

ISE Posture 리디렉션 플로우를 ISE Posture 리디렉션 플로우와 비교 Redirectionless Flow

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[Posture Flow Pre ISE 2.2](#)

[ISE 2.2 이후 상태 흐름](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[클라이언트 프로비저닝 컨피그레이션](#)

[상태 정책 및 조건](#)

[클라이언트 프로비저닝 포털 구성](#)

[권한 부여 프로파일 및 정책 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[일반 정보](#)

[일반적인 문제 해결](#)

[SSO 관련 문제](#)

[클라이언트 프로비저닝 정책 선택 문제 해결](#)

[상태 프로세스 트러블슈팅](#)

소개

이 문서에서는 ISE 2.2 이상 버전에서 지원되는 상태 리디렉션 흐름과 이전 ISE 버전 이후 지원되는 상태 리디렉션 흐름의 비교에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE의 상태 흐름
- ISE의 상태 구성 요소 구성
- VPN(Virtual Private Networks)을 통한 보안 상태 확인을 위한 ASA(Adaptive Security Appliance) 컨피그레이션

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 버전 2.2
- Cisco ASAv with software 9.6(2)


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

배경 정보

이 문서에서는 ISE가 NAD(Network Access Device) 또는 ISE에서 어떤 종류의 리디렉션 지원도 없이 포스처 플로우를 지원할 수 있도록 ISE(Identity Service Engine) 2.2에 도입된 새로운 기능에 대해 설명합니다.

Posture는 Cisco ISE의 핵심 구성 요소입니다. 구성 요소로서의 Posture는 세 가지 주요 요소로 나뉠 수 있습니다.

1. ISE를 정책 컨피그레이션 배포 및 결정 지점으로 사용합니다.
ISE에 대한 관리자 관점에서 포스처 정책(디바이스를 기업 규정 준수로 표시하려면 어떤 정확한 조건을 충족해야 함), 클라이언트 프로비저닝 정책(어떤 유형의 디바이스에 어떤 에이전트 소프트웨어를 설치해야 하는지), 권한 부여 정책(포스처 상태에 따라 어떤 유형의 권한을 할당해야 하는지)을 구성합니다.
2. 정책 시행 지점으로서의 네트워크 액세스 디바이스.
NAD 측에서는 사용자 인증 시 실제 권한 부여 제한이 적용됩니다. 정책 포인트로 ISE는 dACL(Downloaded ACL)/VLAN/Redirect-URL/Redirect ACL(Access Control List) 등의 권한 부여 매개변수를 제공합니다. 전통적으로 포스처가 발생하려면 NAD가 리디렉션(ISE 노드가 연결되어야 하는 사용자 또는 에이전트 소프트웨어에 지시하기 위해) 및 CoA(Change of Authorization)를 지원하여 엔드포인트의 포스처 상태가 결정된 후 사용자를 재인증해야 합니다.
3. 에이전트 소프트웨어를 데이터 수집 및 최종 사용자와의 상호 작용 지점으로 사용합니다.
Cisco ISE는 AnyConnect ISE Posture Module, NAC Agent 및 Web Agent의 세 가지 유형의 에이전트 소프트웨어를 사용합니다. 에이전트는 ISE로부터 포스처 요구 사항에 대한 정보를 수신하고 요구 사항의 상태에 대한 보고서를 ISE에 제공합니다.

 참고: 이 문서는 리디렉션 없이 상태를 완전히 지원하는 유일한 Anyconnect ISE Posture Module을 기반으로 합니다.

ISE 2.2 이전 흐름 상태에서 NAD는 사용자를 인증하고 액세스를 제한하는 데 사용될 뿐만 아니라, 연락해야 하는 특정 ISE 노드에 대한 정보를 에이전트 소프트웨어에 제공하는 데 사용됩니다. 리디렉션 프로세스의 일부로 ISE 노드에 대한 정보가 에이전트 소프트웨어로 반환됩니다.

과거에는 NAD 또는 ISE 측에서 리디렉션 지원이 상태 구현에 필수적인 요건이었습니다. ISE 2.2에서는 초기 클라이언트 프로비저닝 및 포스터 프로세스 모두에 대해 리디렉션을 지원해야 하는 요구 사항이 제거됩니다.

리디렉션 없이 클라이언트 프로비저닝 - ISE 2.2에서는 포털 FQDN(Fully Qualified Domain Name)을 통해 CPP(Client Provisioning Portal)에 직접 액세스할 수 있습니다. 이는 스폰서 포털 또는 내 디바이스 포털에 액세스하는 방법과 유사합니다.

리디렉션이 없는 포스터 프로세스 - CPP 포털에서 에이전트를 설치하는 동안 ISE 서버에 대한 정보가 직접 통신을 가능하게 하는 클라이언트측에 저장됩니다.

Posture Flow Pre ISE 2.2

이 그림에서는 ISE 2.2 이전의 Anyconnect ISE Posture Module 흐름에 대한 단계별 설명을 보여줍니다.

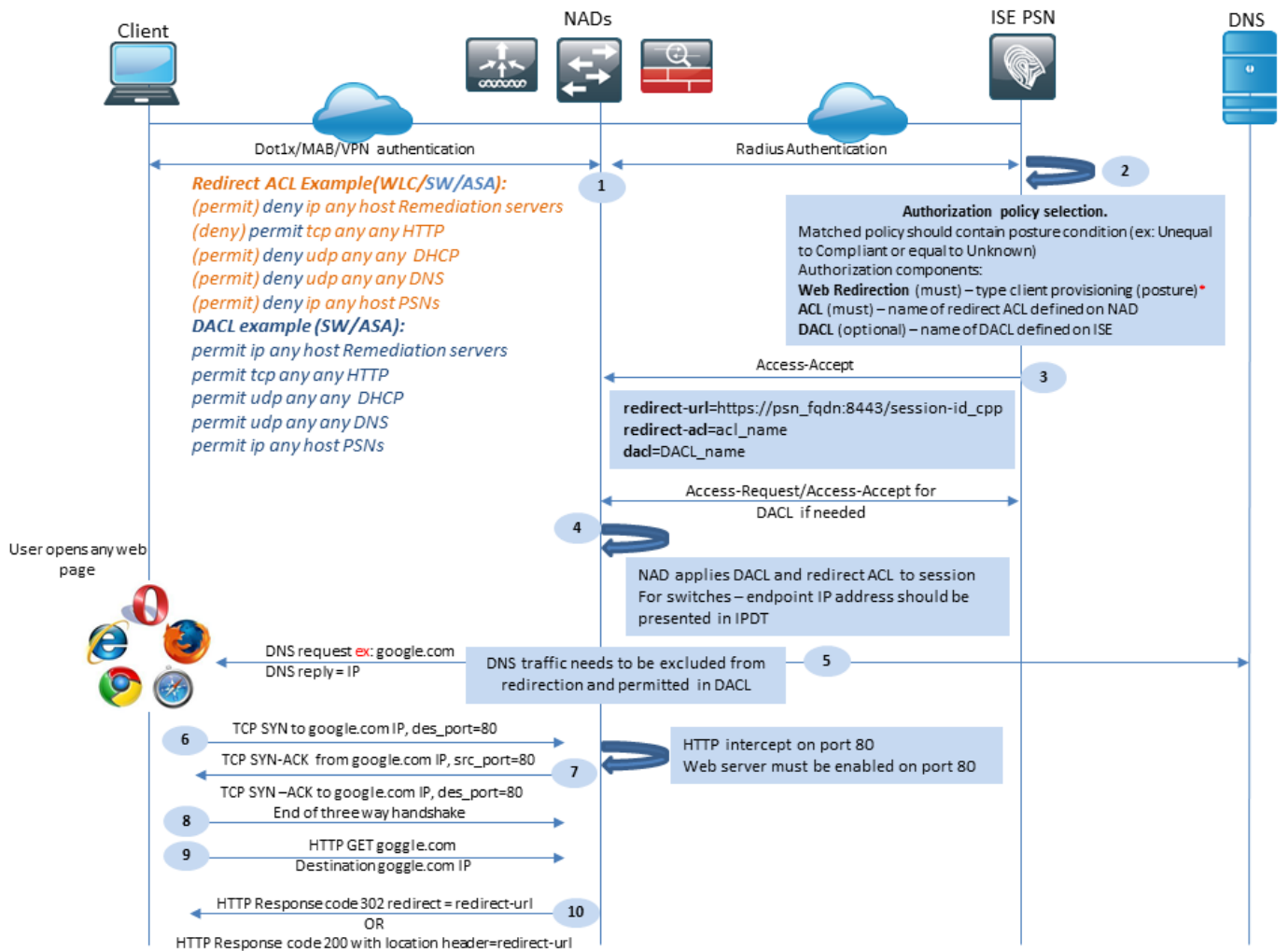


그림 1-1


1단계. 인증은 흐름의 첫 번째 단계로 dot1x, MAB 또는 VPN일 수 있습니다.

2단계. ISE는 사용자에게 대한 인증 및 권한 부여 정책을 선택해야 합니다. 포스처 시나리오에서 선택한 권한 부여 정책은 포스처 상태에 대한 참조를 포함해야 하며, 처음에는 알 수 없거나 해당 사항이 없어야 합니다. 이 두 경우를 모두 포함하기 위해, 상태 상태가 불균등한 규정준수를 갖는 조건을 사용할 수 있습니다.

선택한 권한 부여 프로파일은 리디렉션에 대한 정보를 포함해야 합니다.

- Web Redirection(웹 리디렉션) - 포스처 케이스의 경우 웹 리디렉션 유형을 클라이언트 프로 비저닝(포스처)으로 지정해야 합니다.
- ACL - 이 섹션에는 NAD측에 구성된 ACL 이름이 포함되어야 합니다. 이 ACL은 리디렉션을 우회해야 하는 트래픽과 실제로 리디렉션되어야 하는 NAD에 지시하는 데 사용됩니다.
- DACL - 리디렉션 액세스 목록과 함께 사용할 수 있지만, 여러 플랫폼이 DACL 및 리디렉션 ACL을 다른 순서로 처리한다는 점을 염두에 두어야 합니다.

예를 들어 ASA는 항상 ACL을 리디렉션하기 전에 DACL을 처리합니다. 이와 동시에 일부 스위치 플랫폼은 ASA와 동일한 방식으로 이를 처리하며, 다른 스위치 플랫폼은 먼저 Redirect ACL을 처리한 다음 트래픽이 삭제되거나 허용되어야 하는 경우 DACL/Interface ACL을 확인합니다.

 참고: 권한 부여 프로파일에서 웹 리디렉션 옵션을 활성화한 후에는 리디렉션을 위한 대상 포털을 선택해야 합니다.

3단계. ISE는 권한 부여 특성이 있는 Access-Accept를 반환합니다. 권한 부여 특성의 리디렉션 URL은 ISE에서 자동으로 생성됩니다. 여기에는 다음 구성 요소가 포함됩니다.

- 인증이 발생한 ISE 노드의 FQDN입니다. 경우에 따라 웹 리디렉션 섹션의 권한 부여 프로파일 컨피그레이션(고정 IP/호스트 이름/FQDN)에서 동적 FQDN을 덮어쓸 수 있습니다. 고정 값을 사용하는 경우 인증이 처리된 동일한 ISE 노드를 가리켜야 합니다. 로드 밸런서(LB)의 경우 이 FQDN은 LB VIP를 가리킬 수 있지만 LB가 Radius 및 SSL 연결을 연결하도록 구성된 경우에만 가능합니다.
- Port(포트) - 포트 값은 대상 포털 컨피그레이션에서 가져옵니다.
- 세션 ID - 이 값은 ISE에서 Access-Request에 표시된 Cisco AV 쌍 감사 세션 ID에서 가져옵니다. 값 자체는 NAD에 의해 동적으로 생성됩니다.
- Portal ID(포털 ID) - ISE 측의 대상 포털의 식별자입니다.

4단계. NAD는 권한 부여 정책을 세션에 적용합니다. 또한 DACL이 구성된 경우 권한 부여 정책이 적용되기 전에 콘텐츠가 요청됩니다.

중요한 고려 사항:

- 모든 NADs- 장치는 Access-Accept에서 redirect-acl로 받은 것과 동일한 이름으로 로컬에서 구성된 ACL이 있어야 합니다.
- Switches(스위치) - 클라이언트의 IP 주소가 `show authentication session interface details` 명령을 사용하여 리디렉션 및 ACL을 성공적으로 적용합니다. 클라이언트 IP 주소는 IPDT(IP Device Tracking Feature)에 의해 학습됩니다.

5단계. 클라이언트는 웹 브라우저에 입력된 FQDN에 대한 DNS 요청을 보냅니다. 이 단계에서 DNS 트래픽은 리디렉션을 우회해야 하며 DNS 서버에서 올바른 IP 주소를 반환해야 합니다.

6단계. 클라이언트는 DNS 회신에서 받은 IP 주소로 TCP SYN을 보냅니다. 패킷의 소스 IP 주소는 클라이언트 IP이고 목적지 IP 주소는 요청된 리소스의 IP입니다. 클라이언트 웹 브라우저에 직접 HTTP 프록시가 구성된 경우를 제외하고 대상 포트는 80입니다.

7단계 NAD는 클라이언트 요청을 가로채고 요청된 리소스 IP와 같은 소스 IP, 클라이언트 IP와 같은 대상 IP, 80과 같은 소스 포트를 사용하여 SYN-ACK 패킷을 준비합니다.

