アイデンティティベースネットワーク用のSXPおよびIBNS 2.0を備えたスイッチの設定

内容

はじめに

このドキュメントでは、IDベースのネットワーキングのためにSXPおよびIBNS 2.0を使用してCiscoスイッチを設定する手順について説明します。

前提条件

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Identity Services Engine(ISE)バージョン3.3パッチ4
- Cisco Catalyst スイッチ 3850

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

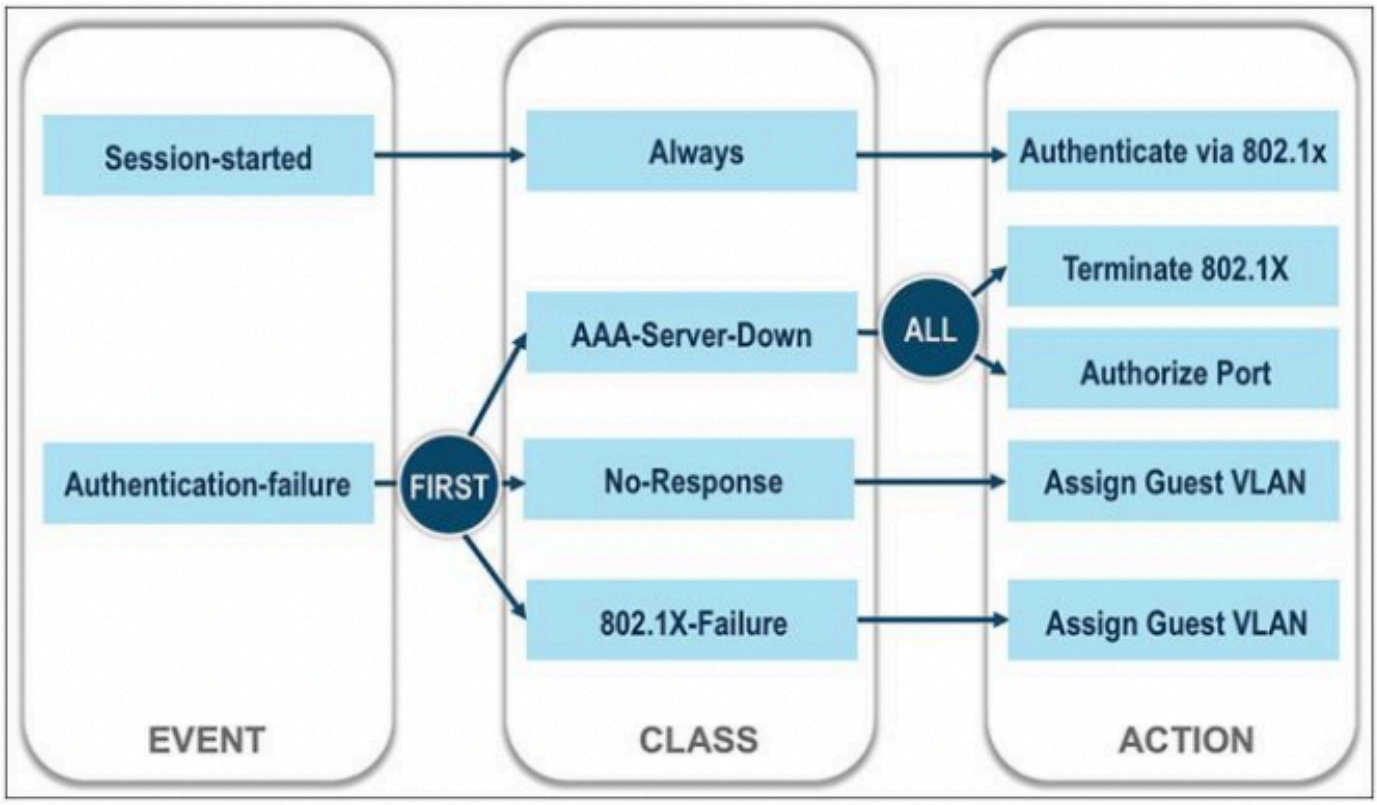
背景説明

アイデンティティコントロールポリシーは、特定の条件やエンドポイントイベントに応じてアク

セスセッションマネージャが実行するアクションを定義します。一貫したポリシー言語を使用して、さまざまなシステムアクション、条件、およびイベントを組み合わせて、これらのポリシーを形成できます。

