Configuration du commutateur avec SXP et IBNS 2.0 pour les réseaux basés sur l'identité

Table des matières

Introduction

Ce document décrit les procédures de configuration des commutateurs Cisco avec SXP et IBNS 2.0 pour la mise en réseau basée sur l'identité.

Conditions préalables

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Identity Services Engine (ISE) version 3.3 correctif 4
- commutateur Cisco Catalyst 3850

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

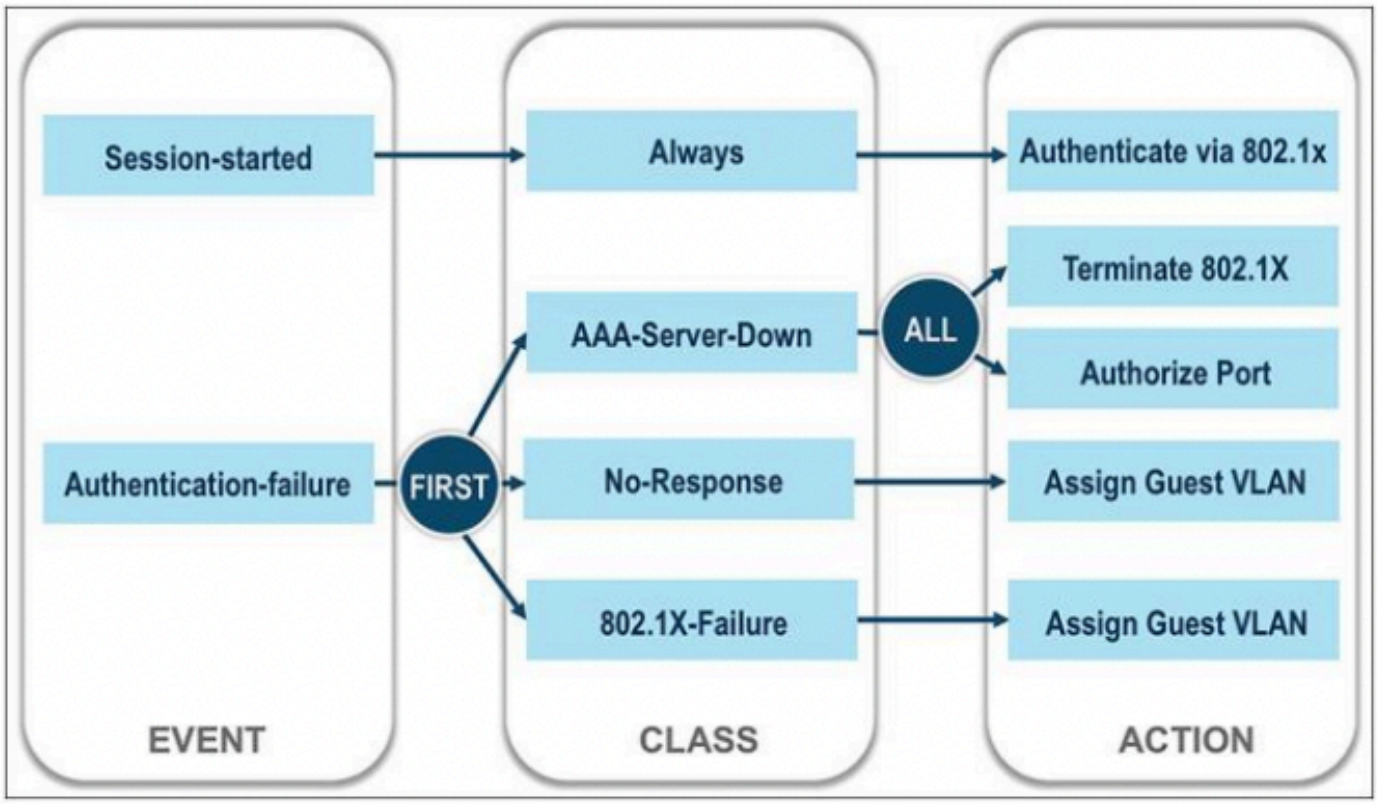
Informations générales

Les stratégies de contrôle d'identité définissent les actions que le gestionnaire de session d'accès

effectue en réponse à des conditions et des événements de point de terminaison spécifiques. Grâce à un langage de stratégie cohérent, il est possible de combiner diverses actions, conditions et événements du système pour former ces stratégies.

Les stratégies de contrôle sont appliquées sur les interfaces et sont principalement responsables de la gestion de l'authentification des terminaux et de l'activation des services sur les sessions. Chaque stratégie de contrôle est composée d'une ou de plusieurs règles et d'une stratégie de décision qui détermine la manière dont ces règles sont évaluées.

