ID 기반 네트워크용 SXP 및 IBNS 2.0으로 스위치 구성

목차

소개

이 문서에서는 ID 기반 네트워킹을 위해 SXP 및 IBNS 2.0을 사용하는 Cisco 스위치를 구성하는 절차에 대해 설명합니다.

사전 요구 사항

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE(Identity Services Engine) 버전 3.3 패치 4
- Cisco Catalyst 스위치 3850

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.

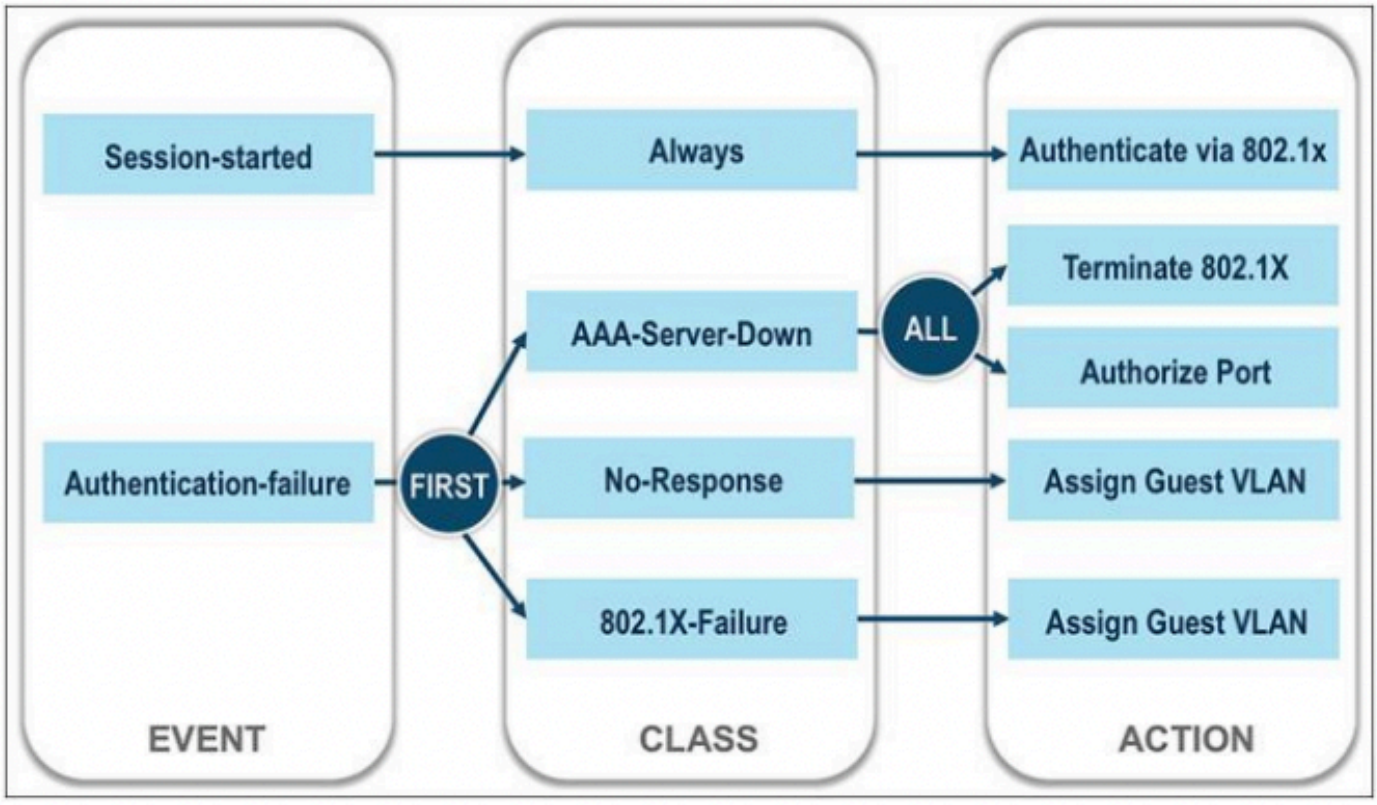
배경 정보

ID 제어 정책은 액세스 세션 관리자가 특정 조건 및 엔드포인트 이벤트에 대한 응답으로 수행하는 작업을 정의합니다. 일관된 정책 언어를 사용하여 다양한 시스템 작업, 조건 및 이벤트를 결합하여

이러한 정책을 구성할 수 있습니다.

제어 정책은 인터페이스에 적용되며 주로 세션에서 엔드포인트 인증 관리 및 서비스 활성화를 담당합니다. 각 제어 정책은 하나 이상의 규칙 및 해당 규칙의 평가 방법을 결정하는 결정 전략으로 구성됩니다.

제어 정책 규칙은 제어 클래스(유연한 조건문), 조건 평가를 트리거하는 이벤트 및 하나 이상의 작업을 포함한다. 관리자는 특정 이벤트에 의해 트리거되는 작업을 정의하지만, 일부 이벤트에는 미리 정의된 기본 작업이 함께 제공됩니다.



