Switch configureren met SXP en IBNS 2.0 voor op identiteit gebaseerde netwerken

Inhoud

Inleiding

In dit document worden de procedures beschreven voor het configureren van Cisco-Switches met SXP en IBNS 2.0 voor Identity-Based Networking.

Voorwaarden

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Identity Services Engine (ISE) versie 3.3 patch 4
- Cisco Catalyst switch 3850

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

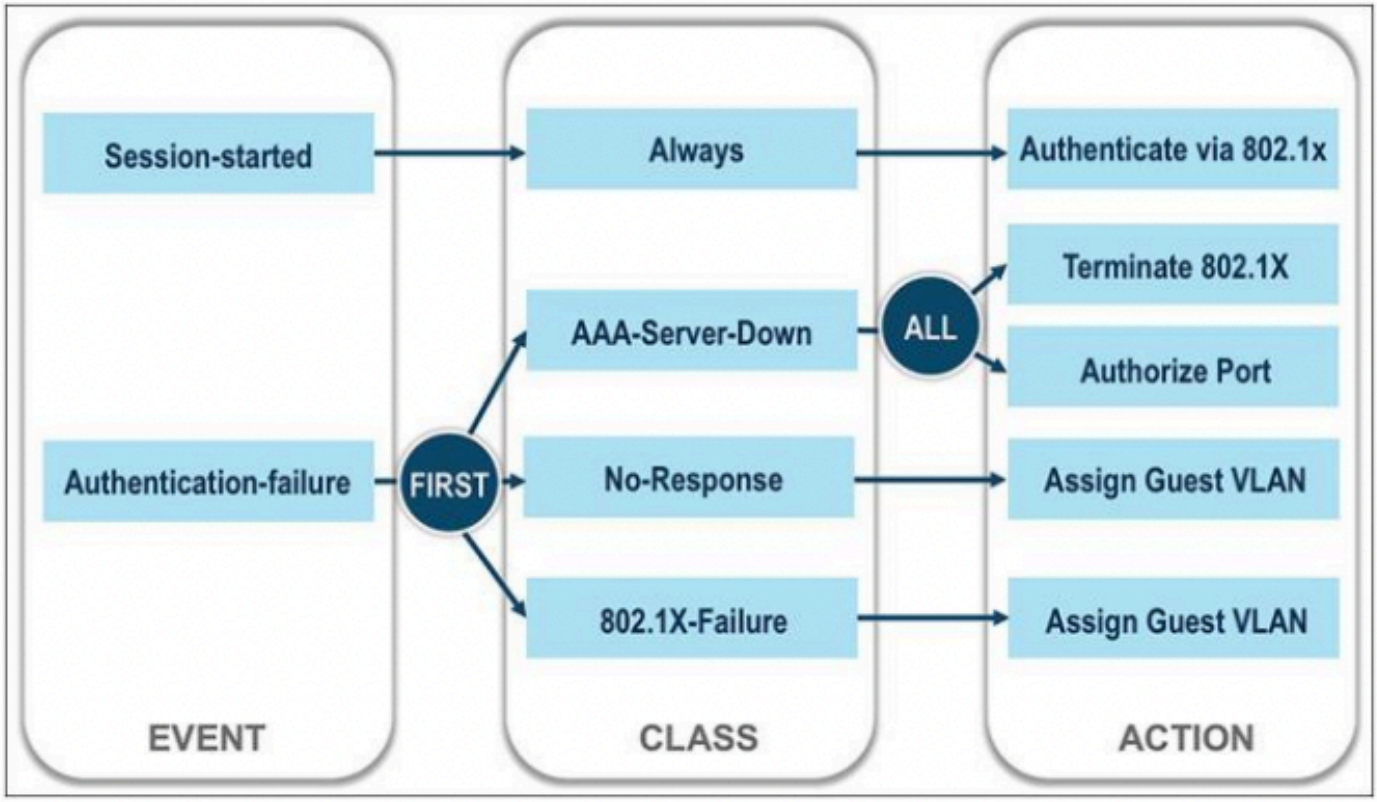
Achtergrondinformatie

Identiteitscontrolebeleid definieert de acties die de Access Session Manager uitvoert als reactie op

specifieke omstandigheden en eindpuntgebeurtenissen. Met behulp van een consistente beleidstaal kunnen verschillende systeemacties, voorwaarden en gebeurtenissen worden gecombineerd om dit beleid te vormen.

Het controlebeleid wordt toegepast op interfaces en is primair verantwoordelijk voor het beheer van endpointverificatie en het activeren van services op sessies. Elk controlebeleid bestaat uit een of meer regels en een beslissingsstrategie die bepaalt hoe die regels worden geëvalueerd.

