Configurazione dello switch con SXP e IBNS 2.0 per reti con identità

Sommario

Introduzione

In questo documento vengono descritte le procedure per configurare gli switch Cisco con SXP e IBNS 2.0 per Identity-Based Networking.

Prerequisiti

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Patch 4 per Identity Services Engine (ISE) versione 3.3
- Cisco Catalyst 3850

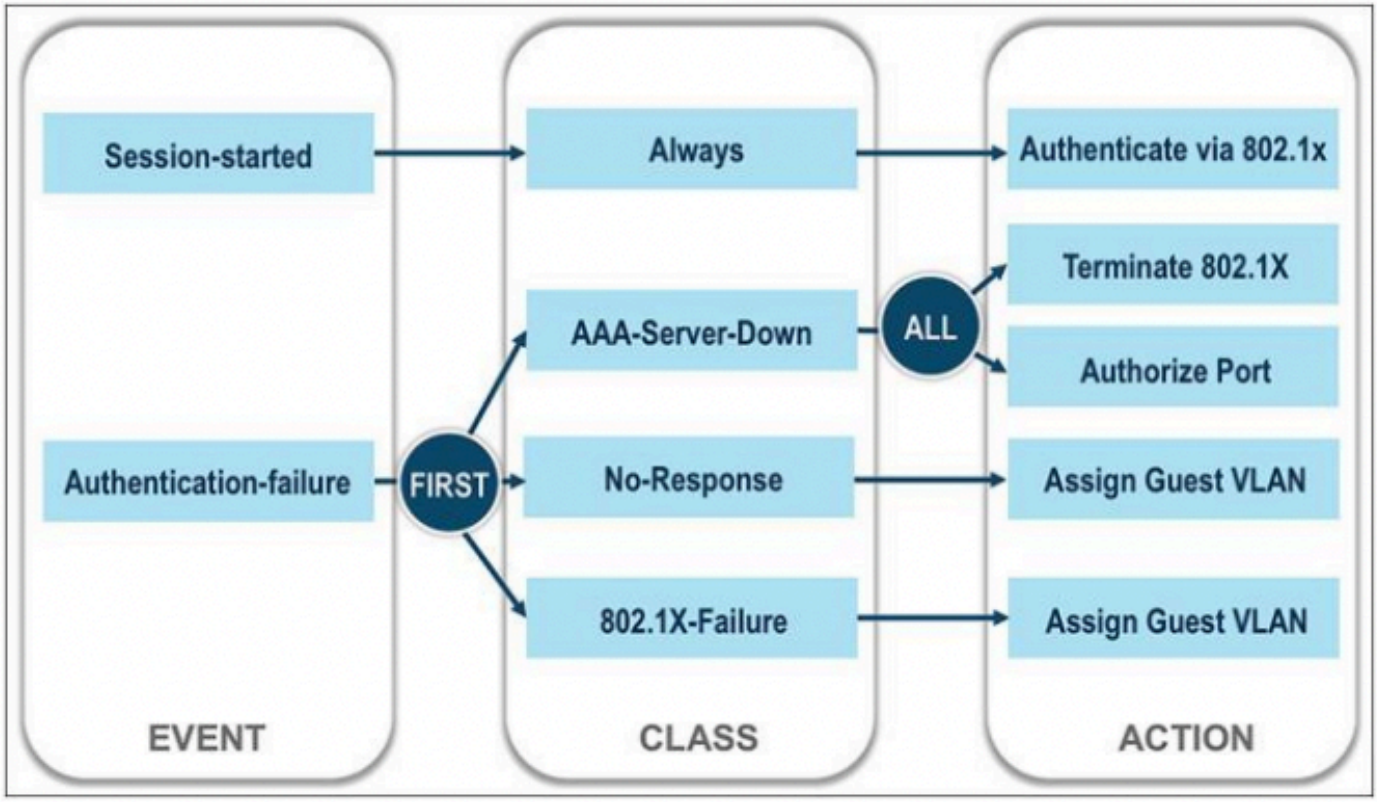
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

I criteri di controllo dell'identità definiscono le azioni che Access Session Manager esegue in risposta a condizioni ed eventi endpoint specifici. Utilizzando un linguaggio coerente, è possibile combinare varie azioni, condizioni ed eventi di sistema per creare tali criteri.

I criteri di controllo vengono applicati alle interfacce e sono principalmente responsabili della gestione dell'autenticazione degli endpoint e dell'attivazione dei servizi nelle sessioni. Ogni politica di controllo è costituita da una o più regole e da una strategia decisionale che determina il modo in cui tali regole vengono valutate.