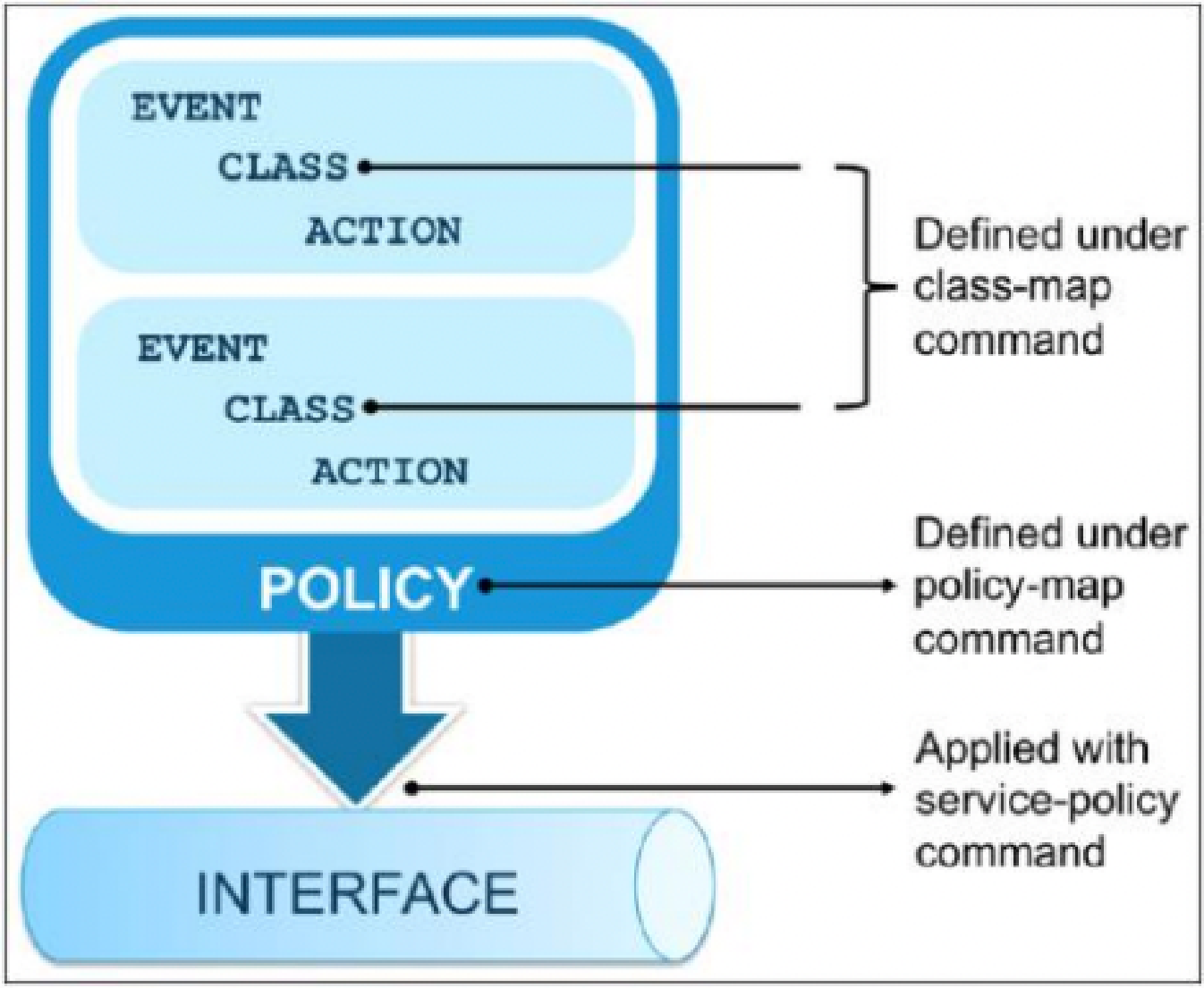
ID 제어 정책

ID 제어 정책 컨피그레이션 개요

제어 정책은 이벤트, 조건 및 작업을 사용하여 시스템 동작을 정의합니다. 제어 정책 구성에는 세 가지 주요 단계가 포함됩니다.

1. 컨트롤 클래스 만들기:
   제어 클래스는 제어 정책을 활성화하는 데 필요한 조건을 정의합니다. 각 클래스에는 true 또는 false로 평가되는 여러 조건이 있을 수 있습니다. 클래스가 true로 간주되기 위해 모든, 모든 또는 어떤 조건도 true여야 하는지 여부를 설정할 수 있습니다. 또는 관리자는 조건이 없고 항상 true로 평가되는 기본 클래스를 사용할 수 있습니다.
2. 제어 정책을 생성합니다.
   제어 정책에는 하나 이상의 규칙이 포함되어 있습니다. 각 규칙에는 제어 클래스, 조건 검사를 트리거하는 이벤트 및 하나 이상의 작업이 포함됩니다. 작업은 순서대로 번호가 매겨지고 실행됩니다.
3. 제어 정책을 적용합니다.

