تكوين ISE 2.2 IPsec لتأمين اتصال NAD (IOS)

المحتويات

المقدمة

في هذا المستند كيفية تكوين TACACS IPSec واستكشاف أخطائه وإصلاحها لتأمين اتصال مخرج خدمة الهوية (ISE) من Cisco 2.2 - زاج الوصول إلى الشبكة (NAD). يمكن تشفير حركة مرور TACACS باستخدام نفق بادل مفاتيح الإنترنت الإصدار 2 (IKEv2) من IPSec موقع إلى موقع (LAN-to-LAN) بين الموجه و ISE. ال تغطي هذه المستند جزء تكوين TACACS.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- محرك خدمات كشف الهوية (ISE)
- موجه Cisco
- مفاهيم IPSec العامة
- المفاهيم العامة ل TACACS

المكونات المستخدمة

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

- الموجه Cisco ISR4451-X Router الذي يشغل الإصدار 15.4(3)S2 من البرنامج
- Cisco Identity Service Engine، الإصدار 2.2
- حزمة الخدمة 1 لنظام التشغيل Windows 7

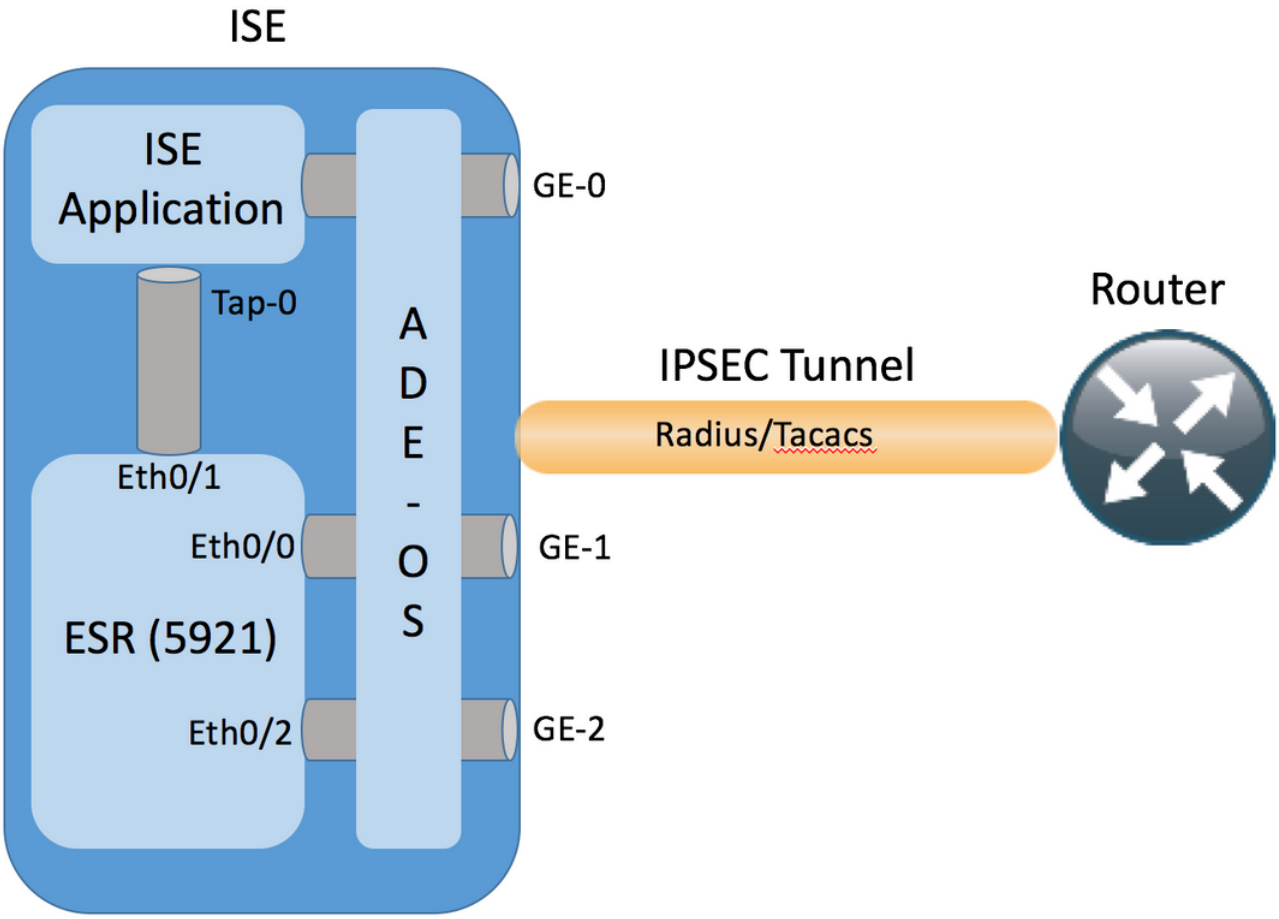
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

والهدف هو تأمين البروتوكولات التي تستخدم تجزئة MD5 غير الآمنة و RADIUS و TACACS مع IPSec. قليل من الحقائق التي يجب أخذها بعين الاعتبار:

- يدعم Cisco ISE بروتوكول IPSec في وضعي النفق والنقل.
- عند تمكين IPSec على واجهة Cisco ISE، 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 ETH1 من خلال واجهات ETH5. أنت يستطيع شكلت IPSec على قطع واحد cisco ISE قارن لكل PSN.