중요한 고려 사항:

- NADs는 클라이언트가 요청을 보내는 포트에서 실행 중인 HTTP 서버가 있어야 합니다. 기본적으로 포트 80입니다.
- 클라이언트가 직접 HTTP 프록시 웹 서버를 사용하는 경우 HTTP 서버는 NAS의 프록시 포트에서 실행해야 합니다. 이 시나리오는 이 문서의 범위를 벗어납니다.
- NAD가 클라이언트에 로컬 IP 주소를 가지고 있지 않은 경우, 서브넷 SYN-ACK는 (일반적으로 관리 인터페이스를 통해) NAD 라우팅 테이블과 함께 전송됩니다. 이 시나리오에서 패킷은 L3 인프라를 통해 라우팅되며 L3 업스트림 디바이스를 통해 클라이언트로 다시 라우팅되어야 합니다. L3 디바이스가 스테이트풀 방화벽인 경우 이러한 비대칭 라우팅에 대해 추가 예외가 부여되어야 합니다.

8단계. 클라이언트가 ACK에 의해 TCP 3방향 핸드셰이크를 완료합니다.

9단계. 대상 리소스에 대한 HTTP GET은 클라이언트에 의해 전송됩니다.

10단계. NAD는 HTTP 코드 302(페이지 이동)를 사용하여 클라이언트에 리디렉션 URL을 반환합니다. 일부 NAD에서는 위치 헤더의 HTTP 200 OK 메시지 내부에서 리디렉션이 반환될 수 있습니다.

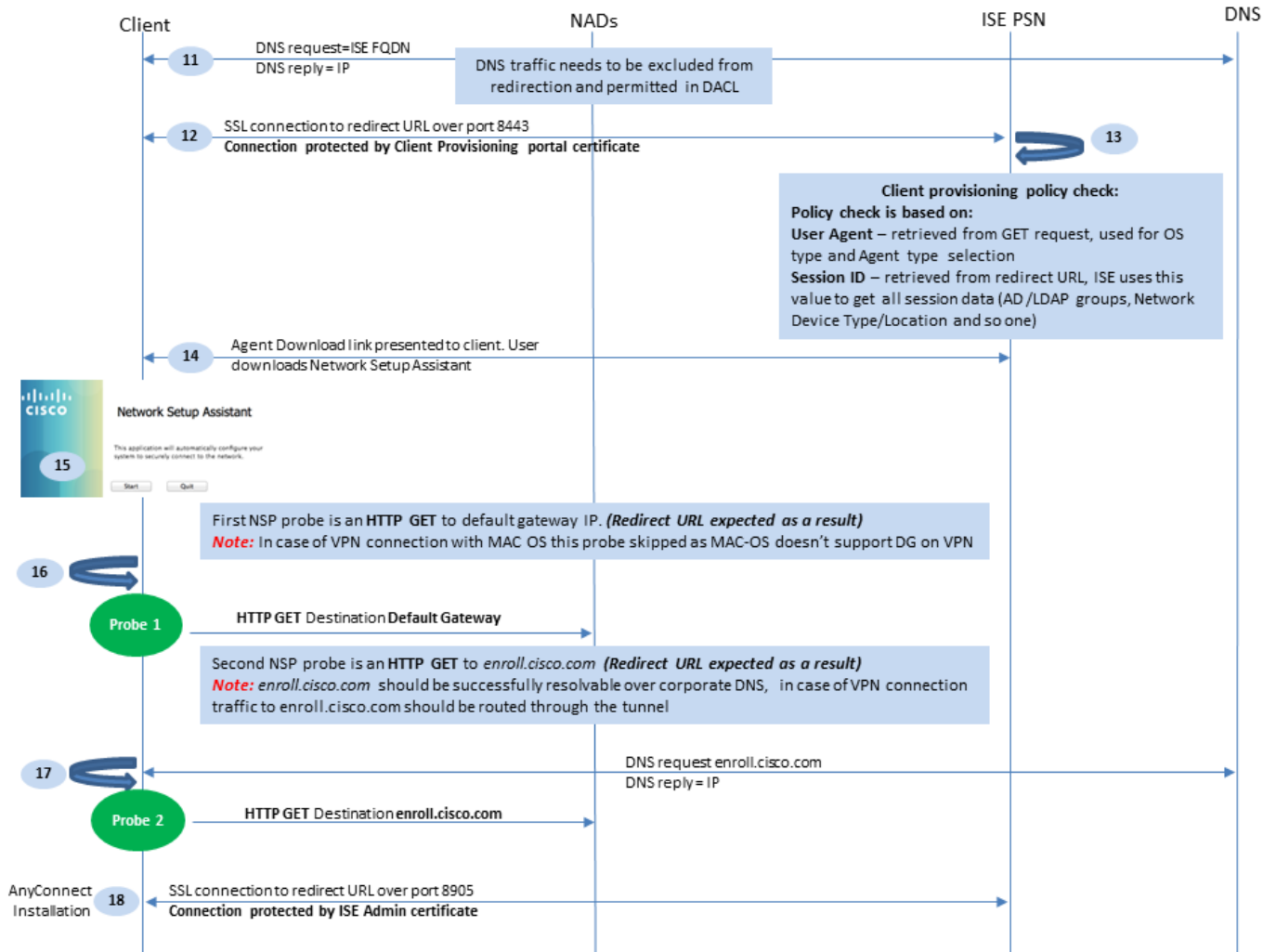



그림 1-2

11단계. 클라이언트는 리디렉션 URL에서 FQDN에 대한 DNS 요청을 보냅니다. FQDN은 DNS 서버 측에서 확인할 수 있어야 합니다.

12단계. 리디렉션 URL에서 수신된 포트를 통한 SSL 연결이 설정됩니다(기본값 8443). 이 연결은 ISE 측의 포털 인증서로 보호됩니다. CPP(Client Provisioning Portal)가 사용자에게 표시됩니다.


13단계 클라이언트에 다운로드 옵션을 제공하기 전에 ISE가 대상 클라이언트 프로비저닝(CP) 정책을 선택해야 합니다. 브라우저 사용자 에이전트에서 탐지된 클라이언트의 운영 체제(OS) 및 CPP 정책 선택에 필요한 기타 정보는 인증 세션(예: AD/LDAP 그룹 등)에서 검색됩니다. ISE는 리디렉션 URL에 표시되는 세션 ID에서 대상 세션을 인식합니다.

14단계. NSA(Network Setup Assistant) 다운로드 링크가 클라이언트로 반환됩니다. 클라이언트가 응용 프로그램을 다운로드합니다.

 참고: 일반적으로 NSA를 Windows 및 Android용 BYOD 흐름의 일부로 볼 수 있지만 이 애플리케이션은 ISE에서 Anyconnect 또는 해당 구성 요소를 설치하는 데 사용할 수도 있습니다.

15단계. 사용자가 NSA 애플리케이션을 실행합니다.

16단계. NSA는 첫 번째 검색 프로브(HTTP/auth/discovery)를 기본 게이트웨이로 전송합니다. NSA는 결과적으로 리디렉션-url을 예상한다.

 참고: MAC OS 디바이스에서 VPN을 통한 연결의 경우 MAC OS에는 VPN 어댑터에 기본 게이트웨이가 없으므로 이 프로브는 무시됩니다.

17단계. NSA는 첫 번째 프로브가 실패하면 두 번째 프로브를 보냅니다. 두 번째 프로브는 HTTP GET /auth/discovery enroll.cisco.com. 이 FQDN은 DNS 서버에서 성공적으로 확인할 수 있어야 합니다. 스플릿 터널이 있는 VPN 시나리오에서 트래픽을 enroll.cisco.com 터널을 통과해야 합니다.

18단계. 프로브가 성공하면 NSA는 redirect-url에서 얻은 정보를 사용하여 포트 8905를 통해 SSL 연결을 설정합니다. 이 연결은 ISE 관리자 인증서로 보호됩니다. 이 연결 안에서 NSA는 Anyconnect를 다운로드합니다.

중요한 고려 사항:

- ISE 2.2 릴리스 이전에는 포트 8905를 통한 SSL 통신이 포스터를 위한 요구 사항입니다.
- 인증서 경고를 방지하려면 클라이언트 측에서 포털 및 관리자 인증서를 모두 신뢰해야 합니다.
- 다중 인터페이스 ISE 구축 인터페이스에서는 G0 이외의 인터페이스를 시스템 FQDN과 다르게 FQDN에 바인딩할 수 있습니다(를 사용하는 경우). ip host CLI 명령). 이로 인해 주체 이름 (SN)/주체 대체 이름(SAN) 검증에 문제가 발생할 수 있습니다. 예를 들어 클라이언트가 인터페이스 G1에서 FQDN으로 리디렉션되는 경우 시스템 FQDN은 8905 통신 인증서의 리디렉션 URL의 FQDN과 다를 수 있습니다. 이 시나리오의 해결 방법으로 관리 인증서 SAN 필드에 추가 인터페이스의 FQDN을 추가하거나 관리 인증서에서 와일드카드를 사용할 수 있습니다.

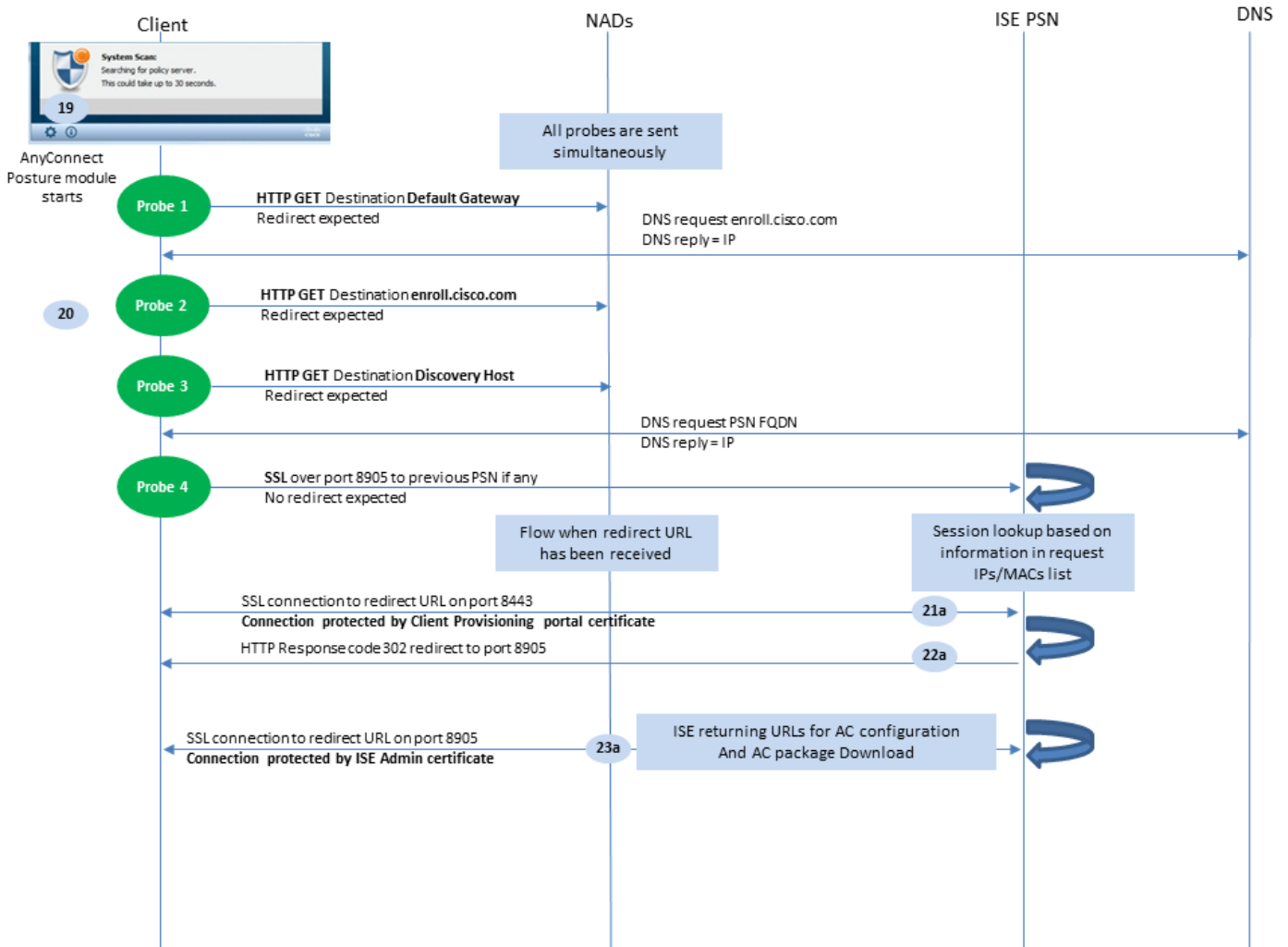


그림 1-3

19단계. Anyconnect ISE Posture 프로세스가 시작됩니다.


Anyconnect ISE Posture 모듈은 다음 상황에서 시작됩니다.

- 설치 후
- 기본 게이트웨이 값이 변경된 후
- 시스템 사용자 로그인 이벤트 후
- 시스템 전원 이벤트 후

20단계. 이 단계에서 Anyconnect ISE Posture Module은 정책 서버 탐지를 시작합니다. 이는 Anyconnect ISE Posture 모듈에서 동시에 전송되는 일련의 프로브로 수행됩니다.