Een regel voor controlebeleid bevat een controleklasse (een instructie voor flexibele voorwaarden), een gebeurtenis die de voorwaardevaluatie activeert en een of meer acties. Terwijl beheerders bepalen welke acties worden geactiveerd door specifieke gebeurtenissen, worden sommige gebeurtenissen geleverd met vooraf gedefinieerde standaardacties.



identiteitscontrolebeleid

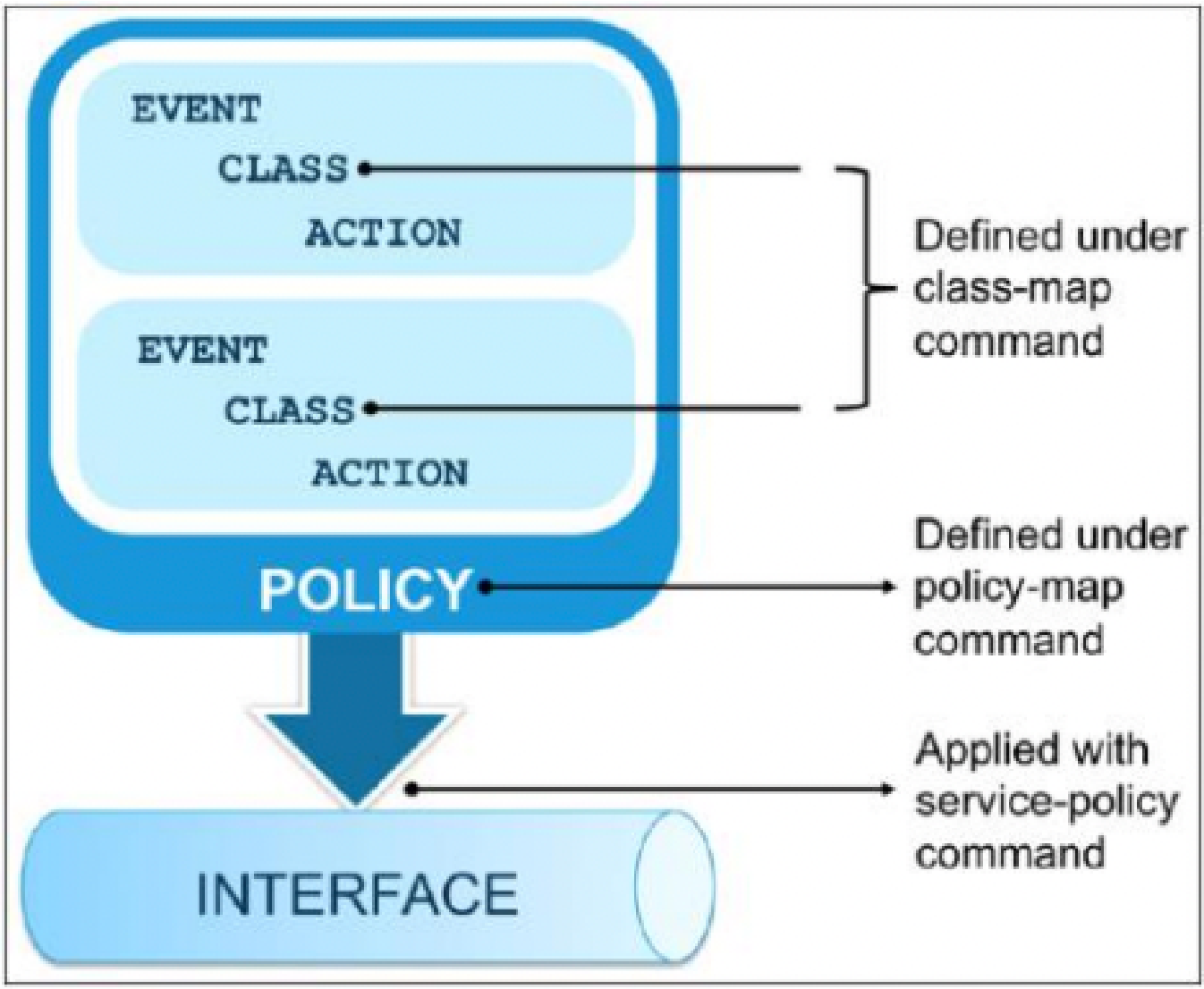
Overzicht van de configuratie van het identiteitscontrolebeleid

Controlebeleid definieert systeemgedrag met behulp van een gebeurtenis, een voorwaarde en een actie. Het configureren van een controlebeleid bestaat uit drie belangrijke stappen:

1. Besturingsklassen maken:
   Een controleklasse definieert de voorwaarden die vereist zijn om een controlebeleid te activeren. Elke klasse kan meerdere voorwaarden hebben die als waar of onwaar worden beoordeeld. U kunt instellen of alle, enige of geen van de voorwaarden waar moet zijn om de klasse als waar te beschouwen. Als alternatief kunnen beheerders een standaardklasse gebruiken die geen voorwaarden heeft en altijd evalueert als true.
2. Het controlebeleid maken:

Een controlebeleid bevat een of meer regels. Elke regel bevat een controleklasse, een gebeurtenis die de conditiecontrole activeert en een of meer acties. Acties worden genummerd en uitgevoerd in volgorde.