Una regola dei criteri di controllo include una classe di controllo (un'istruzione condizionale flessibile), un evento che attiva la valutazione della condizione e una o più azioni. Mentre gli amministratori definiscono quali azioni vengono attivate da eventi specifici, alcuni eventi vengono forniti con azioni predefinite.



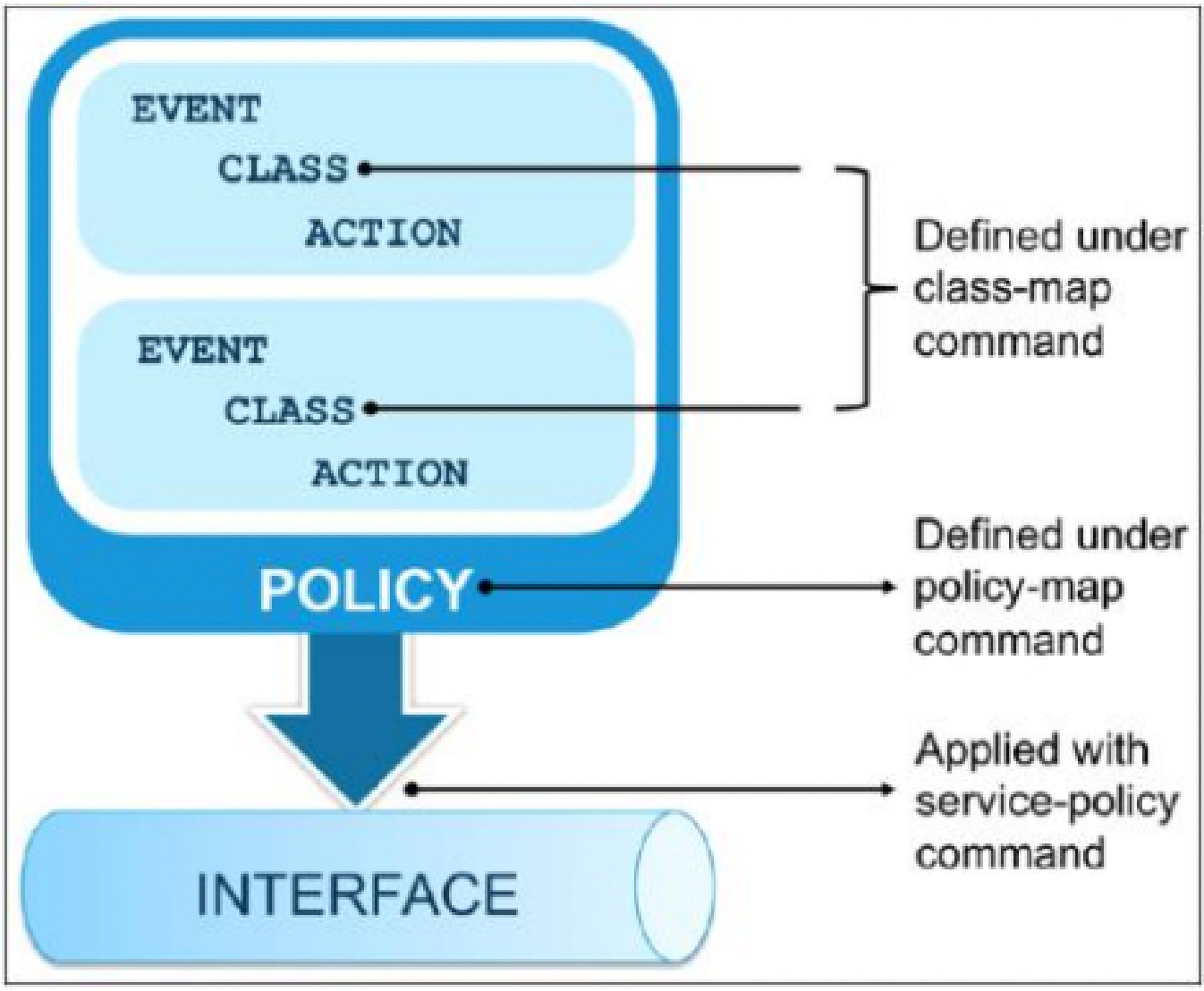
Criteri di controllo identità

Panoramica sulla configurazione dei criteri di controllo dell'identità

I criteri di controllo definiscono il comportamento del sistema utilizzando un evento, una condizione e un'azione. La configurazione di un criterio di controllo prevede tre passaggi principali:

1. Creare le classi di controllo:
   Una classe di controllo definisce le condizioni necessarie per attivare un criterio di controllo. Ogni classe può avere più condizioni che restituiscono true o false. È possibile impostare se tutte, qualsiasi o nessuna delle condizioni deve essere true affinché la classe venga considerata true. In alternativa, gli amministratori possono utilizzare una classe predefinita che non presenta condizioni e che restituisce sempre true.

