تكوين نفق IPsec بين Cisco WLC و ISE

المحتويات

المقدمة

يصف هذا المستند تكوين أمان بروتوكول الإنترنت (IPsec) بين 9800 WLC وخادم ISE لتأمين اتصال RADIUS و TACACS.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- محرك خدمات كشف الهوية (ISE)
- تكوين Cisco IOS® XE WLC
- مفاهيم IPSec العامة
- مفاهيم RADIUS العامة
- المفاهيم العامة ل TACACS

المكونات المستخدمة

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

- وحدة التحكم اللاسلكية: C9800-40-K9 ريك 17.09.04a
- Cisco ISE: برنامج تصحيح الإصدار 3 قيد التشغيل 4
- المحول: 9200-L-24P

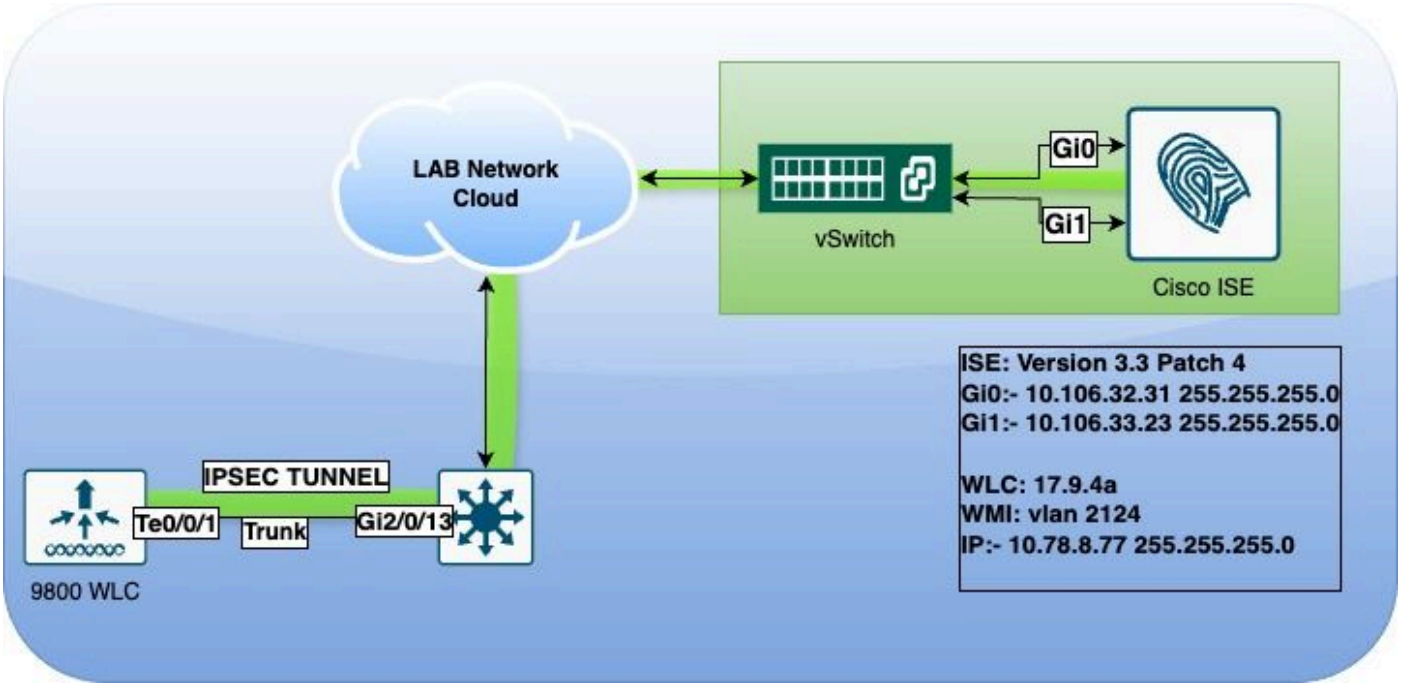
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

IPsec هو إطار للمعايير المفتوحة تم تطويره بواسطة IETF. وهو يوفر الأمان لنقل المعلومات الحساسة عبر الشبكات غير المحمية مثل الإنترنت. يعمل IPsec في طبقة الشبكة، مما يحمي حزم IP ويصادق عليها بين أجهزة IPsec المشاركة (النظراء)، مثل موجهات Cisco. أستخدم IPsec بين وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) طراز 9800 وخادم ISE لتأمين اتصال RADIUS و TACACS.