制御ポリシーはインターフェイスに適用され、主にエンドポイント認証の管理とセッションでのサービスのアクティブ化を行います。各制御ポリシーは、1つ以上のルールと、それらのルールの評価方法を決定する決定戦略で構成されます。

制御ポリシールールには、制御クラス（柔軟な条件文）、条件評価をトリガーするイベント、および1つ以上のアクションが含まれます。管理者は特定のイベントによってトリガーされるアクションを定義しますが、一部のイベントには定義済みのデフォルトアクションが付属しています。



アイデンティティコントロールポリシー

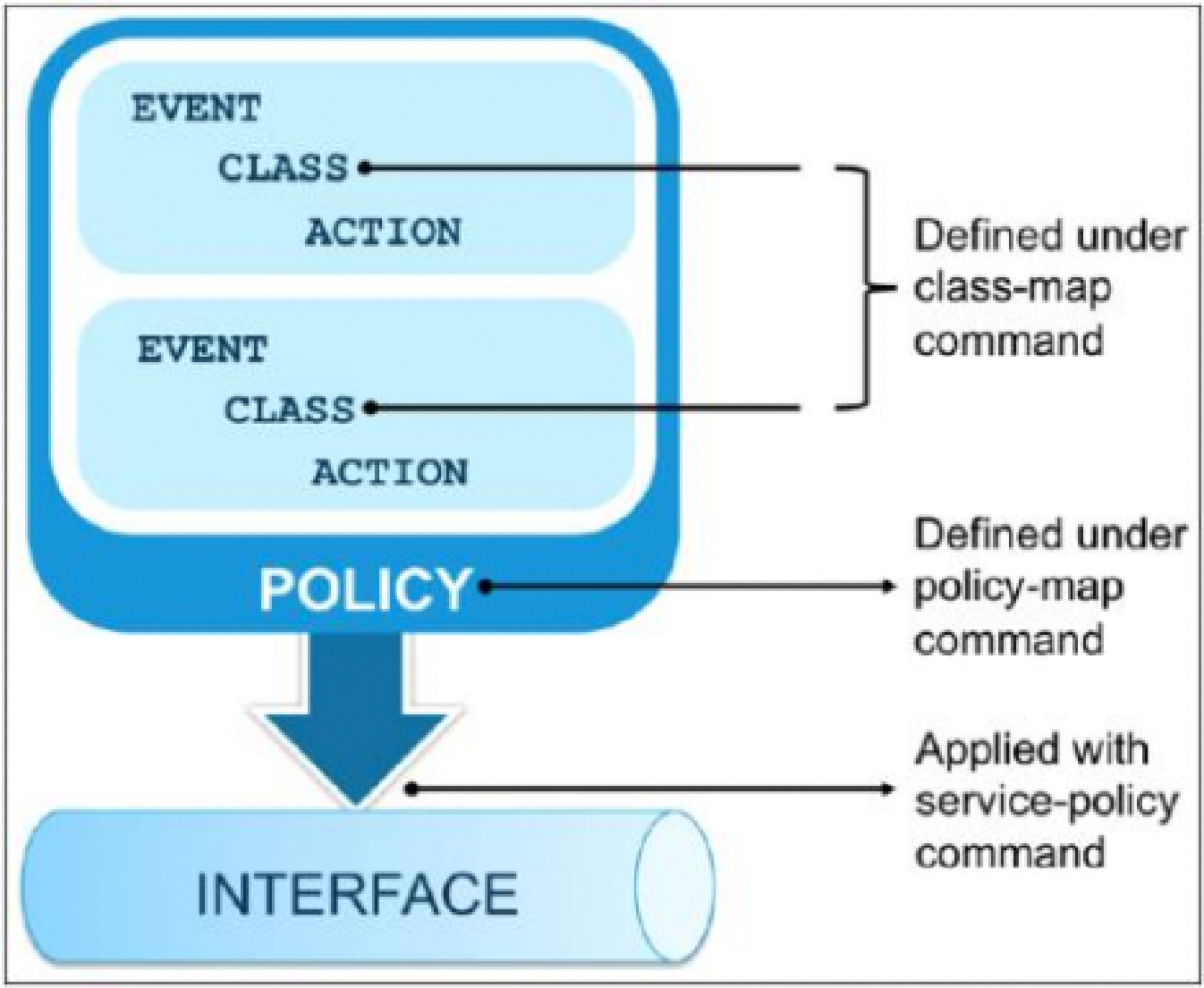
アイデンティティコントロールポリシー設定の概要

コントロールポリシーは、イベント、条件、およびアクションを使用してシステムの動作を定義します。制御ポリシーの設定には、主に3つのステップがあります。

