TrustSec 인식 서비스를 위한 ISE와 WSA 통합 구성

목차

소개

이 문서에서는 WSA(Web Security Appliance)를 ISE(Identity Services Engine)와 통합하는 방법에 대해 설명합니다.ISE 버전 1.3은 pxGrid라는 새 API를 지원합니다.이 현대적이고 유연한 프로토콜은 다른 보안 솔루션과 쉽게 통합할 수 있는 인증, 암호화 및 권한(그룹)을 지원합니다.

WSA 버전 8.7은 pxGrid 프로토콜을 지원하며 ISE에서 컨텍스트 ID 정보를 검색할 수 있습니다.따라서 WSA에서는 ISE에서 검색된 TrustSec SGT(Security Group Tag) 그룹을 기반으로 정책을 작성할 수 있습니다.

사전 요구 사항

요구 사항

Cisco에서는 Cisco ISE 컨피그레이션 및 이러한 주제에 대한 기본 지식을 보유하고 있는 것이 좋습니다.

- ISE 구축 및 권한 부여 구성
- TrustSec 및 VPN 액세스를 위한 ASA(Adaptive Security Appliance) CLI 컨피그레이션
- WSA 컨피그레이션
- TrustSec 구축에 대한 기본적인 이해

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft Windows 7
- Cisco ISE 소프트웨어 버전 1.3 이상
- Cisco AnyConnect Mobile Security 버전 3.1 이상
- Cisco ASA 버전 9.3.1 이상
- Cisco WSA 버전 8.7 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

> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

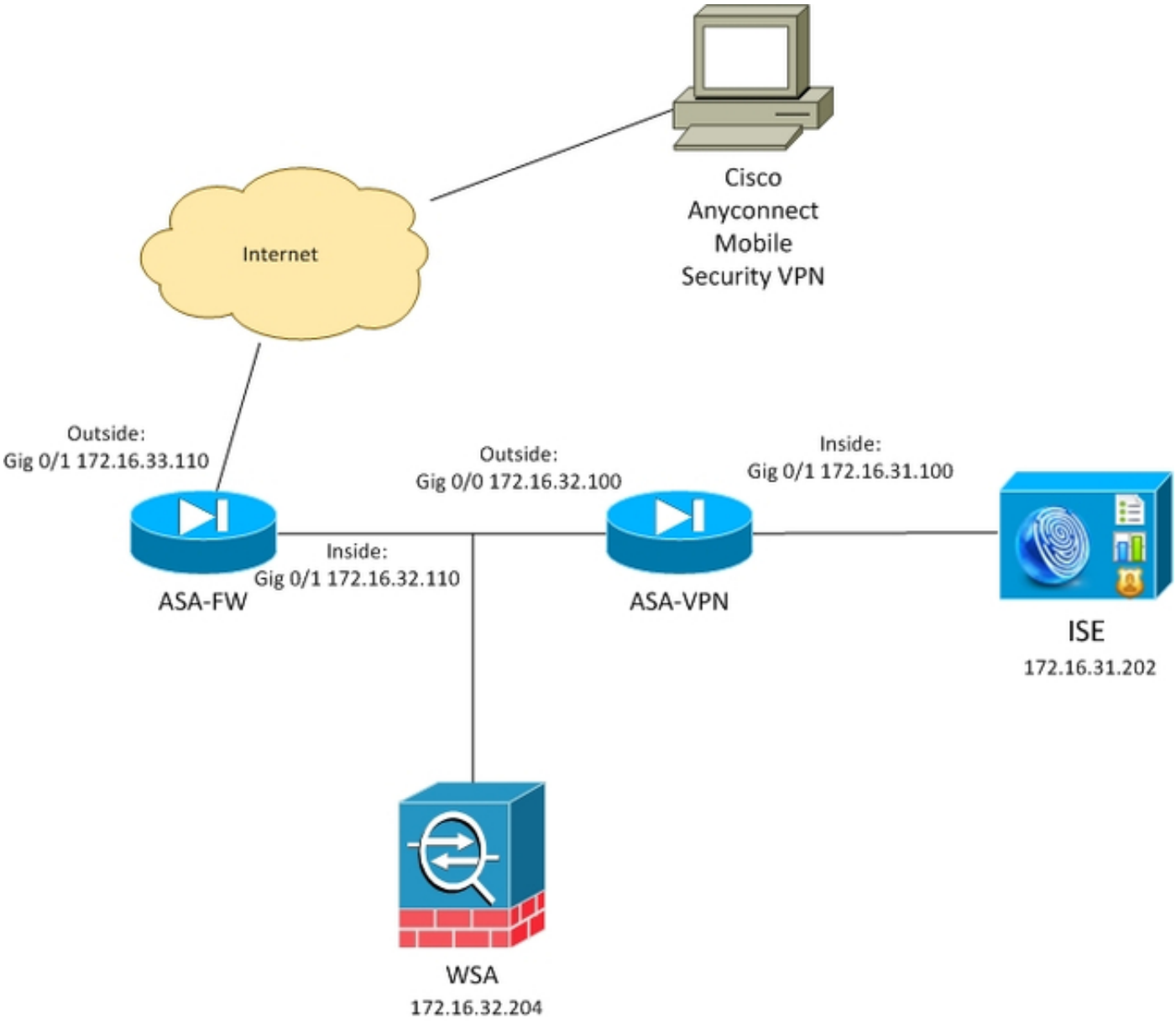
네트워크 다이어그램 및 트래픽 흐름

TrustSec SGT 태그는 기업 네트워크에 액세스하는 모든 유형의 사용자에 대해 인증 서버로 사용되는 ISE에 의해 할당됩니다.여기에는 802.1x 또는 ISE 게스트 포털을 통해 인증하는 유무선 사용자가 포함됩니다.또한 인증에 ISE를 사용하는 원격 VPN 사용자입니다.

WSA의 경우 사용자가 네트워크에 액세스하는 방법은 중요하지 않습니다.

이 예에서는 ASA-VPN에서 세션을 종료하는 원격 VPN 사용자를 보여줍니다.해당 사용자에게 특정 SGT 태그가 할당되었습니다.인터넷에 대한 모든 HTTP 트래픽은 ASA-FW(방화벽)에 의해 차단되

고 검사를 위해 WSA로 리디렉션됩니다.WSA는 SGT 태그를 기반으로 사용자를 분류하고 이를 기반으로 액세스 또는 암호 해독 정책을 작성할 수 있는 ID 프로필을 사용합니다.



자세한 플로우는 다음과 같습니다.

1. AnyConnect VPN 사용자는 ASA-VPN에서 SSL(Secure Sockets Layer) 세션을 종료합니다.ASA-VPN은 TrustSec에 대해 구성되며 VPN 사용자 인증에 ISE를 사용합니다.인증된 사용자에게 SGT 태그 값 = 2(이름 = IT)가 할당됩니다. 사용자는 172.16.32.0/24 네트워크(이 예에서는 172.16.32.50)에서 IP 주소를 수신합니다.
2. 사용자는 인터넷의 웹 페이지에 액세스하려고 시도합니다.ASA-FW는 WCCP(Web Cache Communication Protocol)에 대해 구성되어 WSA로 트래픽을 리디렉션합니다.
3. WSA는 ISE 통합을 위해 구성됩니다.pxGrid를 사용하여 ISE에서 정보를 다운로드합니다.사용자 IP 주소 172.16.32.50에 SGT 태그 2가 할당되었습니다.
4. WSA는 사용자의 HTTP 요청을 처리하고 액세스 정책 PolicyForIT에 액세스합니다.이 정책은 스포츠 사이트로의 트래픽을 차단하도록 구성됩니다.다른 모든 사용자(SGT 2에 속하지 않음)는 기본 액세스 정책에 도달하고 스포츠 사이트에 대한 전체 액세스 권한을 가집니다.

ASA-VPN

TrustSec에 대해 구성된 VPN 게이트웨이입니다.자세한 구성은 이 문서의 범위를 벗어납니다.다음 예를 참조하십시오.

- ASA 및 Catalyst 3750X Series Switch TrustSec 컨피그레이션 예 및 문제 해결 가이드
- ASA 버전 9.2 VPN SGT 분류 및 시행 컨피그레이션 예

ASA-FW

ASA 방화벽은 WSA로의 WCCP 리디렉션을 담당합니다.이 장치는 TrustSec을 인식하지 못합니다.