التكوين

الرسم التخطيطي للشبكة



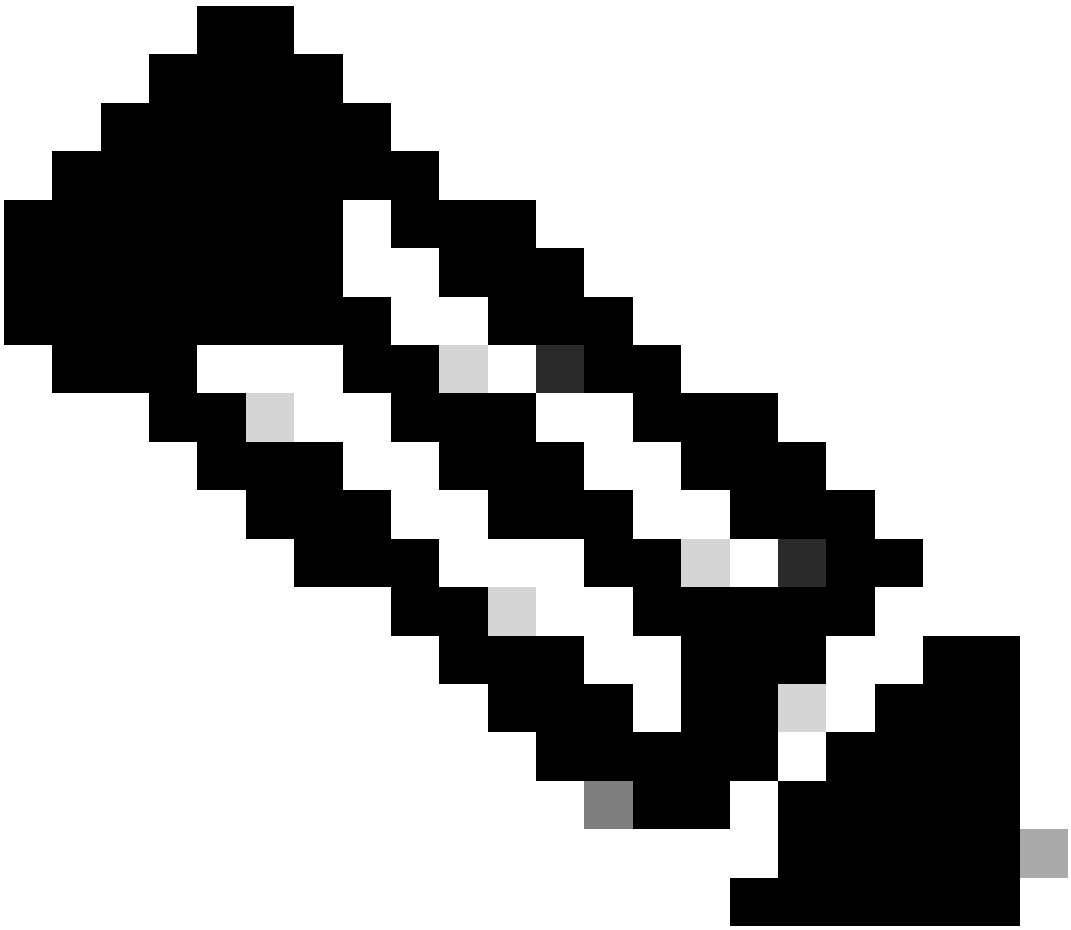
الرسم التخطيطي للشبكة

تكوين ISE

يدعم Cisco ISE بروتوكول IPsec في أوضاع الأنفاق والنقل. عند تمكين IPsec على واجهة Cisco ISE وتكوين الأقران، يتم إنشاء نفق IPsec بين Cisco ISE و NAD لتأمين الاتصال.