بنية ISE IPSec



بمجرد إستلام الحزم المشفرة بواسطة واجهة ISE GE-1، يعترض موجه الخدمات المضمنة (ESR) الحزم على واجهة ETH0/0.

```
interface Ethernet0/0
 description e0/0->connection to external NAD
 ip address 10.48.17.87 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 no ip route-cache
 crypto map radius
```

يقوم ESR بفك تشفيرها ووقائع لقواعد NAT التي تم تكوينها مسبقا بتنفيذ ترجمة العنوان. تتم ترجمة حزم RADIUS/TACACS الصادرة (نحو NAD) إلى عنوان واجهة Ethernet0/0 وتشفيرها بعد ذلك.

```
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
ip nat inside source static tcp 10.1.1.2 49 interface Ethernet0/0 49
access-list 1 permit 10.1.1.0 0.0.0.3
```

يجب إرسال الحزم الموجهة إلى واجهة ETH0/0 على منافذ RADIUS/TACACS عبر واجهة ETH0/1 إلى عنوان IP 10.1.1.2، وهو العنوان الداخلي ل ISE. تكوين ESR ل ETH0/1

```
interface Ethernet0/1
 description e0/1->tap0 internal connection to ISE
 ip address 10.1.1.1 255.255.255.252
```

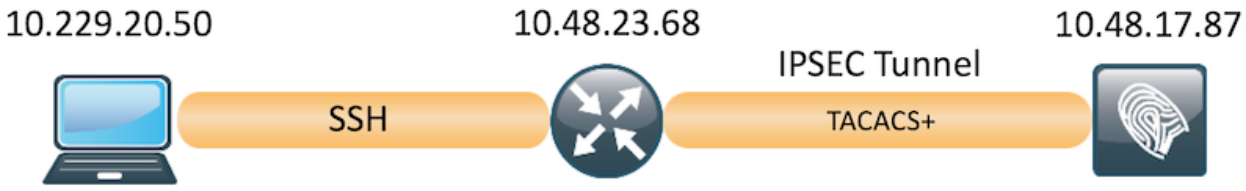
```
 ip nat inside
 ip virtual-reassembly in
 no ip route-cache
```

تكوين ISE لواجهة TAP-0 الداخلية:

```
ISE22-1ek/admin# show interface | b tap0
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 10.1.1.2  netmask 255.255.255.252  broadcast 10.1.1.3
       inet6 fe80::6c2e:37ff:fe5f:b609  prefixlen 64  scopeid 0x20<link>
       ether 6e:2e:37:5f:b6:09  txqueuelen 500  (Ethernet)
       RX packets 81462  bytes 8927953 (8.5 MiB)
       RX errors 0  dropped 68798  overruns 0  frame 0
       TX packets 105  bytes 8405 (8.2 KiB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

الرسم التخطيطي للشبكة

تستخدم المعلومات الواردة في هذا المستند إعداد الشبكة التالي:



تكوين IKEv1 IPsec VPN باستخدام مفتاح مشترك مسبق (خارج المربع)

يوضح هذا القسم كيفية إكمال تكوينات IOS CLI و ISE.

تكوين واجهة سطر الأوامر لموجه IOS

تكوين الواجهات

إذا لم يتم تكوين واجهات موجه IOS بعد، فيجب تكوين واجهة WAN على الأقل. فيما يلي مثال:

```
interface GigabitEthernet0/0/0
 ip address 10.48.23.68 255.255.255.0
 negotiation auto
no shutdown
!
```

تأكد من وجود اتصال بالنظير البعيد الذي يجب إستخدامه لإنشاء نفق شبكة VPN من موقع إلى موقع. يمكنك إستخدام إختبار الاتصال للتحقق من الاتصال الأساسي.

تكوين سياسة ISAKMP (IKEv1)

دخلت in order to شكلت ال isakmp سياسة ل ال IKEv1 توصيل، **ال crypto isakmp سياسة**

<priority> أمر في شامل تشكيل أسلوب. فيما يلي مثال:

```
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 16
```

ملاحظة: يمكنك تكوين سياسات IKE متعددة على كل نظير شارك في IPSec. عند بدء تفاوض IKE، فإنه يحاول العثور على سياسة مشتركة تم تكوينها على كل من النظراء، وتبدأ بسياسات الأولوية العليا التي تم تحديدها على النظير البعيد.

تكوين مفتاح ISAKMP تشفير

دخلت in order to شكلت *سابق* صحة هوية مفتاح، ال crypto isakmp **مفتاح** أمر في شامل تشكيل أسلوب:

```
crypto isakmp key Krakow123 address 10.48.17.87
```

تكوين قائمة تحكم في الوصول (ACL) لحركة مرور VPN ذات الأهمية

أستخدم قائمة الوصول الموسعة أو المسماة لتحديد حركة المرور التي يجب حمايتها بالتشفير. فيما يلي مثال:

```
access-list 101 permit ip 10.48.23.68 0.0.0.0 10.48.17.87 0.0.0.0
```

ملاحظة: تستخدم قائمة التحكم في الوصول لحركة مرور VPN عناوين IP للمصدر والوجهة بعد NAT.

تكوين مجموعة تحويل

لتحديد مجموعة تحويل IPSec (مجموعة مقبولة من بروتوكولات الأمان والخوارزميات)، أدخل الأمر **crypto ipSec transform-set** في وضع التكوين العام. فيما يلي مثال:

```
crypto ipsec transform-set SET esp-aes esp-sha256-hmac
 mode transport
```

تكوين خريطة تشفير وتطبيقها على واجهة

دخلت in order to خلقت أو عدلت تشفير خريطة مدخل وأدخلت ال crypto خريطة تشكيل أسلوب، ال **crypto map** شامل تشكيل أمر. حتى يكتمل إدخال خريطة التشفير، هناك بعض الجوانب التي يجب تعريفها كحد أدنى:

- يجب تحديد نظائر IPsec التي يمكن إعادة توجيه حركة المرور المحمية إليها. وهؤلاء هم الأقران الذين يمكن معهم إنشاء مساعد خدمة. دخلت in order to عينت IPSec نظير في تشفير خريطة مدخل، **النظير** أمر.
- يجب تحديد مجموعات التحويل المقبولة للاستخدام مع حركة المرور المحمية. دخلت in order to عينت التحويل مجموعة أن يستطيع كنت استعملت مع ال crypto خريطة مدخل، **المجموعة تحويل-set** أمر.

- يجب تحديد حركة المرور التي يجب حمايتها. دخلت in order to عينت موسع منفذ قائمة ل crypto خريطة مدخل، ال match عنوان أمر.

فيما يلي مثال:

```
crypto map MAP 10 ipsec-isakmp
 set peer 10.48.17.87
 set transform-set SET
 match address 101
```

تتمثل الخطوة الأخيرة في تطبيق مجموعة خريطة التشفير المحددة مسبقا على واجهة. دخلت in order to طبقت هذا، ال crypto map قارن تشكيل أمر:

```
interface GigabitEthernet0/0
crypto map MAP
```

التكوين النهائي IOS

فيما يلي تكوين CLI لموجه IOS النهائي:

```
aaa group server tacacs+ ISE_TACACS
 server name ISE22
!
aaa authentication login default group ISE_TACACS
aaa authorization exec default group ISE_TACACS
!
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 16
!
crypto isakmp key Krakow123 address 10.48.17.87
!
crypto ipsec transform-set SET esp-aes esp-sha256-hmac
 mode transport
!
crypto map MAP 10 ipsec-isakmp
 set peer 10.48.17.87
 set transform-set SET
 match address 101
!
access-list 101 permit ip 10.48.23.68 0.0.0.0 10.48.17.87 0.0.0.0
!
interface GigabitEthernet0/0/0
 ip address 10.48.23.68 255.255.255.0
 negotiation auto
 no shutdown
!
crypto map MAP 10 ipsec-isakmp
 set peer 10.48.17.87
 set transform-set SET
 match address 101
!
tacacs server ISE22
 address ipv4 10.48.17.87
 key cisco
```

تكوين ISE

تكوين عنوان IP على ISE

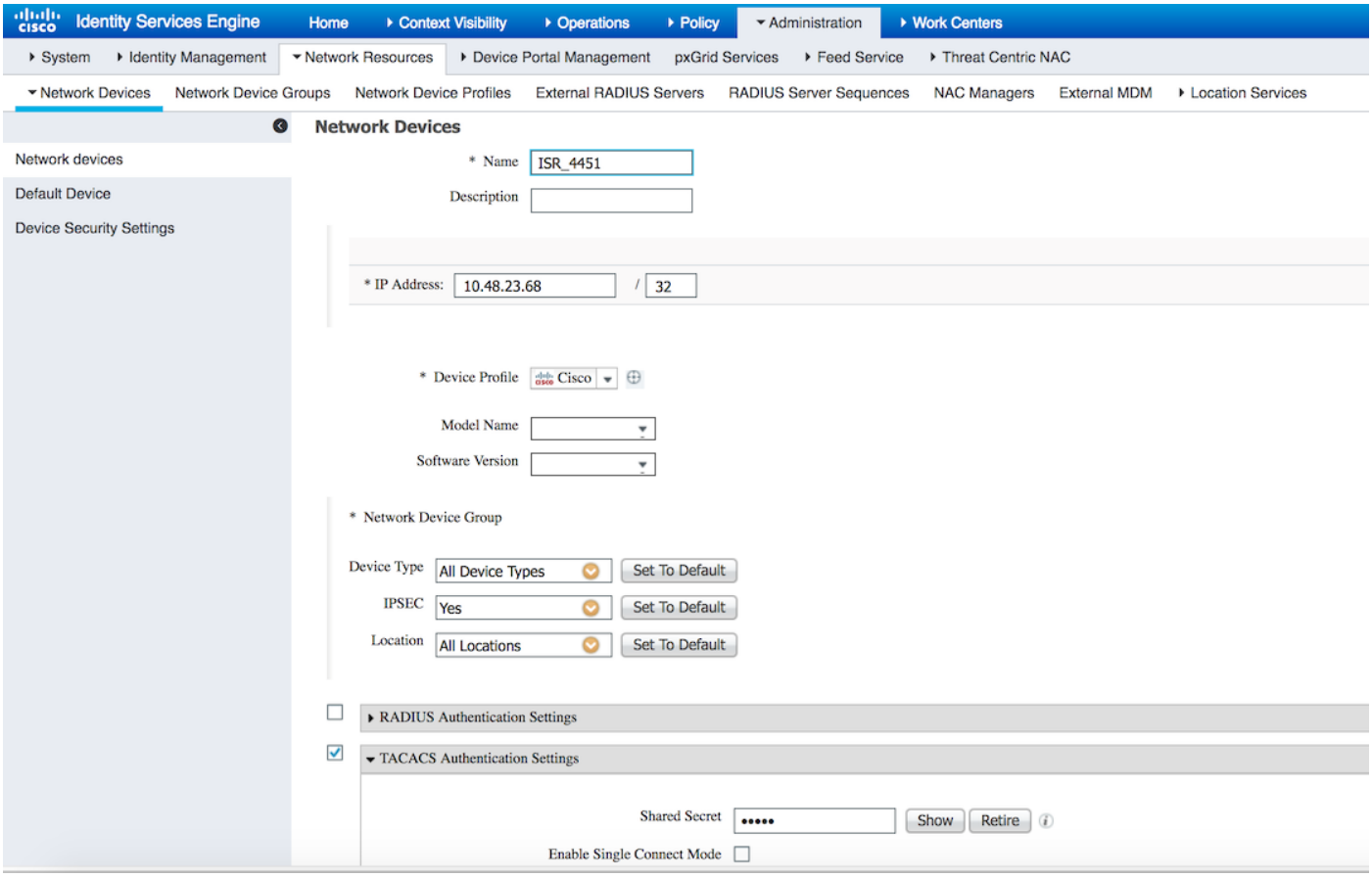
يجب تكوين العنوان على الواجهة ge1-GE5 من واجهة سطر الأوامر، الى يتم دعم ge0.

