Configuración del switch con SXP e IBNS 2.0 para redes basadas en identidad

Contenido

Introducción

Este documento describe los procedimientos para configurar los switches Cisco con SXP e IBNS 2.0 para las redes basadas en identidad.

Prerequisites

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- parche 4 de Identity Services Engine (ISE) versión 3.3
- Switch Cisco Catalyst 3850

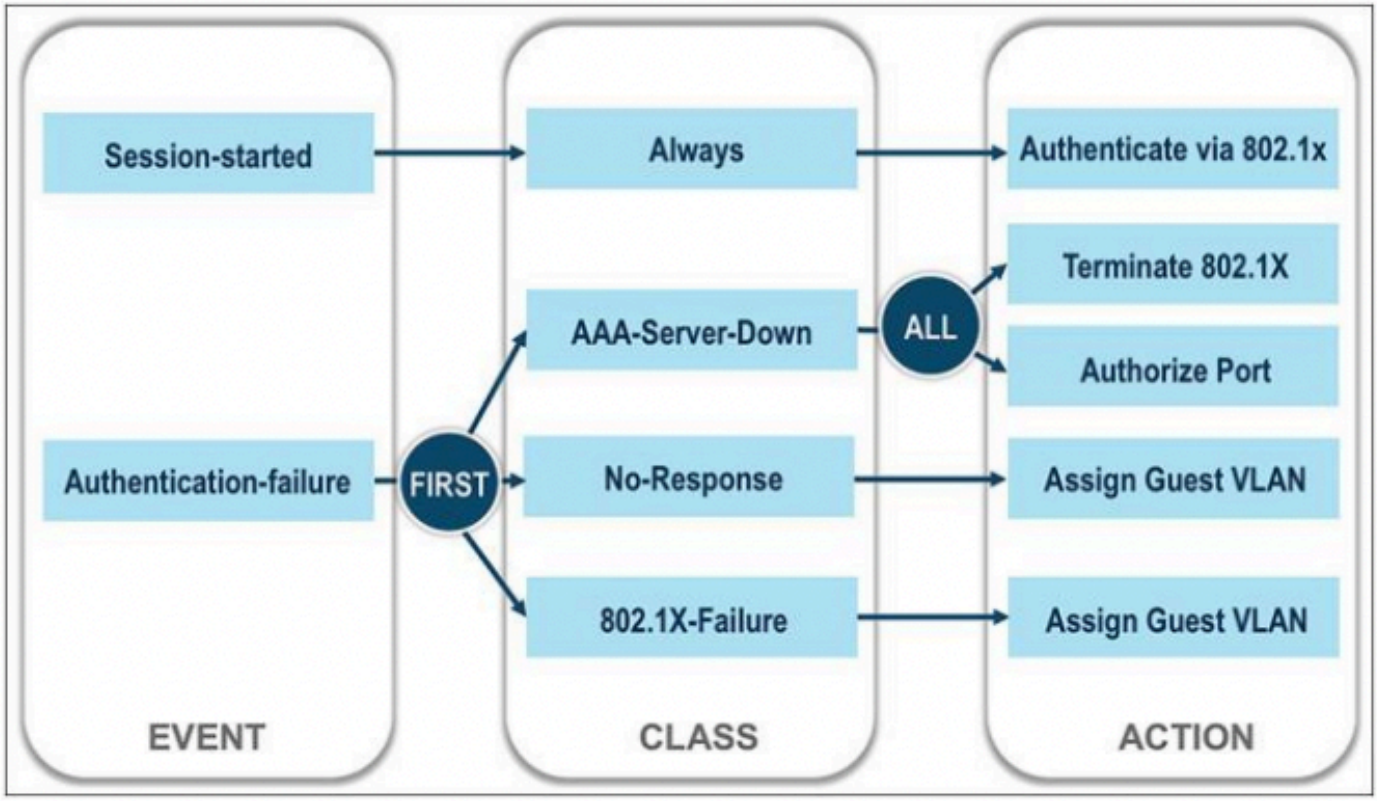
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Las directivas de control de identidad definen las acciones que el Administrador de sesiones de Access realiza en respuesta a condiciones específicas y eventos de extremos. Mediante un lenguaje de políticas coherente, se pueden combinar varias acciones, condiciones y eventos del sistema para formar estas políticas.

Las políticas de control se aplican en las interfaces y son principalmente responsables de administrar la autenticación de terminales y activar los servicios en las sesiones. Cada directiva de control se compone de una o varias reglas y una estrategia de decisión que determina cómo se evalúan dichas reglas.

