ASA 및 Catalyst 3750X Series Switch TrustSec 구성 예 및 문제 해결 가이드

목차

소개

이 문서에서는 Cisco ASA(Secure Adaptive Security Appliance) 및 Cisco Catalyst 3750X Series 스위치(3750X)에서 Cisco TrustSec(CTS)을 구성하는 방법에 대해 설명합니다.

SGT(Security Group Tag)와 IP 주소 간의 매핑을 학습하기 위해 ASA는 SXP(SGT Exchange Protocol)를 사용합니다. 그런 다음 SGT 기반의 ACL(Access Control List)을 사용하여 트래픽을 필터링합니다. 3750X는 Cisco ISE(Identity Services Engine)에서 RBACL(Role-Based Access Control List) 정책을 다운로드하고 이를 기반으로 트래픽을 필터링합니다. 이 문서에서는 통신 작동

방식과 예상 디버그를 설명하기 위해 패킷 레벨에 대해 자세히 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

- CTS 구성 요소
- ASA 및 Cisco IOS의 CLI 구성®

사용되는 구성 요소

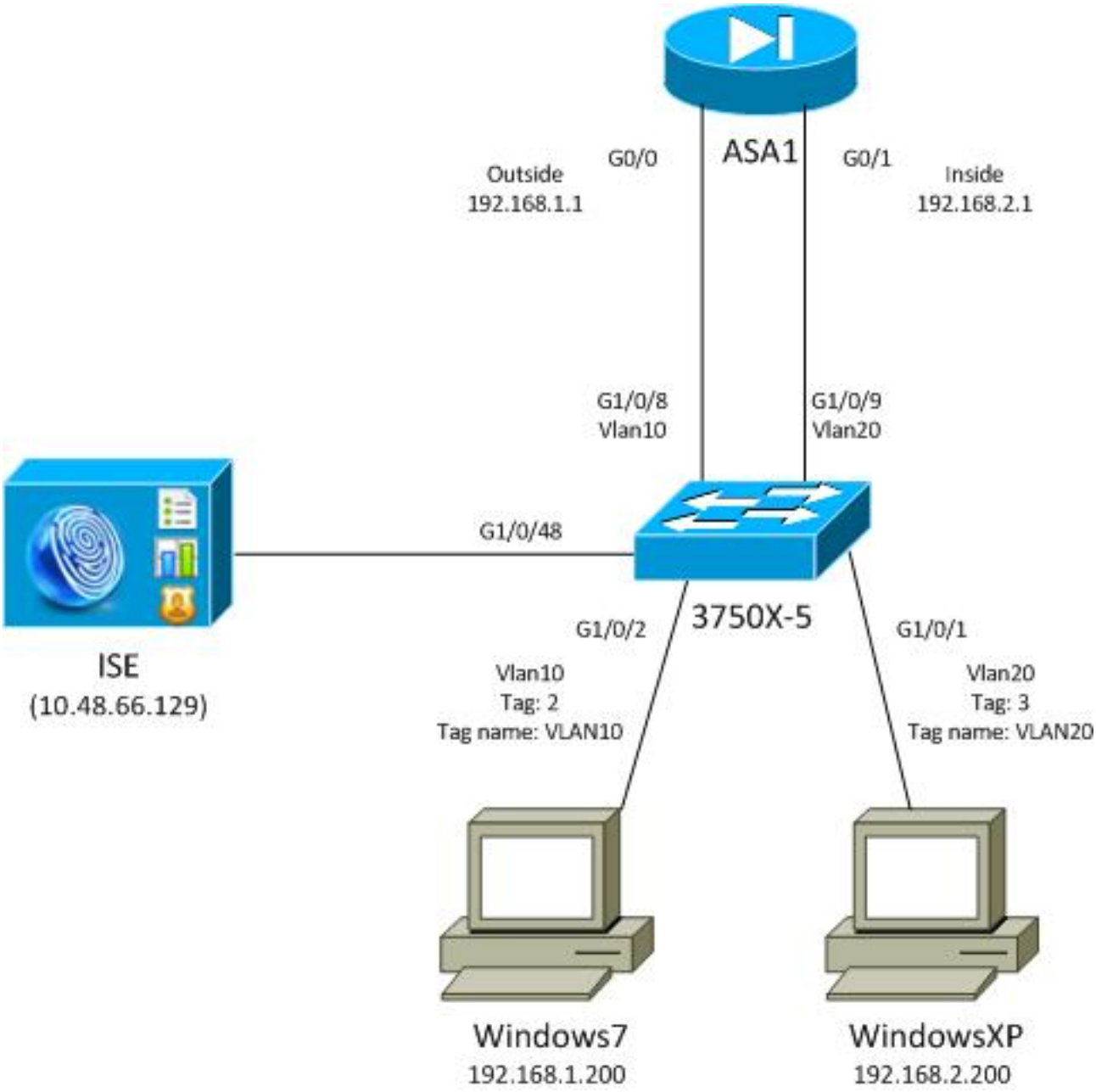
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 소프트웨어 버전 9.1 이상
- Microsoft(MS) Windows 7 및 MS Windows XP
- Cisco 3750X 소프트웨어, 버전 15.0 이상
- Cisco 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



트래픽 흐름

다음은 트래픽 흐름입니다.

- 3750X는 포트 인증을 위해 **G1/0/1** 및 **G1/0/2**에 구성됩니다.
- ISE는 AAA(Authentication, Authorization, and Accounting) 서버로 사용됩니다.
- MAB(MAC Address Bypass)는 MS Windows 7의 인증에 사용됩니다.
- IEEE 802.1x는 어떤 인증 방법을 사용하든 상관없음을 입증하기 위해 MS Windows XP에 사용됩니다.

인증에 성공하면 ISE는 SGT를 반환하며 3750X는 해당 태그를 인증 세션에 바인딩합니다. 또한 스위치는 ip device tracking 명령을 사용하여 두 스테이션의 **IP 주소를** 학습합니다. 그런 다음 스위치는 SXP를 사용하여 SGT와 IP 주소 간의 매핑 테이블을 ASA에 전송합니다. 두 MS Windows PC에는 모두 ASA를 가리키는 기본 라우팅이 있습니다.

ASA는 SGT에 매핑된 IP 주소에서 트래픽을 수신한 후, SGT를 기반으로 ACL을 사용할 수 있습니다. 또한 3750X를 라우터(두 MS Windows 스테이션의 기본 게이트웨이)로 사용할 경우 ISE에서 다운로드한 정책을 기반으로 트래픽을 필터링할 수 있습니다.

컨피그레이션 및 확인을 위한 단계는 다음과 같습니다. 각 단계는 이 문서의 뒷부분에 자세히 설명되어 있습니다.

- 3750X에서 **ip device tracking** 명령을 사용한 포트 인증
- 인증, SGT 및 SGACL(Security Group Access Control List) 정책에 대한 ISE 컨피그레이션
- ASA 및 3750X의 CTS 컨피그레이션
- 3750X(자동) 및 ASA(수동)에서 PAC(Protected Access Credential) 프로비저닝
- ASA 및 3750X에서 환경 업데이트
- 3750X에서 포트 인증 확인 및 적용
- 3750X에서 정책 새로 고침
- SXP 교환(리스너로서의 ASA 및 스피커로서의 3750X)
- SGT ACL을 사용하는 ASA의 트래픽 필터링
- ISE에서 다운로드한 정책을 사용하여 3750X에서 트래픽 필터링

설정

3750X에서 *ip device tracking* 명령을 사용한 포트 인증

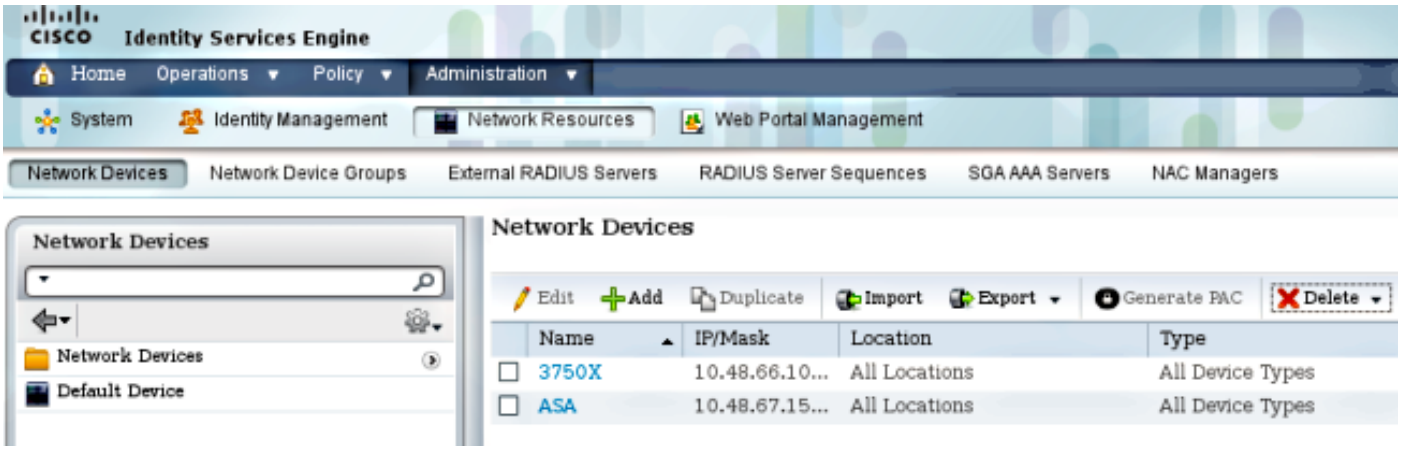
이는 802.1x 또는 MAB에 대한 일반적인 컨피그레이션입니다. RADIUS CoA(Change of Authorization)는 ISE의 활성 알림을 사용하는 경우에만 필요합니다.

```
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
```

