ISE 상태 구축 모범 사례 및 고려 사항

목차

소개

이 문서에서는 리디렉션 기반 상태의 여러 활용 사례를 처리하는 몇 가지 기본 구성에 대해 설명합니다.이러한 컨피그레이션에서는 클라이언트가 규정을 준수하지만 NAD(Network Access Device)는 리디렉션 상태이므로 액세스를 제한합니다.

제한 사항

이 문서의 컨피그레이션은 Cisco NAD에서 작동하지만 반드시 서드파티 NAD에는 적용되지 않습니다.

상태 클라이언트 동작

상태 클라이언트는 다음 시간에 프로브를 트리거합니다.

- 초기 로그인
- 레이어 3(L3) 변경/NIC(Network Interface Card) 변경(새 IP 주소, NIC 상태 변경)

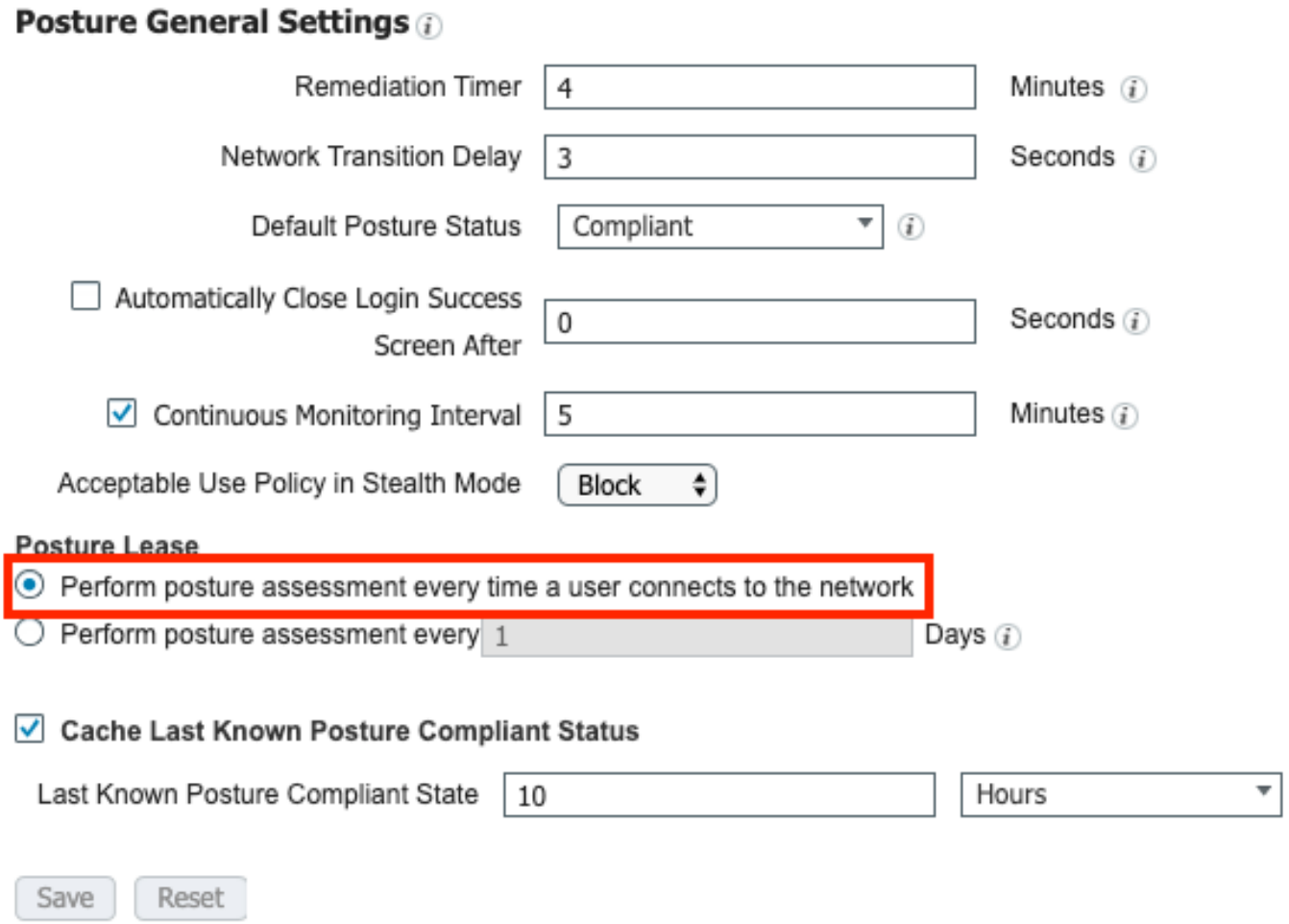
활용 사례

활용 사례 1 - 클라이언트 재인증은 NAD가 새 세션 ID를 생성하도록 강제합니다.