يمكنك تحديد مفتاح مشترك مسبقا وأ إستخدام شهادات X.509 لمصادقة IPsec. يمكن تمكين IPsec على إيثرنت جيجابت 1 من خلال واجهات Gigabit Ethernet 5.

ISE الإصدارات 2.2 من Cisco والإصدارات الأحدث من IPsec.



ملاحظة: تأكد من أن لديك ترخيص Cisco ISE Essentials.

إضافة جهاز وصول إلى الشبكة (NAD) بعنوان خاص إلى IP في نافذة أجهزة الشبكة.

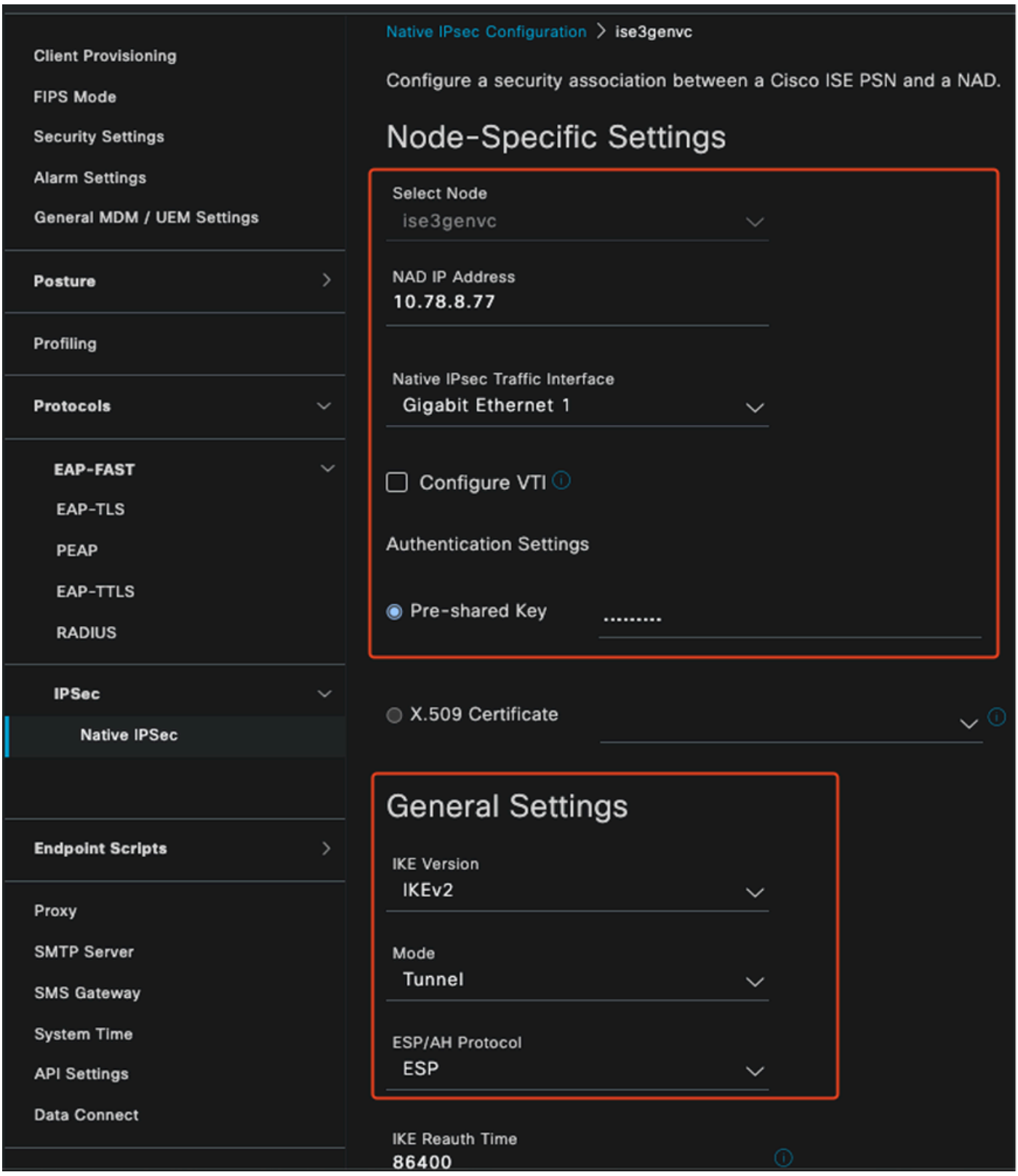
في واجهة المستخدم الرسومية Cisco ISE، انتقل عبر الإدارة وانتقل إلى النظام > إعدادات > بروتوكولات > IPsec > IPsec أصلي طبيعي.