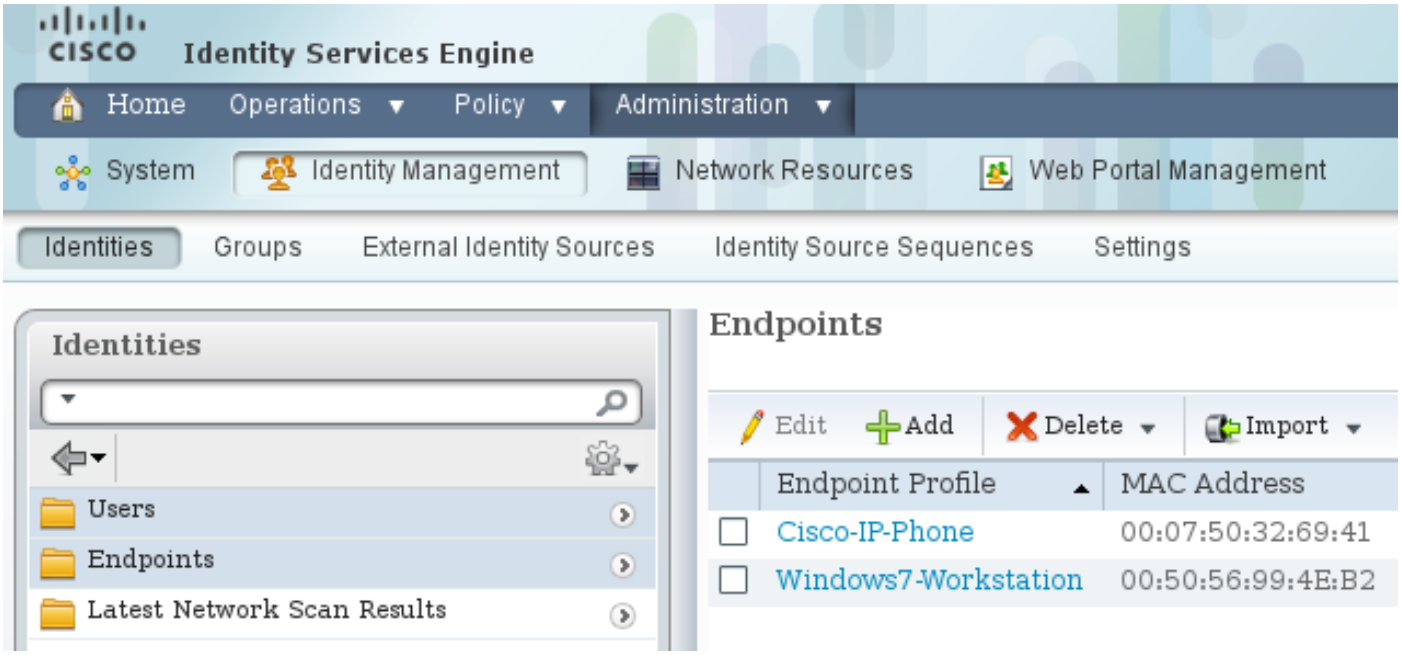
```
radius-server vsa send authentication
```

인증, SGT 및 SGACL 정책에 대한 ISE 컨피그레이션

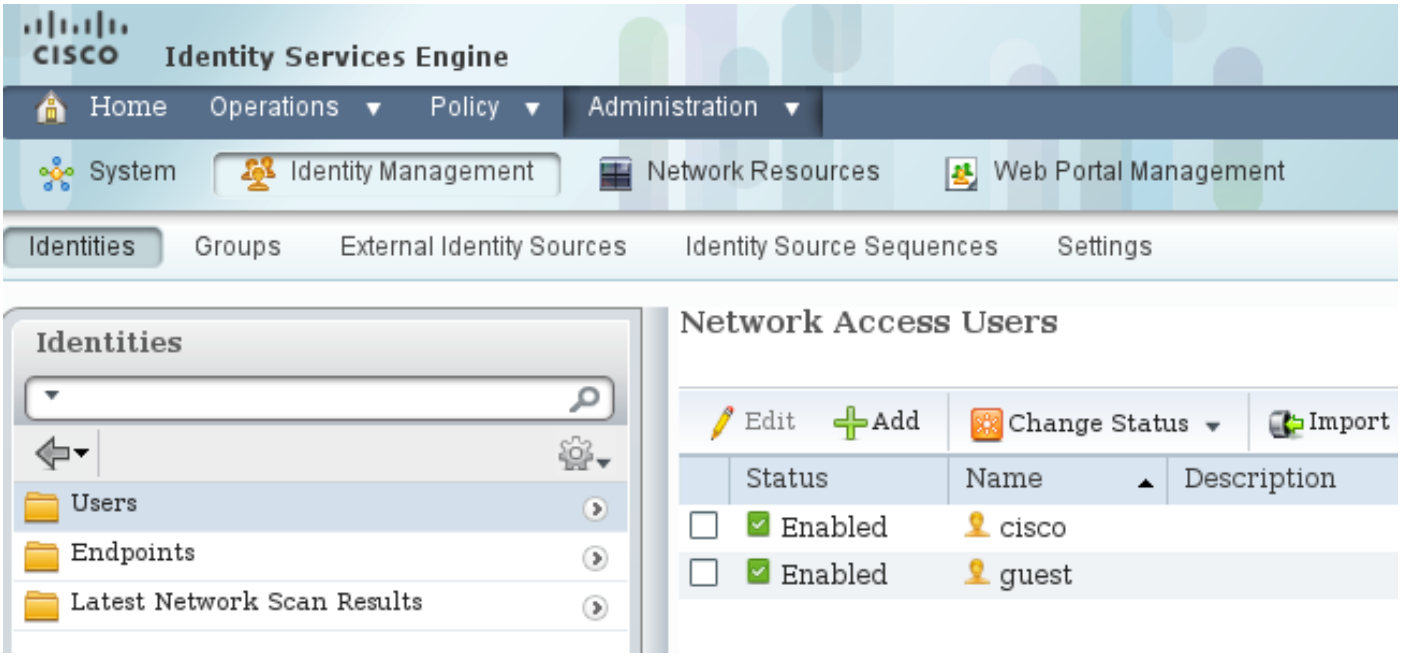
ISE에는 Administration(관리) > Network Devices(네트워크 디바이스)에서 두 **네트워크 디바이스가 모두 구성되어** 있어야 합니다.



MAB 인증을 사용하는 MS Windows 7의 경우 **Administration(관리) > Identity Management(ID 관리) > Identities(ID) > Endpoints(엔드포인트) 아래에서 엔드포인트 ID(MAC 주소)를** 만들어야 합니다.

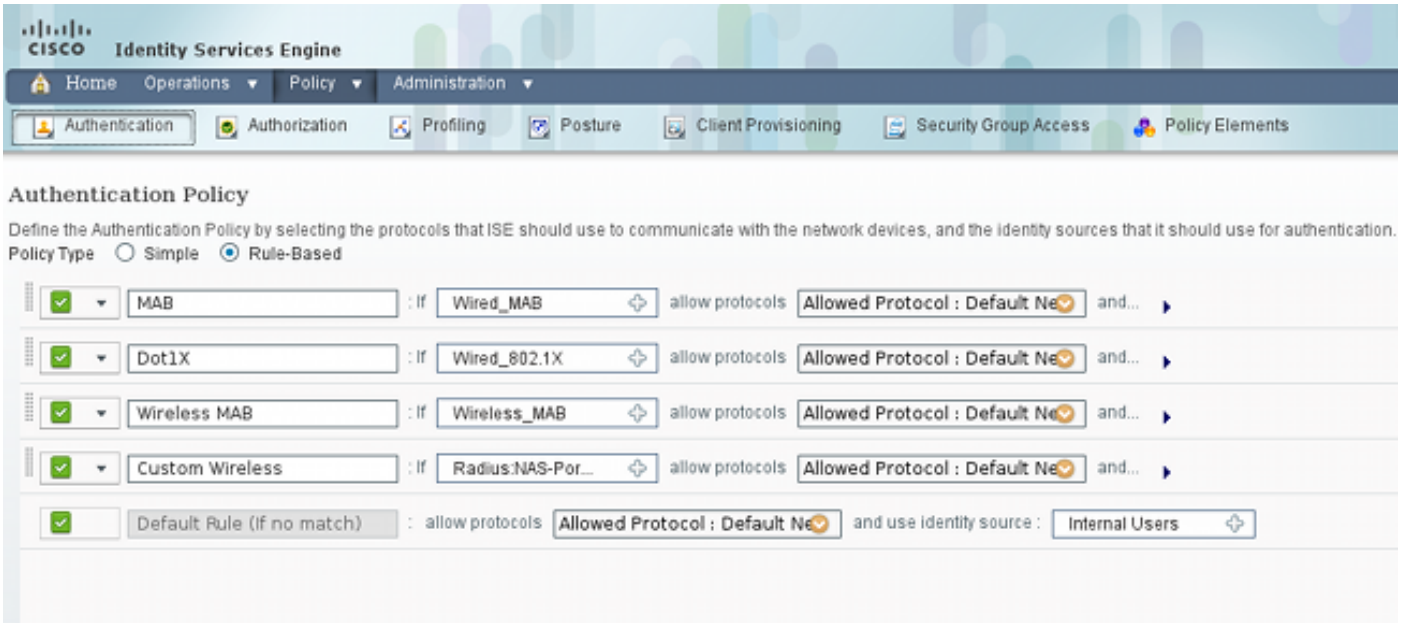


802.1x 인증을 사용하는 MS Windows XP의 경우 **Administration(관리) > Identity Management(ID 관리) > Identities(ID) > Users(사용자) 아래에서 사용자 ID(사용자 이름)를** 만들어야 합니다.