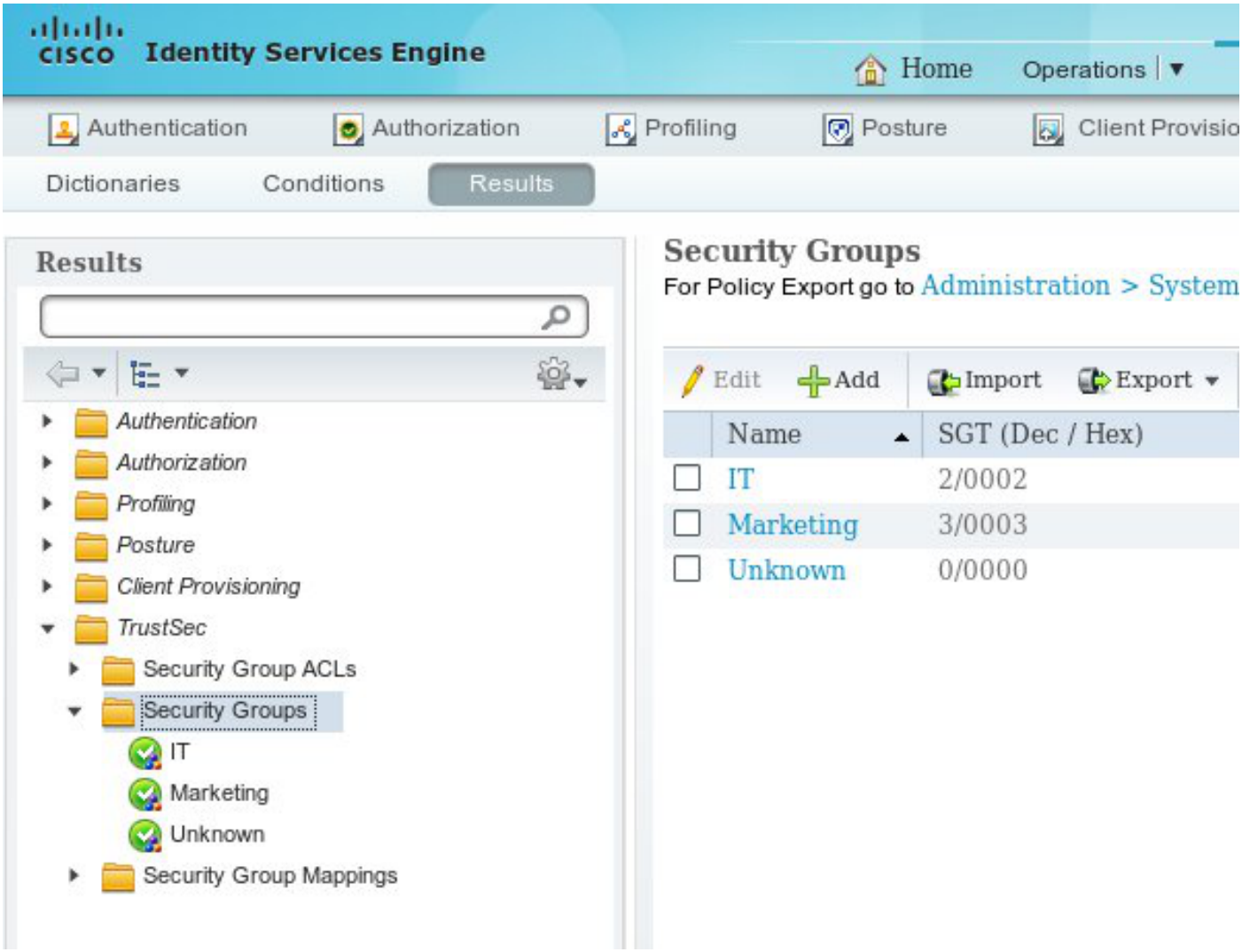
```
interface GigabitEthernet0/0
 nameif outside
 security-level 100
 ip address 172.16.33.110 255.255.255.0

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.110 255.255.255.0

access-list wccp-routers extended permit ip host 172.16.32.204 any
access-list wccp-redirect extended deny tcp any host 172.16.32.204
access-list wccp-redirect extended permit tcp any any eq www
access-list wccp-redirect extended permit tcp any any eq https

wccp 90 redirect-list wccp-redirect group-list wccp-routers
wccp interface inside 90 redirect in
```

ISE

ISE는 TrustSec 구축의 중앙 지점입니다.네트워크에 액세스하고 인증하는 모든 사용자에게 SGT 태그를 할당합니다.기본 구성에 필요한 단계는 이 섹션에 나와 있습니다.

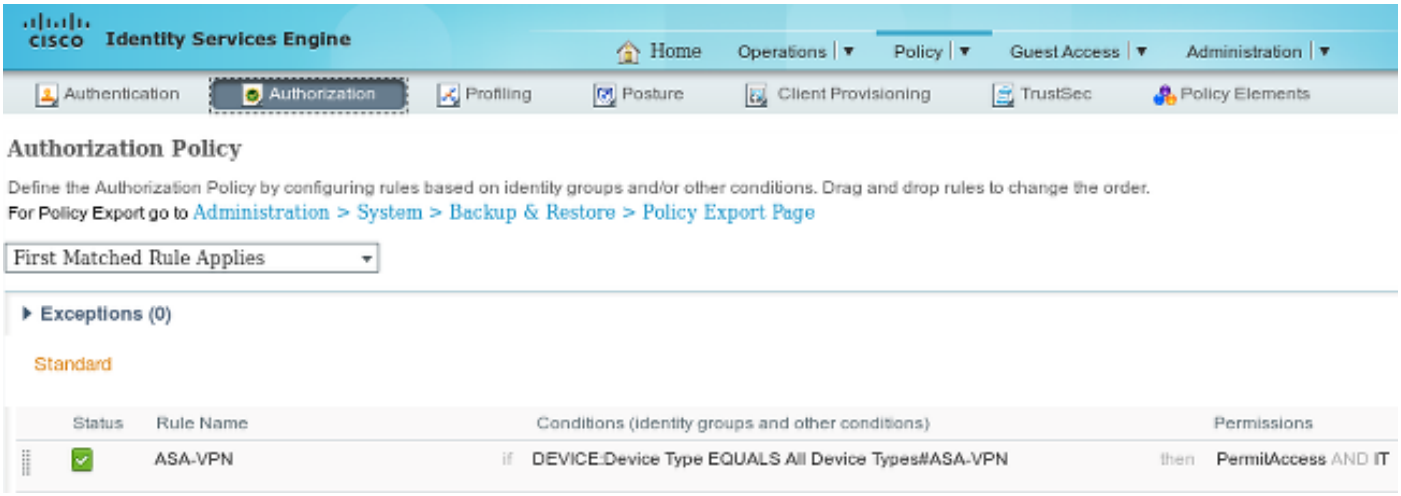
1단계. IT 및 기타 그룹용 SGT

Policy(**정책) > Results(결과) > Security Group Access(보안 그룹 액세스) > Security Groups(보안 그룹**)를 선택하고 SGT를 생성합니다.



2단계. SGT = 2(IT)를 할당하는 VPN 액세스에 대한 권한 부여 규칙

Policy(**정책) > Authorization(권한 부여**)을 선택하고 원격 VPN 액세스를 위한 규칙을 생성합니다 .ASA-VPN을 통해 설정된 모든 VPN 연결은 전체 액세스(PermitAccess)를 얻고 SGT 태그 2(IT)를 할당합니다.



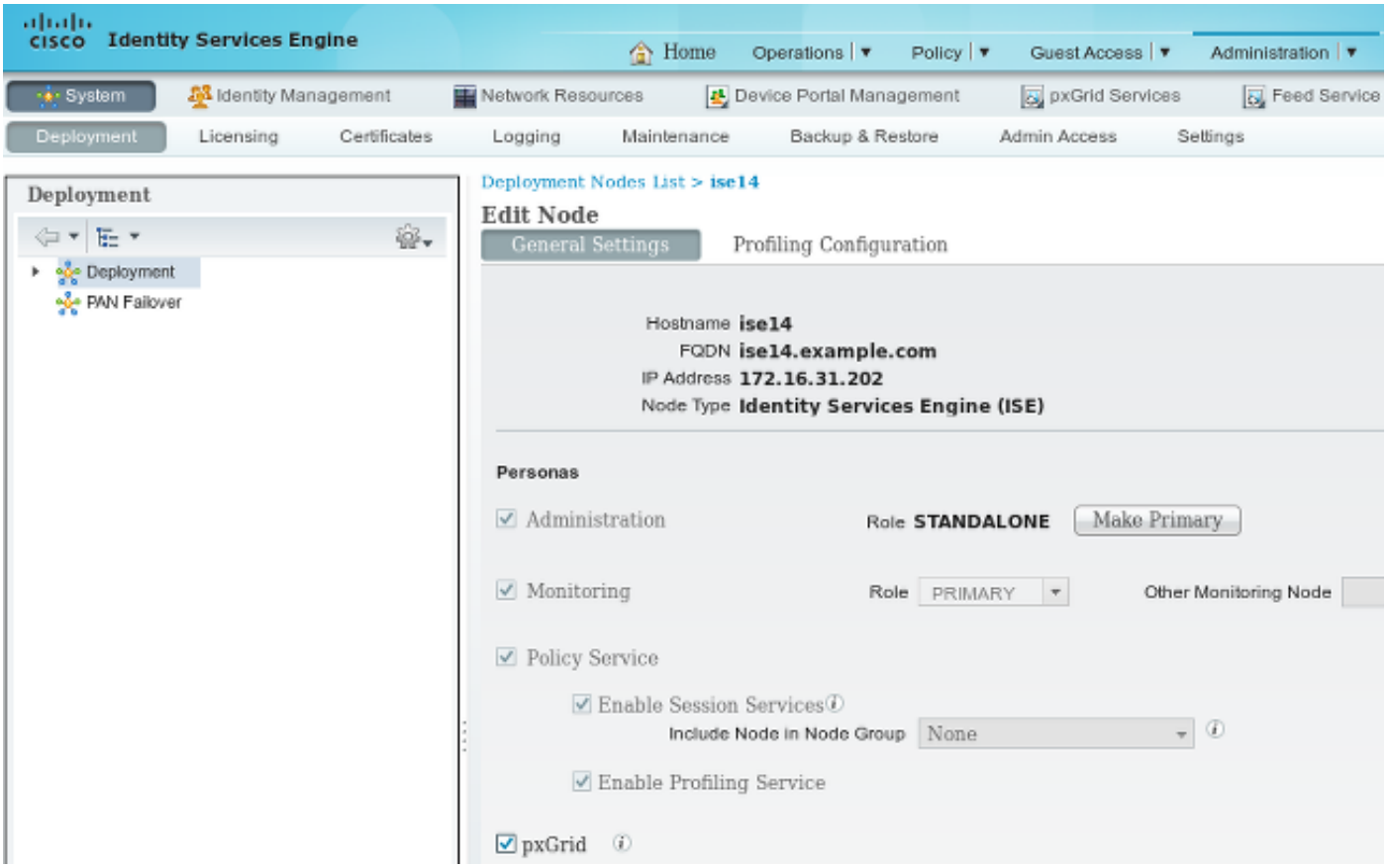
3단계. 네트워크 디바이스 추가 및 ASA-VPN용 PAC 파일 생성

ASA-VPN을 TrustSec 도메인에 추가하려면 프록시 PAC(Auto Config) 파일을 수동으로 생성해야 합니다.해당 파일은 ASA에서 가져옵니다.