- 프로브 1 - 기본 게이트웨이 IP에 대한 HTTP get /auth/discovery. MAC OS 장치에는 VPN 어댑터에 기본 게이트웨이가 없다는 것을 기억해야 합니다. 프로브에 필요한 결과는 redirect-url입니다.
- 프로브 2 - HTTP GET /auth/discovery to enroll.cisco.com. 이 FQDN은 DNS 서버에서 성공적으로 확인할 수 있어야 합니다. 스플릿 터널이 있는 VPN 시나리오에서 트래픽을 enroll.cisco.com 터널을 통과해야 합니다. 프로브에 필요한 결과는 redirect-url입니다.
- 프로브 3 - 검색 호스트에 대한 HTTP get /auth/discovery. AC Posture 프로필에서 설치하는 동안 ISE에서 검색 호스트 값이 반환됩니다. 프로브에 필요한 결과는 redirect-url입니다.

- 프로브 4 - 이전에 연결된 PSN에 대한 포트 8905의 HTTP GET /auth/status over SSL 이 요청에는 ISE 측의 세션 조회를 위한 클라이언트 IP 및 MAC 목록에 대한 정보가 포함되어 있습니다. 이 문제는 첫 번째 포스터 시도 중에는 표시되지 않습니다. ISE 관리자 인증서로 연결이 보호됩니다. 이 프로브의 결과, ISE는 프로브가 착륙한 노드가 사용자가 인증된 노드와 동일한 경우 세션 ID를 클라이언트로 다시 반환할 수 있습니다.

 참고: 이 프로브의 결과, 일부 상황에서는 리디렉션 작업 없이도 포스터를 성공적으로 수행할 수 있습니다. 리디렉션 없이 성공적인 상태를 유지하려면 세션을 인증한 현재 PSN이 이전에 성공적으로 연결된 PSN과 동일해야 합니다. ISE 2.2 이전에는 리디렉션 없이 성공적인 상태가 규칙이라기보다는 예외입니다.

다음 단계에서는 프로브 중 하나의 결과로 리디렉션 URL이 수신된 경우(a 문자로 표시된 플로우)의 포스터 프로세스를 설명합니다.

21단계. Anyconnect ISE Posture 모듈은 검색 단계에서 검색된 URL을 사용하여 클라이언트 프로비저닝 포털에 대한 연결을 설정합니다. 이 단계에서 ISE는 인증된 세션의 정보를 사용하여 클라이언트 프로비저닝 정책 검증을 다시 한 번 수행합니다.

22단계. 클라이언트 프로비저닝 정책이 탐지되면 ISE는 포트 8905로 리디렉션을 반환합니다.

23단계. 에이전트는 포트 8905를 통해 ISE에 대한 연결을 설정합니다. 이 연결 중에 ISE는 상태 프로파일, 규정 준수 모듈 및 anyconnect 업데이트에 대한 URL을 반환합니다.

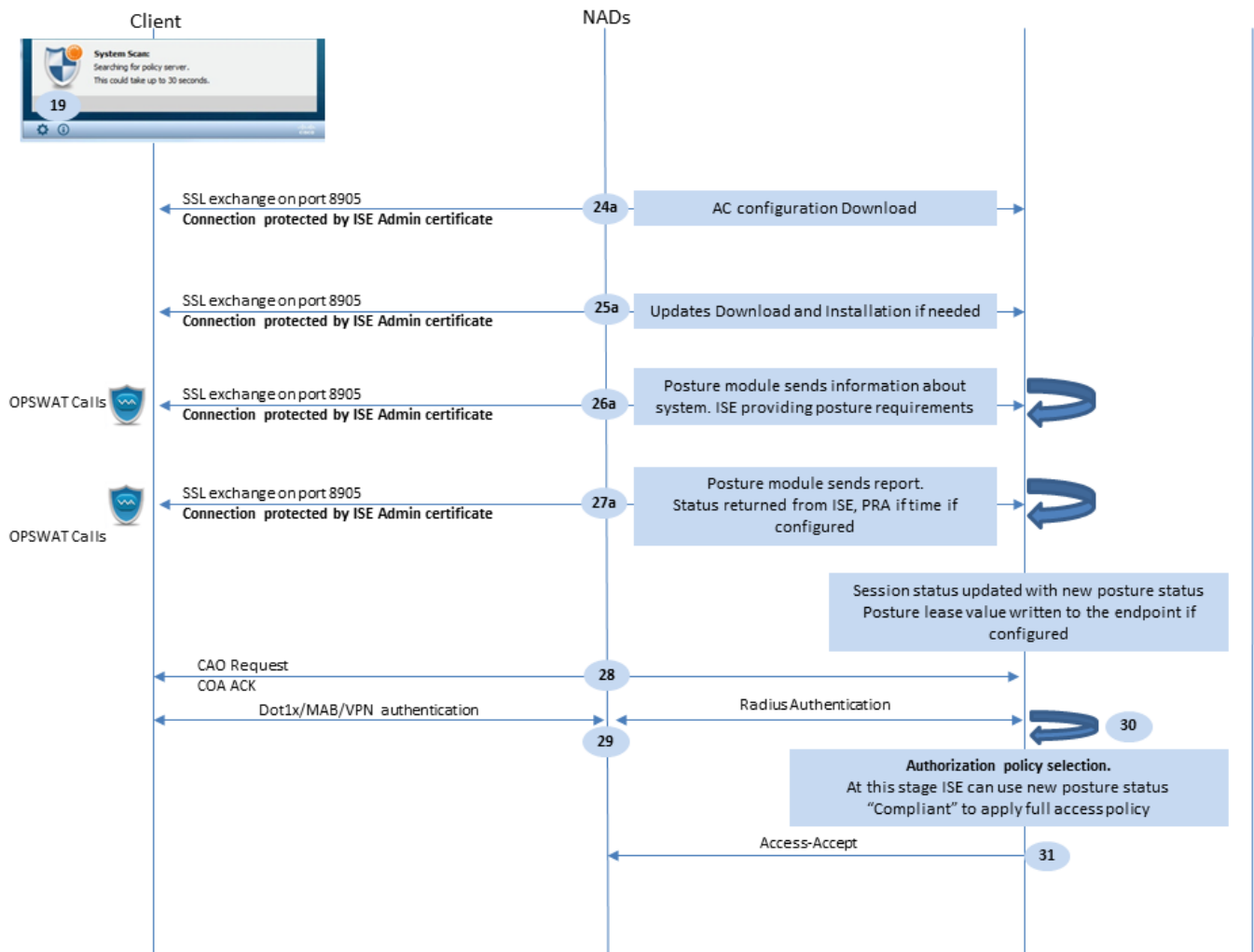


그림 1-4

24단계 ISE에서 AC ISE Posture 모듈 컨피그레이션 다운로드.


25단계.필요한 경우 다운로드 및 설치를 업데이트합니다.

26단계. AC ISE Posture 모듈은 시스템에 대한 초기 정보(예: OS 버전, 설치된 보안 제품, 정의 버전)를 수집합니다. 이 단계에서 AC ISE Posture 모듈은 보안 제품에 대한 정보를 수집하기 위해 OPSWAT API를 포함합니다. 수집된 데이터는 ISE로 전송됩니다. 이 요청에 대한 응답으로 ISE는 상태 요구 사항 목록을 제공합니다. 상태 정책 처리의 결과로 요구 사항 목록이 선택 됩니다. 올바른 정책과 일치시키기 위해 ISE는 디바이스 OS 버전(요청에 있음) 및 세션 ID 값을 사용하여 다른 필수 특성(AD/LDAP 그룹)을 선택합니다. 세션 ID 값은 클라이언트에서도 전송됩니다.

27단계. 이 단계에서 클라이언트는 포스처 요건을 확인하기 위해 OPSWAT 통화 및 기타 메커니즘을 포함합니다. 요구 사항 목록 및 해당 상태가 포함된 최종 보고서가 ISE로 전송됩니다. ISE는 엔드포인트 규정 준수 상태에 대한 최종 결정을 내려야 합니다. 이 단계에서 엔드포인트가 규정을 준수하지 않는 것으로 표시된 경우 교정 작업 집합이 반환됩니다. 규정 준수 엔드 포인트의 경우 ISE는 규정 준수 상태를 세션에 기록 하고 상태 임대가 구성된 경우 엔드 포인트 특성에 마지막 상태 타임스탬프를 지정 합니다. 포스처 결과가 엔드포인트로 다시 전송됩니다. PRA(Posture Reassessment) 시간의 경우 PRA는 ISE에서 이 패킷에도 배치합니다.

규정을 준수하지 않는 시나리오에서는 다음 사항을 고려합니다.

- 일부 교정 작업(예: 표시 텍스트 메시지, 링크 교정, 파일 교정 등)은 포스처 에이전트 자체에서 실행됩니다.
- 기타 교정 유형(예: AV) AS, WSUS, SCCM에서는 포스처 에이전트와 대상 제품 간 OPSWAT API 통신이 필요합니다. 이 시나리오에서 상태 에이전트는 개선 요청을 제품에 전송 합니다. 위협 요소 제거 자체는 보안 제품이 직접 수행합니다.

 참고: 보안 제품이 외부 리소스(내부/외부 업데이트 서버)와 통신해야 하는 경우 Redirect-ACL/DACL에서 이 통신이 허용되는지 확인해야 합니다.

28단계 ISE는 NAD에 사용자의 새 인증을 트리거해야 하는 COA 요청을 보냅니다. NAD는 COA ACK를 통해 이 요청을 확인해야 합니다. VPN 케이스의 경우 COA 푸시가 사용되므로 새 인증 요청이 전송되지 않습니다. 대신 ASA는 세션에서 이전 권한 부여 매개변수(리디렉션 URL, 리디렉션 ACL, DAACL)를 제거하고 COA 요청에서 새 매개변수를 적용합니다.

29단계. 사용자에게 대한 새 인증 요청.

중요한 고려 사항:

- 일반적으로 Cisco NAD COA의 경우 ISE에서 reauth를 사용하며, 이는 NAD가 이전 세션 ID를 사용하여 새 인증 요청을 시작하도록 지시합니다.
- ISE 측에서 동일한 세션 ID 값은 이전에 수집된 세션 특성을 재사용하고(이 경우 불만 상태) 이러한 특성에 기반한 새 권한 부여 프로파일을 할당해야 함을 나타냅니다.
- 세션 ID가 변경되는 경우 이 연결은 새 연결로 처리되며 전체 포스처 프로세스가 다시 시작됩니다.
- 포스처 재구축을 방지하기 위해 세션 id를 변경할 때마다 포스처 임대를 사용할 수 있습니다. 이 시나리오에서 상태 상태에 대한 정보는 세션 ID가 ge인 경우에도 ISE에 유지되는 엔드포인트 특성에 저장됩니다(가) 변경되었습니다.

30단계. 상태 상태에 따라 ISE 측에서 새 권한 부여 정책이 선택됩니다.

31단계. 새 권한 부여 특성이 있는 Access-Accept가 NAD로 전송됩니다.

다음 흐름은 리디렉션 URL이 포스처 프로브에서 검색되지 않고(문자 b로 표시됨) 이전에 연결된 PSN이 마지막 프로브에서 쿼리된 경우를 설명합니다. 여기의 모든 단계는 PSN에서 프로브 4의 결과로 반환되는 재생을 제외하고 리디렉션 URL의 경우와 정확히 동일합니다. 이 프로브가 현재 인증 세션의 소유자인 동일한 PSN에 연결된 경우, 나중에 포스처 에이전트가 프로세스를 완료하는데 사용하는 세션 ID 값이 재생에 포함됩니다. 이전에 연결된 헤드엔드가 현재 세션 소유자와 동일하지 않은 경우, 세션 조회가 실패하고 빈 응답이 AC ISE Posture 모듈로 반환됩니다. 결과적으로 , No Policy Server Detected 메시지가 최종 사용자에게 반환됩니다.

