iPEP ISE 및 ASA를 사용하는 VPN 인라인 상태

목차

소개

이 문서에서는 ASA(Adaptive Security Appliance) 및 ISE(Identity Services Engine)를 사용하여 인라인 상태를 설정하는 방법에 대한 정보를 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 ASA의 버전 8.2(4) 및 ISE의 버전 1.1.0.665을 기반으로 합니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

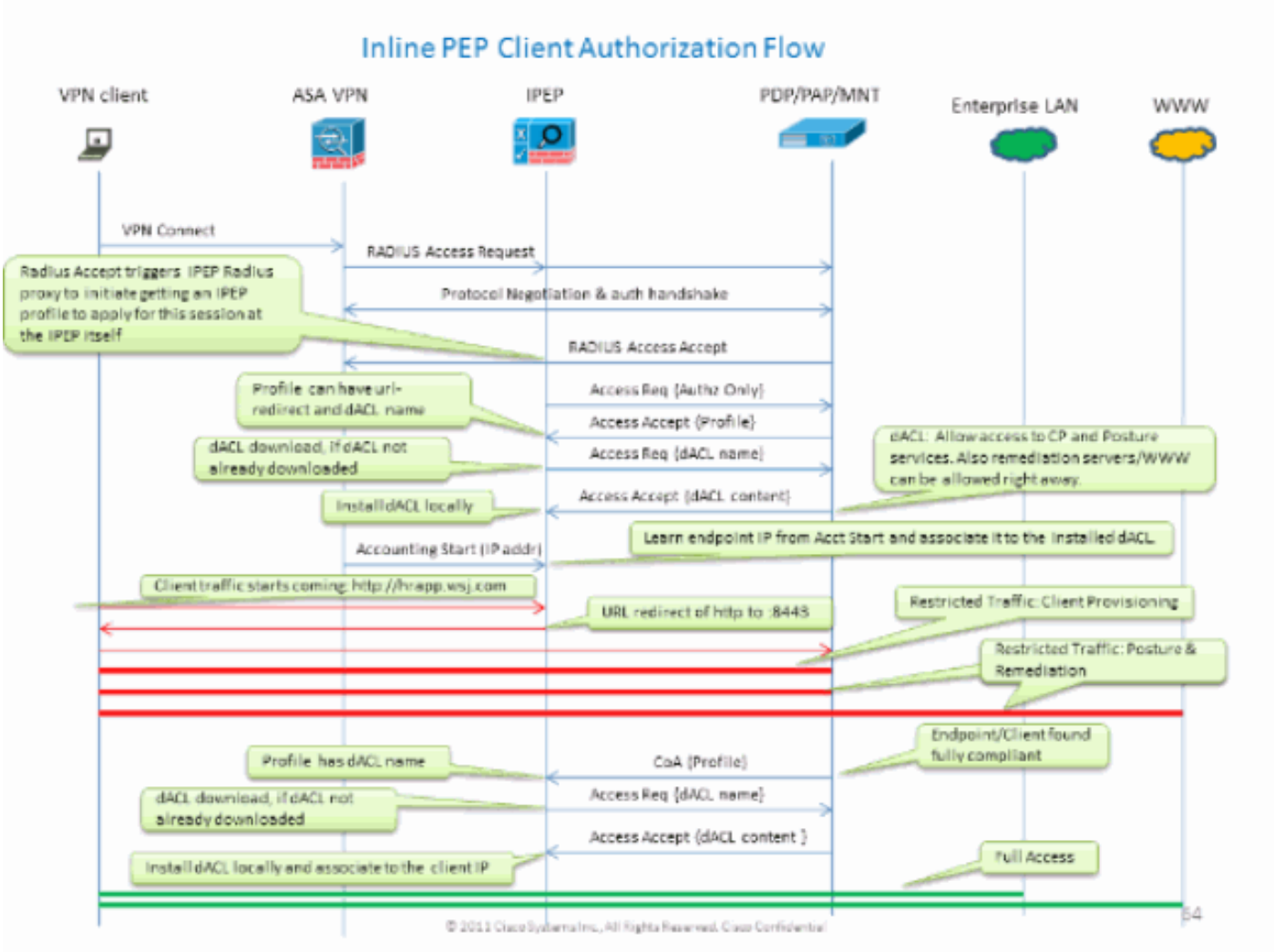
ISE는 많은 AAA 서비스(상태, 프로파일링, 인증 등)를 제공합니다. 일부 NAD(Network Devices)는 Posture 또는 Profiling 결과를 기반으로 엔드 디바이스의 권한 부여 프로파일을 동적으로 변경할 수 있는 CoA(Radius Change Of Authorization)를 지원합니다.ASA와 같은 다른 NAD는 이 기능을 아직 지원하지 않습니다.즉, 엔드 디바이스의 네트워크 액세스 정책을 동적으로 변경하려면 iPEP(Inline Posture Enforcement Mode)에서 실행 중인 ISE가 필요합니다.

기본 개념은 모든 사용자 트래픽이 iPEP를 통과하고 노드가 Radius 프록시 역할을 한다는 것입니다.

