تكوين المحول مع SXP و IBNS 2.0 للشبكات المستندة إلى الهوية

المحتويات

المقدمة

يصف هذا المستند إجراءات تكوين محولات Cisco باستخدام SXP و IBNS 2.0 للشبكات المستندة إلى الهوية.

المتطلبات الأساسية

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Identity Services Engine (ISE)، الإصدار 3.3 Patch 4
- المحول Cisco Catalyst Switch 3850

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

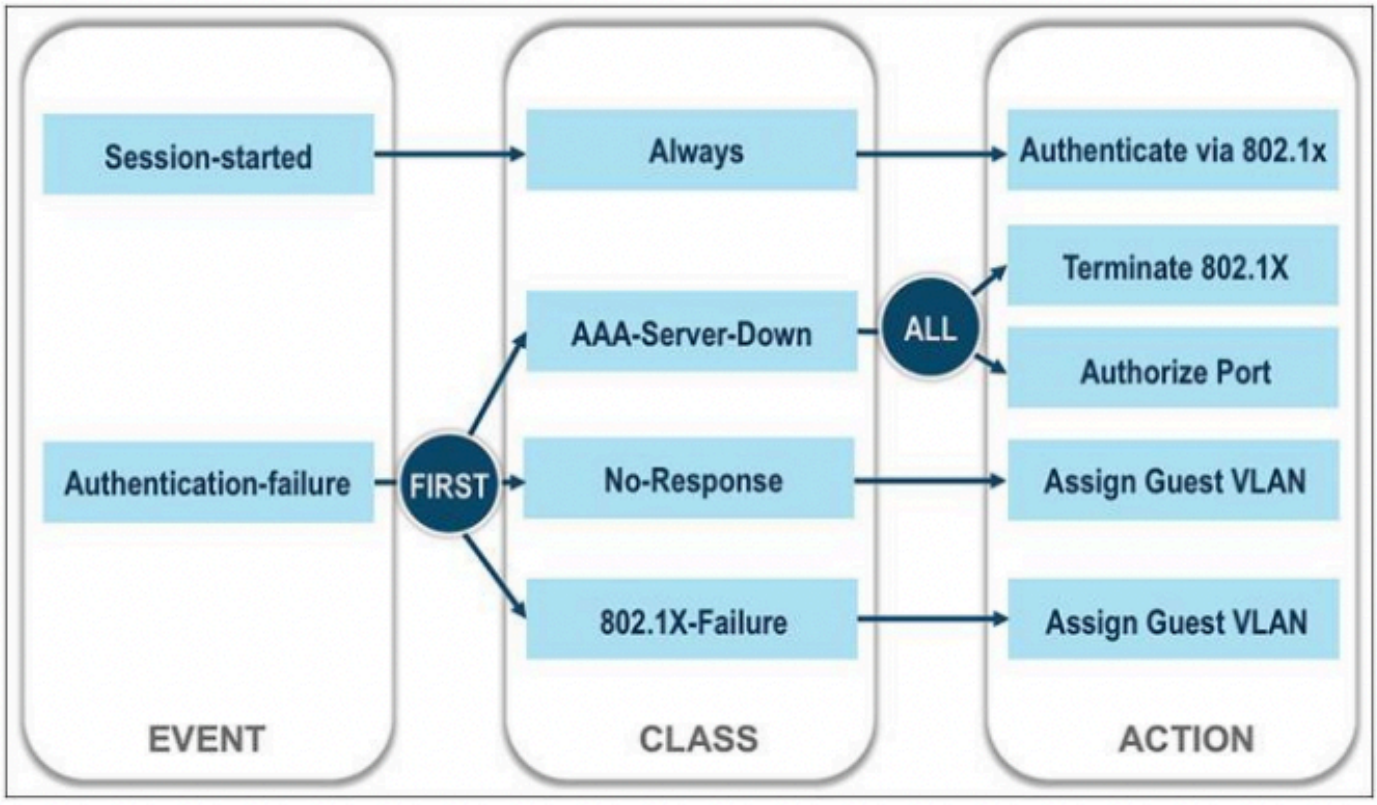
معلومات أساسية

تحدد سياسات التحكم في الهوية الإجراءات التي ينفذها مدير جلسة الوصول إستجابة لظروف محددة وأحداث نقطة النهاية. وباستخدام لغة سياسية متناسقة، يمكن الجمع بين

إجراءات النظام المختلفة وظروف وأحداث معينة لتشكيل هذه السياسات.

يتم تطبيق سياسات التحكم على الواجهات وتكون مسؤولة بشكل أساسي عن إدارة مصادقة نقطة النهاية وتنشيط الخدمات على الجلسات. تتكون كل سياسة تحكم من قاعدة واحدة أو أكثر واستراتيجية قرار تحدد كيفية تقييم تلك القواعد.