Une règle de politique de contrôle comprend une classe de contrôle (une instruction de condition flexible), un événement qui déclenche l'évaluation de la condition et une ou plusieurs actions. Tandis que les administrateurs définissent les actions déclenchées par des événements spécifiques, certains événements sont associés à des actions par défaut prédéfinies.



Politique de contrôle des identités

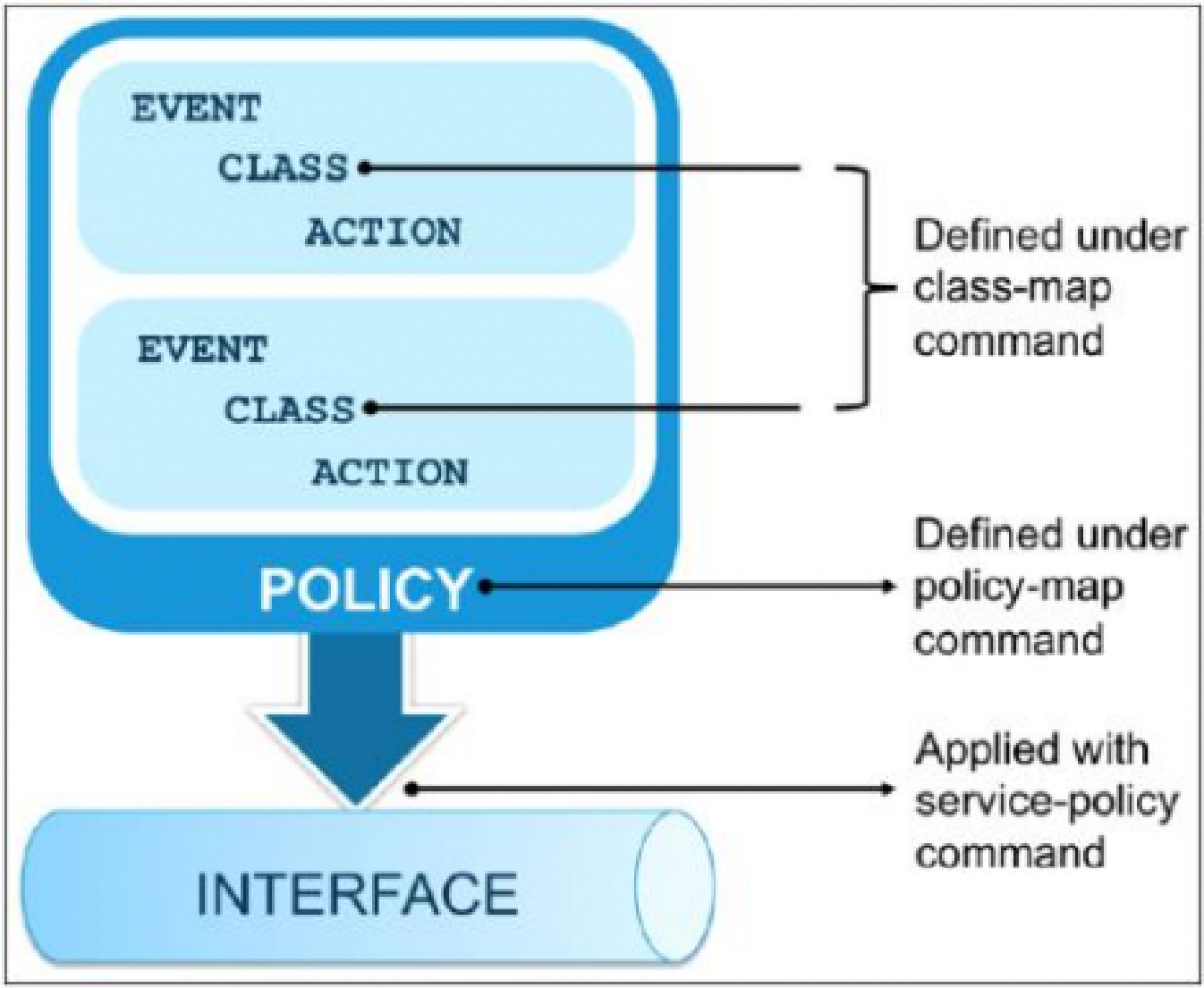
Présentation de la configuration de la stratégie de contrôle des identités

Les stratégies de contrôle définissent le comportement du système à l'aide d'un événement, d'une condition et d'une action. La configuration d'une stratégie de contrôle comprend trois étapes principales :

1. Créer des classes de contrôle :
   Une classe de contrôle définit les conditions requises pour activer une stratégie de contrôle. Chaque classe peut avoir plusieurs conditions qui s'évaluent comme true ou false. Vous pouvez définir si toutes, toutes ou aucune des conditions doivent être vraies pour que la classe soit considérée comme vraie. Les administrateurs peuvent également utiliser une

classe par défaut qui n'a aucune condition et qui est toujours évaluée comme vraie.

