为基于身份的网络配置SXP和IBNS 2.0的交换机

目录

简介

本文档介绍使用SXP和IBNS 2.0为基于身份的网络配置思科交换机的过程。

先决条件

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 身份服务引擎(ISE)版本3.3补丁4
- Cisco Catalyst交换机3850

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

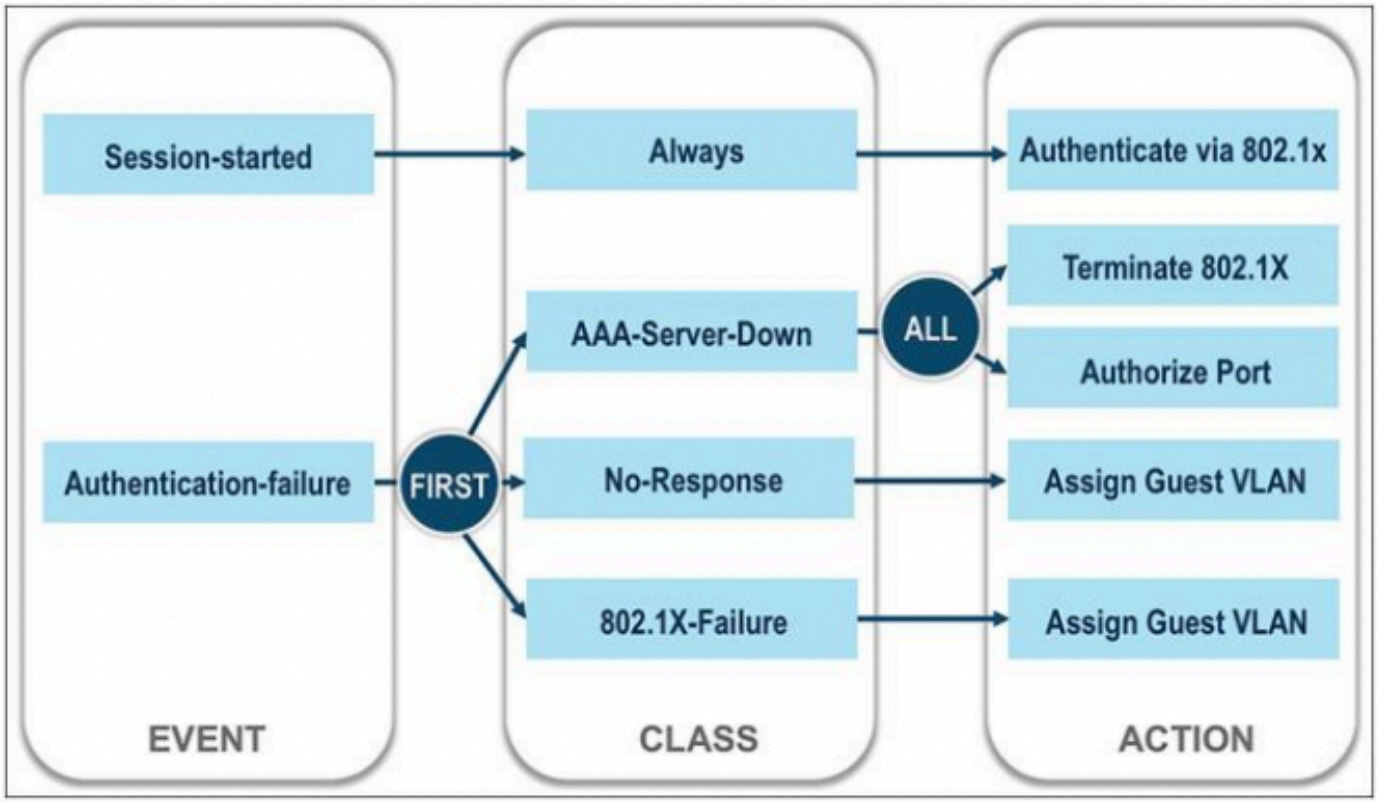
背景信息

身份控制策略定义访问会话管理器响应特定条件和终端事件执行的操作。使用一致的策略语言，可以将各种系统操作、条件和事件组合以形成这些策略。