이는 Administration(관리) > **Network Devices(네트워크 디바이스)**에서 구성할 수 있습니다.ASA를 추가한 후 아래로 스크롤하여 TrustSec 설정으로 이동하여 PAC 파일을 생성합니다.에 대한 세부 정보는 별도의 참조 문서에 설명되어 있습니다.

4단계. pxGrid 역할 활성화

pxGrid 역할을 활성화하려면 Administration(관리) > Deployment(구축)를 선택합니다.



5단계. 관리를 위한 인증서 및 pxGrid 역할을 생성합니다.

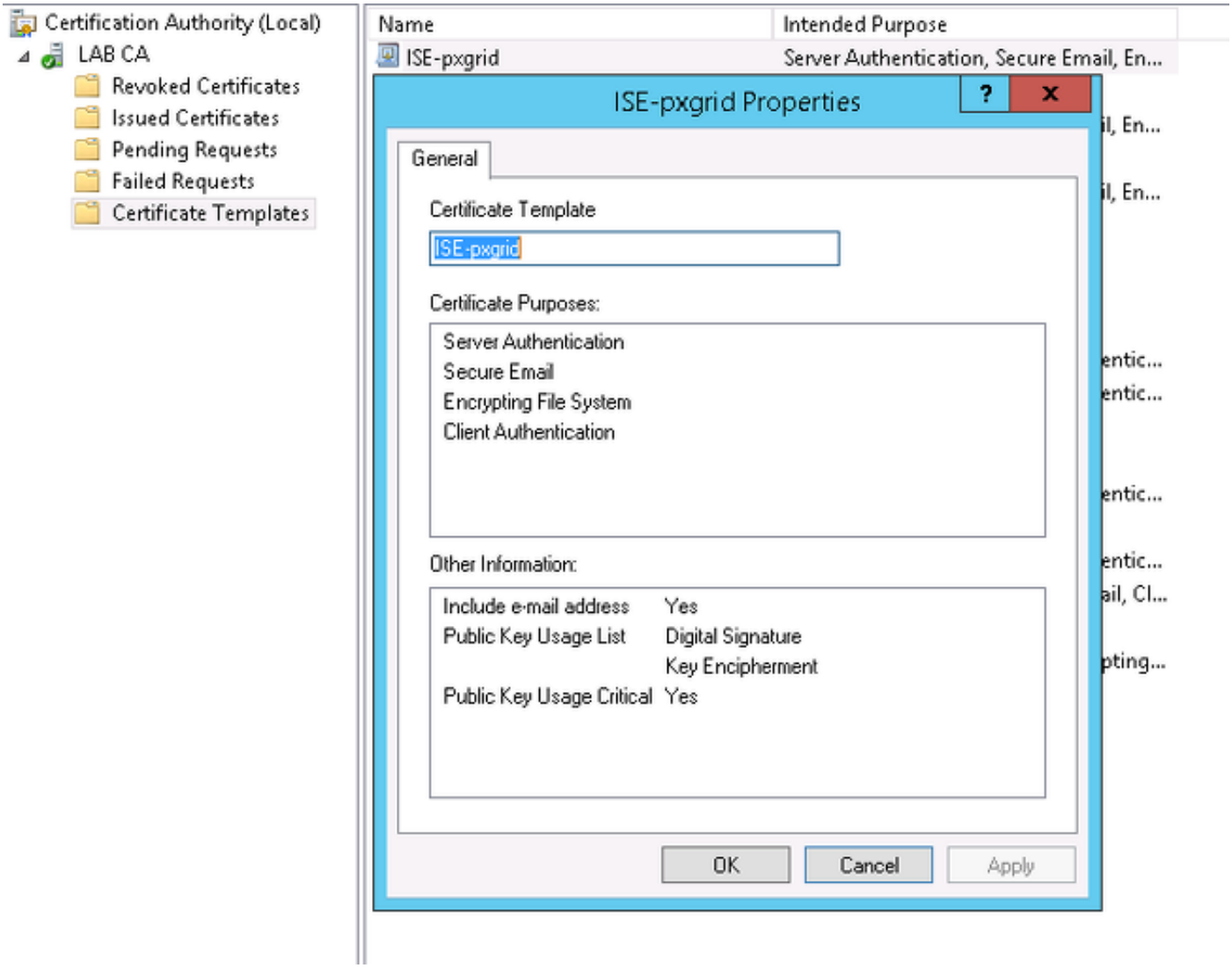
pxGrid 프로토콜은 클라이언트와 서버 모두에 인증서 인증을 사용합니다.ISE와 WSA 모두에 대해 올바른 인증서를 구성하는 것이 매우 중요합니다.두 인증서 모두 제목에 FQDN(Fully Qualified Domain Name)을, 클라이언트 인증 및 서버 인증을 위한 x509 확장을 포함해야 합니다.또한 ISE와 WSA 모두에 대해 올바른 DNS A 레코드가 생성되어 해당 FQDN과 일치하는지 확인합니다.

두 인증서가 다른 CA(Certificate Authority)에 의해 서명된 경우 해당 CA를 신뢰할 수 있는 저장소에 포함하는 것이 중요합니다.

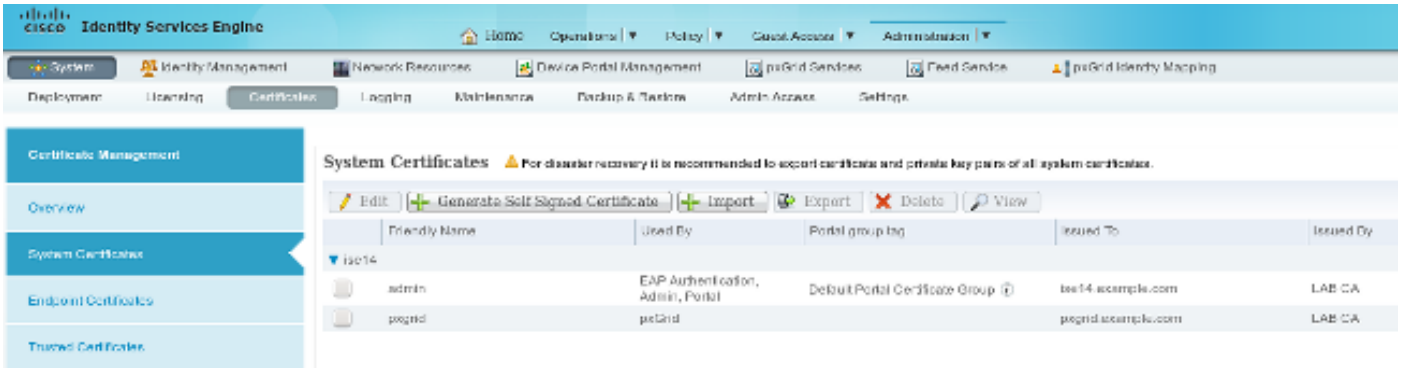
인증서를 구성하려면 Administration(관리) > **Certificates(인증서)를** 선택합니다.

ISE는 각 역할에 대해 CSR(Certificate Signing Request)을 생성할 수 있습니다.pxGrid 역할의 경우 외부 CA로 CSR을 내보내고 서명합니다.

이 예에서는 Microsoft CA가 이 템플릿과 함께 사용되었습니다.



최종 결과는 다음과 같습니다.

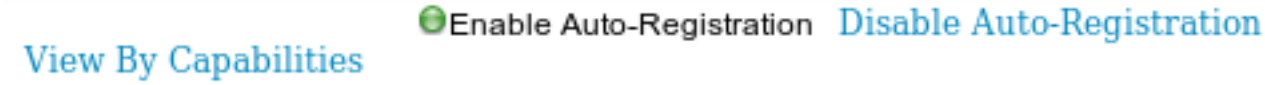


ise14.example.com 및 pxgrid.example.com에 대해 172.16.31.202을 가리키는 DNS A 레코드를 생성하는 것을 잊지 마십시오.

6단계. pxGrid 자동 등록

기본적으로 ISE는 pxGrid 가입자를 자동으로 등록하지 않습니다.관리자가 수동으로 승인해야 합니다.WSA 통합을 위해 해당 설정을 변경해야 합니다.