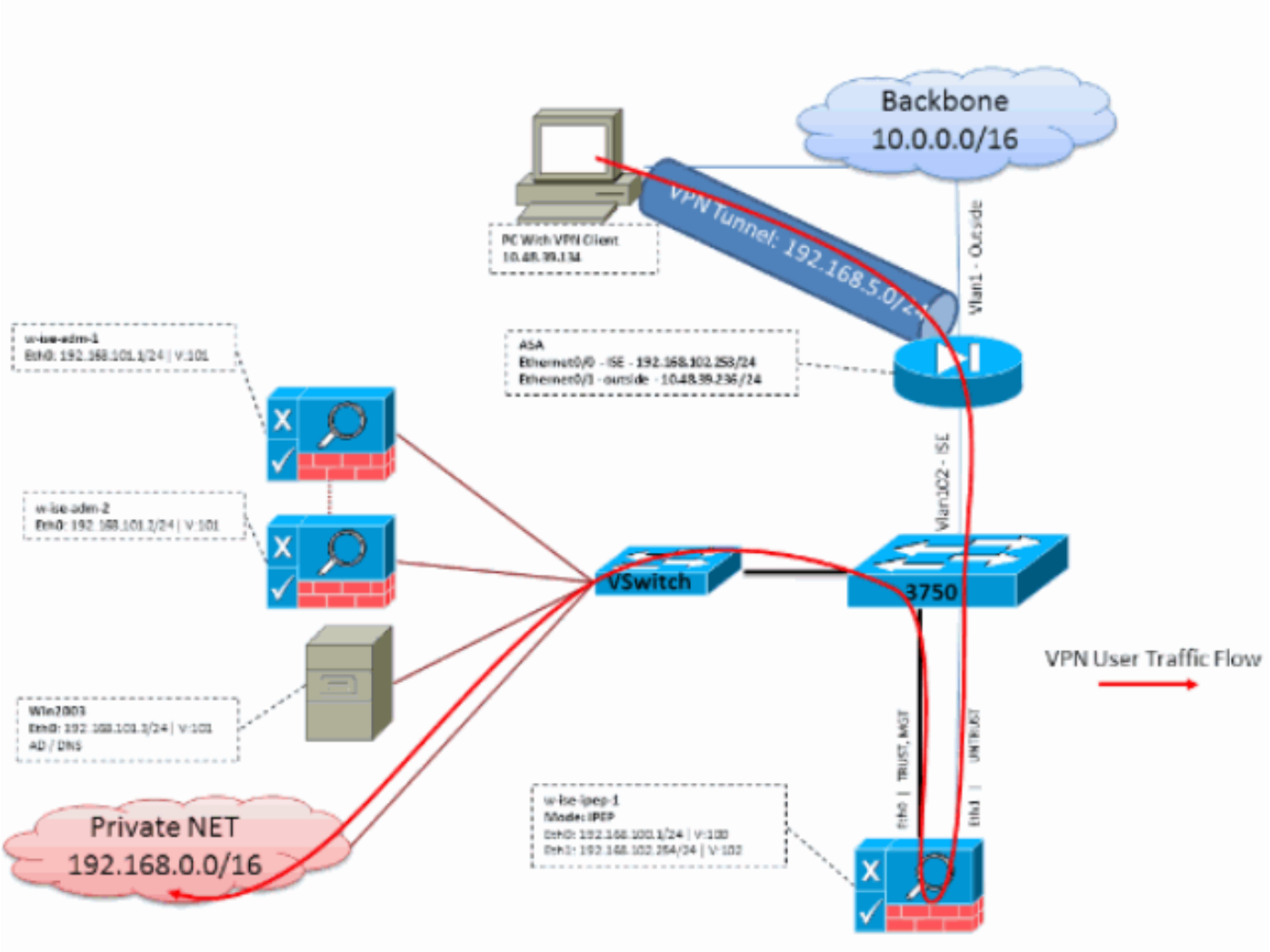
기본 흐름

1. VPN 사용자가 로그인합니다.
2. ASA는 iPEP 노드(ISE)에 요청을 보냅니다.
3. iPEP는 요청을 재작성하고(iPEP 인증임을 나타내기 위해 Cisco AV-PAIR 특성을 추가) 요청을 ISE 정책 노드(PDP)에 보냅니다.
4. PDP는 NAD로 전달될 iPEP에 다시 회신합니다.
5. 사용자가 인증된 경우 NAD는 어카운팅 시작 요청을 보내야 합니다(CSCtz84826 참조). 이렇게 하면 iPEP에서 세션 시작이 트리거됩니다.이 단계에서는 사용자가 상태를 위해 리디렉션됩니다.또한 ISE는 radius 어카운팅에서 특성 framed-ip 주소를 가질 것으로 예상하므로 WEBVPN 포털에서 설정된 터널에 대해 interim-accounting-update를 활성화해야 합니다.그러나 포털에 연결할 때 터널이 설정되지 않았기 때문에 클라이언트의 VPN IP 주소를 아직 알 수 없습니다.그러면 ASA가 터널 설정 시기 등 임시 업데이트를 보낼 수 있습니다.
6. 사용자는 상태 평가를 거치고, 결과에 따라 PDP는 iPEP의 CoA를 사용하여 세션을 업데이트합니다.

이 스크린샷은 다음 프로세스를 보여줍니다.


Inline PEP Client Authorization Flow
VPN client
ASA VPN
IPEP
PDP/PAP/MNT
Enterprise LAN
WWW
VPN Connect
RADIUS Access Request
Protocol Negotiation & auth handshake
Radius Accept triggers IPEP Radius proxy to initiate getting an IPEP profile to apply for this session at the IPEP itself
RADIUS Access Accept
Profile can have url-redirect and dACL name
Access Req (Authz Only)
Access Accept (Profile)
dACL download, if dACL not already downloaded
Access Req (dACL name)
dACL: Allow access to CP and Posture services. Also remediation servers/WWW can be allowed right away.
Access Accept (dACL content)
Install dACL locally
Learn endpoint IP from Acct Start and associate it to the installed dACL
Accounting Start (IP addr)
Client traffic starts coming: http://hr.app.wsj.com
URL redirect of http to :8443
Restricted Traffic: Client Provisioning
Restricted Traffic: Posture & Remediation
Endpoint/Client found fully compliant
Profile has dACL name
CoA (Profile)
dACL download, if dACL not already downloaded
Access Req (dACL name)
Access Accept (dACL content)
Install dACL locally and associate to the client IP
Full Access
64

토폴로지 예



ASA 컨피그레이션

ASA 구성은 간단한 IPSEC 원격 VPN입니다.

```
!
interface Ethernet0/0
nameif ISE
security-level 50
ip address 192.168.102.253 255.255.255.0
!
interface Ethernet0/1
nameif outside
security-level 0
ip address 10.48.39.236 255.255.255.0
!
access-list split extended permit ip 192.168.0.0 255.255.0.0 any
!
aaa-server ISE protocol radius
interim-accounting-update
!--- Mandatory if tunnel established from WEBVPN Portal aaa-server ISE (ISE) host
192.168.102.254 !--- this is the iPEP IP key cisco crypto ipsec transform-set TS1 esp-aes esp-
sha-hmac crypto ipsec security-association lifetime seconds 28800 crypto ipsec security-
association lifetime kilobytes 4608000 crypto dynamic-map DMAP1 10 set transform-set TS1 crypto
dynamic-map DMAP1 10 set reverse-route crypto map CM1 10 ipsec-isakmp dynamic DMAP1 crypto map
CM1 interface outside crypto isakmp enable outside crypto isakmp policy 1 authentication pre-
share encryption aes hash sha group 2 lifetime 86400 ! ip local pool VPN 192.168.5.1-
```

```
192.168.5.100 ! group-policy DfltGrpPolicy attributes dns-server value 192.168.101.3 !--- The
VPN User needs to be able to resolve the CN from the !--- ISE HTTPS Certificate (which is sent
in the radius response) vpn-tunnel-protocol IPSec svc webvpn split-tunnel-policy tunnelspecified
split-tunnel-network-list value split address-pools value VPN ! tunnel-group cisco general-
attributes address-pool VPN authentication-server-group ISE accounting-server-group ISE !---
Does not work without this (see introduction) ! tunnel-group cisco ipsec-attributes pre-shared-
key cisco ! route outside 0.0.0.0 0.0.0.0 10.48.39.5 1 route ISE 192.168.0.0 255.255.0.0
192.168.102.254 1 !--- You need to make sure the traffic to the local subnets !--- are going
through the inline ISE !
```

ISE 컨피그레이션

iPEP 컨피그레이션

첫 번째 작업은 iPEP 노드로 ISE를 추가하는 것입니다.이 프로세스에 대한 추가 정보는 여기에서 확인할 수 있습니다.

http://www.cisco.com/en/US/docs/security/ise/1.1/user_guide/ise_ipep_deploy.html#wp1110248

이는 기본적으로 다양한 탭에서 구성해야 하는 작업입니다(이 섹션에서 제공하는 스크린샷은 다음과 같습니다).

- 신뢰할 수 없는 IP 및 전역 IP 설정을 구성합니다(이 경우 신뢰할 수 없는 IP는 192.168.102.254).
- 구축은 라우팅 모드입니다.
- ASA가 iPEP 상자를 통과할 수 있도록 정적 필터를 설치합니다(그렇지 않으면 ISE를 통해 iPEP 상자를 통해 ISE에 대한/의 연결이 끊김).
- 정책 ISE를 Radius 서버로 구성하고 ASA를 Radius 클라이언트로 구성합니다.
- ASA를 가리키는 VPN 서브넷에 경로를 추가합니다.
- 모니터링 ISE를 로깅 호스트(기본적으로 포트 20514,이 경우 정책 ISE도 모니터링 중입니다.)

중요한 인증서 구성 요구 사항:

iPEP 노드를 등록하기 전에 다음 인증서 확장 키 사용 요구 사항이 충족되었는지 확인합니다.iPEP 및 관리 노드에서 인증서가 제대로 구성되지 않은 경우 등록 프로세스가 완료됩니다.그러나 iPEP 노드에 대한 관리자 액세스 권한은 잃게 됩니다.다음 세부사항은 ISE 1.1.x iPEP 구축 가이드에서 추정한 것입니다.

관리 및 인라인 상태 노드의 로컬 인증서에 특정 특성 조합이 있으면 상호 인증이 작동하지 않을 수 있습니다.

특성은 다음과 같습니다.

