ISE 및 FirePower Integration으로 리미디에이션 서비스 구성

목차

소개

이 문서에서는 Cisco FireSight 어플라이언스에서 리미디에이션 모듈을 사용하여 공격을 탐지하고 Cisco ISE(Identity Service Engine)를 정책 서버로 사용하여 공격자를 자동으로 치료하는 방법에 대해 설명합니다.이 문서에서 제공하는 예는 ISE를 통해 인증하는 원격 VPN 사용자의 교정에 사용되는 방법을 설명하지만 802.1x/MAB/WebAuth 유선 또는 무선 사용자에게도 사용할 수 있습니다.

참고:이 문서에서 참조하는 리미디에이션 모듈은 Cisco에서 공식적으로 지원하지 않습니다

.커뮤니티 포털에서 공유되며 누구나 사용할 수 있습니다.버전 5.4 이상에는 pxGrid 프로토콜을 기반으로 하는 최신 리미디에이션 모듈이 *있습니다*.이 모듈은 버전 6.0에서 지원되지 않지만 향후 버전에서 지원될 예정입니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ASA(Adaptive Security Appliance) VPN 컨피그레이션
- Cisco AnyConnect Secure Mobility Client 컨피그레이션
- Cisco FireSight 기본 구성
- Cisco FirePower 기본 구성
- Cisco ISE 컨피그레이션

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft Windows 7
- Cisco ASA 버전 9.3 이상
- Cisco ISE 소프트웨어 버전 1.3 이상
- Cisco AnyConnect Secure Mobility Client 버전 3.0 이상
- Cisco FireSight Management Center 버전 5.4
- Cisco FirePower 버전 5.4(VM)

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

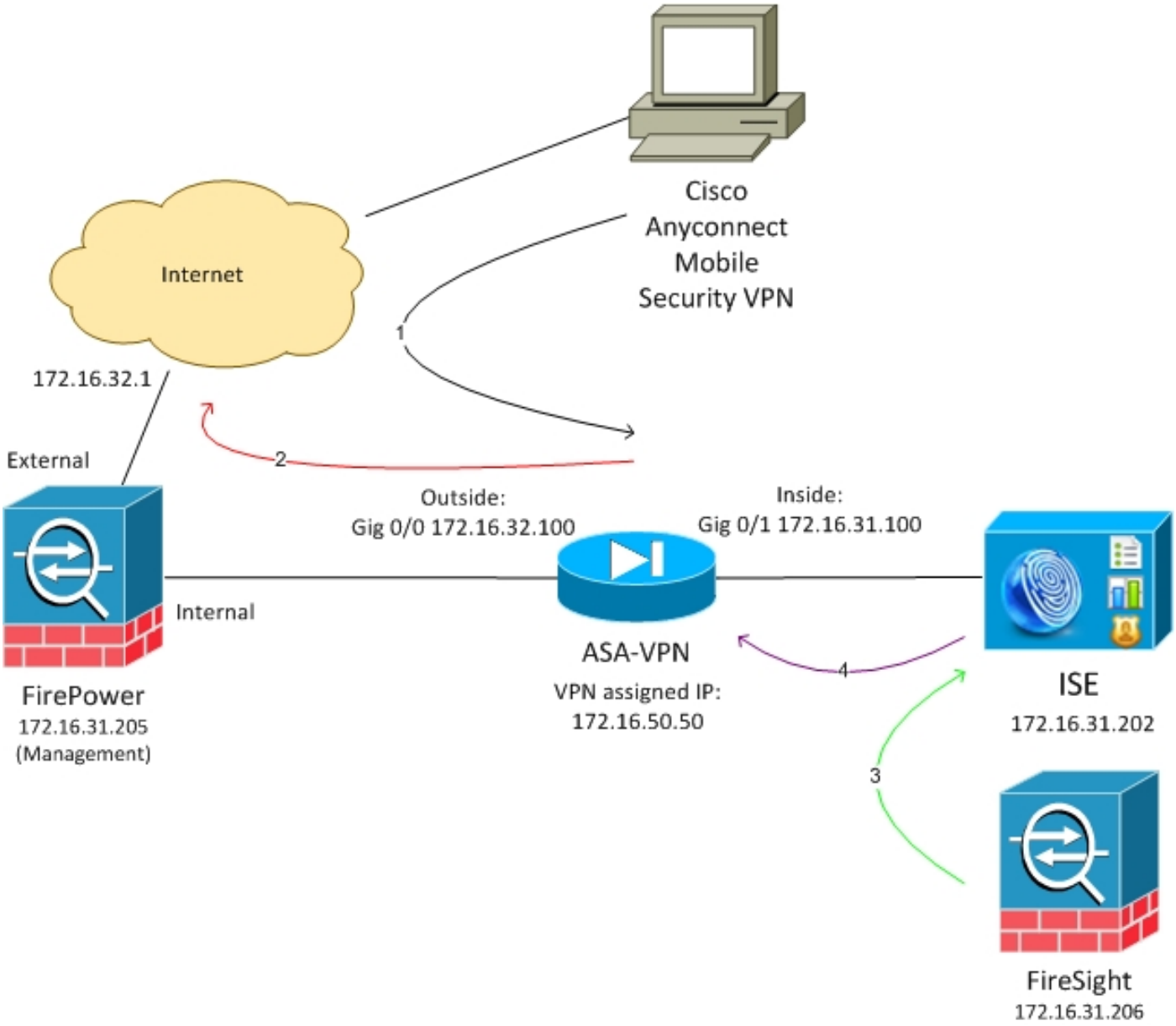
시스템을 구성하려면 이 섹션에서 제공하는 정보를 사용하십시오.

참고:이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고

객만 해당)을 사용합니다.

네트워크 다이어그램

이 문서에 설명된 예에서는 이 네트워크 설정을 사용합니다.



이 네트워크 설정에 대한 플로우는 다음과 같습니다.

1. 사용자는 Cisco AnyConnect Secure Mobility Version 4.0을 통해 ASA로 원격 VPN 세션을 시작합니다.

2. 사용자는 http://172.16.32.1*에* 액세스하려고 시도합니다. 트래픽은 VM에 설치되고 FireSight에서 관리하는 FirePower를 통해 이동합니다.

3. FirePower는 특정 트래픽(액세스 정책)을 차단(인라인)하도록 구성되지만 트리거되는 상관관계 정책도 있습니다.따라서 REST API(Application Programming Interface)를 통해 ISE 교정을 시작합니다(QuarantineByIP 방법).

4. ISE가 REST API 호출을 받으면 세션을 조회하고 ASA에 RADIUS CoA(Change of Authorization)를 전송하여 해당 세션을 종료합니다.

5. ASA는 VPN 사용자의 연결을 끊습니다.AnyConnect는 *Always-On* VPN 액세스로 구성되었으므로 새 세션이 설정됩니다.그러나 이번에는 다른 ISE 권한 부여 규칙이 일치하며(격리된 호스트의 경우) 제한된 네트워크 액세스가 제공됩니다.이 단계에서는 사용자가 네트워크에 어떻게 연결하고 인증하는지가 중요하지 않습니다.ISE가 인증 및 권한 부여에 사용되는 한 사용자는 격리로 인해 네트워크 액세스가 제한됩니다.

앞에서 언급한 대로, 이 시나리오는 ISE가 인증에 사용되고 네트워크 액세스 디바이스가 RADIUS CoA(모든 최신 Cisco 디바이스)를 지원하는 경우 모든 유형의 인증된 세션(VPN, 유선 802.1x/MAB/Webauth, 무선 802.1x/MAB/Webauth)에 대해 작동합니다.

> **팁:**사용자를 쿼런틴에서 이동하려면 ISE GUI를 사용할 수 있습니다.향후 버전의 리미디에이션 모듈에서도 이를 지원할 수 있습니다.