控制策略应用于接口，主要负责管理终端身份验证和激活会话服务。每个控制策略由一个或多个规则和决定如何评估这些规则的决策策略组成。

控制策略规则包括控制类（灵活的条件语句）、触发条件评估的事件以及一个或多个操作。在管理

员定义由特定事件触发的操作时，某些事件附带预定义的默认操作。

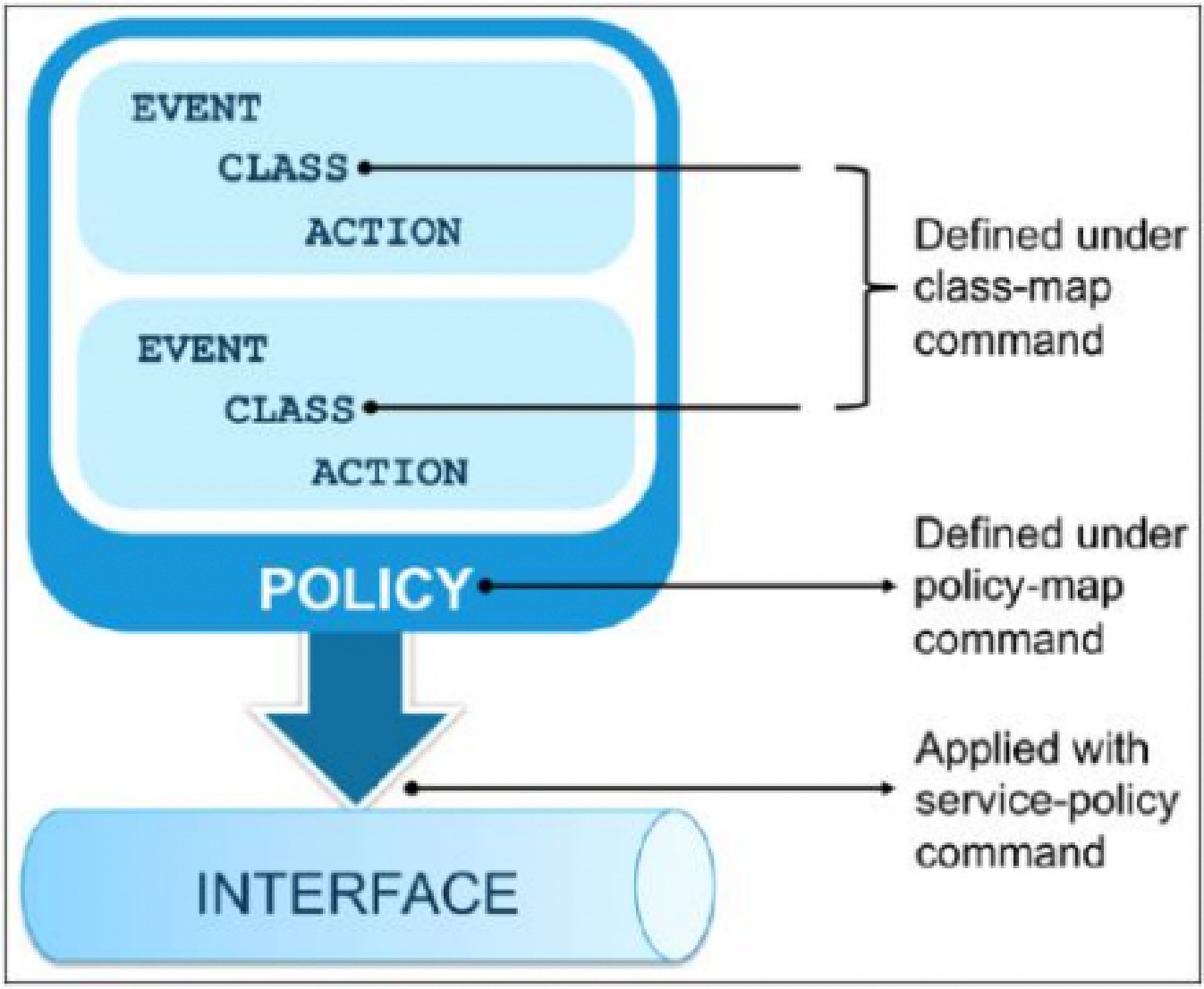


身份控制策略

身份控制策略配置概述

控制策略使用事件、条件和操作来定义系统行为。配置控制策略包括三个主要步骤：

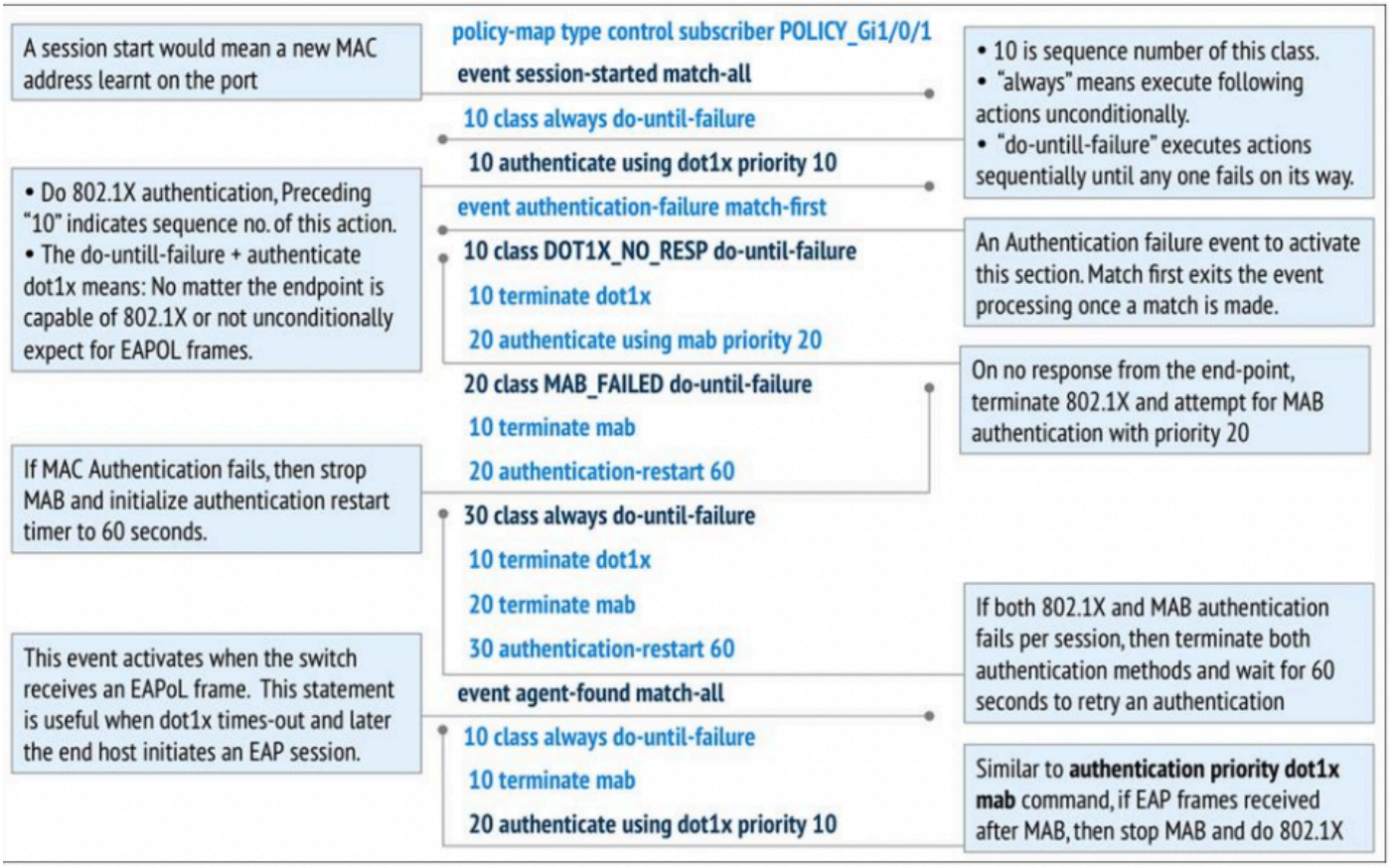
1. 创建控制类：
   控制类定义激活控制策略所需的条件。每个类可以有多个评估为true或false的条件。可以设置all、any或none条件是否必须为true才能将类视为true。或者，管理员可以使用没有条件并始终评估为true的默认类。
2. 创建控制策略：
   控制策略包含一个或多个规则。每个规则包括一个控制类、一个触发条件检查的事件和一个或多个操作。操作按顺序编号和执行。
3. 应用控制策略：
   最后，将控制策略应用到接口以激活它。



身份控制策略配置

authentication display new-style命令可将旧版配置转换为新样式。

switch#authentication display new-style



解释身份控制策略

配置

交换机配置

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

!