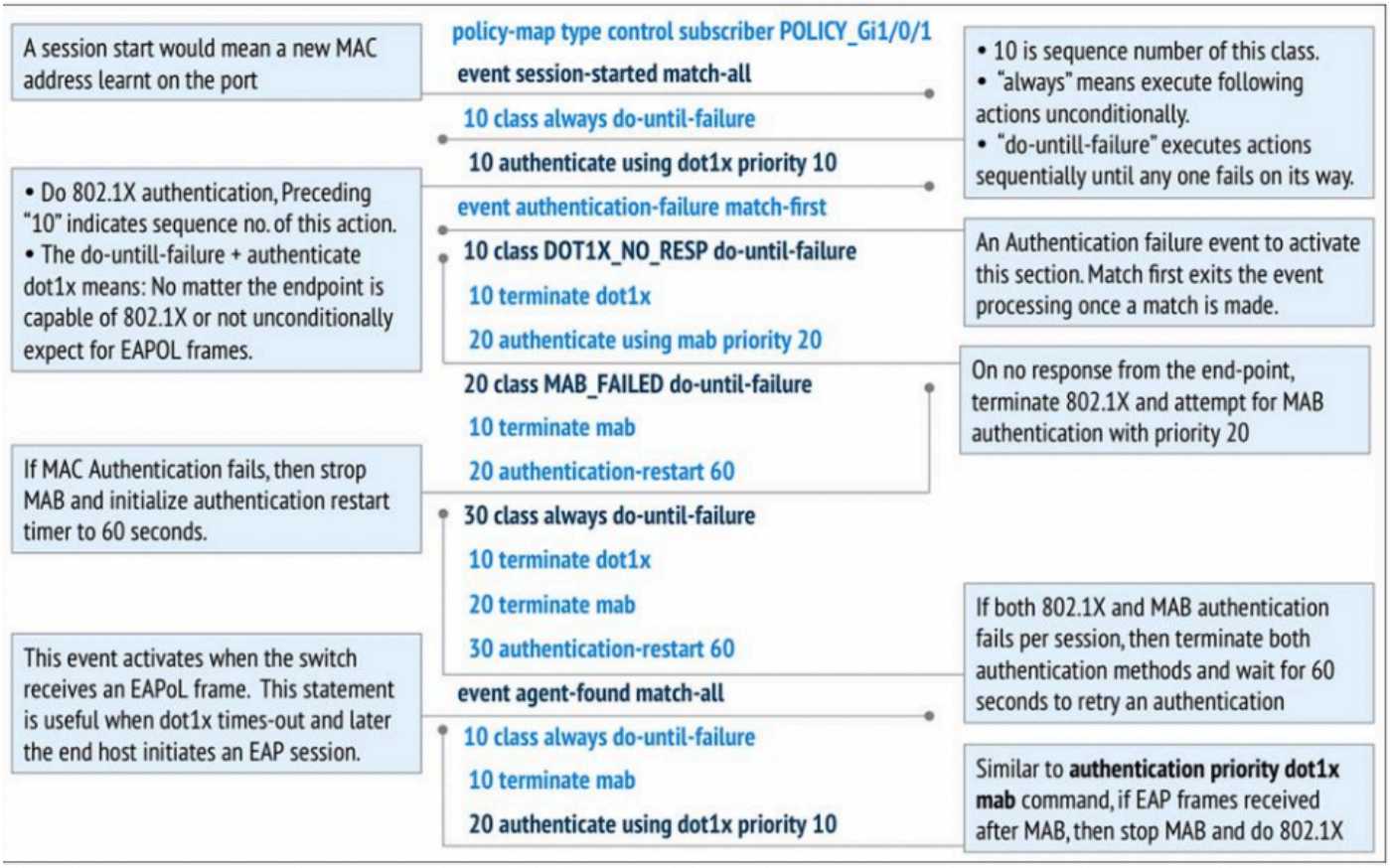
마지막으로, 인터페이스에 제어 정책을 적용하여 활성화합니다.



ID 제어 정책 컨피그레이션

authentication display new-style 명령은 레거시 컨피그레이션을 새 스타일로 변환합니다.

switch#authentication display new-style



ID 제어 정책 해석

구성

스위치 구성

WS-C3850-48F-E#show run aaa

!

aaa 인증 dot1x 기본 그룹 radius 로컬

aaa 인증 네트워크 기본 그룹 radius 로컬

사용자 이름 admin 비밀번호 0 xxxxxx

!

!

!

!

radius 서버 ISE1

주소 ipv4 10.127.197.xxx 인증 포트 1812 계정 포트 1813

pac 키 xxxx@123

!

!

aaa 그룹 서버 radius ISE2

서버 이름 ISE1

!

!

!

!

aaa 새 모델

aaa session-id common

!

aaa 서버 radius 동적 작성자

클라이언트 10.127.197.xxx 서버 키 xxxx@123

dot1x 시스템 인증 제어

!