FirePower

> **참고:**VM 어플라이언스는 이 문서에 설명된 예제에 사용됩니다.초기 컨피그레이션만 CLI를 통해 수행됩니다.모든 정책은 Cisco Defense Center에서 구성됩니다.자세한 내용은 이 문서의 관련 정보 섹션을 참조하십시오.

VM에는 3개의 인터페이스가 있습니다. 하나는 관리용이고 다른 하나는 인라인 검사용입니다(내부/외부).

VPN 사용자의 모든 트래픽은 FirePower를 통해 이동합니다.

FireSight Management Center(Defense Center)

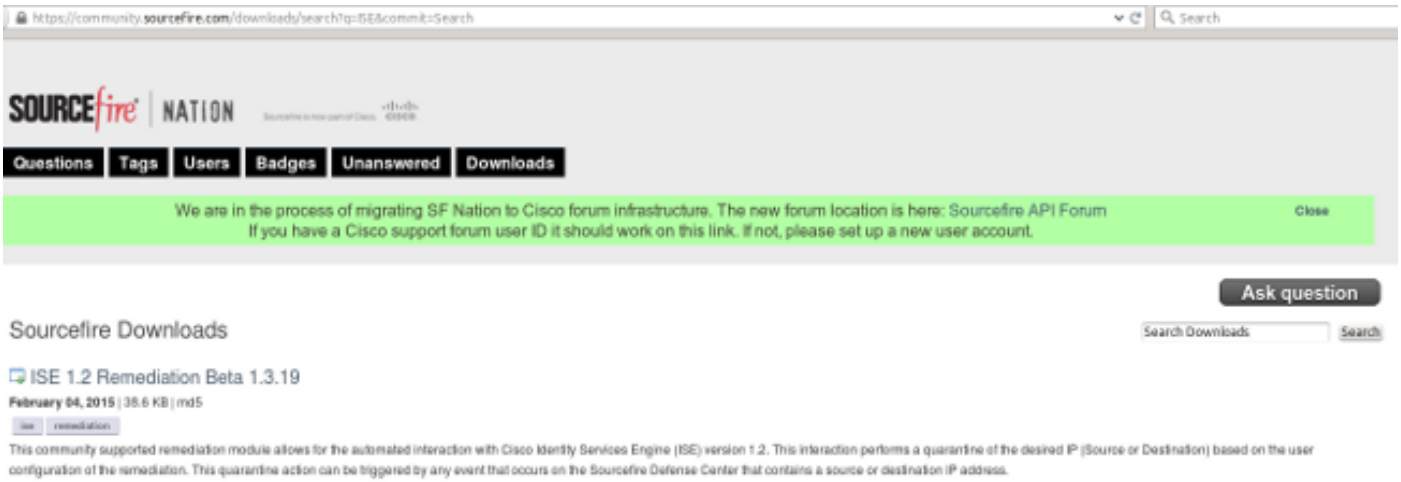
액세스 제어 정책

올바른 라이센스를 설치하고 FirePower 디바이스를 추가한 후 **Policies(정책) > Access Control(액세스 제어)**으로 이동하고 HTTP 트래픽을 172.16.32.1으로 삭제하기 위해 사용되는 액세스 정책을 생성합니다.

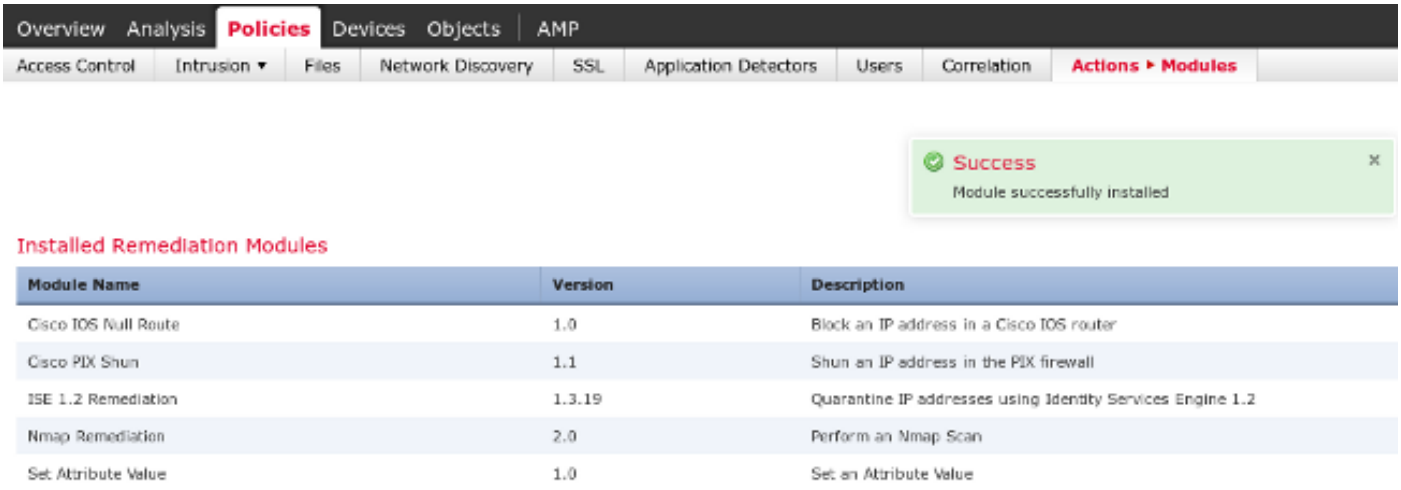
다른 모든 트래픽은 허용됩니다.

ISE 리미디에이션 모듈

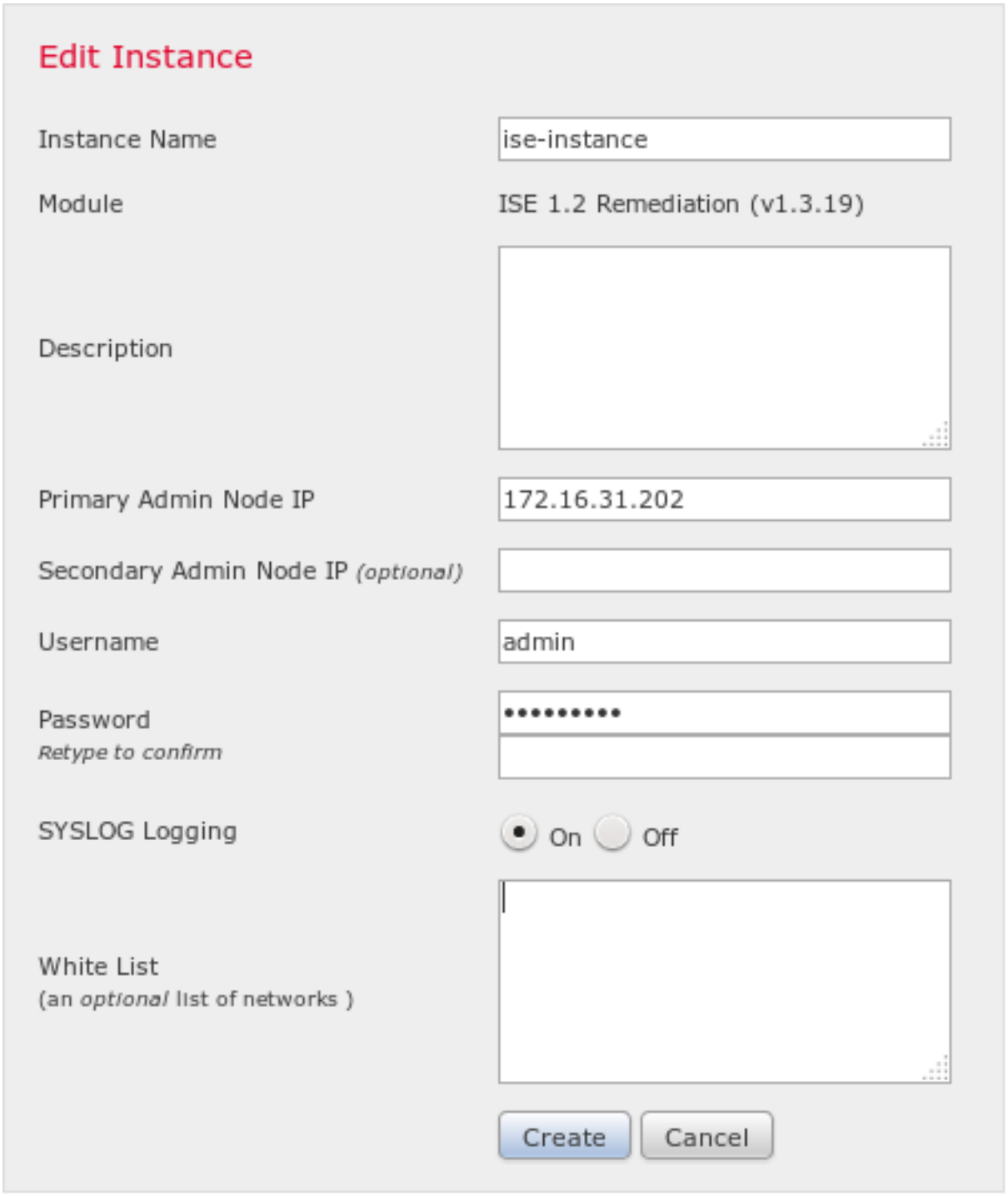
커뮤니티 포털에서 공유되는 ISE 모듈의 현재 버전은 *ISE 1.2 Remediation Beta 1.3.19입니다*.