تتضمن قاعدة سياسة التحكم فئة تحكم (بيان شرط مرن)، وحدث يشغل تقييم الشرط، وإجراء واحد أو أكثر. بينما يحدد المسؤولون الإجراءات التي يتم تشغيلها بواسطة أحداث معينة، تأتي بعض الأحداث مع إجراءات افتراضية محددة مسبقا.



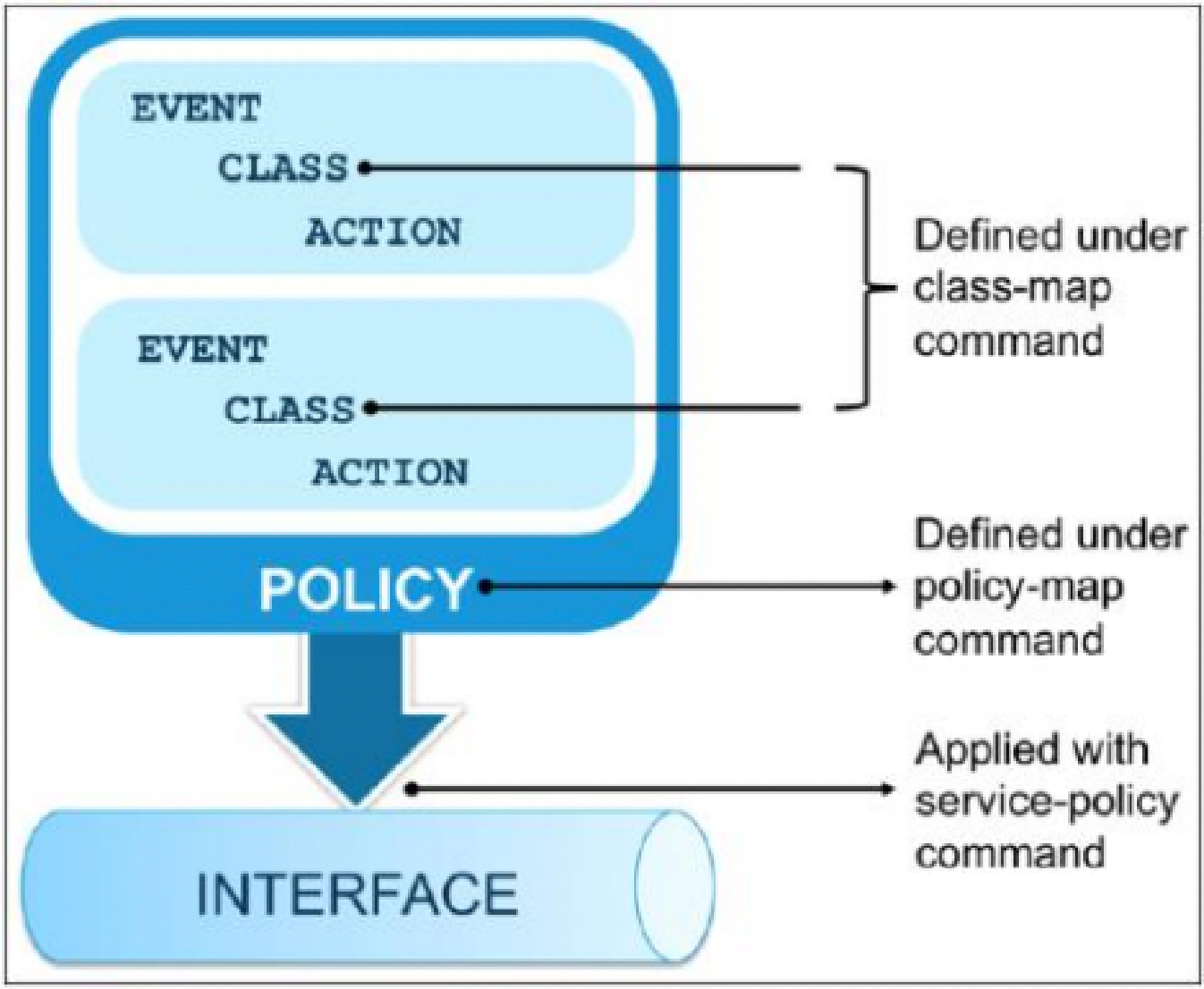
سياسة التحكم بالهوية

نظرة عامة على تكوين سياسة التحكم في الهوية

تحدد سياسات التحكم سلوك النظام باستخدام حدث، وشرط، وإجراء. يتضمن تكوين سياسة تحكم ثلاث خطوات رئيسية:

1. إنشاء فئات التحكم:
   تحدد فئة التحكم الشروط المطلوبة لتنشيط نهج التحكم. يمكن أن يكون لكل فئة شروط متعددة يتم تقييمها على أنها صحيحة أو خاطئة. يمكنك تعيين ما إذا كان كل أو أي أو ال يجب أن يكون أي من الشروط صحيحا لكي يتم إعتبار الفئة صحيحة. بدلا من ذلك، يمكن للمسؤولين إستخدام فئة افتراضية ال تتضمن شروط ويتم تقييمها دائما على أنها صحيحة.
2. إنشاء نهج التحكم:
   يحتوي نهج التحكم على قاعدة واحدة أو أكثر. تتضمن كل قاعدة فئة تحكم وحدث يؤدي إلى تشغيل التحقق من الشرط وإجراء واحد أو أكثر. يتم ترقيم الإجراءات وتنفيذها بالترتيب.