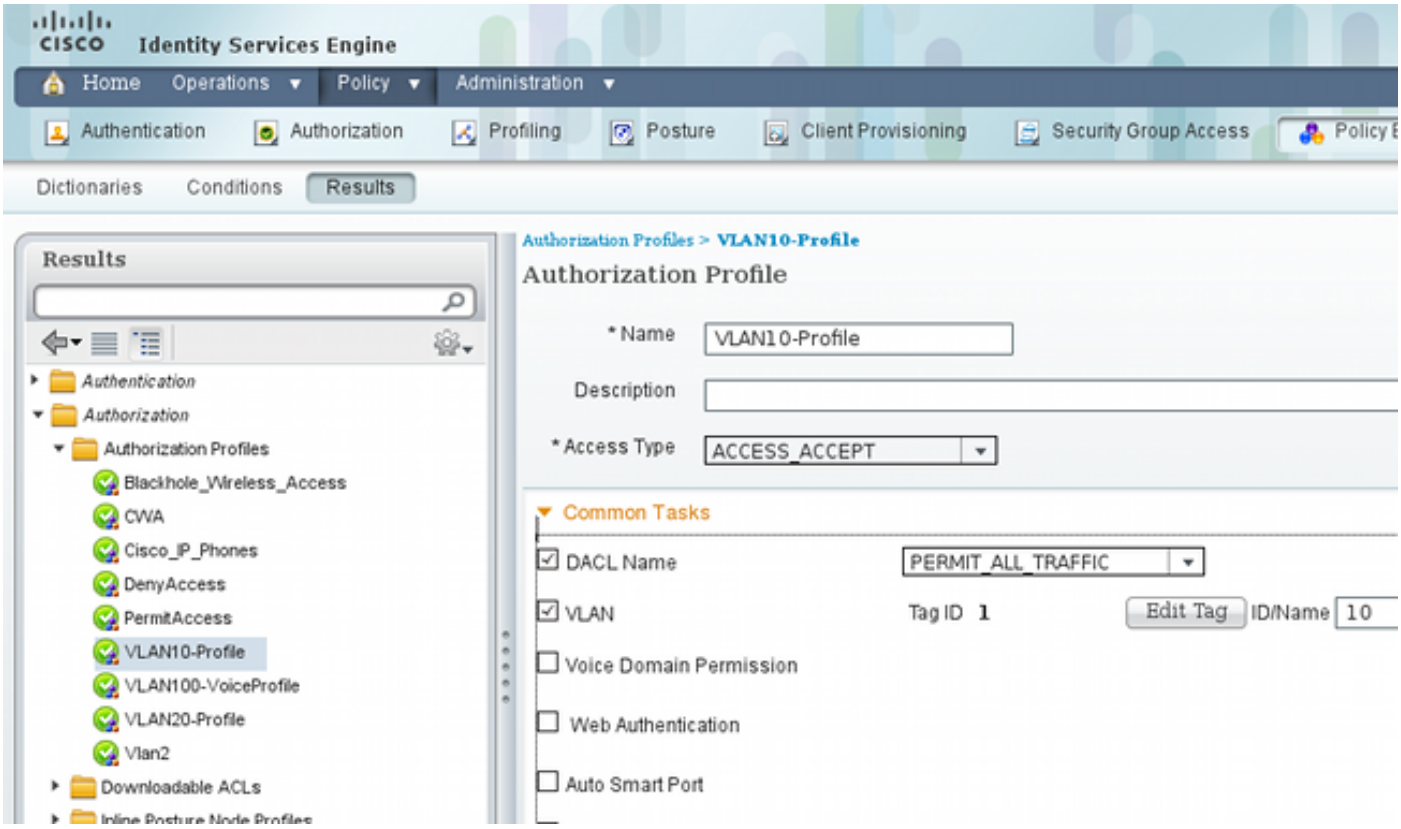


사용자 이름 **cisco**가 사용됩니다. 이 자격 증명으로 EAP-PEAP(Extensible Authentication Protocol-Protected EAP)에 대해 MS Windows XP를 구성합니다.

ISE에서는 기본 인증 정책이 사용됩니다(이 변경 안 함). 첫 번째는 MAB 인증을 위한 정책이고, 두 번째는 802.1x입니다.



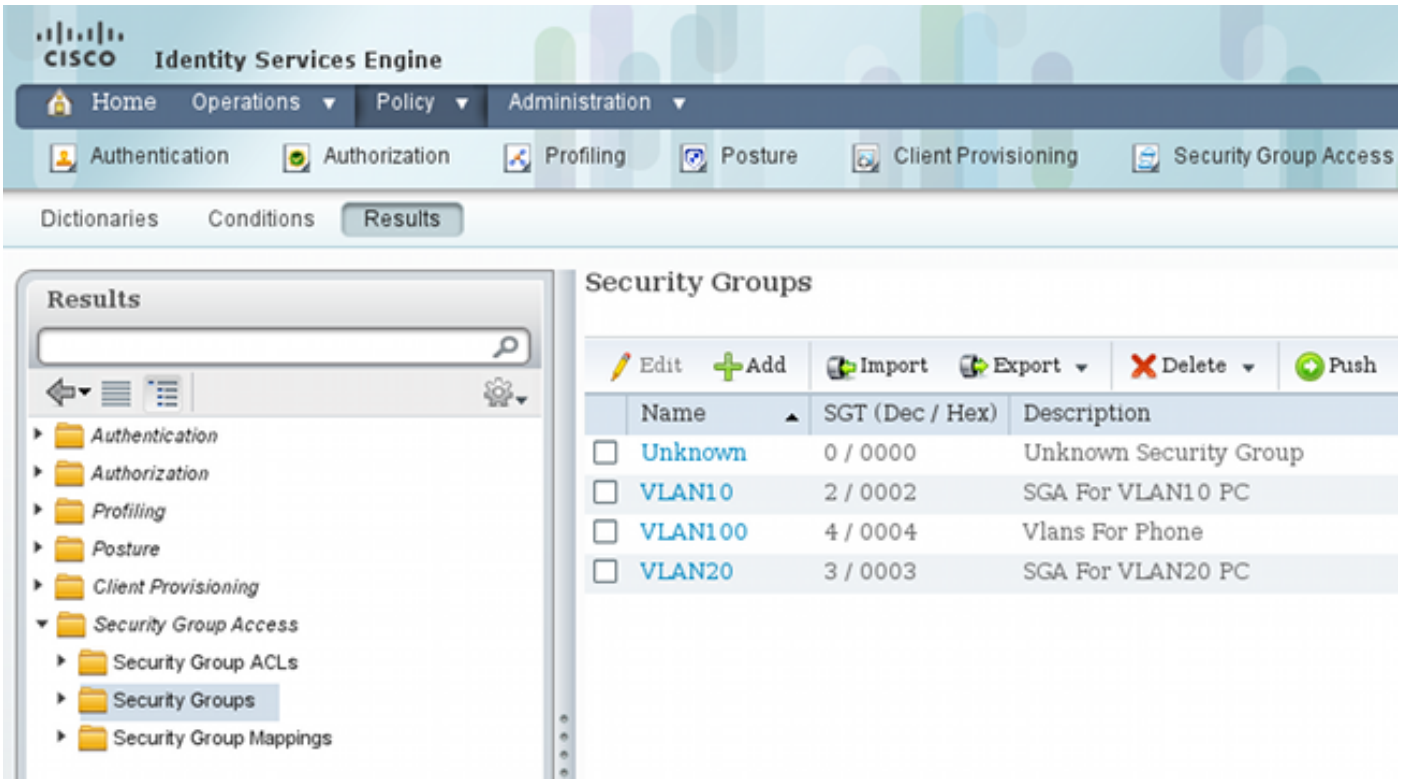
권한 부여 정책을 구성하려면 Policy(정책) > Results(결과) > Authorization(권한 부여) > **Authorization Profiles(권한 부여 프로파일)에서 권한 부여 프로파일을** 정의해야 합니다. 모든 트래픽을 허용하는 DACL(Downloadable ACL)이 있는 VLAN10-Profile은 MS Windows 7 프로필에 사용됩니다.