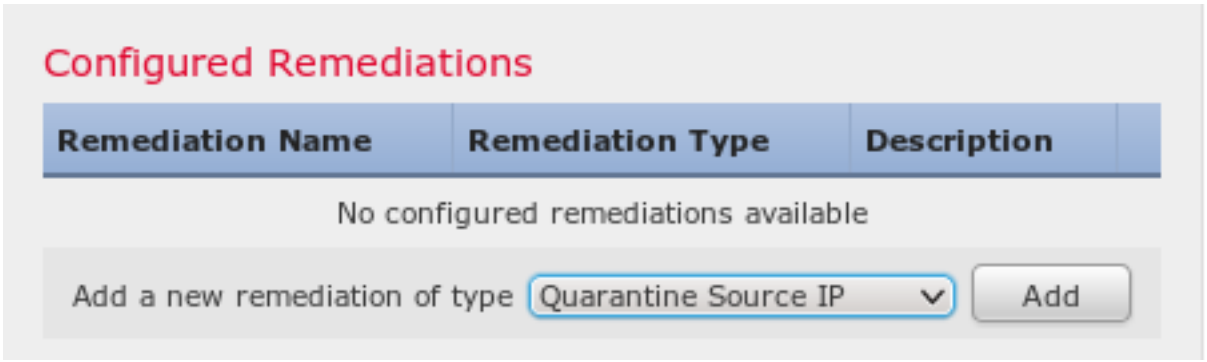
Policies(**정책) > Actions(작업) > Remediations(교정) > Modules(모듈)로 이동하여** 파일을 설치합니다.



그런 다음 올바른 인스턴스를 만들어야 합니다.Policies(**정책) > Actions(작업) > Remediations(교정) > Instances(인스턴스)로 이동하고** REST API에 필요한 ISE 관리 자격 증명과 함께 PAN(정책 관리 노드)의 IP 주소를 제공합니다(*ERS Admin* 역할을 사용하는 별도의 사용자 권장).

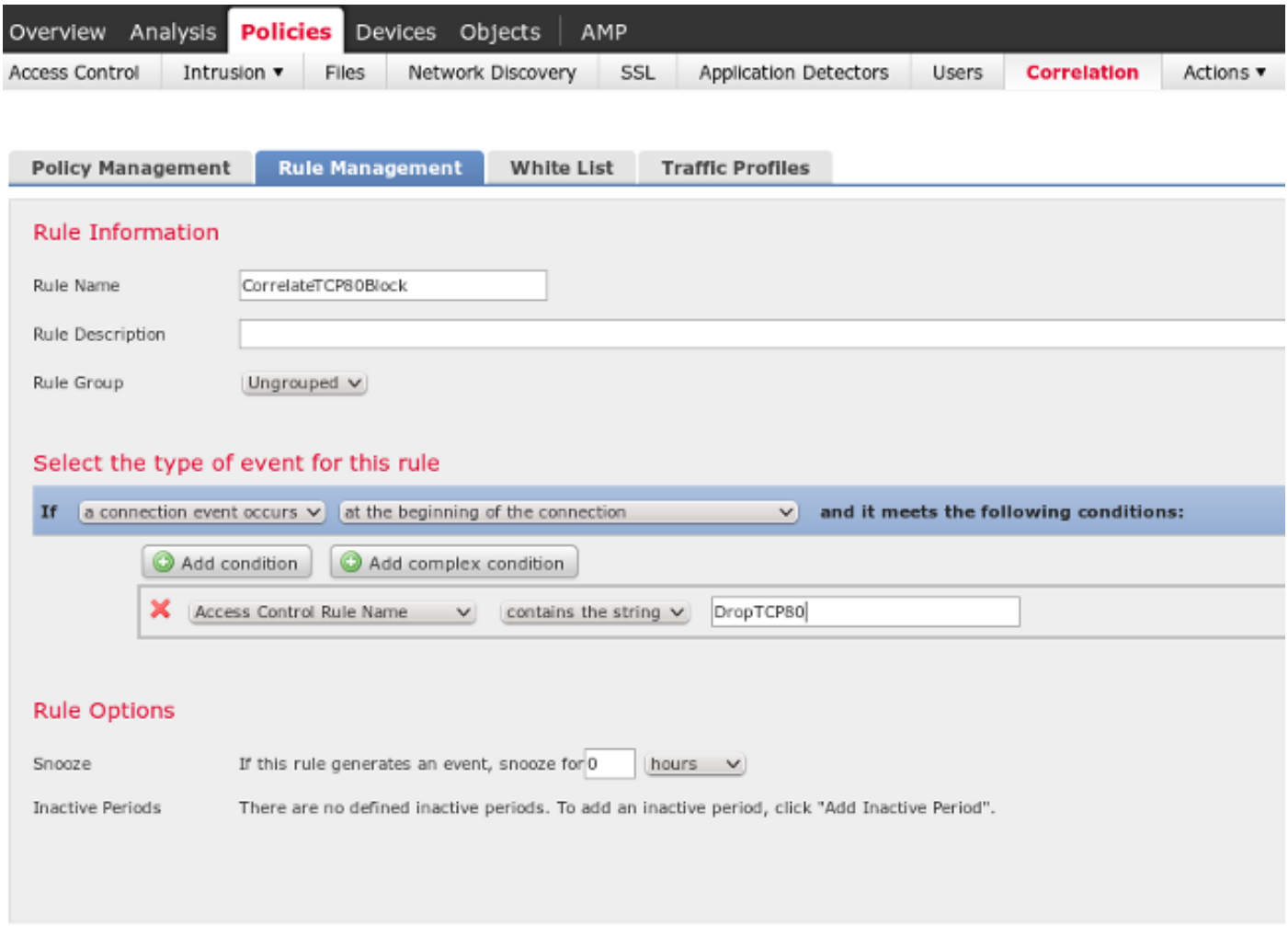


원본 IP 주소(공격자)도 교정에 사용해야 합니다.