Una regla de directiva de control incluye una clase de control (una instrucción de condición flexible), un evento que desencadena la evaluación de la condición y una o más acciones. Mientras los administradores definen qué acciones desencadenan eventos específicos, algunos eventos incluyen acciones predeterminadas predefinidas.



Política de control de identidad

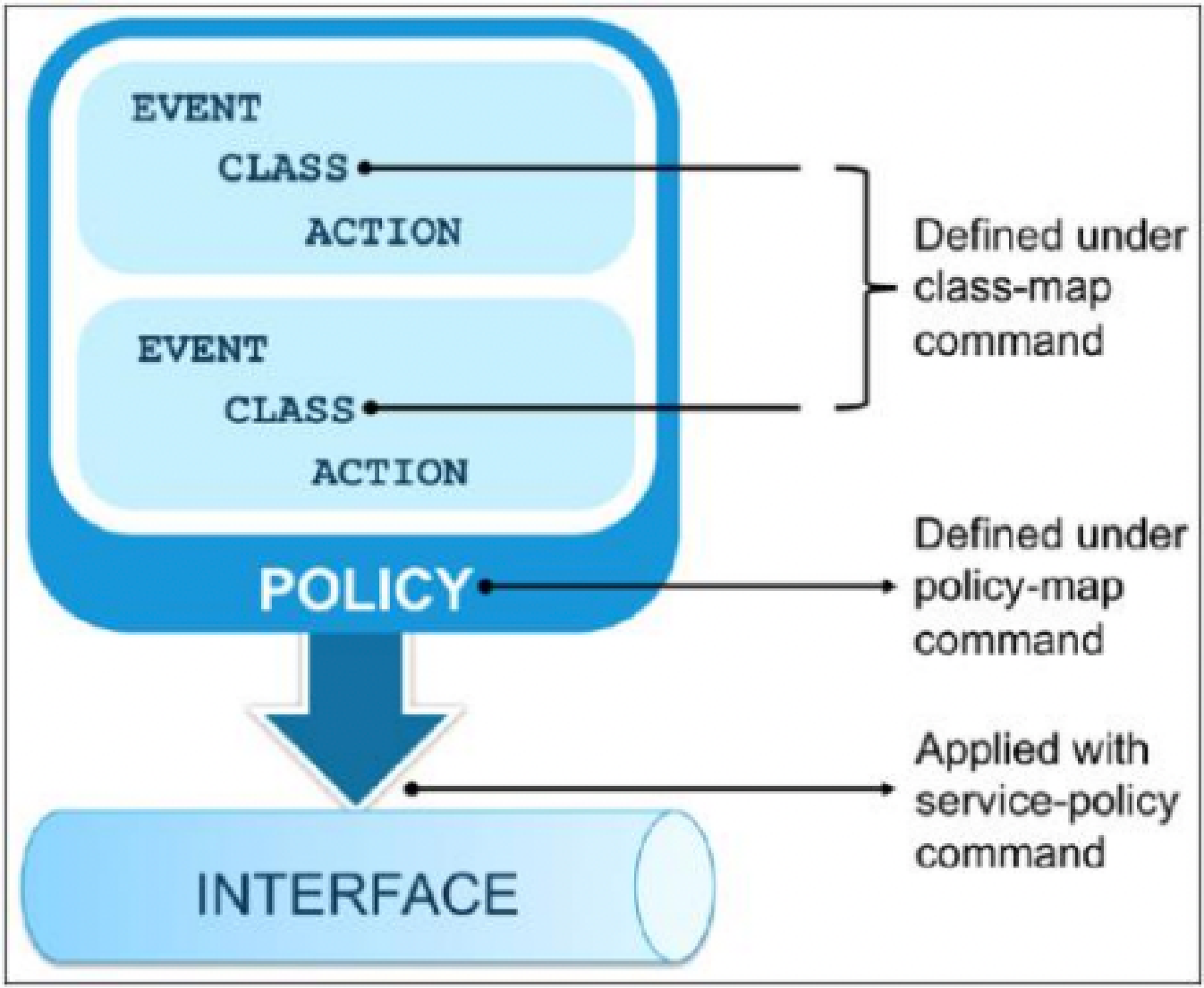
Información general sobre configuración de políticas de control de identidad

Las directivas de control definen el comportamiento del sistema mediante un evento, una condición y una acción. La configuración de una política de control implica tres pasos principales:

1. Crear clases de control:
   Una clase de control define las condiciones necesarias para activar una directiva de control. Cada clase puede tener varias condiciones que se evalúan como true o false. Puede establecer si todas, cualquiera o ninguna de las condiciones deben ser verdaderas para que la clase se considere verdadera. Como alternativa, los administradores pueden utilizar una

clase predeterminada que no tenga condiciones y que siempre se evalúe como true.