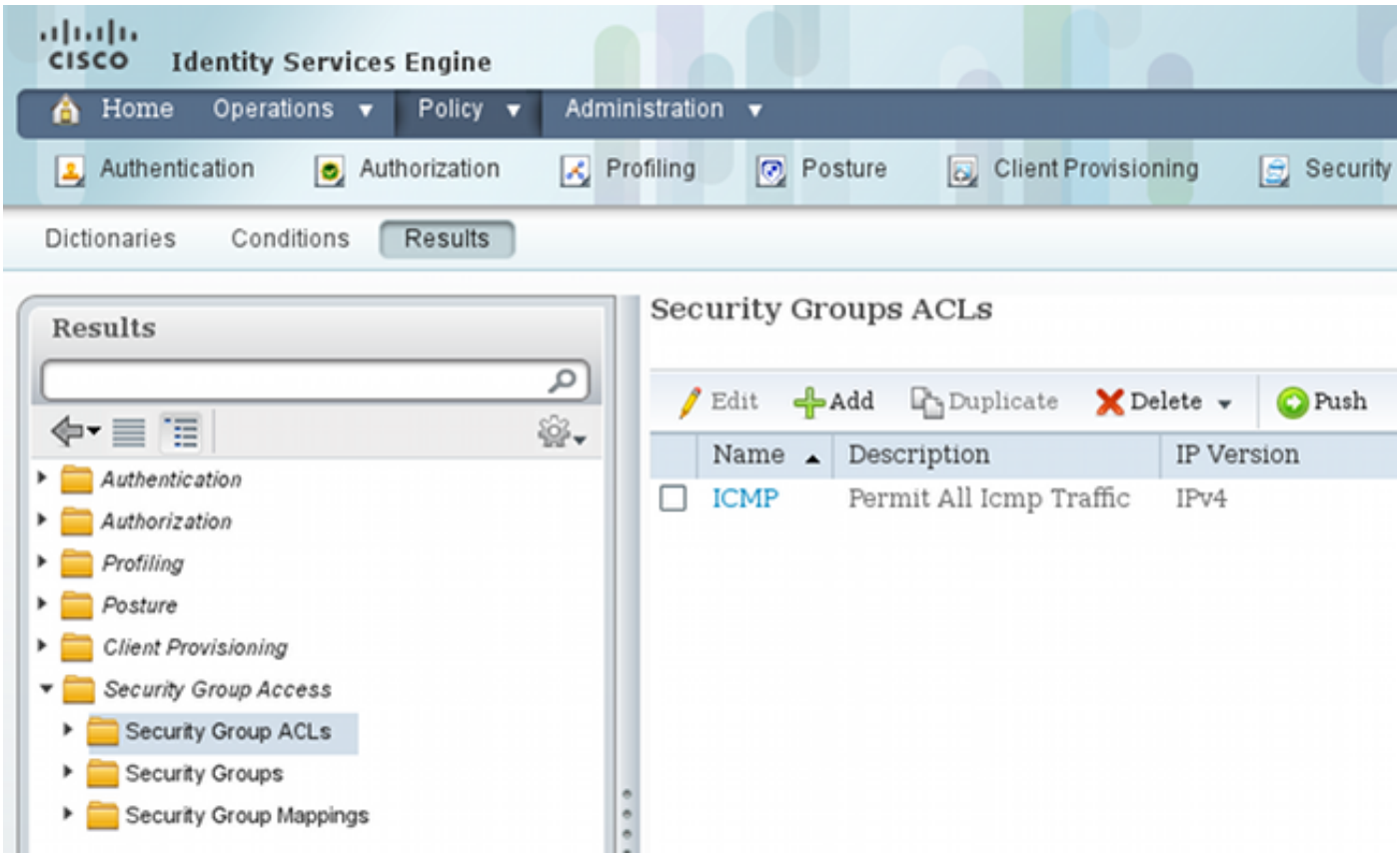
유사한 컨피그레이션 VLAN20-Profile이 MS Windows XP에서 사용되지만 VLAN 번호(20)는 예외입니다.

ISE에서 SGT 그룹(태그)을 구성하려면 **Policy(정책) > Results(결과) > Security Group Access(보안 그룹 액세스) > Security Groups(보안 그룹)로 이동합니다**.

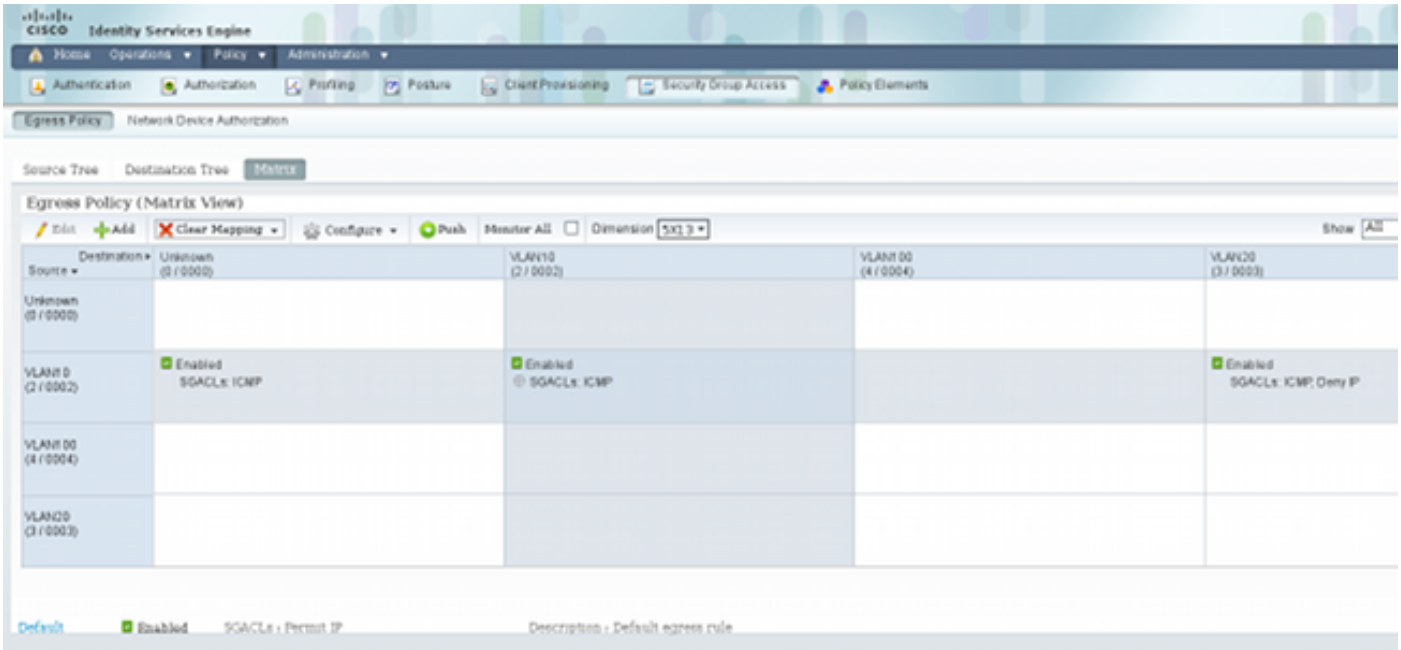
> **참고**: 태그 번호는 선택할 수 없습니다. 태그 번호는 1을 제외한 첫 번째 사용 가능한 번호에 의해 자동으로 선택됩니다. SGT 이름만 구성할 수 있습니다.



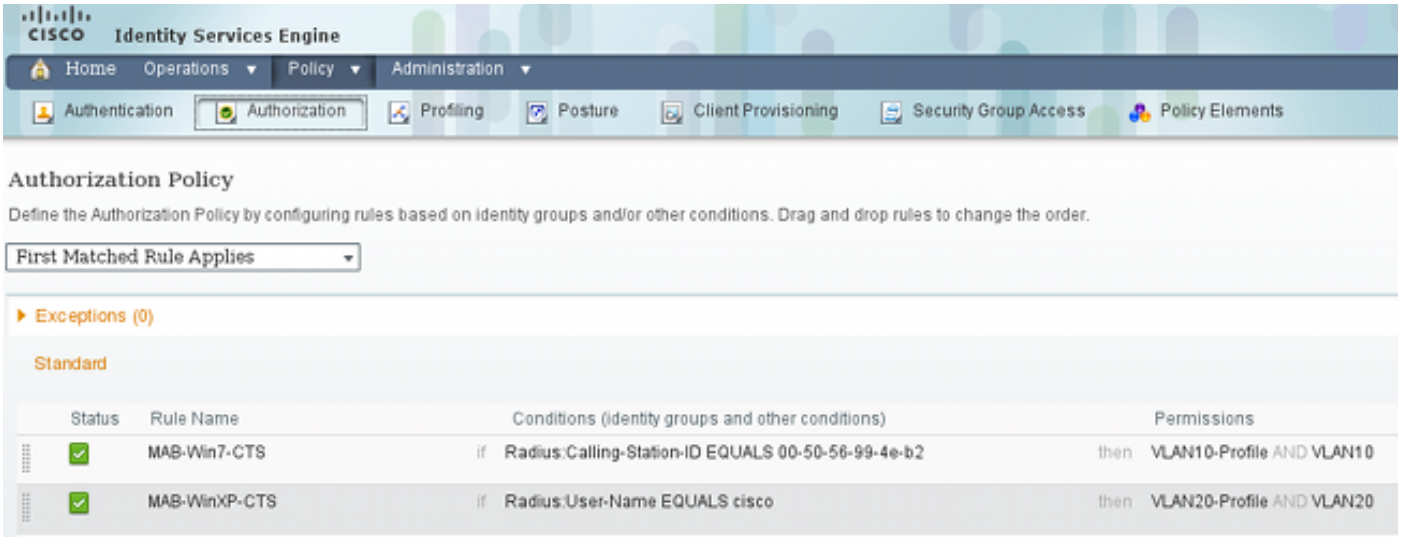
ICMP(Internet Control Message Protocol) 트래픽을 허용하는 SGACL을 생성하려면 **Policy(정책) > Results(결과) > Security Group Access(보안 그룹 액세스) > Security Group ACLs(보안 그룹 ACL)로** 이동합니다.