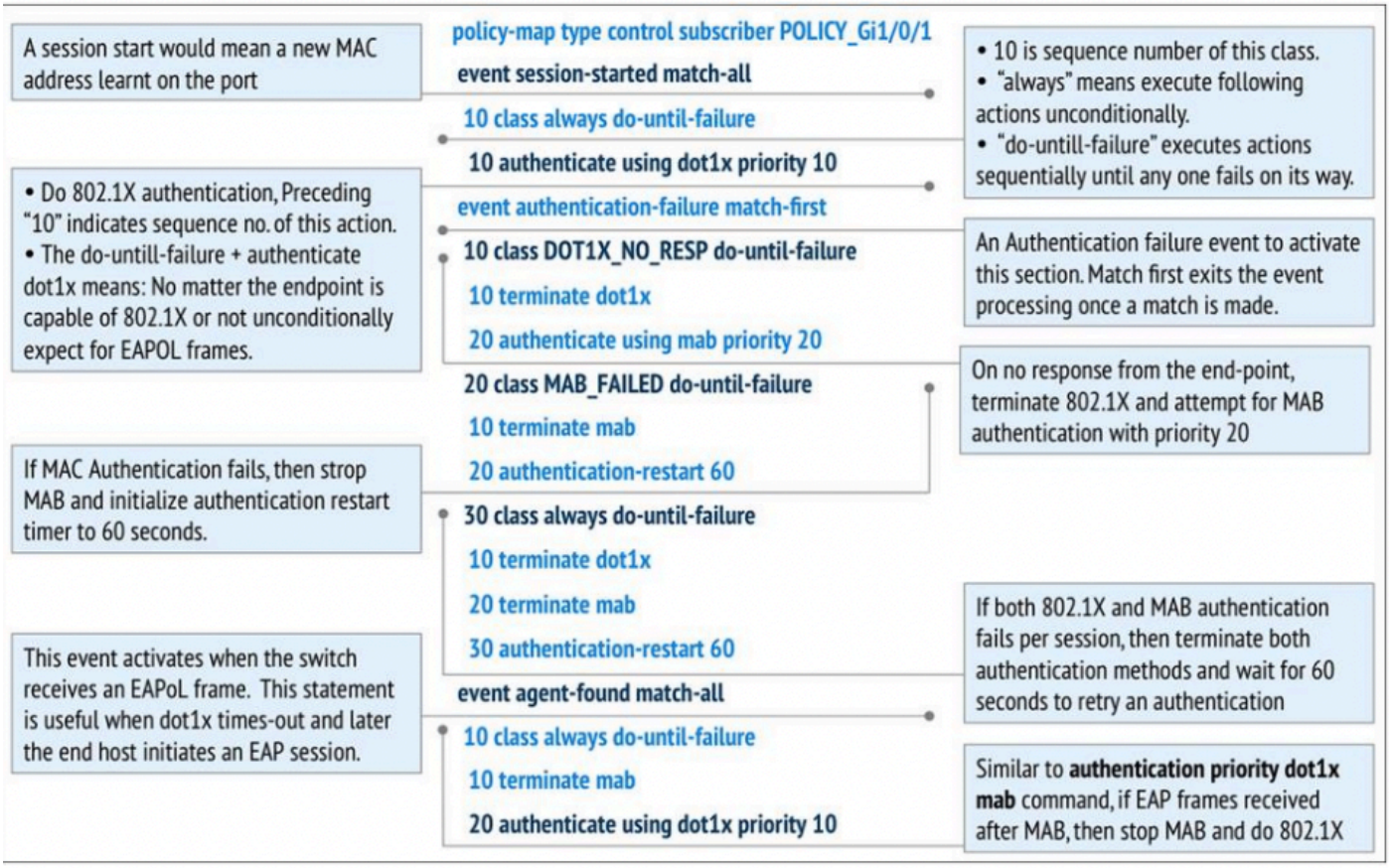
3. تطبيق نهج التحكم:
أخيرا، قم بتطبيق نهج التحكم على واجهة لتنشيطه.



تكوين نهج التحكم بالهوية

يحول أمر عرض نمط جديد للمصادقة التكوينات القديمة إلى نمط جديد.

switch#authentication عرض نمط جديد



تفسير سياسة التحكم بالهوية

التكوين

تكوين المبدّل

WS-C3850-48F-E#show يركض AAA

!