이 활용 사례에서는 클라이언트가 여전히 규정을 준수하지만 재인증 때문에 NAD는 리디렉션 상태(리디렉션 URL 및 액세스 목록)에 있습니다.

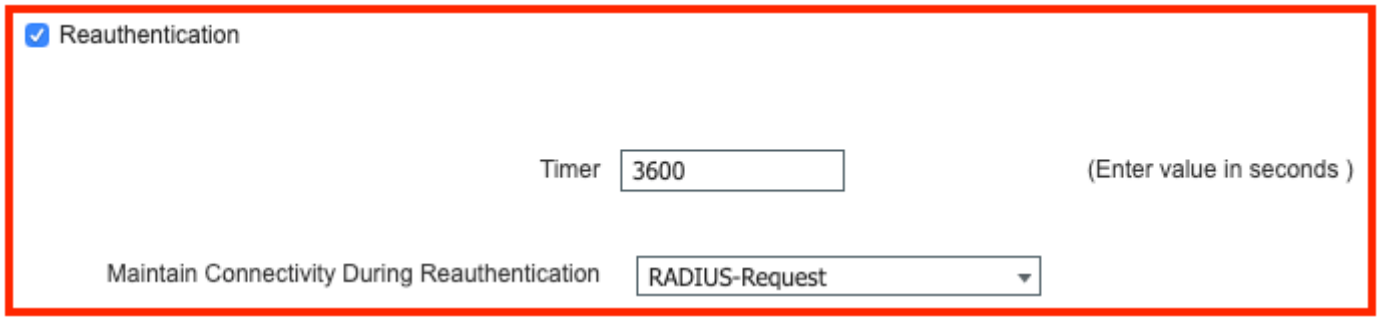
기본적으로 ISE(Identity Services Engine)는 네트워크에 연결할 때마다, 특히 각 새 세션에 대해 상태 평가를 수행하도록 구성됩니다.

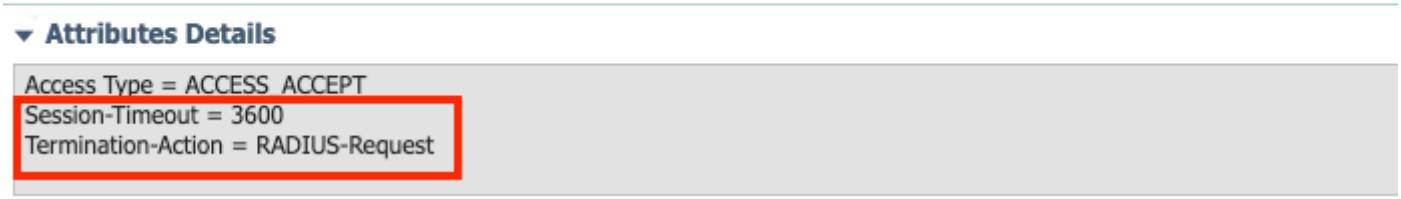
이 설정은 Work Centers(작업 센터) > Posture(포스처) > Settings(설정) > Posture General Settings(포스처 일반 설정)에서 구성됩니다.



NAD가 재인증 시 새 세션 ID를 생성하지 않도록 하려면 권한 부여 프로파일에서 이러한 재인증 값을 구성합니다.표시되는 재인증 타이머는 표준 권장 사항이 아닙니다. 재인증 타이머는 연결 유형(무선/유선), 설계(로드 밸런서의 지속성 규칙이란 무엇입니까) 등을 기반으로 구축별로 고려되어야 합니다.