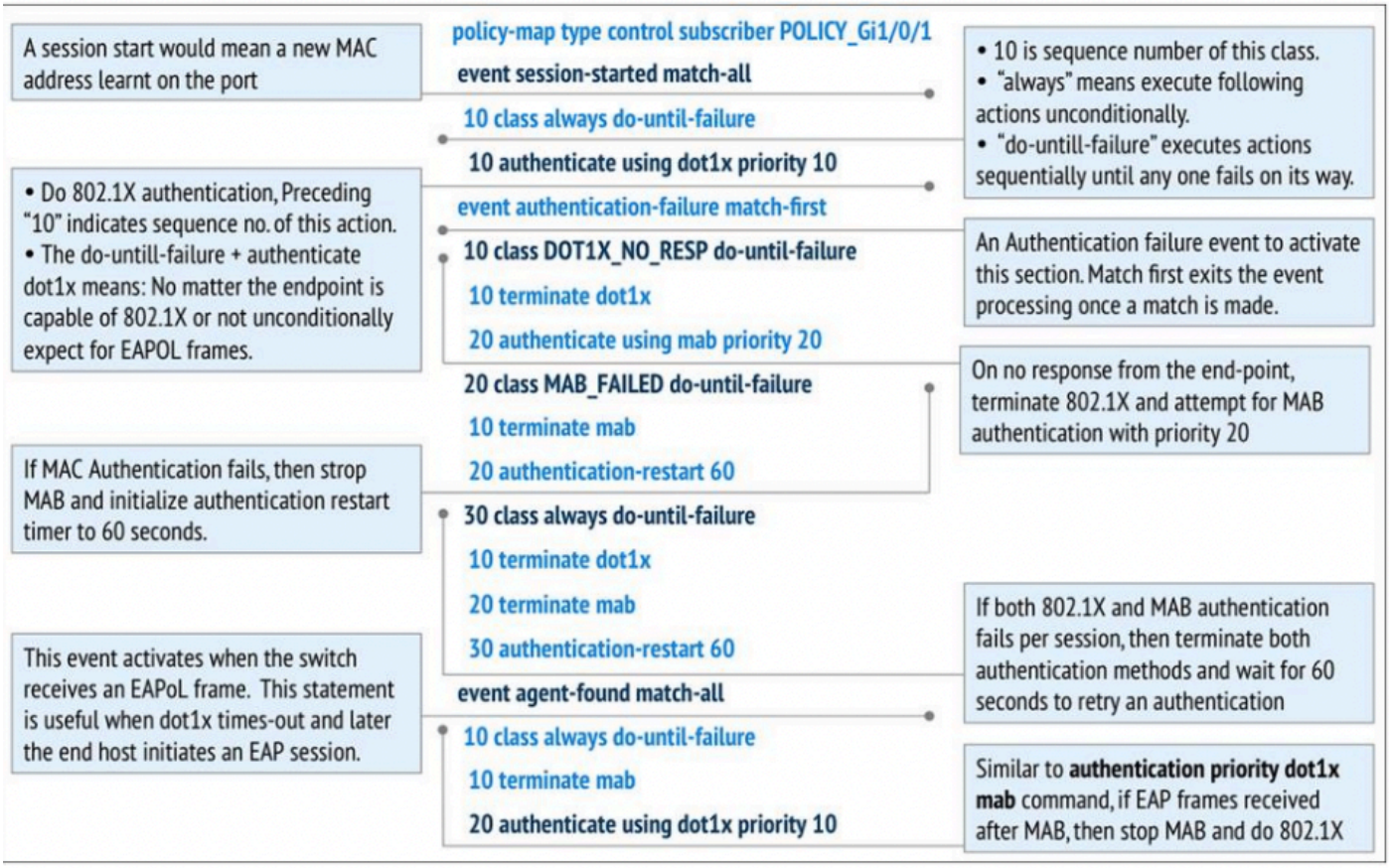
2. Créez la stratégie de contrôle :
   Une stratégie de contrôle contient une ou plusieurs règles. Chaque règle comprend une classe de contrôle, un événement qui déclenche la vérification de condition et une ou plusieurs actions. Les actions sont numérotées et exécutées dans l'ordre.
3. Appliquez la stratégie de contrôle :
   Enfin, appliquez la stratégie de contrôle à une interface pour l'activer.



