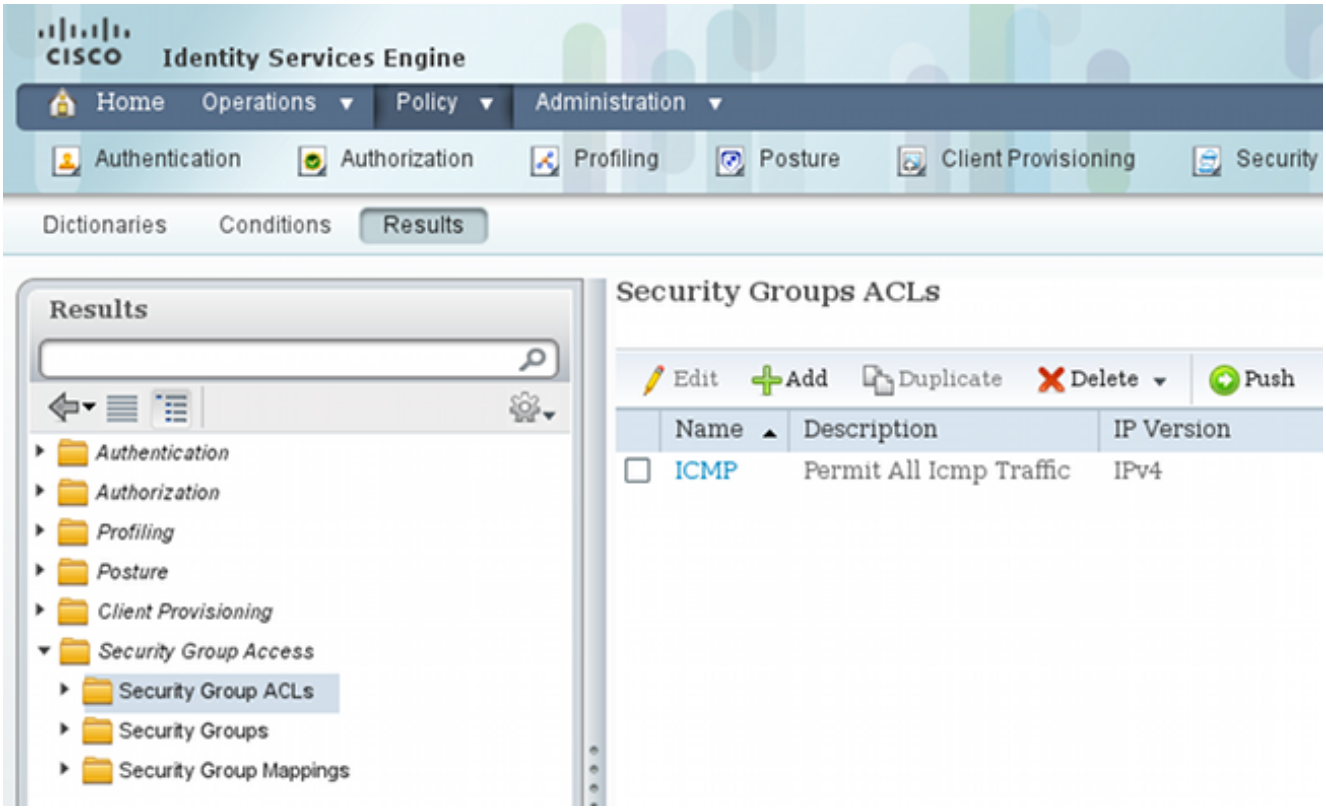
1. **Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로** 이동하고 두 스위치를 모두 NADs(Network Access Devices)로 추가합니다. Advanced **TrustSec Settings(고급** TrustSec 설정) 아래에서 스위치 CLI에서 나중에 사용할 CTS 비밀번호를 구성합니다.