정책 > 정책 구성 요소 > 결과 > 권한 부여 > 권한 부여 프로파일





스위치에서 ISE에서 재인증 타이머를 가져오려면 각 인터페이스 또는 템플릿을 구성해야 합니다.

```
authentication timer reauthenticate server
```

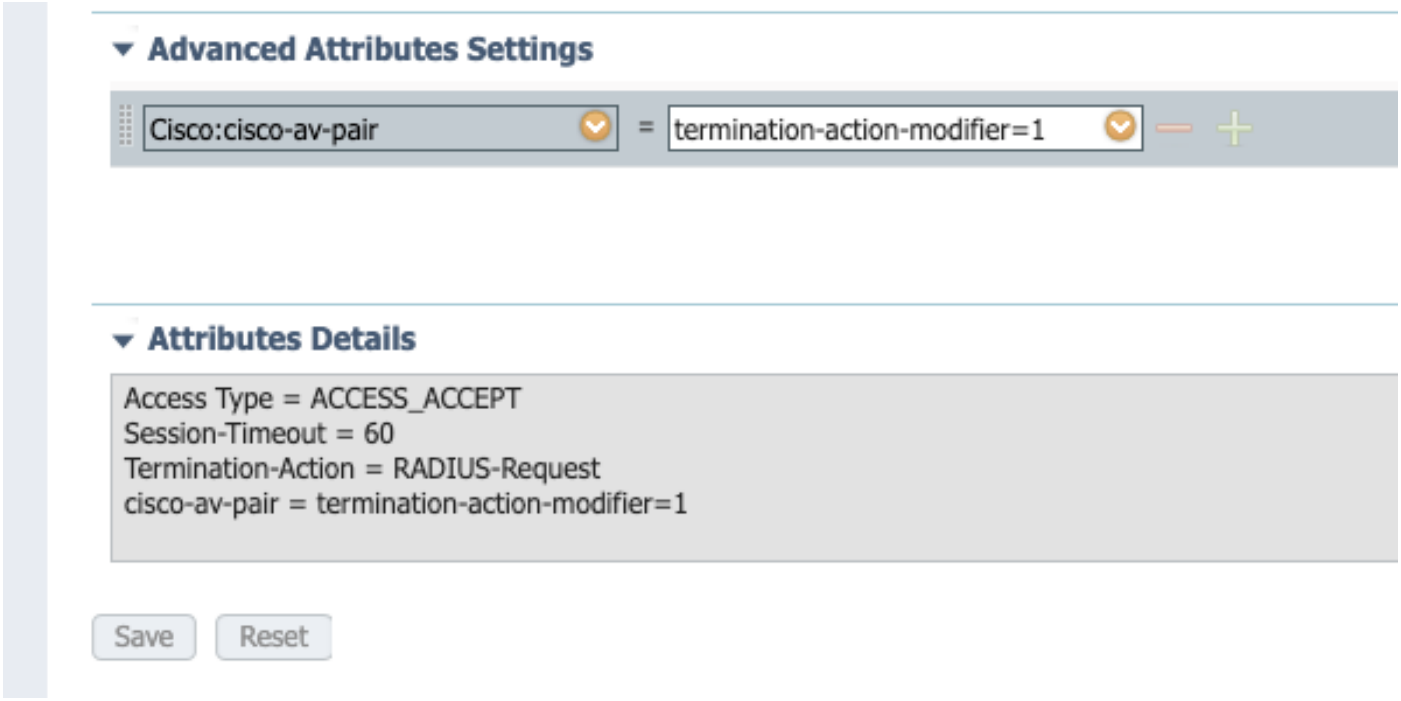
> **참고:**로드 밸런서가 있는 경우 재인증이 원래 PSN(Policy Service)으로 반환되는 방식으로 지속성이 구성되었는지 확인해야 합니다.

활용 사례 2 - 스위치가 주문 MAB DOT1X 및 우선순위 DOT1X MAB(유선)로 구성됩니다.

이 경우 재인증 중에 MAB(MAC Authentication Bypass)가 시도될 때 802.1x 세션에 대한 계정 중지가 전송되기 때문에 재인증이 종료됩니다.

- 인증에 실패할 때 MAB 프로세스에 대해 전송되는 어카운팅 중지가 올바릅니다. 클라이언트의 사용자 이름이 802.1X 사용자 이름에서 MAB 사용자 이름으로 변경되기 때문입니다.
- 어카운팅 중지의 method-id로 dot1x도 올바른 인증 방법이 dot1x이므로 정확합니다.
- Dot1x 메서드가 성공하면 method-id로 계정 시작을 dot1x로 보냅니다.여기에서도 이 동작이 예상대로 수행됩니다.