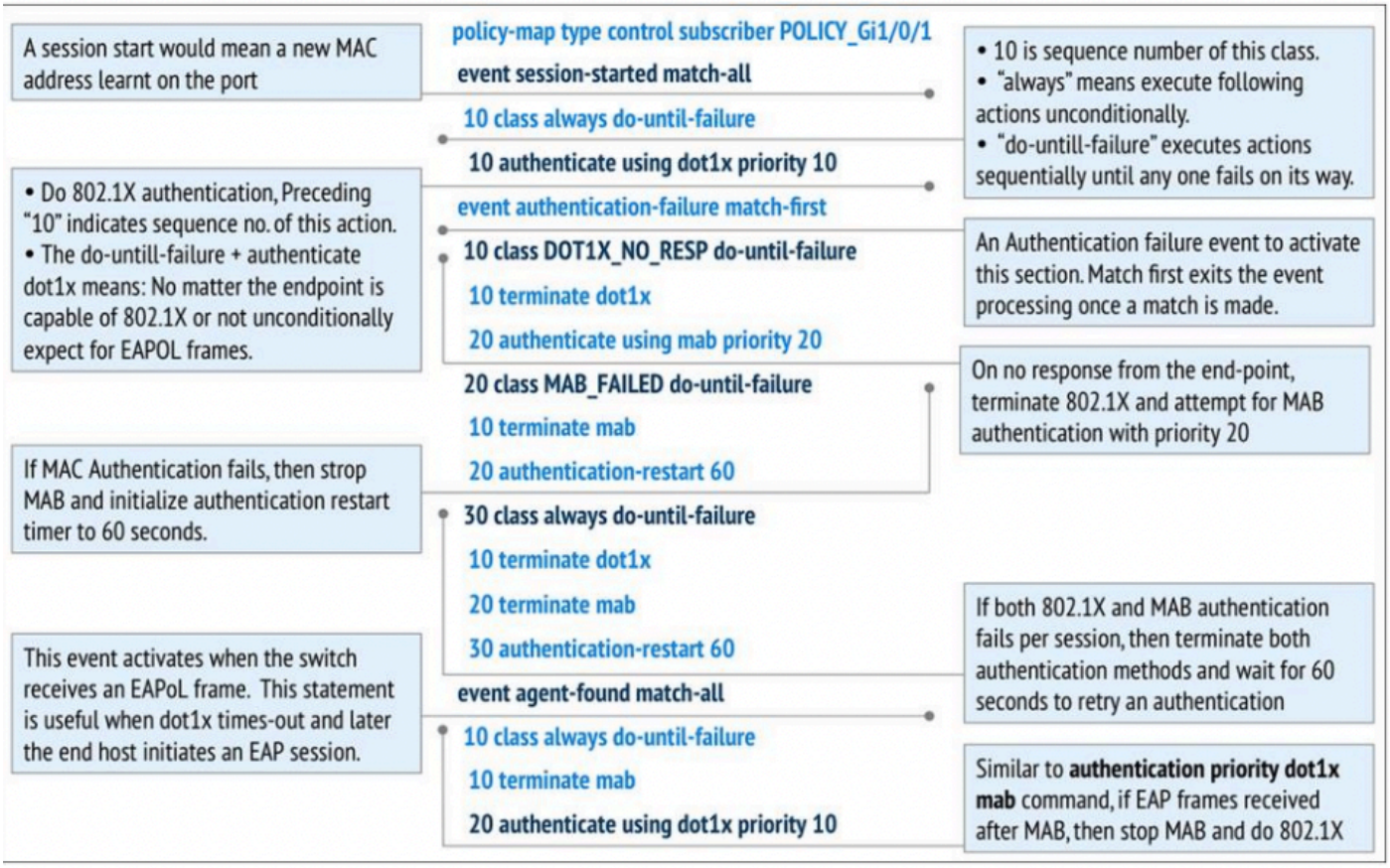
2. Creare il criterio di controllo:
   Un criterio di controllo contiene una o più regole. Ogni regola include una classe di controllo, un evento che attiva la verifica della condizione e una o più azioni. Le azioni vengono numerate ed eseguite in ordine.
3. Applica il criterio di controllo:
   Infine, applicare i criteri di controllo a un'interfaccia per attivarla.



Configurazione criteri di controllo identità

Il comando authentication display new-style converte le configurazioni legacy in un nuovo stile.

switch#authentication display new-style



Interpretazione dei criteri di controllo delle identità

Configurazione

Configurazione degli switch

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

!

autenticazione aaa dot1x valore predefinito gruppo raggio locale

autorizzazione aaa rete predefinita gruppo radius locale

username admin password 0 xxxxxx

!

!

!