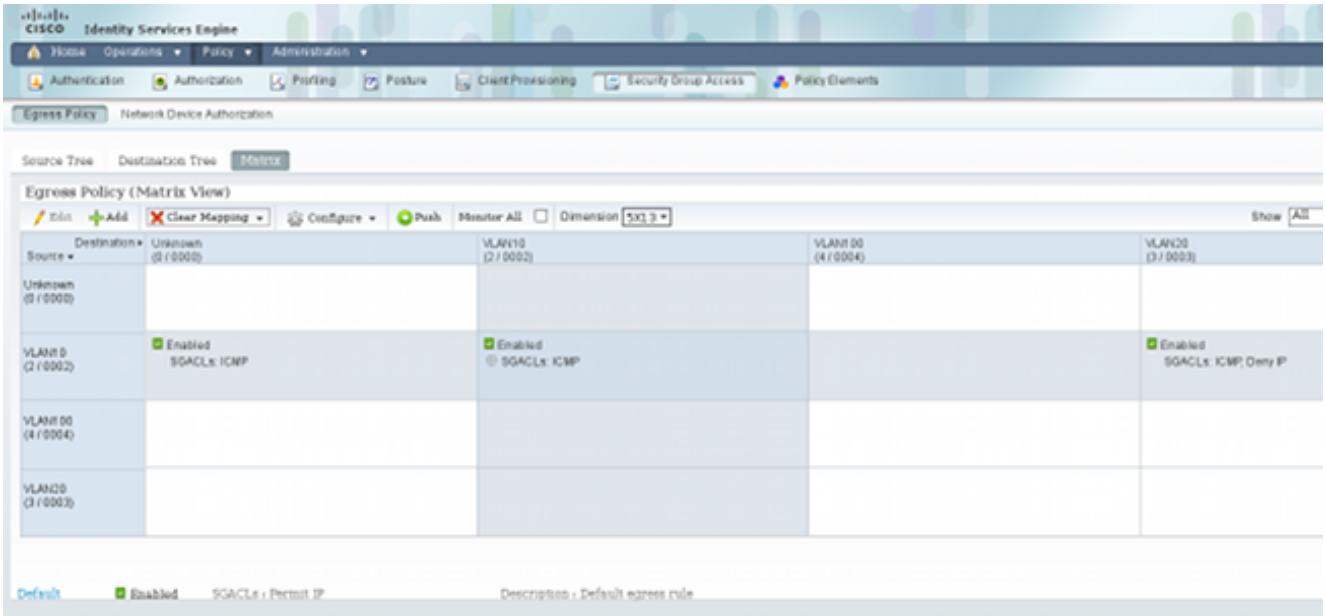
2. Policy(**정책**) > **Policy Elements(정책 요소)** > **Results(결과)** > **Security Group Access(보안 그룹 액세스)** > **Security Groups(보안 그룹)**로 이동하고 적절한 SGT를 추가합니다. 이 태그는 스위치에서 환경 새로고침을 요청할 때 다운로드됩니다.



3. Policy(**정책**) > **Policy Elements(정책 요소)** > **Results(결과)** > **Security Group Access(보안 그룹 액세스)** > **Security Group ACLs(보안 그룹 ACL)**로 이동하고 SGACL을 구성합니다.



4. Policy(**정책**) > **Security Group Access(보안 그룹 액세스**)로 이동하고 매트릭스로 정책을 정의합니다.



참고: MS Windows 신청자가 올바른 태그를 수신하도록 하려면 해당 신청자에 대한 권한 부여 정책을 구성해야 합니다. 이에 대한 자세한 [컨피그레이션은 ASA 및 Catalyst 3750X Series Switch TrustSec 컨피그레이션 예 및](#) 트러블슈팅 가이드를 참조하십시오.

3750X-5용 PAC 프로비저닝

PAC는 CTS 도메인의 인증에 필요하며(EAP-FAST의 1단계) ISE에서 환경 및 정책 데이터를 가져오는 데에도 사용됩니다. 올바른 PAC가 없으면 ISE에서 해당 데이터를 가져올 수 없습니다.

3750X-5에서 올바른 자격 증명을 제공하면 PAC를 다운로드합니다.

```
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
```

PAC는 CLI에 제공된 자격 증명과 ISE에 구성된 동일한 자격 증명과 함께 Microsoft의 MSCHAPv2(Challenge Handshake Authentication Protocol)를 사용하여 EAP-FAST를 통해 다운로드됩니다.

PAC는 환경 및 정책 새로 고침에 사용됩니다. 이러한 스위치의 경우 **cisco av 쌍 cts-pac-opaque**와 함께 RADIUS 요청을 사용합니다. 이는 PAC 키에서 파생되며 ISE에서 해독될 수 있습니다.

3750X-6 및 NDAC 인증을 위한 PAC 프로비저닝

새 디바이스가 CTS 도메인에 연결할 수 있으려면 해당 포트에서 802.1x를 활성화해야 합니다.

SAP 프로토콜은 키 관리 및 암호 그룹 협상에 사용됩니다. GMAC(Galois Message Authentication Code)는 인증에 사용되고 GCM(Galois/Counter Mode)은 암호화에 사용됩니다.

시드 스위치에서 다음을 수행합니다.

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

Non-seed 스위치에서

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

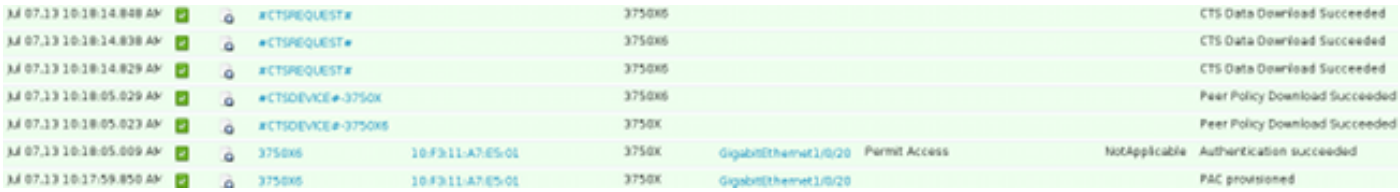
이는 트렁크 포트(스위치 스위치 MACsec)에서만 지원됩니다. SAP 대신 MKA(MACsec Key Agreement) 프로토콜을 사용하는 스위치 호스트 MACsec의 경우, MACsec 암호화 구성을 참조하십시오.