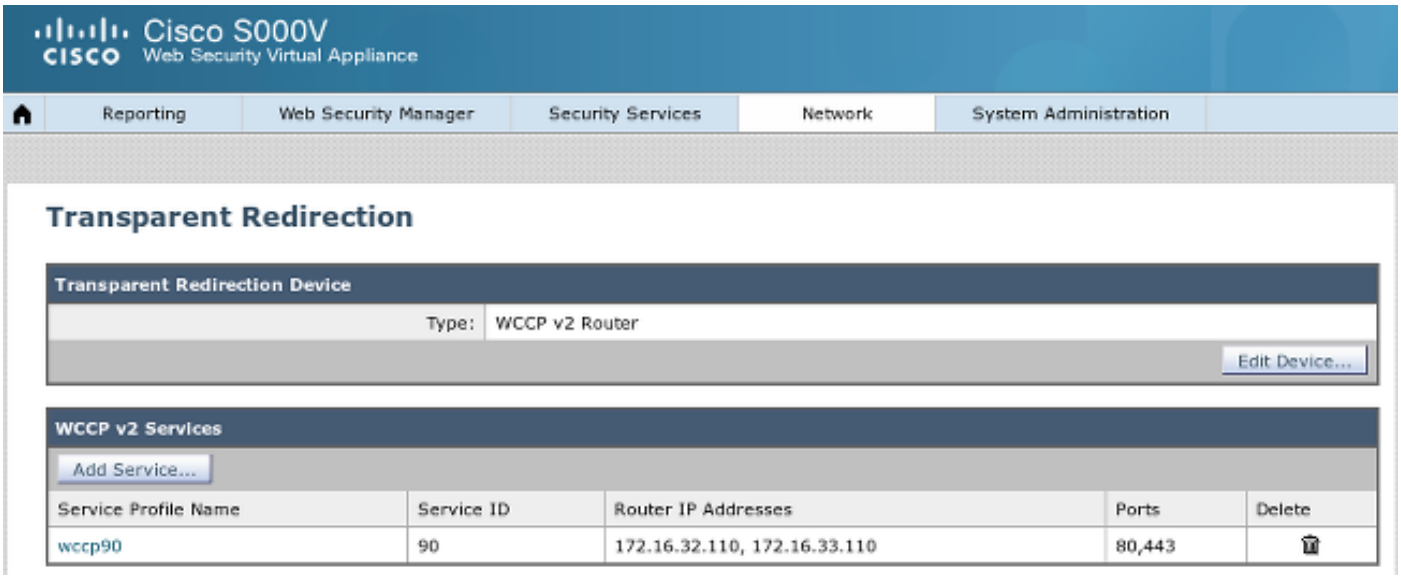
Administration(**관리) > pxGrid Services(pxGrid 서비스**)를 선택하고 Enable **Auto-Registration(자동 등록 활성화)을 설정합니다**.



WSA

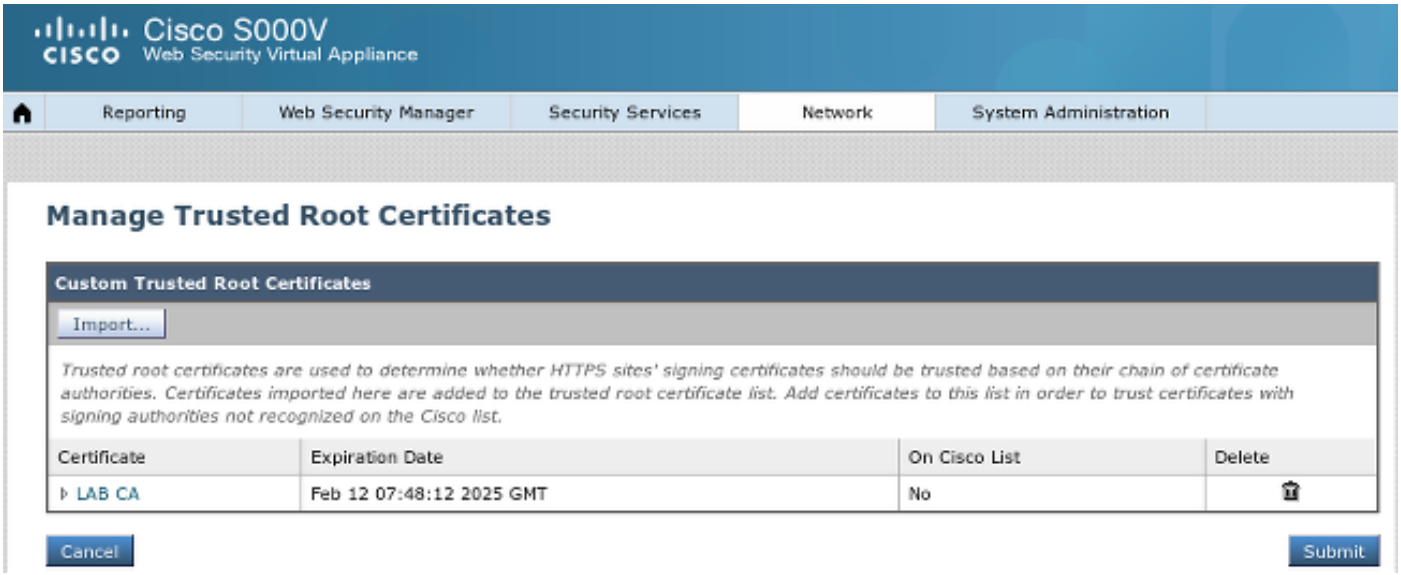
1단계. 투명 모드 및 리디렉션

이 예에서 WSA는 관리 인터페이스, 투명 모드 및 ASA로부터의 리디렉션만 사용하여 구성됩니다.



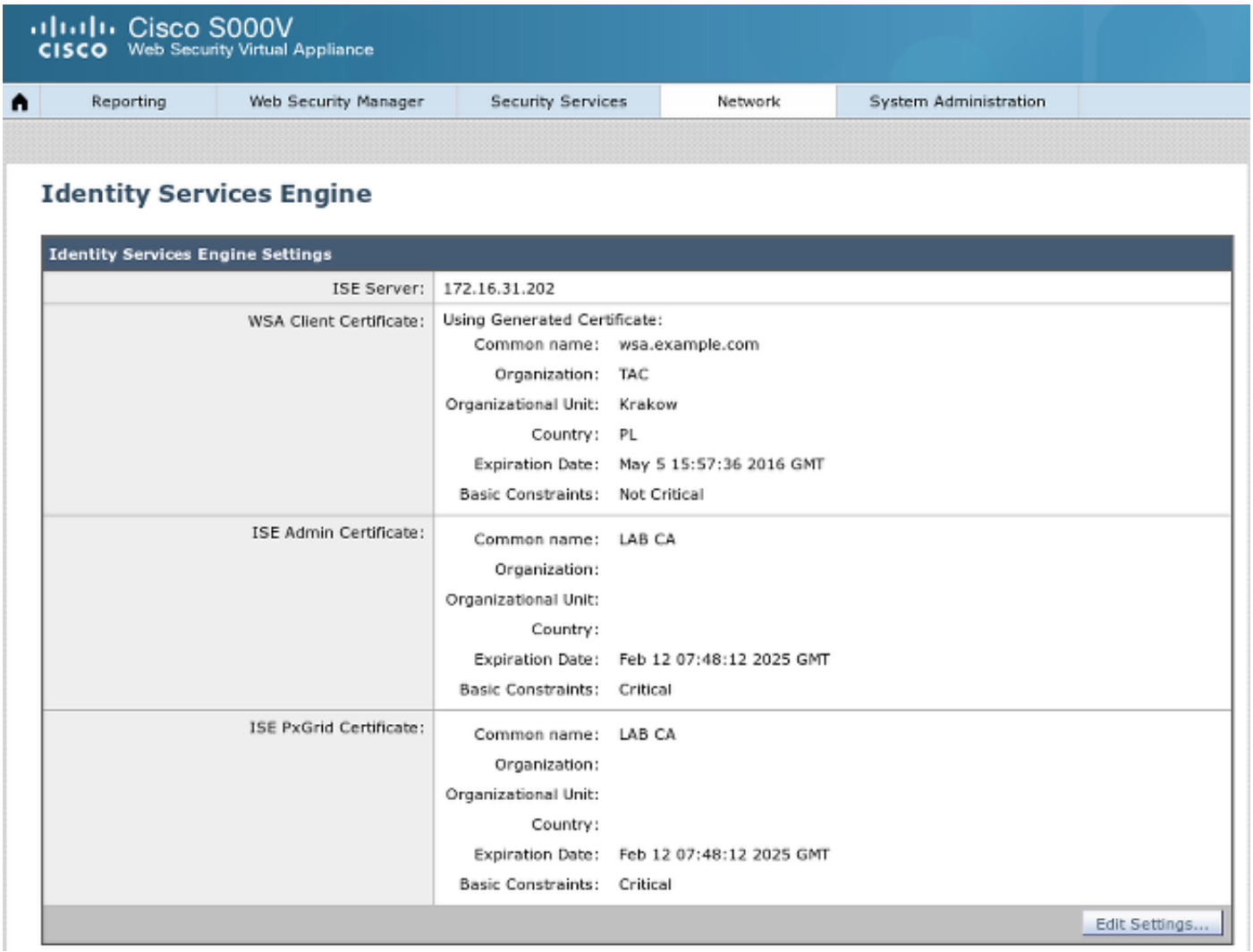
2단계. 인증서 생성

WSA는 CA가 모든 인증서에 서명하도록 신뢰해야 합니다.CA 인증서를 추가하려면 Network(**네트워크**) > Certificate Management(**인증서 관리**)를 선택합니다.



pxGrid에 인증하기 위해 WSA에서 사용할 인증서를 생성해야 합니다.CSR을 생성하고 올바른 CA 템플릿(ISE-pxgrid)으로 서명하고 다시 가져오려면 **Network > Identity Services Engine > WSA Client 인증서**를 선택합니다.

또한 "ISE Admin Certificate(ISE 관리 인증서)" 및 "ISE pxGrid Certificate(ISE pxGrid 인증서)"에서 CA 인증서를 가져옵니다(ISE에서 제공하는 pxGrid 인증서를 신뢰하기 위해).