!

server radius ISE1

indirizzo ipv4 10.127.197.xxx porta auth 1812 porta acct 1813

chiave pac xxxx@123

!

!

aaa group server radius ISE2

nome server ISE1

!

!

!

!

aaa new-model

id sessione aaa comune

!

autore dinamico radius server aaa

client 10.127.197.xxx chiave-server xxxx@123

dot1x system-auth-control

!

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

policy-map type control subscriber POLICY_Gi1/0/45

sottoscrittore di controllo del tipo di criteri di servizio POLICY_Gi1/0/45

WS-C3850-48F-E#show run | sec Gi1/0/45

policy-map type control subscriber POLICY_Gi1/0/45

event session-STARTED match-all

  10 classi sempre "do-until-failure"

   10 esegue l'autenticazione con priorità dot1x 10

event authentication-failure match-first

  5 class DOT1X_FAILED do-until-failure

   10 punto finale1x

```
   20 autenticazione-riavvio 60
  10 class DOT1X_NO_RESP do-until-failure
   10 punto finale1x
   20 autenticazione con priorità mab 20
  20 class MAB_FAILED do-until-failure
   10 terminazione mab
   20 autenticazione-riavvio 60
  40 classe sempre "do-until-failure"
   10 punto finale1x
   20 terminare mab
   30 autenticazione-riavvio 60
event agent-found match-all
  10 classi sempre "do-until-failure"
   10 terminazione mab
   20 autenticazione con priorità dot1x 10
event authentication-success match-all
  10 classi sempre "do-until-failure"
   10 attivare il modello di servizio DEFAULT_LINKSEC_POLICY_MUST_SECURE
sottoscrittore di controllo del tipo di criteri di servizio POLICY_Gi1/0/45
WS-C3850-48F-E#show run interface gig1/0/45
Creazione della configurazione in corso...
Configurazione corrente: 303 byte
!
interfaccia Gigabit Ethernet1/0/45
switchport access vlan 503
switchport mode access
host singolo in modalità host sessione di accesso
```

sessione di accesso chiusa

access-session port-control auto

mab

nessuna imposizione basata su ruoli cts

autenticatore pagina dot1x

sottoscrittore di controllo del tipo di criteri di servizio POLICY_Gi1/0/45

end

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

!

cts elenco autorizzazioni ISE2

cts sxp enable

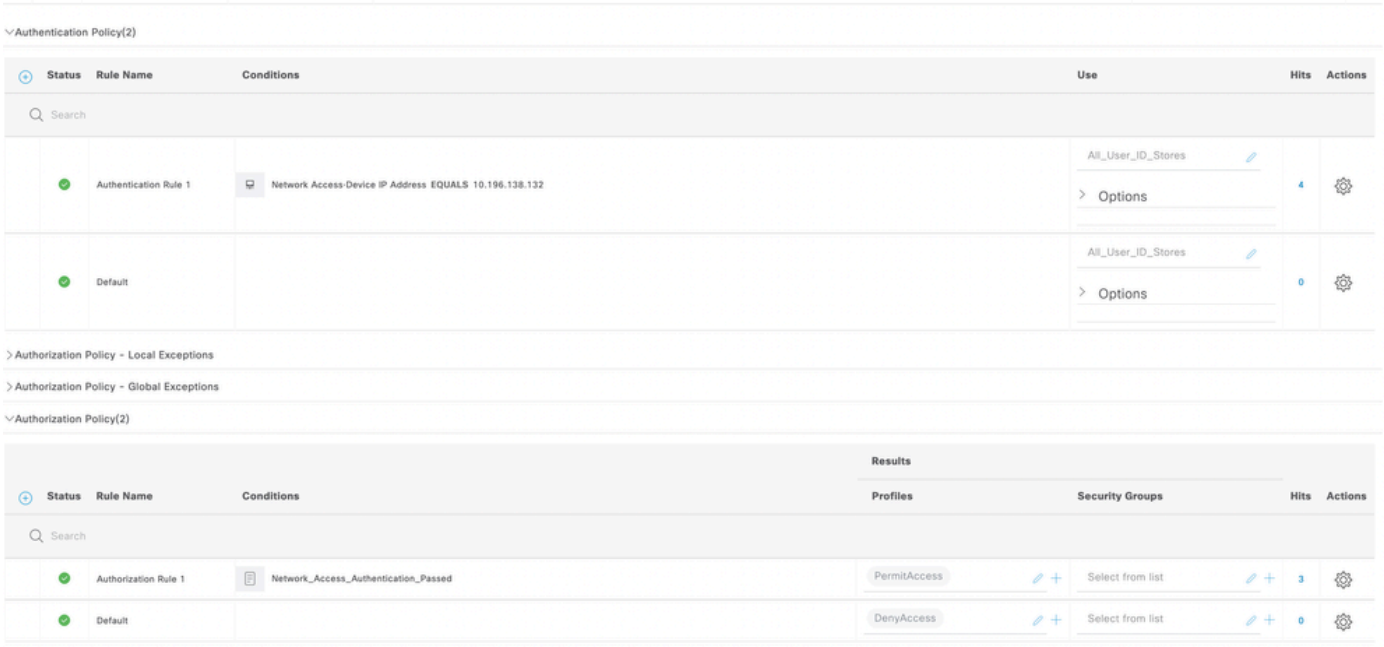
cts connessione sxp 10.127.197.xxx password none mode peer speaker hold-time 0