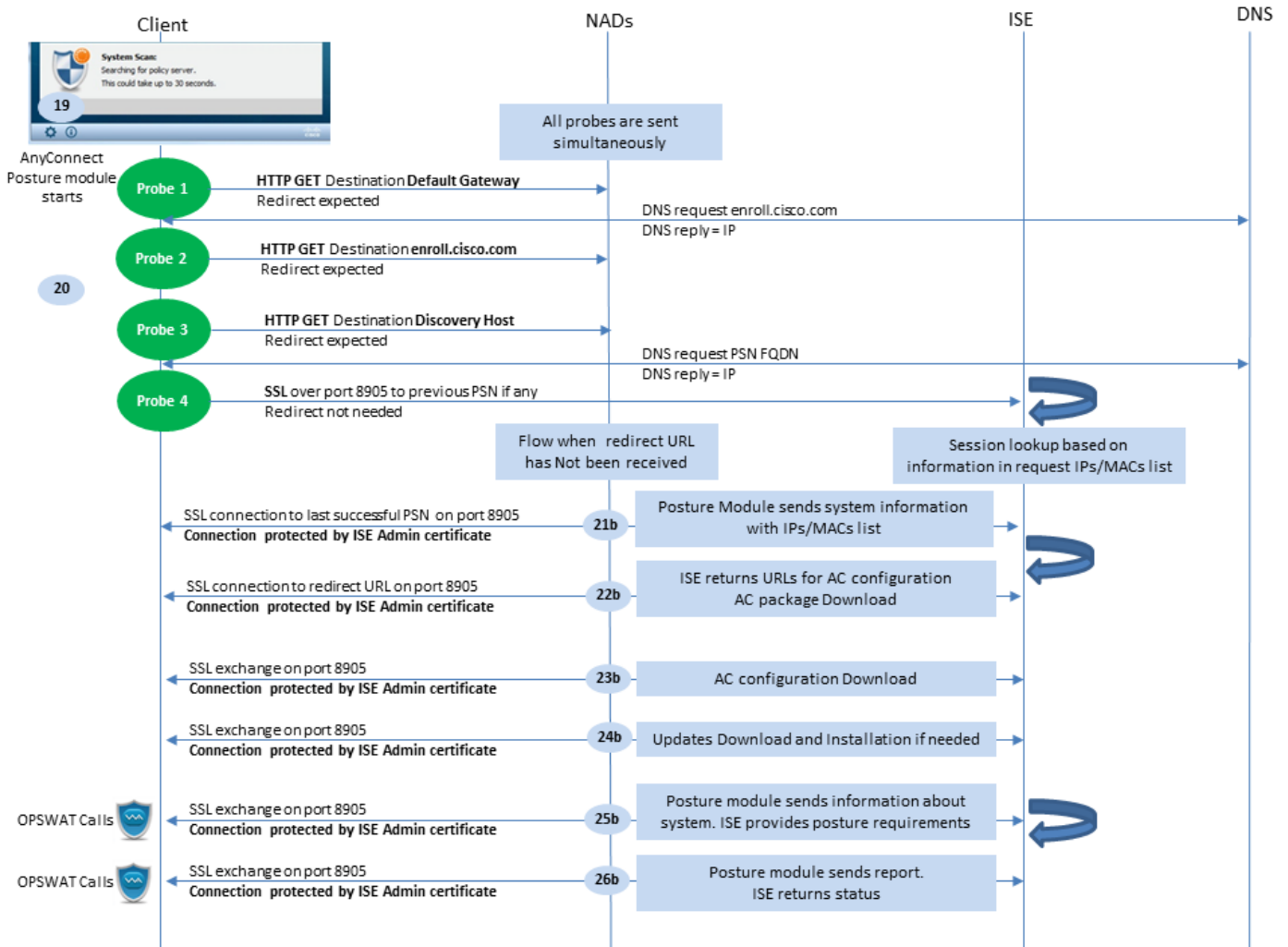


그림 1-5

ISE 2.2 이후 상태 흐름

ISE 2.2 이상 버전에서는 리디렉션과 리디렉션 없는 플로우를 동시에 지원합니다. 다음은 리디렉션 없는 상태 흐름에 대한 자세한 설명입니다.

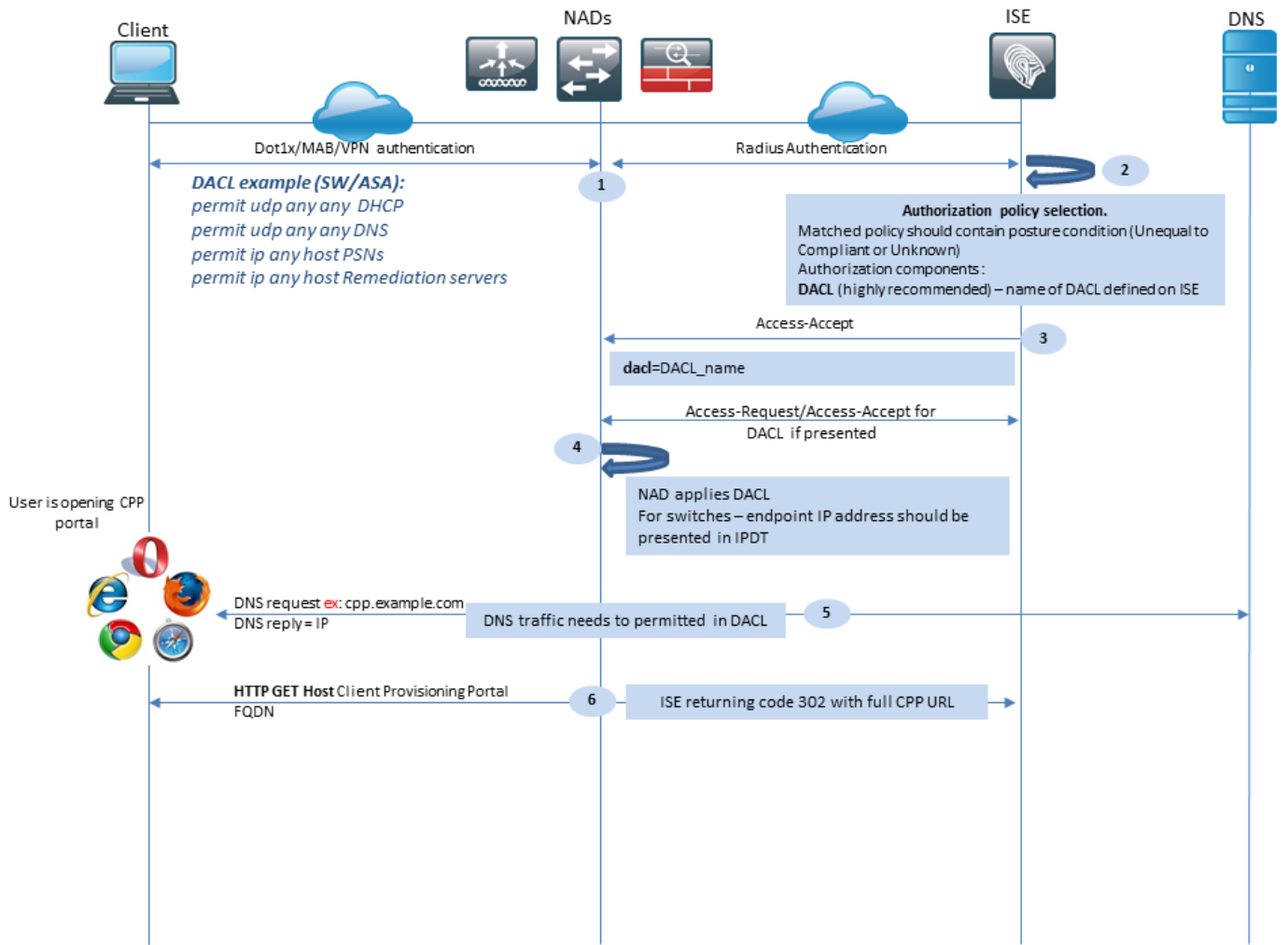


그림 2-1

1단계. 인증은 흐름의 첫 번째 단계입니다. dot1x, MAB 또는 VPN일 수 있습니다.

2단계. ISE는 사용자에 대한 인증 및 권한 부여 정책을 선택해야 합니다. Posture에서 선택한 권한 부여 정책에 포스처 상태에 대한 참조가 포함되어야 하며, 처음에는 알 수 없거나 적용할 수 없어야 합니다. 이 두 경우를 모두 포함하기 위해, 상태 상태가 불균등한 규정준수를 갖는 조건을 사용할 수 있습니다. 리디렉션이 없는 상태의 경우 권한 부여 프로파일에서 웹 리디렉션 컨피그레이션을 사용할 필요가 없습니다. 포스처 상태를 사용할 수 없는 경우 단계에서 사용자 액세스를 제한하기 위해 DACL 또는 Airspace ACL을 사용하는 것을 고려할 수 있습니다.

3단계. ISE는 권한 부여 특성이 있는 Access-Accept를 반환합니다.

4단계. DACL 이름이 Access-Accept에서 반환되고 NAD가 DACL 콘텐츠 다운로드를 시작하고 권한 부여 프로파일을 얻은 후 세션에 적용하는 경우

5단계. 새 접근 방식에서는 리디렉션이 불가능한 것으로 간주하므로 사용자는 클라이언트 프로비저닝 포털 FQDN을 수동으로 입력해야 합니다. CPP 포털의 FQDN은 ISE 측의 포털 컨피그레이션에 정의되어야 합니다. DNS 서버 관점에서 A-record는 PSN 역할이 활성화된 ISE 서버를 가리켜야 합니다.

6단계. 클라이언트는 HTTP를 전송하여 클라이언트 프로비저닝 포털 FQDN에 연결합니다. 이 요청

은 ISE 측에서 구문 분석되며 전체 포털 URL이 클라이언트로 다시 반환됩니다.

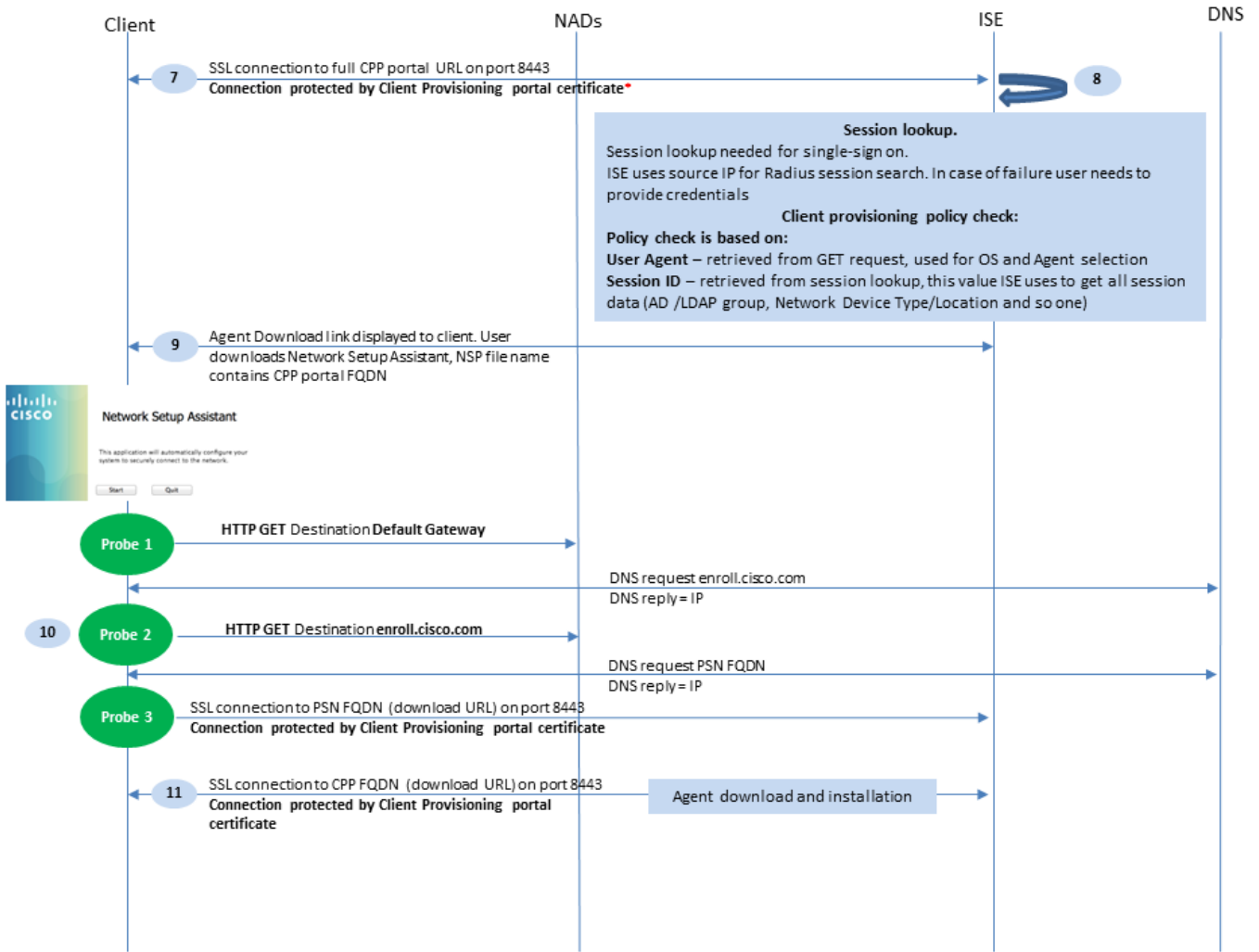


그림 2-2

7단계. 리디렉션 URL에서 수신된 포트를 통한 SSL 연결이 설정됩니다(기본값 8443). 이 연결은 ISE 측의 포털 인증서로 보호됩니다. CPP(Client Provisioning Portal)가 사용자에게 표시됩니다.


8단계. 이 단계에서는 ISE에서 다음 두 가지 이벤트가 발생합니다.

- SSO(Single Sign On) - ISE가 이전에 성공한 인증을 조회하려고 시도합니다. ISE는 패킷의 소스 IP 주소를 라이브 RADIUS 세션에 대한 검색 필터로 사용합니다.

참고: 패킷의 소스 IP와 세션의 프레임 IP 주소 간의 일치 여부를 기반으로 세션이 검색됩니다. 프레임 IP 주소는 일반적으로 ISE에서 중간 어카운팅 업데이트에서 검색되므로, NAD 측에서 어카운팅을 활성화해야 합니다. 또한 세션을 소유하는 노드에서만 SSO가 가능하다는 점을 기억해야 합니다. 예를 들어 세션이 PSN 1에서 인증되었지만 FQDN 자체가 PSN2를 가리키는 경우 SSO 메커니즘이 실패합니다.

- 클라이언트 프로비저닝 정책 조회 - 성공적인 SSO의 경우 ISE는 인증된 세션의 데이터 및 클라이언트 브라우저의 사용자 에이전트를 사용할 수 있습니다. SSO가 실패할 경우 사용자는

자격 증명을 제공해야 하며 내부 및 외부 ID 저장소(AD/LDAP/내부 그룹)에서 사용자 인증 정보를 검색한 후 클라이언트 프로비저닝 정책 검사에 사용할 수 있습니다.

 참고: Cisco 버그 ID [CSCvd11574](#)로 인해, 외부 사용자가 외부 ID 저장소 컨피그레이션에 추가된 여러 AD/LDAP 그룹의 구성원인 경우 비 SSO 사례에 대한 클라이언트 프로비저닝 정책을 선택할 때 오류가 표시될 수 있습니다. 언급된 결함은 ISE 2.3 FCS에서 시작하여 수정되며, 이 수정에서는 EQUAL 대신 AD 그룹이 있는 조건에서 CONTAINS를 사용해야 합니다.