- EKU(Extended Key Usage) - 서버 인증
- EKU(Extended Key Usage) - 클라이언트 인증
- Netscape Cert Type - SSL 서버 인증
- Netscape Cert Type - SSL 클라이언트 인증

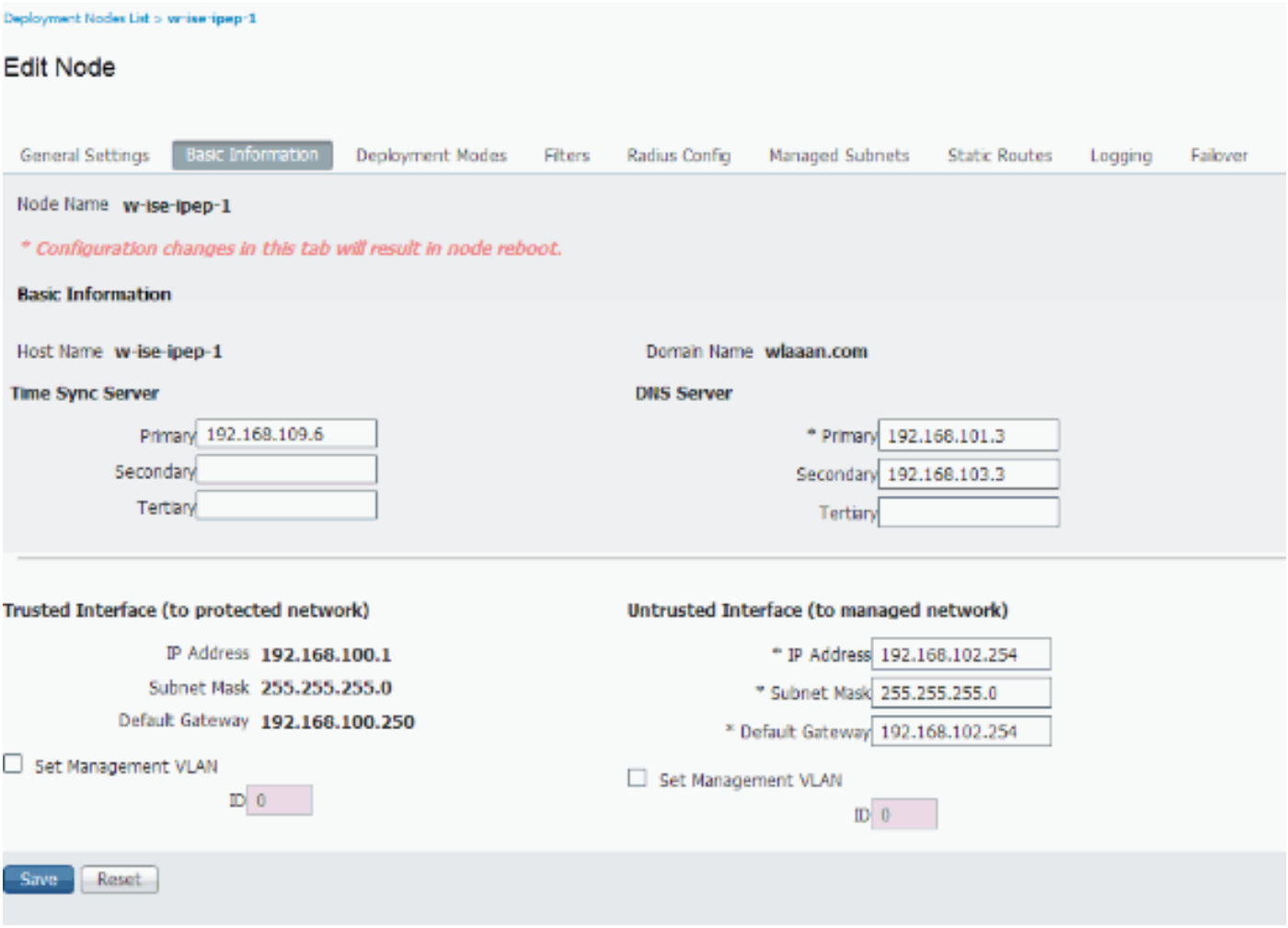
관리 인증서에 다음 조합 중 하나가 필요합니다.

- Inline Posture 인증서에서 두 EKU 특성이 모두 비활성화된 경우 두 EKU 특성을 모두 비활성화하거나, 서버 특성이 Inline Posture 인증서에서 활성화된 경우 두 EKU 특성을 모두 활성화해야 합니다.
- 두 Netscape Cert Type 특성을 모두 비활성화하거나 둘 다 활성화해야 합니다.

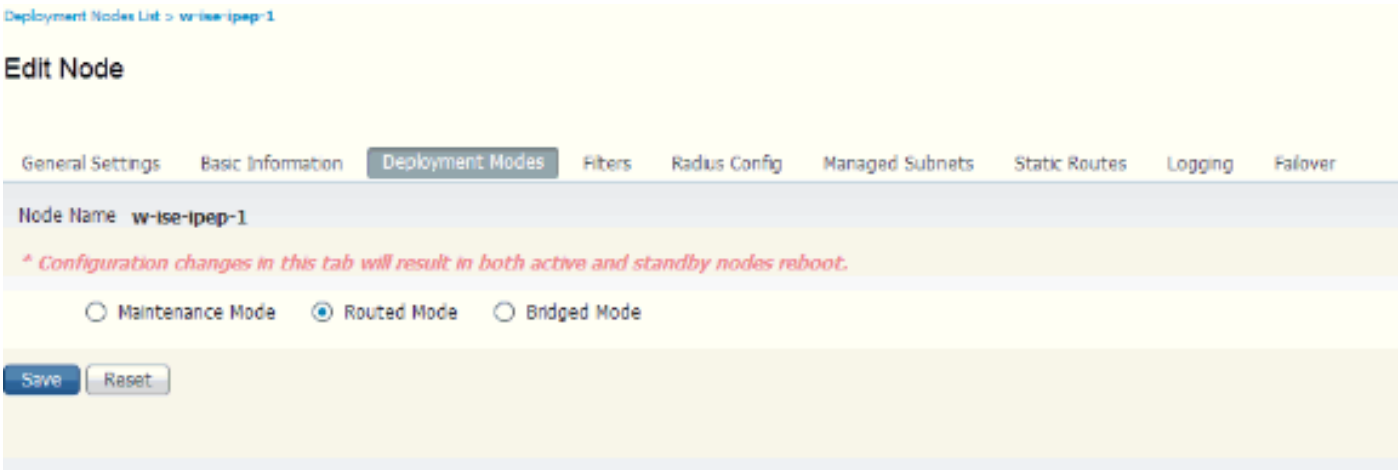
인라인 상태 인증서에 다음 조합 중 하나가 필요합니다.

- 두 EKU 특성을 모두 비활성화하거나 둘 다 활성화하거나 서버 특성만 활성화해야 합니다.
- 두 Netscape Cert Type 특성을 모두 비활성화하거나 둘 다 활성화하거나 서버 특성만 활성화해야 합니다.
- Administration(관리) 및 Inline Posture(인라인 포스처) 노드에서 자체 서명 된 로컬 인증서를 사용 하는 경우, 인라인 포스처 노드의 신뢰 목록에 관리 노드의 자체 서명 된 인증서를 설치 해야 합니다.또한 구축에 기본 및 보조 관리 노드가 모두 있는 경우, 인라인 상태 노드의 신뢰 목록에 관리 노드 둘 다의 자체 서명 인증서를 설치해야 합니다.
- CA 서명 로컬 인증서가 관리 및 인라인 상태 노드에서 사용 되는 경우 상호 인증이 올바르게 작동해야 합니다.이 경우 등록 전에 서명 CA의 인증서가 관리 노드에 설치되고 이 인증서는 인라인 상태 노드에 복제 됩니다.
- CA에서 발급한 키가 관리 및 인라인 상태 노드 간의 통신을 보호하는 데 사용되는 경우, 인라인 상태 노드를 등록 하기 전에 관리 노드에서 CA 인증서 (공개 키) 를 인라인 상태 노드의 CA 인증서 목록에 추가 해야 합니다.