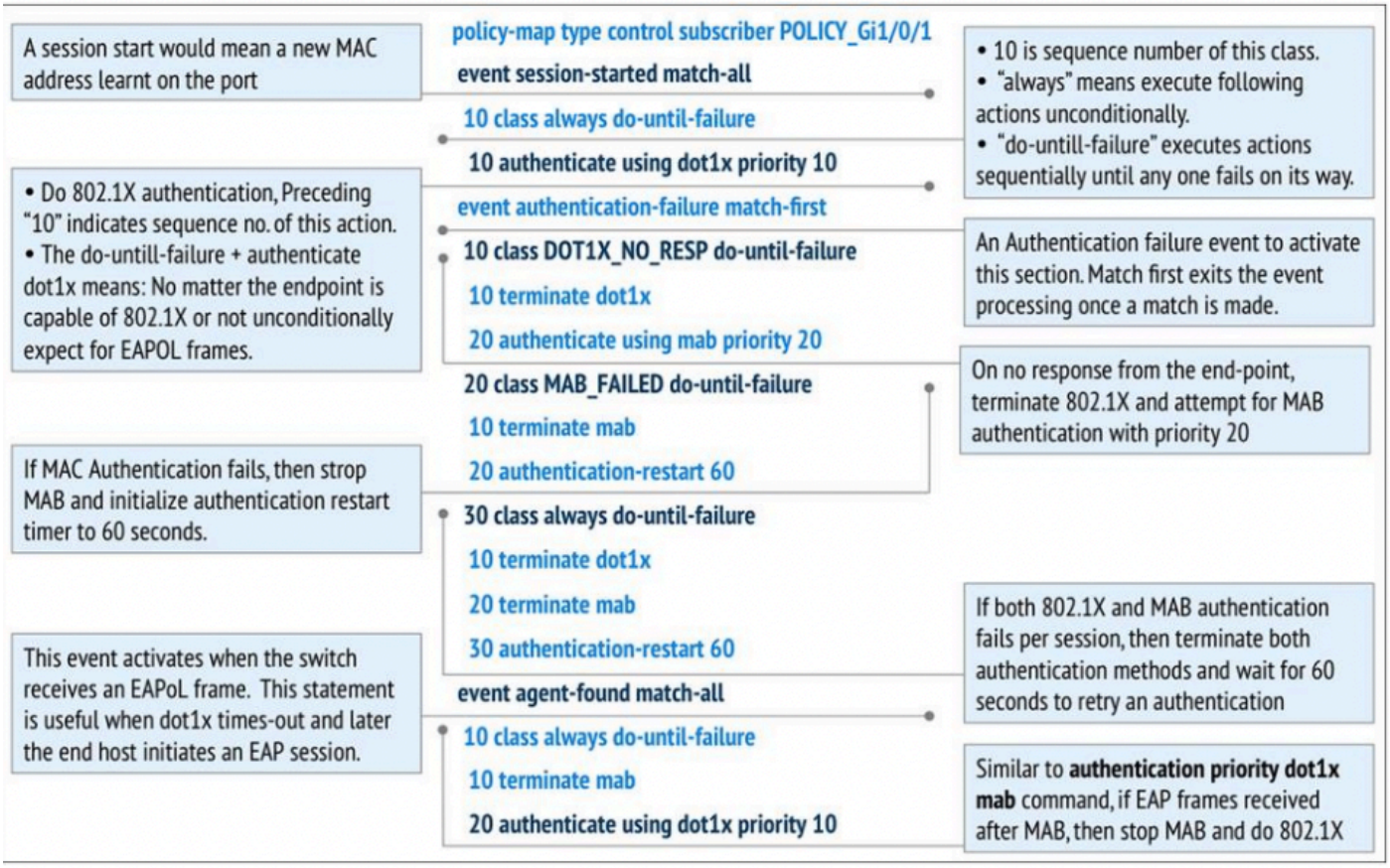
2. Cree la política de control:
   Una directiva de control contiene una o varias reglas. Cada regla incluye una clase de control, un evento que activa la comprobación de condición y una o más acciones. Las acciones se numeran y ejecutan en orden.
3. Aplicar la política de control:
   Finalmente, aplique la política de control a una interfaz para activarla.



Configuración de políticas de control de identidad

El comando authentication display new-style convierte las configuraciones heredadas en un nuevo estilo.

switch#authentication display new-style



Interpretación de la política de control de identidad

Configurar

Configuración del switch

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

!

aaa authentication dot1x default group radius local

aaa authorization network default group radius local

username admin password 0 xxxxxx

!