WS-C3850-48F-E#show run | in POLICY_Gi1/0/45

policy-map type control subscriber POLICY_Gi1/0/45

service-policy type control 가입자 POLICY_Gi1/0/45

WS-C3850-48F-E#show run | sec POLICY_Gi1/0/45

policy-map type control subscriber POLICY_Gi1/0/45

이벤트 세션 시작됨 match-all

  10 클래스는 항상 실패하기 전까지 수행

   10 dot1x 우선 순위를 사용하여 인증 10

event authentication-failure match-first

  5 클래스 DOT1X_FAILED do-until-failure

   10 dot1x 종료

20 인증-재시작 60

10 클래스 DOT1X_NO_RESP do-until-failure

10 dot1x 종료

20 mab 우선순위를 사용하여 인증 20

20 클래스 MAB_FAILED do-until-failure

10 mab 종료

20 인증-재시작 60

40 클래스는 항상 실패할 때까지 수행

10 dot1x 종료

20 mab 종료

30 authentication-restart 60

이벤트 에이전트에서 찾은 match-all

10 클래스는 항상 실패하기 전까지 수행

10 mab 종료

20 dot1x 우선 순위 10을 사용하여 인증

event authentication-success match-all

10 클래스는 항상 실패하기 전까지 수행

10 service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE 활성화

service-policy type control 가입자 POLICY_Gi1/0/45

WS-C3850-48F-E#show run interface gig1/0/45

구성을 빌드하는 중...

현재 구성: 303바이트

!

인터페이스 GigabitEthernet1/0/45

switchport access vlan 503

스위치포트 모드 액세스

액세스 세션 호스트 모드 단일 호스트

액세스 세션 닫힘

access-session port-control auto

MAB

cts 역할 기반 적용 없음

dot1x 페이지 인증자

service-policy type control 가입자 POLICY_Gi1/0/45

끝

WS-C3850-48F-E#show run cts

!

cts 권한 부여 목록 ISE2

cts sxp 사용

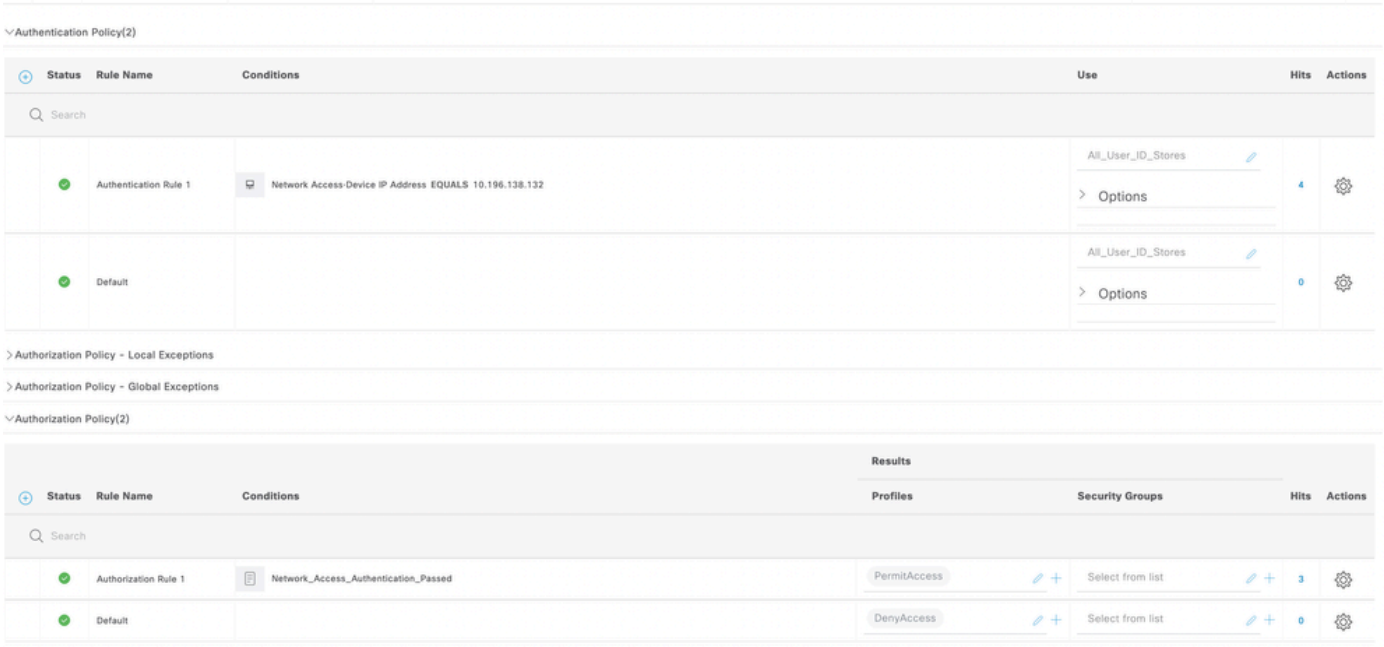
cts sxp 연결 10.127.197.xxx 암호 없음 모드 피어 스피커 보류 시간 0 0