이 문제를 해결하려면 엔드포인트가 호환 시 사용 되는 authZ 프로파일에서 cisco-av-pair:termination-action-modifier = 1을 구성 합니다.이 AV(Attribute-Value) 쌍은 NAD가 구성된 순서에 관계없이 원래 인증에서 선택한 방법을 재사용하도록 지정합니다.



활용 사례 3 - 무선 클라이언트가 서로 다른 AP에 대한 로밍 및 인증을 서로 다른 컨트롤러로 이동합니다.

이러한 경우, 로밍을 위해 액세스 포인트(AP)가 다른 AP에 도달할 수 있도록 무선 네트워크를 설계해야 합니다.한 가지 예는 WLC(Wireless LAN Controller) SSO(Stateful Switchover) 장애 조치입니다.WLC용 HA(고가용성) SSO에 대한 자세한 내용은 SSO(고가용성) 구축 가이드를 참조하십시오.

활용 사례 4 - 로드 밸런서가 있는 구축(Pre 2.6 Patch 6, 2.7 Patch P2 및 3.0).

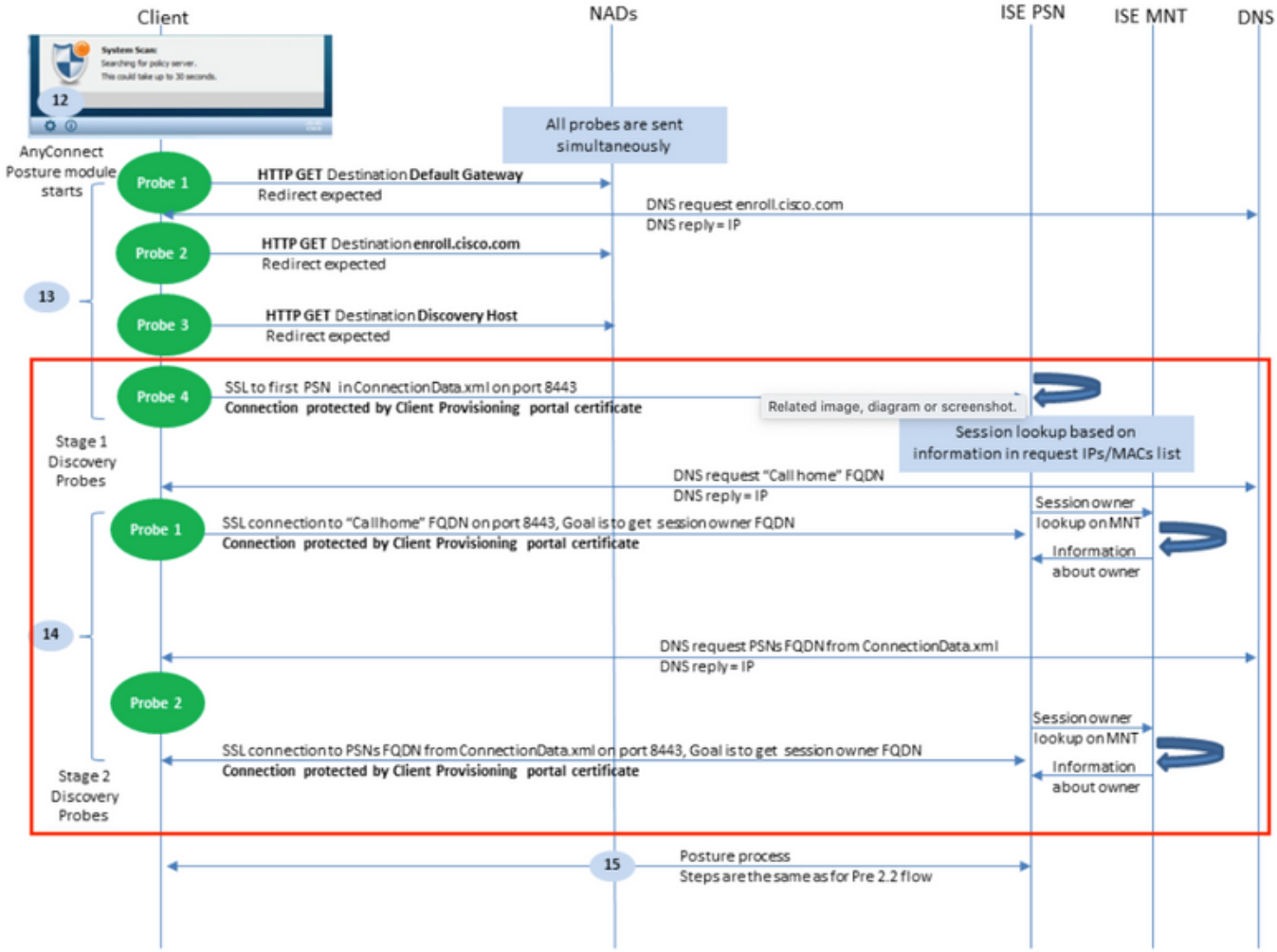
로드 밸런서가 포함된 구축에서는 이전 활용 사례를 변경한 후 세션이 동일한 PSN으로 계속 이동하는지 확인해야 합니다.이 단계에 나열된 버전/패치 이전에 상태 상태는 Light Data Diruption(이전의 Light Session Directory)을 통해 노드 간에 복제되지 않습니다. 따라서 서로 다른 PSN에서 다른 상태 결과를 반환할 수 있습니다.