!

!

!

ISE1 del servidor RADIUS

address ipv4 10.127.197.xxx auth-port 1812 acct-port 1813

```
pac key xxxx@123
!
!
aaa group server radius ISE2
nombre del servidor ISE1
!
!
!
!
aaa new-model
aaa session-id common
!
aaa server radius dynamic-author
client 10.127.197.xxx server-key xxxx@123
dot1x system-auth-control
!
WS-C3850-48F-E#show run | en POLICY_Gi1/0/45
policy-map type control subscriber POLICY_Gi1/0/45
service-policy type control subscriber POLICY_Gi1/0/45
WS-C3850-48F-E#show run | seg. POLICY_Gi1/0/45
policy-map type control subscriber POLICY_Gi1/0/45
event session-started match-all
  10 class always do-until-failure
   10 autenticar usando la prioridad dot1x 10
event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminales dot1x
```

```
    20 authentication-restart 60
   10 class DOT1X_NO_RESP do-until-failure
    10 terminales dot1x
    20 autenticación mediante prioridad mab 20
   20 class MAB_FAILED do-until-failure
    10 mab de finalización
    20 authentication-restart 60
   40 class always do-until-failure
    10 terminales dot1x
    20 mab de finalización
    30 authentication-restart 60
event agent-found match-all
   10 class always do-until-failure
    10 mab de finalización
    20 autenticar con prioridad dot1x 10
event authentication-success match-all
   10 class always do-until-failure
    10 activate service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
service-policy type control subscriber POLICY_Gi1/0/45
WS-C3850-48F-E#show run interface gig1/0/45
Creando configuración...
Configuración actual 303 bytes
!
interface GigabitEthernet1/0/45
switchport access vlan 503
switchport mode access
access-session host-mode single-host
```

access-session closed

access-session port-control auto

mab

no cts role-based forcement

dot1x page authenticator

service-policy type control subscriber POLICY_Gi1/0/45

Finalizar

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

!

cts authorization list ISE2

cts sxp enable

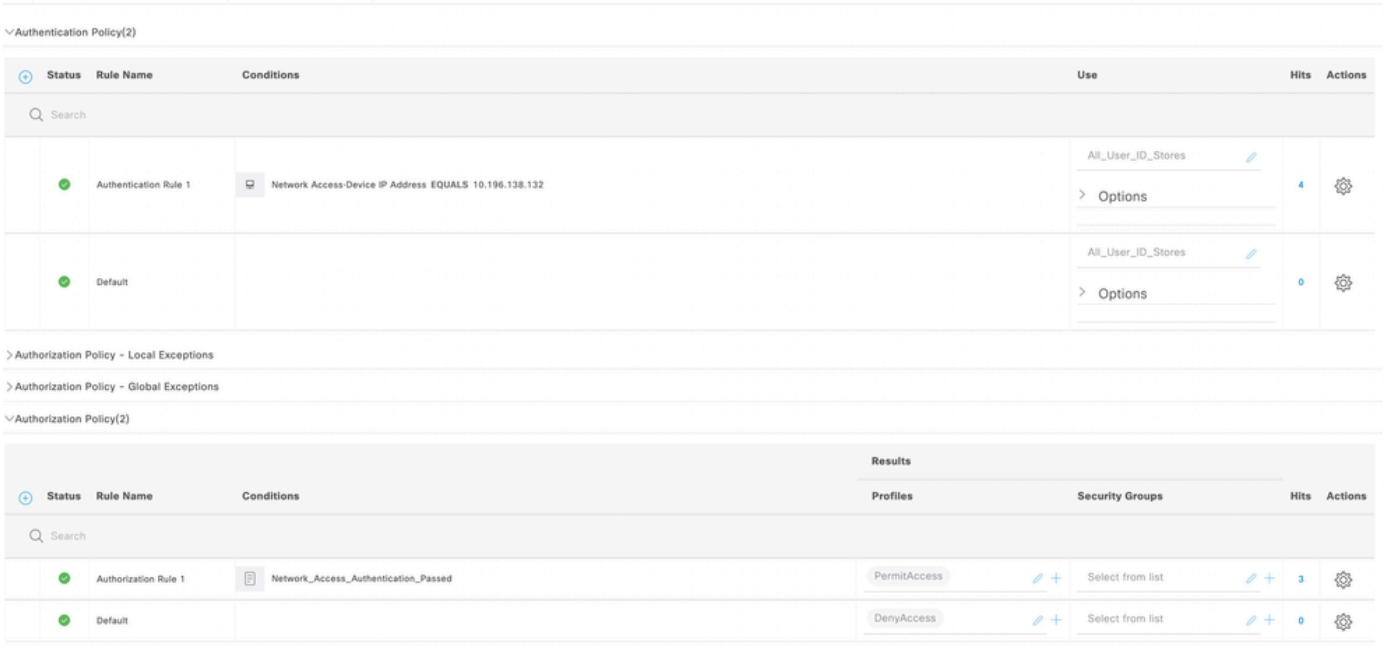
cts sxp connection 10.127.197.xxx password none mode peer spoke hold-time 0