```
interface GigabitEthernet 1
 ip address 10.48.17.87 255.255.255.0
 ipv6 address autoconfig
 ipv6 enable
```

ملاحظة: تتم إعادة تشغيل التطبيق بعد تكوين عنوان IP على الواجهة:
٪ قد يؤدي تغيير عنوان IP إلى إعادة تشغيل خدمات ISE
هل تريد المتابعة مع تغيير عنوان IP؟ Y/N [N]: Y

إضافة NAD إلى مجموعة IPSec على ISE

انتقل إلى **إدارة > موارد الشبكة > أجهزة الشبكة**. انقر فوق **إضافة (Add)**. تأكد من تكوين الاسم وعنوان IP والسر المشترك. لإنهاء نفق IPSec من NAD، ثم حدد "نعم" مقابل مجموعة أجهزة شبكة IPSec.

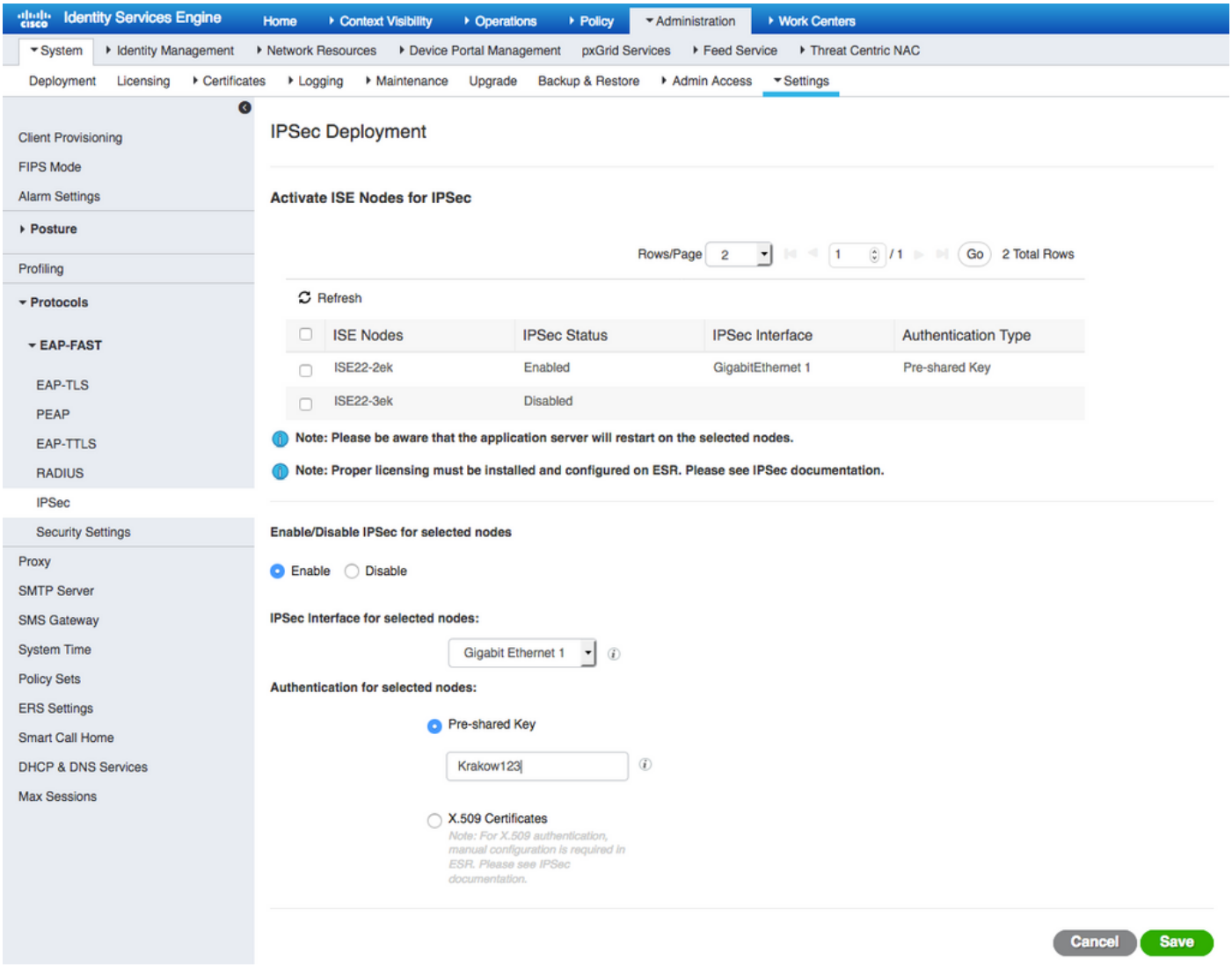


وبمجرد إضافة NAD، يجب إنشاء مسار إضافي على محرك خدمات الهوية (ISE)، لضمان أن حركة مرور RADIUS تمر عبر بروتوكول ESR وتتم تشفيرها:

```
ip route 10.48.23.68 255.255.255.255 gateway 10.1.1.1
```

تمكين IPSec على ISE

انتقل إلى **إدارة > نظام > إعدادات**. انقر فوق RADIUS ثم فوق IPSec. حدد PSN (أحادي/متعدد/كلي) حدد خيار تمكين، واختر الواجهة وحدد أسلوب المصادقة. طقطقة **حفظ**. إعادة تشغيل الخدمات في العقدة المحددة في هذه النقطة.



لاحظ أنه بعد إعادة تشغيل الخدمات يقوم تكوين واجهة سطر الأوامر (CLI) الخاصة ب ISE بعرض الواجهة التي تم تكوينها بدون عنوان IP وفي حالة إيقاف التشغيل، من المتوقع أن يقوم ESR (موجه الخدمات المضمنة) بالتحكم في واجهة ISE.

```
interface GigabitEthernet 1
 shutdown
 ipv6 address autoconfig
 ipv6 enable
```

بمجرد إعادة تشغيل الخدمات، يتم تمكين وظيفة ESR. لتسجيل الدخول إلى ESR ون ESR في سطر الأوامر:

```
ISE22-1ek/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE
SOFTWARE (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, <CTRL-C> to exit
```

```
ise-esr5921>en
ise-esr5921#
```

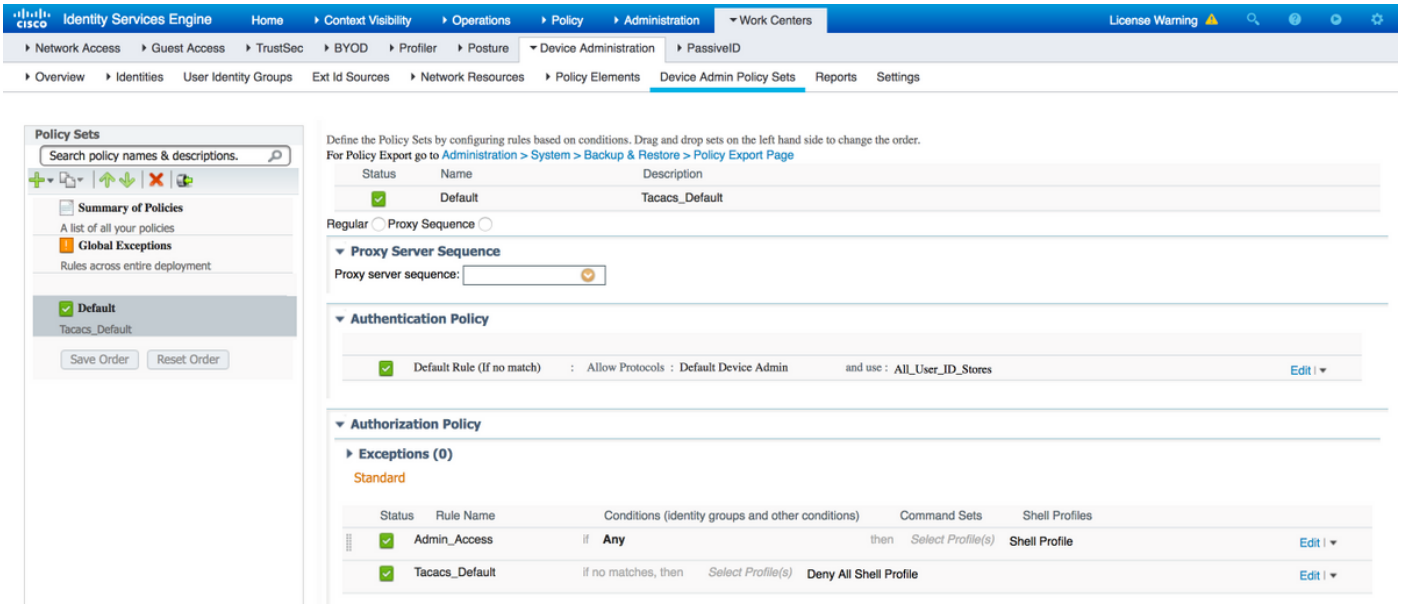
يأتي ESR مع تكوين التشفير هذا، والذي يكون كافيا لإنهاء نفق IPsec باستخدام مفاتيح مشتركة مسبقا:

```
crypto keyring MVPN-spokes
 pre-shared-key address 0.0.0.0 0.0.0.0 key Krakow123
!
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 16
!
crypto isakmp policy 20
 encr aes
 hash sha256
 authentication pre-share
 group 14
!
crypto isakmp key Krakow123 address 0.0.0.0
!
crypto isakmp profile MVPN-profile
  description LAN-to-LAN for spoke router(s) connection
  keyring MVPN-spokes
  match identity address 0.0.0.0
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
 mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
 mode transport
!
crypto dynamic-map MVPN-dynmap 10
 set transform-set radius radius-2
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
```

تأكد من أن ESR لديه مسار لإرسال الحزم المشفرة:

```
ip route 0.0.0.0 0.0.0.0 10.48.26.1
```

تعيين نهج Tacacs على ISE



التحقق من الصحة

موجه IOS

قبل بدء جلسة SSH إلى الموجه، ال توجد إتصالات VPN نشطة:

```
ISR4451#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA
```

يتصل العميل بالموجه، عند إستخدام مصدر مصادقة ISE 2.2.

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh alice@10.48.23.68
Password:
ISR4451#
```