지속성이 올바르게 구성되지 않은 경우 재인증되는 세션은 원래 사용된 세션과 다른 PSN으로 이동할 수 있습니다.이 경우 새 PSN은 세션 규정 준수 상태를 알 수 없음으로 표시하고 ACL(Redirect Access Control List)/URL로 authZ 결과를 전달하여 엔드포인트 액세스를 제한할 수 있습니다.다시, NAD의 이 변경 사항은 상태 모듈에서 인식되지 않으며 프로브는 트리거되지 않습니다.

로드 밸런서를 구성하는 방법에 대한 자세한 내용은 Cisco 및 F5 구축 가이드를 참조하십시오.BIG-IP를 사용한 ISE 로드 밸런싱.부하 분산 환경에서 ISE 구축을 위한 모범 사례 설계의 개요 및 F5 관련 구성을 제공합니다.

활용 사례 5 - 2단계 검색 프로브는 클라이언트가 인증되는 것과 다른 서버에서 응답합니다(2.6 이전 패치 6, 2.7 패치 2 및 3.0).

이 다이어그램의 빨간색 상자 내의 프로브를 확인합니다.



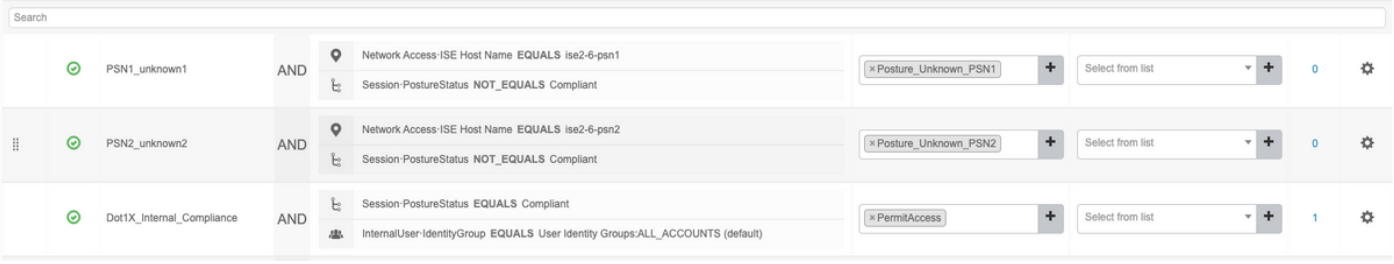
PSN은 5일 동안 세션 데이터를 저장하므로, 클라이언트가 해당 노드를 더 이상 인증하지 않더라도 "호환" 세션에 대한 세션 데이터는 원래 PSN에 계속 유지됩니다.빨간색 상자에 포함된 프로브가 현재 세션을 인증하는 PSN 이외의 PSN에 의해 응답되며 PSN이 이전에 이 엔드포인트를 소유했으며 이 규정 준수를 표시한 경우, 엔드포인트의 상태 모듈의 상태 및 현재 인증 PSN이 일치하지 않을 수 있습니다.

다음은 이러한 불일치가 발생할 수 있는 몇 가지 일반적인 시나리오입니다.

- 네트워크 연결을 끊으면 엔드포인트에 대한 계정 관리 중지가 수신되지 않습니다.
- NAD가 한 PSN에서 다른 PSN으로 장애 조치되었습니다.
- 로드 밸런서는 동일한 엔드포인트의 다른 PSN에 인증을 전달합니다.