포트에서 802.1x를 활성화한 직후 비 시드 스위치는 인증자인 시드 스위치에 대한 신청자 역할을 합니다.

이 프로세스를 NDAC라고 하며, CTS 도메인에 새 디바이스를 연결하는 것이 목적입니다. 인증은 양방향입니다. 새 디바이스에는 인증 서버 ISE에서 확인되는 자격 증명이 있습니다. PAC 프로비저닝 후 디바이스는 CTS 도메인에 연결되는지 확인합니다.

> **참고**: PAC는 EAP-FAST를 위한 TLS(Transport Layer Security) 터널을 구축하는 데 사용됩니다. 3750X-6은 클라이언트가 EAP-TLS 방법을 위한 TLS 터널에 대해 서버에서 제공한 인증서를 신뢰하는 방식과 마찬가지로 서버에서 제공한 PAC 자격 증명을 신뢰합니다.

여러 RADIUS 메시지가 교환됩니다.



3750X(시드 스위치)의 첫 번째 세션은 PAC 프로비저닝에 사용됩니다. EAP-FAST는 PAC 없이 사용됩니다(MSCHAPv2 인증을 위한 익명 터널이 구축됨).

```
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
```

cts credentials 명령을 통해 구성된 MSCHAPv2 사용자 이름 및 **비밀번호**가 사용됩니다. 또한 PAC가 이미 프로비저닝된 후 추가 인증이 필요하지 않으므로 RADIUS Access-Reject가 마지막에 반환됩니다.

로그의 두 번째 항목은 802.1x 인증을 참조합니다. EAP-FAST는 이전에 프로비저닝된 PAC와 함께 사용됩니다.

```
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
```

이번에는 터널이 익명이 아니라 PAC에 의해 보호됩니다. MSCHAPv2 세션에 대해서도 동일한 자격 증명이 사용됩니다. 그런 다음 ISE의 인증 및 권한 부여 규칙에 대해 확인되고 RADIUS Access-Accept가 반환됩니다. 그런 다음 인증자 스위치가 반환된 특성을 적용하고 해당 포트에 대한 802.1x 세션이 인증된 상태로 이동합니다.

처음 두 개의 802.1x 세션에 대한 프로세스는 시드 스위치에서 어떻게 표시됩니까?

씨드에서 가장 중요한 디버그가 여기에 있습니다. 시드는 포트가 작동 중임을 감지하고 802.1x(신청자 또는 인증자)에 대해 어떤 역할을 사용해야 하는지 확인합니다.

```
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
```

마지막으로, 스위치가 ISE에 액세스할 수 있으므로 인증자 역할이 사용됩니다. 3750X-6에서 신청자 역할이 선택됩니다.

802.1x 역할 선택 세부 정보

> **참고**: 서 플리 컨 트 스위치는 PAC를 얻고 802.1x 인증 된 후, 환경 데이터를 다운로드 하고 (나중에 설명) AAA 서버의 IP 주소를 학습 합니다. 이 예에서 두 스위치 모두 ISE를 위한 전용 (백본) 연결을 갖습니다. 나중에 역할은 다를 수 있습니다. AAA 서버의 응답을 받은 첫 번째 스위치가 인증자가 되고 두 번째 스위치가 신청자가 됩니다.

이는 ALIVE로 표시된 AAA 서버의 두 스위치에서 모두 EAP(Extensible Authentication Protocol) 요청 ID를 보내기 때문에 가능합니다. EAP ID 응답을 처음 수신하는 것이 인증자가 되고 후속 ID 요청을 삭제합니다.

No.	Time	Source	Destination	Protocol	Length	Info
1	2013-07-08 22:20:28.255317000	Cisco_25:a5:14	Nearest	EAPOL	60	Start
2	2013-07-08 22:20:28.278219000	Cisco_a7:e5:01	Nearest	EAPOL	60	Start
3	2013-07-08 22:20:28.280005000	Cisco_25:a5:14	Nearest	EAP	60	Request, Identity
4	2013-07-08 22:20:28.289280000	Cisco_a7:e5:01	Nearest	EAP	60	Request, Identity
5	2013-07-08 22:20:28.290800000	Cisco_a7:e5:01	Nearest	EAP	60	Response, Identity
6	2013-07-08 22:20:28.317915000	Cisco_25:a5:14	Nearest	EAP	60	Request, Identity
7	2013-07-08 22:20:28.324109000	Cisco_a7:e5:01	Nearest	EAP	60	Response, Identity
8	2013-07-08 22:20:28.325778000	Cisco_25:a5:14	Nearest	EAP	60	Response, Identity
9	2013-07-08 22:20:28.330537000	Cisco_a7:e5:01	Nearest	EAP	60	Request, Identity
10	2013-07-08 22:20:28.401497000	Cisco_25:a5:14	Nearest	TLSv1	60	Ignored Unknown Record
11	2013-07-08 22:20:28.407817000	Cisco_a7:e5:01	Nearest	TLSv1	266	Client Hello

```
▸ Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Cisco_a7:e5:01 (10:f3:11:a7:e5:01), Dst: Nearest (01:80:c2:00:00:03)
▾ 802.1X Authentication
    Version: 802.1X-2010 (3)
    Type: EAP Packet (0)
    Length: 15
  ▾ Extensible Authentication Protocol
      Code: Response (2)
      Id: 1
      Length: 15
      Type: Identity (1)
      Identity: CTS client
```