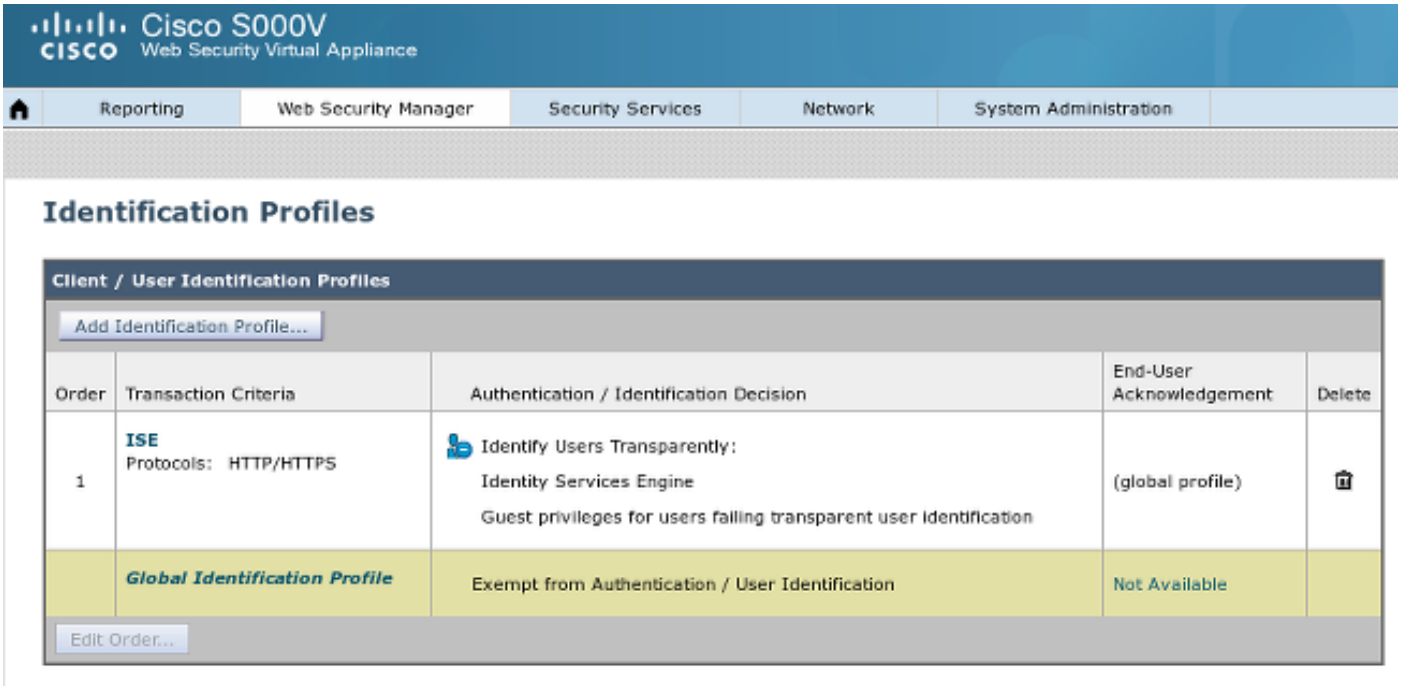


3단계. ISE 연결 테스트

ISE에 대한 연결을 테스트하려면 Network(네트워크) > Identity Services Engine을 선택합니다.

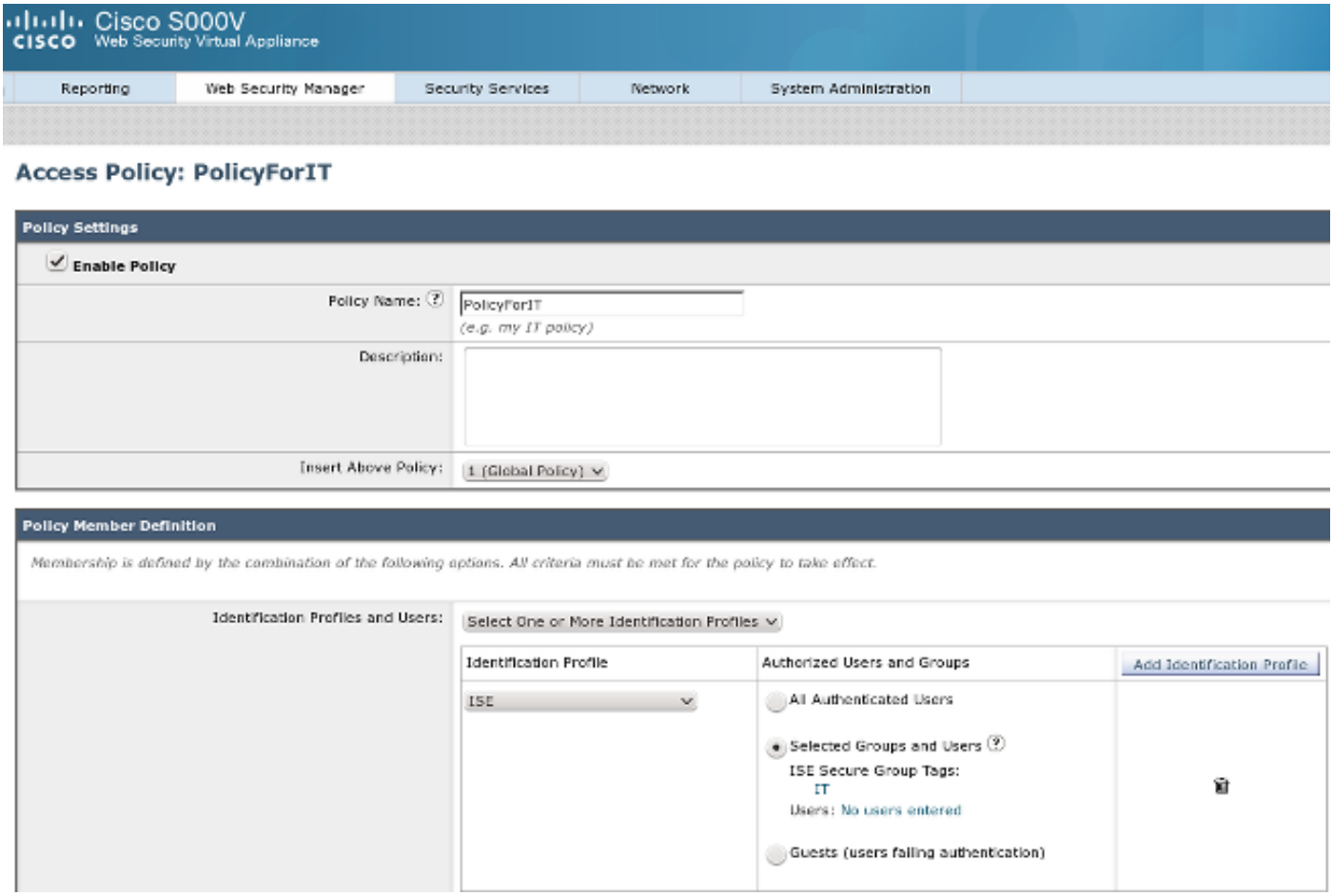
4단계. ISE 식별 프로필

ISE에 대한 새 프로필을 추가하려면 Web Security Manager > Identification **profiles**를 선택합니다 ."*Identification and Authentication(식별 및 인증)*"의 경우 "*Transparently identify users with ISE(ISE로 사용자를 투명하게 식별)*"를 사용합니다.