1. 制御クラスを作成します。
   制御クラスは、制御ポリシーをアクティブにするために必要な条件を定義します。各クラスには、trueまたはfalseとして評価される複数の条件を指定できます。クラスがtrueと見なされるためには、条件のall、any、またはnoneをtrueに設定する必要があります。または、条件を持たず、常にtrueと評価される既定のクラスを使用することもできます。
2. 制御ポリシーを作成します。
   制御ポリシーには1つ以上の規則が含まれています。各ルールには、制御クラス、条件チェックをトリガーするイベント、および1つ以上のアクションが含まれます。アクションは順

番に番号付けされ、実行されます。

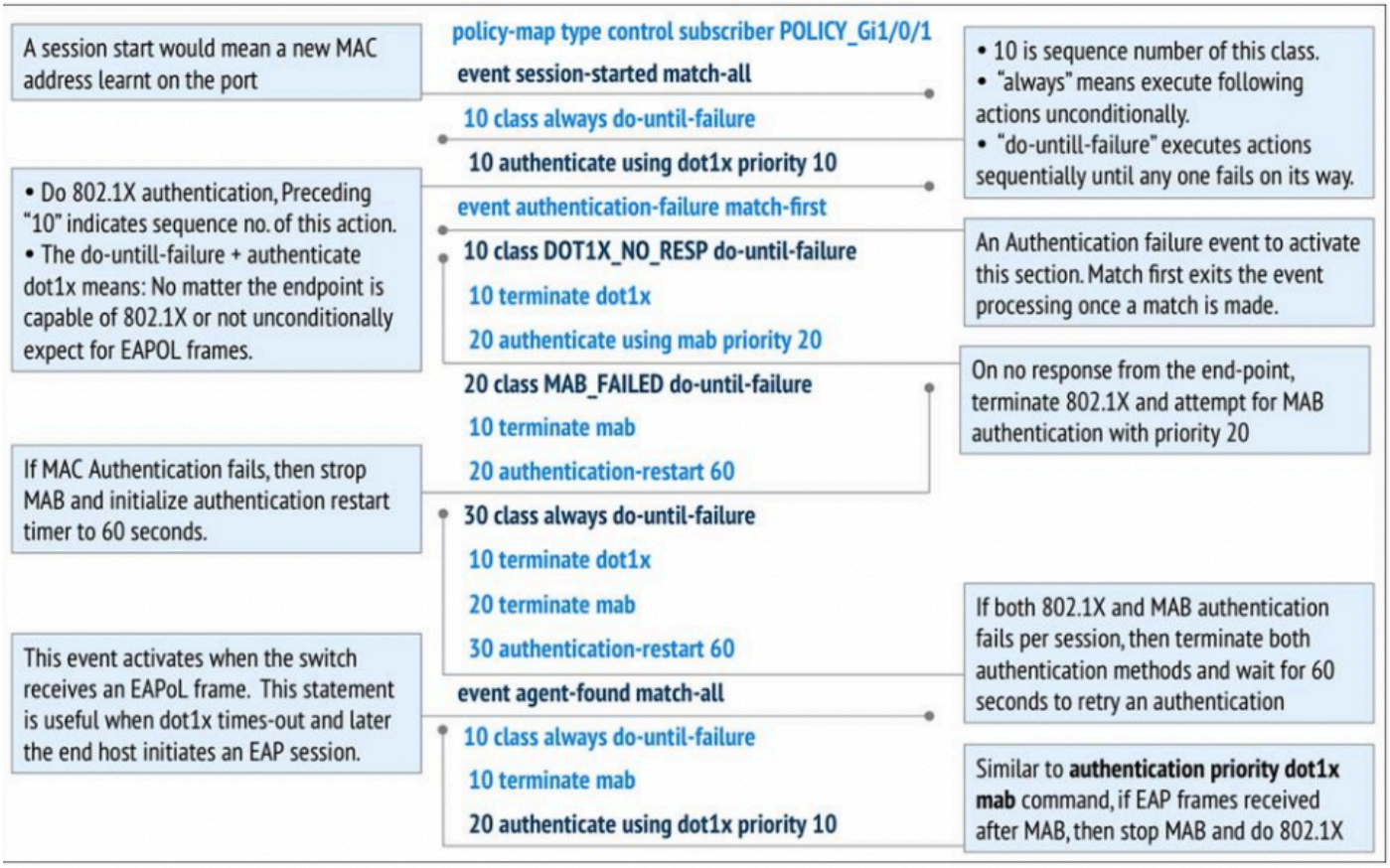
3. 制御ポリシーを適用します。
   最後に、制御ポリシーをインターフェイスに適用してアクティブにします。