정책을 생성하려면 Policy(정책) > **Security Group Access(보안 그룹 액세스) > Egress Policy(이그레스 정책)로 이동합니다**. VLAN10과 알 수 없는 VLAN 또는 VLAN10 또는 VLAN20 간의 트래픽에는 ICMP ACL이 사용됩니다(**허용 icmp**).



권한 부여 규칙을 설정하려면 **Policy > Authorization**으로 **이동합니다**. MS Windows 7(특정 MAC 주소)의 경우 VLAN**10-Profile**이 사용되며, VLAN10 및 DACL을 반환하고 SGT가 VLAN10인 보안 프로필 **VLAN10을 반환합니다**. MS Windows XP(특정 사용자 이름)의 경우 VLAN**20-Profile이** 사용되며 VLAN 20 및 DACL을 반환하고 SGT가 VLAN20인 보안 프로필 **VLAN20이 반환됩니다**.



스위치 및 ASA 컨피그레이션을 완료하여 SGT RADIUS 특성을 수락합니다.

ASA 및 3750X의 CTS 컨피그레이션

기본 CTS 설정을 구성해야 합니다. 3750X에서 어떤 서버 정책을 다운로드해야 하는지를 나타내야 합니다.

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

ASA에서는 해당 서버를 가리키는 CTS와 함께 AAA 서버만 필요합니다.

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

> **참고**: 3750X에서는 **group radius** 명령을 사용하여 ISE 서버를 명시적으로 **가리켜야** 합니다. 이는 3750X에서 자동 PAC 프로비저닝을 사용하기 때문입니다.

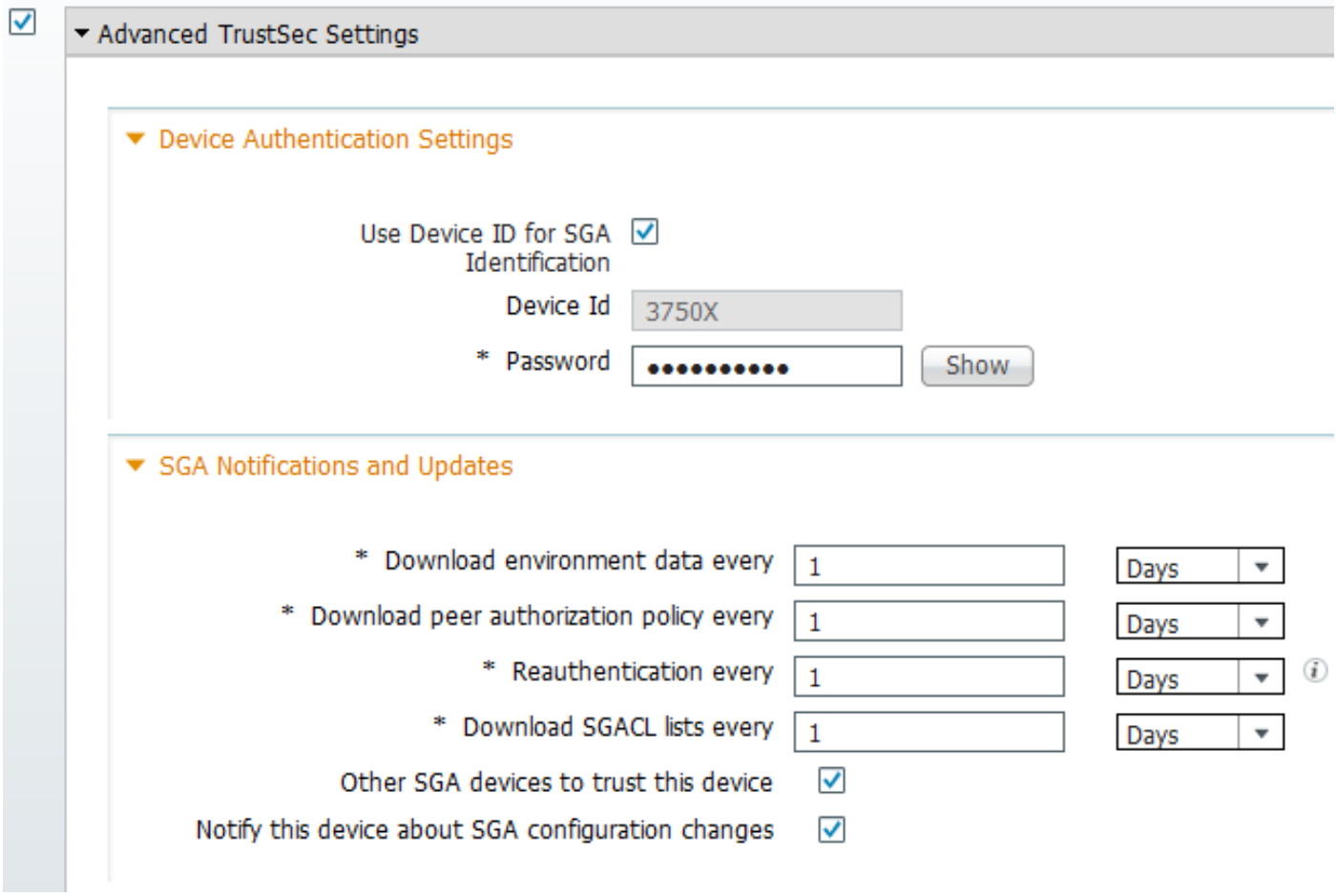
3750X(자동) 및 ASA(수동)의 PAC 프로비저닝

CTS 클라우드의 각 디바이스는 다른 디바이스에서 신뢰하기 위해 ISE(인증 서버)에 인증해야 합니다. 이를 위해 EAP-FAST(Extensible Authentication Protocol-Flexible Authentication via Secure Protocol) 방법(RFC 4851)을 사용합니다. 이 방법을 사용하려면 PAC를 대역 외로 제공해야 합니다. 이 프로세스는 phase0이라고도 **하며**, 어떤 RFC에도 정의되어 있지 않습니다. EAP-FAST용 PAC는 EAP-TLS(Extensible Authentication Protocol-Transport Layer Security)용 인증서와 유사한 역할을 합니다. PAC는 2단계에서 인증에 필요한 보안 터널(phase1)을 설정하기 위해 사용됩니다.

3750X에서 PAC 프로비저닝

3750X는 자동 PAC 프로비저닝을 지원합니다. 공유 비밀번호는 스위치 및 ISE에서 PAC를 다운로드하기 위해 사용됩니다. 해당 비밀번호와 ID는 ISE의 Administration(관리) > Network Resources(네트워크 리소스) **> Network Devices(네트워크 디바이스) 아래에서 구성해야 합니다**. 스위치를 선택하고 Advanced TrustSec **Settings(고급 TrustSec 설정)** 섹션을 확장하여 다음을 구성

합니다.



PAC에서 이러한 자격 증명을 사용하도록 하려면 다음 명령을 입력합니다.

```
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
```

ASA의 PAC 프로비저닝

ASA는 수동 PAC 프로비저닝만 지원합니다. 즉 ISE에서(네트워크 디바이스/ASA에서) 수동으로 생성해야 합니다.

그런 다음 파일을 설치해야 합니다(예: 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
```

ASA 및 3750X의 환경 업데이트

이 단계에서 두 디바이스 모두 PAC가 올바르게 설치되어 있고 자동으로 ISE 환경 데이터 다운로드가 시작됩니다. 이 데이터는 기본적으로 태그 번호와 이름입니다. ASA에서 환경 새로고침을 트리거하려면 다음 명령을 입력합니다.

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

ASA에서 이를 확인하려면(안타깝게도 특정 SGT 태그/이름을 볼 수 없지만 나중에 확인됨) 다음 명령을 입력합니다.

```
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)
```

3750X에서 확인하려면 다음 명령으로 환경 새로고침을 트리거합니다.

```
bsns-3750-5#cts refresh environment-data
```
결과를 확인하려면 다음 명령을 입력합니다.