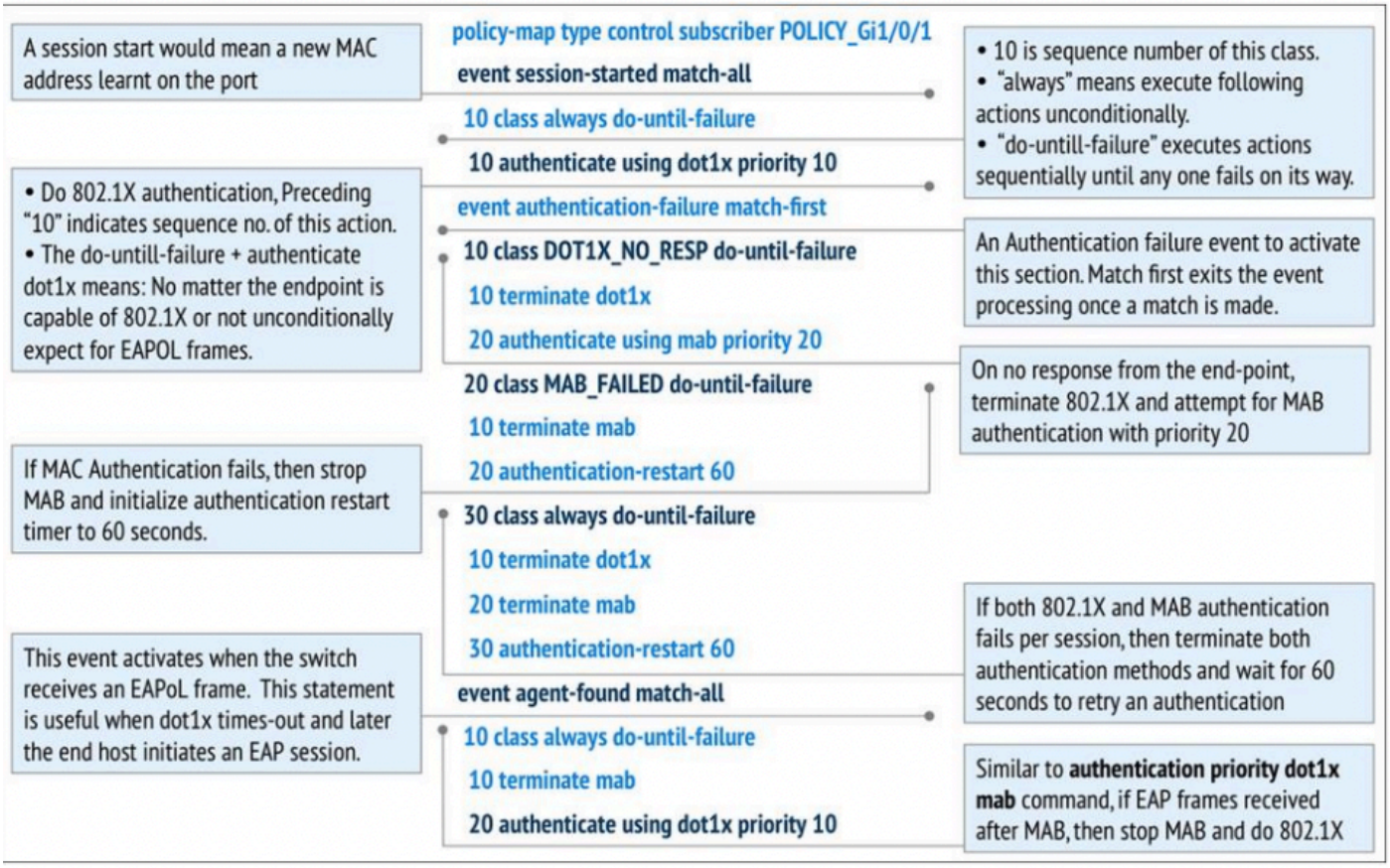
3. Het controlebeleid toepassen:
   Pas ten slotte het controlebeleid toe op een interface om deze te activeren.



Configuratie identiteitscontrolebeleid

Met de opdracht Nieuwe stijl voor weergave van verificatie worden de bestaande configuraties omgezet in een nieuwe stijl.

switch#authenticatie Nieuwe stijl weergeven



Beleid voor identiteitscontrole interpreteren

Configureren

Switchconfiguratie

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

Ja!

AAA-verificatie dot1x Standaardgroepstraal lokaal

AAA Authorization Network Standaardgroep Radius Local

Gebruikersnaam Beheerderswachtwoord 0 xxxxxx

Ja!