يرسل IOS حزمة TACACS، والتي تقوم بتشغيل إنشاء جلسة VPN، ما إن النفق يكون فوق هذا إنتاج رأيت على المسحاج تخديد. إنه يؤكد أن المرحلة الأولى من النفق قد انتهت:

```
ISR4451#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.48.17.87     10.48.23.68     QM_IDLE           1962 ACTIVE

IPv6 Crypto ISAKMP SA

ISR4451#
```

تكون المرحلة 2 قيد التشغيل، ويتم تشفير الحزم وفك تشفيرها:

```
ISR4451#sh cry ipsec sa

interface: GigabitEthernet0/0/0
   Crypto map tag: MAP, local addr 10.48.23.68

  protected vrf: (none)
```

```
  local  ident (addr/mask/prot/port): (10.48.23.68/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (10.48.17.87/255.255.255.255/0/0)
  current_peer 10.48.17.87 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 48, #pkts encrypt: 48, #pkts digest: 48
   #pkts decaps: 48, #pkts decrypt: 48, #pkts verify: 48
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

    local crypto endpt.: 10.48.23.68, remote crypto endpt.: 10.48.17.87
    plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
    current outbound spi: 0x64BD51B8(1690128824)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0xFAE51DF8(4209319416)
       transform: esp-aes esp-sha256-hmac ,
       in use settings ={Transport, }
       conn id: 2681, flow_id: ESG:681, sibling_flags FFFFFFFF80004008, crypto map: MAP
       sa timing: remaining key lifetime (k/sec): (4607998/3127)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x64BD51B8(1690128824)
       transform: esp-aes esp-sha256-hmac ,
       in use settings ={Transport, }
       conn id: 2682, flow_id: ESG:682, sibling_flags FFFFFFFF80004008, crypto map: MAP
       sa timing: remaining key lifetime (k/sec): (4607997/3127)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
ISR4451#
```

ESR

يمكن التحقق من نفس المخرجات على ESR، المرحلة الأولى قيد التشغيل:

```
ise-esr5921#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.48.17.87     10.48.23.68     QM_IDLE           1002 ACTIVE

IPv6 Crypto ISAKMP SA

ise-esr5921#
```

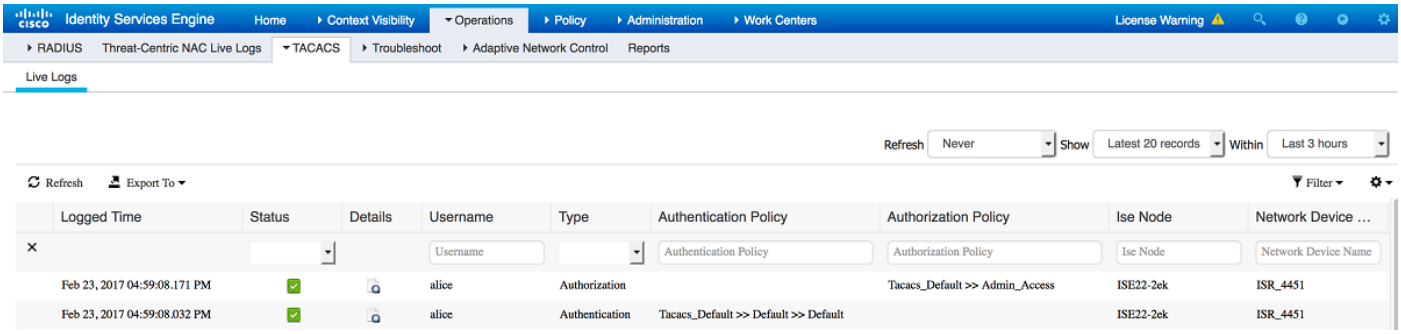
تكون المرحلة 2 قيد التشغيل، ويتم تشفير الحزم وفك تشفيرها بنجاح:

```
ise-esr5921#sh cry ipsec sa
```