Configuration de la stratégie de contrôle d'identité

La commande authentication display new-style convertit les configurations héritées en nouveau style.

switch#authentication afficher new-style



Interprétation de la politique de contrôle des identités

Configurer

Configuration du commutateur

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

!

!

!

!

Serveur RADIUS ISE1

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

pac key xxxx@123

!

!

serveur de groupe aaa radius ISE2

nom du serveur ISE1

!

!

!

!

aaa new-model

aaa session-id common

!

serveur aaa radius dynamic-author

client 10.127.197.xxx clé-serveur xxxx@123

dot1x system-auth-control

!

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

policy-map type control subscriber POLICY_Gi1/0/45

event session-started match-all

  10 classes toujours do-until-failure

   10 authentification à l'aide de la priorité dot1x 10

event authentication-failure match-first

  5 class DOT1X_FAILED do-until-failure

   10 terminaison dot1x

```
   20 authentication-restart 60
  10 class DOT1X_NO_RESP do-until-failure
   10 terminaison dot1x
   20 authentification à l'aide de mab priority 20
  20 class MAB_FAILED do-until-failure
   10 terminer mab
   20 authentication-restart 60
  40 classes toujours do-until-failure
   10 terminaison dot1x
   20 terminer mab
   30 authentication-restart 60
event agent-found match-all
  10 classes toujours do-until-failure
   10 terminer mab
   20 authentification à l'aide de dot1x priority 10
event authentication-success match-all
  10 classes toujours do-until-failure
   10 activer le modèle de service DEFAULT_LINKSEC_POLICY_MUST_SECURE
service-policy type control subscriber POLICY_Gi1/0/45
WS-C3850-48F-E#show run interface gig1/0/45
Construction de la configuration...
Configuration actuelle : 303 octets
!
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

aucune application basée sur les rôles cts

authentificateur de page dot1x

service-policy type control subscriber POLICY_Gi1/0/45

tranche

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

!

cts authorization list ISE2

cts sxp enable

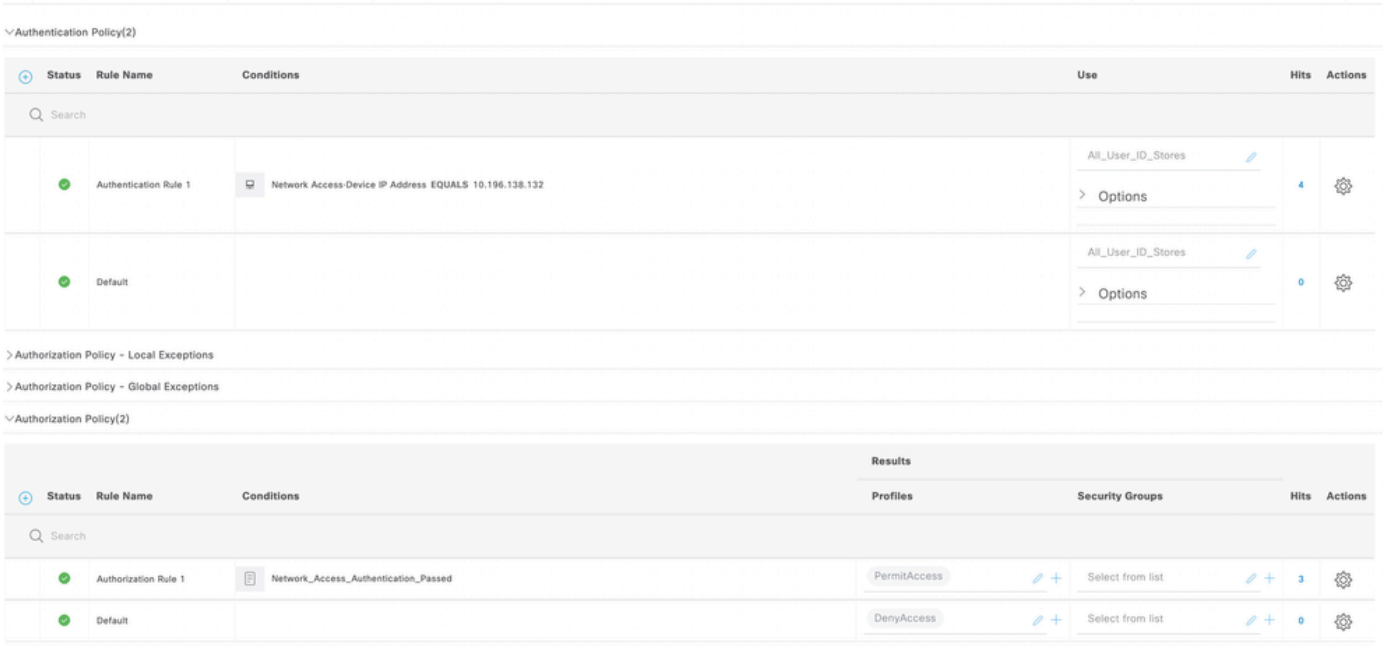
cts sxp connection 10.127.197.xxx password aucun mode peer speaker hold-time 0 0

cts sxp default source-ip 10.196.138.yyy

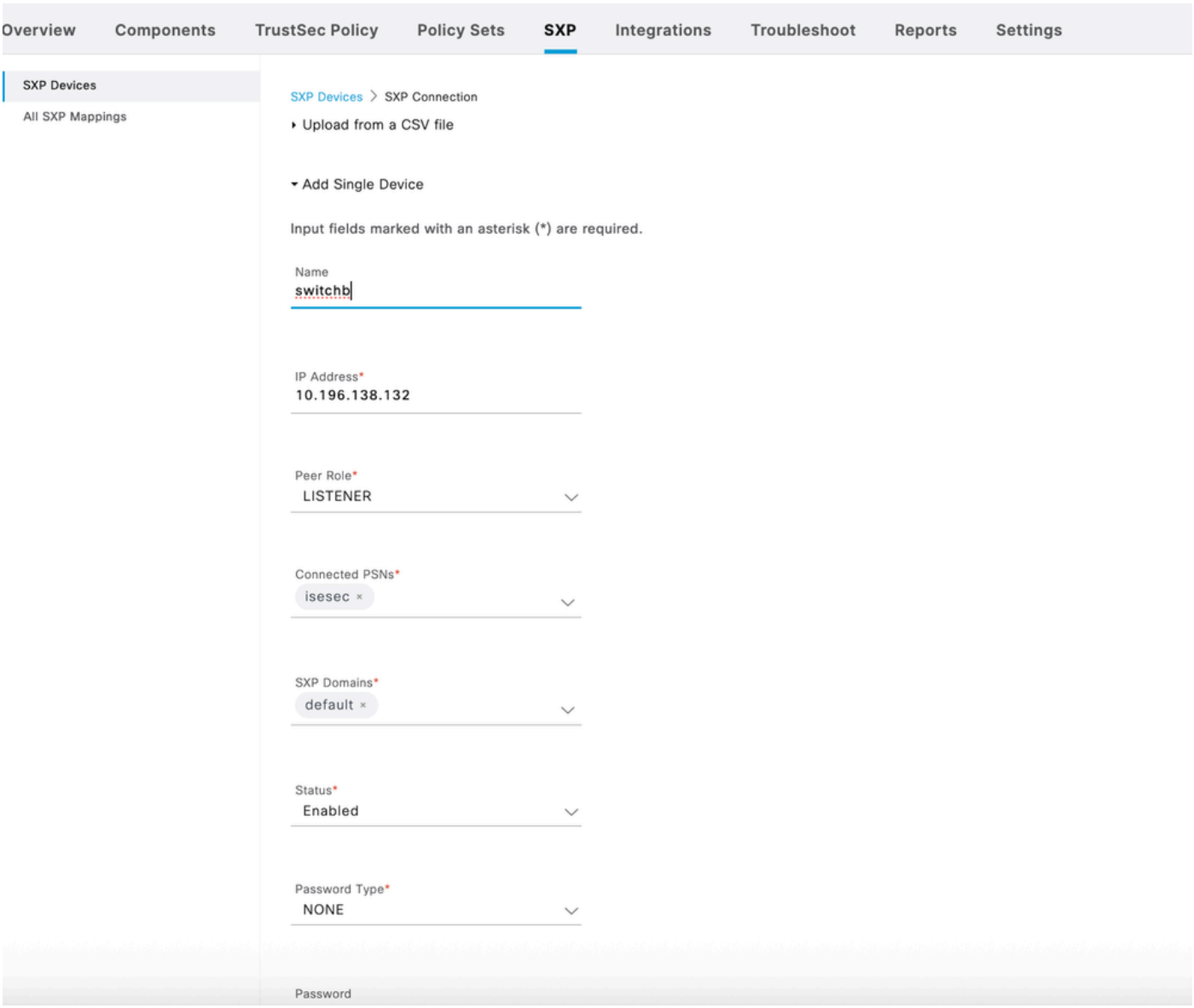
cts sxp default password xxxx@123

Configuration ISE

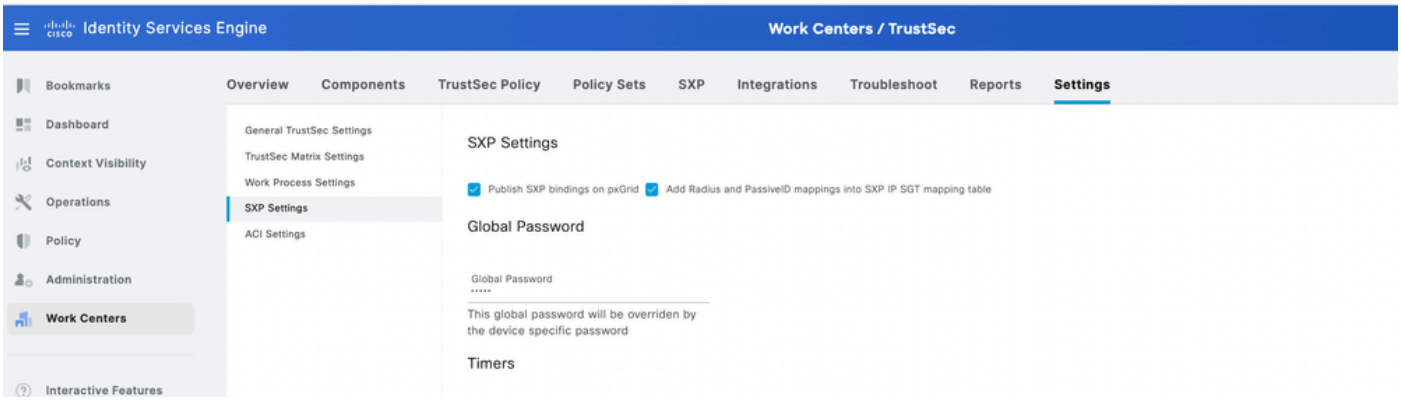
Étape 1 : Créer des stratégies d'authentification et d'autorisation sur ISE



Étape 2 : Configuration d'un périphérique SXP sur ISE



Étape 3 : Configurer le mot de passe global sous Paramètres SXP



Vérifier