cts sxp default source-ip 10.196.138.yyy

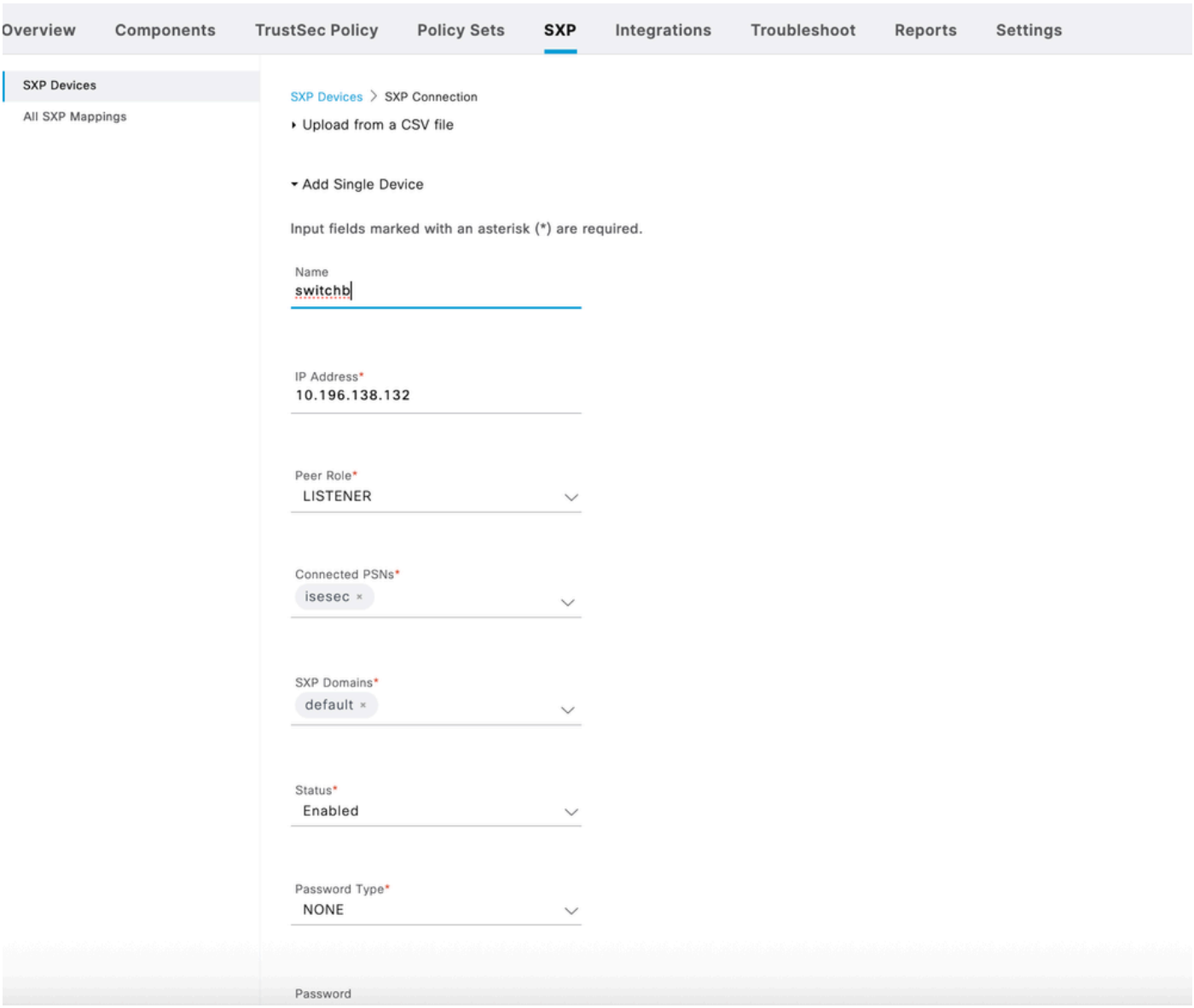
password predefinita sxp cts xxxx@123

Configurazione di ISE

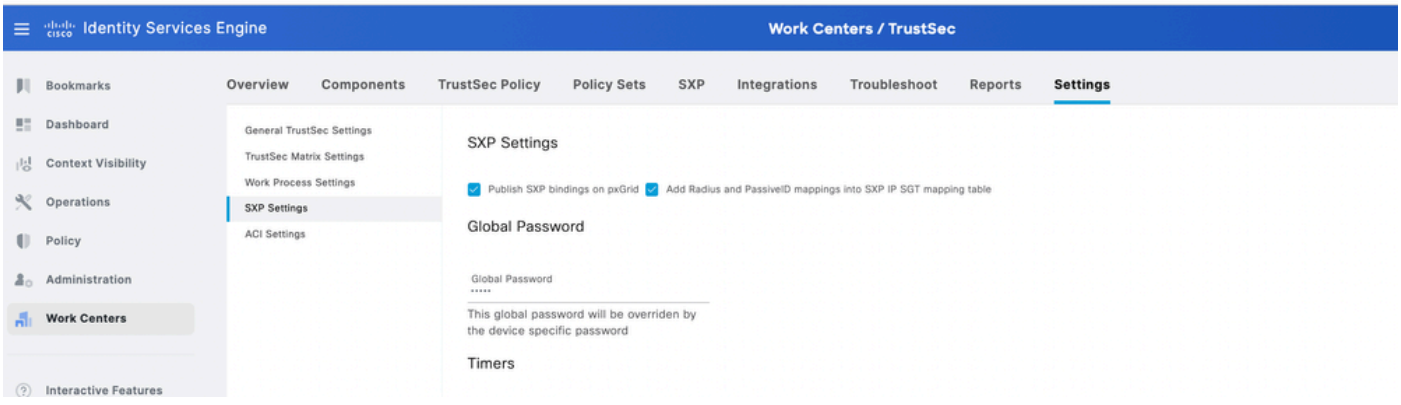
Passaggio 1: Creazione di policy di autenticazione e autorizzazione su ISE



Passaggio 2: Configurazione di una periferica SXP su ISE



Passaggio 3: Configurazione password globale in Impostazioni SXP



Verifica

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

Interfaccia: Gigabit Ethernet 1/0/45

IIF-ID: 0x1A146F96

Indirizzo MAC: b496.9126.decc

Indirizzo IPv6: Sconosciuto

Indirizzo IPv4: Sconosciuto

Nome utente: diya123

Stato: Autorizzato

Dominio: DATI

Modalità host operativo: host singolo

Direzione controllo operazioni: entrambi

Timeout sessione: N/D

ID sessione comune: 000000000000000B95163D98

ID sessione account: Sconosciuto

Maniglia: 0x6f000001

Criterio corrente: POLICY_Gi1/0/45

Criteri locali:

Modello di servizio: DEFAULT_LINKSEC_POLICY_MUST_SECURE (priorità 150)

Criterio di protezione: Protezione obbligatoria

Stato protezione: Collegamento non protetto

Criteri server:

Elenco stato metodo:

Stato metodo

dot1x Autenticazione riuscita

WS-C3850-48F-E#

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

SXP : Attivato

Versione più recente supportata: 4

Password predefinita: Imposta

Catena di chiavi predefinita: Non impostato

Nome catena di chiavi predefinita: Non applicabile

IP di origine predefinito: 10.196.138.yyy

Periodo di apertura tentativi di connessione: 120 sec

Periodo di riconciliazione: 120 sec

Il timer di riavvio è in esecuzione

Limite di attraversamento sequenza peer per esportazione: Non impostato

Limite di attraversamento sequenza peer per importazione: Non impostato

—

IP peer: 10.127.197.xxx

IP di origine: 10.196.138.yyy

Stato conn: On

Conversione : 4

Funzionalità Conn: Subnet IPv4-IPv6

Tempo di attesa continuo : 120 secondi

Modalità locale: Listener SXP

N. inizializzazione connessione: 1

TCP conn fd : 1

Password conn TCP: nessuna

Timer di attesa in esecuzione

Durata dall'ultima modifica dello stato: 0:00:00:22 (gg:hr:mm:sec)