نقطة مصادقة AAA1x نصف قطر مجموعة افتراضية محلي

مجموعة AAA الافتراضية لنصف قطر محلي لشبكة تفويض AAA

كلمة مرور مسؤول username 0 xxxx

!

!

!

!

ISE1 لخادم RADIUS

عنوان IPv4 10.127.197.xxx auth-port 1812 acct-port 1813

مفتاح مسوغات الوصول المحمي xxxx@123

!

!

AAA مجموعة لدان radius ISE2

اسم الخادم ISE1

!

!

!

!

aaa new-model

AAA جلسة-id مشترك

!

الملف الديناميكي لنص قطر خادم AAA

العميل 10.127.197.xxx server-key xxxx@123

dot1x system-auth-control

!

تشغيل WS-C3850-48F-E#show | في POLICY_GI1/0/45

Policy-Map Type Control Subscriber Policy_Gi1/0/45

سياسة المشترك في التحكم من نوع الخدمة-السياسة_Gi1/0/45

تشغيل WS-C3850-48F-E#show | sec policy_gi1/0/45

Policy-Map Type Control Subscriber Policy_Gi1/0/45

جلسة عمل الحدث - تم عدم مطابقة الكل

الفئة 10 زيادة حتى الفشل

10 مصادقة باستخدام dot1x priority 10

مصادقة الحدث-الفشل المطابق الأول

5 class DOT1X_FAILED do-until-failure

10 إنهاء dot1x

20 رايعملل اقفو 60 ةقداصملا ليغشت ةداعإ

10 class DOT1X_NO_RESP do-until-failure

10 ءاهنإ dot1x

20 ةيولوألا مادختساب ةقداصم MAB 20

20 class MAB_FAILED Do-to-Failure

10 ءاهنإ بام

20 رايعملل اقفو 60 ةقداصملا ليغشت ةداعإ

40 لشفلا ىتح لعف امئاد فص

10 ءاهنإ dot1x

20 ءاهنإ بام

30 ةقداصملا ليغشت ةداعإ 60

مت العثور على لماع الحدث match-all

10 ةئفلا امئاد ىتح لشفلا

10 ءاهنإ بام

20 مادختساب ةقداصم dot1x priority 10

مصادقة الحدث - حاجن الملطابقة الكل

10 ةئفلا امئاد ىتح لشفلا

10 طيشنت بلاق الخدمة default_linksec_policy_must_secure

سياسة المشترك في التحكم نم عون الخدمة-السياسة_Gi1/0/45

WS-C3850-48F-E#show Run Interface gig1/0/45

جاري إنشاء التكوين...

التكوين الحالي : 303 بايت

!

ةهجاو GigabitEthernet1/0/45

switchport access vlan 503

الوصول إلى وضع Switchport

مضيف الوضع الأحادي لجلسة الوصول

إغلاق جلسة عمل الوصول

التحكم التلقائي في المنفذ ل Access-Session

مابا

ال يوجد تطبيق قائم على الأدوار ل CTS

dot1x Pae Authenticator

سياسة المشترك في التحكم من نوع الخدمة-السياسة_Gi1/0/45

نهاية

WS-C3850-48F-E#show تشغيل CTS

!

ISE2 لقائمة تفويض CTS

تمكين CTS sxp

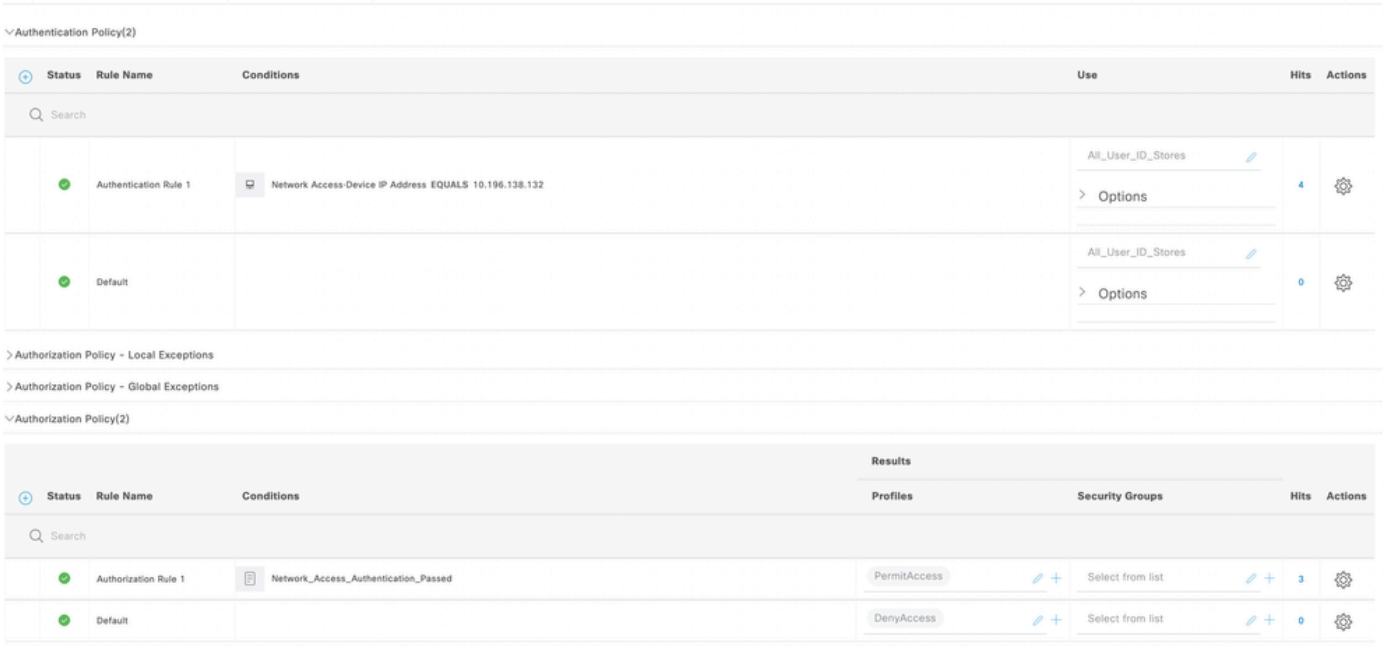
اتصال CTS SXP 10.127.197.xxx كلمة مرور ال يوجد وضع ووقت انتظار مكبر صوت النظير 0