!

!

!

radius服务器ISE1

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

pac密钥xxxx@123

!

!

aaa group server radius ISE2

服务器名称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 |在POLICY_Gi1/0/45中

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类always do-to-failure

   10使用dot1x priority 10进行身份验证

event authentication-failure匹配优先

  5类DOT1X_FAILED do-until-failure

   10端接dot1x

20 authentication-restart 60

10类DOT1X_NO_RESP do-until-failure

10端接dot1x

20使用mab优先级进行身份验证20

20类MAB_FAILED do-until-failure

10终止mab

20 authentication-restart 60

40类always do-until-failure

10端接dot1x

20终止mab

30 authentication-restart 60

事件代理找到的匹配全部

10类always do-to-failure

10终止mab

20使用dot1x priority 10进行身份验证

event authentication-success match-all

10类always do-to-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

正在构建配置…

当前配置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 enforcement

dot1x pae authenticator

service-policy type control subscriber POLICY_Gi1/0/45

结束

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

!

cts authorization list ISE2

cts sxp enable

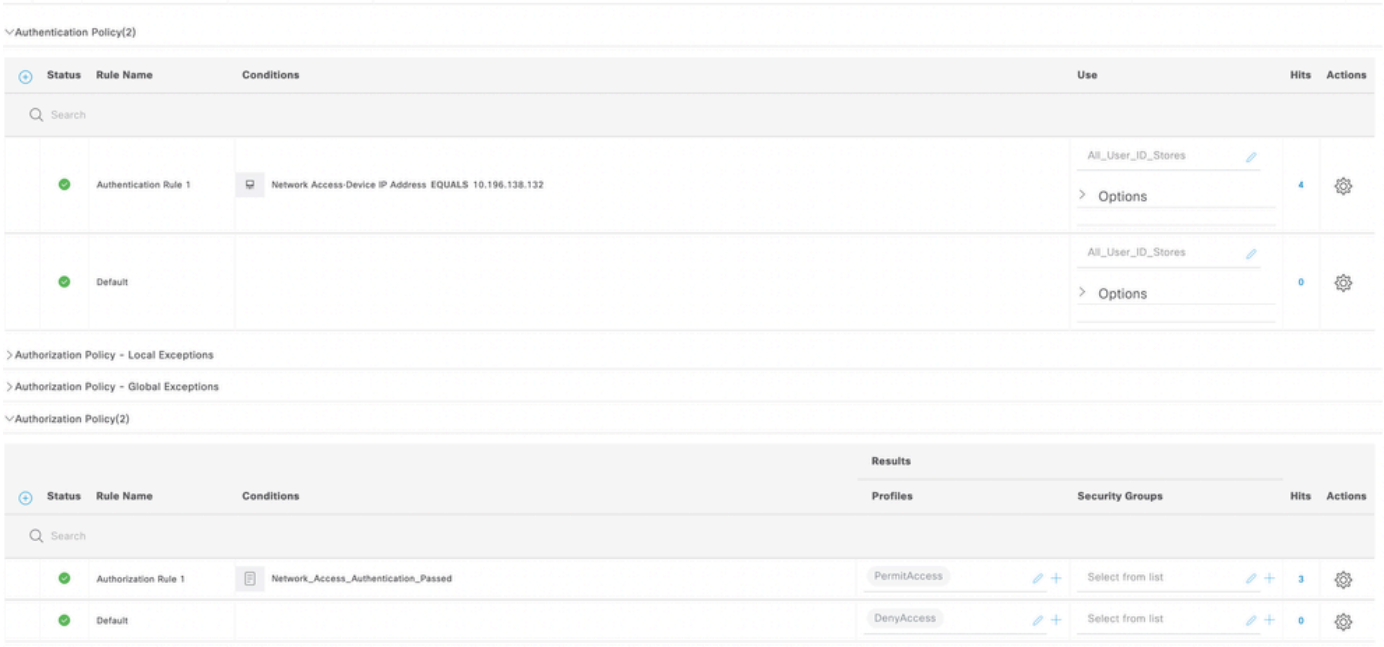
cts sxp connection 10.127.197.xxx password none mode peer speaker hold-time 0 0