cts sxp 기본 소스-ip 10.196.138.yyy

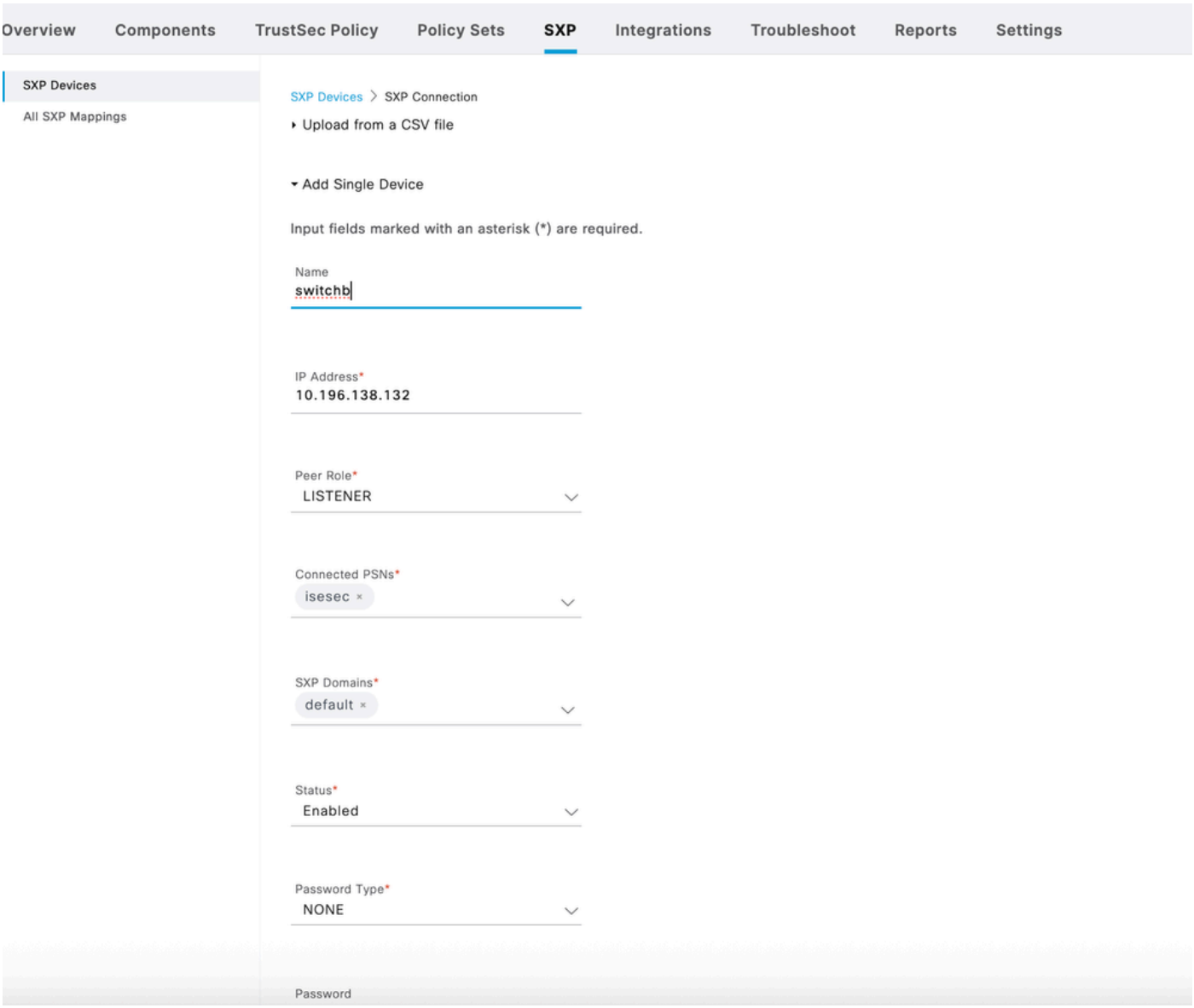
cts sxp 기본 비밀번호 xxxx@123

ISE 구성

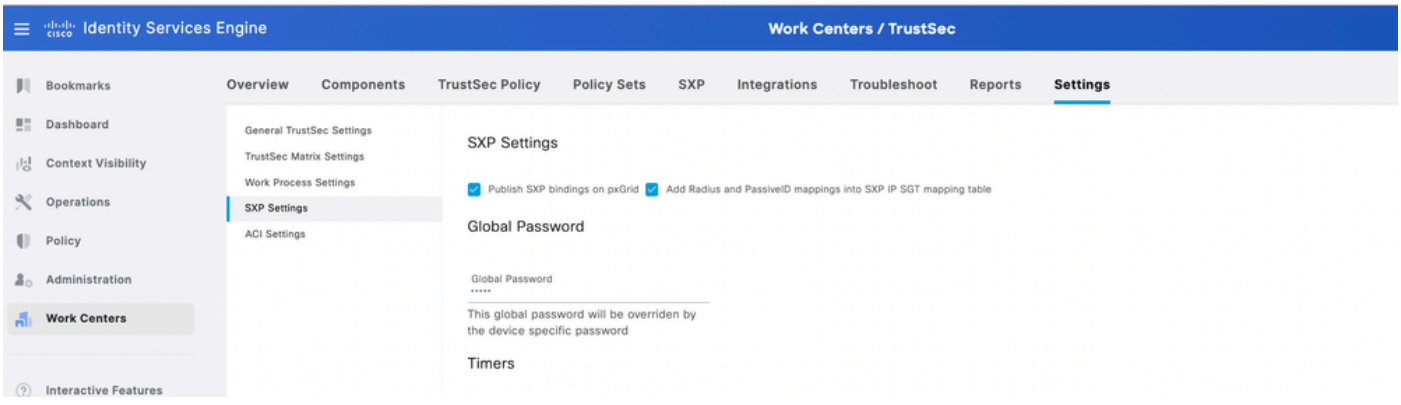
1단계: ISE에서 인증 및 권한 부여 정책 생성



2단계: ISE에서 SXP 디바이스 구성



3단계: SXP Settings(SXP 설정)에서 전역 비밀번호 구성



다음을 확인합니다.

WS-C3850-48F-E#show access-session interface gig1/0/45 상세 정보

인터페이스: GigabitEthernet1/0/45

IIF-ID: 0x1A146F96

MAC 주소: b496.9126.decc

IPv6 주소: 알 수 없음

IPv4 주소: 알 수 없음

사용자 이름: divya123

상태: 승인

도메인: 데이터

작동 호스트 모드: 단일 호스트

작업 제어 디렉터리: 둘 다

세션 시간 초과: 해당 없음

공통 세션 ID: 000000000000000B95163D98

계정 세션 ID: 알 수 없음

핸들: 0x6f000001

현재 정책: POLICY_Gi1/0/45

로컬 정책:

서비스 템플릿: DEFAULT_LINKSEC_POLICY_MUST_SECURE(우선순위 150)

보안 정책: 보안 필요

보안 상태: 링크 보안 해제됨

서버 정책:

메서드 상태 목록:

메서드 상태

dot1x 인증 성공