アイデンティティコントロールポリシーの設定

authentication display new-styleコマンドを使用すると、の従来の設定が新しいスタイルに変換されます。

switch#authentication display new-style



アイデンティティコントロールポリシーの解釈

設定

スイッチの設定

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

!

aaa authentication dot1x default group radiusローカル

aaa authorization network default group radius local（認可ネットワークのデフォルトグループradiusローカル）

username admin password 0 xxxxxx

!

!

!

!

radiusサーバISE1

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

pacキーxxxx@123

!

!

aaaグループサーバradius ISE2

サーバ名ISE1

!

!

!

!

aaa new-model

aaa session-id共通

!

aaaサーバradius dynamic-author

クライアント10.127.197.xxxサーバキー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

service-policyタイプのコントロールサブスクライバ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（イベントセッション開始の一致 – すべて）

  10クラスalways do-until-failure

   10 dot1x priority 10を使用して認証

event authentication-failure match-first（イベント認証失敗マッチファースト）

  5クラスDOT1X_FAILED do-until-failed

10 dot1xの終了

20認証再起動60

10クラスDOT1X_NO_RESP do-until-failure

10 dot1xの終了

20 mabプライオリティ20を使用して認証

20クラスMAB_FAILED do-until-failed

10 mabの終了

20認証再起動60

40クラスalways do-until-failure

10 dot1xの終了

20 mabの終了

30認証再起動60

event agent-found match-all（イベントエージェントが見つけた一致 – すべて）

10クラスalways do-until-failure

10 mabの終了

20 dot1x priority 10を使用した認証

event authentication-success match-all（イベント認証 – 成功の一致 – すべて）

10クラスalways do-until-failure

10 service-template DEFAULT_LINKSEC_POLICY_MUST_SECUREのアクティブ化

service-policyタイプのコントロールサブスクライバPOLICY_Gi1/0/45

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

Building configuration...

Current configuration :303 bytes

!

interface GigabitEthernet1/0/45

switchport access vlan 503

switchport mode access

access-session host-mode single-hostコマンド

アクセスセッションが閉じている

access-session port-control auto（自動アクセスセッションポート制御）

mab

ctsロールベースの適用なし

dot1x pae authenticator

service-policyタイプのコントロールサブスクライバPOLICY_Gi1/0/45

最後

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

!

cts許可リストISE2

cts sxpの有効化

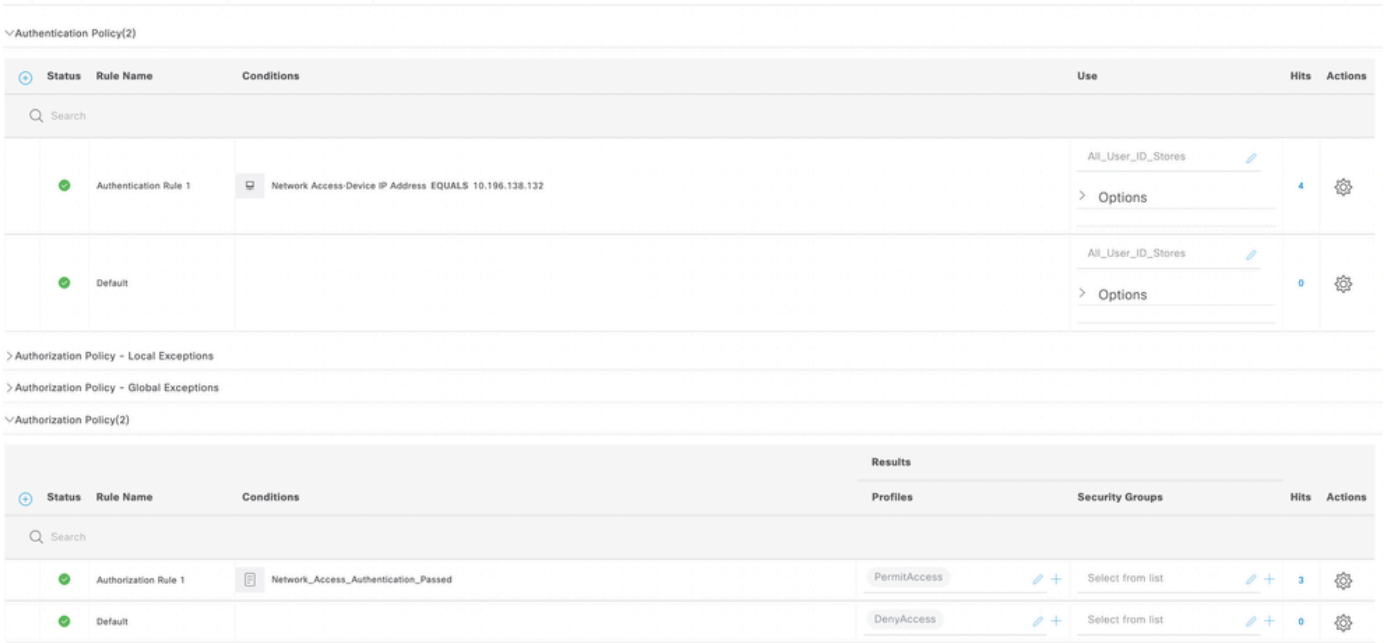
cts sxp connection 10.127.197.xxx password none mode peer speaker hold-time 0