```
WS-C3850-48F-E#show access-session interface gig1/0/45 details
            Interface:  GigabitEthernet1/0/45
              IIF-ID :  0x1A146F96
           Adresse MAC :  b496.9126.decc
          Adresse IPv6 :  Inconnu
          Adresse IPv4 :  Inconnu
            Nom d'utilisateur :  divya123
              État :  Autorisé
              Domaine :  DONNÉES
        Mode hôte d’exploitation :  hôte unique
      Oper control dir :  les deux
       Expiration de session :  S/O
     ID de session commun :  000000000000000B95163D98
       ID de session de compte :  Inconnu
              Poignée :  0x6f000001
        Politique actuelle :  POLICY_Gi1/0/45
Stratégies locales :
         Modèle de service : DEFAULT_LINKSEC_POLICY_MUST_SECURE (priorité 150)
       Stratégie de sécurité :  Doit être sécurisé
       État de sécurité :  Liaison non sécurisée
Stratégies de serveur :
Liste d'état de méthode :
        Method State
         dot1x Authc Success
WS-C3850-48F-E#
WS-C3850-48F-E(config)#do show cts sxp conn
SXP : Activée
```

Version la plus élevée prise en charge : 4

Mot de passe par défaut : Jeu

Chaîne de clés par défaut : non défini

Nom de la chaîne de clés par défaut : Sans objet

Adresse IP source par défaut : 10.196.138.yyy

Période d'ouverture des tentatives de connexion : 120 s

Période de rapprochement : 120 s

Le minuteur de nouvelle tentative est en cours

Limite de parcours de la séquence homologue pour l'exportation : non défini

Limite de parcours de la séquence homologue pour l'importation : non défini

---

IP homologue : 10.127.197.xxx

Source IP : 10.196.138.yyy

État de connexion : On (activé)

Conn version : 4

Fonctionnalité de connexion : IPv4-IPv6-Sous-réseau

Durée d'attente conn : 120 secondes

Mode local : Écouteur SXP

Inst# de connexion : 1

Conn. TCP fd : 1

Mot de passe de connexion TCP : none

Le minuteur de mise en attente est actif

Durée depuis le dernier changement d'état : 0:00:00:22 (jj:hr:mm:sec)

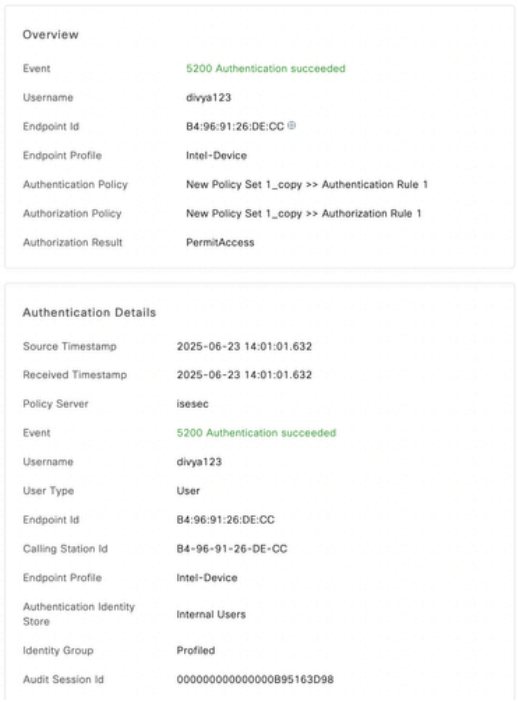
Nombre total de connexions SXP = 1

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

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

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

Le rapport du journal en direct affiche la balise SGT Guest appliquée :

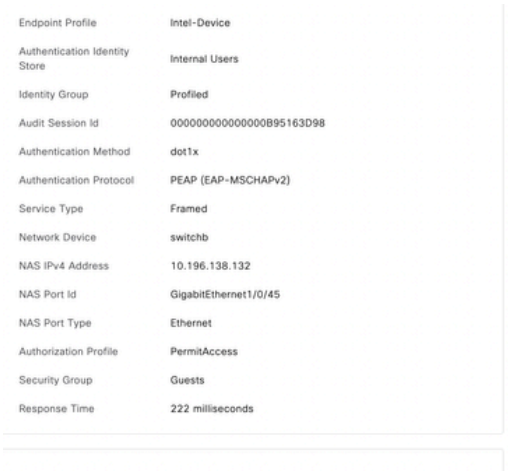


Overview

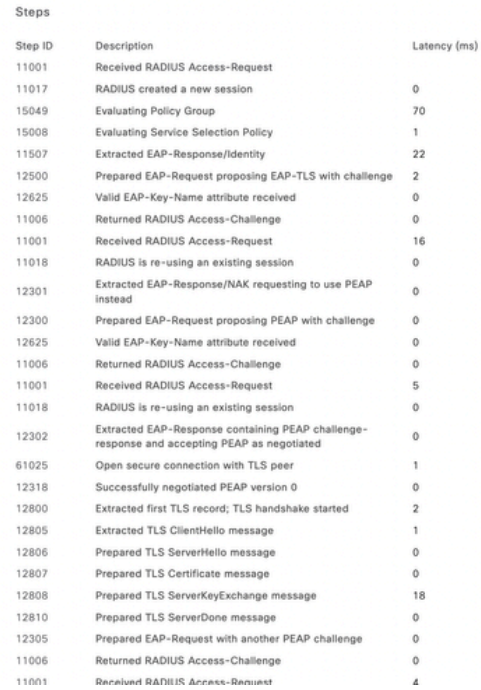
Event	5200 Authentication succeeded
Username	divya123