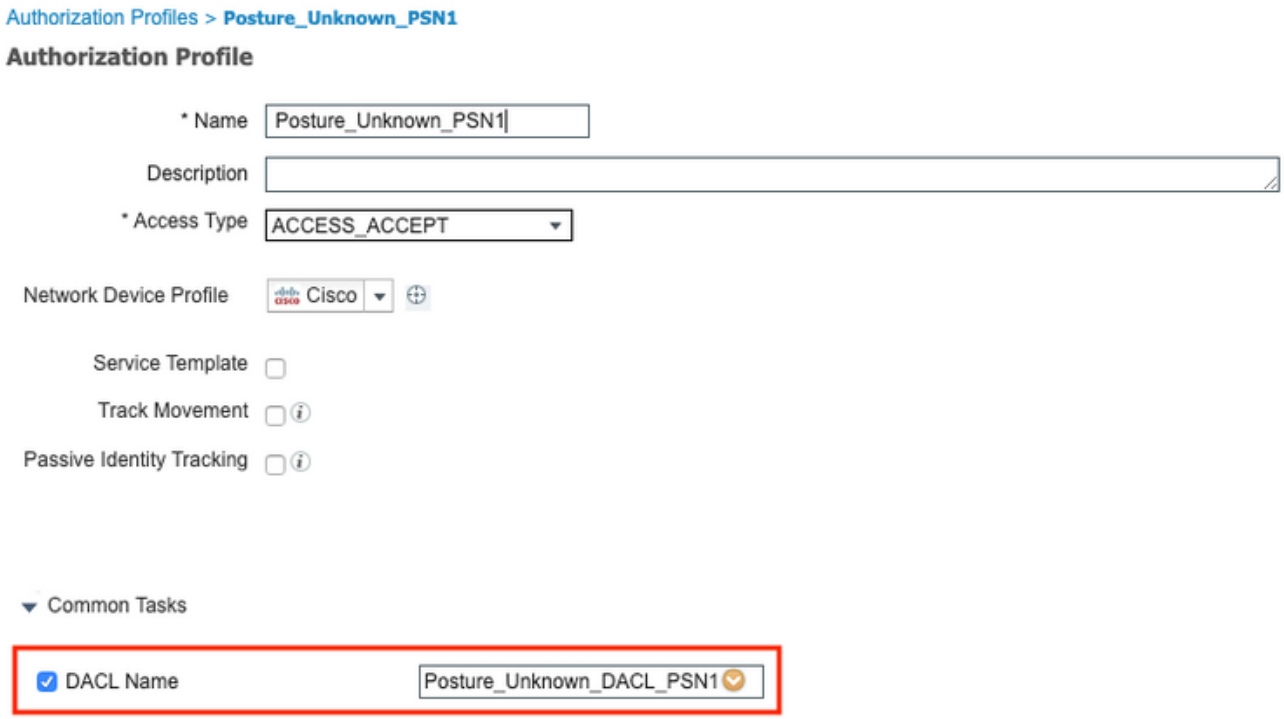
이 동작으로부터 보호하기 위해 ISE는 특정 엔드포인트의 검색 프로브만 현재 인증하는 PSN에 연결하도록 구성할 수 있습니다.이를 위해 구축의 각 PSN에 대해 다른 권한 부여 정책을 구성합니다.이러한 정책에서는 authZ 조건에 지정된 PSN에만 프로브를 허용하는 DACL(Downloadable Access Control List)을 포함하는 다른 authZ 프로파일을 참조합니다.다음 예를 참조하십시오.

각 PSN에는 알 수 없는 상태 상태에 대한 규칙이 있습니다.