انقر فوق إضافة لتكوين اقتران أمان بين Cisco ISE PSN و NAD.

- حدد العقدة.
- حدد عنوان NAD IP.
- أختر واجهة حركة مرور IPsec المطلوبة.
- أدخل المفتاح المشترك مسبقا الذي سيتم إستخدامه على NAD أيضا.

في القسم العام، أدخل التفاصيل المحددة.

- أختر IKEv2.
- حدد وضع النفق.
- حدد ESP كبروتوكول ESP/AH.



تكوين ISE الأصلي IPSec

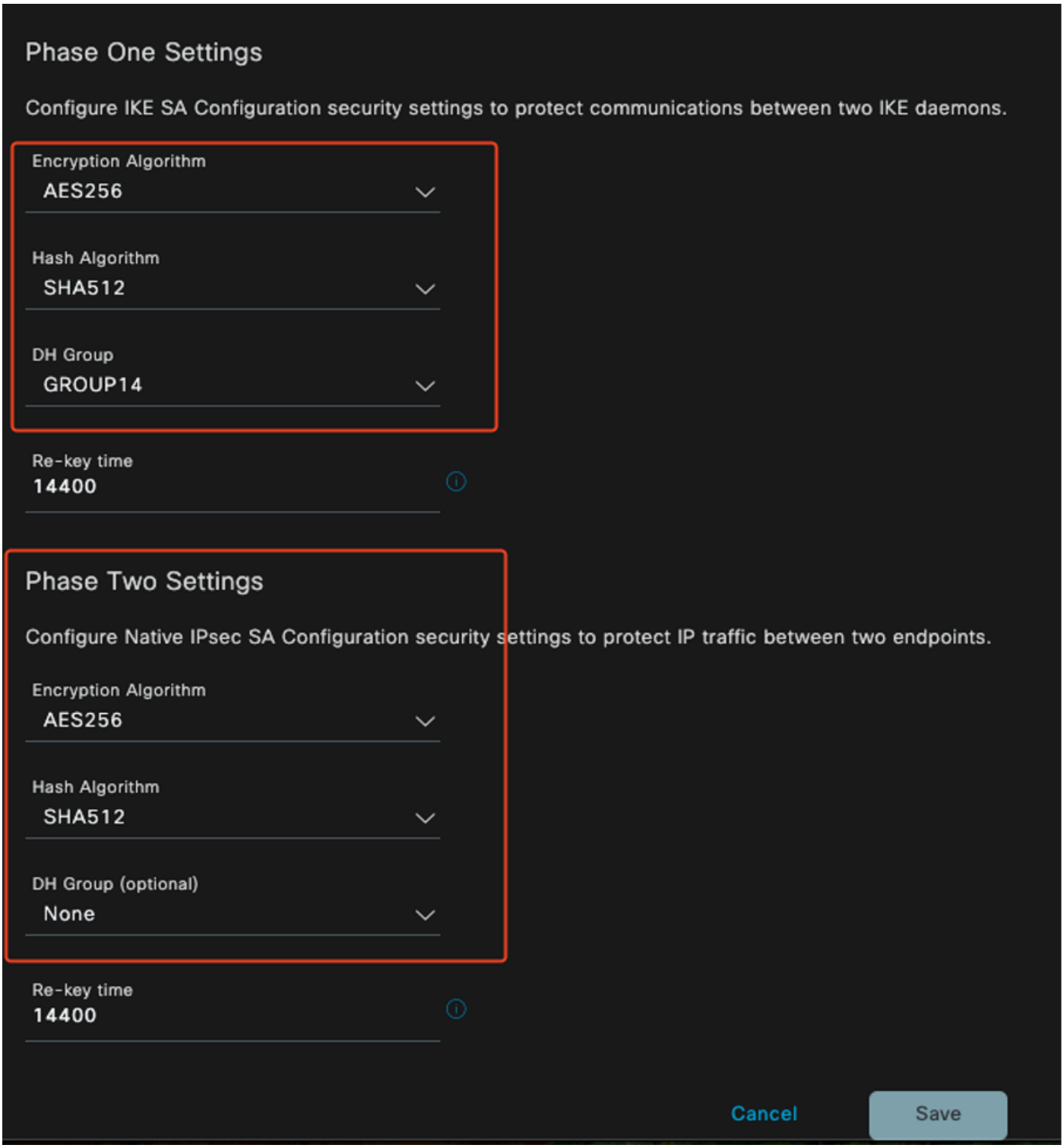
في إعدادات المرحلة الأولى:

- أختر AES256 كخوارزمية تشفير.

- حدد SHA512 كما يتضمن الخوارزمية.
- حدد المجموعة 14 كمجموعة DH.

في إعدادات المرحلة الثانية:

- أختر AES256 كخوارزمية تشفير.
- حدد SHA512 كما يتضمن الخوارزمية.



تكوين المرحلة 1 والمرحلة 2 من IPSec

قم بتكوين مسار من واجهة سطر أوامر ISE إلى عنصر التحكم في الشبكة المحلية

اللاسلكية (WLC) باستخدام بوابة ETH1 كالخطوة التالية.

<#root>

```
ise3genvc/admin#configure t
Entering configuration mode terminal
```

ise3genvc/admin(config)#ip route 10.78.8.77 255.255.255.255 gateway 10.106.33.1

```
ise3genvc/admin(config)#end
ise3genvc/admin#show ip route | include 10.78.8.77
10.78.8.77 10.106.33.1 eth1
```

9800 WLC تشكيل

تم عرض تكوين IPSec الخاص بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) المدارة بواسطة واجهة المستخدم الرسومية (GUI)، لذلك يلزم إجراء جميع التكوين من واجهة سطر الأوامر (CLI).

فيما يلي خطوات التكوين لخادم ISE. يتم إرفاق كل خطوة بأوامر CLI ذات الصلة في هذه القسم لتوفير التوجيه.

خطوات تكوين WLC IPSec

تكوين مقترح IKEv2

لبدء التكوين، أدخل وضع التكوين العام وأنشئ مقترح IKEv2. قم بتعيين اسم فريد للمقترح لأغراض التعريف.

```
crypto ikev2 proposal ipsec-prop
encryption aes-cbc-256
integrity sha512
group 14
exit
```

بعد ذلك، قم بتكوين سياسة وتعيين الاقتراح الذي تم إنشاؤه مسبقا ضمن هذا النهج.

```
crypto ikev2 policy ipsec-policy
proposal ipsec-prop
exit
```