WS-C3850-48F-E#

WS-C3850-48F-E(config)#do cts sxp conn 표시

SXP: 활성화됨

지원되는 최고 버전: 4

기본 비밀번호: 설정

기본 키 체인: 설정되지 않음

기본 키 체인 이름: 해당 없음

기본 소스 IP: 10.196.138.yyy

연결 다시 시도 열기 기간: 120초

조정 기간: 120초

열기 재시도 타이머가 실행 중입니다.

내보내기에 대한 피어 시퀀스 통과 제한: 설정되지 않음

가져오기에 대한 피어 시퀀스 통과 제한: 설정되지 않음

피어 IP: 10.127.197.xxx

소스 IP: 10.196.138.yyy

연결 상태: On

Conn 버전: 4

연결 기능: IPv4-IPv6-서브넷

연결 보류 시간: 120초

로컬 모드: SXP 수신기

연결 인스턴스 번호: 1

TCP conn fd: 1

TCP 연결 암호: none

보류 타이머가 실행 중입니다.

마지막 상태 변경 이후 기간: 0:00:00:22(dd:hr:mm:초)

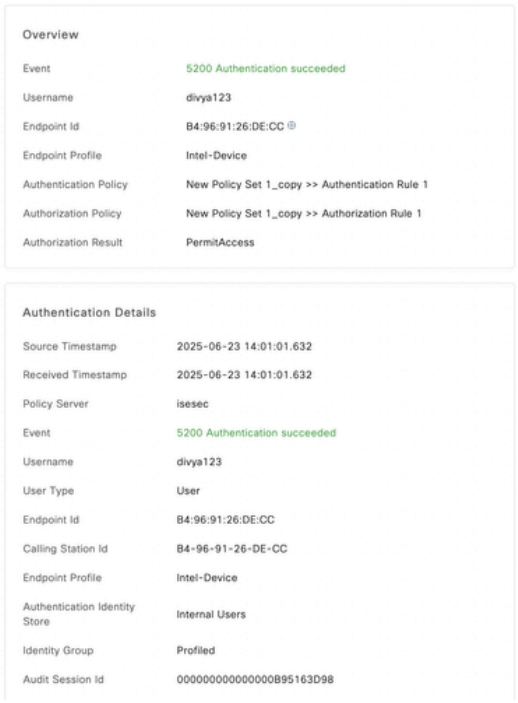
총 SXP 연결 수 = 1

0xFF8CBFC090 VRF:, fd: 1, 피어 ip: 10.127.197.xxx

cdbp:0xFF8CBFC090 <10.127.197.145, 10.196.138.yyy> tableid:0x0

WS-C3850-48F-E(config)#

라이브 로그 보고서에는 적용된 SGT 태그 게스트가 표시됩니다.