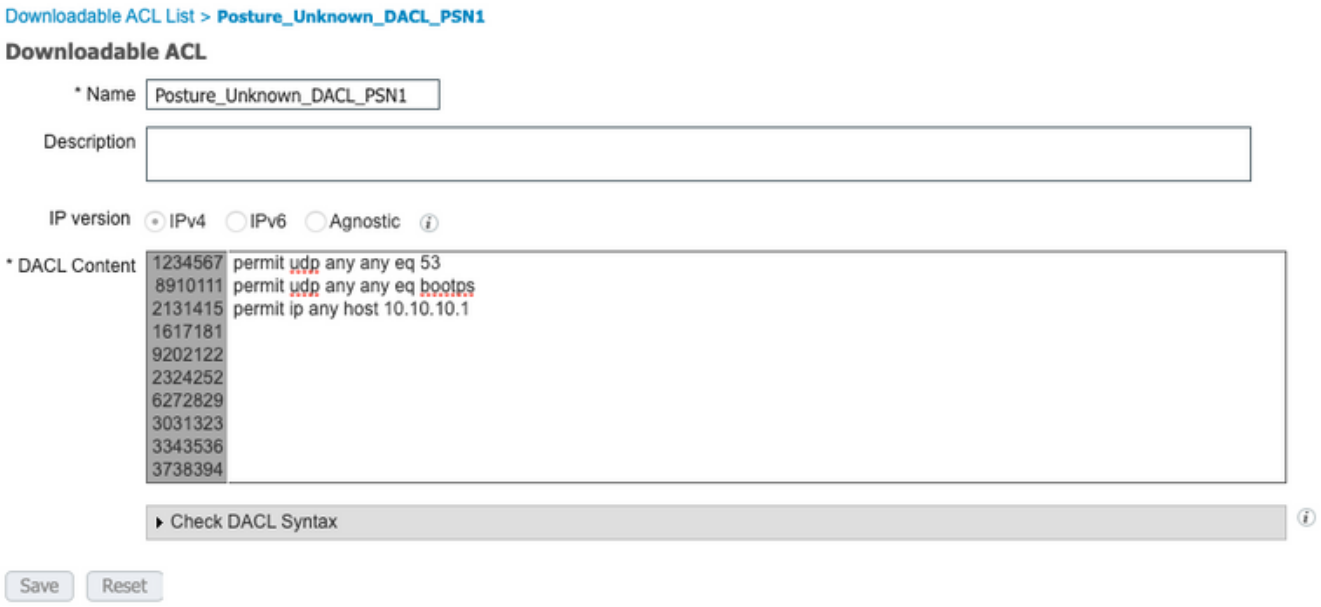


각 개별 프로파일은 다른 DACL을 참조합니다.

참고:무선의 경우 Airespace ACL을 사용합니다.



각 DACL은 인증을 처리하는 PSN에 대한 프로브 액세스만 허용합니다.



이전 예에서 10.10.10.1은 PSN 1의 IP 주소입니다. 참조되는 DACL은 필요에 따라 추가 서비스 /IP에 대해 변경될 수 있지만 인증을 처리하는 PSN에만 대한 액세스를 제한해야 합니다.

동작 변경 포스트 2.6 패치 6, 2.7 패치 2 및 3.0

상태 상태가 Light Data Distribution 프레임워크를 통해 RADIUS 세션 디렉토리에 추가되었습니다

.모든 PSN에서 상태 상태 업데이트를 수신할 때마다 구축의 모든 PSN에 복제됩니다.이 변경 사항이 적용되면, 서로 다른 인증에서 서로 다른 PSN에 도달하는 인증 및 프로브의 영향이 제거되며, 모든 PSN은 현재 인증 위치에 관계없이 모든 엔드포인트에 응답할 수 있어야 합니다.

이 문서의 5가지 활용 사례에서는 다음 동작을 고려합니다.

활용 사례 1 - 클라이언트 재인증은 NAD가 새 세션 ID를 생성하도록 강제합니다.클라이언트는 여전히 규정을 준수하지만 재인증 때문에 NAD는 리디렉션 상태(리디렉션 URL 및 액세스 목록)입니다.

- 이 동작은 변경되지 않으며 ISE 및 NAD에 이 컨피그레이션을 구현해야 합니다.

활용 사례 2 - 스위치가 주문 MAB DOT1X 및 우선순위 DOT1X MAB(유선)로 구성됩니다.

- 이 동작은 변경되지 않으며 ISE 및 NAD에 이 컨피그레이션을 구현해야 합니다.

활용 사례 3 - 무선 클라이언트가 서로 다른 AP에 대한 로밍 및 인증을 서로 다른 컨트롤러로 이동합니다.

- 이 동작은 변경되지 않으며 ISE 및 NAD에 이 컨피그레이션을 구현해야 합니다.

활용 사례 4 - 로드 밸런서가 있는 구축.