```
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
```
이는 모든 태그와 해당 이름이 올바르게 다운로드되었음을 보여줍니다.

3750X에서 포트 인증 확인 및 적용

3750X에 환경 데이터가 있으면 SGT가 인증된 세션에 적용되었는지 확인해야 합니다.

MS Windows 7이 올바르게 인증되었는지 확인하려면 다음 명령을 입력합니다.

```
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:  C0A800010000001002B67334C
     Acct Session ID:  0x00000179
              Handle:  0x94000101
```

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

이 출력은 VLAN10이 모든 트래픽을 허용하는 SGT 0002 및 DACL과 함께 사용됨을 보여줍니다.

MS Windows XP가 올바르게 인증되었는지 확인하려면 다음 명령을 입력합니다.

```
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
```

출력에 VLAN 20이 모든 **트래픽**을 허용하는 SGT 0003 및 DACL과 함께 사용되는 것으로 표시됩니다

IP 주소는 **IP 디바이스 추적 기능**으로 탐지됩니다. DHCP 스누핑을 위해 DHCP 스위치를 **구성해야 합니다**. 그런 다음 스누핑 DHCP 응답 후 클라이언트의 IP 주소를 학습합니다. 이 예와 같이 정적으로 구성된 IP 주소의 경우 arp **스누핑 기능**이 사용되며, PC는 스위치가 IP 주소를 탐지할 수 있도록 모든 패킷을 전송해야 합니다.

디바이스 **추적**의 경우 포트에서 활성화하려면 숨겨진 명령이 필요할 수 있습니다.

```
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
```

3750X에서 정책 새로 고침

3750X(ASA와 다름)는 ISE에서 정책을 다운로드할 수 있습니다. 정책을 다운로드하고 시행하기 전에 다음 명령으로 활성화해야 합니다.

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

정책을 활성화하지 않으면 정책은 다운로드되지만 설치되지 않으며 시행에 사용되지 않습니다.

정책 새로 고침을 트리거하려면 다음 명령을 입력합니다.

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

정책이 ISE에서 다운로드되었는지 확인하려면 다음 명령을 입력합니다.

```
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
```

출력은 정책의 필요한 부분만 다운로드됨을 보여줍니다.

CTS 클라우드에서 패킷은 소스 호스트의 SGT를 포함하고 **대상 디바이스에서 시행됩니다**. 즉, 패킷이 소스에서 목적지 호스트에 직접 연결된 마지막 디바이스로 전달됩니다. 이 디바이스는 직접 연결된 호스트의 SGT를 알고, 소스 SGT가 있는 수신 패킷이 특정 대상 SGT에 대해 허용되거나 거부되어야 하는지 알기 때문에 시행 지점입니다.

이 결정은 ISE에서 다운로드한 정책을 기반으로 합니다.

이 시나리오에서는 모든 정책이 다운로드됩니다. 그러나 MS Windows XP 인증 세션(SGT=VLAN20)을 지우면 스위치에 연결된 SGT에서 더 이상 디바이스가 없기 때문에 스위치에서 VLAN20에 해당하는 정책(행)을 다운로드할 필요가 없습니다.

고급(트러블슈팅) 섹션에서는 3750X에서 패킷 레벨 검사와 함께 어떤 정책을 다운로드할지 결정하는 방법에 대해 설명합니다.

SXP Exchange(ASA를 리스너로, 3750X를 스피커로)

ASA는 SGT를 지원하지 않습니다. SGT가 포함된 모든 프레임은 ASA에서 삭제됩니다. 따라서 3750X는 ASA에 SGT 태그가 지정된 프레임을 전송할 수 없습니다. 대신 SXP가 사용됩니다. 이 프로토콜을 사용하면 ASA가 스위치로부터 IP 주소와 SGT 간의 매핑에 대한 정보를 받을 수 있습니다. 이 정보를 통해 ASA는 IP 주소를 SGT에 매핑하고 SGACL을 기반으로 결정을 내릴 수 있습니다

.

3750X를 스피커로 구성하려면 다음 명령을 입력합니다.

```
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
```

ASA를 리스너로 구성하려면 다음 명령을 입력합니다.

```
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
```

ASA에서 매핑을 수신했는지 확인하려면 다음 명령을 입력합니다.

```
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
```

이제 ASA가 소스 IP 주소 **192.168.1.200**의 수신 패킷을 수신하면 SGT**=2**에서 오는 것처럼 처리할 수 있습니다. 소스 IP 주소 **192.168.200.2**의 경우 SGT **=3**에서 온 것처럼 처리할 수 있습니다. 대상 IP 주소도 마찬가지입니다.

> **참고**: 3750X는 연결된 호스트의 IP 주소를 알아야 합니다. 이는 IP 디바이스 추적에 의해 수행됩니다. 엔드 호스트에 정적으로 구성된 IP 주소의 경우, 스위치는 인증 후 모든 패킷을 수신해야 합니다. 그러면 IP 주소를 찾기 위해 IP 디바이스 추적이 트리거되며, 이는 SXP 업데이트를 트리거합니다. SGT만 알 경우 SXP를 통해 전송되지 않습니다.

SGT ACL을 사용하는 ASA의 트래픽 필터링

다음은 ASA 컨피그레이션에 대한 검사입니다.

```
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
```

ACL이 생성되어 내부 인터페이스에 적용됩니다. SGT=3에서 SGT=2로의 모든 ICMP 트래픽(VLAN10)을 허용합니다.

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

참고: 태그 번호 또는 태그 이름을 사용할 수 있습니다.

소스 IP 주소가 192.168.2.200(SGT=3)인 MS Windows XP에서 IP 주소가 192.168.1.200(SGT=2)인 MS Windows 7로 ping하는 경우 **ASA는 연결**을 구축합니다.

```
%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)
```

텔넷으로 동일한 작업을 시도하면 트래픽이 차단됩니다.

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

ASA에는 더 많은 컨피그레이션 옵션이 있습니다. 소스와 대상 모두에 보안 태그와 IP 주소를 모두 사용할 수 있습니다. 이 규칙은 SGT **태그 = 3** 및 IP 주소 192.168.2.200에서 VLAN10이라는 SGT 태그 및 대상 호스트 주소 192.168.1.200으로 ICMP 에코 트래픽**을 허용합니다**.

```
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
```

객체 그룹에서도 이 작업을 수행할 수 있습니다.

```
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
```

ISE(RBACL)에서 다운로드한 정책을 사용하여 3750X에서 트래픽 필터링

스위치에서 로컬 정책을 정의할 수도 있습니다. 그러나 이 예에서는 ISE에서 다운로드한 정책을 표시합니다. ASA에 정의된 정책은 하나의 규칙에서 IP 주소와 SGT(및 Active Directory의 사용자 이름)를 모두 사용할 수 있습니다. 스위치에 정의된 정책(로컬 및 ISE에서 모두)은 SGT에 대해서만 허용합니다. 규칙에서 IP 주소를 사용해야 하는 경우 ASA에서 필터링하는 것이 좋습니다.

MS Windows XP와 MS Windows 7 간의 ICMP 트래픽을 테스트합니다. 이를 위해 ASA에서 MS Windows의 3750X로 기본 게이트웨이를 변경해야 합니다. 3750X에는 라우팅 인터페이스가 있으며 패킷을 라우팅할 수 있습니다.

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

정책이 ISE에서 이미 다운로드되었습니다. 이를 확인하려면 다음 명령을 입력합니다.

```
 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
```

VLAN10(MS Windows 7)에서 VLAN20(MS WindowsXP)으로의 트래픽은 ICMP-20 ACL에 적용되며, 이는 ISE에서 다운로드됩니다.

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

ACL을 확인하려면 다음 명령을 입력합니다.

```
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
```

두 호스트의 트래픽이 올바르게 태그되었는지 확인하기 위해 SGT 매핑을 확인하려면 다음 명령을 입력합니다.

```
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
```

MS Windows 7(SGT=2)에서 MS Windows XP(SGT=3)로의 ICMP는 ACL ICMP-20에서 작동합니다. 이는 2에서 3(허용된 패킷 15개)까지의 트래픽에 대한 카운터를 확인하여 확인합니다.

```
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
```

Telnet 카운터를 사용하려고 하면 거부된 패킷이 증가합니다(ICMP-20 ACL에서는 허용되지 않음).

```
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
```

참고: 출력에 표시된 별(*) 문자는 태그가 지정되지 않은 모든 트래픽과 관련이 있습니다(이 열과 행은 ISE의 Matrix에서 **unknown**으로 불리며 태그 번호 **0**을 **사용합니다**).

ISE에 정의된 log 키워드와 함께 ACL 항목이 있는 경우 해당 패킷 세부사항 및 수행한 작업이 log 키워드와 함께 ACL에 기록됩니다.

다음을 확인합니다.

확인 절차에 대해서는 개별 컨피그레이션 섹션을 참조하십시오.

문제 해결

PAC 프로비저닝

자동 PAC 프로비저닝을 사용할 때 문제가 나타날 수 있습니다. RADIUS 서버에 대해 **pac** 키워드를 사용해야 합니다. 3750X의 자동 PAC 프로비저닝은 Microsoft의 EAP-MSCHAPv2(Challenge Handshake Authentication Protocol) 인증을 사용하는 내부 방법과 함께 확장 가능 인증 프로토콜과 함께 EAP-FAST 방법을 사용합니다. 디버깅할 때 보안 터널을 구축하기 위해 사용되는 EAP-FAST 협상의 일부인 여러 RADIUS 메시지가 표시되며, 이는 인증에 구성된 ID 및 비밀번호와 함께 EAP-MSCHAPv2를 사용합니다.

첫 번째 RADIUS 요청은 ISE에 PAC 요청임을 알리기 위해 AAA **service-type=**cts-pac-provisioning을 사용합니다.