cts sxp default source-ip 10.196.138.yy

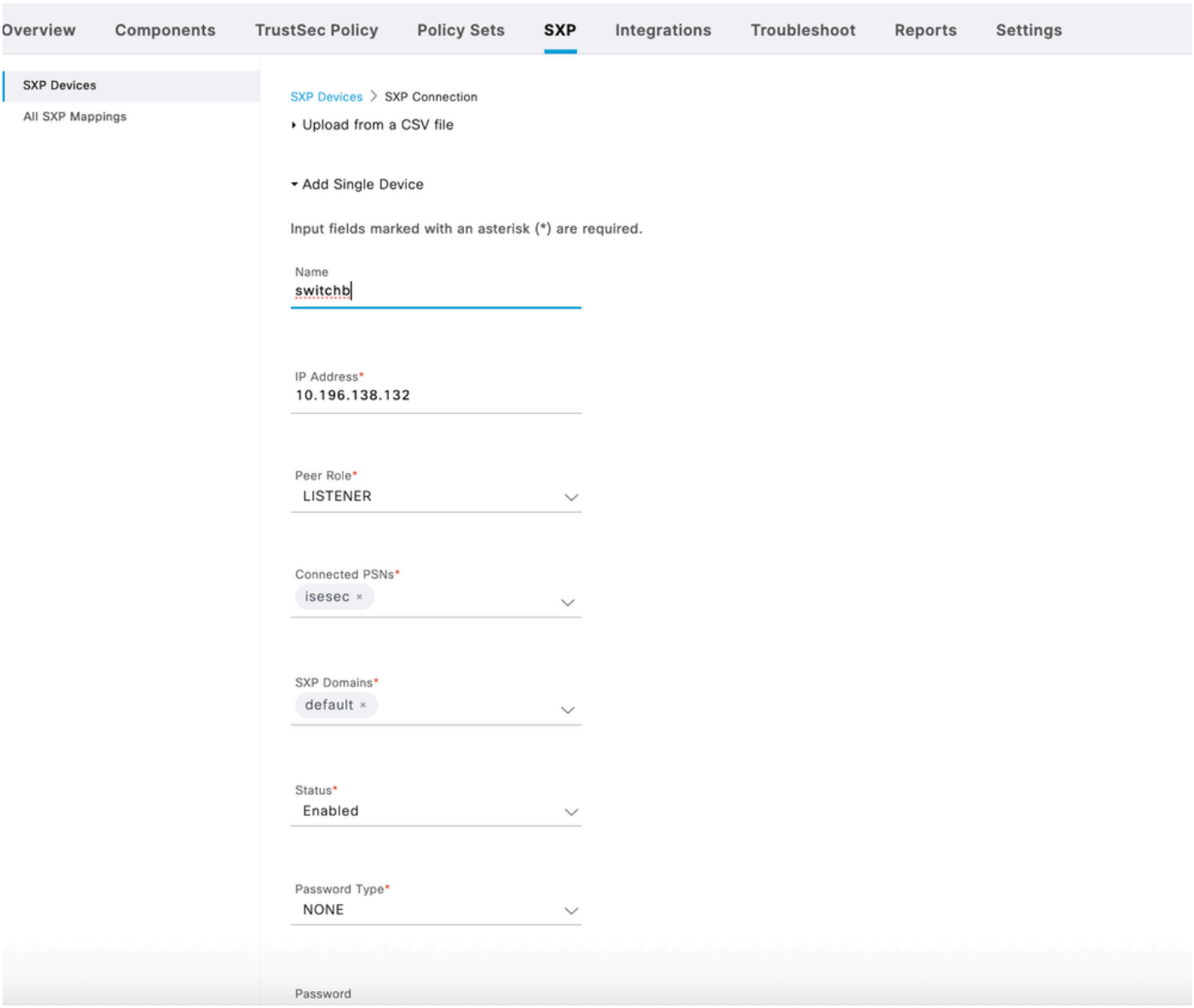
كلمة المرور الافتراضية ل CTS sxp xxxx@123