- 로드 밸런싱 가이드에 정의된 모범 사례를 계속 따라야 하지만, 로드 밸런서가 인증을 다른 PSN으로 전달하는 경우 올바른 상태 상태를 클라이언트에 반환해야 합니다.

활용 사례 5 - 2단계 검색 프로브는 클라이언트가 인증되는 서버와 다른 서버에서 응답합니다.

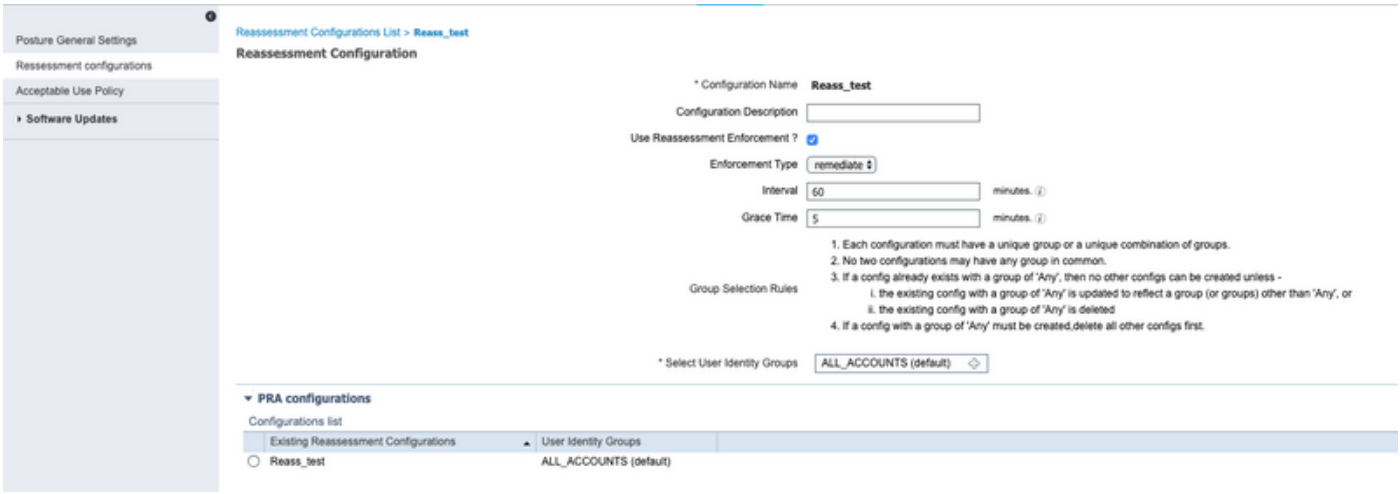
- 새 동작에 문제가 되어서는 안 되며 PSN별 권한 부여 프로파일이 필요하지 않아야 합니다.

동일한 SessionID를 유지할 때 고려할 사항

이 문서에 나열된 방법을 사용할 경우 네트워크에 연결된 상태로 남아 있는 사용자는 오랫동안 규정을 준수할 수 있습니다.재인증하더라도 sessionID는 변경되지 않으므로 ISE는 규정 준수 상태와 일치하는 규칙에 대해 AuthZ 결과를 계속 전달합니다.

이 경우 엔드포인트가 정의된 간격으로 기업 정책을 계속 준수하도록 Posture가 필요하도록 정기 재평가를 구성해야 합니다.

Work Centers(작업 센터) > Posture(포스처) > Settings(설정) > Ressessment configurations(평가 컨피그레이션)에서 구성할 수 있습니다.


Posture General Settings
Ressessment configurations
Acceptable Use Policy
Software Updates
Reassessment Configurations List > Reass_test
Reassessment Configuration
* Configuration Name
Reass_test
Configuration Description
Use Reassessment Enforcement ?
Enforcement Type
remediate
Interval
60
minutes.
Grace Time
5
minutes.
Group Selection Rules
1. Each configuration must have a unique group or a unique combination of groups.
2. No two configurations may have any group in common.
3. If a config already exists with a group of 'Any', then no other configs can be created unless -
i. the existing config with a group of 'Any' is updated to reflect a group (or groups) other than 'Any', or
ii. the existing config with a group of 'Any' is deleted
4. If a config with a group of 'Any' must be created,delete all other configs first.
* Select User Identity Groups
ALL_ACCOUNTS (default)
PRA configurations
Configurations list
Existing Reassessment Configurations
User Identity Groups
Reass_test
ALL_ACCOUNTS (default)