قم بتحديد حلقة مفاتيح تشفير ليتم إستخدامها أثناء مصادقة IKE. تحمل حلقة المفاتيح هذه بيانات اعتماد المصادقة الضرورية.

```
crypto ikev2 keyring mykey
peer ise
address 10.106.33.23 255.255.255.255
pre-shared-key Cisco!123
exit
```

تكوين ملف تعريف IKEv2 الذي يعمل كمستودع للمعلمات غير القابلة للتداول الخاصة ب IKE SA. ويتضمن ذلك الهويات المحلية أو البعيدة وأساليب المصادقة والخدمات المتاحة للأقران المصدق عليهم.

```
crypto ikev2 profile ipsec-profile
 match identity remote address  10.106.33.23 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local mykey
exit
```

قم بإنشاء مجموعة تحويل وتكوينها للعمل في وضع النفق.

```
crypto ipsec transform-set TSET esp-aes 256 esp-sha512-hmac
mode tunnel
exit
```

قم بإنشاء قائمة تحكم في الوصول (ACL) للسماح بالاتصال فقط ب ISE Interface IP.

```
ip access-list extended ISE_ALLOW
 10 permit ip host  10.78.8.77 host 10.106.33.23
```

تكوين خريطة تشفير من التكوين العام. إرفاق مجموعة التحويل، وملف تعريف IPsec، وقائمة التحكم في الوصول (ACL) بخريطة التشفير.

```
crypto map ikev2-cryptomap 1 ipsec-isakmp
set peer 10.106.33.23
set transform-set TSET
set ikev2-profile ipsec-profile
match address ISE_ALLOW
```

أخيرا، قم بإرفاق خريطة التشفير بالواجهة. في هذا السيناريو، يتم تعيين واجهة الإدارة اللاسلكية التي تحمل حركة مرور RADIUS ضمن شبكة VLAN الخاصة بواجهة الإدارة.

```
int vlan 2124
crypto map ikev2-cryptomap
```

التحقق من الصحة

WLC

تتوفر أوامر show للتحقق من IPSec على 9800 WLC.

- show ip access-lists
- عرض خريطة التشفير
- show crypto ikev2 sa detail
- عرض تفاصيل IPsec للتشفير

<#root>

```
POD6_9800#show ip access-lists ISE_ALLOW
Extended IP access list ISE_ALLOW
10 permit ip host 10.78.8.77 host 10.106.33.23 (6 matches)

POD6_9800#show crypto map
Interfaces using crypto map MAP-IKEV2:

Crypto Map IPv4 "ikev2-cryptomap" 1 ipsec-isakmp
```

Peer = 10.106.33.23

```
IKEv2 Profile:
```

ipsec-profile

Access-List SS dynamic: False
Extended IP access list ISE_ALLOW

access-list ISE_ALLOW

permit ip host 10.78.8.77 host 10.106.33.23
Current peer: 10.106.33.23
Security association lifetime: 4608000 kilobytes/3600 seconds
Dualstack (Y/N): N

Responder-Only (Y/N): N
PFS (Y/N): N
Mixed-mode : Disabled

Transform sets={

TSET: { esp-256-aes esp-sha512-hmac } ,

}

Interfaces using crypto map ikev2-cryptomap:

Vlan2124

POD6_9800#show crypto ikev2 sa detailed
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1

10.78.8.77/500 10.106.33.23/500

none/none READY

Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:14, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/617 sec
CE id: 1699, Session-id: 72
Local spi: BA3FFBBFCF57E6A1 Remote spi: BEE60CB887998D58
Status Description: Negotiation done