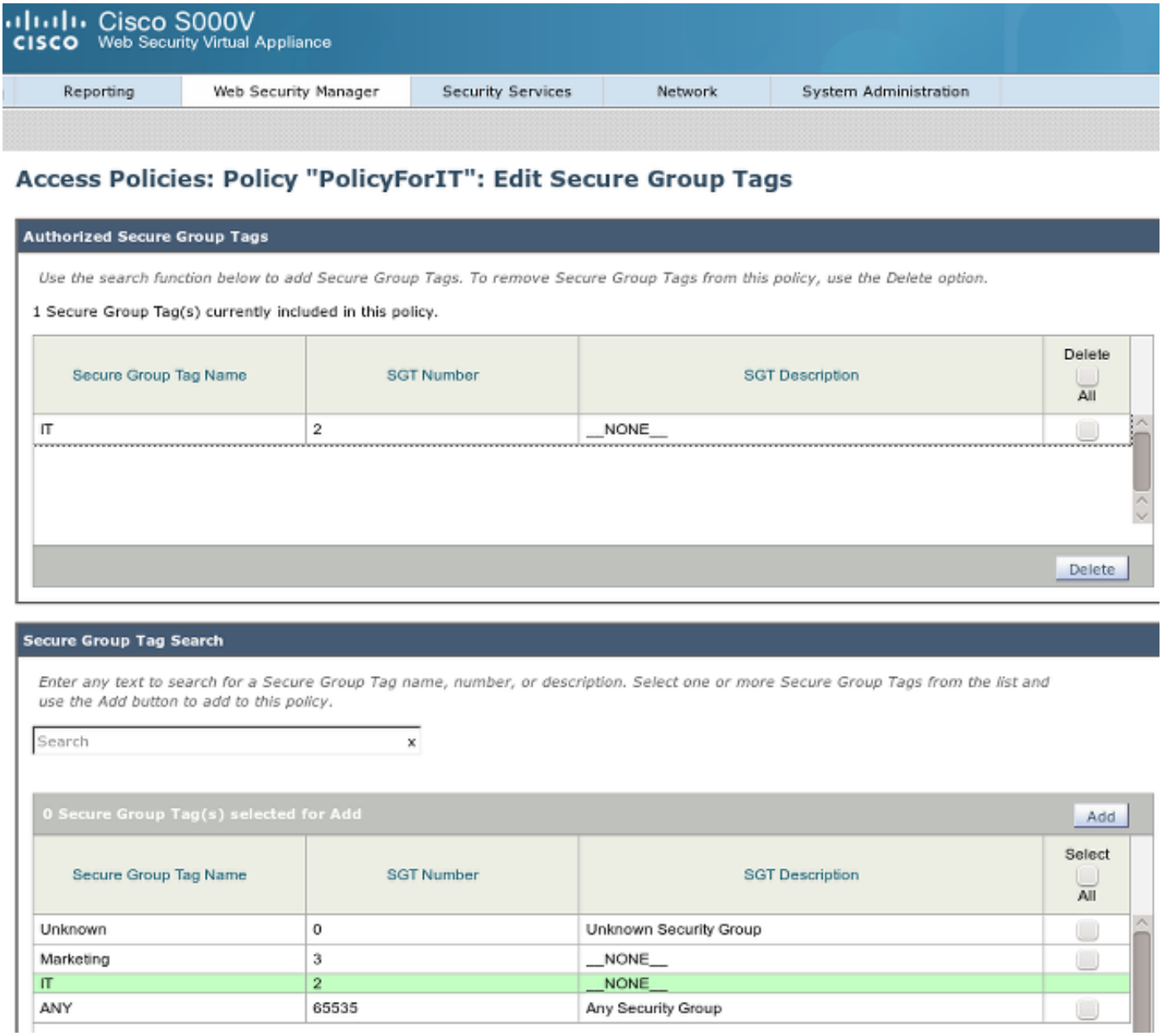


5단계. SGT 태그를 기반으로 정책에 액세스

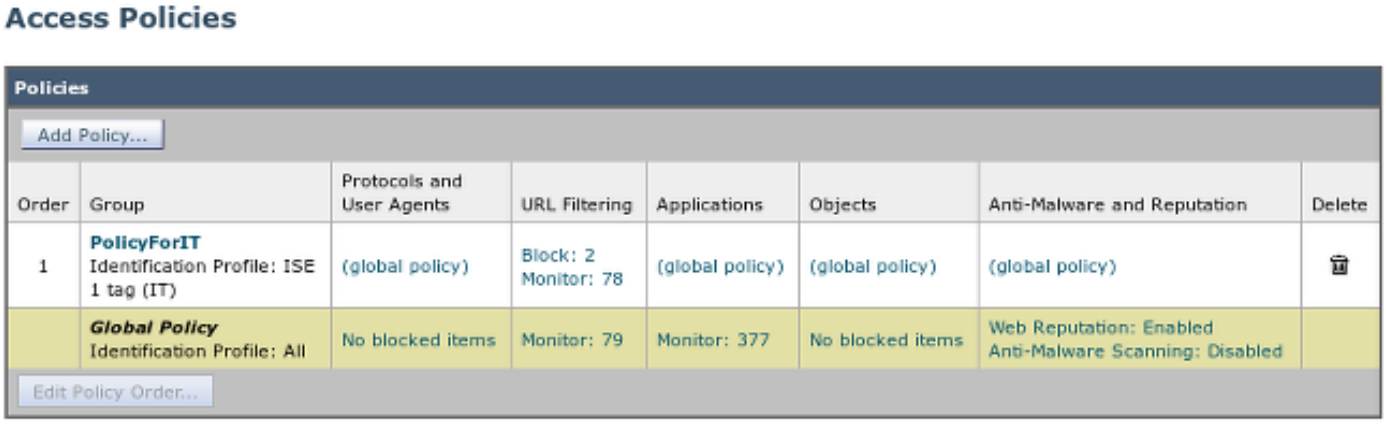
새 정책을 추가하려면 **Web Security Manager > Access Policies**를 선택합니다.멤버십은 ISE 프로파일을 사용합니다.



선택한 그룹 및 사용자의 경우 SGT 태그 2가 추가됩니다(IT).



이 정책은 SGT IT에 속한 사용자의 모든 스포츠 사이트에 대한 액세스를 거부합니다.

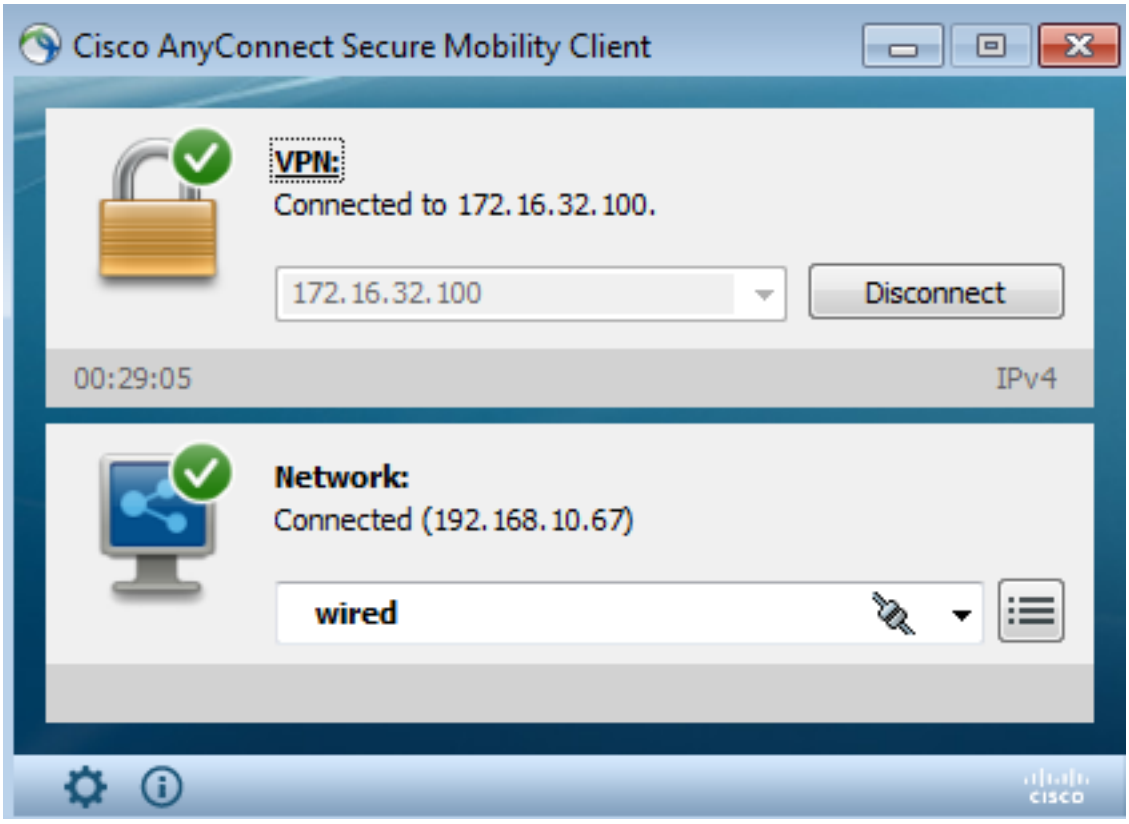


다음을 확인합니다.

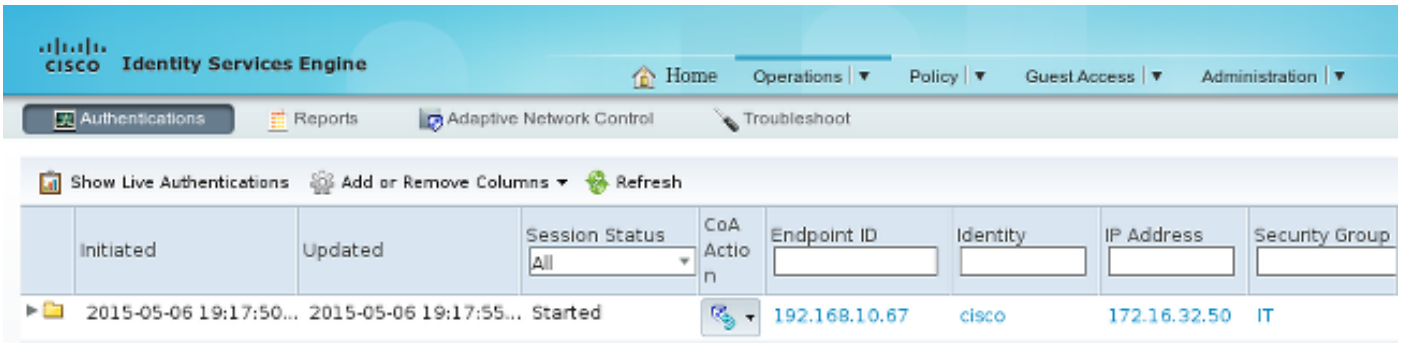
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

1단계. VPN 세션

VPN 사용자는 ASA-VPN에 대한 VPN 세션을 시작합니다.



ASA-VPN은 인증에 ISE를 사용합니다.ISE는 세션을 생성하고 SGT 태그 2(IT)를 할당합니다.



인증에 성공하면 ASA-VPN은 SGT 태그 2를 사용하여 VPN 세션을 생성합니다(cisco-av-pair에서 Radius Access-Accept로 표시됨).

```
asa-vpn# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 2
Assigned IP  : 172.16.32.50           Public IP    : 192.168.10.67
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 12979961               Bytes Rx     : 1866781
Group Policy : POLICY                 Tunnel Group : SSLVPN
Login Time   : 21:13:26 UTC Tue May 5 2015
```

```
Duration     : 6h:08m:03s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                     VLAN         : none
Audt Sess ID : ac1020640000200055493276
Security Grp : 2:IT
```

ASA-VPN과 ASA-FW 간의 링크가 TrustSec을 활성화하지 않았으므로 ASA-VPN은 해당 트래픽에 대해 태그가 지정되지 않은 프레임을 보냅니다(삽입된 CMD/TrustSec 필드로 이더넷 프레임을 캡슐화할 수 없음).

2단계. WSA에서 검색한 세션 정보

이 단계에서 WSA는 IP 주소, 사용자 이름 및 SGT(pxGrid 프로토콜을 통해) 간의 매핑을 수신해야 합니다.

```
wsa.example.com> isedata


Choose the operation you want to perform:
- STATISTICS - Show the ISE server status and ISE statistics.
- CACHE - Show the ISE cache or check an IP address.
- SGTS - Show the ISE Secure Group Tag (SGT) table.
[]> CACHE


Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[]> SHOW


IP               Name                                                SGT#
172.16.32.50     cisco                                               2

Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[]>
```

3단계. WSA로의 트래픽 리디렉션

VPN 사용자는 sport.pl에 대한 연결을 시작합니다. 이 연결은 ASA-FW에 의해 차단됩니다.