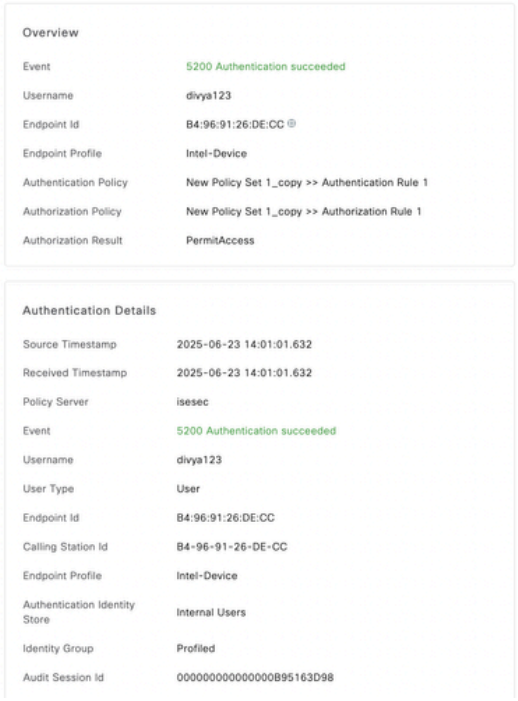
Numero totale di connessioni SXP = 1

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

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

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

Il report registro dal vivo mostra il tag SGT Guest applicato:

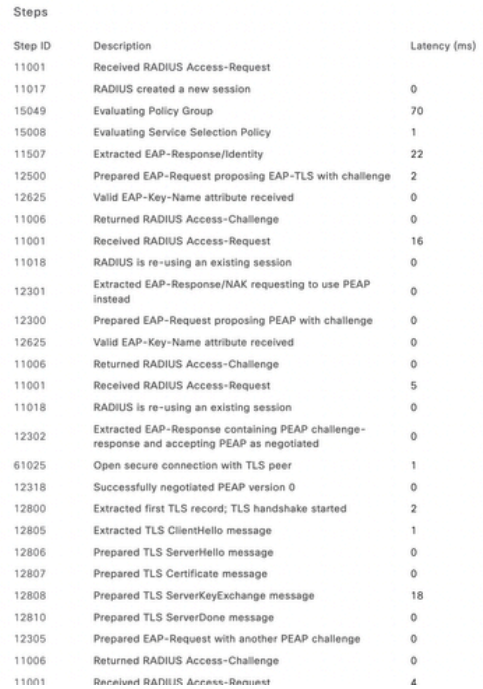


Overview

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

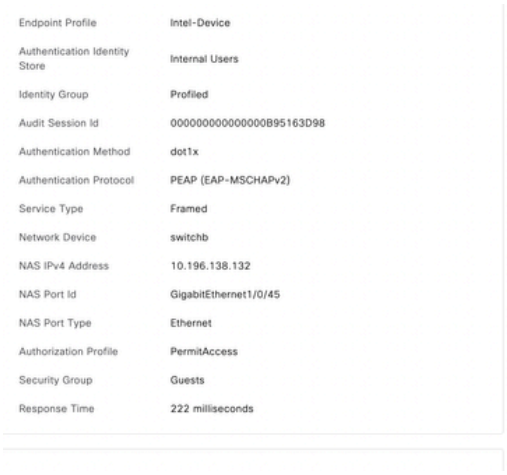
Authentication Details

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

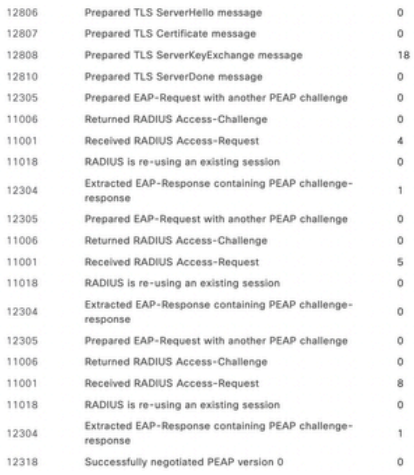


Steps

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

Risoluzione dei problemi

Abilitare questo debug sullo switch per la risoluzione dei problemi relativi al dot1x:

- debug dot1x all

Spiegazione registro

dot1x-packet:EAPOL pak rx - Versione: Tipo 0x1: 0x1 **>>>>>>** Pacchetto EAPoL ricevuto dallo switch
pacchetto dot1x: lunghezza: 0x0000

dot1x-ev:[b496.9126.decc, Gig1/0/45] rilevato client, invio evento di avvio sessione per b496.9126.decc **>>>** rilevato client dot1x

dot1x-ev:[b496.9126.decc, Gig1/0/45] Autenticazione Dot1x avviata per 0x26000007 (b496.9126.decc)**>>>>>** dot1x avviata