Local id: 10.78.8.77

Remote id: 10.106.33.23

Local req msg id: 0 Remote req msg id: 2
Local next msg id: 0 Remote next msg id: 2
Local req queued: 0 Remote req queued: 2
Local window: 5 Remote window: 1
DPD configured for 0 seconds, retry 0
Fragmentation not configured.
Dynamic Route Update: disabled

```
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No
PEER TYPE: Other

IPv6 Crypto IKEv2 SA

POD6_9800#show crypto ipsec sa detail


interface: Vlan2124



Crypto map tag: ikev2-cryptomap, local addr 10.78.8.77



protected vrf: (none)
local ident (addr/mask/prot/port): (10.78.8.77/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.106.33.23/255.255.255.255/0/0)
current_peer 10.106.33.23 port 500
PERMIT, flags={origin_is_acl,}

#pkts encaps: 285, #pkts encrypt: 285, #pkts digest: 285



#pkts decaps: 211, #pkts decrypt: 211, #pkts verify: 211


#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts tagged (send): 0, #pkts untagged (rcv): 0
#pkts not tagged (send): 0, #pkts not untagged (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 10.78.8.77, remote crypto endpt.: 10.106.33.23
plaintext mtu 1022, path mtu 1100, ip mtu 1100, ip mtu idb Vlan2124
current outbound spi: 0xCCC04668(3435153000)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xFEACCF3E(4272738110)
transform: esp-256-aes esp-sha512-hmac ,
in use settings ={Tunnel, }
conn id: 2379, flow_id: HW:379, sibling_flags FFFFFFFF80000048, crypto map: ikev2-cryptomap, initiator
sa timing: remaining key lifetime (k/sec): (4607994/2974)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:
```

```
outbound esp sas:
spi: 0xCCC04668(3435153000)
transform: esp-256-aes esp-sha512-hmac ,
in use settings ={Tunnel, }
conn id: 2380, flow_id: HW:380, sibling_flags FFFFFFFF80000048, crypto map: ikev2-cryptomap, initiator
sa timing: remaining key lifetime (k/sec): (4607994/2974)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

محرك خدمات كشف الهوية (ISE)

<#root>

```
ise3genvc/admin#application configure ise
```

It will present multiple options. Select option 34.

[34]View Native IPSec status

```
45765332-52dd-4311-93ed-44fd64c55585: #1, ESTABLISHED, IKEv2, bee60cb887998d58_i* ba3ffbbfcf57e6a1_r
local '10.106.33.23' @ 10.106.33.23[500]
remote '10.78.8.77' @ 10.78.8.77[500]
AES_CBC-256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MODP_2048
established 1133s ago, rekeying in 6781s, reauth in 78609s
net-net-45765332-52dd-4311-93ed-44fd64c55585: #2, reqid 1, INSTALLED,
```

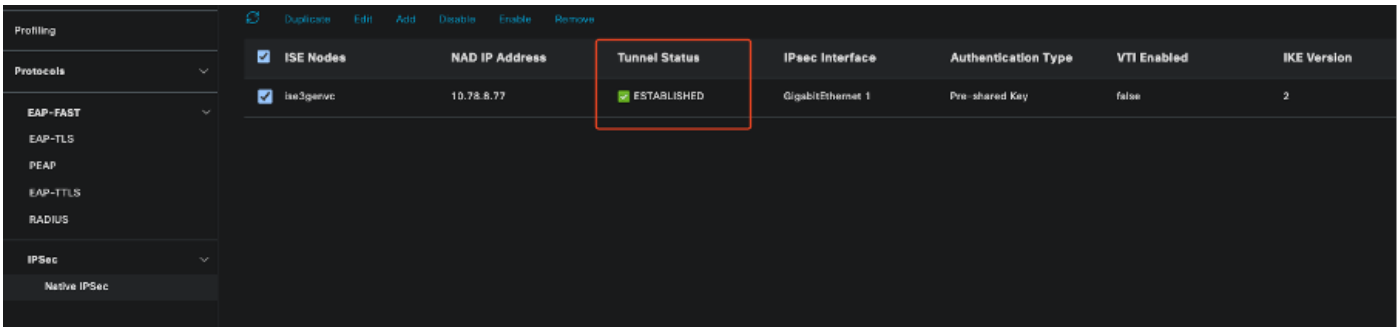
TUNNEL, ESP:AES_CBC-256/HMAC_SHA2_512_256