9단계. 클라이언트 프로비저닝 정책을 선택하면 ISE는 사용자에게 에이전트 다운로드 URL을 표시합니다. 다운로드 NSA를 클릭 한 후, 응용 프로그램은 사용자에게 푸시됩니다. NSA 파일 이름에는 CPP 포털의 FQDN이 포함되어 있습니다.

10단계. 이 단계에서 NSA는 ISE와의 연결을 설정하기 위한 프로브를 실행합니다. 두 프로브는 기존 프로브이며 세 번째 프로브는 URL 리디렉션이 없는 환경에서 ISE 검색을 허용하도록 설계되었습니다.

- NSA는 첫 번째 검색 프로브(HTTP/auth/discovery)를 기본 게이트웨이로 전송합니다. NSA는 결과적으로 리디렉션-url을 예상한다.
- NSA는 첫 번째 프로브가 실패하면 두 번째 프로브를 보냅니다. 두 번째 프로브는 HTTP GET /auth/discovery enroll.cisco.com. 이 FQDN은 DNS 서버에서 성공적으로 확인할 수 있어야 합니다. 스플릿 터널이 있는 VPN 시나리오에서 트래픽을 enroll.cisco.com 터널을 통과해야 합니다.
- NSA는 CPP 포털 포트를 통해 클라이언트 프로비저닝 포털 FQDN에 세 번째 프로브를 전송합니다. 이 요청에는 ISE가 제공해야 하는 리소스를 식별할 수 있도록 하는 포털 세션 ID에 대한 정보가 포함되어 있습니다.

11단계. NSA는 Anyconnect 및/또는 특정 모듈을 다운로드합니다. 다운로드 프로세스는 클라이언트 프로비저닝 포털 포트를 통해 수행됩니다.

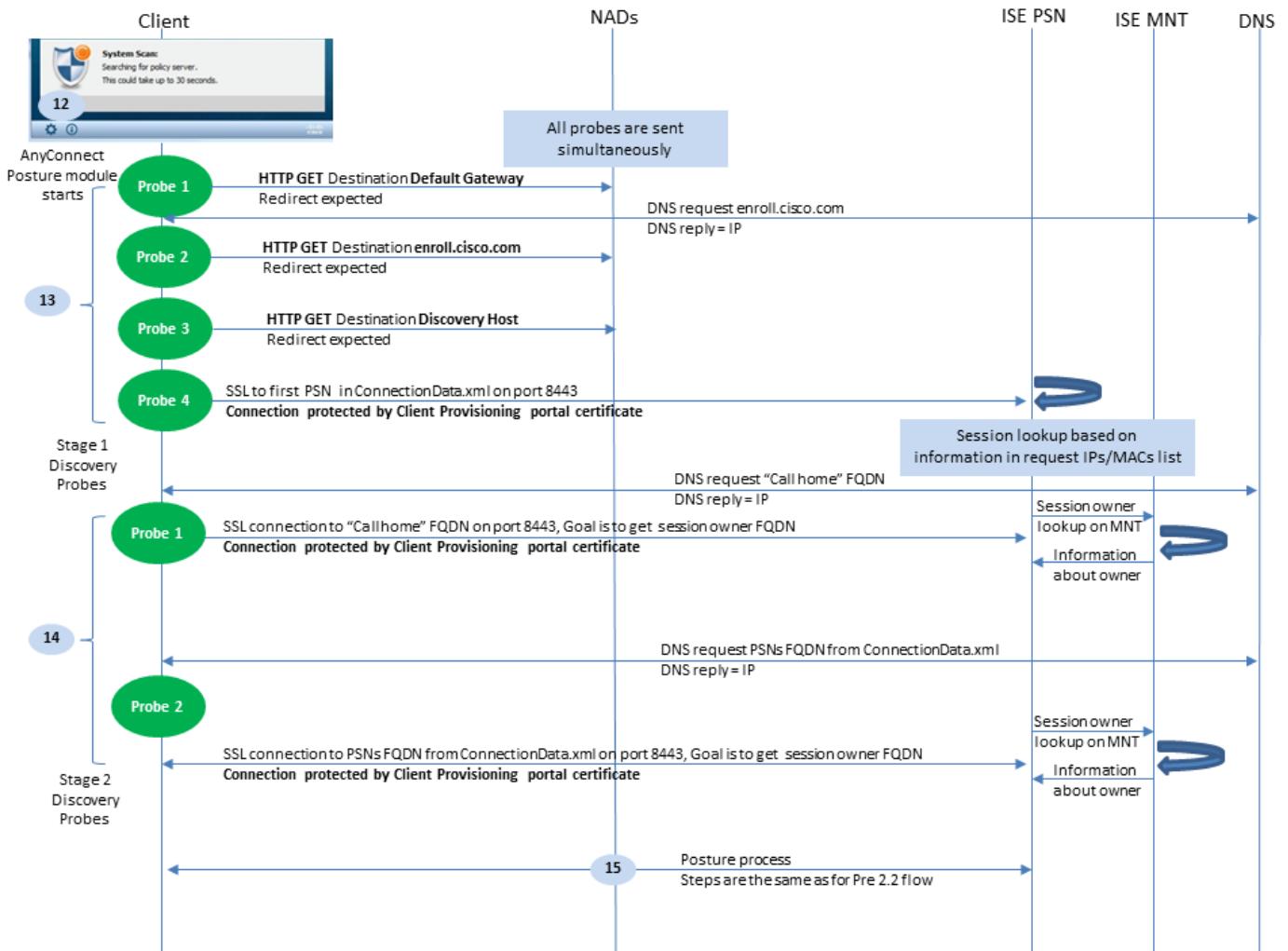


그림 2-3

12단계. ISE 2.2에서는 포스처 프로세스가 두 단계로 나뉩니다. 첫 번째 단계에는 url 리디렉션을 사용하는 구축과의 이전 버전과의 호환성을 지원하기 위한 전통적인 포스처 검색 프로브 집합이 포함되어 있습니다.

13단계. 첫 번째 단계에는 모든 기존 포스처 검색 프로브가 포함되어 있습니다. 프로브에 대한 자세한 내용을 보려면 20단계(ISE 2.2 이전 상태 흐름)를 검토하십시오.

14단계 2단계에서는 리디렉션이 지원되지 않는 환경에서 세션이 인증되는 PSN에 대한 연결을 AC ISE Posture 모듈이 설정할 수 있도록 하는 2개의 검색 프로브가 포함되어 있습니다. 2단계에서는 모든 프로브가 순차적입니다.

- 프로브 1 - 첫 번째 프로브에서 AC ISE Posture 모듈은 'Call Home List'의 IP/FQDN으로 설정을 시도합니다. 프로브에 대한 대상 목록은 ISE 측의 AC Posture 프로파일에서 구성해야 합니다. 쉼표로 구분하여 IP/FQDN을 정의할 수 있으며, 콜론으로 각 Call Home 대상에 대한 포트 번호를 정의할 수 있습니다. 이 포트는 클라이언트 프로비저닝 포털이 실행되는 포트와 같아야 합니다. Call Home 서버에 대한 클라이언트 측 정보는 ISEPostureCFG.xml, 이 파일은 폴더에서 찾을 수 있습니다. C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\.
- Call Home 대상이 세션을 소유하지 않는 경우 이 단계에서 소유자에 대한 조회가 필요합니다. AC ISE Posture 모듈은 특별한 대상 URL을 사용하여 소유자 조회를 시작하도록 ISE에 지시합니다. /auth/ng-discovery 요청하십시오. 클라이언트 IP 및 MAC 목록도 포함되어 있습니다. 이 메

시지가 PSN 세션에 의해 수신된 후, 먼저 로컬에서 조회가 수행됩니다(이 조회는 AC ISE Posture 모듈에 의해 전송된 요청의 IP 및 MAC를 모두 사용합니다). 세션을 찾을 수 없는 경우 PSN은 MNT 노드 쿼리를 시작합니다. 이 요청에는 MAC 목록만 포함되어 있으므로 소유자의 FQDN을 MNT에서 가져와야 합니다. 그런 다음 PSN은 소유자 FQDN을 클라이언트로 다시 반환합니다. 클라이언트의 다음 요청은 URL과 IP 및 MAC 목록에서 인증/상태를 사용하여 세션 소유자 FQDN으로 전송됩니다.

- 프로브 2 - 이 단계에서 AC ISE Posture 모듈은 의 PSN FQDN을 시도합니다 ConnectionData.xml. 이 파일은 다음 위치에서 찾을 수 있습니다. C:\Users\

\AppData\Local\Cisco\Cisco AnyConnect Secure Mobility Client\


. AC ISE Posture 모듈은 첫 번째 포스처 시도 후 이 파일을 생성합니다. 이 파일에는 ISE PSN FQDN 목록이 포함되어 있습니다. 목록의 내용은 다음 연결 시도 중에 동적으로 업데이트될 수 있습니다. 이 프로브의 최종 목표는 현재 세션 소유자의 FQDN을 가져오는 것입니다. 구현은 프로브 1과 동일합니다. 프로브 대상 선택에만 차이가 있습니다.

파일 자체는 여러 사용자가 디바이스를 사용하는 경우 현재 사용자의 폴더에 위치합니다. 다른 사용자가 이 파일의 정보를 사용할 수 없습니다. 따라서 사용자는 Call Home 대상이 지정되지 않은 경우 리디렉션이 없는 환경에서 치킨 및 에그 문제를 겪을 수 있습니다.

15단계. 세션 소유자에 대한 정보를 얻은 후에는 모든 후속 단계가 ISE 2.2 이전 흐름과 동일합니다.

구성

이 문서에서는 ASA가 네트워크 액세스 디바이스로 사용됩니다. 모든 테스트는 VPN을 통해 포스처를 사용하여 수행됩니다. VPN을 통한 보안 상태 지원에 대한 ASA 컨피그레이션은 이 문서의 범위를 벗어납니다. 자세한 내용은 [ASA 버전 9.2.1 VPN Posture with ISE 컨피그레이션 예를 참조하십시오](#).

 참고: VPN 사용자가 있는 배포의 경우 권장 설정은 리디렉션 기반 포스처입니다. callhomelist는 구성하지 않는 것이 좋습니다. 모든 비 vpn 기반 사용자의 경우, DACL이 적용되어 상태가 구성된 PSN과 통신하지 않도록 해야 합니다.

네트워크 다이어그램

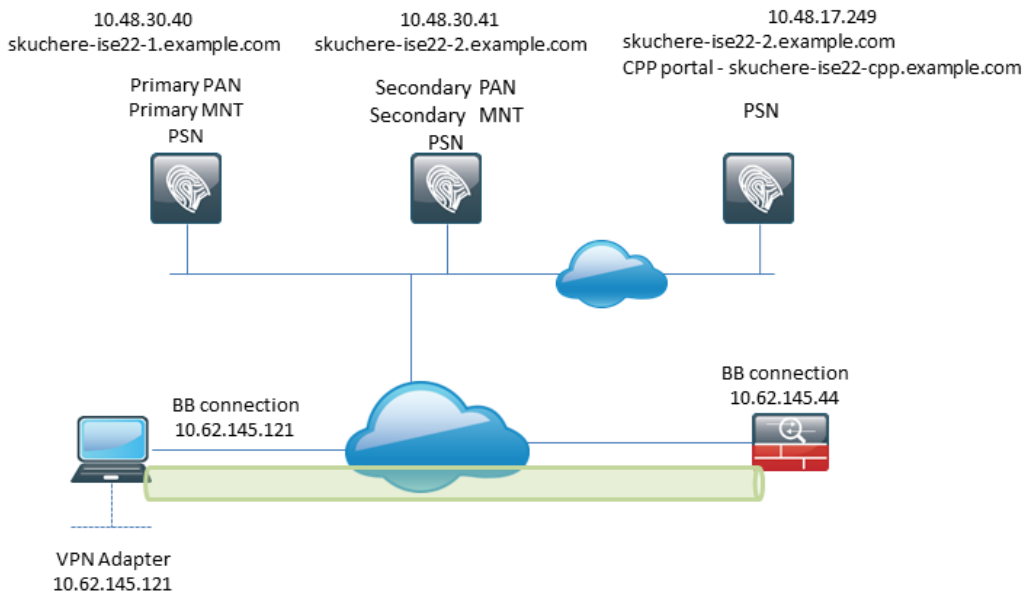


그림 3-1

이 토폴로지는 테스트에 사용됩니다. ASA에서는 NAT 기능 때문에 PSN측에서 클라이언트 프로비저닝 포털에 대한 SSO 메커니즘이 실패할 경우 시나리오를 쉽게 시뮬레이션할 수 있습니다. VPN을 통한 일반 상태 흐름의 경우, 사용자가 기업 네트워크에 들어갈 때 VPN IP에 대해 NAT가 일반적으로 시행되지 않으므로 SSO가 제대로 작동해야 합니다.

설정

클라이언트 프로비저닝 컨피그레이션

다음은 Anyconnect 컨피그레이션을 준비하는 단계입니다.

1단계. Anyconnect 패키지 다운로드 Anyconnect 패키지 자체는 ISE에서 직접 다운로드할 수 없으므로 시작하기 전에 PC에서 AC를 사용할 수 있는지 확인하십시오. 이 링크는 AC 다운로드에 사용할 수 있습니다. <https://www.cisco.com/site/us/en/products/security/secure-client/index.html> 이 문서에서는 anyconnect-win-4.4.00243-webdeploy-k9.pkg 패키지가 사용됩니다.