802.1x 역할을 선택한 후(이 시나리오에서 3750X-6은 아직 AAA 서버에 액세스할 수 없으므로 신청자), 다음 패킷에는 PAC 프로비저닝을 위한 EAP-FAST 교환이 포함됩니다. 사용자 이름 **CTS 클라이언트**는 RADIUS 요청 사용자 이름 및 EAP ID로 사용됩니다.

```
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]
```

익명 EAP-FAST 터널이 구축되면 사용자 이름 **3750X6**(cts **자격 증명**)에 대해 MSCHAPv2 세션이 발생합니다. TLS 터널(암호화됨)이기 때문에 스위치에서 이를 확인할 수는 없지만, PAC 프로비저닝을 위한 ISE의 자세한 로그가 이를 입증합니다. RADIUS 사용자 이름**에** 대한 CTS 클라이언트 및 EAP ID 응답을 볼 수 있습니다. 그러나 내부 방법(MSCHAP)에는 3750**X6 사용자 이름**이 사용됩니다.

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

두 번째 EAP-FAST 인증이 발생합니다. 이번에는 이전에 프로비저닝된 PAC를 사용합니다. 다시 CTS **클라이언트**는 RADIUS 사용자 이름 및 외부 ID로 사용되지만 **3750X6**은 내부 ID(MSCHAP)에 사용됩니다. 인증 성공:

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)

그러나 이번에는 ISE가 RADIUS Accept 패킷의 여러 특성을 반환합니다.

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
```

여기서 인증자 스위치는 포트를 인증된 상태로 변경합니다.