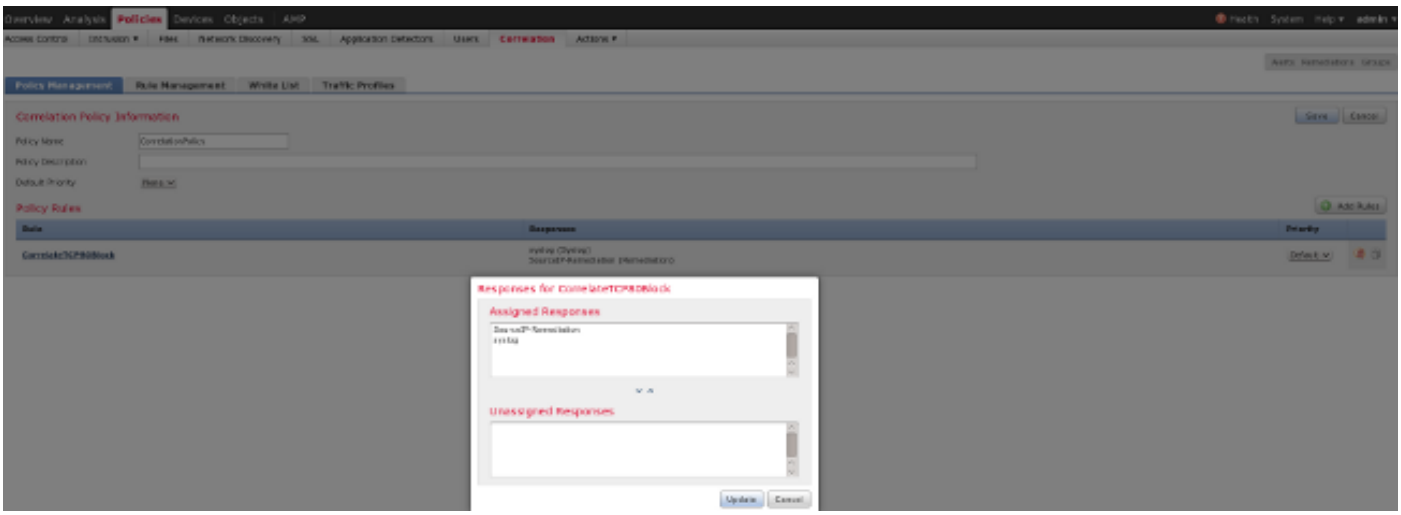


상관관계 정책

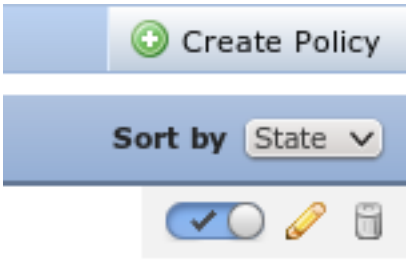
이제 특정 상관관계 규칙을 구성해야 합니다.이 규칙은 이전에 구성된 액세스 제어 규칙 (DropTCP*80*)과 일치하는 연결의 시작 시 트리거됩니다. 규칙을 구성하려면 Policies > Correlation **> Rule Management로 이동합니다**.



이 규칙은 상관관계 정책에서 사용됩니다.새 정책을 생성하려면 **Policies > Correlation > Policy Management**로 이동한 다음 구성된 규칙을 추가합니다.오른쪽에서 Remediate(교정)를 클릭하고 두 가지 작업을 추가합니다.**sourceIP**(이전에 구성) 및 syslog에 대한 **교정**:



상관관계 정책을 활성화해야 합니다.



ASA

VPN 게이트웨이로 작동하는 ASA는 인증에 ISE를 사용하도록 구성됩니다.또한 어카운팅 및 RADIUS CoA를 활성화해야 합니다.

```
tunnel-group SSLVPN-FIRESIGHT general-attributes
 address-pool POOL-VPN
 authentication-server-group ISE
 accounting-server-group ISE
 default-group-policy POLICY

aaa-server ISE protocol radius
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE (inside) host 172.16.31.202
 key *****

webvpn
 enable outside
 enable inside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 error-recovery disable
```

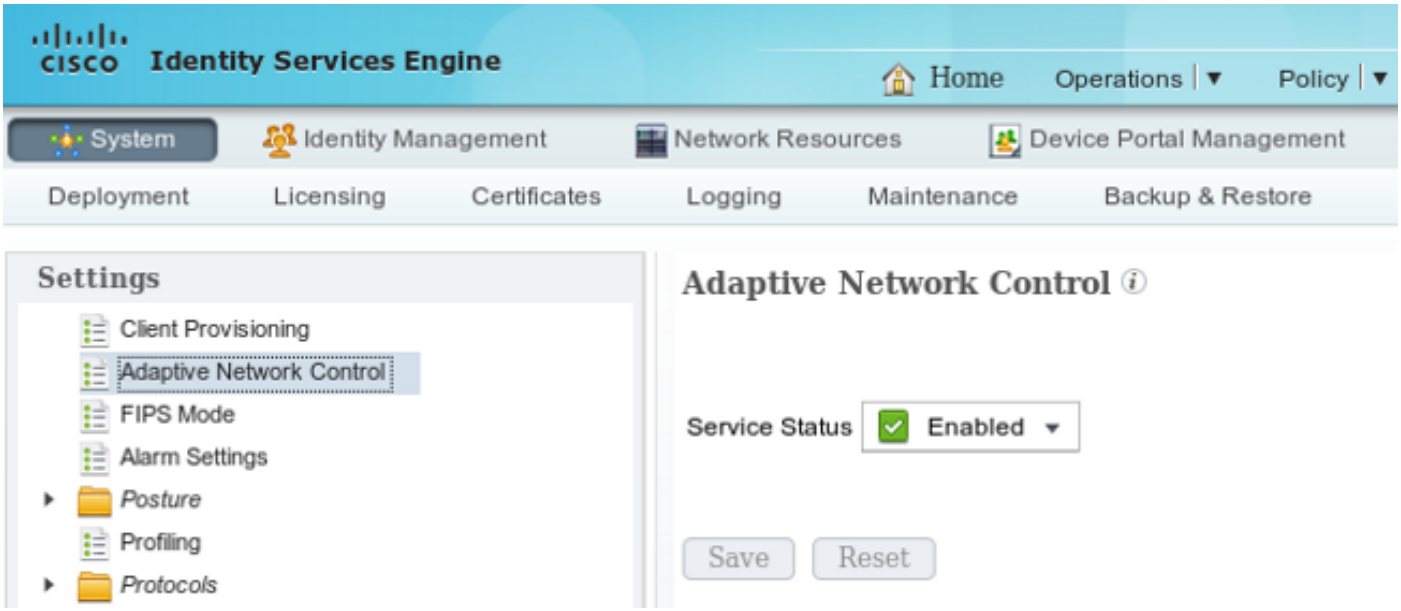
ISE

NAD(Network Access Device) 구성

Administration(**관리) > Network Devices(네트워크 디바이스**)로 이동하고 RADIUS 클라이언트로 작동하는 ASA를 추가합니다.

적응형 네트워크 제어 사용

격리 API 및 기능을 활성화하려면 **Administration(관리) > System(시스템) > Settings(설정) > Adaptive Network Control(적응형 네트워크 제어)**으로 이동합니다.