%AUTHMGR-5-START: Avvio di 'dot1x' per il client (b496.9126.decc) sull'interfaccia Gig1/0/45 AuditSessionID 0A6A258E000003500C9CFC3

dot1x-sm:[b496.9126.decc, Gig1/0/45] Invio di !EAP_RESTART sul client 0x26000007 **/>>>** Richiesta al client di riavviare il processo EAP

dot1x-sm:[b496.9126.decc, Gig1/0/45] Invio di RX_REQ sul client 0x26000007 **>>>** Attesa del pacchetto EAPoL dal client

dot1x-sm:[b496.9126.decc, Gig1/0/45] Invio di AUTH_START per 0x26000007 **>>>** Avvio del processo di autenticazione

dot1x-ev:[b496.9126.decc, Gig1/0/45] Invio del pacchetto EAPOL in corso **>>>>** Richiesta identità
dot1x-packet:EAPOL pak Tx - Versione: Tipo 0x3: 0x0
pacchetto dot1x: lunghezza: 0x0005
dot1x-packet:codice EAP: ID 0x1: 0x1 lunghezza: 0x0005
pacchetto dot1x: tipo: 0x1
pacchetto dot1x:[b496.9126.decc, Gig1/0/45] Pacchetto EAPOL inviato al client 0x26000007

dot1x-ev:[Gig1/0/45] Ricevuto pkt saddr =b496.9126.decc , daddr = 0180.c200.0003, pae-ther-type = 888e.0100.000a
dot1x-packet:EAPOL pak rx - Versione: Tipo 0x1: 0x0 // Risposta identità
pacchetto dot1x: lunghezza: 0x000A

dot1x-sm:[b496.9126.decc, Gig1/0/45] Invio di EAPOL_EAP per 0x26000007 **>>>>** Pacchetto EAPoL (risposta EAP) ricevuto, preparazione della richiesta al server

dot1x-sm:[b496.9126.decc, Gig1/0/45] Invio di EAP_REQ per 0x26000007 **>>>** Risposta del server ricevuta. Preparazione della richiesta EAP in corso...

dot1x-ev:[b496.9126.decc, Gig1/0/45] Invio del pacchetto EAPOL
dot1x-packet:EAPOL pak Tx - Versione: Tipo 0x3: 0x0
pacchetto dot1x: lunghezza: 0x0006
dot1x-packet:codice EAP: ID 0x1: 0xE5 lunghezza: 0x0006
pacchetto dot1x: tipo: 0xD
dot1x-packet:[b496.9126.decc, Gig1/0/45] Pacchetto EAPOL inviato al client 0x26000007 **>>>** Richiesta EAP inviata

dot1x-ev:[Gig1/0/45] Ricevuto pkt saddr =b496.9126.decc , daddr = 0180.c200.0003, tipo pae-etere = 888e.0100.0006 //Ricevuta risposta EAP
dot1x-packet:EAPOL pak rx - Versione: Tipo 0x1: 0x0
pacchetto dot1x: lunghezza: 0x0006
||
||
||

|| Si verificano numerosi eventi EAPOL-EAP e EAP_REQ in quanto lo switch e il client si scambiano molte informazioni
|| Se gli eventi successivi non seguono, è necessario controllare i timer e le informazioni inviate fino a questo momento
||
||
||
dot1x-packet:[b496.9126.decc, Gig1/0/45] Ricevuto EAP riuscito **>>>>>** EAP riuscito ricevuto dal server

dot1x-sm:[b496.9126.decc, Gig1/0/45] Invio di EAP_SUCCESS per 0x26000007 **>>>** Invio evento EAP riuscito

dot1x-sm:[b496.9126.decc,Gig1/0/45] Invio di AUTH_SUCCESS sul client 0x26000007 **>>>** Invio dell'autenticazione riuscito

%DOT1X-5-OPERAZIONE RIUSCITA: Autenticazione riuscita per il client (b496.9126.decc) sull'interfaccia Gig1/0/45 AuditSessionID 0A6A258E000003500C9CFC3

dot1x-packet:[b496.9126.decc, Gig1/0/45] Rilevati dati di chiave EAP che aggiungono all'elenco attributi **>>>>** Rilevati dati di chiave aggiuntivi inviati dal server

%AUTHMGR-5-OPERAZIONE RIUSCITA: Autorizzazione completata per il client (b496.9126.decc) sull'interfaccia Gig1/0/45 AuditSessionID 0A6A258E000003500C9CFC3

dot1x-ev:[b496.9126.decc, Gig1/0/45] Ricevuto successo di autenticazione per il client 0x26000007 (b496.9126.decc) **>>>>>** Operazioni di autorizzazione riuscite

dot1x-ev:[b496.9126.decc, Gig1/0/45] Invio del pacchetto EAPOL **>>>>** Invio di EAP riuscito al client
dot1x-packet:EAPOL pak Tx - Versione: Tipo 0x3: 0x0
pacchetto dot1x: lunghezza: 0x0004
dot1x-packet:codice EAP: ID 0x3: 0xLunghezza ED: 0x0004
pacchetto dot1x:[b496.9126.decc, Gig1/0/45] Pacchetto EAPOL inviato al client 0x26000007

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).