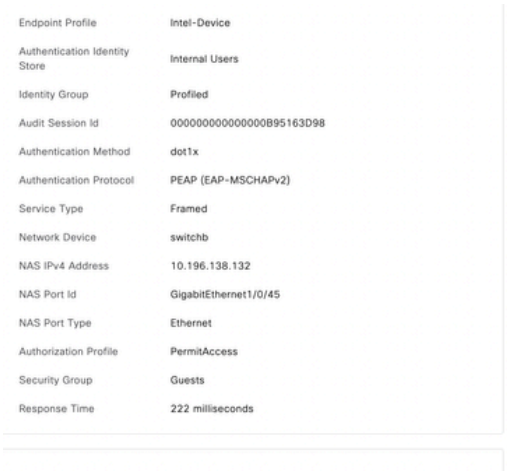


Overview

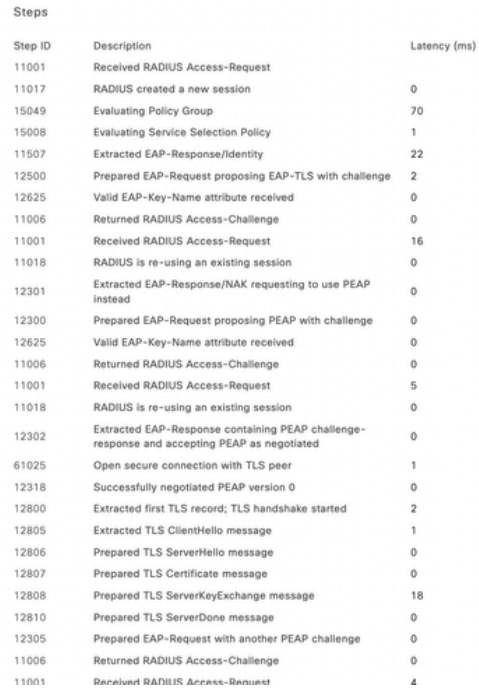
Event	5200 Authentication succeeded
Username	divya123
Endpoint Id	B4:96:91:26:DE:CC
Endpoint Profile	Intel-Device
Authentication Policy	New Policy Set 1_copy >> Authentication Rule 1
Authorization Policy	New Policy Set 1_copy >> Authorization Rule 1
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2025-06-23 14:01:01.632
Received Timestamp	2025-06-23 14:01:01.632
Policy Server	isesec
Event	5200 Authentication succeeded
Username	divya123
User Type	User
Endpoint Id	B4:96:91:26:DE:CC
Calling Station Id	B4-96-91-26-DE-CC
Endpoint Profile	Intel-Device
Authentication Identity Store	Internal Users
Identity Group	Profiled
Audit Session Id	000000000000000B95163D98

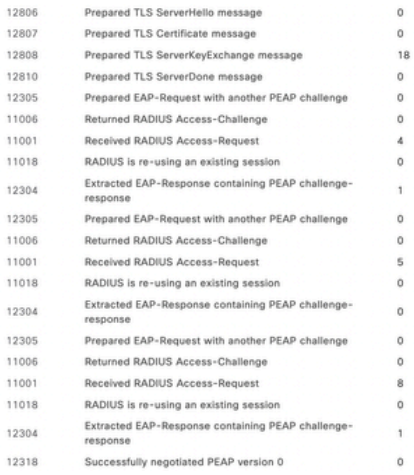


Endpoint Profile	Intel-Device
Authentication Identity Store	Internal Users
Identity Group	Profiled
Audit Session Id	000000000000000B95163D98
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	switchb
NAS IPv4 Address	10.196.138.132
NAS Port Id	GigabitEthernet1/0/45
NAS Port Type	Ethernet
Authorization Profile	PermitAccess
Security Group	Guests
Response Time	222 milliseconds



Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
15049	Evaluating Policy Group	70
15008	Evaluating Service Selection Policy	1
11507	Extracted EAP-Response/Identity	22
12500	Prepared EAP-Request proposing EAP-TLS with challenge	2
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	16
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	0
61025	Open secure connection with TLS peer	1
12318	Successfully negotiated PEAP version 0	0
12800	Extracted first TLS record; TLS handshake started	2
12805	Extracted TLS ClientHello message	1
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	18
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	4



12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	18
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	4
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-response	1
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-response	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	8
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-response	1
12318	Successfully negotiated PEAP version 0	0

문제 해결

스위치에서 dot1x 문제를 해결 하려면 이 디버그를 활성화 합니다.

- 모두 dot1x 디버그

로그 설명

dot1x 패킷:EAPOL pak rx - 버전: 0x1 형식: 0x1 **>>>>>>** 스위치에서 받은 EAPoL 패킷
dot1x 패킷: 길이: 0x0000

dot1x-ev:[b496.9126.decc, Gig1/0/45] 클라이언트가 탐지됨, b496.9126.decc에 대한 세션 시작 이벤트 보내기 **>>>>>** dot1x 클라이언트가 탐지됨

dot1x-ev:[b496.9126.decc, Gig1/0/45] 0x26000007(b496.9126.decc)에 대해 Dot1x 인증이 시작되

었습니다.>>>> dot1x가 시작되었습니다.