cts sxp default source-ip 10.196.138.yyy（日本での対応時期未定）

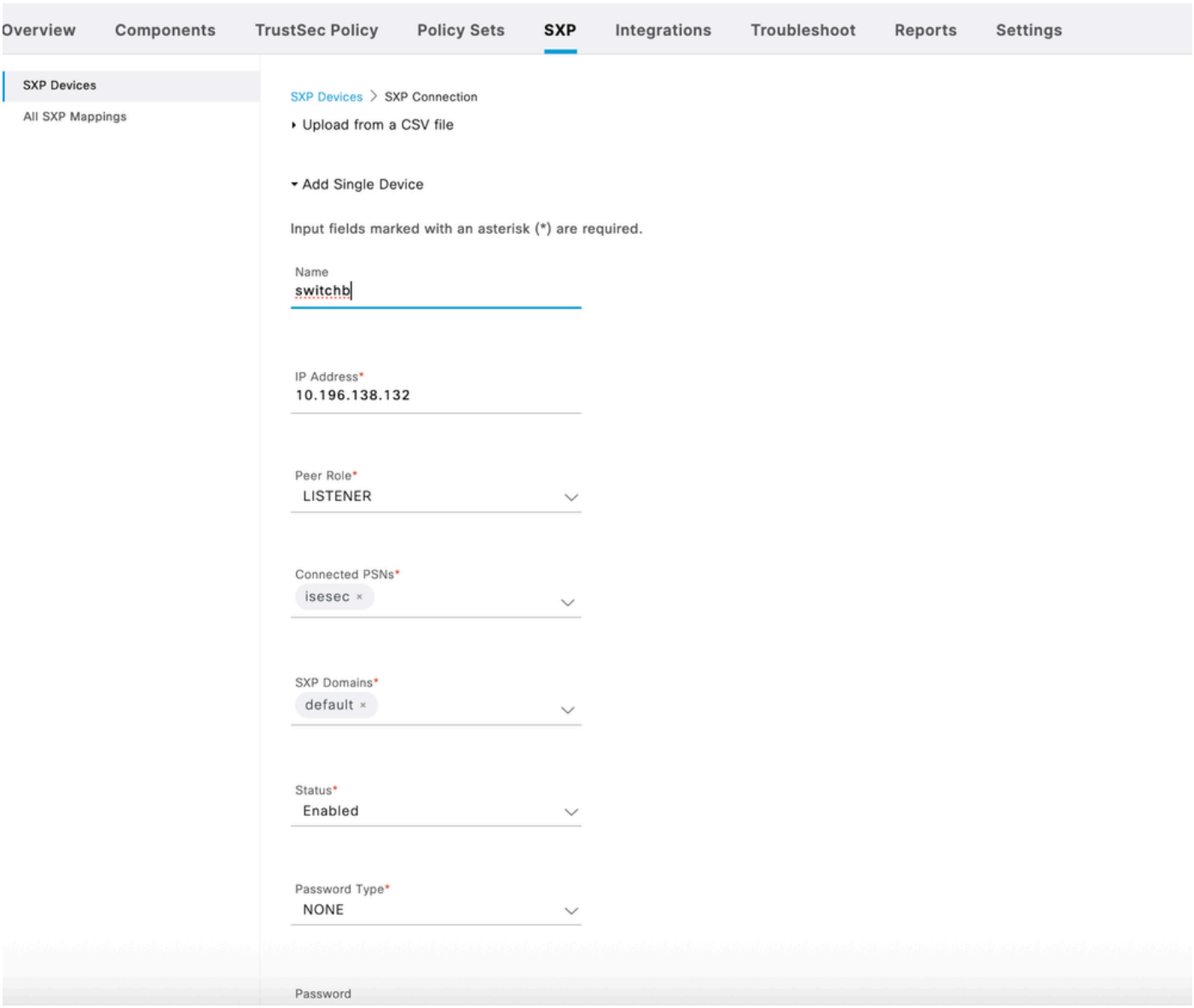
cts sxpデフォルトパスワードxxxx@123

ISE 設定

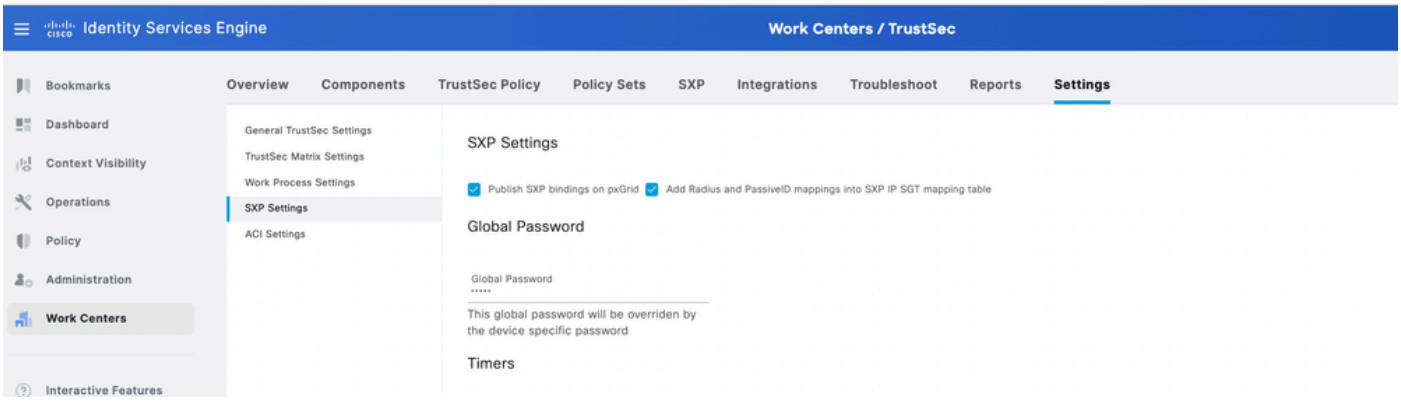
手順1:ISEでの認証および認可ポリシーの作成



ステップ2:ISEでSXPデバイスを設定します。



ステップ3:SXP設定でグローバルパスワードを設定します。



確認

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

インターフェイス：GigabitEthernet1/0/45

IIF-ID: 0x1A146F96

MACアドレス：b496.9126.decc

IPv6アドレス：不明

IPv4アドレス：不明

ユーザ名：divya123

ステータス：承認済み

ドメイン：DATA

Oper hostモード：single-host

Oper control dir:both(オペレーションコントロールディレクトリ：両方)

セッションタイムアウト：なし

共通セッションID:000000000000000B95163D98

アカウントセッションID:不明

ハンドル：0x6f000001

現在のポリシー：POLICY_Gi1/0/45

ローカルポリシー：