```
bsns-3750-5#show authentication sessions int g1/0/20
```

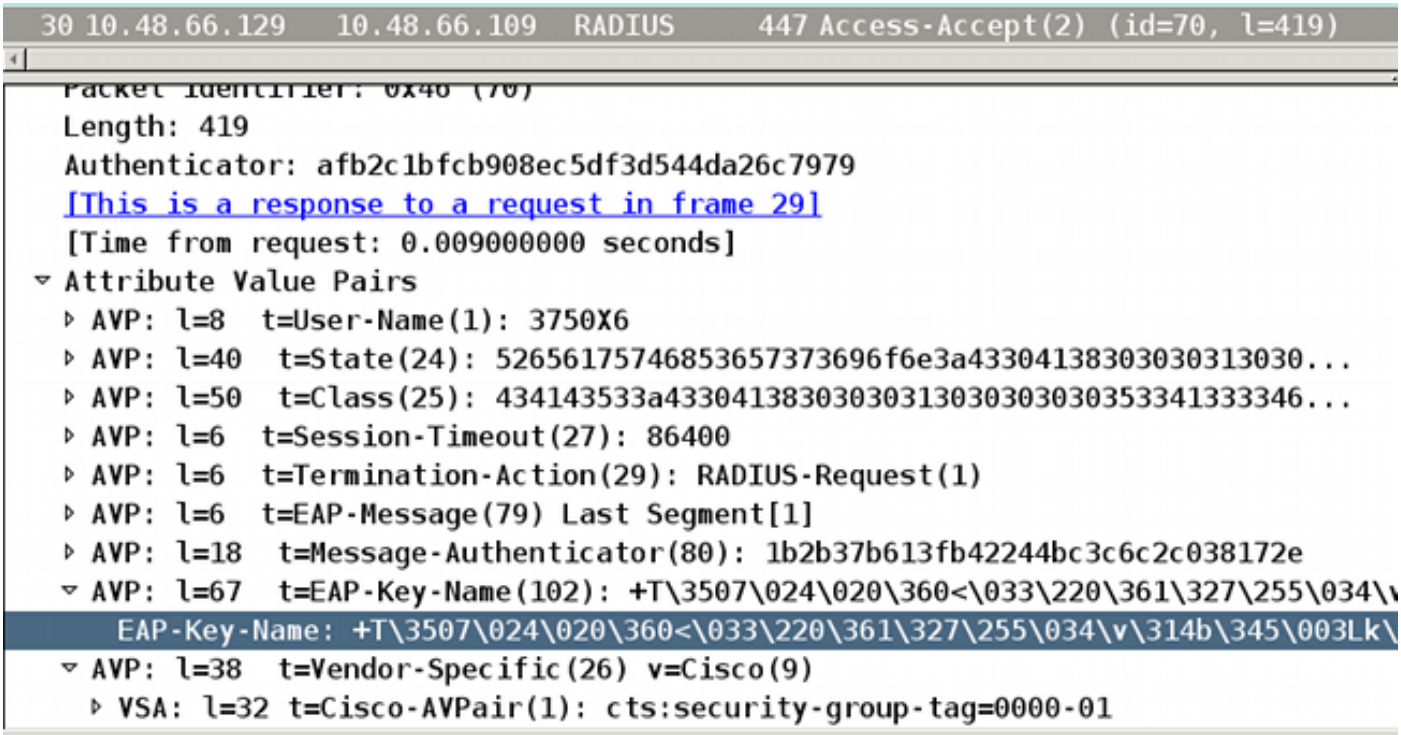
```
          Interface:  GigabitEthernet1/0/20
        MAC Address:  10f3.11a7.e501
         IP Address:  Unknown
           User-Name:  3750X6
              Status:  Authz Success
             Domain:  DATA
    Security Policy:  Should Secure
    Security Status:  Unsecure
     Oper host mode:  multi-host
   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
```

인증자 스위치는 사용자 이름이 3750**X6**임을 어떻게 **인식합니까**? RADIUS 사용자 이름 및 외부 EAP ID의 경우 **CTS 클라이언트**가 사용되며 내부 ID는 암호화되며 인증자에 대해 표시되지 않습니다. 사용자 이름은 ISE에서 학습합니다. 마지막 RADIUS 패킷(Access-Accept)에는 **username=3750X6이 포함되어** 있지만 다른 모든 패킷에는 **username = Cts 클라이언트가 포함되어 있습니다**. 서 플리 컨 트 스위치가 실제 사용자 이름을 인식 하는 이유입니다. 이 동작은 RFC 규격입니다. RFC3579 섹션 3.0에서:

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

802.1x 인증 세션의 마지막 패킷에서 ISE는 EAP-**Key-Name이** 포함된 RADIUS Accept 메시지 **cisco-av-pair를 반환합니다**.

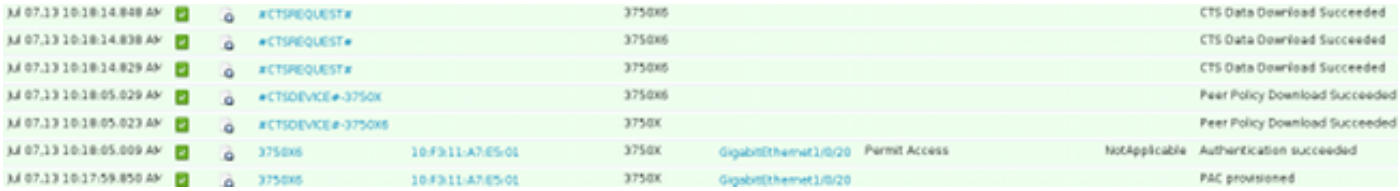


이는 SAP 협상의 핵심 자료로 사용됩니다.

또한 SGT가 전달됩니다. 즉, 인증자 스위치는 **기본값 = 0**으로 서 플리 컨 트의 트래픽에 **태그를 지정 합니다**. ISE에서 특정 값을 구성하여 다른 값을 반환할 수 있습니다. 태그되지 않은 트래픽에만 적용됩니다. 기본적으로 인증자 스위치는 인증된 신청자의 트래픽을 신뢰하므로 태그된 트래픽은 재작성되지 않습니다(그러나 ISE에서 변경할 수도 있음).

SGA 정책 다운로드