cts sxp default source-ip 10.196.138.yyy

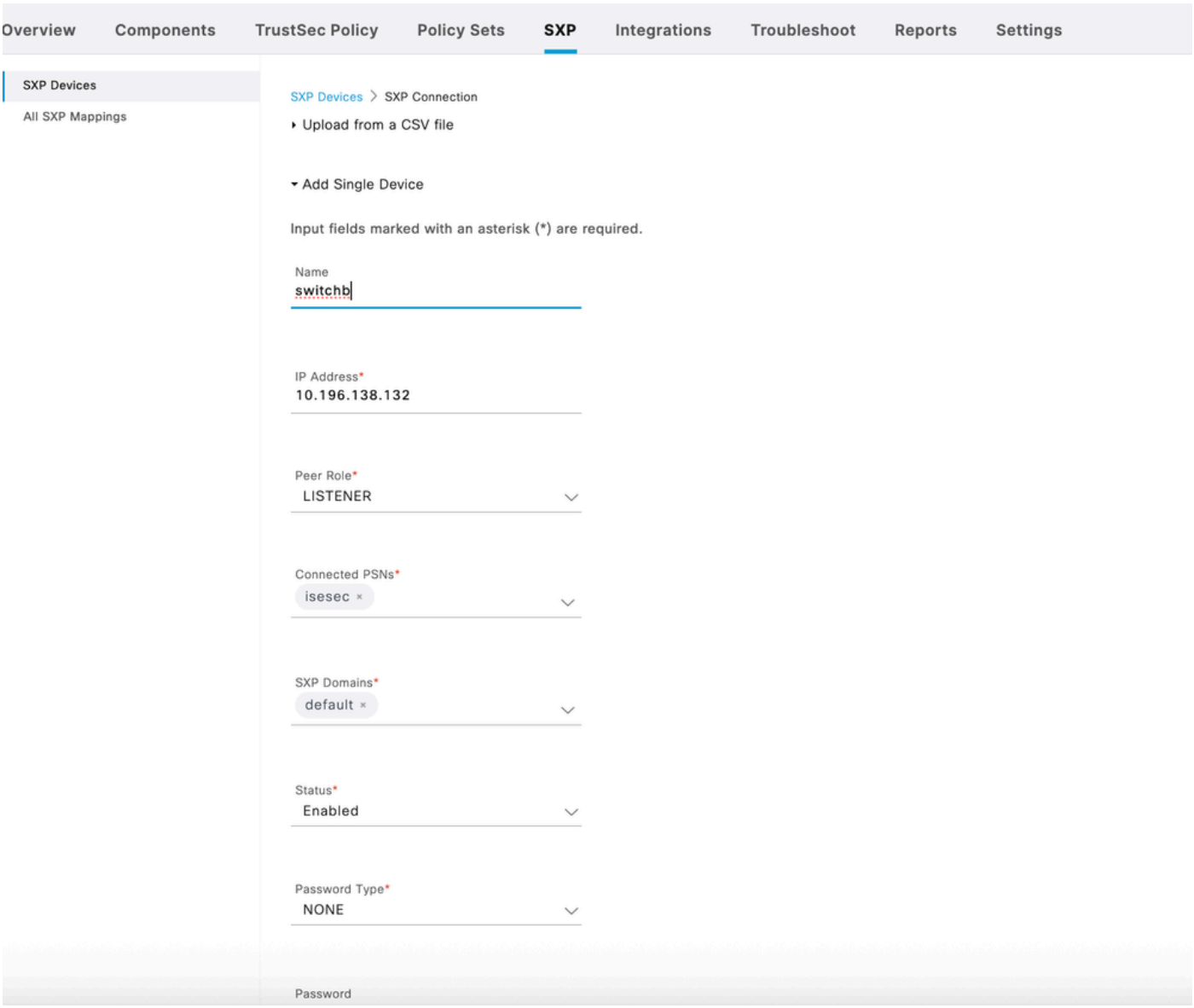
cts sxp default password xxxx@123

ISE 配置

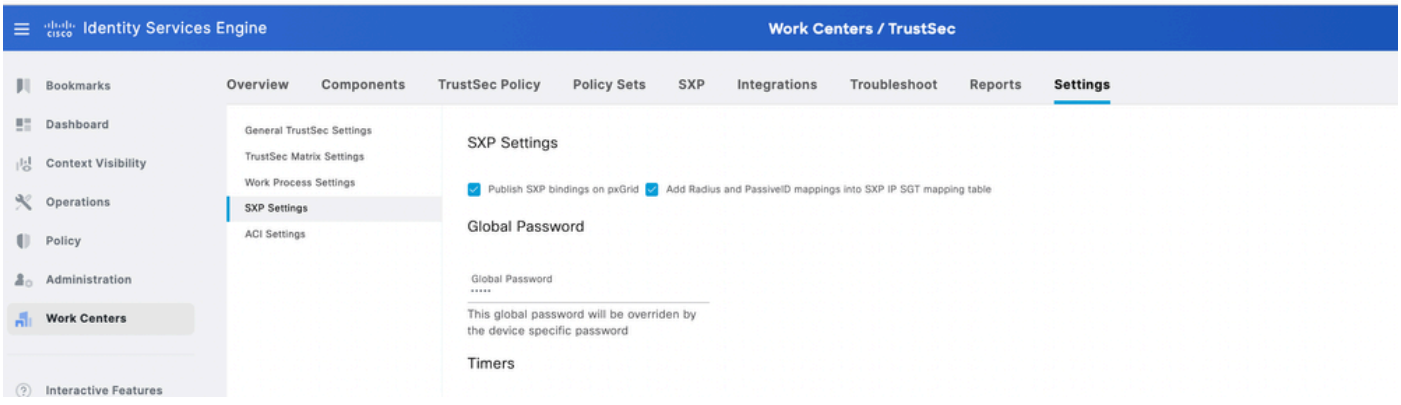
步骤 1：在ISE上创建身份验证和授权策略



步骤 2：在ISE上配置SXP设备



步骤 3：在SXP设置下配置全局密码



验证

WS-C3850-48F-E#show access-session interface gig1/0/45详细信息

接口: GigabitEthernet1/0/45

IIF-ID: 0x1A146F96

MAC 地址： b496.9126.decc

IPv6地址： 未知

IPv4地址： 未知

用户名： divya123

状态: 已授权

域名： 数据

操作主机模式： 单主机

操作控制目录： 两者

会话超时: 不适用

通用会话ID: 000000000000000B95163D98

客户会话ID: 未知

句柄： 0x6f000001

当前策略： POLICY_Gi1/0/45

本地策略：

服务模板：DEFAULT_LINKSEC_POLICY_MUST_SECURE（优先级150）

安全策略: 必须安全

安全状态: 链路不安全

服务器策略：

方法状态列表：

方法状态

dot1x验证成功

WS-C3850-48F-E#

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

SXP:启用

支持的最高版本：4

默认密码：设置

默认密钥链：未设置

默认密钥链名称：不能应用

默认源IP:10.196.138.yyy

连接重试打开时间：120秒

对帐期间：120秒

重试打开计时器正在运行

用于导出的对等序列遍历限制：未设置

导入的对等序列遍历限制：未设置

对等IP:10.127.197.xxx

源 IP：10.196.138.yyy

连接状态:开启

Conn版本:4

连接功能:IPv4-IPv6 — 子网

Conn保持时间:120 秒

本地模式:SXP监听程序

Connection inst# :1

TCP连接fd:1

TCP连接密码：none

保持计时器正在运行

自上次状态更改以来的持续时间：0:00:00:22(dd:hr:mm:sec)