サービステンプレート：DEFAULT_LINKSEC_POLICY_MUST_SECURE（優先度150）

セキュリティポリシー：セキュリティ保護が必要

セキュリティの状態：リンクは保護されていません

サーバポリシー：

メソッドの状態リスト：

メソッドの状態

dot1x Authc成功

WS-C3850-48F-E番号

WS-C3850-48F-E（設定）#doshow cts sxp conn

SXP：有効

サポートされる最新バージョン：4

デフォルトパスワード：設定

既定のキーチェーン：未設定

デフォルトのキーチェーン名：該当なし

デフォルトの送信元IP:10.196.138.yyy

接続再試行オープン時間：120秒

調整期間：120秒

リトライのオープンタイマーが実行中です

エクスポートのピアシーケンスのトラバース制限：未設定

インポートのピアシーケンスのトラバース制限：未設定

ピアIP:10.127.197.xxx

送信元IP:10.196.138.yyy

Conn status：オン

Connバージョン:4

接続機能:IPv4-IPv6-Subnet

Connホールドタイム:120秒

ローカルモード:SXPリスナー

接続インスタンス#:1

TCP conn fd :1

TCP conn password：なし

ホールドタイマーが実行中

前回の状態変更からの継続時間： 0:00:00:22 (dd:hr:mm:sec)