첫 번째 802.1x EAP-FAST 세션 2개(첫 번째 PAC 프로비저닝 세션 및 두 번째 인증 세션) 이외의 추가 RADIUS 교환(EAP 없음)이 있습니다. 다음은 다시 ISE 로그입니다.



세 번째 로그(**피어 정책 다운로드**)는 3760**X6 사용자**에 대한 간단한 RADIUS 교환 RADIUS 요청 및 RADIUS **수락**을 나타냅니다. 이는 신청자로부터 트래픽에 대한 정책을 다운로드하기 위해 필요합니다. 가장 중요한 두 가지 특성은 다음과 같습니다.

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

따라서 인증자 스위치는 신청자가 SGT 태깅한 트래픽을 신뢰하며(cts:**trusted-device=true**), 태그가 지정되지 않은 트래픽도 **tag=0**으로 **태깅합니다**.

네 번째 로그는 동일한 RADIUS 교환을 나타냅니다. 그러나 이번에는 **3750X5** 사용자(인증자)를 위한 것입니다. 이는 두 피어가 서로에 대한 정책을 가지고 있어야 하기 때문이다. 신청자는 여전히 AAA 서버의 IP 주소를 알지 못한다는 점이 흥미롭습니다. 따라서 인증자 스위치는 신청자 대신 정책을 다운로드합니다. 이 정보는 나중에 SAP 협상에서 신청자(ISE IP 주소와 함께)에게 전달됩니다 .

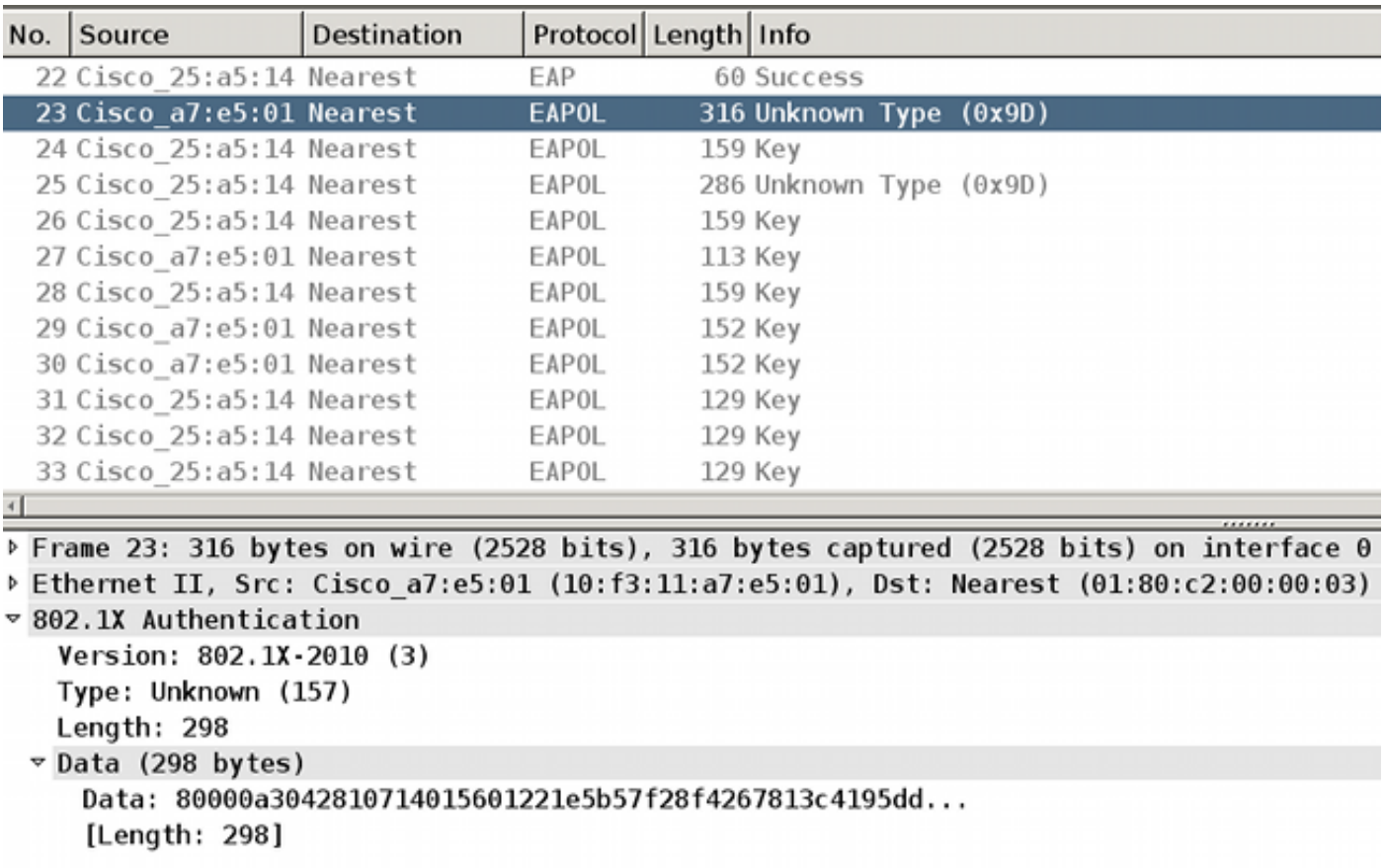
SAP 협상

802.1x 인증 세션이 끝나면 즉시 SAP 협상이 발생합니다. 이 협상은 다음을 위해 필요합니다.

- 암호화 수준 협상(**sap mode-list gcm-encrypt** 명령 사용) 및 암호 그룹
- 데이터 트래픽에 대한 세션 키 도출
- 키 재설정 프로세스 진행
- 추가 보안 검사를 수행하고 이전 단계가 안전한지 확인합니다

SAP는 Cisco Systems에서 802.11i/D6.0의 초안 버전을 기반으로 설계된 프로토콜입니다. 자세한 내용은 Cisco TrustSec Security Association Protocol - Cisco Nexus 7000 페이지용 Cisco Trusted Security를 지원하는 프로토콜에서 액세스를 요청합니다.

SAP Exchange는 802.1AE를 준수합니다. EAPOL(Extensible Authentication Protocol over LAN) 키 교환은 암호 그룹을 협상하고, 보안 매개변수를 교환하고, 키를 관리하기 위해 신청자와 인증자 간에 수행됩니다. 안타깝게도 Wireshark에는 모든 필수 EAP 유형에 대한 디코더가 없습니다.



이러한 작업을 성공적으로 완료하면 SA(Security Association)가 설정됩니다.

서 플리 컨 트 스위치에서:

```
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
```

인증자:

```
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
```

여기서 포트는 gcm-encrypt 모드를 사용합니다. 즉, 트래픽은 인증 및 암호화되었을 뿐만 아니라 올바르게 SGT 태그가 지정되었음을 의미합니다. 두 디바이스 모두 ISE에서 특정 네트워크 디바이스 권한 부여 정책을 사용하지 않습니다. 즉, 디바이스에서 시작된 모든 트래픽이 기본 태그 **0을** 사용합니다. 또한 두 스위치 모두 피어 정책 다운로드 단계의 RADIUS 특성 때문에 피어에서 수신한 SGT를 신뢰합니다.

환경 및 정책 업데이트

두 디바이스가 모두 CTS 클라우드에 연결되면 환경 및 정책 업데이트가 시작됩니다. SGT와 이름을 가져오려면 환경을 새로 고쳐야 하며, ISE에 정의된 SGACL을 다운로드하려면 정책을 새로 고쳐야 합니다.

이 단계에서 신청자는 이미 AAA 서버의 IP 주소를 알고 있으므로 자체적으로 할 수 있습니다.

환경 및 정책 업데이트에 대한 자세한 내용은 ASA 및 Catalyst 3750X Series Switch TrustSec 컨피그레이션 예 및 트러블슈팅 가이드를 참조하십시오.

신청자 스위치는 구성된 RADIUS 서버가 없고 CTS 링크가 (인증자 스위치로) 다운될 때에도 RADIUS 서버 IP 주소를 기억합니다. 그러나 스위치에서 다음 사항을 무시하도록 강제할 수 있습니다.

```
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
```

서 플리 컨 트 스위치의 환경 및 정책을 확인 하려면 다음 명령을 입력 합니다.

```
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
```

정책이 표시되지 않는 이유는 무엇입니까? 정책을 적용하려면 cts 시행을 활성화해야 하므로 정책이 표시되지 않습니다.

```
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
```

인증자가 추가 정보를 가지고 있는 동안 신청자가 Unknown을 **그룹화하는** 정책이 하나만 있는 이유는 무엇입니까?

```
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
```

클라이언트에 대한 포트 인증

MS Windows 클라이언트가 3750-5 스위치의 **g1/0/1** 포트에 연결되어 인증됩니다.

```
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
```

여기서 스위치(3750-5)는 CTS 클라우드로 전송할 때 해당 호스트의 트래픽이 **SGT=3**으로 태그되어야 함을 알고 있습니다.

SGT를 사용한 트래픽 태깅

트래픽을 어떻게 탐지하고 확인합니까?

이는 다음과 같은 이유 때문에 어렵습니다.

- 내장형 패킷 캡처는 IP 트래픽에 대해서만 지원됩니다(그리고 SGT 및 MACsec 페이로드가 있는 수정된 이더넷 프레임).
- **복제 키워드가** 있는 SPAN(Switched Port Analyzer) 포트 - 이 방법이 작동할 수 있지만, 문제는 모니터링 세션의 대상 포트에 연결된 Wireshark가 있는 모든 PC가 하드웨어 레벨에서 발생할 수 있는 802.1ae의 지원 부족으로 인해 프레임을 삭제하는 것입니다.
- replication 키워드가 없는 **SPAN** 포트는 대상 **포트**에 배치되기 전에 cts 헤더를 제거합니다.

SGACL로 정책 시행

CTS 클라우드에서의 정책 시행은 항상 목적지 포트에서 수행됩니다. 마지막 디바이스만 해당 스위치에 직접 연결된 엔드포인트 디바이스의 대상 SGT를 알고 있기 때문입니다. 패킷은 소스 SGT만 전달합니다. 결정을 내리기 위해서는 소스 및 대상 SGT가 모두 필요합니다.

따라서 디바이스에서 ISE의 모든 정책을 다운로드할 필요가 없습니다. 대신 디바이스가 직접 연결된 SGT와 관련된 정책의 부분만 필요합니다.

다음은 신청자 스위치인 3750-6입니다.