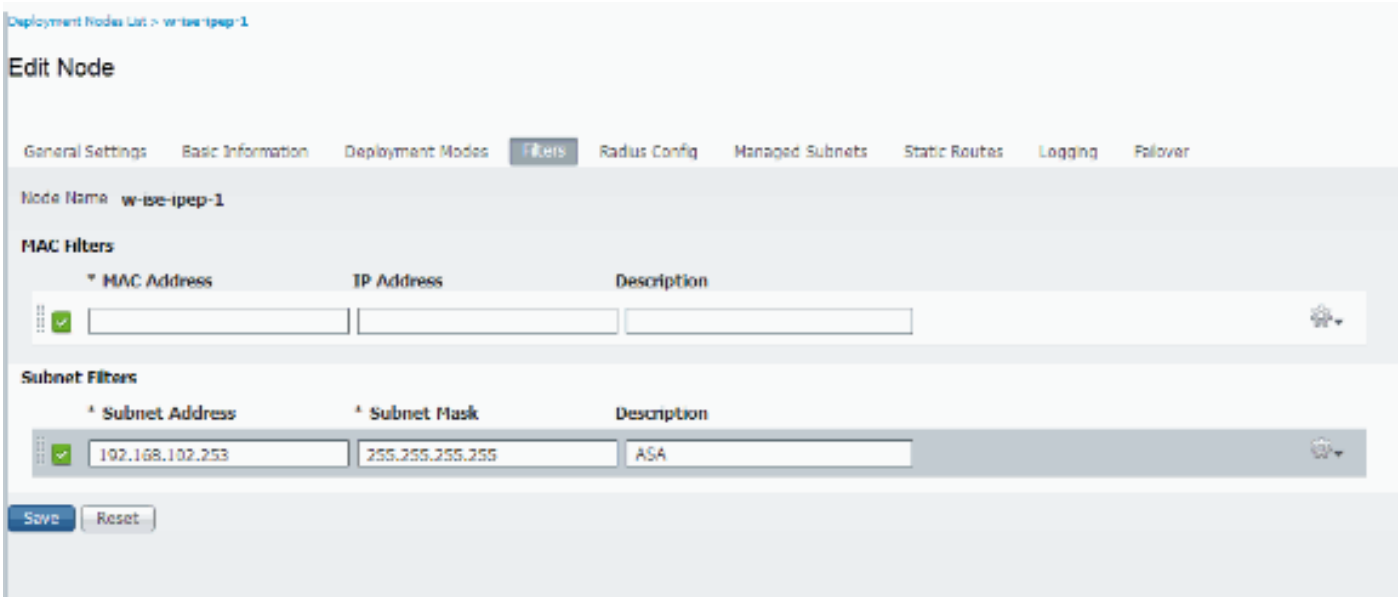
기본 구성:



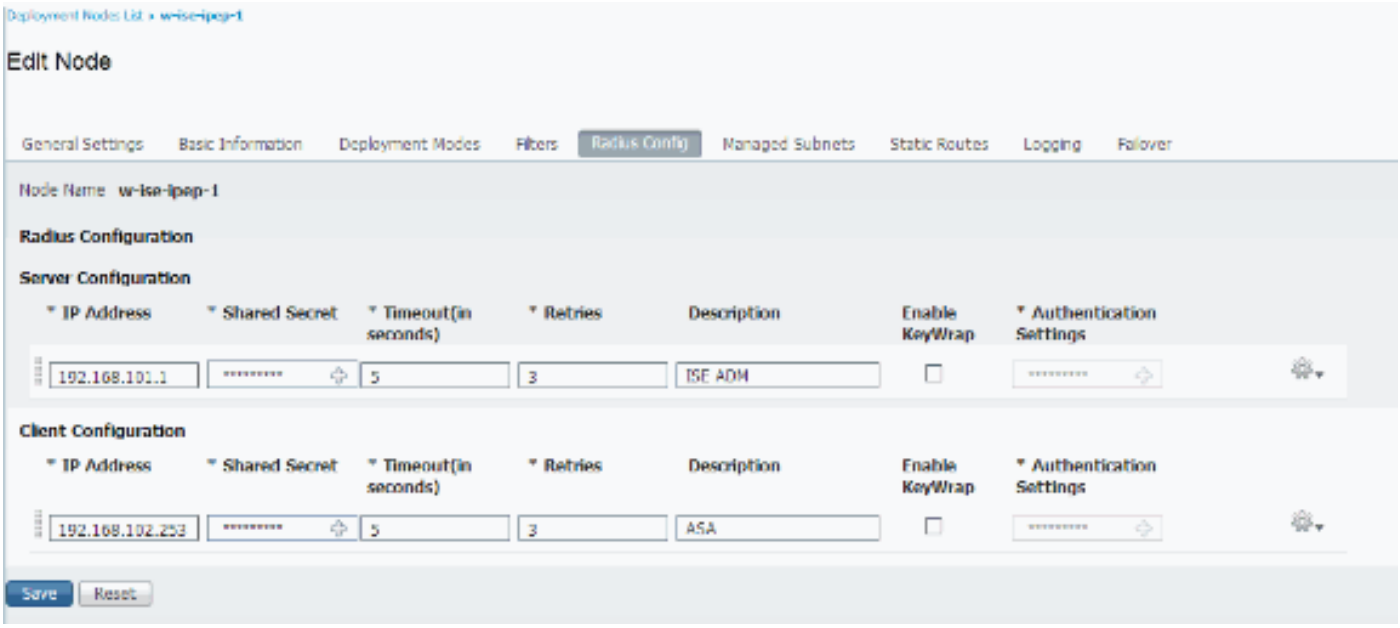
배포 모드 구성:



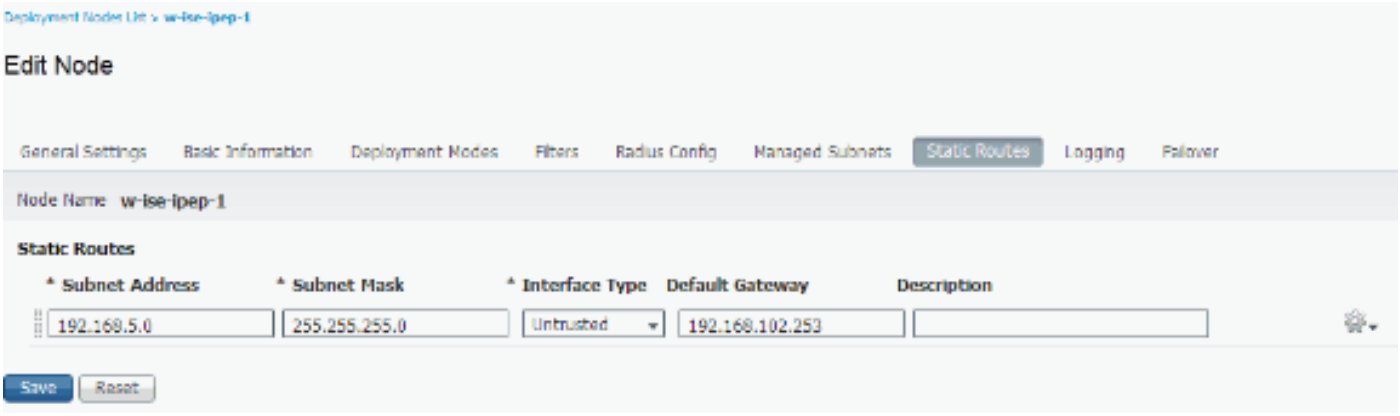
필터 구성:



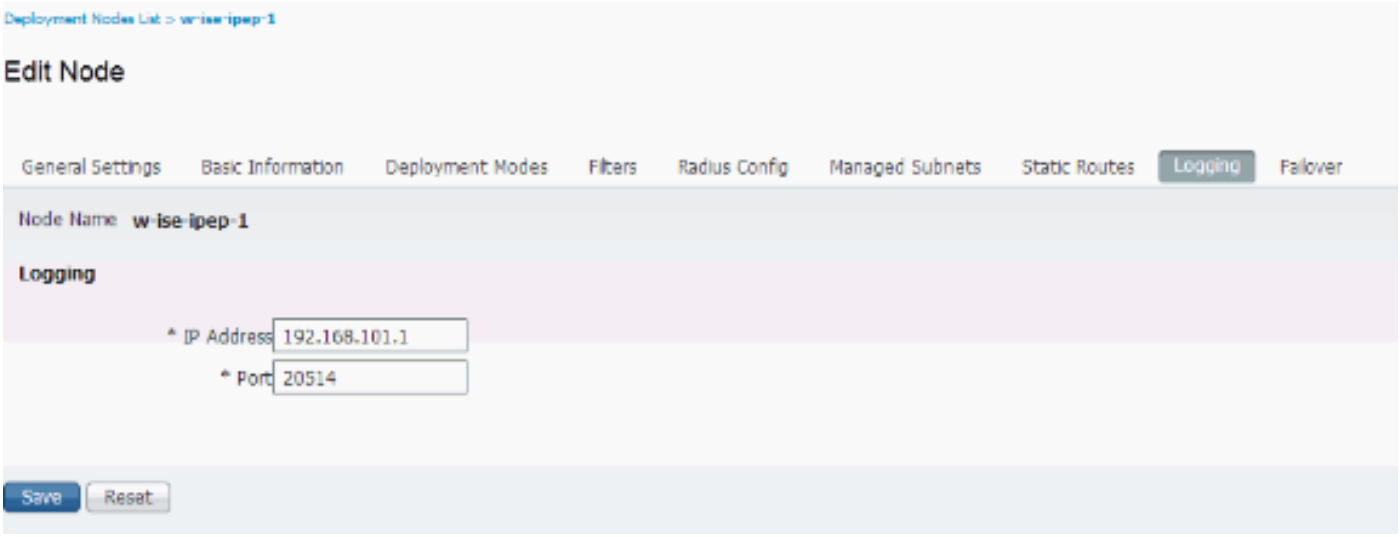
RADIUS 구성:



고정 경로:



로깅:



인증 및 상태 구성

3가지 상태 상태가 있습니다.

- 알 수 없음:상태가 아직 설정되지 않았습니다.
- 규정 준수:상태가 설정되고 시스템이 규정 준수
- 비준수:상태가 설정되었지만 시스템이 하나 이상의 검사에 실패했습니다.

이제 권한 부여 프로파일을 생성해야 합니다(인라인 권한 부여 프로파일:이렇게 하면 차이점 케이스에 사용할 ipep-authz=true 특성이 Cisco AV-Pair에 추가됩니다.

일반적으로 Unknown 프로필은 사용자의 트래픽을 ISE에 전달하여 NAC Agent를 설치하도록 요청하는 리디렉션 URL(포스처 검색)을 반환합니다.NAC Agent가 이미 설치된 경우 HTTP Discovery 요청을 ISE로 전달할 수 있습니다.

이 프로파일에서 ISE 및 DNS에 대한 HTTP 트래픽을 적어도 허용하는 ACL이 사용됩니다.

Compliant 및 Non-compliant 프로파일은 일반적으로 다운로드 가능한 ACL을 반환하여 사용자 프로필에 따라 네트워크 액세스를 부여합니다.규정을 준수하지 않는 프로필은 사용자가 웹 서버에 액세스하여 안티바이러스(예: 안티바이러스)를 다운로드하거나 제한된 네트워크 액세스 권한을 부여할 수 있습니다.

이 예에서는 알 수 없음 및 호환 프로파일이 생성되고 요구 사항에 따라 notepad.exe가 있는지 확인합니다.

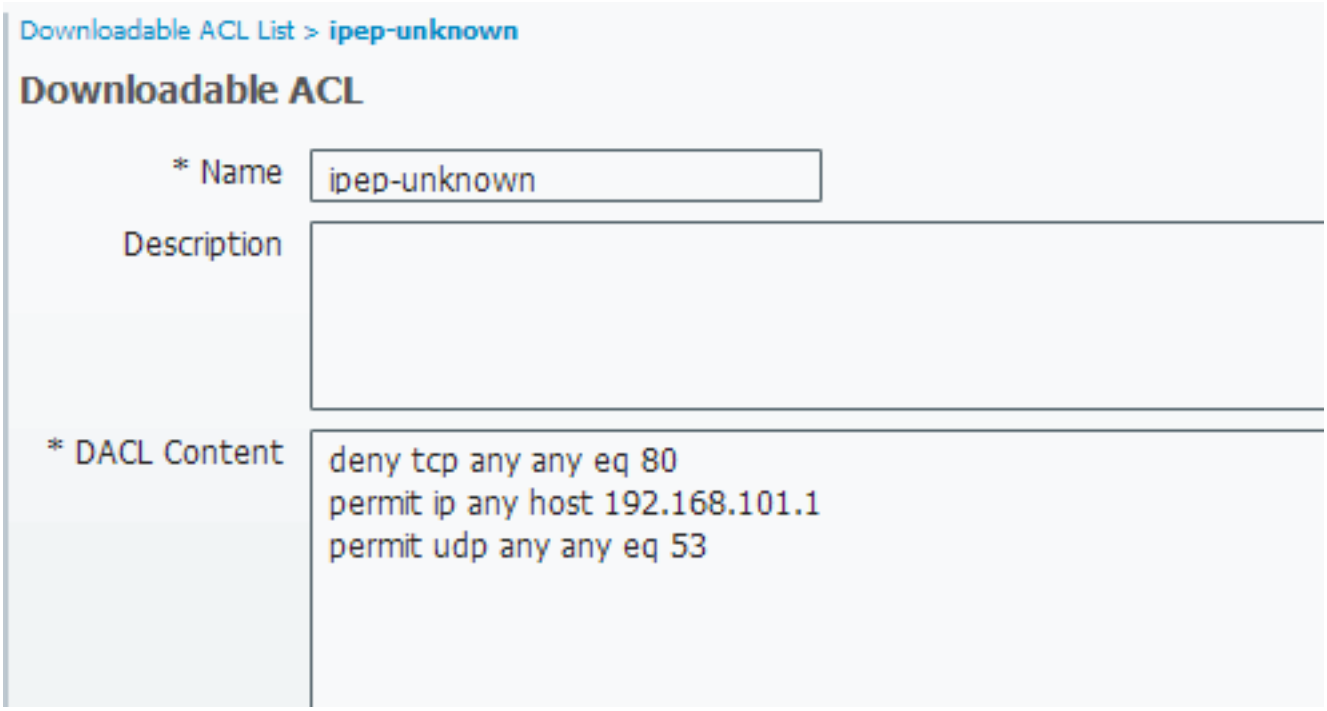
상태 프로파일 컨피그레이션

먼저 dACL(Downloadable ACL) 및 프로파일을 생성하는 것이 좋습니다.

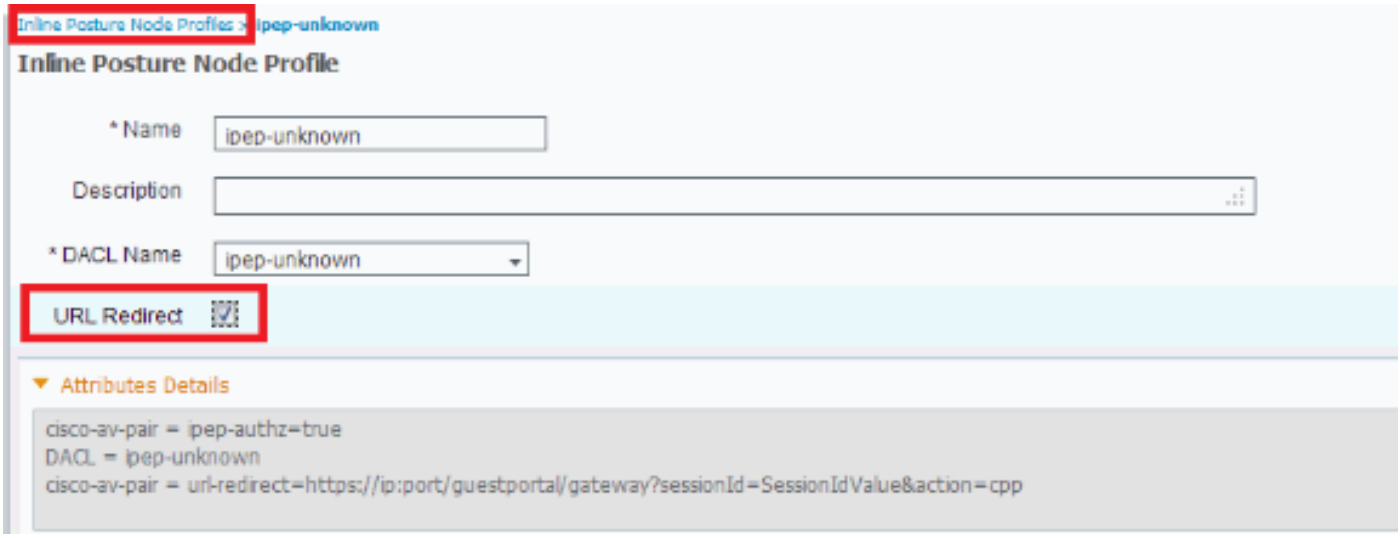
참고: 프로필 이름과 일치하는 dACL 이름을 가져야 하는 것은 아닙니다.