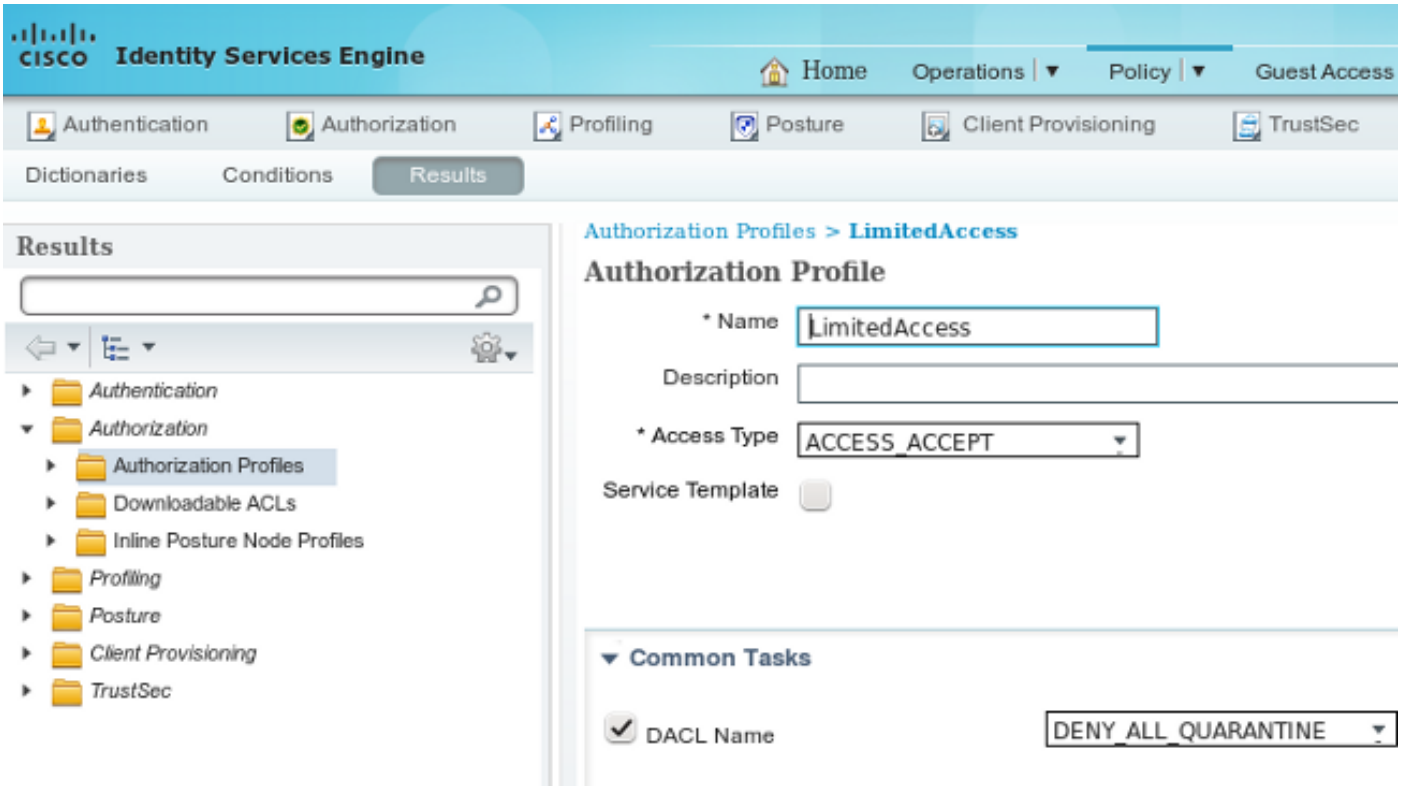
참고:버전 1.3 이하에서는 이 기능을 엔드포인트 *보호 서비스라고 합니다*.

쿼런틴 DACL

격리된 호스트에 사용되는 DACL(Downloadable Access Control List)을 생성하려면 **Policy(정책) > Results(결과) > Authorization(권한 부여) > Downloadable ACL(다운로드 가능한 ACL)로 이동합니다**.

격리에 대한 권한 부여 프로파일

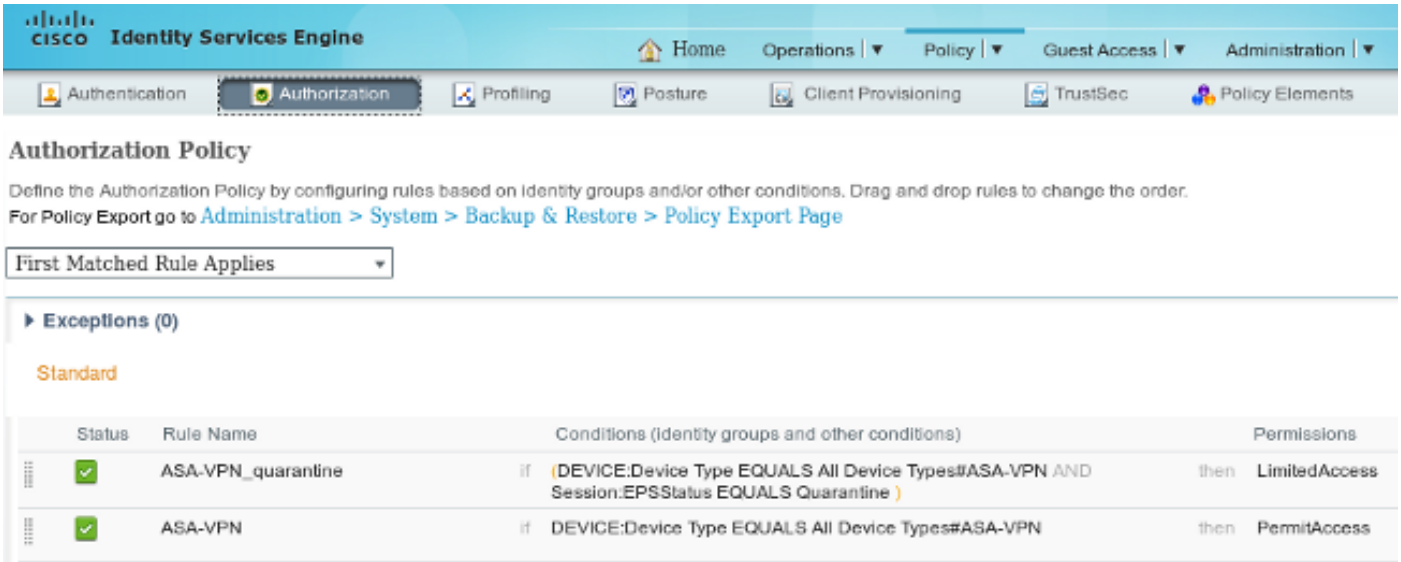
Policy(**정책) > Results(결과) > Authorization(권한 부여) > Authorization Profile(권한 부여 프로파일)로 이동하고** 새 DACL을 사용하여 권한 부여 프로파일을 생성합니다.



권한 부여 규칙

두 개의 권한 부여 규칙을 생성해야 합니다.첫 번째 규칙(ASA-VPN)은 ASA에서 종료되는 모든 VPN 세션에 대한 전체 액세스를 제공합니다.호스트가 이미 격리되어 *있는* 경우 재인증된 VPN 세션에 대해 규칙 ASA-VPN_*quarantine*이 적중됩니다(제한된 네트워크 액세스가 제공됨).