2단계. AC 패키지를 ISE에 업로드하려면 Policy > Policy Elements > Results > Client Provisioning > Resources 을 클릭하고 Add. 로컬 디스크에서 Agent resources(에이전트 리소스)를 선택합니다. 새 창에서 다음을 선택합니다 Cisco Provided Packages, 클릭 browse PC에서 AC 패키지를 선택합니다.

Agent Resources From Local Disk

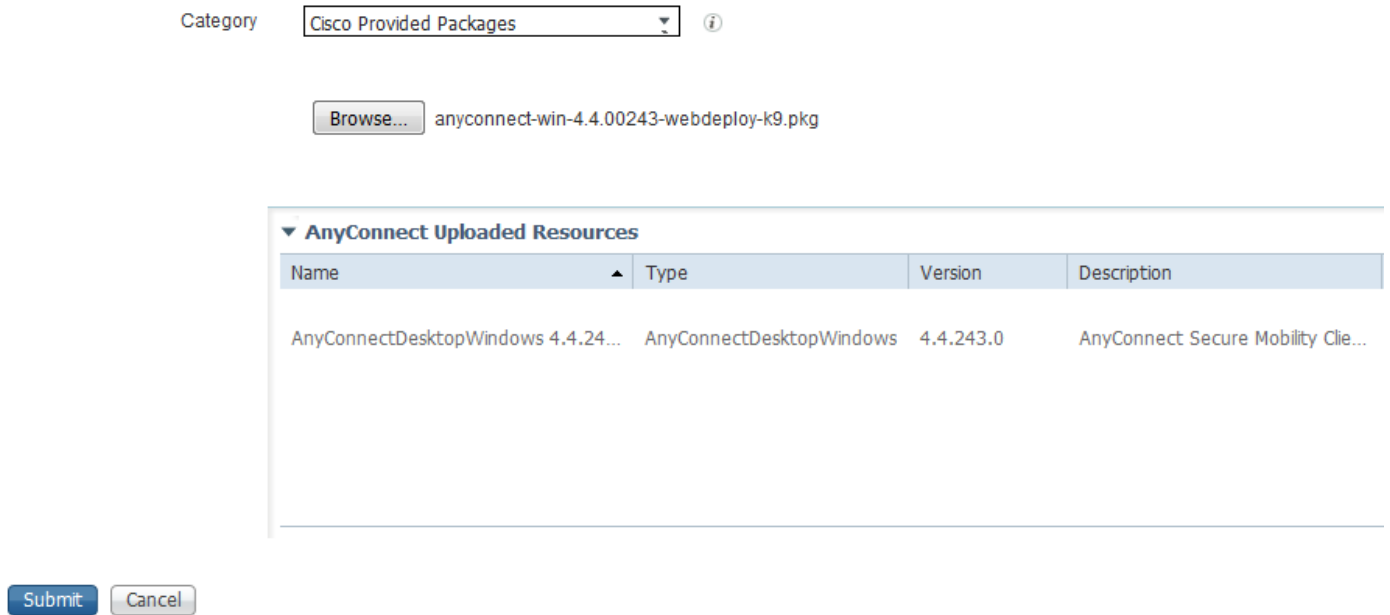


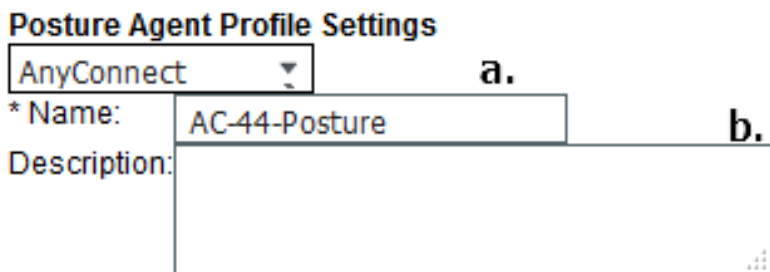
그림 3-2

클릭 **Submit** 가져오기를 마칩니다.

3단계. 규정 준수 모듈을 ISE에 업로드해야 합니다. 같은 페이지에서 **Add Firepower Threat Defense** Agent resources from Cisco site. 리소스 목록에서 규정 준수 모듈을 확인해야 합니다. 이 문서의 경우 **AnyConnectComplianceModuleWindows 4.2.508.0** 규정 준수 모듈이 사용됩니다.

4단계. 이제 AC Posture 프로파일을 생성해야 합니다. 클릭 **Add Firepower Threat Defense** NAC agent or Anyconnect posture profile.

ISE Posture Agent Profile Settings > New Profile



Agent Behavior

그림 3-3


- 프로파일 유형을 선택합니다. 이 시나리오에서는 AnyConnect를 사용해야 합니다.
- 프로파일 이름을 지정합니다. 탐색: Posture Protocol 섹션을 참조하십시오.

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	<input type="text" value="120"/> secs	
Discovery host	<input type="text"/>	
* Server name rules	<input type="text" value="*"/> a.	need to be blank by default to force admin to enter a value. "*" means agent will connect to all
Call Home List	<input type="text" value="skuchere-ise22-2.examp"/> b.	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)
Back-off Timer	<input type="text" value="30"/> secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.

그림 3-4

- 다음을 지정합니다. Server Name Rules, 이 필드는 비워둘 수 없습니다. 이 필드에는 적절한 네임스페이스에서 PSN에 대한 AC ISE 상태 모듈 연결을 제한하는 와일드카드가 포함된 FQDN을 포함할 수 있습니다. FQDN을 허용해야 하는 경우 별을 입력합니다.
- 여기에 지정된 이름 및 IP는 상태 검색의 단계 2에서 사용 중입니다. 콜론을 사용하여 FQDN/IP 뒤에 포트 번호를 추가할 수 있을 뿐만 아니라 이름을 쉼표로 구분할 수도 있습니다. GPO 또는 Call Home 주소의 다른 소프트웨어 프로비저닝 시스템 프레즌스를 사용하여 AC가 대역 외(ISE 클라이언트 프로비저닝 포털에서 구축되지 않음)로 구축된 경우, 이는 ISE PSN에 성공적으로 연결할 수 있는 유일한 프로브이므로 필수적입니다. 즉, 대역 외 AC 프로비저닝의 경우 관리자가 AC 프로파일 편집기를 사용하여 AC ISE 포스처 프로파일을 생성하고 AC 설치와 함께 이 파일을 프로비저닝해야 합니다.

 참고: 다중 사용자 PC에는 콜 홈 주소가 반드시 포함되어야 합니다. Posture flow post-ISE 2.2에서 14단계를 검토합니다.

5단계.AC 컨피그레이션을 생성합니다. 탐색 Policy > Policy Elements > Results > Client Provisioning > Resources, 클릭 Add을 선택한 다음 AnyConnect Configuration.

* Select AnyConnect Package: AnyConnectDesktopWindows 4.4.243.0 a.
* Configuration Name: AC-44-CCO b.
Description:
DescriptionValue
* Compliance Module: AnyConnectComplianceModuleWindows 4.2.508.0 c.

Notes

AnyConnect Module Selection

- ISE Posture
- VPN
- Network Access Manager
- Web Security
- AMP Enabler
- ASA Posture
- Network Visibility
- Umbrella Roaming Security
- Start Before Logon
- Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: AC-44-Posture d.

그림 3-5

- AC 패키지를 선택합니다.
- AC 컨피그레이션 이름을 제공합니다.
- 규정 준수 모듈 버전을 선택합니다.
- 드롭다운 목록에서 AC Posture 컨피그레이션 프로파일을 선택합니다.

6단계. 클라이언트 프로비저닝 정책을 구성합니다. 탐색 Policy > Client Provisioning. 초기 컨피그레이션의 경우 기본값으로 제공되는 정책의 빈 값을 채울 수 있습니다. 존재하는 포스처 컨피그레이션에 정책을 추가해야 하는 경우 재사용 가능한 정책으로 이동하여 선택합니다 Duplicate Above 또는 Duplicate Below . 새로운 정책을 생성할 수도 있습니다.

문서에 사용된 정책의 예입니다.

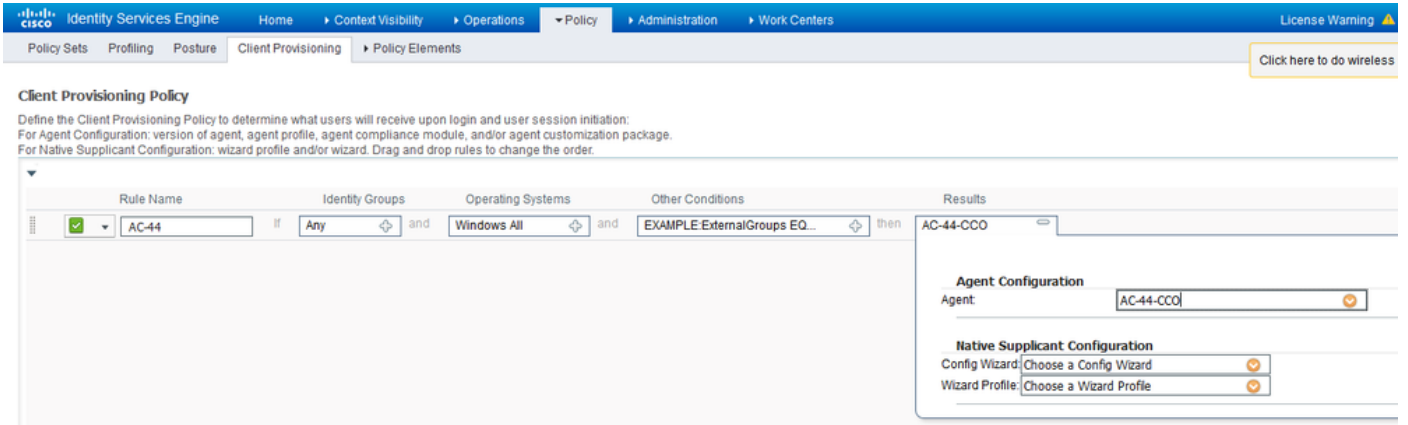


그림 3-6

결과 섹션에서 AC 컨피그레이션을 선택합니다. SSO 실패의 경우 ISE는 로그인에서 포털로의 특성만 가질 수 있습니다. 이러한 특성은 내부 및 외부 ID 저장소에서 사용자에게 대해 검색할 수 있는 정보로 제한됩니다. 이 문서에서는 AD 그룹이 클라이언트 프로비저닝 정책의 조건으로 사용됩니다.

상태 정책 및 조건

간단한 상태 검사가 사용됩니다. ISE는 엔드 디바이스 측에서 Window Defender 서비스의 상태를 확인하도록 구성됩니다. 실제 시나리오는 훨씬 더 복잡할 수 있지만 일반적인 컨피그레이션 단계는 동일합니다.

1단계. 포스처 조건을 생성합니다. 상태 조건은 다음 위치에 있습니다. Policy > Policy Elements > Conditions > Posture. 상태 조건의 유형을 선택 합니다. 다음은 Windows Defender 서비스가 실행 중인지 확인해야 하는 서비스 조건의 예입니다.

Service Conditions List > WinDefend

Service Condition

* Name	<input type="text" value="WinDefend"/>
Description	<input type="text"/>
* Operating Systems	<input type="text" value="Windows All"/>
Compliance Module	Any version
* Service Name	<input type="text" value="WinDefend"/>
Service Operator	<input type="text" value="Running"/>

그림 3-7

2단계. 포스처 요건 컨피그레이션. 탐색 Policy > Policy Elements > Results > Posture > Requirements. 다음은 Window Defender 검사의 예입니다.

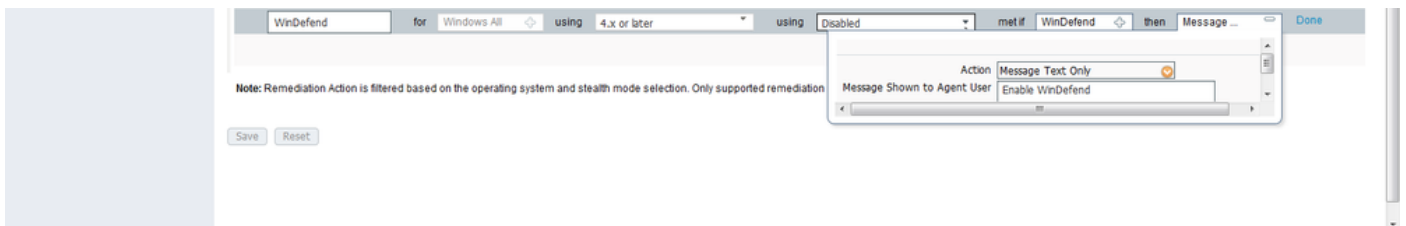


그림 3-8

새 요구 사항에서 상태 조건을 선택 하고 개선 조치를 지정 합니다.

3단계. 상태 정책 컨피그레이션 탐색 Policy > Posture. 여기에서 이 문서에 사용된 정책의 예를 찾을 수 있습니다. 정책에는 Windows Defender 요구 사항이 필수로 할당되어 있으며 외부 AD 그룹 이름만 조건으로 포함되어 있습니다.