تكوين ISE

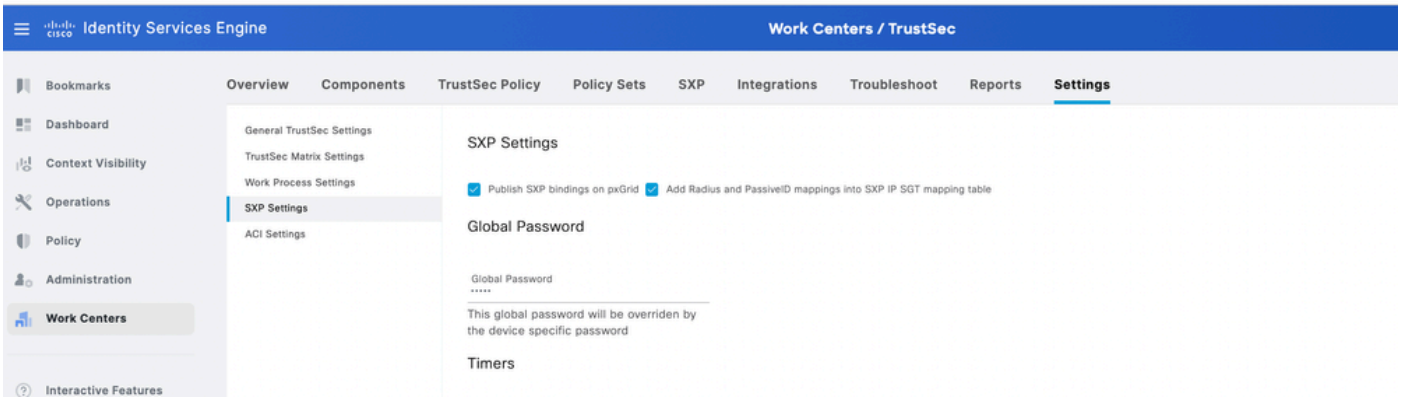
الخطوة 1: إنشاء سياسات المصادقة والتفويض على ISE



الخطوة 2: تكوين جهاز SXP على ISE



الخطوة 3: تكوين كلمة المرور العامة تحت إعدادات SXP



التحقق من الصحة

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

الواجهة: GigabitEthernet 1/0/45

IIF-ID: 0x1A146F96

عنوان MAC: b496.9126.decc

عنوان IPv6: غير معروف

عنوان IPv4: غير معروف

اسم المستخدم: ديفاي 123

الحالة: مُفوض

المجال: البيانات

وضع مضيف Oper: مضيف واحد

مفاتيح التحكم DIR: كلاهما

مهلة انتهاء الجلسة: غير متوفر

معرف الجلسة المشتركة: 0000000000000b95163d98

معرف جلسة العمل: غير معروف

المقبض: 0x6f00001

النهج الحالي: Policy_Gi1/0/45

السياسات المحلية:

قالب الخدمة: DEFAULT_LINKSEC_POLICY_MUST_SECURE (الأولوية 150)

نهج الأمان: يجب تأمين

حالة الأمان: إرتباط غير آمن

نهج الخادم:

قائمة حالة الأسلوب:

حالة الأسلوب

dot1x Authc نجاح

WS-C3850-48F-E#

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

SXP : ممكن

أعلى إصدار مدعوم: 4

كلمة المرور الافتراضية : مجموعة

سلسلة المفاتيح الافتراضية: غير معين

اسم سلسلة المفاتيح الافتراضية: غير قابل للتطبيق

مصدر IP الافتراضي: 10,196,138,yy

الفترة المفتوحة لإعادة محاولة الاتصال: 120 ثوان

تسوية الفترة: 120 ثوان

إعادة محاولة تشغيل المؤقت المفتوح

حد إجتياز تسلسل النظير للتصدير: غير معين

حد إجتياز تسلسل النظير للاستيراد: غير معين

—

IP النظير : 10,127,197,xxx

IP المصدر : 10,196,138,yy

حالة المخالفة : تشغيل

إصدار المخطوط : 4

إمكانية CONN : الشبكة الفرعية IPv4-IPv6-Subnet

وقت الانتظار : 120 ثانية

الوضع المحلي : مستمع SXP

رقم تعريف الاتصال : 1

قوافق TCP على : 1

كلمة مرور توافق TCP: none

المؤقت الاحتجاز قيد التشغيل

المدة منذ آخر تغيير للحالة: 0:00:00:22 (dd:hr:mm:sec)