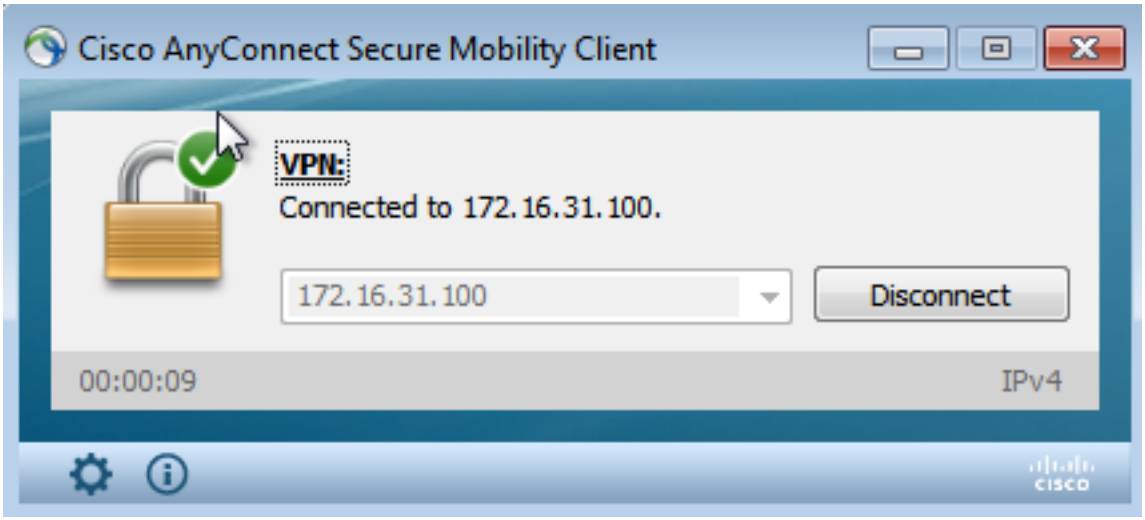
이러한 규칙을 생성하려면 Policy(정책) **> Authorization(권한 부여)**으로 이동합니다.



다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 이 섹션에 제공된 정보를 사용하십시오.

AnyConnect가 ASA VPN 세션 시작



ASA는 DACL 없이 세션을 생성합니다(전체 네트워크 액세스).

```
asav# show vpn-sessiondb details anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 37
Assigned IP  : 172.16.50.50           Public IP    : 192.168.10.21
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     : 18706                  Bytes Rx     : 14619
Group Policy : POLICY                 Tunnel Group : SSLVPN-FIRESIGHT
Login Time   : 03:03:17 UTC Wed May 20 2015
Duration     : 0h:01m:12s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : ac10206400025000555bf975
Security Grp : none

.......
DTLS-Tunnel:
 <some output omitted for clarity>
```

사용자 액세스 시도

사용자가 http://172.16.32.1에 액세스하려고 시도하면 액세스 정책이 적중되고, 해당 트래픽이 인라인으로 차단되며, syslog 메시지가 FirePower 관리 IP 주소에서 전송됩니다.

```
May 24 09:38:05 172.16.31.205 SFIMS: [Primary Detection Engine
(cbe45720-f0bf-11e4-a9f6-bc538df1390b)][AccessPolicy] Connection Type: Start, User:
Unknown, Client: Unknown, Application Protocol: Unknown, Web App: Unknown,
 Access Control Rule Name: DropTCP80, Access Control Rule Action: Block,
Access Control Rule Reasons: Unknown, URL Category: Unknown, URL Reputation:
Risk unknown, URL: Unknown, Interface Ingress: eth1, Interface Egress: eth2,
Security Zone Ingress: Internal, Security Zone Egress: External, Security
Intelligence Matching IP: None, Security Intelligence Category: None, Client Version:
(null), Number of File Events: 0, Number of IPS Events: 0, TCP Flags: 0x0,
```

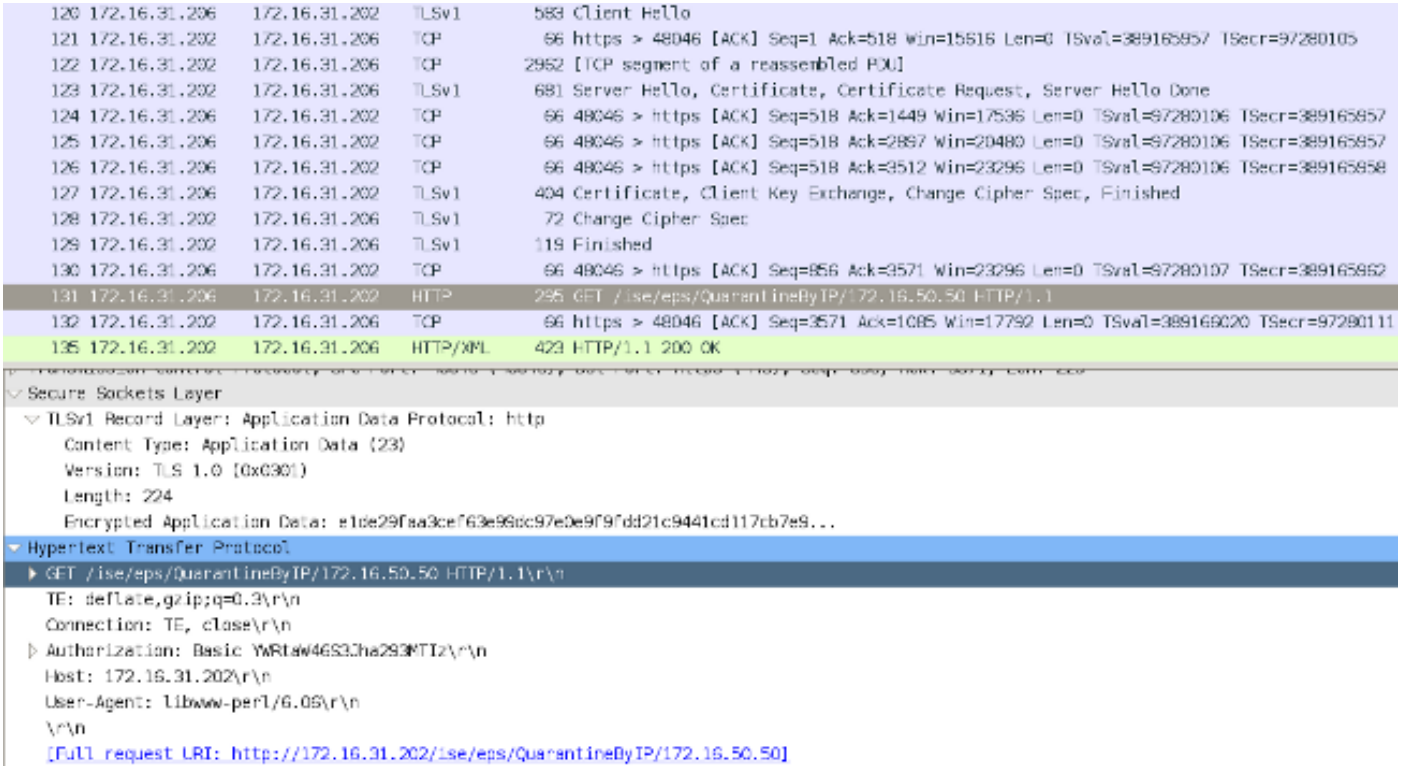
```
NetBIOS Domain: (null), Initiator Packets: 1, Responder Packets: 0, Initiator Bytes:
66, Responder Bytes: 0, Context: Unknown, SSL Rule Name: N/A, SSL Flow Status: N/A,
SSL Cipher Suite: N/A, SSL Certificate: 0000000000000000000000000000000000000000,
SSL Subject CN: N/A, SSL Subject Country: N/A, SSL Subject OU: N/A, SSL Subject Org:
N/A, SSL Issuer CN: N/A, SSL Issuer Country: N/A, SSL Issuer OU: N/A, SSL Issuer Org:
N/A, SSL Valid Start Date: N/A, SSL Valid End Date: N/A, SSL Version: N/A, SSL Server
Certificate Status: N/A, SSL Actual Action: N/A, SSL Expected Action: N/A, SSL Server
Name: (null), SSL URL Category: N/A, SSL Session ID:
0000000000000000000000000000000000000000000000000000000000000000, SSL Ticket Id:
00000000000000000000000000000000000000, {TCP} 172.16.50.50:49415 -> 172.16.32.1:80
```

FireSight 상관관계 정책 적중

FireSight 관리(Defense Center) 상관관계 정책이 적중되었으며, 이는 Defense Center에서 전송되는 syslog 메시지에 의해 보고됩니다.

```
May 24 09:37:10 172.16.31.206 SFIMS: Correlation Event:
CorrelateTCP80Block/CorrelationPolicy at Sun May 24 09:37:10 2015 UTCConnection Type:
FireSIGHT 172.16.50.50:49415 (unknown) -> 172.16.32.1:80 (unknown) (tcp)
```

이 단계에서 Defense Center는 ISE에 대한 REST API(격리) 호출을 사용합니다. ISE는 HTTPS 세션이며 Wireshark(SSL(Secure Sockets Layer) 플러그인과 PAN 관리 인증서의 개인 키 사용)에서 해독할 수 있습니다.