Ja!

Ja!

Ja!

radiusserver ISE1

Adres IPv4 10.127.197.xxx Auth-Port 1812 ACCT-Port 1813

PAC-toets xxxx@123

Ja!

Ja!

aaa-groepsserverradius ISE2

servernaam ISE1

Ja!

Ja!

Ja!

Ja!

nieuw AAA-model

AAA Session-ID Algemeen

Ja!

AAA Server Radius Dynamic-Author

Client10.127.197.xxx Serversleutel xxxx@123

dot1x-systeem-auth-controle

Ja!

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

policy-map type controle abonnee POLICY_Gi1/0/45

service-policy type control subscriber POLICY_Gi1/0/45

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

policy-map type controle abonnee POLICY_Gi1/0/45

door een gebeurtenissessie gestarte match-all

  10 Klasse Altijd doen-tot-falen

   10 Verifiëren met DOT1X-prioriteit 10

gebeurtenisverificatie-mislukking match-first

  5 klasse DOT1X_FAILED do-until-failure

   10 punt1x beëindigen

20 Authenticatie-herstart 60

10 klasse DOT1X_NO_RESP do-until-failure

10 punt1x beëindigen

20 Authenticeren met behulp van mab Priority 20

20 klasse MAB_FAILED do-until-failure

10 Beëindig MAB

20 Authenticatie-herstart 60

40 Klasse Altijd doen-tot-falen

10 punt1x beëindigen

20 Beëindig MAB

30 Verificatie-Opnieuw starten 60

Event Agent-Found Match-All

10 Klasse Altijd doen-tot-falen

10 Beëindig MAB

20 Verifiëren met DOT1X-prioriteit 10

evenementenverificatie-succesvergelijking

10 Klasse Altijd doen-tot-falen

10 servicesjabloon DEFAULT_LINKSEC_POLICY_MUST_SECURE activeren

service-policy type control subscriber POLICY_Gi1/0/45

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

Configuratie van gebouw...

Huidige configuratie: 303 bytes

Ja!

interface Gigabit Ethernet1/0/45

SwitchPort Access VLAN 503

toegang in switchpoortmodus

Access-Session Host-Mode Single-Host

toegangsessie gesloten

toegangssessie-poortcontrole-auto

mab

Geen op rollen gebaseerde handhaving van CTS

dot1x pae-verificator

service-policy type control subscriber POLICY_Gi1/0/45

einde

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

Ja!

icts-autorisatielijst ISE2

CTS SXP inschakelen

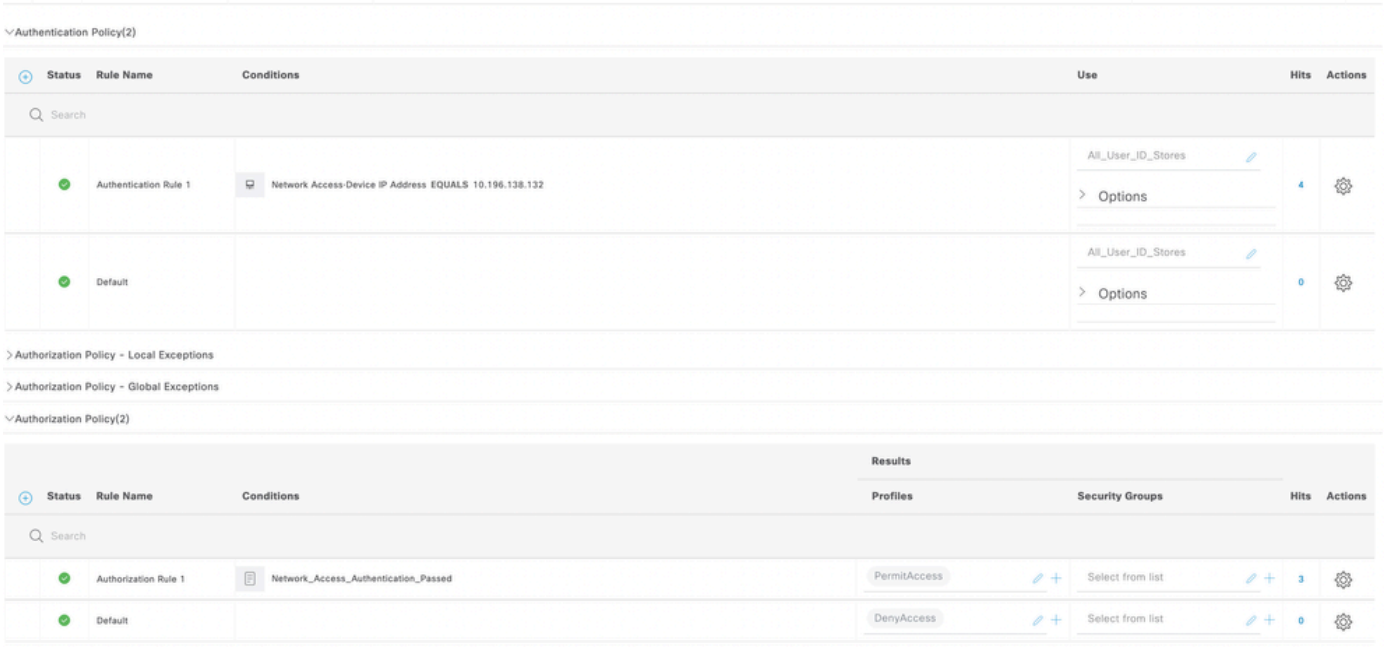
CTS SXP-verbinding 10.127.197.xxx Wachtwoord Geen modus Peer Speaker Hold-time 0 0