- 규정 준수ACL:알 수 없음권한 부여 프로파일:알 수 없음
- 비준수ACL:ipep 비준수권한 부여 프로파일:ipep 비준수

알 수 없는 dACL:

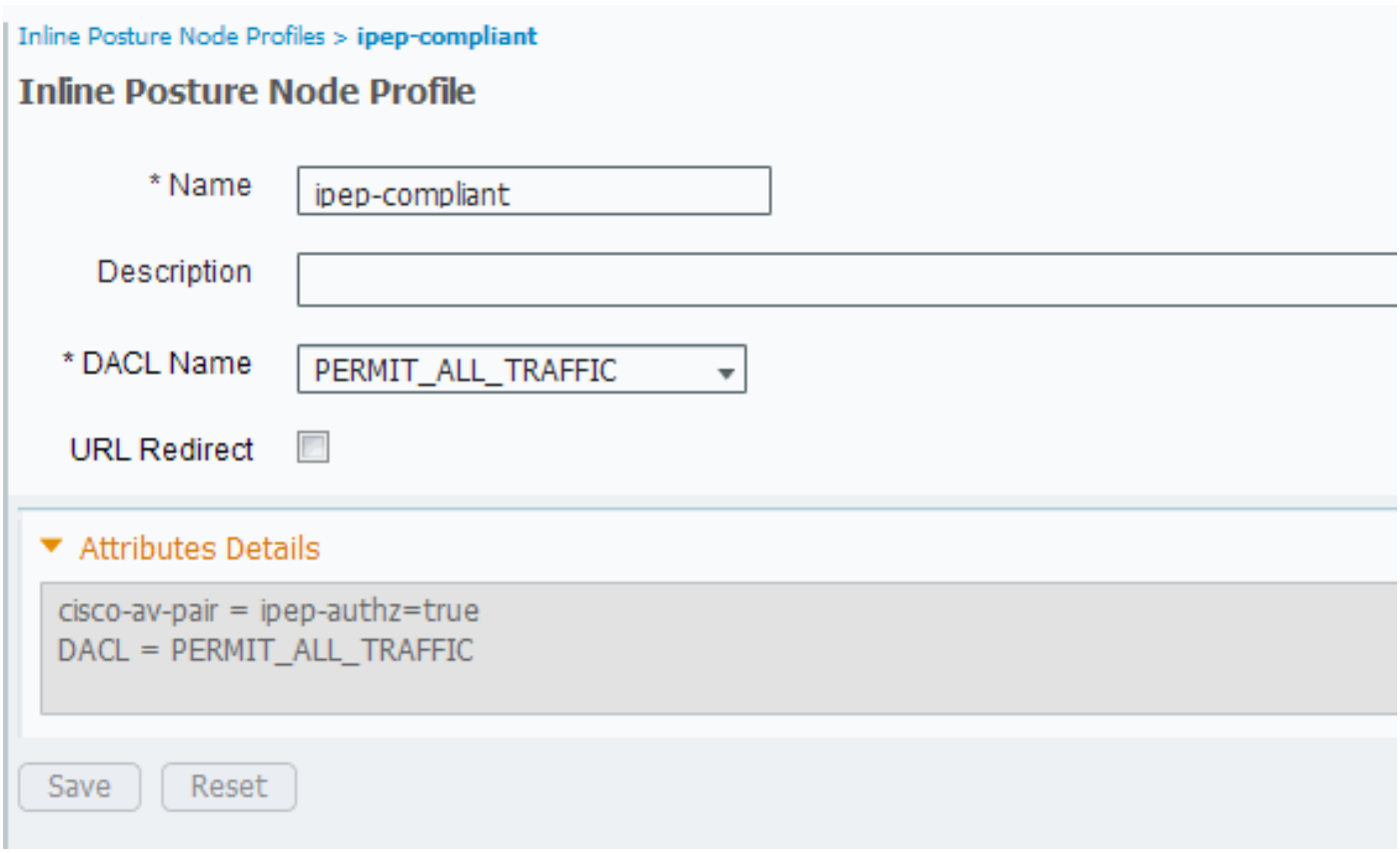


알 수 없는 프로필:



호환 dACL:

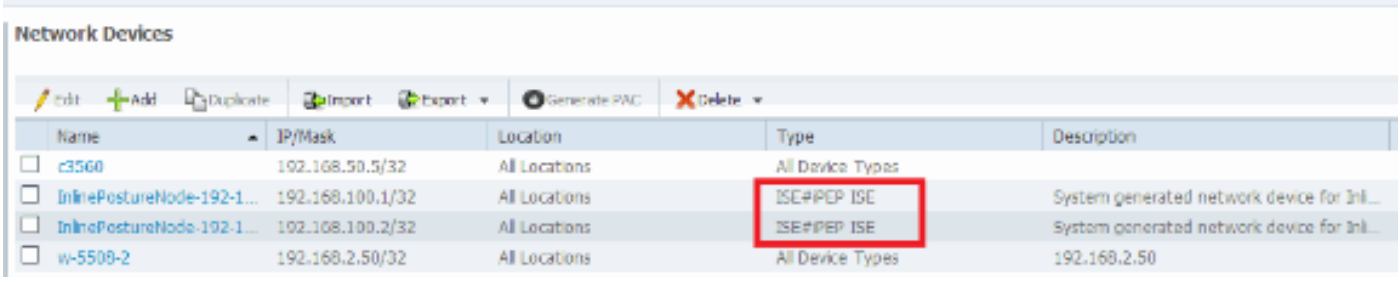
호환 프로필:



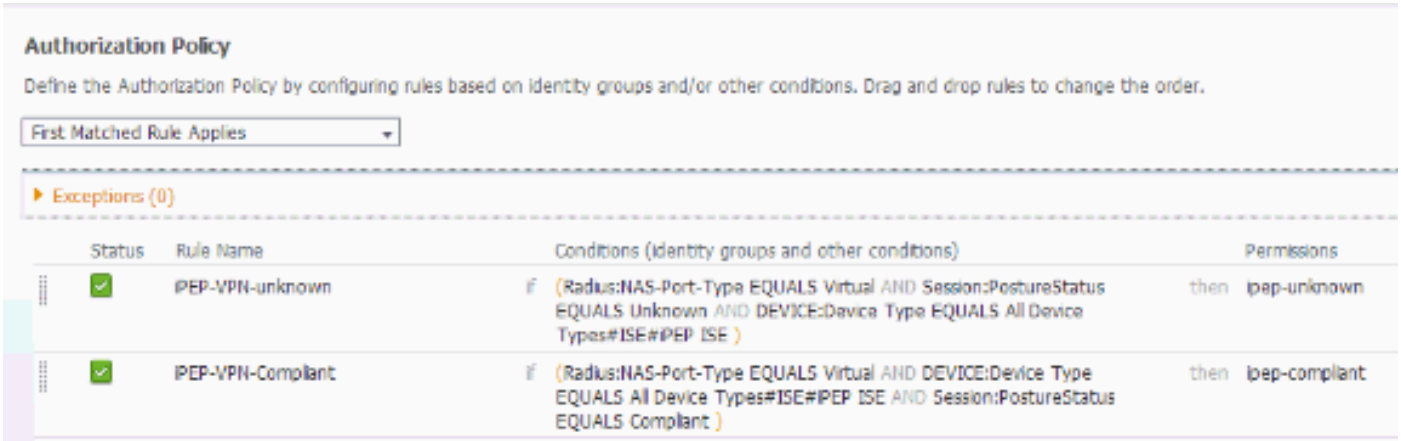
권한 부여 구성

이제 프로파일이 생성되었으므로 iPEP에서 수신되는 Radius 요청과 일치시키고 올바른 프로파일에 적용해야 합니다.iPEP ISE는 권한 부여 규칙에서 사용될 특수 장치 유형으로 정의됩니다.