공격자의 IP 주소에 대한 GET 요청에서 (172.16.50.50)이 전달되고 해당 호스트는 ISE에 의해 격리됩니다.

Analysis(**분석) > Correlation(상관관계) > Status(상태)**로 이동하여 성공적인 교정을 확인합니다.

ISE는 격리 및 CoA 전송

이 단계에서 ISE *port-management.log*는 CoA를 전송해야 함을 알립니다.

```
DEBUG  [RMI TCP Connection(142)-127.0.0.1][] cisco.cpm.prrt.impl.PrRTLoggerImpl
-:::::- send() - request instanceof DisconnectRequest
        clientInstanceIP = 172.16.31.202
        clientInterfaceIP = 172.16.50.50
       portOption = 0
       serverIP = 172.16.31.100
       port = 1700
       timeout = 5
       retries = 3
       attributes = cisco-av-pair=audit-session-id=ac10206400021000555b9d36
Calling-Station-ID=192.168.10.21
Acct-Terminate-Cause=Admin Reset
```

런타임(prrt-server.log)은 CoA *종료* 메시지를 NAD에 전송하여 세션을 종료합니다(ASA).

```
DEBUG,0x7fad17847700,cntx=0000010786,CPMSessionID=2e8cdb62-bc0a-4d3d-a63e-f42ef8774893,
CallingStationID=08:00:27:DA:EF:AD, RADIUS PACKET: Code=40 (
DisconnectRequest) Identifier=9 Length=124
    [4] NAS-IP-Address - value: [172.16.31.100]
     [31] Calling-Station-ID - value: [08:00:27:DA:EF:AD]
    [49] Acct-Terminate-Cause - value: [Admin Reset]
    [55] Event-Timestamp - value: [1432457729]
    [80] Message-Authenticator - value:
[00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00]
    [26] cisco-av-pair - value: [audit-session-id=ac10206400021000555b9d36],
RadiusClientHandler.cpp:47
```

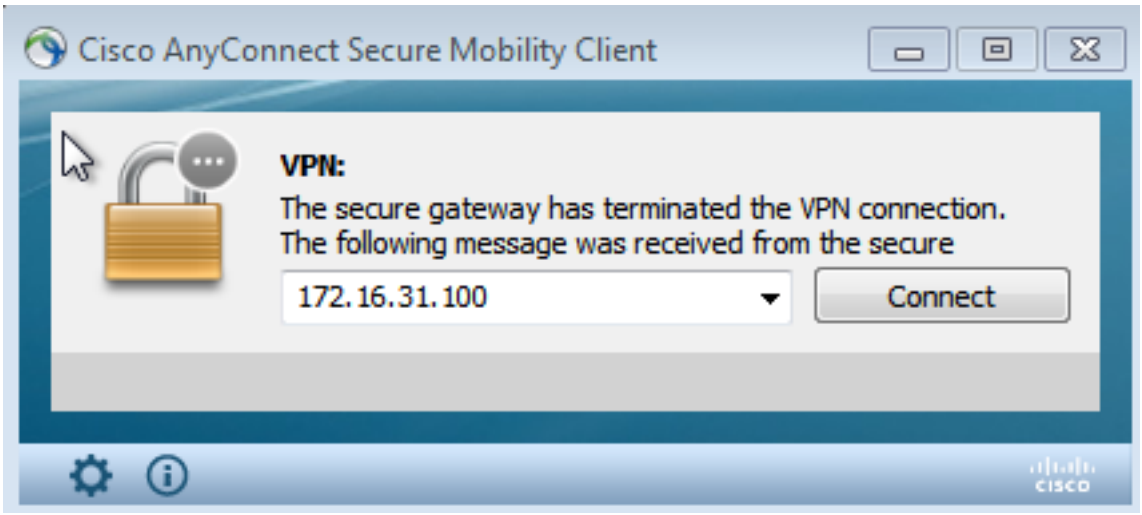
ise.*psc*는 다음과 유사한 알림을 전송합니다.

```
INFO   [admin-http-pool51][] cisco.cpm.eps.prrt.PrrtManager -::::::- PrrtManager
disconnect session=Session CallingStationID=192.168.10.21 FramedIPAddress=172.16.50.50
AuditSessionID=ac10206400021000555b9d36 UserName=cisco PDPIPAddress=172.16.31.202
NASIPAddress=172.16.31.100 NASPortID=null option=PortDefault
```

Operations(작업) > **Authentication(인증)으로** 이동할 때 Dynamic Authorization succeeded(*동적 권한 부여 성공*)가 표시되어야 합니다.

VPN 세션 연결이 끊겼습니다.

엔드 유저는 세션 연결이 끊겼음을 알리기 위해 알림을 보냅니다(802.1x/MAB/게스트 유무선, 이 프로세스는 투명함).

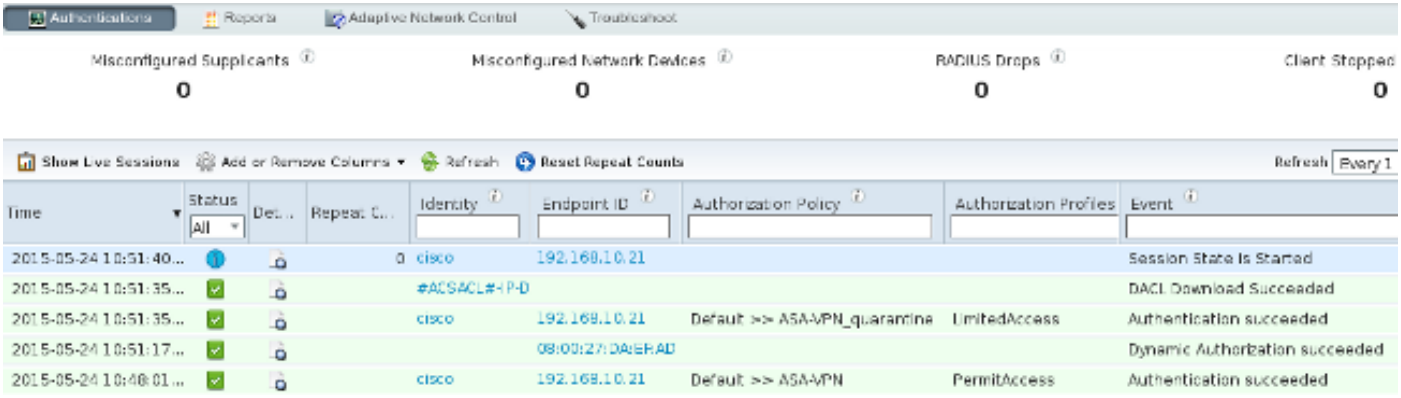


Cisco AnyConnect 로그의 세부 정보는 다음과 같습니다.

```
10:48:05 AM Establishing VPN...
10:48:05 AM Connected to 172.16.31.100.
10:48:20 AM Disconnect in progress, please wait...
10:51:20 AM The secure gateway has terminated the VPN connection.
The following message was received from the secure gateway: COA initiated
```

제한된 액세스가 있는 VPN 세션(격리)

Always-*On VPN*이 구성되었으므로 새 세션이 즉시 구축됩니다.이번에는 ISE *ASA-VPN_quarantine* 규칙이 적중하여 제한된 네트워크 액세스를 제공합니다.