CTS SXP Standaardbron-IP 10.196.138.jjj

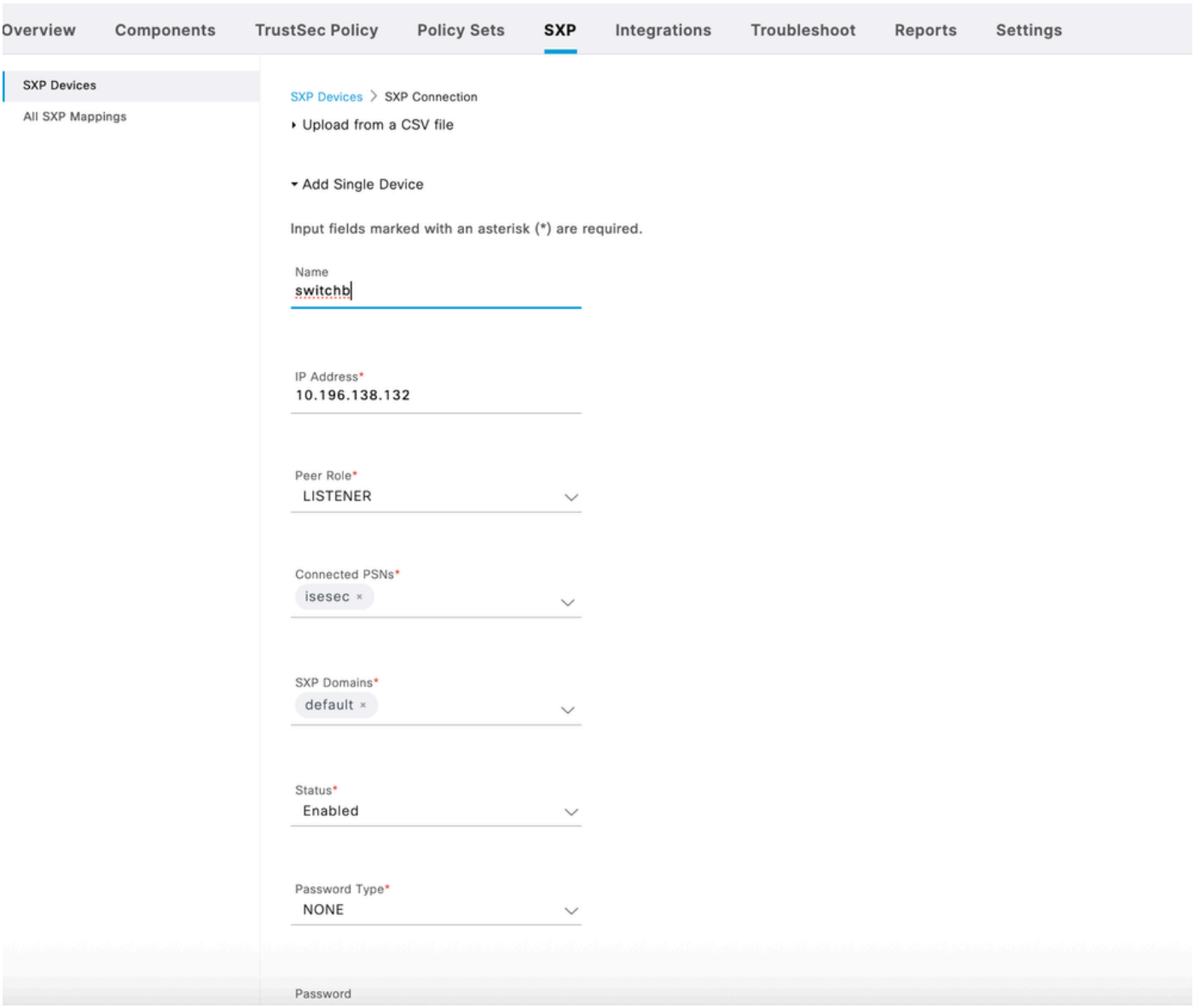
CTS SXP - Standaardwachtwoord xxxx@123

ISE-configuratie

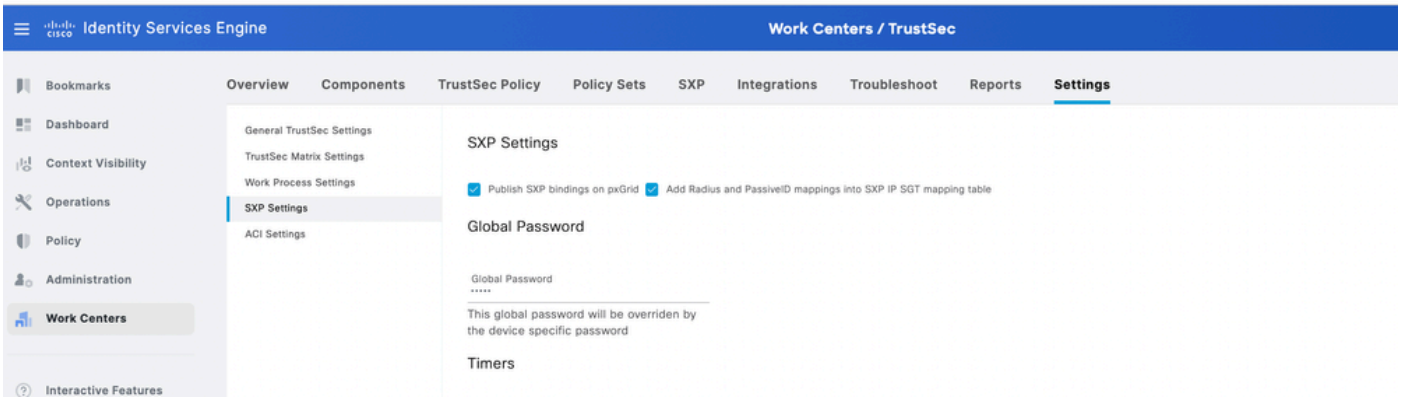
Stap 1: Authenticatie- en autorisatiebeleid maken op ISE



Stap 2: Een SXP-apparaat configureren op ISE



Stap 3: Algemeen wachtwoord configureren onder SXP-instellingen



Verifiëren

```
WS-C3850-48F-E#toon toegangssessie-interface gig1/0/45 details
            Interface: Gigabit Ethernet1/0/45
              IIF-ID: 0x1A146F96
           MAC-adres: b496.9126.decc
          IPv6-adres: onbekend
          IPv4-adres: onbekend
            Gebruikersnaam: divya123
              Status: geautoriseerd
              Domein: DATA
        Open hostmodus: enkele host
      Oper control dir: beide
       Time-out sessie: NVT
     Algemene sessie-ID: 000000000000000B95163D98
       ID ACT-sessie: onbekend
              Handvat: 0x6f000001
        Huidig beleid: POLICY_GI1/0/45
Lokaal beleid:
         Servicesjabloon: DEFAULT_LINKSEC_POLICY_MUST_SECURE (prioriteit 150)