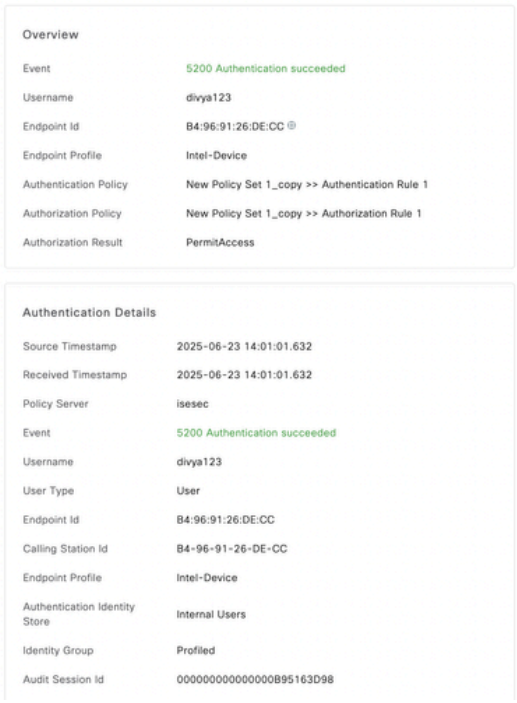
إجمالي num إتصالات SXP = 1

0xFF8CBFC090 VRF:، fd: 1، IP النظير: 10,127,197,xxx

cdbp:0xFF8CBFC090 <10.127.197.145، 10.196.138.yy> tableid:0x0

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

يظهر تقرير السجل النشط تطبيق رقيب العلامة Guest:



Overview

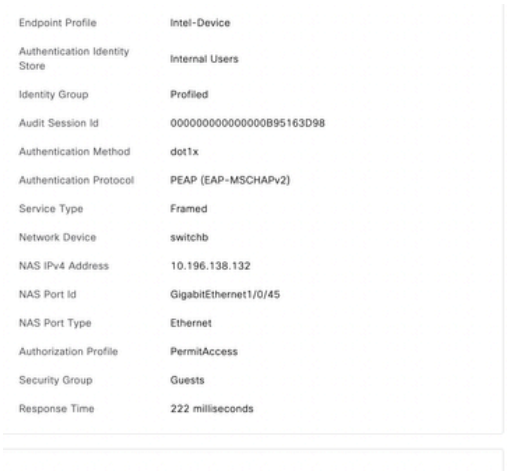
Event	5200 Authentication succeeded
Username	divya123
Endpoint Id	B4:96:91:26:DE:CC
Endpoint Profile	Intel-Device
Authentication Policy	New Policy Set 1_copy >> Authentication Rule 1
Authorization Policy	New Policy Set 1_copy >> Authorization Rule 1
Authorization Result	PermitAccess

Authentication Details

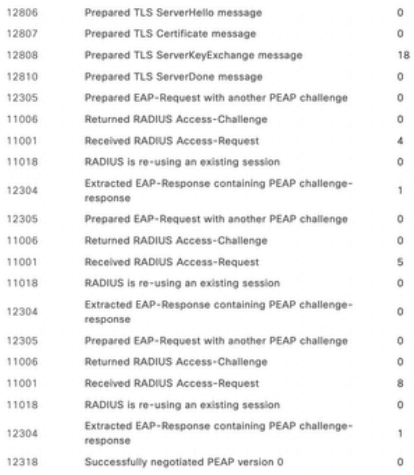
Source Timestamp	2025-06-23 14:01:01.632
Received Timestamp	2025-06-23 14:01:01.632
Policy Server	isesec
Event	5200 Authentication succeeded
Username	divya123
User Type	User
Endpoint Id	B4:96:91:26:DE:CC
Calling Station Id	B4-96-91-26-DE-CC
Endpoint Profile	Intel-Device
Authentication Identity Store	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

استكشاف الأخطاء وإصلاحها

يمكنك هذا debug على المفاتيح أن يتحرى dot1x إصدار:

- debug dot1x all

تسجيل الشرح

dot1x-packet:EAPOL pak rx - الإصدار: نوع 0x1: حزمة 0x1 >>> EAPoL المستلمة بواسطة المحول
dot1x-packet: الطول: 0x000

dot1x-ev:[b496.9126.decc، Gig1/0/45] زبون كشف، يرسل حدث بدء جلسة عمل ل
b496.9126.decc >>> dot1x زبون كشف

dot1x-ev:[b496.9126.decc، gig1/0/45] dot1x بدأت المصادقة ل 0x26000007
(b496.9126.decc)>>>> dot1x بدأت