Endpoint Id	B4:96:91:26:DE:CC
Endpoint Profile	Intel-Device
Authentication Policy	New Policy Set 1_copy >> Authentication Rule 1
Authorization Policy	New Policy Set 1_copy >> Authorization Rule 1
Authorization Result	PermitAccess

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

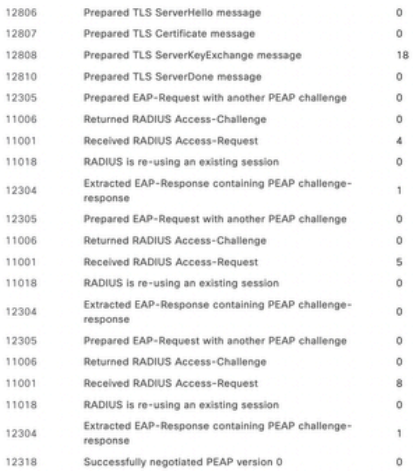


Endpoint Profile	Intel-Device
Authentication Identity Store	Internal Users
Identity Group	Profiled
Audit Session Id	000000000000000B95163D98
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	switchb
NAS IPv4 Address	10.196.138.132
NAS Port Id	GigabitEthernet1/0/45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

Dépannage

Activez ce débogage sur le commutateur pour résoudre les problèmes dot1x :

- debug dot1x all

Explication du journal

dot1x-packet:EAPOL pak rx - Ver: Type 0x1 : 0x1 **>>>>>>** Paquet EAPoL reçu par le commutateur
dot1x-packet : longueur: 0x0000

dot1x-ev : [b496.9126.decc, Gig1/0/45] client détecté, envoi de l'événement de démarrage de session pour b496.9126.decc **>>>>>** client dot1x détecté

dot1x-ev : [b496.9126.decc, Gig1/0/45] Authentification dot1x démarrée pour 0x26000007 (b496.9126.decc)**>>>>>** dot1x démarrée

%AUTHMGR-5-START : Démarrage de « dot1x » pour le client (b496.9126.decc) sur l'interface Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-sm :[b496.9126.decc, Gig1/0/45] Publication de !EAP_RESTART sur le client 0x26000007 **/>>>>>** Demande au client de redémarrer le processus EAP

dot1x-sm :[b496.9126.decc, Gig1/0/45] Publication de RX_REQ sur le client 0x26000007 **>>>>>>** en attente du paquet EAPoL du client

dot1x-sm :[b496.9126.decc, Gig1/0/45] Publication d'AUTH_START pour 0x26000007 **>>>>>** Démarrage du processus d'authentification

dot1x-ev : [b496.9126.decc, Gig1/0/45] Envoi du paquet EAPOL **>>>>>** Demande d’identité
dot1x-packet:EAPOL pak Tx - Ver: Type 0x3 : 0x0
dot1x-packet : longueur: 0x0005
dot1x-packet:code EAP: 0x1 id : Longueur 0x1 : 0x0005
dot1x-packet : type : 0x1
dot1x-packet : [b496.9126.decc, Gig1/0/45] paquet EAPOL envoyé au client 0x26000007

dot1x-ev : [Gig1/0/45] paquet reçu saddr = b496.9126.decc, daddr = 0180.c200.0003, pae-ether-type = 888e.0100.000a
dot1x-packet:EAPOL pak rx - Ver: Type 0x1 : 0x0 // Réponse d'identité
dot1x-packet : longueur: 0x000A

dot1x-sm :[b496.9126.decc, Gig1/0/45] Publication d'EAPOL_EAP pour 0x26000007 **>>>>>>** paquet EAPoL (réponse EAP) reçu, préparation de la requête au serveur