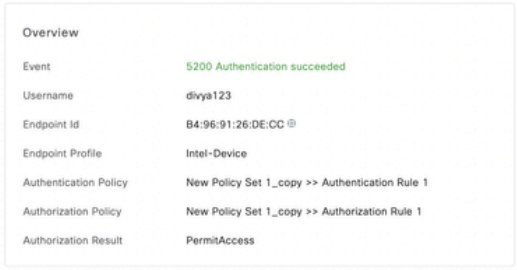
SXP连接总数= 1

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

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

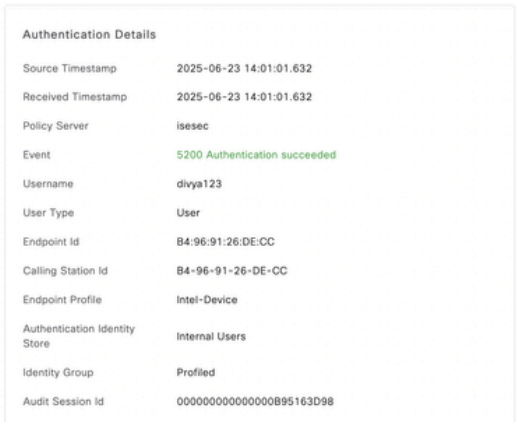
WS-C3850-48F-E(config)#

实时日志报告显示已应用的SGT标记:



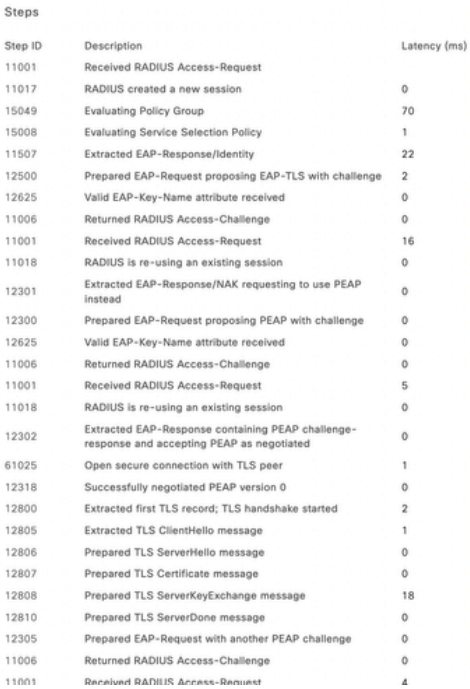
Overview

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



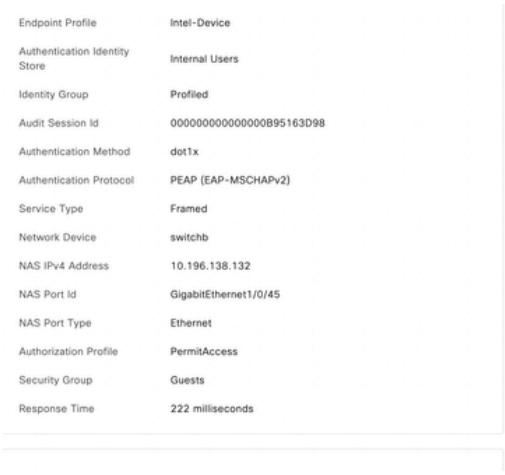
Authentication Details

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

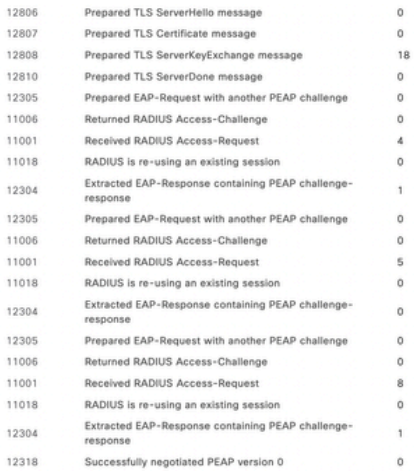


Steps

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

故障排除

在交换机上启用此调试以排除dot1x故障：

- debug dot1x all

日志说明

dot1x-packet:EAPOL产品激活密钥 — 版本：0x1类型：0x1 >>>>交换机收到的EAPoL数据包
dot1x-packet:篇幅：0x0000

dot1x-ev:[b496.9126.decc， Gig1/0/45]客户端被检测到，正在发送b496.9126.decc >>>> dot1x客户端的会话开始事件

dot1x-ev:[b496.9126.decc， Gig1/0/45] Dot1x authentication started for

0x26000007(b496.9126.decc)>>>> dot1x started

%AUTHMGR-5-START:在接口Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3上为客户端(b496.9126.decc)启动“dot1x”