```
installed 1133s ago, rekeying in 12799s, expires in 14707s
in ccc04668, 5760 bytes, 96 packets, 835s ago
out feaccf3e, 5760 bytes, 96 packets, 835s ago
```

local 10.106.33.23/32

remote 10.78.8.77/32

```
Enter 0 to exit from this context.
```



واجهة المستخدم الرسومية (GUI) ل ISE التي تظهر حالة IPSec

التقاط الحزم

أدخل وحدة تحكم في الوصول (EPC) على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لضمان عبور حركة مرور بيانات RADIUS الخاصة بالعميل عبر نفق ESP. باستخدام التقاط مستوى التحكم، يمكنك مراقبة الحزم التي تخرج من مستوى التحكم في حالة غير مشفرة، والتي يتم بعد ذلك تشفيرها وإرسالها إلى الشبكة السلكية.

No.	Time	Source	Destination	Protocol	Length	Info
136	13:…	10.78.8.77	10.106.33.23	RADIUS	432	Access-Request id=119
137	13:…	10.78.8.77	10.106.33.23	ESP	526	ESP (SPI=0xc3a824d7)
138	13:…	10.106.33.23	10.78.8.77	ESP	254	ESP (SPI=0xc19b26e9)
139	13:…	10.106.33.23	10.78.8.77	RADIUS	165	Access-Challenge id=119
144	13:…	10.78.8.77	10.106.33.23	RADIUS	705	Access-Request id=120
145	13:…	10.78.8.77	10.106.33.23	ESP	798	ESP (SPI=0xc3a824d7)
194	13:…	10.106.33.23	10.78.8.77	ESP	1262	ESP (SPI=0xc19b26e9)
195	13:…	10.106.33.23	10.78.8.77	RADIUS	1177	Access-Challenge id=120
214	13:…	10.78.8.77	10.106.33.23	RADIUS	507	Access-Request id=121
215	13:…	10.78.8.77	10.106.33.23	ESP	590	ESP (SPI=0xc3a824d7)
216	13:…	10.106.33.23	10.78.8.77	ESP	1262	ESP (SPI=0xc19b26e9)
217	13:…	10.106.33.23	10.78.8.77	RADIUS	1173	Access-Challenge id=121
240	13:…	10.78.8.77	10.106.33.23	RADIUS	507	Access-Request id=122
241	13:…	10.78.8.77	10.106.33.23	ESP	590	ESP (SPI=0xc3a824d7)
242	13:…	10.106.33.23	10.78.8.77	ESP	414	ESP (SPI=0xc19b26e9)

حزم IPSec بين WLC و ISE

استكشاف الأخطاء وإصلاحها

تصحيح أخطاء WLC

بما أن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) طراز 9800 يعمل على برنامج Cisco IOS XE، فيمكنك إستخدام أوامر تصحيح أخطاء IPSec مماثلة لتلك الموجودة على الأنظمة الأساسية الأخرى من Cisco IOS XE. فيما يلي أمران رئيسيان مفيدان لاستكشاف أخطاء IPSec وإصلاحها.

- debug crypto ikev2
- خطأ debug crypto ikev2

تصحيح أخطاء ISE

أستخدم هذه الأمر على واجهة سطر الأوامر (CLI) الخاصة ب ISE لعرض سجلات IPSec. أوامر التصحيح غير ضرورية على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

- show logging application strongswan/charon.log tail

المراجع

دليل تكوين برنامج Cisco Catalyst 9800 Series Wireless Controller Software، Cisco IOS XE Cupertino 17.9.x

أمان IPsec لتأمين الاتصال بين Cisco ISE و NAD

تكوين الإصدار 2 من مفتاح الإنترنت التبادلي (IKEv2)

تكوين اتصال ISE 3.3 الأصلي إلى أمان NAD (Cisco IOS XE)

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).