NAD:

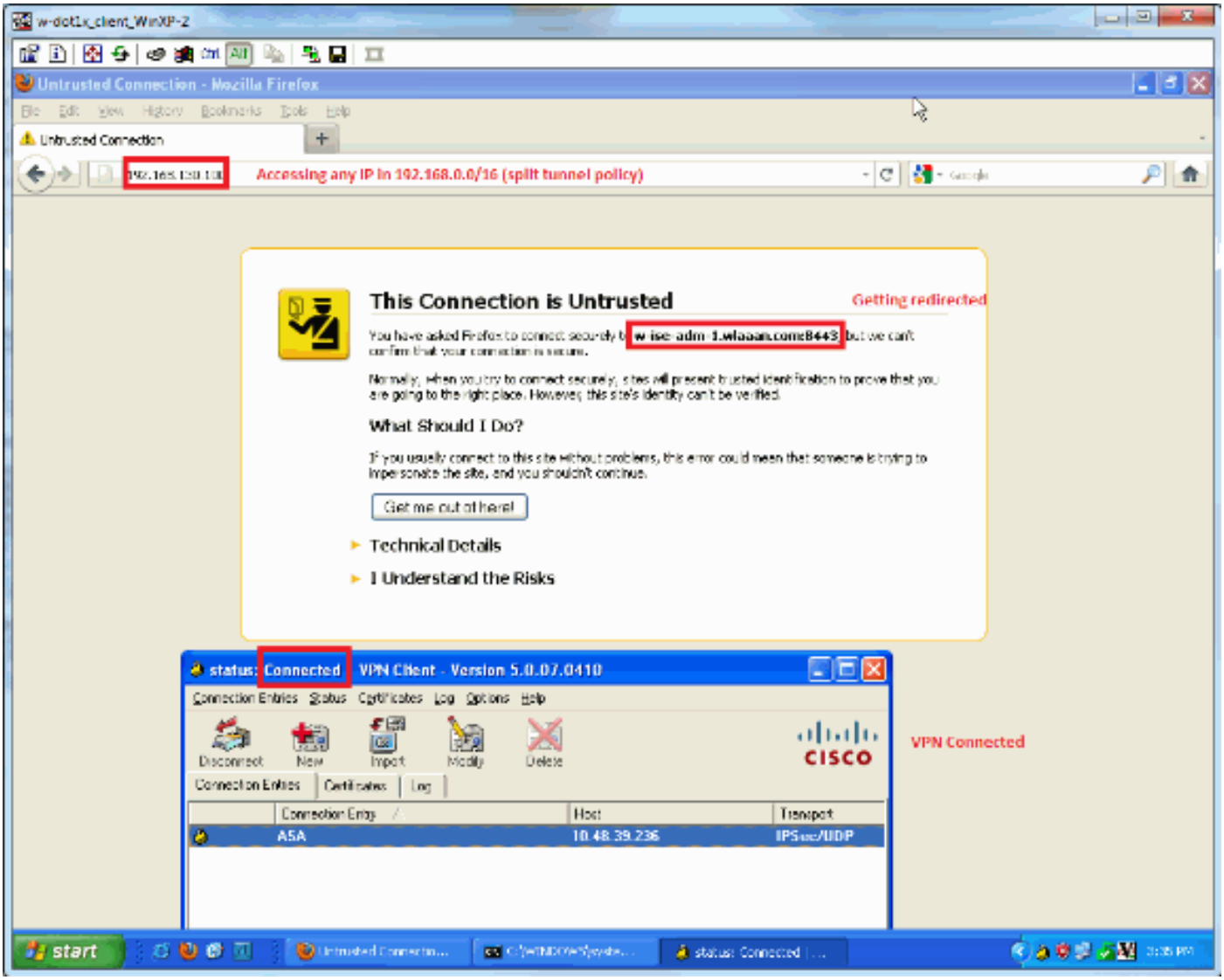


권한 부여:

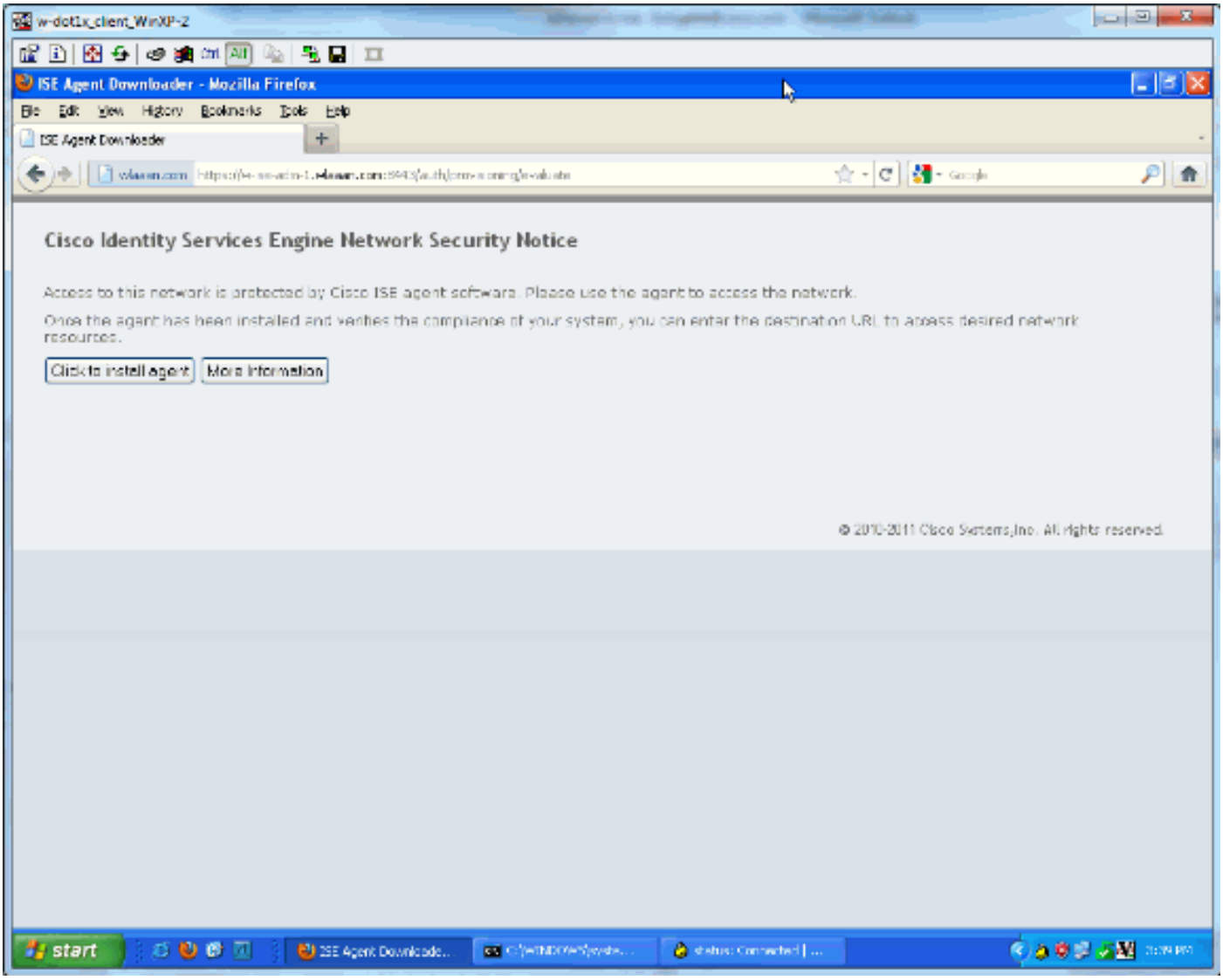


참고: 에이전트가 시스템에 설치되어 있지 않으면 클라이언트 프로비저닝 규칙을 정의할 수 있습니다.