```
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
```

여기에는 두 가지 정책이 있습니다. 첫 번째는 태그가 지정되지 않은 트래픽(시작/종료)에 대한 기본 값입니다. 두 번째는 **SGT=2**에서 태그가 지정되지 않은 SGT(**0**)로 **이동합니다**. 디바이스 자체가 ISE의 SGA 정책을 사용하고 SGT**=0**에 속하기 때문에 이 **정책이 존재합니다**. 또한 **SGT=0**은 기본 태그입니다. 따라서 SGT**=0**으로/**에서** 트래픽에 대한 규칙이 **있는** 모든 **정책을 다운로드해야** 합니다. 매트릭스를 보면 **2**에서 **0**까지의 정책이 하나만 **표시됩니다**.

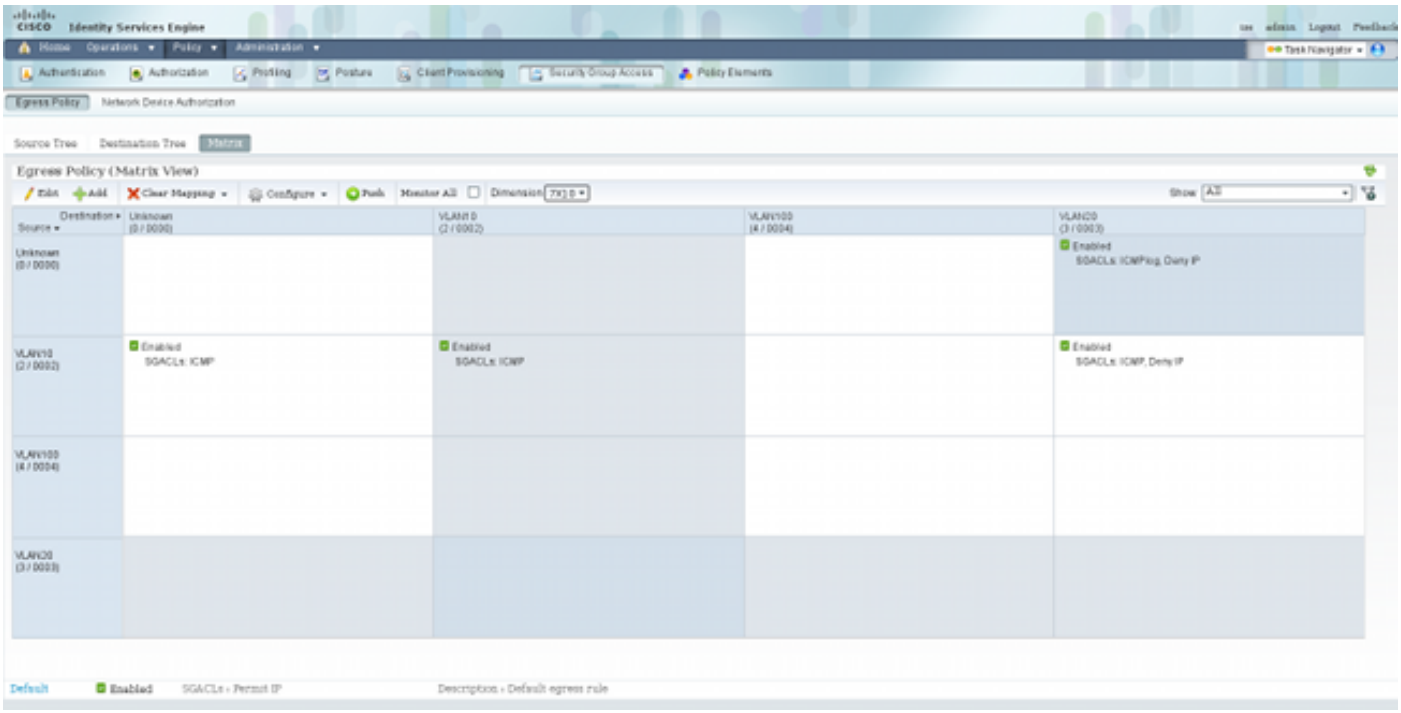
다음은 인증자 스위치인 3750-5입니다.

```
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
```

여기에 **2**시부터 **3**시까지의 **정책이** 하나 더 **있습니다**. 이는 802.1x 클라이언트(MS Windows)가 **g1/0/1에** 연결되고 SGT**=3**으로 **태그가 지정되었기** 때문입니다. 따라서 모든 정책을 SGT **=3**에 **다운로드해야 합니다**.

3750X-6(SGT**=0)**에서 MS Windows XP(SGT**=3)로 ping**을 시도합니다. 3750X-5는 시행 장치입니다.

이 전에 SGT=0에서 SGT=3으로의 트래픽에 대해 ISE**에서 정책을 구성해야 합니다**. 이 예에서는 라인만 있는 SGACL ICMP(Internet Control Message Protocol) 로그를 만들고 **허용 icmp 로그**를 생성한 다음, SGT=**0에서 SGT=3으로 이동하는 트래픽에** 대해 행렬에서 **사용합니다**.



다음은 시행 스위치에서 정책을 새로 고치고 새 정책을 확인하는 내용입니다.

```
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
```

ACL(Access Control List)이 ISE에서 다운로드되었는지 확인하려면 다음 명령을 입력합니다.

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

ACL이 적용되었는지(하드웨어 지원) 확인하려면 다음 명령을 입력합니다.

```
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
```

다음은 ICMP 이전의 카운터입니다.

```
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
```

다음은 SGT=0(3750-6 스위치)에서 MS Windows XP(SGT=3)로 ping 및 카운터입니다.

```
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
```

다음은 ACL 카운터입니다.

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

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- 3750용 Cisco TrustSec 컨피그레이션 가이드
- Cisco TrustSec Configuration Guide for ASA 9.1
- Cisco TrustSec 구축 및 로드맵
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.