       Veiligheidsbeleid: moet veilig zijn
       Beveiligingsstatus: koppeling onbeveiligd
Serverbeleid:
Methodestatuslijst:
        Methode-toestand
         dot1x Authc-succes
WS-C3850-48F-E#
WS-C3850-48F-E(config)#do show cts sxp conn
SXP: ingeschakeld
```

Hoogste ondersteunde versie: 4

Standaardwachtwoord: instellen

Standaardsleutelhanger: niet ingesteld

Standaardsleutelketennaam: niet van toepassing

Standaardbron IP: 10.196.138.jjj

Open periode voor opnieuw verbinden: 120 sec

Reconciliatieperiode: 120 sec

Open timer opnieuw proberen wordt uitgevoerd

Verplaatsingslimiet van peer-sequentie voor export: niet ingesteld

Verplaatsingslimiet van peer-sequentie voor importeren: niet ingesteld

---

IP-peer: 10.127.197.xxx

Bron IP : 10.196.138.jjj

Conn-status : op

Conversie : 4

Conn-mogelijkheid : IPv4-IPv6-subnet

Conn hold-tijd : 120 seconden

Lokale modus : SXP Listener

Verbinding inst#: 1

TCP conn fd : 1

TCP conn wachtwoord: geen

Hold-timer wordt uitgevoerd

Duur sinds laatste statuswijziging: 0:00:00:22 (dd:hr:mm:sec)