결과



에이전트를 설치하라는 메시지가 표시됩니다(이 예에서는 클라이언트 프로비저닝이 이미 설정되어 있음).



이 단계의 일부 출력:

```
ciscoasa# show vpn-sessiondb remote

Session Type: IPsec
Username     : cisco                  Index        : 26
Assigned IP  : 192.168.5.2            Public IP    : 10.48.39.134
Protocol     : IKE IPsec
License      : IPsec
Encryption   : AES128                 Hashing      : SHA1
Bytes Tx     : 143862                 Bytes Rx     : 30628
Group Policy : DfltGrpPolicy          Tunnel Group : cisco
Login Time   : 13:43:55 UTC Mon May 14 2012
Duration     : 0h:09m:37s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

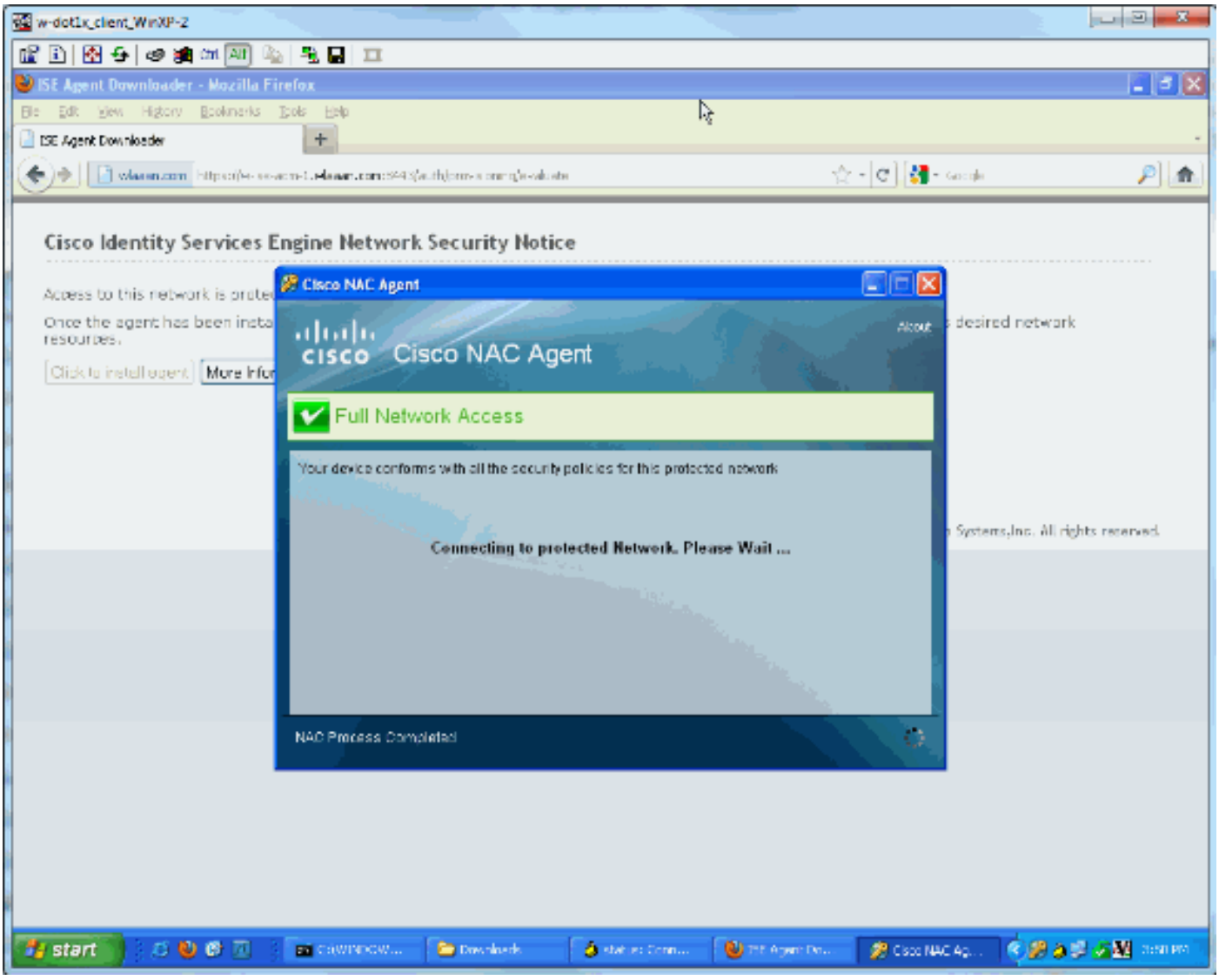
iPEP에서

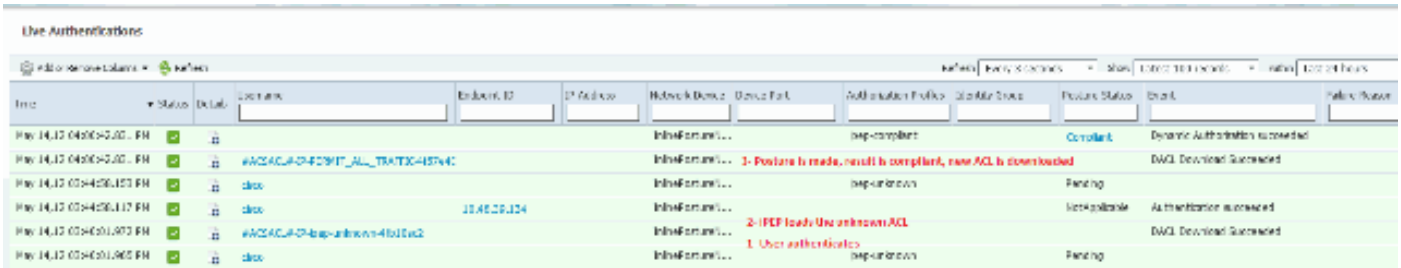
```
w-ise-ipep-1/admin# show pep table session

Current Sessions (IP, MAC(if available), Profile ID, VLAN (if any)):
192.168.5.2 00:00:00:00:00:00 2 0
w-ise-ipep-1/admin# show pep table accesslist normal
#ACSACL#-IP-ipep-unknown-4fb10ac2:
```

```
deny tcp any host 192.168.101.1 eq 80
deny tcp any host 192.168.101.1 eq 443
permit ip any host 192.168.101.1
permit udp any any eq 53
```

에이전트를 다운로드하고 설치한 후:

에이전트는 자동으로 ISE를 탐지하고 포스처 평가를 실행해야 합니다(다른 주제인 포스처 규칙이 이미 정의되어 있다고 가정). 이 예에서 상태는 성공적이며 다음과 같이 나타납니다.





참고: 위 스크린샷에는 두 가지 인증이 있습니다.그러나 iPEP 상자는 ACL을 캐시하므로 매번 다운로드되지 않습니다.

iPEP:

```
w-ise-ipep-1/admin# show pep table session
```

```
Current Sessions (IP, MAC(if available), Profile ID, VLAN (if any)):
192.168.5.2 00:00:00:00:00:00 3 0
w-ise-ipep-1/admin# show pep table accesslist normal
#ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f57e406:
permit ip any any

#ACSACL#-IP-ipep-unknown-4fb10ac2:
deny tcp any host 192.168.101.1 eq 80
deny tcp any host 192.168.101.1 eq 443
permit ip any host 192.168.101.1
permit udp any any eq 53
w-ise-ipep-1/admin#
```

관련 정보

- 기술 지원 및 문서 – Cisco Systems