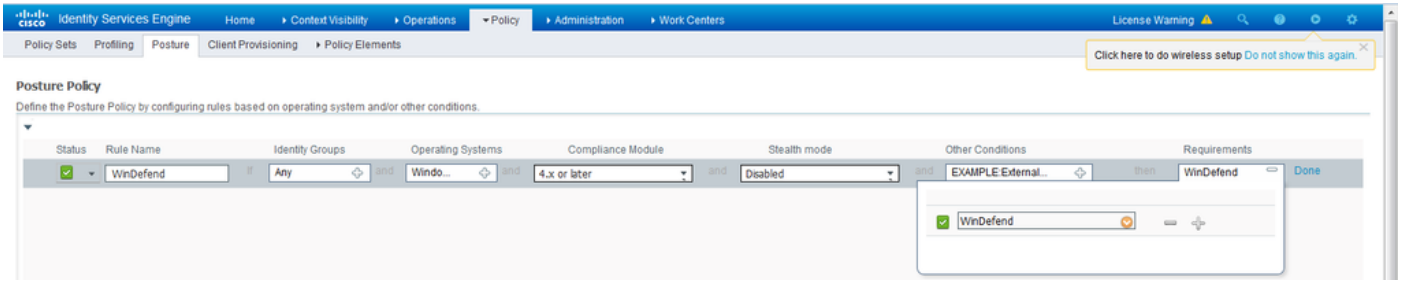


그림 3-9

클라이언트 프로비저닝 포털 구성

리디렉션이 없는 상태의 경우 클라이언트 프로비저닝 포털의 컨피그레이션을 편집해야 합니다. 탐색 Administration > Device Portal Management > Client Provisioning 기본 포털을 사용하거나 직접 만들 수 있습니다. 동일한 포털을 리디렉션이 있는 상태와 없는 상태 모두에 사용할 수 있습니다.

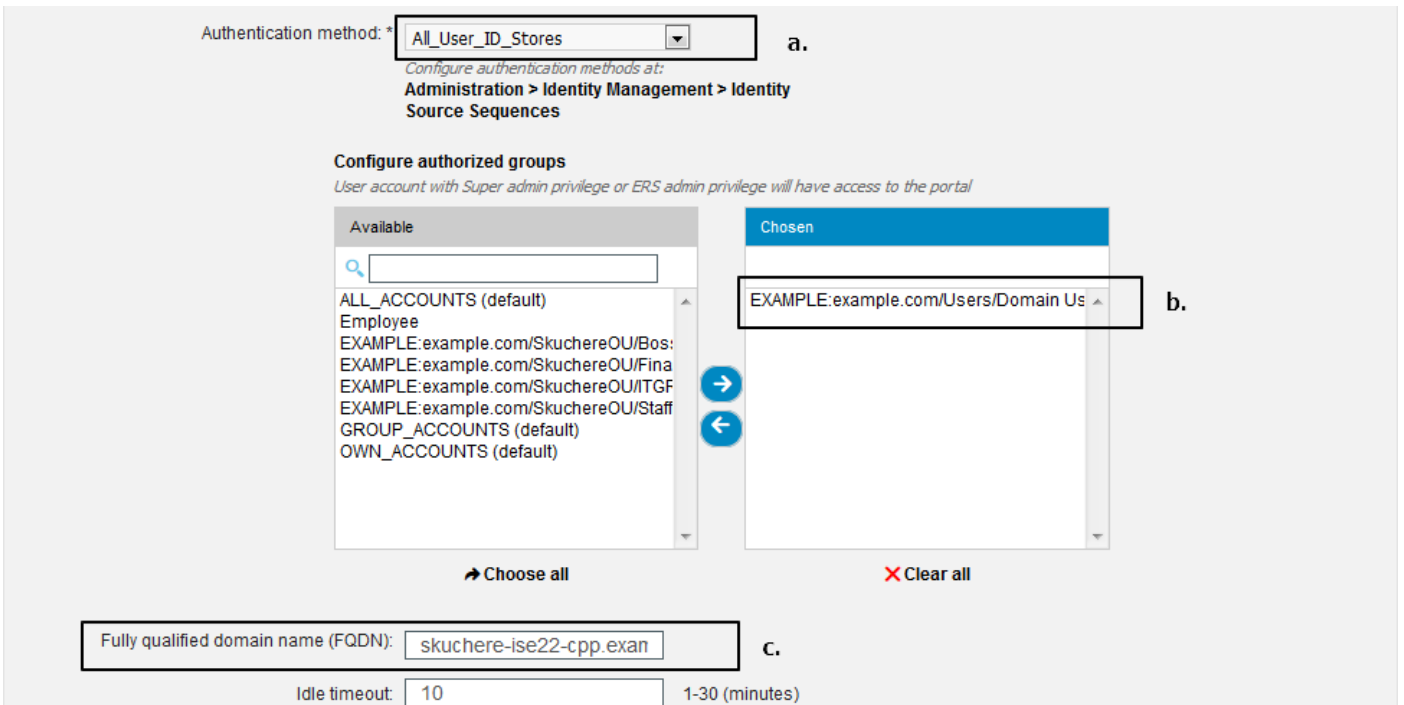


그림 3-10

리디렉션이 아닌 시나리오의 경우 포털 컨피그레이션에서 다음 설정을 편집해야 합니다.

- Authentication(인증)에서 SSO가 사용자에게 대한 세션을 찾을 수 없는 경우 사용해야 할 Identity Source Sequence(ID 소스 시퀀스)를 지정합니다.
- 선택한 ID 소스 시퀀스 목록에 따라 사용 가능한 그룹이 채워집니다. 이때 포털 로그인에 대한 권한이 있는 그룹을 선택해야 합니다.
- 클라이언트 프로비저닝 포털에서 AC를 구축해야 하는 시나리오에 대해 클라이언트 프로비저닝 포털의 FQDN을 지정해야 합니다. 이 FQDN은 ISE PSN IP에 대해 확인 가능해야 합니다. 사용자는 첫 번째 연결 시도 중에 웹 브라우저에서 FQDN을 지정하라는 지시를 받아야 합니다.

권한 부여 프로파일 및 정책 구성

포스처 상태를 사용할 수 없을 때 클라이언트에 대한 초기 액세스를 제한해야 합니다. 이는 다음과 같은 여러 가지 방법으로 달성할 수 있습니다.

- DACL Assignment(DACL 할당) - 제한된 액세스 단계에서 사용자에게 DACL을 할당하여 액세스를 제한할 수 있습니다. 이 접근 방식은 Cisco Network Access Devices에 사용할 수 있습니다.
- VLAN 할당 - 성공적인 포스처 사용자를 제한된 VLAN에 배치하기 전에 이 접근 방식은 거의 모든 NAD 벤더에 대해 잘 작동해야 합니다.
- Radius Filter-Id - 이 특성을 사용하면 NAD에 로컬로 정의된 ACL을 알 수 없는 상태 상태의 사용자에게 할당할 수 있습니다. 표준 RFC 특성이므로 이 접근 방식은 모든 NAD 공급업체에 잘 적용되어야 합니다.

1단계. DACL을 구성합니다. 이 예는 ASA를 기반으로 하므로 NAD DACL을 사용할 수 있습니다. 실제 시나리오의 경우 가능한 옵션으로 VLAN 또는 Filter-ID를 고려해야 합니다.

DACL을 생성하려면 Policy > Policy Elements > Results > Authorization > Downloadable ACLs을 클릭하고 Add.

알 수 없는 상태 중, 적어도 다음 권한을 제공 해야 합니다.

- DNS 트래픽
- DHCP 트래픽
- ISE PSN에 대한 트래픽(포털의 친숙한 FQDN을 열 수 있는 가능성을 위한 포트 80 및 443). CP 포털이 실행 중인 포트는 기본적으로 8443이며, 이전 버전과의 호환성을 위해 8905입니다.)
- 필요한 경우 리미디에이션 서버에 대한 트래픽

다음은 리미디에이션 서버가 없는 DACL의 예입니다.

Downloadable ACL List > [New Downloadable ACL](#)

Downloadable ACL

* Name

Description

* DACL Content

```
1 permit udp any any eq 53
2 permit udp any any eq bootps
3 permit tcp any host 10.48.30.40 eq 80
4 permit tcp any host 10.48.30.40 eq 443
5 permit tcp any host 10.48.30.40 eq 8443
6 permit tcp any host 10.48.30.40 eq 8905
7 permit tcp any host 10.48.30.41 eq 80
8 permit tcp any host 10.48.30.41 eq 443
9 permit tcp any host 10.48.30.41 eq 8443
10 permit tcp any host 10.48.30.41 eq 8905
```

▶ Check DACL Syntax

Submit

Cancel

그림 3-11

2단계. 권한 부여 프로파일을 구성합니다.

포스처에 대해 평소와 같이 2개의 권한 부여 프로파일이 필요합니다. 첫 번째는 어떤 종류의 네트워크 액세스 제한도 포함해야 합니다(이 예에서는 DACL이 사용된 프로파일). 이 프로파일은 포스처 상태가 규정 준수와 같지 않은 인증에 적용할 수 있습니다. 두 번째 권한 부여 프로파일은 액세스 허용만 포함할 수 있으며 규정 준수와 같은 포스처 상태의 세션에 적용할 수 있습니다.

권한 부여 프로파일을 생성하려면 Policy > Policy Elements > Results > Authorization > Authorization Profiles.

제한된 액세스 프로파일의 예:

Authorization Profiles > VPN-No-Redirect-Unknown

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement ⓘ

Passive Identity Tracking ⓘ

▼ Common Tasks

DACL Name ⓘ

그림 3-12

이 예에서 기본 ISE 프로파일 PermitAccess는 성공적인 상태 확인 후 세션에 사용됩니다.

3단계. 권한 부여 정책을 구성합니다. 이 단계에서 두 가지 권한 부여 정책을 생성해야 합니다. 하나는 알 수 없는 상태와 초기 인증 요청을 일치하는 것이고 두 번째 하나는 성공적인 상태 프로세스 후 전체 액세스를 할당하는 것입니다.

다음은 이 경우에 대한 단순 권한 부여 정책의 예입니다.

▼ Authorization Policy

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✔	Posture-Compliant	if (Session:PostureStatus EQUALS Compliant AND EXAMPLE:ExternalGroups EQUALS example.com/Users/Domain Users)	then PermitAccess
✔	Posture-Unknown-No-Redirect	if (Session:PostureStatus NOT_EQUALS Compliant AND EXAMPLE:ExternalGroups EQUALS example.com/Users/Domain Users)	then VPN-No-Redirect-Unknown
✔	Default	if no matches, then	DenyAccess

그림 3-13

인증 정책의 구성은 이 문서의 일부가 아니지만 권한 부여 정책 처리 성공 적인 인증을 수행 하기 전에 유념해야 합니다.

다음을 확인합니다.

플로우의 기본 검증은 세 가지 주요 단계로 구성될 수 있습니다.

1단계. 인증 흐름 확인.

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Profiles	IP Address
Feb 23, 2017 06:00:07.028 PM	✔			Identity	Endpoint ID	Endpoint Prof	Authenticator	Authorization	Authorization Profiles	IP Address
Feb 23, 2017 06:00:07.028 PM	✔			e.	10.62.145.95				PermitAccess	
Feb 23, 2017 06:00:04.368 PM	ⓘ		0	d. user1	00:0B:7F:D0:F8:F4	Windows7-...	VPN-LAB >>...	VPN-LAB >>...	VPN-No-Redirect-Unknown	172.16.31.12
Feb 23, 2017 05:59:04.750 PM	✔			c. user1					PermitAccess	
Feb 23, 2017 05:44:57.921 PM	✔			b. #ACSACL#-IP-VPN-No-Redi...						
Feb 23, 2017 05:44:57.680 PM	✔			a. user1	00:0B:7F:D0:F8:F4	Windows7-...	VPN-LAB >>...	VPN-LAB >>...	VPN-No-Redirect-Unknown	

그림 4-1

1. 초기 인증. 이 단계에서는 권한 부여 프로파일이 적용된 검증에 관심을 가질 수 있습니다. 예 기치 않은 권한 부여 프로파일이 적용된 경우 자세한 인증 보고서를 조사합니다. 세부 정보 열 에서 돋보기를 클릭하여 이 보고서를 열 수 있습니다. 상세 인증 보고서의 특성을 일치할 것으 로 예상되는 권한 부여 정책의 조건과 비교할 수 있습니다.
2. DACL 다운로드 이벤트. 이 문자열은 초기 인증을 위해 선택한 권한 부여 프로파일에 DACL 이름이 포함된 경우에만 표시됩니다.
3. 포털 인증 - 흐름의 이 단계는 SSO 메커니즘이 사용자 세션을 찾지 못했음을 나타냅니다. 다 음과 같은 여러 가지 이유로 인해 이러한 문제가 발생할 수 있습니다.
 - NAD가 어카운팅 메시지를 전송하도록 구성되지 않았거나 프레임 IP 주소가 어카운팅 메시지에 없습니다

- CPP 포털 FQDN은 초기 인증이 처리된 노드와 다른 ISE 노드의 IP로 확인되었습니다
- 클라이언트는 NAT 뒤에 있습니다

4. 세션 데이터 변경. 이 특정 예에서는 세션 상태가 Unknown에서 Compliant로 변경되었습니다.

5. 네트워크 액세스 디바이스에 대한 COA. 이 COA는 NAD측에서 새 인증을 푸시하고 ISE측에서 새 권한 부여 정책을 할당하려면 성공해야 합니다. COA가 실패한 경우 자세한 보고서를 열어 이유를 조사할 수 있습니다. COA의 가장 일반적인 문제는 다음과 같습니다.

- COA 시간 초과 - 요청을 보낸 PSN이 NAD 측에서 COA 클라이언트로 구성되지 않았거나 COA 요청이 도중에 삭제되었습니다.
- COA negative ACK - COA가 NAD에 수신되었지만 COA 작업을 확인할 수 없는 이유를 나타냅니다. 이 시나리오에서는 세부 보고서에 자세한 설명이 포함되어야 합니다.