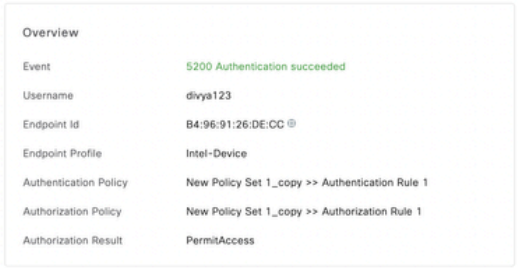
Totaal aantal SXP-verbindingen = 1

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

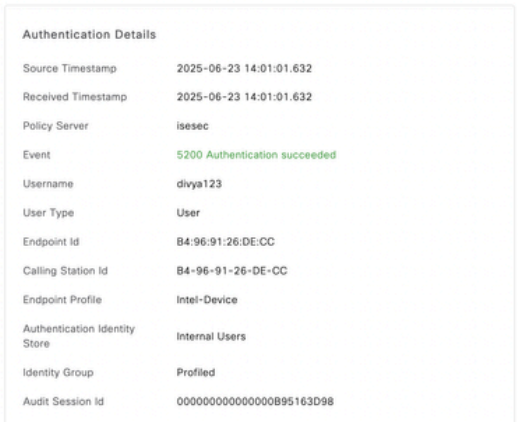
cdbp:0xFF8CBFC090 <10.127.197.145, 10.196.138.yyy> tableid:0x0

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

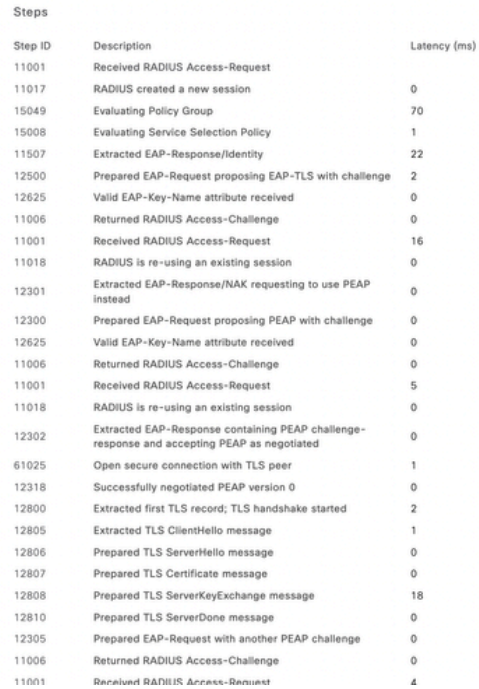
In het live logboekrapport wordt de SGT-tag Guest weergegeven die is toegepast:



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

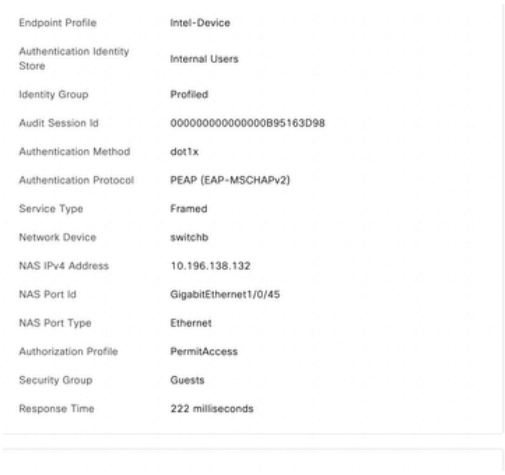


Authentication Details	
Source Timestamp	2025-06-23 14:01:01.632
Received Timestamp	2025-06-23 14:01:01.632
Policy Server	isesec
Event	5200 Authentication succeeded
Username	divya123
User Type	User
Endpoint Id	B4:96:91:26:DE:CC
Calling Station Id	B4-96-91-26-DE-CC
Endpoint Profile	Intel-Device
Authentication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

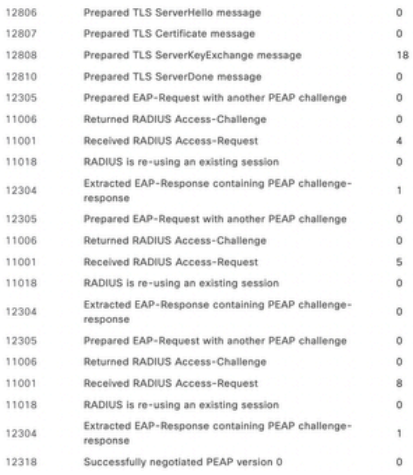


Steps

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



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



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

Problemen oplossen

Schakel deze foutopsporing op de switch in om dot1x-problemen op te lossen:

- Foutopsporingsstip1x Alle

logboekuitleg

dot1x-packet: EAPOL pak rx - Ver: 0x1 type: 0x1 **>>>>>** EAPoL pakket ontvangen door de switch dot1x-pakket: lengte: 0x0000

dot1x-ev: [b496.9126.decc, Gig1/0/45] client gedetecteerd, verzenden sessie start event voor b496.9126.decc **>>>>** dot1x client gedetecteerd

dot1x-ev: [b496.9126.decc, Gig1/0/45] Dot1x-verificatie gestart voor 0x26000007

(b496.9126.decc)>>>> dot1x gestart

%AUTHMGR-5-START: 'dot1x' starten voor client (b496.9126.decc) op interface Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-sm: [b496.9126.decc, Gig1/0/45] Posting: ˂EAP_RESTART op client 0x26000007 />>>> Client vragen om het EAP-proces opnieuw te starten

dot1x-sm: [b496.9126.decc, Gig1/0/45] RX_REQ wordt gepost op client 0x26000007 >>>> wachtend op het EAPoL-pakket van de client

dot1x-sm: [b496.9126.decc, Gig1/0/45] AUTH_START plaatsen voor 0x26000007 >>>>> Verificatieproces starten

dot1x-ev: [b496.9126.decc, Gig1/0/45] EAPOL-pakket verzenden >>>> Identiteitsverzoek
dot1x-packet: EAPOL pak Tx - Ver: 0x3 type: 0x0
dot1x-pakket: lengte: 0x0005
dot1x-pakket: EAP-code: 0x1 id: 0x1 lengte: 0x0005
dot1x-pakket: type: 0x1
dot1x-packet: [b496.9126.decc, Gig1/0/45] EAPOL-pakket verzonden naar client 0x26000007

dot1x-ev: [Gig1/0/45] Ontvangen pkt saddr =b496.9126.decc, daddr = 0180.c200.0003, pae-ether-type = 888e.0100.000a
dot1x-packet: EAPOL pak rx - Ver: 0x1 type: 0x0 // Identity Response
punt1x-pakket: lengte: 0x000A

dot1x-sm: [b496.9126.decc, Gig1/0/45] EAPOL_EAP plaatsen voor 0x26000007 >>>> EAPoL-pakket (EAP-respons) ontvangen, aanvraag voorbereiden voor server

dot1x-sm: [b496.9126.decc, Gig1/0/45] EAP_REQ plaatsen voor 0x26000007 >>>> Serverrespons ontvangen, EAP-aanvraag wordt voorbereid

dot1x-ev: [b496.9126.decc, Gig1/0/45] EAPOL-pakket verzenden
dot1x-packet: EAPOL pak Tx - Ver: 0x3 type: 0x0
dot1x-pakket: lengte: 0x0006
dot1x-pakket: EAP-code: 0x1 id: 0xE5 lengte: 0x0006
punt1x-pakket: type: 0xD
dot1x-packet: [b496.9126.decc, Gig1/0/45] EAPOL-pakket verzonden naar client 0x26000007 >>>>> EAP-verzoek verzonden

dot1x-ev: [Gig1/0/45] Ontvangen pkt saddr =b496.9126.decc, daddr = 0180.c200.0003, pae-ether-type = 888e.0100.0006 //EAP-reactie ontvangen
dot1x-packet: EAPOL pak rx - Ver: 0x1 type: 0x0
dot1x-pakket: lengte: 0x0006
| |
| |
| |
|| Hier vinden veel EAPOL-EAP- en EAP_REQ-gebeurtenissen plaats omdat er veel informatie

wordt uitgewisseld tussen de switch en de client
Indien de gebeurtenissen hierna niet volgen, moeten de timers en de tot nu toe verzonden informatie worden gecontroleerd
| |
| |
| |
dot1x-packet: [b496.9126.decc, Gig1/0/45] Ontvangen EAP-succes **>>>>>** EAP-succes ontvangen van server

dot1x-sm: [b496.9126.decc, Gig1/0/45] EAP_SUCCESS plaatsen voor 0x26000007 **>>>>** EAP-gebeurtenis met succes plaatsen

dot1x-sm: [b496.9126.decc, Gig1/0/45] AUTH_SUCCESS plaatsen op client 0x26000007 **>>>>** Authenticatiesucces plaatsen

%DOT1X-5-SUCCES: verificatie succesvol voor client (b496.9126.decc) op interface Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-packet:[b496.9126.decc, Gig1/0/45] EAP-sleutelgegevens gedetecteerd bij toevoegen aan attribuutlijst **>>>>>** Extra sleutelgegevens gedetecteerd verzonden door server

%AUTHMGR-5-SUCCES: autorisatie geslaagd voor client (b496.9126.decc) op interface Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-ev: [b496.9126.decc, Gig1/0/45] Ontvangen Authz Succes voor de client 0x26000007 (b496.9126.decc) **>>>>>** Autorisatie Succes

dot1x-ev: [b496.9126.decc, Gig1/0/45] EAPOL-pakket verzenden **>>>>** EAP-succes naar de client verzenden
dot1x-packet: EAPOL pak Tx - Ver: 0x3 type: 0x0
dot1x-pakket: lengte: 0x0004
dot1x-pakket: EAP-code: 0x3 id: 0xED lengte: 0x0004
dot1x-packet: [b496.9126.decc, Gig1/0/45] EAPOL-pakket verzonden naar client 0x26000007

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.