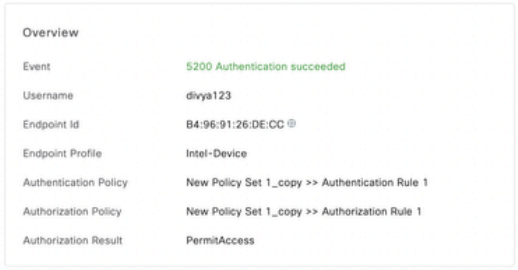
SXP接続の総数= 1

0xFF8CBFC090 VRF:、fd: 1、ピアIP: 10.127.197.xxx

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

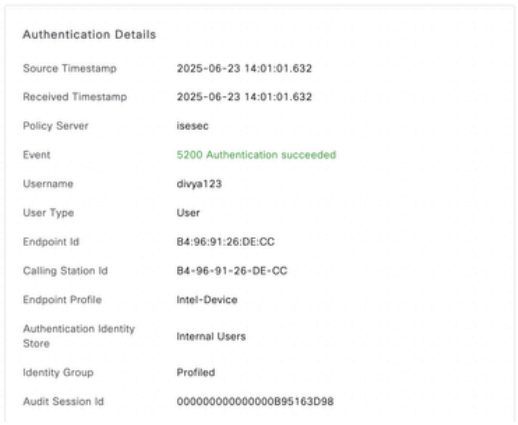
WS-C3850-48F-E(config)#

ライブログレポートに、SGTタグGuest appliedが表示されます。



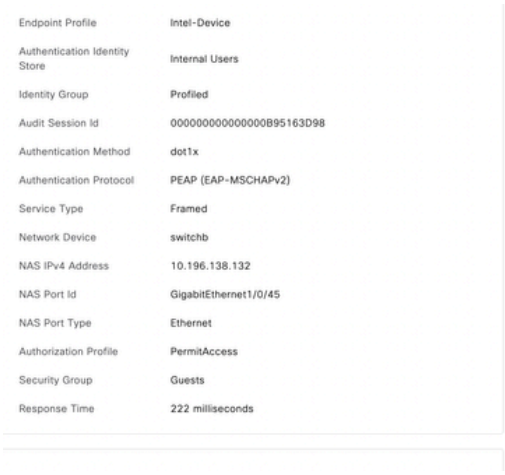
Overview

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

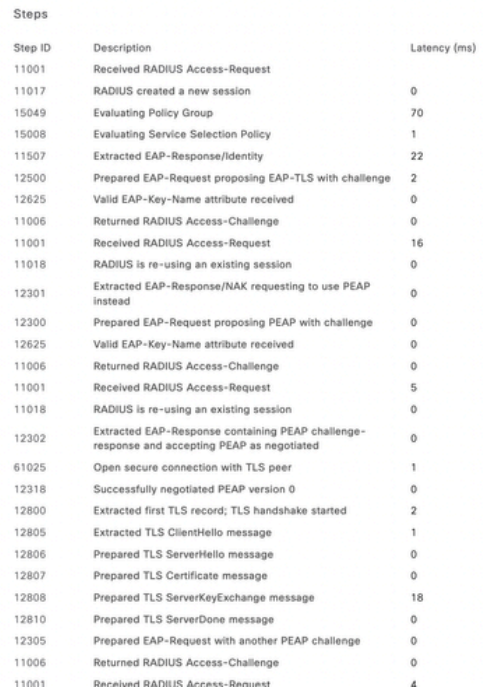


Authentication Details

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

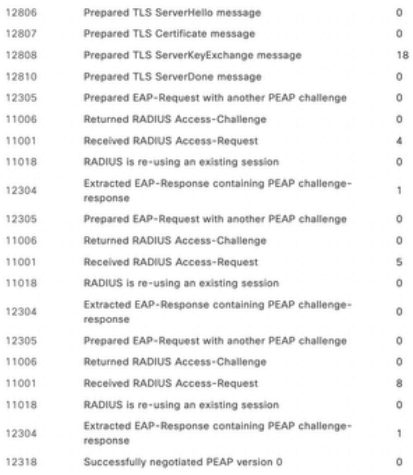


Endpoint Profile	Intel-Device
Authentication Identity Store	Internal Users
Identity Group	Profiled
Audit Session Id	000000000000000B95163D98
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	switchb
NAS IPv4 Address	10.196.138.132
NAS Port Id	GigabitEthernet1/0/45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