%AUTHMGR-5-START: بداية 'dot1x' للعميل (b496.9126.decc) على قارن gig1/0/45
AuditSessionID 0A6A258E00003500C9CFC3

dot1x-sm:[b496.9126.decc، gig1/0/45] نشر !EAP_RESTART على العميل 0x2600007 /<<< طلب من العميل إعادة تشغيل خيارات EAP

dot1x-sm:[b496.9126.decc، Gig1/0/45] تم نشر RX_REQ على العميل 0x2600007>> في انتظار حزمة EAPoL من العميل

dot1x-sm:[b496.9126.decc، gig1/0/45] ترحيل AUTH_START ل 0x2600007>>> بدء عملية المصادقة

dot1x-ev:[b496.9126.decc، gig1/0/45] إرسال حزمة EAPOL >> طلب الهوية
dot1x-packet:EAPOL pak Tx - الإصدار: نوع 0x3: 0x0
dot1x-packet: الطول: 0x0005
dot1x-packet:رمز EAP: معرف 0x1: طول 0x1: 0x0005
dot1x-packet: النوع: 0x1
dot1x-packet:[b496.9126.decc، gig1/0/45] حزمة EAPOL مرسلة إلى العميل 0x2600007

dot1x-ev:[Gig1/0/45] تم استلام pkt saddr =b496.9126.decc، daddr = 0180.c200.003، pae-ether-type = 888e.0100.000a
dot1x-packet:EAPOL pak rx - الإصدار: نوع 0x1: 0x0 // استجابة الهوية
dot1x-packet: الطول: 0x000a

dot1x-sm:[b496.9126.decc، Gig1/0/45] تم الآن ترحيل EAPOL_EAP ل 0x2600007>>> EAPoL Packet(استجابة EAP) التي تم تلقيها، يتم إعداد طلب إلى الخادم

dot1x-sm:[b496.9126.decc، gig1/0/45] يتم الآن إعداد طلب EAP_REQ ل 0x2600007>> استجابة الخادم، ويتم إعداد طلب EAP

dot1x-ev:[b496.9126.decc، gig1/0/45] إرسال حزمة EAPOL للخارج
dot1x-packet:EAPOL pak Tx - الإصدار: نوع 0x3: 0x0
dot1x-packet: الطول: 0x0006
dot1x-packet:رمز EAP: معرف 0x1: 0xE5 الطول: 0x0006
dot1x-packet: النوع: 0xD
dot1x-packet:[b496.9126.decc، gig1/0/45] حزمة EAPOL مرسلة إلى العميل 0x2600007<<< تم إرسال طلب EAP

dot1x-ev:[Gig1/0/45] تم استلام PKT saddr =b496.9126.decc، daddr = 0180.c200.003، pae-ether-type = 888e.0100.006 //EAP تم تلقي استجابة
dot1x-packet:EAPOL pak rx - الإصدار: نوع 0x1: 0x0
dot1x-packet: الطول: 0x0006
||
||
||

|| انه الكثير من أحداث EAPOL-EAP و EAP_REQ حيث يتم تبادل الكثير من المعلومات بين المحول والعميل
|| إذا لم تتبع الأحداث بعد ذلك، فيجب التحقق من وحدات التوقيت والمعلومات المرسلة حتى الآن
||
||
||
dot1x-packet:[b496.9126.decc، gig1/0/45] تلقى نجاح EAP >>>> EAP Success من الخادم

dot1x-sm:[b496.9126.decc، gig1/0/45] نشر EAP_SUCCESS ل 0x2600007>>> نشر حدث نجاح نشر EAP

dot1x-sm:[b496.9126.decc،gig1/0/45] يتم الآن ترحيل AUTH_SUCCESS على العميل 0x2600007>> يتم نشر نجاح المصادقة

%DOT1X-5-SUCCESS: تمت المصادقة بنجاح للعميل (b496.9126.decc) على الواجهة gig1/0/45 AuditSessionID 0A6A258E00003500C9CFC3

dot1x-packet:[b496.9126.decc، gig1/0/45] كشف بيانات مفتاح EAP عن إضافة إلى قائمة السمات >>> بيانات المفتاح الإضافية التي تم الكشف عنها بواسطة الخادم

%AUTHMGR-5-SUCCESS: نجح التفويض للعميل (b496.9126.decc) على الواجهة gig1/0/45 AuditSessionID 0A6A258E00003500C9CFC3

dot1x-ev:[b496.9126.decc، gig1/0/45] تم تلقي Authz Success للعميل 0x2600007 (b496.9126.decc) >> نجاح التفويض

dot1x-ev:[b496.9126.decc، gig1/0/45] إرسال حزمة EAPOL >> إرسال نجاح EAP إلى العميل
dot1x-packet:EAPOL pak Tx - الإصدار: 0x3 :نوع 0x0
dot1x-packet: الطول: 0x0004
dot1x-packet:رمز EAP: 0x3 :معرف 0xED :طول 0x0004
dot1x-packet:[b496.9126.decc، gig1/0/45] حزمة EAPOL مرسلة إلى العميل 0x2600007

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).