이 예에서 ASA가 NAD로 사용되므로 사용자에 대한 후속 인증 요청이 표시되지 않습니다. 이는 ISE가 VPN 서비스 중단을 방지하는 ASA에 대한 COA 푸시를 사용한다는 사실 때문에 발생합니다. 이러한 시나리오에서는 COA 자체에 새로운 권한 부여 매개변수가 포함되므로 재인증이 필요하지 않습니다.

2단계. 클라이언트 프로비저닝 정책 선택 확인 - 이 작업을 위해 어떤 클라이언트 프로비저닝 정책이 사용자에 대해 적용되었는지 파악하는 데 도움이 되는 ISE에 대한 보고서를 실행할 수 있습니다.

탐색 Operations > Reports Endpoint and Users > Client Provisioning 필요한 날짜에 보고서를 실행합니다.

Client Provisioning ⓘ
From 2017-02-04 00:00:00.0 to 2017-03-06 21:06:33.980

+ My Reports Export To Schedule

Logged At	Server	Event	Identity	Client Provisioning Policy Matched	Failure Reason
2017-02-24 18:33:46...	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44	
2017-02-23 18:46:42...	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44	
2017-02-23 17:59:07...	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44	

그림 4-2

이 보고서를 사용하여 어떤 클라이언트 프로비저닝 정책이 선택되었는지 확인할 수 있습니다. 또한, 실패의 경우, 이유를 제시해야 합니다. Failure Reason 열.

3단계. 상태 보고서 확인 - 탐색 Operations > Reports Endpoint and Users > Posture Assessment by Endpoint.

Posture Assessment by Endpoint ⓘ
From 2017-02-04 00:00:00.0 to 2017-03-06 21:24:17.603

+ My Reports Export To Schedule

Logged At	Status	Details	Identity	Endpoint ID	IP Address	Endpoint OS
2017-02-24 18:34:31...	✓		user1	00:0B:7F:D0:F8:F4	10.62.145.44	Windows 7 Professional 64-
2017-02-23 19:33:35...	✓		user1	00:0B:7F:D0:F8:F4	10.62.145.44	Windows 7 Professional 64-

그림 4-3

여기서 각 특정 이벤트에 대한 세부 보고서를 열 수 있습니다. 예를 들어, 이 보고서가 속한 세션 ID,

ISE에서 엔드포인트에 대해 선택한 정확한 상태 요구 사항 및 각 요구 사항의 상태를 확인할 수 있습니다.

문제 해결

일반 정보

포스처 프로세스 트러블슈팅을 위해 포스처 프로세스가 발생할 수 있는 ISE 노드에서 이러한 ISE 구성 요소를 디버그하도록 활성화해야 합니다.

- client-webapp - 에이전트 프로비저닝을 담당하는 구성 요소입니다. 대상 로그 파일 `guest.log` 및 `ise-psc.log`.
- guestaccess - 클라이언트 프로비저닝 포털 구성 요소 및 세션 소유자 조회를 담당하는 구성 요소 (요청이 잘못된 PSN으로 오는 경우). 대상 로그 파일 - `guest.log`.
- provisioning - 클라이언트 프로비저닝 정책 처리를 담당하는 구성 요소입니다. 대상 로그 파일 - `guest.log`.
- posture - 모든 상태 관련 이벤트. 대상 로그 파일 - `ise-psc.log`.

클라이언트 측 문제 해결의 경우 다음을 사용할 수 있습니다.

- acisensa.log -클라이언트 측에서 클라이언트 프로비저닝 실패 시, 이 파일은 NSA가 다운로드 (일반적으로 Windows의 다운로드 디렉토리) 된 같은 폴더에 생성 됩니다.
- AnyConnect_ISEPosture.txt - 이 파일은 디렉토리의 DART 번들에서 찾을 수 있습니다. Cisco AnyConnect ISE Posture Module. ISE PSN 검색 및 포스처 플로우의 일반적인 단계에 대한 모든 정보가 이 파일에 기록됩니다.

일반적인 문제 해결

SSO 관련 문제

SSO가 성공한 경우 `ise-psc.log`, 이 메시지 집합은 세션 조회가 성공적으로 완료되었으며 포털에서 인증을 건너뛸 수 있음을 나타냅니다.

<#root>

```
2016-11-09 15:07:35,951 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] cisco.cpm.posture.runtime.PostureRu
looking for Radius session with input values : sessionId: null, MacAddr: null, ipAddr: 10.62.145.121
```

```
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] cisco.cpm.posture.runtime.PostureRu
```

```
Found session c0a801010002600058232bb8 using ipAddr 10.62.145.121
```

텍스트 창 5-1

엔드포인트 IP 주소를 검색 키로 사용하여 이 정보를 찾을 수 있습니다.

게스트 로그에서 조금 더 나중에 인증을 건너뛰었음을 확인해야 합니다.

<#root>

```
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] guestaccess.flowmanager.step.cp.CPI
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] com.cisco.ise.portalSessionManager.
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] com.cisco.ise.portalSessionManager.
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] guestaccess.flowmanager.step.cp.CPI

Login step will be skipped, as the session =c0a801010002600058232bb8 already established for mac address

2016-11-09 15:07:36,066 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] cpm.guestaccess.flowmanager.process
```

텍스트 창 5-2

SSO가 작동하지 않을 경우 ise-psc log 파일에 세션 조회 실패에 대한 정보가 포함되어 있습니다.

<#root>

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cisco.cpm.posture.runtime.PostureRu

looking for session using IP 10.62.145.44

2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cisco.cpm.posture.runtime.PostureRu

No Radius session found
```

텍스트 창 5-3

의 guest.log 이러한 경우 포털에서 전체 사용자 인증을 확인해야 합니다.

<#root>

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cpm.guestaccess.flowmanager.step.St
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cpm.guestaccess.flowmanager.step.St
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cpm.guestaccess.flowmanager.step.St
```

Returning next step =LOGIN

2017-02-23 17:59:00,780 INFO [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.Ste

텍스트 창 5-4

포털에서 인증이 실패할 경우 포털 컨피그레이션 확인에 주력해야 합니다. 어떤 ID 저장소가 사용 중입니까? 어떤 그룹에 로그인할 권한이 있습니까?

클라이언트 프로비저닝 정책 선택 문제 해결

클라이언트 프로비저닝 정책 실패 또는 잘못된 정책 처리 시 다음을 확인할 수 있습니다. `guest.log` 자세한 내용은 다음 파일을 참조하십시오.

<#root>

2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.C

2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.common.utils.OSMap
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.common.utils.OSMap
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.
2017-02-23 17:59:07,505 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.

:user1:- CP Policy Status =SUCCESS, needToDoVlan=false, CoaAction=NO_COA

텍스트 창 5-5

첫 번째 문자열에서 세션에 대한 정보가 정책 선택 엔진에 주입되는 방법을 확인할 수 있습니다. 정책 일치가 없거나 잘못된 정책 일치의 경우 여기에서 클라이언트 프로비저닝 정책 컨피그레이션과 특성을 비교할 수 있습니다. 마지막 문자열은 정책 선택 상태를 나타냅니다.

상태 프로세스 트러블슈팅

클라이언트 측에서는 프로브 및 그 결과의 조사에 관심을 가져야 합니다. 다음은 성공적인 1단계 프로브의 예입니다.

Date : 02/23/2017
Time : 17:59:57
Type : Unknown
Source : acise

Description : Function: Target::Probe
Thread Id: 0x4F8
File: SwiftHttpRunner.cpp
Line: 1415
Level: debug

PSN probe skuchere-ise22-cpp.example.com with path /auth/status, status is -1..

텍스트 창 5-6

이 단계에서 PSN은 세션 소유자에 대한 AC 정보로 돌아갑니다. 나중에 다음 두 개의 메시지를 볼 수 있습니다.

Date : 02/23/2017
Time : 17:59:58
Type : Unknown
Source : acise

Description : Function: Target::probeRecentConnectedHeadEnd
Thread Id: 0xBE4
File: SwiftHttpRunner.cpp
Line: 1674
Level: debug

Target skuchere-ise22-2.example.com, posture status is Unknown..

텍스트 창 5-7

세션 소유자는 에이전트에게 모든 필수 정보를 반환합니다.

Date : 02/23/2017
Time : 17:59:58
Type : Unknown
Source : acise

Description : Function: SwiftHttpRunner::invokePosture
Thread Id: 0xFCC
File: SwiftHttpRunner.cpp
Line: 1339

Level: debug

```
MSG_NS_SWISS_NEW_SESSION, <?xml version="1.0" ?>
<root>
  <IP></IP>
  <FQDN>skuchere-ise22-2.example.com</FQDN>
  <PostureDomain>posture_domain</PostureDomain>
  <sessionId>c0a801010009e00058af0f7b</sessionId>
  <configUri>/auth/anyconnect?uuid=106a93c0-9f71-471c-ac6c-a2f935d51a36</configUri>
  <AcPackUri>/auth/provisioning/download/81d12d4b-ff58-41a3-84db-5d7c73d08304</AcPackUri>
  <AcPackPort>8443</AcPackPort>
  <AcPackVer>4.4.243.0</AcPackVer>
  <PostureStatus>Unknown</PostureStatus>
  <PosturePort>8443</PosturePort>
  <PosturePath>/auth/perfigo_validate.jsp</PosturePath>
  <PRAConfig>0</PRAConfig>
  <StatusPath>/auth/status</StatusPath>
  <BackupServers>skuchere-ise22-1.example.com,skuchere-ise22-3.example.com</BackupServers>
</root>
```

텍스트 창 5-8

PSN 측에서는 `guest.log` 노드에 오는 초기 요청이 세션을 소유하지 않을 것으로 예상하는 경우:

```
<#root>
```

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
```

```
mac_list from http request ==> 00:0B:7F:D0:F8:F4,00:0B:7F:D0:F8:F4
```

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
```

```
iplist from http request ==> 172.16.31.12,10.62.145.95
```

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
```

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cpm.client.provisioning.utils.Prov
```

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cpm.client.provisioning.utils.Prov
```

```
2017-02-23 17:59:56,368 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
```

```
2017-02-23 17:59:56,369 ERROR [http-bio-10.48.17.249-8443-exec-10] [] cpm.client.provisioning.utils.Prov
```

```
Session Info is null
```

```
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
```

```
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
```

```
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
```

```
Performing MNT look up for macAddress ==> 00-0B-7F-D0-F8-F4
```

```
2017-02-23 17:59:56,539 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
```

```
Performed MNT lookup, found session 0 with session id c0a801010009e00058af0f7b
```

```
2017-02-23 17:59:56,539 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
```

텍스트 창 5-9

여기서 PSN이 먼저 로컬에서 세션을 찾으려고 시도하고 실패 후 IPs 및 MACs 목록을 사용하여 MNT에 대한 요청을 시작하여 세션 소유자를 찾는 것을 볼 수 있습니다.

잠시 후 올바른 PSN에 대한 클라이언트의 요청이 표시되어야 합니다.

<#root>

```
2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
ooking for session using session ID: null, IP addr: [172.16.31.12, 10.62.145.95], mac Addr: [00:0B:7F:D
2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,791 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
Found session c0a801010009e00058af0f7b using ipAddr 172.16.31.12
```

텍스트 창 5-10

다음 단계로, PSN은 이 세션에 대해 클라이언트 프로비저닝 정책 조회를 수행합니다.

<#root>

```
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] com.cisco.cpm.swiss.SwissServer -:::
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,795 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePo
2017-02-23 17:59:58,203 DEBUG [http-bio-10.48.30.41-8443-exec-8][] com.cisco.cpm.swiss.SwissServer -:::
2017-02-23 17:59:58,907 DEBUG [http-bio-10.48.30.41-8443-exec-10][] cisco.cpm.posture.util.AgentUtil -:
Increase Mnt counter at CP:ClientProvisioning.ProvisionedResource.AC-44-Posture
```

텍스트 창 5-11

다음 단계에서 상태 요구 사항 선택 과정을 볼 수 있습니다. 이 단계를 마치면 요구 사항 목록이 준비되고 상담원에게 반환됩니다.

<#root>

```
2017-02-23 18:00:00,372 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureHan
```

```
About to query posture policy for user user1 with endpoint mac 00-0b-7f-d0-f8-f4
```

```
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureMan
```

```
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
```

```
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
```

```
2017-02-23 18:00:00,432 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
```

```
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
```

```
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
```

```
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
```

```
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
```

```
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
```

```
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
```

```
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
```

```
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
```

```
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
```

```
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
```

```
2017-02-23 18:00:03,884 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cpm.posture.runtime.agent.AgentXmlGe
```

```
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cpm.posture.runtime.agent.AgentXmlGe
```

```
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cpm.posture.runtime.agent.AgentXmlGe
```

```
2017-02-23 18:00:04,069 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureHan
```

```
<version>ISE: 2.2.0.470</version>
```

```
<encryption>0</encryption>
```

```
<package>
```

```
<id>10</id>
```

WinDefend

Enable WinDefend

3

0

3

WinDefend

3

301

WinDefend

running

(WinDefend)

```
</package>  
</cleanmachines>
```

텍스트 창 5-12

나중에 상태 보고서가 PSN에 수신되었음을 확인할 수 있습니다.

```
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHan  
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHan
```

텍스트 창 5-13

플로우가 끝나면 ISE는 엔드포인트를 규정 준수로 표시하고 COA를 시작합니다.

```
2017-02-23 18:00:04,272 INFO [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureMana
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureCoA
```

텍스트 창 5-14

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.