dot1x-sm:[b496.9126.decc， Gig1/0/45]在客户端0x26000007上发布！EAP_RESTART />>>>请求客户端重新启动EAP进程

dot1x-sm:[b496.9126.decc， Gig1/0/45]在客户端0x26000007 >>>>>上发布RX_REQ，等待来自客户端的EAPoL数据包

dot1x-sm:[b496.9126.decc， Gig1/0/45]为0x26000007发布AUTH_START >>>>开始身份验证过程

dot1x-ev:[b496.9126.decc， Gig1/0/45]发送EAPOL数据包>>>>身份请求
dot1x-packet:EAPOL产品激活密钥发射机 — 版本：0x3类型：0x0
dot1x-packet:篇幅：0x005
dot1x-packet:EAP代码：0x1 id:0x1长度：0x005
dot1x-packet:type：0x1
dot1x-packet:[b496.9126.decc， Gig1/0/45] EAPOL数据包发送到客户端0x26000007

dot1x-ev:[Gig1/0/45]接收的pkt saddr =b496.9126.decc ,daddr = 0180.c200.0003,pae-ether-type = 888e.0100.000a
dot1x-packet:EAPOL产品激活密钥 — 版本：0x1类型：0x0 //身份响应
dot1x-packet:篇幅：0x000A

dot1x-sm:[b496.9126.decc， Gig1/0/45]为0x26000007发布EAPOL_EAP >>>>收到的EAPoL数据包（EAP响应），正在准备对服务器的请求

dot1x-sm:[b496.9126.decc， Gig1/0/45]发布EAP_REQ for 0x26000007 >>>>已收到服务器响应，正在准备EAP请求

dot1x-ev:[b496.9126.decc， Gig1/0/45]正在发送EAPOL数据包
dot1x-packet:EAPOL产品激活密钥发射机 — 版本：0x3类型：0x0
dot1x-packet:篇幅：0006
dot1x-packet:EAP代码：0x1 id:0xE5长度：0006
dot1x-packet:type：0xD
dot1x-packet:[b496.9126.decc， Gig1/0/45] EAPOL数据包已发送到客户端0x26000007 >>>>
EAP请求已发出

dot1x-ev:[Gig1/0/45]接收的pkt saddr =b496.9126.decc ,daddr = 0180.c200.0003,pae-ether-type = 888e.0100.0006 //EAP响应已接收
dot1x-packet:EAPOL产品激活密钥 — 版本：0x1类型：0x0
dot1x-packet:篇幅：0006
||
||
||
||此处发生许多EAPOL-EAP和EAP_REQ事件，因为交换机和客户端之间交换了许多信息
||如果在此之后发生的事件，则需要检查计时器和现在发送的信息

||
||
||
dot1x-packet:[b496.9126.decc， Gig1/0/45]从服务器收到EAP Success >>>> EAP Success

dot1x-sm:[b496.9126.decc， Gig1/0/45]为0x26000007发布EAP_SUCCESS >>>>发布EAP成功事件

dot1x-sm:[b496.9126.decc，Gig1/0/45]在客户端0x26000007上发布AUTH_SUCCESS >>>>发布身份验证成功

%DOT1X-5-SUCCESS:接口Gig1/0/45上的客户端(b496.9126.decc)身份验证成功AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-packet:[b496.9126.decc， Gig1/0/45] EAP Key data detected adding to attribute list >>>>服务器检测到的其他密钥数据

%AUTHMGR-5-SUCCESS:接口Gig1/0/45上的客户端(b496.9126.decc)授权成功AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-ev:[b496.9126.decc， Gig1/0/45]已收到客户端的授权成功 0x26000007(b496.9126.decc)>>>>授权成功

dot1x-ev:[b496.9126.decc， Gig1/0/45]发送EAPOL数据包>>>>向客户端发送EAP成功
dot1x-packet:EAPOL产品激活密钥发射机 — 版本：0x3类型：0x0
dot1x-packet:篇幅：0x0004
dot1x-packet:EAP代码：0x3 id:0xED长度：0x0004
dot1x-packet:[b496.9126.decc， Gig1/0/45] EAPOL数据包发送到客户端0x26000007

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。