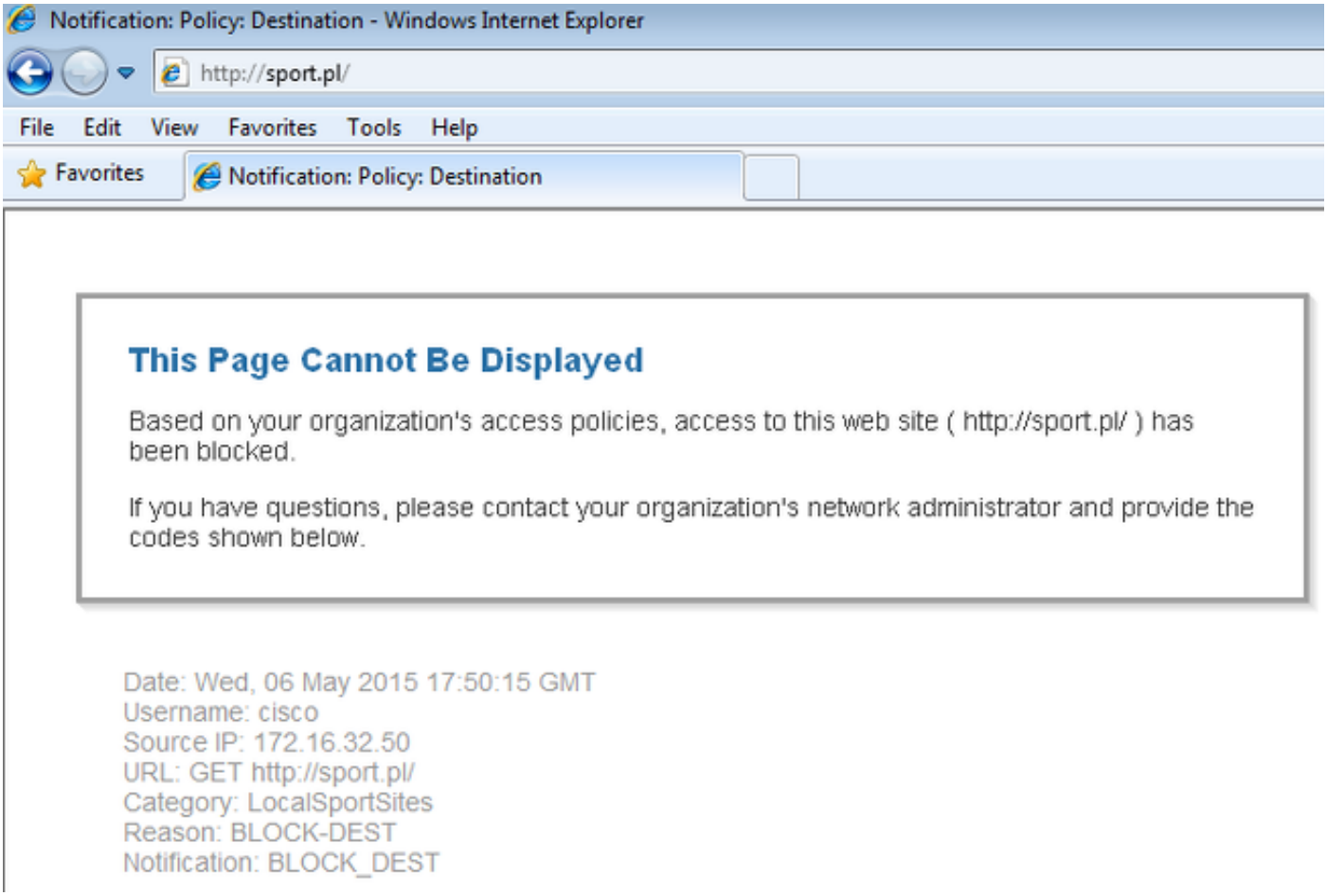
```
asa-fw# show wccp

Global WCCP information:
   Router information:
       Router Identifier:                   172.16.33.110
       Protocol Version:                    2.0

   Service Identifier: 90
       Number of Cache Engines:             1
       Number of routers:                   1
```

```
        Total Packets Redirected:            562
        Redirect access-list:                wccp-redirect
        Total Connections Denied Redirect:   0
        Total Packets Unassigned:            0
        Group access-list:                   wccp-routers
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total Bypassed Packets Received:     0

asa-fw# show access-list wccp-redirect
access-list wccp-redirect; 3 elements; name hash: 0x9bab8633
access-list wccp-redirect line 1 extended deny tcp any host 172.16.32.204 (hitcnt=0)
0xfd875b28
access-list wccp-redirect line 2 extended permit tcp any any eq www (hitcnt=562)
0x028ab2b9
access-list wccp-redirect line 3 extended permit tcp any any eq https (hitcnt=0)
0xe202a11e
```

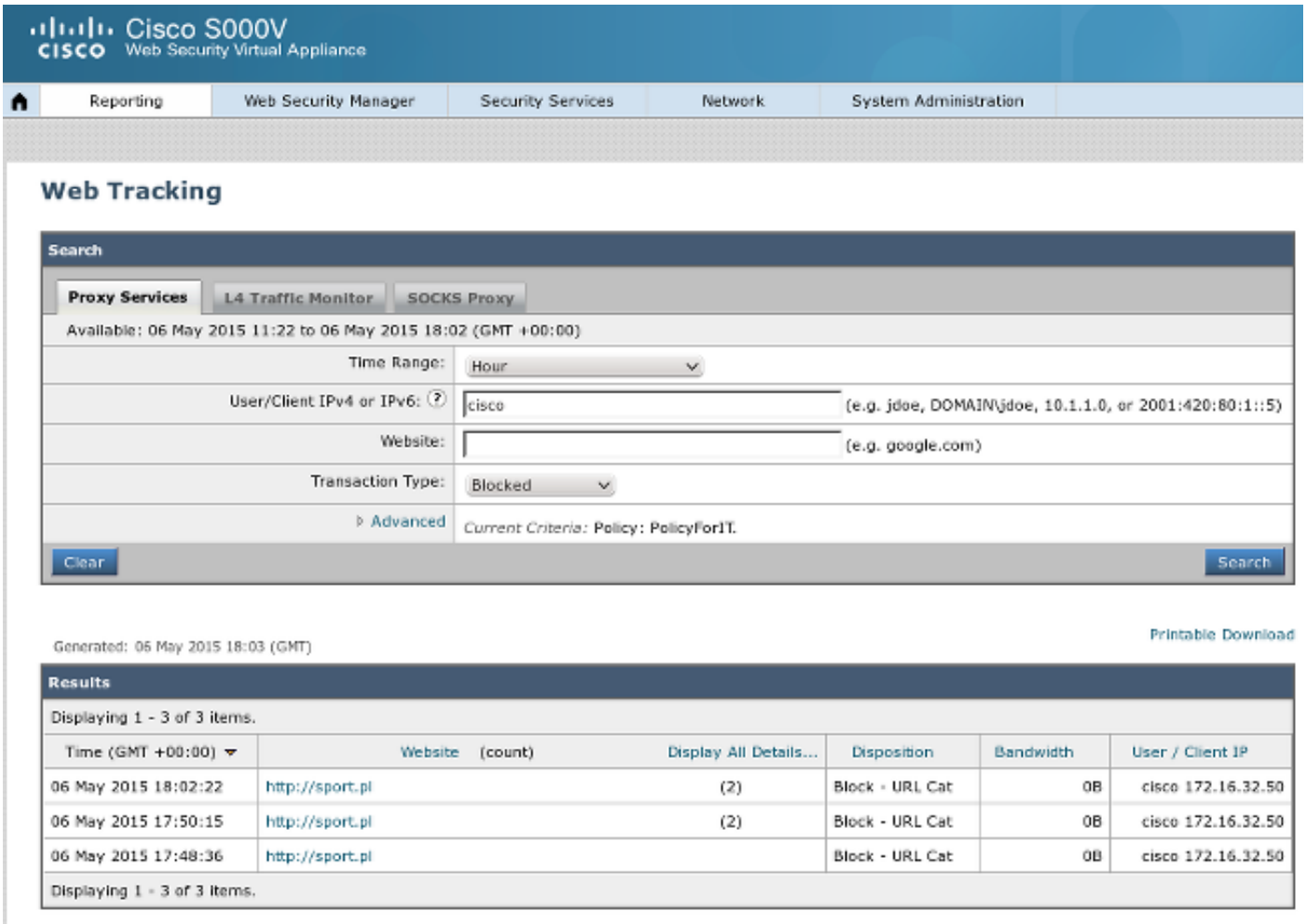
GRE에서 WSA로 터널링됩니다(WCCP 라우터 ID가 구성된 가장 높은 IP 주소).

```
asa-fw# show capture
capture CAP type raw-data interface inside [Capturing - 70065 bytes]
 match gre any any

asa-fw# show capture CAP

525 packets captured

  1: 03:21:45.035657       172.16.33.110 > 172.16.32.204:  ip-proto-47, length 60
  2: 03:21:45.038709       172.16.33.110 > 172.16.32.204:  ip-proto-47, length 48
  3: 03:21:45.039960       172.16.33.110 > 172.16.32.204:  ip-proto-47, length 640
```

WSA는 TCP 핸드셰이크를 계속하고 GET 요청을 처리합니다.따라서 PolicyForIT라는 정책이 적중되고 트래픽이 차단됩니다.