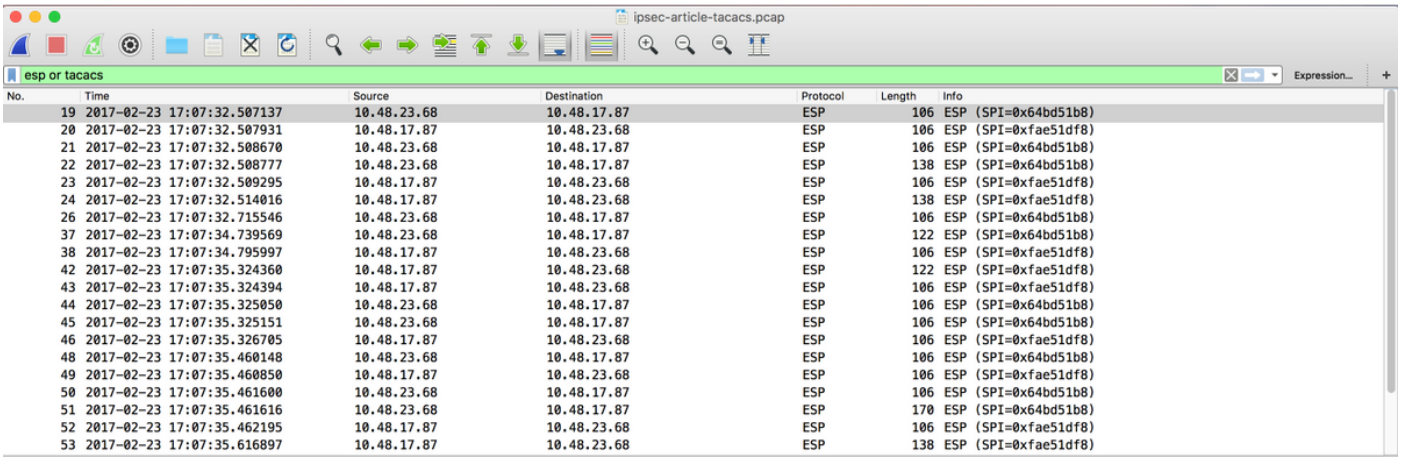
```
interface: Ethernet0/0
   Crypto map tag: radius, local addr 10.48.17.87

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.48.17.87/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (10.48.23.68/255.255.255.255/0/0)
  current_peer 10.48.23.68 port 500
    PERMIT, flags={}
   #pkts encaps: 48, #pkts encrypt: 48, #pkts digest: 48
   #pkts decaps: 48, #pkts decrypt: 48, #pkts verify: 48
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

    local crypto endpt.: 10.48.17.87, remote crypto endpt.: 10.48.23.68
    plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0xFAE51DF8(4209319416)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x64BD51B8(1690128824)
       transform: esp-aes esp-sha256-hmac ,
       in use settings ={Transport, }
       conn id: 3, flow_id: SW:3, sibling_flags 80000000, crypto map: radius
       sa timing: remaining key lifetime (k/sec): (4242722/3056)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xFAE51DF8(4209319416)
       transform: esp-aes esp-sha256-hmac ,
       in use settings ={Transport, }
       conn id: 4, flow_id: SW:4, sibling_flags 80000000, crypto map: radius
       sa timing: remaining key lifetime (k/sec): (4242722/3056)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
ise-esr5921#
```

محرك خدمات كشف الهوية (ISE)

تشير المصادقة المباشرة إلى مصادقة PAP_ASCII العادية:



تؤكد السجلات التي تم التقاطها على واجهة GE1 الخاصة بالإصدار ISE والتي تمت تصفيتها باستخدام بروتوكول ESP أو TACACS، عدم وجود بروتوكول TACACS في نص واضح، ويتم تشفير جميع حركات مرور البيانات:



استكشاف الأخطاء وإصلاحها

يمكن تطبيق تقنية أستكشاف أخطاء VPN وإصلاحها الشائعة لاستكشاف أخطاء IPSec وإصلاحها. يمكنك العثور على وثائق مفيدة أدناه:

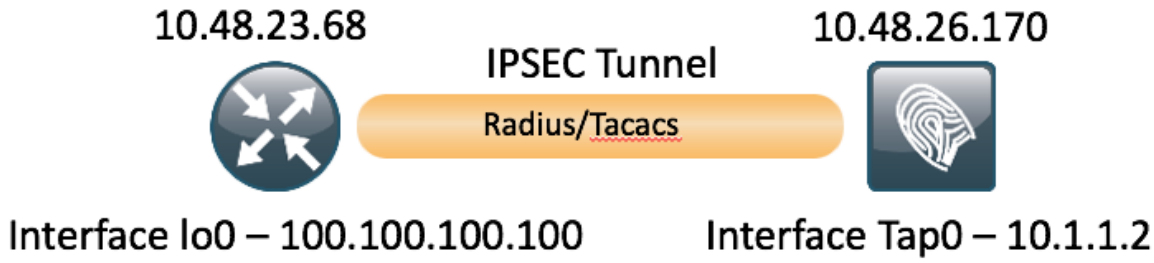
[عمليات تصحيح أخطاء IOS IKEv2 لشبكة VPN من موقع إلى موقع مع PSKs أستكشاف أخطاء وإصلاحها TechNote](#)

[تصحيح أخطاء ASA IKEv2 لشبكة VPN من موقع إلى موقع مع PSKs](#)

[أستكشاف أخطاء IPsec وإصلاحها: فهم أوامر تصحيح الأخطاء واستخدامها](#)

تكوين موقع إلى موقع شبكة FlexVPN (من DVTI إلى SVTI) بين NAD و ISE 2.2

كما يمكن حماية حركة مرور بيانات RADIUS باستخدام FlexVPN. يتم إستخدام المخطط التالي في المثال التالي:



تتسم تهيئة FlexVPN بالوضوح التام. يمكن العثور على مزيد من التفاصيل هنا:

http://www.cisco.com/c/en/us/support/docs/security/flexvpn/115782-flexvpn-site-to-site-00.html

مزايا تصميم Flex VPN

- يمكنك تشغيل Flex على جميع شبكات VPN IPsec السابقة لديك. تتيح معظم السيناريوهات إمكانية التعايش مع التكوين السابق والإصدار المرن.
- تستند الشبكة الخاصة الظاهرية (VPN) المرنة إلى الإصدار الثاني من بروتوكول IKEv2 وليس إلى الإصدار الأول من بروتوكول الإنترنت (IKEv1)، الذي يعمل على تحسين جميع جوانب التفاوض واستقرار البروتوكول تقريبا.
- وظائف متعددة يمكن تحقيقها في إطار عمل واحد.
- سهولة التهيئة باستخدام إعدادات افتراضية منطقية - لا تحتاج إلى تحديد سياسات أو مجموعات تحويل وما إلى ذلك، بل إن IKEv2 قد بنى إعدادات افتراضية منطقية وتم تحديثها.