トラブルシュート

dot1xの問題のトラブルシューティングを行うには、スイッチで次のデバッグを有効にします。

- debug dot1x all

ログの説明

dot1x-packet:EAPOL pak rx - Ver: 0x1 type: 0x1 >>>>スイッチで受信されたEAPoLパケット
dot1x-packet：長さ：0x0000

dot1x-ev:[b496.9126.decc, Gig1/0/45]クライアントの検出、b496.9126.deccのセッション開始イベントの送信>>>>> dot1xクライアントの検出

dot1x-ev:[b496.9126.decc, Gig1/0/45] 0x26000007に対するdot1x認証の開始

(b496.9126.decc)>>>> dot1xの開始

%AUTHMGR-5-START：インターフェイスGig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3上のクライアント(b496.9126.decc)の「dot1x」を開始しています

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting !EAP_RESTART on Client 0x26000007 />>>>：クライアントにEAPプロセスの再起動を要求

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting RX_REQ on Client 0x26000007 >>>>> クライアントからのEAPoLパケットの待機

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting AUTH_START for 0x26000007 >>>> 認証プロセスの開始

dot1x-ev:[b496.9126.decc, Gig1/0/45] Sending out EAPOL packet >>>>> Identity Request
dot1x-packet:EAPOL pak Tx - Ver:0x3タイプ：0x0
dot1x-packet：長さ：0x0005
dot1x-packet:EAPコード：0x1 id: 0x1 length: 0x0005
dot1x-packet：タイプ：0x1
dot1x-packet:[b496.9126.decc, Gig1/0/45]クライアント0x26000007に送信されるEAPOLパケット

dot1x-ev:[Gig1/0/45] Received 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
dot1x-packet：長さ：0x000A

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting EAPOL_EAP for 0x26000007 >>>> EAPoLパケット(EAP Response)を受信し、サーバへの要求を準備

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting EAP_REQ for 0x26000007 >>>> Server response received, EAP Request is being prepared

dot1x-ev:[b496.9126.decc, Gig1/0/45] EAPOLパケットの送信
dot1x-packet:EAPOL pak Tx - Ver:0x3タイプ：0x0
dot1x-packet：長さ：0x0006
dot1x-packet:EAPコード：0x1 id:0xE5 length: 0x0006
dot1x-packet：タイプ：0xD
dot1x-packet:[b496.9126.decc, Gig1/0/45] EAPOLパケットがクライアントに送信される 0x26000007 >>>> EAP要求が送信される

dot1x-ev:[Gig1/0/45] Received pkt saddr =b496.9126.decc , daddr = 0180.c200.0003, pae-ether-type = 888e.0100.0006 //EAP response received
dot1x-packet:EAPOL pak rx - Ver:0x1タイプ：0x0
dot1x-packet：長さ：0x0006
||
||
||
||ここでは、スイッチとクライアントの間で多くの情報が交換されると、多くのEAPOL-EAPおよ

びEAP_REQイベントが発生します
||これ以降のイベントが続かない場合は、タイマーとこれまで送信された情報を確認する必要があります
||
||
||
dot1x-packet:[b496.9126.decc, Gig1/0/45] Received an EAP Success >>> EAP Success eed from Server

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

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

%DOT1X-5-SUCCESS：クライアント(b496.9126.decc)の認証がインターフェイスGig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3で成功しました

dot1x-packet:[b496.9126.decc, Gig1/0/45] EAP Key data detected adding to attribute list >>>> サーバによって送信された追加キーデータ

%AUTHMGR-5-SUCCESS：クライアント(b496.9126.decc)の認証がインターフェイスGig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3で成功しました

dot1x-ev:[b496.9126.decc, Gig1/0/45] Received Authz Success for the client 0x26000007 (b496.9126.decc) >>>> Authorization Success

dot1x-ev:[b496.9126.decc, Gig1/0/45] Sending out EAPOL packet >>>> Sending EAP Success to the client
dot1x-packet:EAPOL pak Tx - Ver:0x3タイプ：0x0
dot1x-packet：長さ：0x0004
dot1x-packet:EAPコード：0x3 id: 0xED長： 0x0004
dot1x-packet:[b496.9126.decc, Gig1/0/45]クライアント0x26000007に送信されるEAPOLパケット

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。