cts sxp default source-ip 10.196.138.yyy

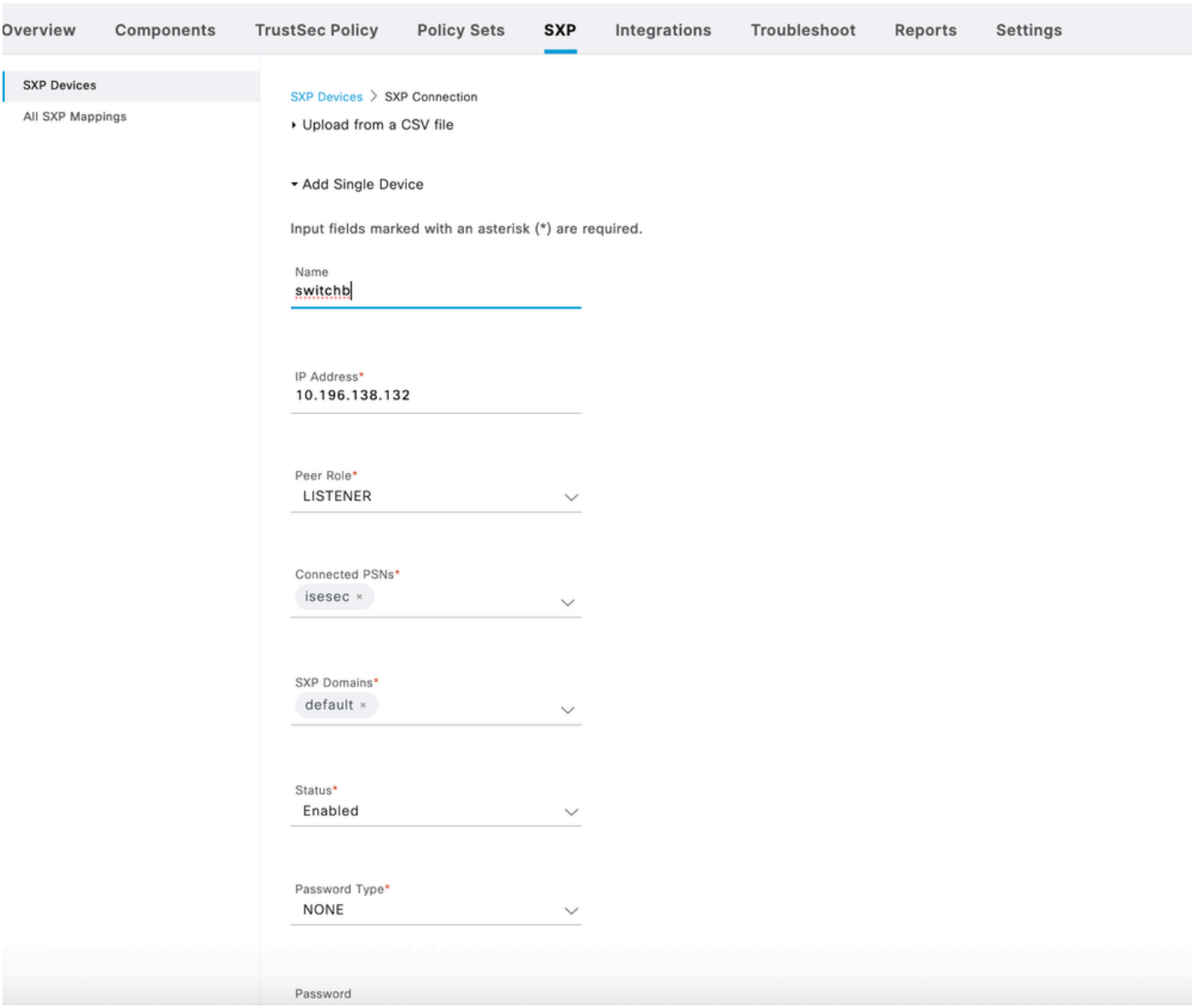
cts sxp default password xxxx@123

Configuración de ISE

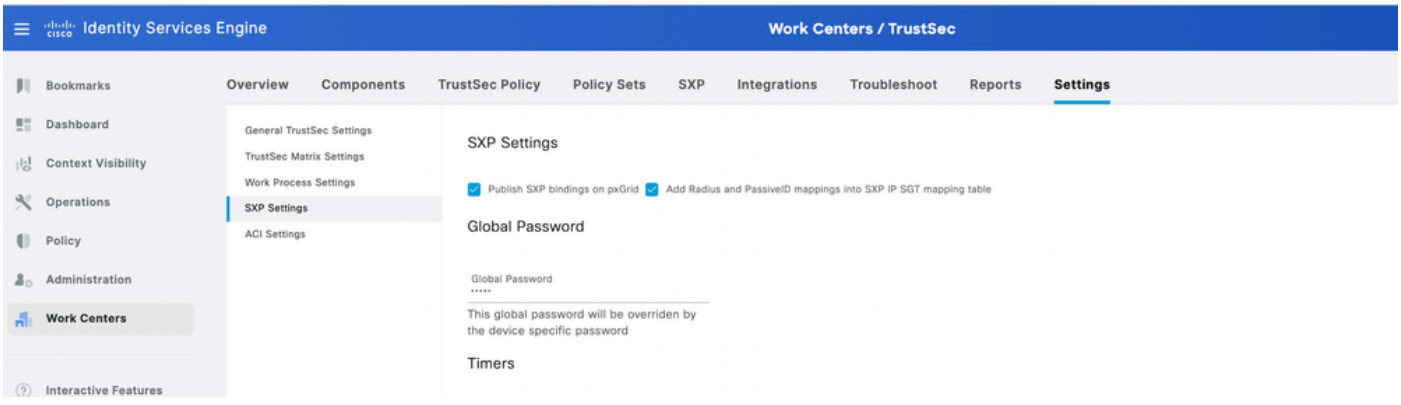
Paso 1: Crear políticas de autenticación y autorización en ISE



Paso 2: Configuración de un dispositivo SXP en ISE



Paso 3: Configurar contraseña global en Configuración de SXP



Verificación

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

Interfaz: GigabitEthernet1/0/45

IIF-ID: 0x1A146F96

Dirección MAC: b496.9126.decc

Dirección IPv6: Desconocido

Dirección IPv4: Desconocido

Nombre de usuario: divya123

Estado: Autorizado

Dominio: DATOS

Modo de host Oper: de host único

Oper control dir: ambas

Tiempo de espera de sesión: N/A

ID de sesión común: 000000000000000B95163D98

ID de sesión de cuenta: Desconocido

Manejar: 0x6f000001

Política actual: POLICY_Gi1/0/45

Políticas locales:

Plantilla de servicio: DEFAULT_LINKSEC_POLICY_MUST_SECURE (prioridad 150)

Política de seguridad: Debe asegurar

Estado de seguridad: Enlace no seguro

Políticas de servidor:

Lista de estados de método:

Estado del método

dot1x Auténtico correcto

WS-C3850-48F-E#

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

SXP: Habilitado

Versión más alta admitida: 4

Contraseña predeterminada: Set

Cadena de teclas predeterminada: no establecido

Nombre predeterminado de la cadena de claves: No aplicable

IP de origen predeterminada: 10.196.138.aaaa

Período de reintento de conexión abierto: 120 segundos

Período de conciliación: 120 segundos

Se está ejecutando el temporizador de reintento abierto

Límite de recorrido de la secuencia de pares para la exportación: no establecido

Límite de recorrido de secuencia de pares para la importación: no establecido

---

IP de peer: 10 127 197 xxx

IP de origen: 10.196.138.aaaa

Estado de conexión: Encendido

Conn version : 4

Capacidad de conexión: Subred IPv4-IPv6

Tiempo de espera de conexión: 120 segundos

Modo local : Receptor SXP

Número de instante de conexión: 1

TCP conn fd : 1

Contraseña de conexión TCP: ninguno

Se está ejecutando el temporizador de espera

Duración desde el último cambio de estado: 0:00:00:22 (dd:hr:mm:sec)