تكوين الموجّه

```
aaa new-model
!
!
aaa group server tacacs+ ISE_TACACS
 server name ISE22_VRF
ip vrf forwarding TACACS
!
aaa authentication login default group ISE_TACACS
aaa authorization exec default group ISE_TACACS
aaa authorization network default local
!
crypto ikev2 authorization policy default
 route set interface Loopback0
 no route set interface
!
!
crypto ikev2 keyring mykeys
 peer ISE22
 address 10.48.17.87
 pre-shared-key Krakow123
 !
!
!
crypto ikev2 profile default
 match identity remote address 10.48.17.87 255.255.255.255
 authentication remote pre-share (with the command authentication remote pre-share key in place
```

```
keyring is not required)
 authentication local pre-share
 keyring local mykeys
 aaa authorization group psk list default default
!
!
ip tftp source-interface GigabitEthernet0
!
!
!
crypto ipsec profile default
 set ikev2-profile default (it is default configuration)
!
!
!
interface Loopback0
ip vrf forwarding TACACS
 ip address 100.100.100.100 255.255.255.0
!
interface Tunnel0
ip vrf forwarding TACACS
 ip address 10.1.12.1 255.255.255.0
 tunnel source GigabitEthernet0/0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.48.17.87
 tunnel protection ipsec profile default
!
interface GigabitEthernet0/0/0
 ip address 10.48.23.68 255.255.255.0
 negotiation auto
!
!
ip route 0.0.0.0 0.0.0.0 10.48.23.1
ip tacacs source-interface Loopback0
!
!
tacacs server ISE22_VRF
 address ipv4 10.1.1.2
 key cisco
!
ISR4451#
```

تكوين ESR على ISE

```
ise-esr5921#sh run
Building configuration...

Current configuration : 5778 bytes
!
! Last configuration change at 17:32:58 CET Thu Feb 23 2017
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service call-home
!
hostname ise-esr5921
!
boot-start-marker
boot host unix:default-config
boot-end-marker
!
```

```
!
!
no aaa new-model
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
clock timezone CET 1 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email
address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
 active
 destination transport-method http
 no destination transport-method email
!
!
!
!
!
!
!
!


!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
!
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
 30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
 32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
 6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
 3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
 43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
 526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
 82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
 CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
 1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
 4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
 7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
 68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
```

```
 C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
 C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
 DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
 06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
 4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
 03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
 604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
 D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
 467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
 7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
 5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
 80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
 418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
 D697DF7F 28
       quit
license udi pid CISCO5921-K9 sn 98492083R3X
username lab password 0 lab
!
redundancy
!
!
!
crypto keyring MVPN-spokes
 pre-shared-key address 0.0.0.0 0.0.0.0 key Krakow123
crypto ikev2 authorization policy default
 route set interface
 route set remote ipv4 10.1.1.0 255.255.255.0
!
!
!
crypto ikev2 keyring mykeys
 peer ISR4451
 address 10.48.23.68
 pre-shared-key Krakow123
 !
!
!
crypto ikev2 profile default
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local mykeys
 aaa authorization group psk list default default local
 virtual-template 1
!
!
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 16
!
crypto isakmp policy 20
 encr aes
 hash sha256
 authentication pre-share
 group 14
crypto isakmp key Krakow123 address 0.0.0.0
crypto isakmp profile MVPN-profile
  description LAN-to-LAN for spoke router(s) connection
  keyring MVPN-spokes
  match identity address 0.0.0.0
!
!
```

```
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
 mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
 mode transport
!
!
!
crypto dynamic-map MVPN-dynmap 10
 set transform-set radius radius-2
!
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
!
!
!
!
!
interface Loopback0
 ip address 10.1.12.2 255.255.255.0
!
interface Ethernet0/0
 description e0/0->connection to external NAD
 ip address 10.48.17.87 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 no ip route-cache
 crypto map radius
!
interface Ethernet0/1
 description e0/1->tap0 internal connection to ISE
 ip address 10.1.1.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly in
 no ip route-cache
!
interface Ethernet0/2
 description e0/2->connection to CSSM backend license server
 no ip address
 ip virtual-reassembly in
 no ip route-cache
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
ip nat inside source static tcp 10.1.1.2 49 interface Ethernet0/0 49
ip route 0.0.0.0 0.0.0.0 10.48.17.1
!
```

```
!
!
access-list 1 permit 10.1.1.0 0.0.0.3
!
control-plane
!
 !
 !
 !
 !
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input none
!
!
end
```

اعتبارات تصميم FlexVPN

- في معظم الحالات يجب إنهاء اتصال Radius على واجهة G0/1 ل ISE، والتي هي واجهة E0/0 ل ESR. أثناء إستخدام خرائط التشفير، يجب تعريف حركة المرور المفيدة باستخدام قوائم الوصول، مع SVTI - باستخدام التوجيه. لن يعمل، إذا تم تكوين موجهتين إلى واجهة ISE واحدة عبر النفق (رفشي) وواحدة عبر الواجهة (إنشاء النفق). تنطبق نفس المشكلة على تكوين الموجه.
- ولهذا السبب تم توصيل حركة المرور المشفرة للاتصال (Encrypted Radius) بين واجهة Lo0 للموجه، وواجهة Tap0 ل ISE (لا حاجة إلى nat في هذه الحالة على ESR). ولهذا السبب، يمكن تكوين مسار بروتوكول الإنترنت، لإجبار حركة مرور RADIUS على المرور عبر النفق والحصول على التشفير.
- بما أن عنوان IP الخاص بواجهة Tap0 الخاصة ب ISE ثابت (10.1.1.2)، فيمكن وضعه في VRF على الموجه، لضمان حدوث الاتصال بعنوان IP هذا فقط ل TACACS ومن خلال النفق فقط.

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).