%AUTHMGR-5-시작: 인터페이스 Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3에서 클라이언트(b496.9126.decc)에 대해 'dot1x'를 시작합니다.

dot1x-sm:[b496.9126.decc, Gig1/0/45] 0x26000007 />>>> 클라이언트에 !EAP_RESTART를 게시하고 EAP 프로세스를 다시 시작하도록 클라이언트 요청

dot1x-sm:[b496.9126.decc, Gig1/0/45] 클라이언트에 RX_REQ 게시 0x26000007 >>>>> 클라이언트에서 EAPoL 패킷 대기 중

26000007 dot1x-sm:[b496.9126.decc, Gig1/0/45] 0x에 대한 AUTH_START 게시 >>>>> 인증 프로세스 시작

dot1x-ev:[b496.9126.decc, Gig1/0/45] EAPOL 패킷 전송 >>>>> ID 요청
dot1x-packet:EAPOL pak Tx - 버전: 0x3 형식: 0x0
dot1x 패킷: 길이: 0x0005
dot1x-packet:EAP 코드: 0x1 id: 0x1 길이: 0x0005
dot1x 패킷: 유형: 0x1
dot1x 패킷:[b496.9126.decc, Gig1/0/45] 클라이언트 0x로 전송된 EAPOL 패킷26000007

dot1x-ev: [Gig1/0/45] 수신 pkt saddr =b496.9126.decc , daddr = 0180.c200.0003, pae-ether-type = 888e.0100.000a
dot1x 패킷:EAPOL pak rx - 버전: 0x1 형식: 0x0 // ID 응답
dot1x 패킷: 길이: 0x000A

dot1x-sm:[b496.9126.decc, Gig1/0/45] EAPOL_EAP 게시(0x26000007 >>>>> EAPoL 패킷(EAP 응답) 수신, 서버에 대한 요청 준비 중

dot1x-sm:[b496.9126.decc, Gig1/0/45] EAP_REQ 게시(0x26000007 >>>>>> 서버 응답을 받았습니다. EAP 요청을 준비하는 중입니다.

dot1x-ev: [b496.9126.decc, Gig1/0/45] EAPOL 패킷 전송
dot1x-packet:EAPOL pak Tx - 버전: 0x3 형식: 0x0
dot1x 패킷: 길이: 0x0006
dot1x-packet:EAP 코드: 0x1 id: 0xE5 길이: 0x0006
dot1x 패킷: 유형: 0xD
dot1x 패킷:[b496.9126.decc, Gig1/0/45] EAPOL 패킷이 클라이언트 0x26000007 >>>>>> EAP 요청 전송됨

dot1x-ev: [Gig1/0/45] 수신 pkt saddr =b496.9126.decc , daddr = 0180.c200.0003, pae-ether-type = 888e.0100.0006 //EAP 응답 수신
dot1x 패킷:EAPOL pak rx - 버전: 0x1 형식: 0x0
dot1x 패킷: 길이: 0x0006
||
||
||
|| 많은 정보가 스위치와 클라이언트 간에 교환됨에 따라 많은 EAPOL-EAP 및 EAP_REQ 이벤트가

발생합니다
|| 이 이후의 이벤트가 뒤따르지 않으면 타이머와 지금까지 전송된 정보를 확인해야 합니다
||
||
||
dot1x 패킷: [b496.9126.decc, Gig1/0/45] EAP Success(EAP 성공 수신) >>>>> 서버에서 받은 EAP Success(EAP 성공)

dot1x-sm:[b496.9126.decc, Gig1/0/45] EAP_SUCCESS 게시(0x26000007 >>>>> 게시(EAP Success event)

dot1x-sm:[b496.9126.decc,Gig1/0/45] 0x26000007 >>>>> Posting Authentication success(인증 성공 게시)

%DOT1X-5 성공: 인터페이스 Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3에서 클라이언트(b496.9126.decc)에 대한 인증에 성공했습니다.

dot1x 패킷: [b496.9126.decc, Gig1/0/45] EAP 키 데이터가 탐지되어 특성 목록에 추가됨 >>>>>> 서버에서 탐지된 추가 키 데이터

%AUTHMGR-5-성공: 인터페이스 Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3에서 클라이언트(b496.9126.decc)에 대한 권한 부여가 성공했습니다.

dot1x-ev:[b496.9126.decc, Gig1/0/45] 클라이언트 0x26000007 (b496.9126.decc) >>>>> Authorization Success에 대한 Authz Success를 받았습니다.

dot1x-ev:[b496.9126.decc, Gig1/0/45] EAPOL 패킷 전송 >>>>> 클라이언트에 EAP 성공 전송
dot1x-packet:EAPOL pak Tx - 버전: 0x3 형식: 0x0
dot1x 패킷: 길이: 0x0004
dot1x-packet:EAP 코드: 0x3 id: 0xED 길이: 0x0004
dot1x 패킷:[b496.9126.decc, Gig1/0/45] 클라이언트 0x로 전송된 EAPOL 패킷26000007

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.