```
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.
```

PAC를 이미 받았으며 추가 인증 프로세스를 따르지 않았으므로 출력 끝에 RADIUS 거부가 필요합니다.

ISE와의 다른 모든 통신에는 PAC가 필요합니다. 그러나 스위치가 없는 경우 환경 또는 정책 새로 고침은 구성 시 계속 시도합니다. 그런 다음 RADIUS 요청에서 cts-opaqueue(PAC)를 연결하지 않으므로 오류가 발생합니다.

PAC 키가 잘못된 경우 이 오류 메시지가 ISE에 표시됩니다.

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

PAC 키가 잘못된 경우 스위치에서 디버그(debug cts provisioning + debug radius)의 이 출력도 표시됩니다.

```
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
```

최신 RADIUS 서버 규칙을 사용하는 경우 다음과 같이 표시됩니다.

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

> **참고**: Device Authentication Settings(디바이스 인증 설정)에서 사용한 것과 동일한 비밀번호를 ISE에서 **사용해야 합니다**.

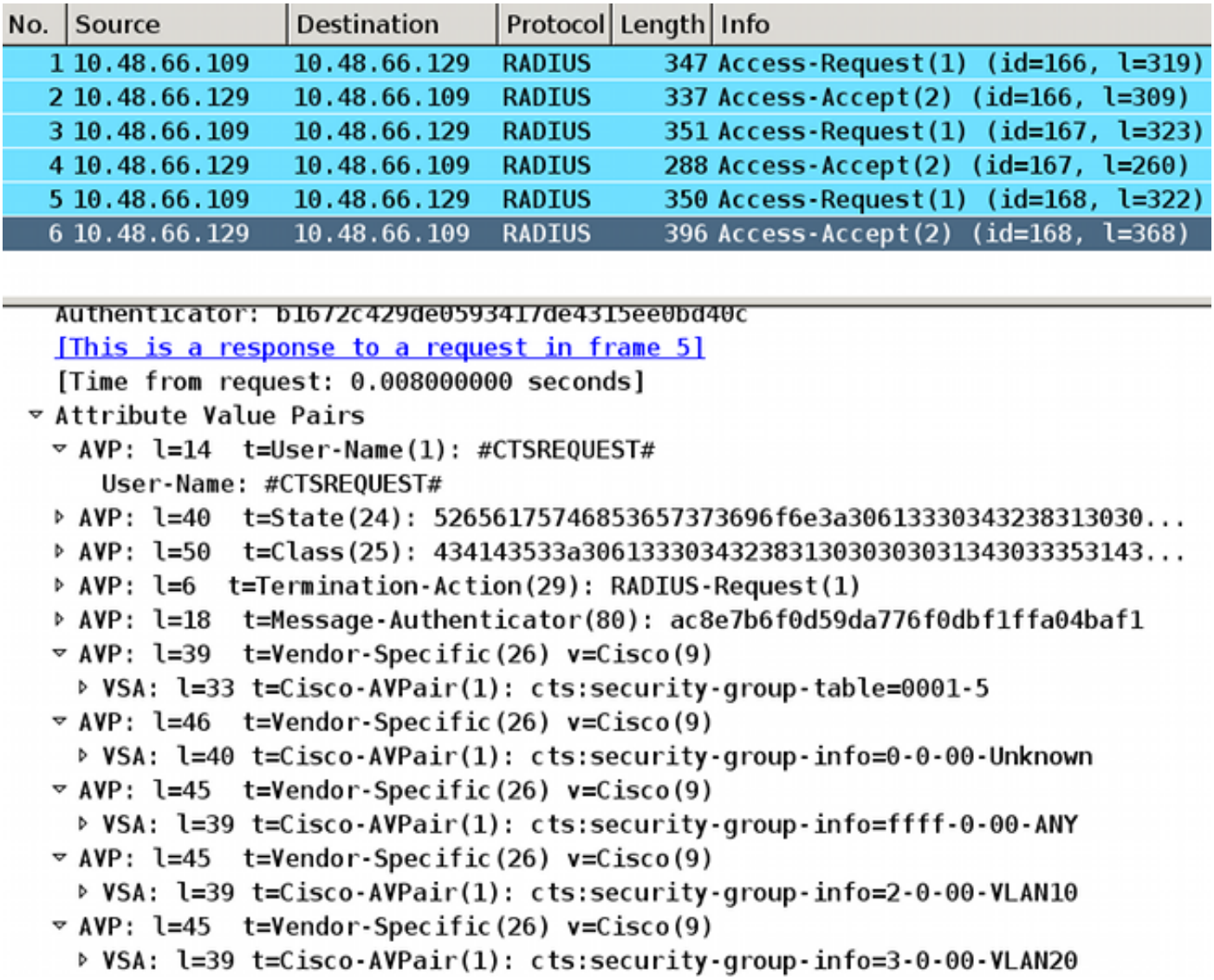
PAC 프로비저닝이 성공하면 ISE에 다음과 같이 표시됩니다.

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)

환경 업데이트

환경 새로 고침은 ISE에서 기본 데이터를 얻기 위해 사용되며, 여기에는 SGT 번호 및 이름이 포함됩니다. 패킷 레벨은 특성이 있는 세 가지 RADIUS 요청 및 응답만 표시합니다.

첫 번째 요청의 경우 스위치에서 CTSServerlist **이름을** 수신합니다. 두 번째 SGT는 해당 목록에 대한 세부사항을 수신하고, 마지막 SGT는 태그와 이름이 있는 모든 SGT를 수신합니다.



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)

여기서 기본 **SGT 0**, **ffff** 및 2개의 사용자 정의 태그가 표시됩니다. SGT 태그 2의 이름은 VLAN**10**이고 SGT 태그 3의 이름은 **VLAN20입니다**.

참고: 모든 RADIUS 요청에는 **PAC 프로비저닝**의 결과로 cts-pac-opaque가 포함됩니다.

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)

```
▷ Raw packet data
▷ Internet Protocol Version 4, Src: 10.48.66.109 (10.48.66.109), Dst: 10.48.66.129
▷ User Datagram Protocol, Src Port: sightline (1645), Dst Port: sightline (1645)
▽ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0xa6 (166)
    Length: 319
    Authenticator: 60a2c0dbab563d6a0f4b44910f646d9e
    [The response to this request is in frame 2]
  ▽ Attribute Value Pairs
    ▽ AVP: l=203  t=Vendor-Specific(26) v=Cisco(9)
      ▷ VSA: l=197 t=Cisco-AVPair(1): cts-pac-opaque=\000\002\000\260\000\003\000\0
    ▽ AVP: l=14  t=User-Name(1): #CTSREQUEST#
        User-Name: #CTSREQUEST#
    ▽ AVP: l=34  t=Vendor-Specific(26) v=Cisco(9)
      ▷ VSA: l=28 t=Cisco-AVPair(1): cts-environment-data=3750X
    ▷ AVP: l=18  t=User-Password(2): Encrypted
    ▷ AVP: l=6  t=Service-Type(6): Dialout-Framed-User(5)
    ▷ AVP: l=6  t=NAS-IP-Address(4): 10.48.66.109
    ▷ AVP: l=18  t=Message-Authenticator(80): a16f5aea9af1cb47abb0d06d229eeec7
```

3750X에서는 세 가지 RADIUS 응답 모두에 대한 디버그와 해당 목록, 목록 세부사항, 특정 SGT-inside 목록을 확인해야 합니다.