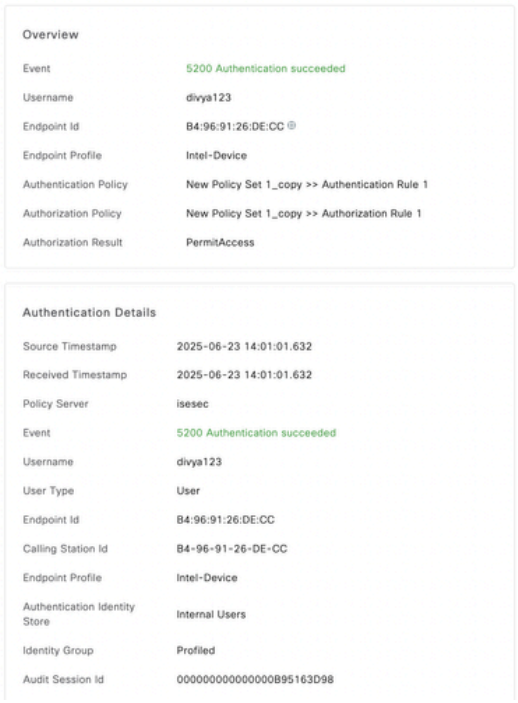
Número total de conexiones SXP = 1

0xFF8CBFC090 VRF:, fd: 1, ip de peer: 10 127 197 xxx

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

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

El informe de registro en directo muestra la etiqueta SGT Invitado aplicada:

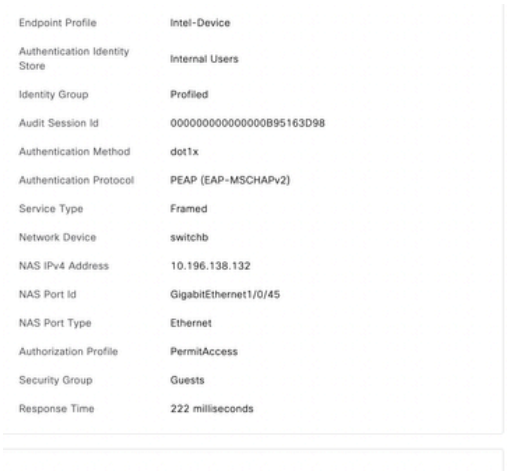


Overview

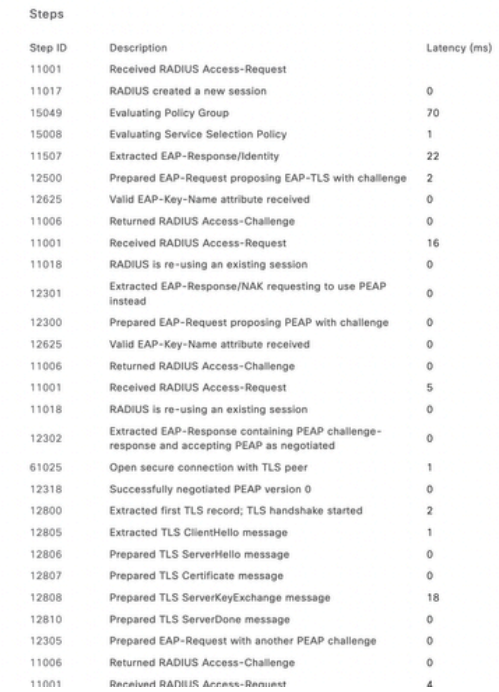
Event	5200 Authentication succeeded
Username	divya123
Endpoint Id	B4:96:91:26:DE:CC
Endpoint Profile	Intel-Device
Authentication Policy	New Policy Set 1_copy >> Authentication Rule 1
Authorization Policy	New Policy Set 1_copy >> Authorization Rule 1
Authorization Result	PermitAccess

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

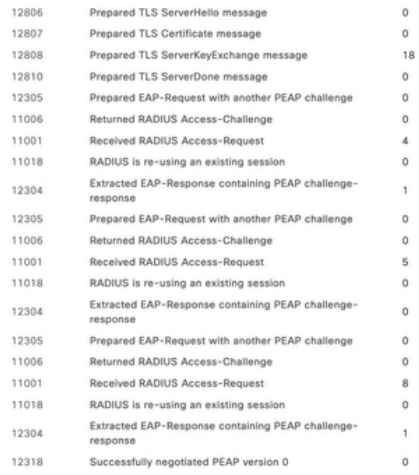


Endpoint Profile	Intel-Device
Authentication Identity Store	Internal Users
Identity Group	Profiled
Audit Session Id	000000000000000B95163D98
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	switchb
NAS IPv4 Address	10.196.138.132
NAS Port Id	GigabitEthernet1/0/45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

Troubleshoot

Habilite esta depuración en el switch para resolver problemas de dot1x:

- debug dot1x all

Explicación del registro

dot1x-packet:EAPOL pak rx - Ver: Tipo 0x1: 0x1 **>>>>** paquetes EAPoL recibidos por el switch dot1x-packet: longitud: 0x0000

dot1x-ev:[b496.9126.decc, Gig1/0/45] cliente detectado, enviando evento de inicio de sesión para b496.9126.decc **>>>>** cliente dot1x detectado

dot1x-ev:[b496.9126.decc, Gig1/0/45] Autenticación dot1x iniciada para 0x26000007

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

%AUTHMGR-5-START: Iniciando 'dot1x' para el cliente (b496.9126.decc) en la interfaz Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-sm:[b496.9126.decc, Gig1/0/45] Publicando !EAP_RESTART en el cliente 0x26000007 />>>> Solicitando al cliente que reinicie el proceso EAP

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting RX_REQ on Client 0x26000007 >>>>> waiting for the EAPoL packet from the client

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting AUTH_START for 0x26000007 >>>> Iniciando proceso de autenticación

dot1x-ev:[b496.9126.decc, Gig1/0/45] Enviando paquete EAPOL >>>> Solicitud de identidad
dot1x-packet:EAPOL pak Tx - Ver: Tipo 0x3: 0x0
dot1x-packet: longitud: 0x0005
dot1x-packet:código EAP: ID 0x1: Longitud 0x1: 0x0005
dot1x-packet: type: 0x1
dot1x-packet:[b496.9126.decc, Gig1/0/45] paquete EAPOL enviado al cliente 0x26000007

dot1x-ev:[Gig1/0/45] Pkt saddr recibido =b496.9126.decc , daddr = 0180.c200.0003, page-ether-type = 888e.0100.000a
dot1x-packet:EAPOL pak rx - Ver: Tipo 0x1: 0x0 // Respuesta de identidad
dot1x-packet: longitud: 0x000 A

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting EAPOL_EAP for 0x26000007 >>>> EAPoL packet(EAP Response) received, prepare request to server

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting EAP_REQ for 0x26000007 >>>>> Respuesta del servidor recibida, EAP Request is being prepare

dot1x-ev:[b496.9126.decc, Gig1/0/45] Enviando paquetes EAPOL
dot1x-packet:EAPOL pak Tx - Ver: Tipo 0x3: 0x0
dot1x-packet: longitud: 0x0006
dot1x-packet:código EAP: ID 0x1: Longitud 0xE5: 0x0006
dot1x-packet: type: 0xD
dot1x-packet:[b496.9126.decc, Gig1/0/45] Paquete EAPOL enviado al cliente 0x26000007 >>>> Solicitud EAP enviada

dot1x-ev:[Gig1/0/45] Pkt saddr recibido =b496.9126.decc , daddr = 0180.c200.0003, pae-ether-type = 888e.0100.0006 //EAP response received
dot1x-packet:EAPOL pak rx - Ver: Tipo 0x1: 0x0
dot1x-packet: longitud: 0x0006
||
||
||
|| Aquí se producen muchos eventos EAPOL-EAP y EAP_REQ porque se intercambia mucha

información entre el switch y el cliente
|| Si los eventos posteriores a esta fecha no se producen a continuación, es necesario comprobar los temporizadores y la información enviada hasta ahora
||
||
||
dot1x-packet:[b496.9126.decc, Gig1/0/45] Recibió un Éxito EAP **>>>>** Éxito EAP recibido del Servidor

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting EAP_SUCCESS for 0x26000007 **>>>>** Posting EAP Success event

dot1x-sm:[b496.9126.decc,Gig1/0/45] Posting AUTH_SUCCESS on Client 0x26000007 **>>>>** Posting Authentication success

%DOT1X-5-SUCCESS: Autenticación satisfactoria para el cliente (b496.9126.decc) en la interfaz Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-packet:[b496.9126.decc, Gig1/0/45] Se detectaron datos de clave EAP que se agregaron a la lista de atributos **>>>>>** Se detectaron datos de clave adicionales enviados por el servidor

%AUTHMGR-5-SUCCESS: Autorización correcta para el cliente (b496.9126.decc) en la interfaz Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-ev:[b496.9126.decc, Gig1/0/45] Éxito de autenticación recibido para el cliente 0x26000007 (b496.9126.decc) **>>>>** Éxito de autorización

dot1x-ev:[b496.9126.decc, Gig1/0/45] Enviando paquete EAPOL **>>>>** Enviando Éxito EAP al cliente
dot1x-packet:EAPOL pak Tx - Ver: Tipo 0x3: 0x0
dot1x-packet: longitud: 0x0004
dot1x-packet:código EAP: ID 0x3: 0xED longitud: 0x0004
dot1x-packet:[b496.9126.decc, Gig1/0/45] paquete EAPOL enviado al cliente 0x26000007

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).