dot1x-sm : [b496.9126.decc, Gig1/0/45] Publication de la requête EAP pour 0x26000007 **>>>>>** Réponse du serveur reçue, la requête EAP est en cours de préparation

dot1x-ev : [b496.9126.decc, Gig1/0/45] Envoi du paquet EAPOL
dot1x-packet:EAPOL pak Tx - Ver: Type 0x3 : 0x0
dot1x-packet : longueur: 0x0006
dot1x-packet:code EAP: 0x1 id : Longueur 0xE5 : 0x0006
dot1x-packet : type : 0xD
dot1x-packet : [b496.9126.decc, Gig1/0/45] Paquet EAPOL envoyé au client 0x26000007 **>>>>>>** Requête EAP envoyée

dot1x-ev : [Gig1/0/45] pkt reçu saddr = b496.9126.decc, daddr = 0180.c200.0003, pae-ether-type = 888e.0100.0006 //réponse EAP reçue
dot1x-packet:EAPOL pak rx - Ver: Type 0x1 : 0x0
dot1x-packet : longueur: 0x0006
||
||
||

|| Ici, de nombreux événements EAPOL-EAP et EAP_REQ se produisent car de nombreuses informations sont échangées entre le commutateur et le client
|| Si les événements qui suivent ne suivent pas, les minuteurs et les informations envoyées jusqu'à présent doivent être vérifiés
||
||
||
dot1x-packet : [b496.9126.decc, Gig1/0/45] Received an EAP Success **>>>>>** EAP Success received from Server

dot1x-sm :[b496.9126.decc, Gig1/0/45] Publication d'EAP_SUCCESS pour 0x26000007 **>>>>>** Publication d'un événement de réussite EAP

dot1x-sm : [b496.9126.decc,Gig1/0/45] Publication de AUTH_SUCCESS sur le client 0x26000007 **>>>>>>** Publication de l'authentification réussie

%DOT1X-5-RÉUSSITE : Authentification réussie pour le client (b496.9126.decc) sur l'interface Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-packet : [b496.9126.decc, Gig1/0/45] Données de clé EAP détectées ajout à la liste d'attributs **>>>>>** Données de clé supplémentaires détectées envoyées par le serveur

%AUTHMGR-5-SUCCESS : Autorisation réussie pour le client (b496.9126.decc) sur l'interface Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-ev : [b496.9126.decc, Gig1/0/45] Réussite de l'autorisation reçue pour le client 0x26000007 (b496.9126.decc) **>>>>>** Réussite de l'autorisation

dot1x-ev : [b496.9126.decc, Gig1/0/45] Envoi du paquet EAPOL **>>>>>** Envoi du succès EAP au client
dot1x-packet:EAPOL pak Tx - Ver: Type 0x3 : 0x0
dot1x-packet : longueur: 0x0004
dot1x-packet:code EAP: 0x3 id : Longueur 0xED : 0x0004
dot1x-packet : [b496.9126.decc, Gig1/0/45] paquet EAPOL envoyé au client 0x26000007

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.