이는 WSA Report에서 확인합니다.



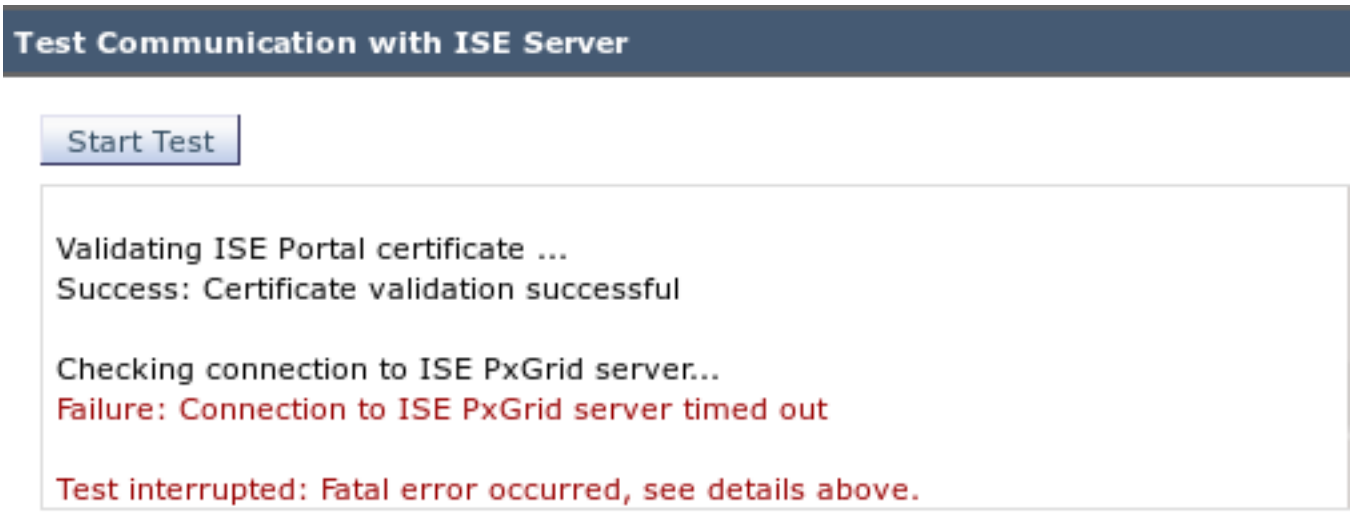
ISE에 사용자 이름이 표시됩니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

잘못된 인증서

WSA가 올바르게 초기화되지 않은 경우(인증서) ISE 연결 실패를 테스트합니다.



ISE pxgrid-cm.log 보고서:

```
[2015-05-06T16:26:51Z] [INFO ] [cm-1.jabber-172-16-31-202]
[TCPSocketStream::_doSSLHandshake] [] Failure performing SSL handshake: 1
```

실패 이유는 Wireshark에서 확인할 수 있습니다.

Source	Destination	Protocol	Info
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=66429032 TSecr=21743402
172.16.32.204	172.16.31.202	XMPP/XML	STREAM > xgrid.cisco.com
172.16.31.202	172.16.32.204	TCP	xmpp-client > 34491 [ACK] Seq=1 Ack=121 Win=14592 Len=0 TSval=21743403 TSecr=66429032
172.16.31.202	172.16.32.204	XMPP/XML	STREAM < xgrid.cisco.com
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=121 Ack=179 Win=131584 Len=0 TSval=66429032 TSecr=21743403
172.16.31.202	172.16.32.204	XMPP/XML	FEATURES
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=121 Ack=362 Win=131584 Len=0 TSval=66429032 TSecr=21743403
172.16.32.204	172.16.31.202	XMPP/XML	STARTTLS
172.16.31.202	172.16.32.204	XMPP/XML	PROCEED
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=172 Ack=412 Win=131712 Len=0 TSval=66429072 TSecr=21743451
172.16.32.204	172.16.31.202	TCP	[TCP segment of a reassembled PDU]
172.16.31.202	172.16.32.204	TCP	[TCP segment of a reassembled PDU]
172.16.31.202	172.16.32.204	TCP	[TCP segment of a reassembled PDU]
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=290 Ack=1860 Win=130304 Len=0 TSval=66429082 TSecr=21743451
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=290 Ack=3260 Win=130368 Len=0 TSval=66429082 TSecr=21743451
172.16.32.204	172.16.31.202	TCP	[TCP segment of a reassembled PDU]
172.16.31.202	172.16.32.204	TLSv1	Server Hello, Certificate, Certificate Request, Server Hello Done, Ignored Unknown Record
172.16.31.202	172.16.32.204	TLSv1	Ignored Unknown Record
172.16.32.204	172.16.31.202	TLSv1	Client Hello, Alert (Level: Fatal, Description: Unknown CA), Alert (Level: Fatal, Descrip

```
▷ Frame 21: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
▷ Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_58:cb:ad (00:0c:29:58:cb:ad)
▷ Internet Protocol Version 4, Src: 172.16.32.204 (172.16.32.204), Dst: 172.16.31.202 (172.16.31.202)
▷ Transmission Control Protocol, Src Port: 34491 (34491), Dst Port: xmpp-client (5222), Seq: 297, Ack: 3310, Len: 14
▷ [3 Reassembled TCP Segments (139 bytes): #13(118), #18(7), #21(14)]
▽ Secure Sockets Layer
  ▷ TLSv1 Record Layer: Handshake Protocol: Client Hello
  ▶ TLSv1 Record Layer: Alert (Level: Fatal, Description: Unknown CA)
  ▷ TLSv1 Record Layer: Alert (Level: Fatal, Description: Unknown CA)
  ▷ TLSv1 Record Layer: Alert (Level: Fatal, Description: Unknown CA)
```

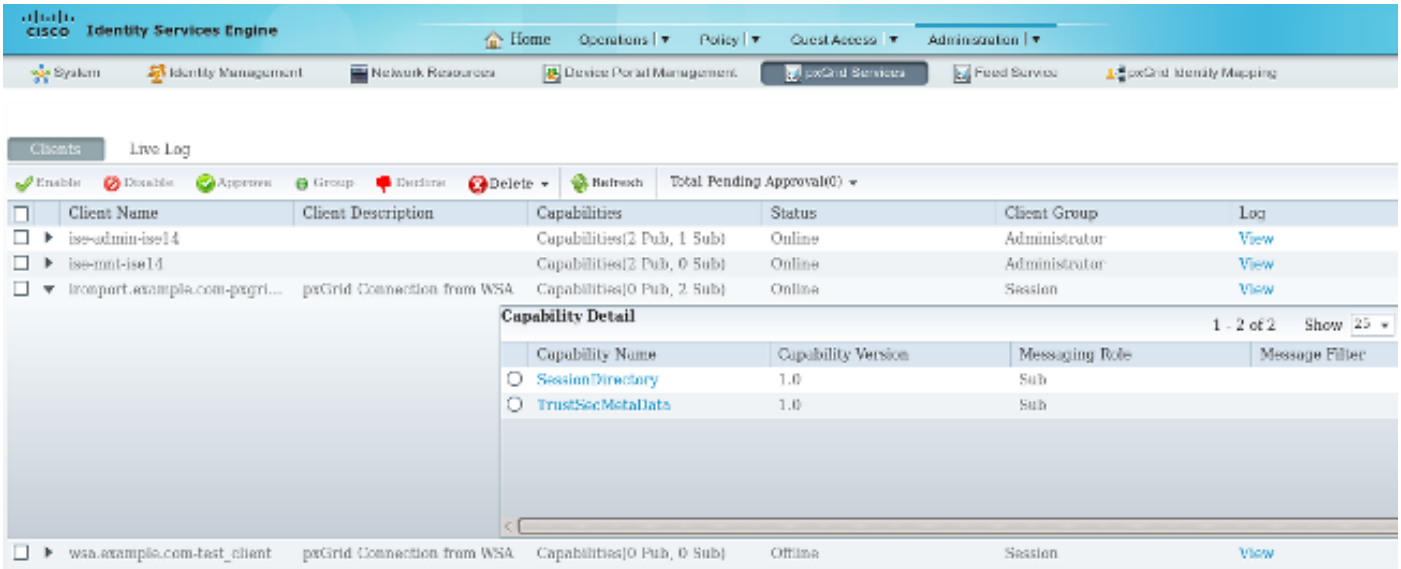
pxGrid에서 사용하는 XMPP(Extensible Messaging and Presence Protocol) 교환을 보호하는 데 사용되는 SSL 세션의 경우 클라이언트가 서버에서 제공하는 알 수 없는 인증서 체인으로 인해 SSL 오류를 보고합니다.

올바른 시나리오

올바른 시나리오의 경우 ISE pxgrid-controller.log 로그:

```
2015-05-06 18:40:09,153 INFO [Thread-7][] cisco.pxgrid.controller.sasl.SaslWatcher
-::::::- Handling authentication for user name wsa.example.com-test_client
```

또한 ISE GUI는 WSA를 올바른 기능을 갖춘 가입자로 표시합니다.



관련 정보

- ASA 버전 9.2.1 VPN Posture with ISE 컨피그레이션 예
- WSA 8.7 사용자 가이드
- ASA 및 Catalyst 3750X Series Switch TrustSec 컨피그레이션 예 및 문제 해결 가이드
- Cisco TrustSec 스위치 구성 가이드:Cisco TrustSec 이해
- 보안 어플라이언스 사용자 권한 부여를 위한 외부 서버 구성
- Cisco ASA Series VPN CLI 컨피그레이션 가이드, 9.1
- Cisco Identity Services Engine 사용 설명서, 릴리스 1.2
- 기술 지원 및 문서 – Cisco Systems