```
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)
```

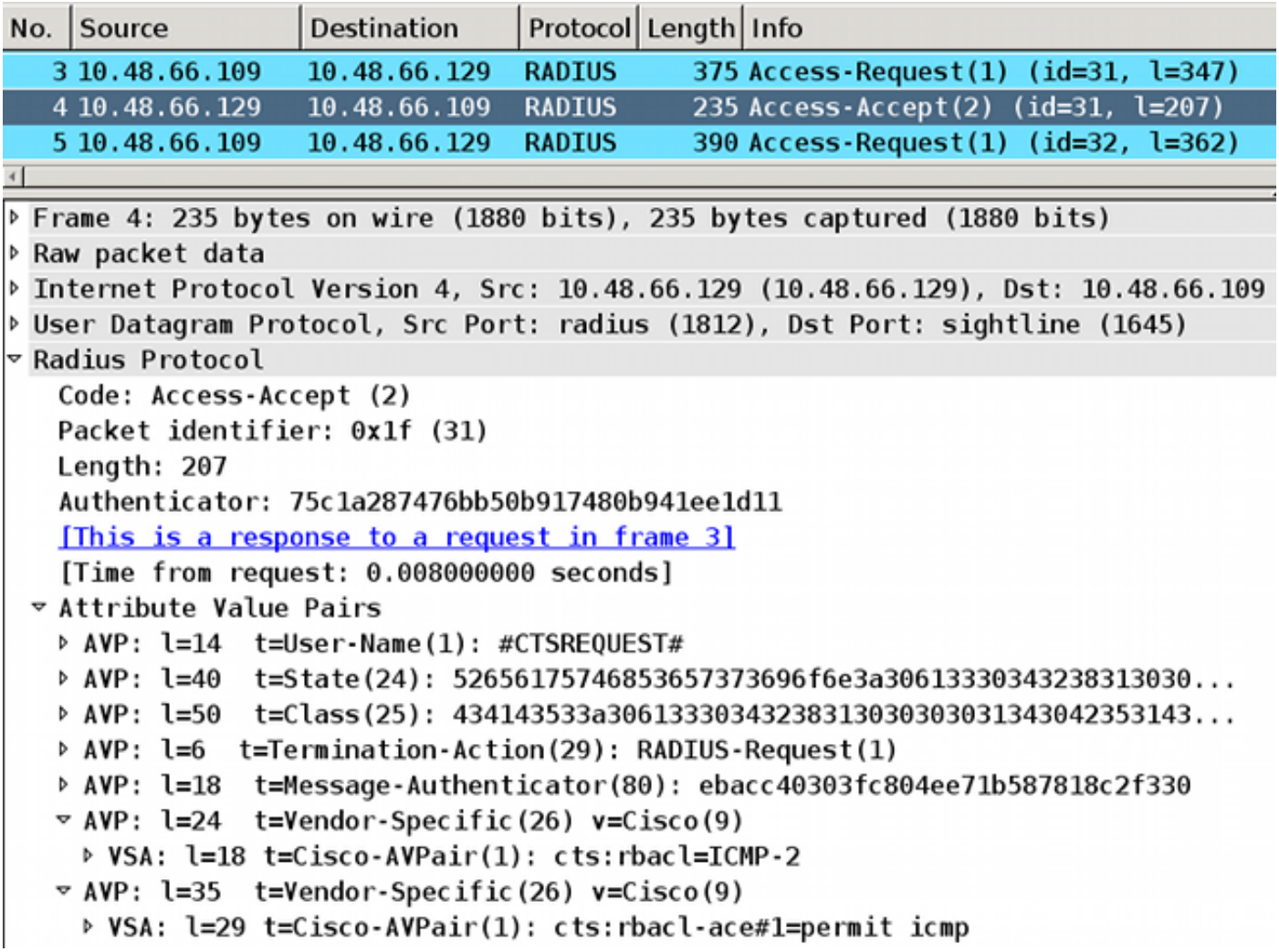
```
*Mar  1 10:05:18.099:     cts_env_data ASSESSING: during state env_data_assessing,
got event 3(env_data_incomplete)
*Mar  1 10:05:18.099: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_waiting_rsp
*Mar  1 10:05:18.099: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.099: 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
```

정책 새로 고침

정책 새로 고침은 스위치에서만 지원됩니다. 이는 환경 업그레이드와 비슷합니다. 이는 단순히 RADIUS 요청 및 수락입니다.

스위치에서 기본 목록 내의 모든 ACL을 요청합니다. 그런 다음 최신 상태가 아니거나 존재하지 않는 각 ACL에 대해 세부사항을 얻기 위해 다른 요청을 보냅니다.

다음은 ICMP-20 ACL을 요청할 때의 응답 예입니다.



해당 ACL을 적용하려면 **cts 역할 기반** 시행을 구성해야 합니다.

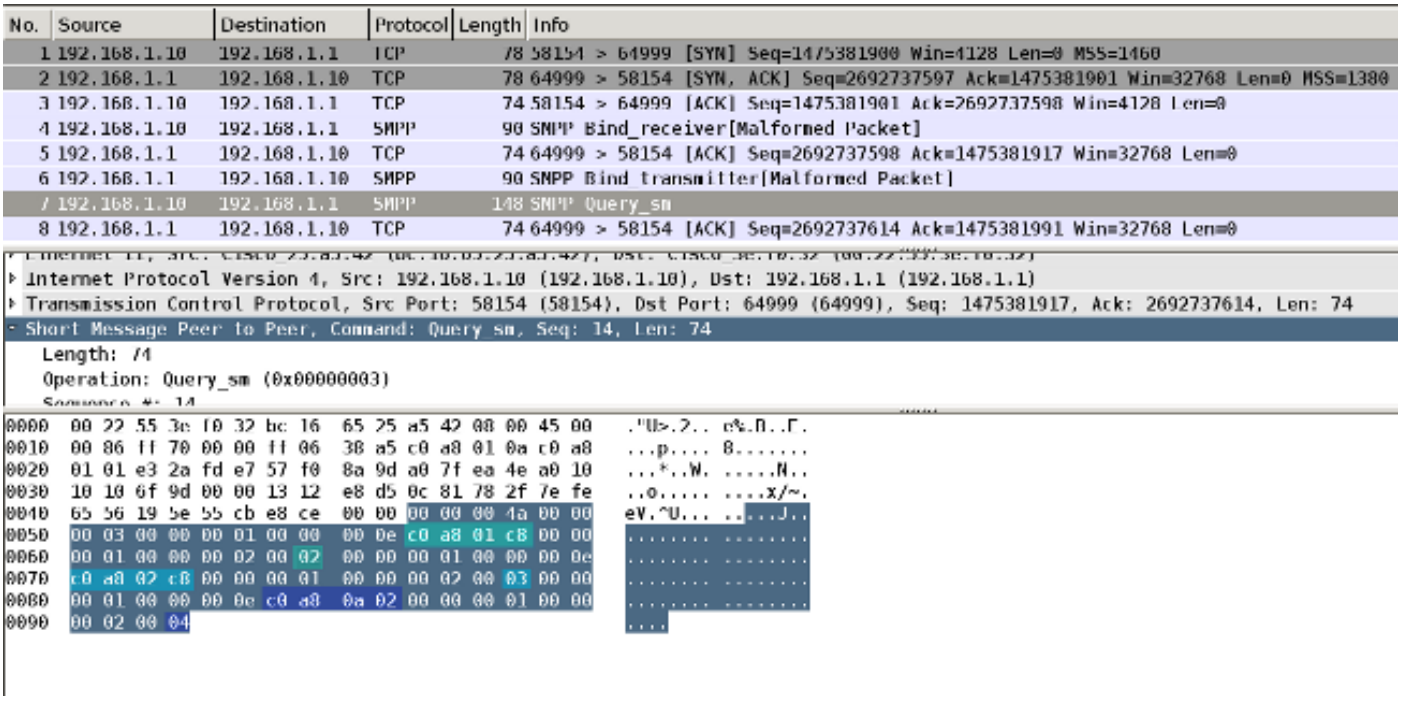
디버깅은 변경 사항이 있는지 여부를 나타냅니다(세대 ID 기준). 이 경우 필요한 경우 이전 정책을 제거하고 새 정책을 설치할 수 있습니다. 여기에는 ASIC 프로그래밍(하드웨어 지원)이 포함됩니다.

```
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

SXP 업데이트는 디바이스의 IP 주소를 찾는 IP 디바이스 추적 코드에 의해 트리거됩니다. 그런 다음 업데이트를 전송하기 위해 SMPP(Short Message Peer-to-Peer) 프로토콜을 사용합니다. BGP(Border Gateway Protocol)와 동일한 인증에 **TCP 옵션 19**를 사용합니다. SMPP 페이로드는 암호화되지 않습니다. Wireshark는 SMPP 페이로드에 적합한 디코더를 갖추고 있지 않지만, 그 안에서 데이터를 쉽게 찾을 수 있습니다.



- 첫 번째 **c0 a8 01 c8**은 **192.168.1.200**이며 **태그 2**가 **있습니다**.
- 두 번째 이름인 **c0 a8 02 c8**은 **192.168.2.200이며 태그 3**을 **갖습니다**.
- 세 번째 **c0 a8 0a 02**는 **192.168.10.2**이며 **태그 4**(이 하나는 **SGT=4**를 테스트하기 위해 사용됨)가 있습니다.

다음은 IP 디바이스 추적에서 MS Windows 7의 IP 주소를 찾은 후의 3750X에 대한 몇 가지 디버깅 입니다.

```
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
```

ASA에 해당하는 디버깅은 다음과 같습니다.

```
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.
```

ASA에서 더 많은 디버그를 보려면 디버깅 세부 정보 수준을 활성화할 수 있습니다.

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

ASA의 SGACL

ASA가 SXP에서 수신한 SGT 매핑을 올바르게 설치한 후에는 보안 그룹 ACL이 제대로 작동해야 합니다. 매핑에 문제가 발생하면 다음을 입력합니다.

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

보안 그룹의 ACL은 IP 주소 또는 사용자 ID와 정확히 동일하게 작동합니다. 로그에 문제가 표시되고 적중된 ACL의 정확한 항목이 표시됩니다.

MS Windows XP에서 MS Windows 7로의 ping은 패킷 추적기가 올바르게 작동함을 보여줍니다.

```
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>
```

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.