참고:DACL은 별도의 RADIUS 요청에 다운로드됩니다.

ASA에서 show vpn-sessiondb detail anyconnect CLI 명령을 사용하여 액세스가 제한된 세션을 확인할 수 있습니다.

```
asav# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : cisco                  Index        : 39
```

```
Assigned IP  : 172.16.50.50           Public IP    : 192.168.10.21
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     : 11436                 Bytes Rx     : 4084
Pkts Tx      : 8                     Pkts Rx      : 36
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : POLICY                Tunnel Group : SSLVPN-FIRESIGHT
Login Time   : 03:43:36 UTC Wed May 20 2015
Duration     : 0h:00m:10s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : ac10206400027000555c02e8
Security Grp : none

.......
DTLS-Tunnel:
 <some output ommited for clarity>
  Filter Name  : #ACSACL#-IP-DENY_ALL_QUARANTINE-5561da76
```

문제 해결

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

FireSight(Defense Center)

ISE 교정 스크립트는 다음 위치에 있습니다.

```
root@Defence:/var/sf/remediations/ISE_1.3.19# ls
_lib_  ise-instance  ise-test.pl  ise.pl  module.template
```

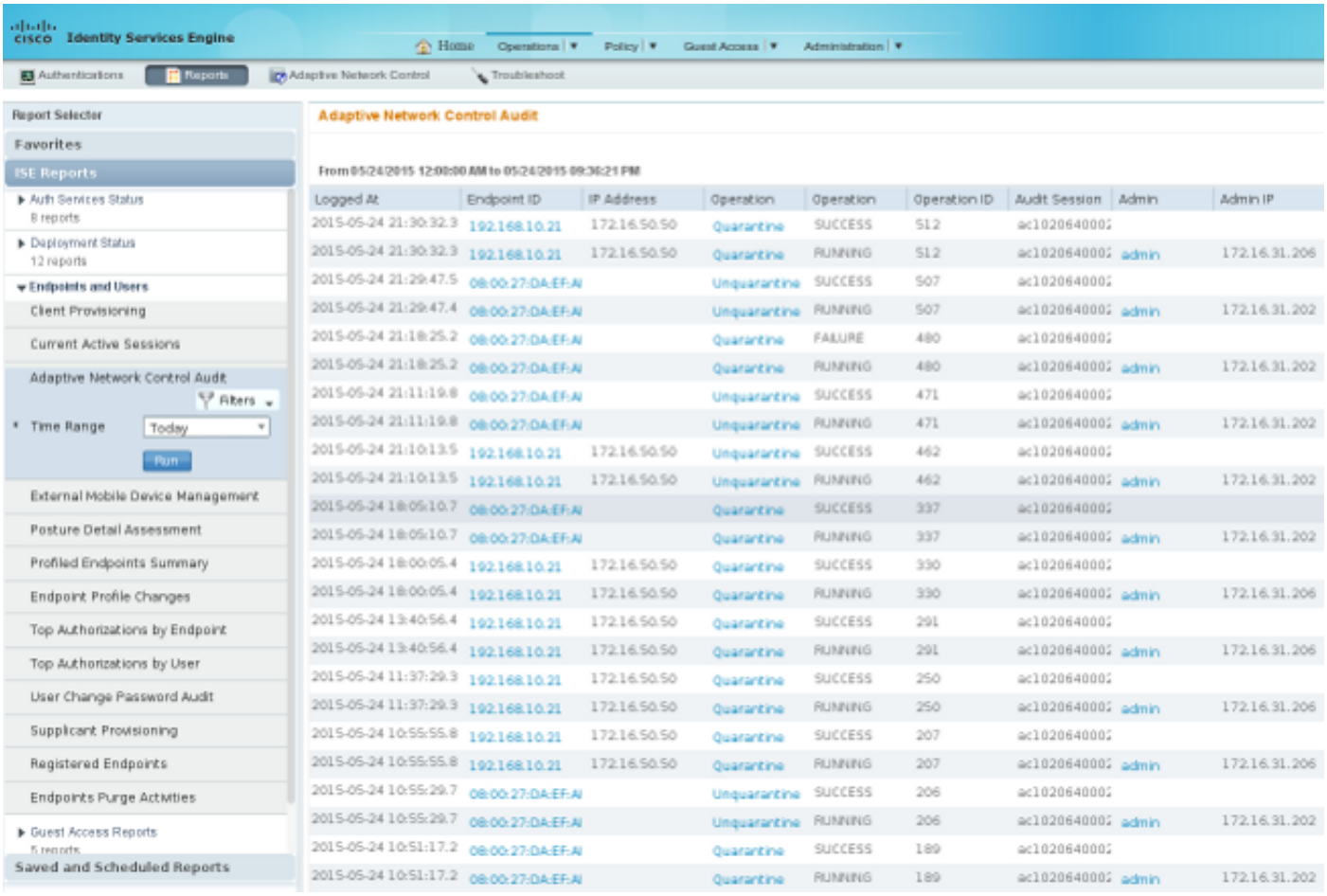
표준 SF(SourceFire) 로깅 하위 시스템을 사용하는 간단한 perl 스크립트입니다.교정이 실행되면 */var/log/messages*를 통해 결과를 확인할 수 있습니다.

```
May 24 19:30:13 Defence SF-IMS[2414]: ise.pl:SourceIP-Remediation [INFO] [2414]
quar_ip:172.16.50.50 (1->3 sid:1) Starting remediation
May 24 19:30:13 Defence SF-IMS[2414]: ise.pl:SourceIP-Remediation [INFO] [2414]
quar_ip:172.16.50.50 (1->3 sid:1) 172.16.31.202 - Success 200 OK - Quarantined
172.16.50.50 as admin
```

ISE

ISE에서 Adaptive Network Control 서비스를 활성화하는 것이 중요합니다.런타임 프로세스에서 자세한 로그를 보려면(prrt-*management.log* 및 prrt-*server.log*) Runtime-AAA에 대한 DEBUG 레벨을 활성화해야 합니다.디버그를 **활성화하려면 Administration > System > Logging > Debug Log Configuration**으로 이동합니다.

또한 Operations(운영) > Reports(**보고서) > Endpoint and Users(엔드포인트 및 사용자) > Adaptive Network Control Audit(적응형 네트워크 제어 감사)로 이동하여** 격리 요청의 모든 시도와 결과에 대한 정보를 볼 수 있습니다.



버그

VPN 세션 실패(802.1x/MAB 정상 작동)와 관련된 ISE 버그에 대한 자세한 내용은 Cisco 버그 ID CSCuu41058(ISE 1.4 엔드포인트 격리 불일치와 VPN 실패)을 참조하십시오.

관련 정보

- TrustSec 인식 서비스를 위한 ISE와 WSA 통합 구성
- ISE 버전 1.3 pxGrid와 IPS pxLog 애플리케이션 통합
- Cisco Identity Services Engine 관리자 가이드, 릴리스 1.4 - Setup Adaptive Network Control
- Cisco Identity Services Engine API 참조 설명서, 릴리스 1.2 - 외부 RESTful 서비스 소개 API
- Cisco Identity Services Engine API 참조 가이드, 릴리스 1.2 - 모니터링 REST API 소개
- Cisco Identity Services Engine 관리자 가이드, 릴리스 1.3
- 기술 지원 및 문서 - Cisco 시스템