تكوين ISE 2.2 IPSec لتأمين اتصال NAD (ASA)

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين RADIUS IPsec واستكشاف أخطائه وإصلاحها لتأمين اتصال محرك خدمة الهوية (ISE) 2.2 من Cisco - جهاز الوصول إلى الشبكة (NAD). يجب تشفير حركة مرور RADIUS داخل نفق تبادل مفتاح الإنترنت IPSec الإصدار 1 و 2 (IKEv1 و IKEv2) بين جهاز الأمان القابل للتكيف (ASA) و ISE من موقع إلى موقع (LAN-LAN). لا يغطي هذا المستند جزء تكوين AnyConnect SSL VPN.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- محرك خدمات كشف الهوية (ISE)
- ASA من Cisco
- مفاهيم IPSec العامة
- مفاهيم RADIUS العامة

المكونات المستخدمة

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

- Cisco 5515-X Series ASA أن يركض برمجية صيغة 9.4(2)11
- Cisco Identity Service Engine، الإصدار 2.2
- حزمة الخدمة 1 لنظام التشغيل Windows 7

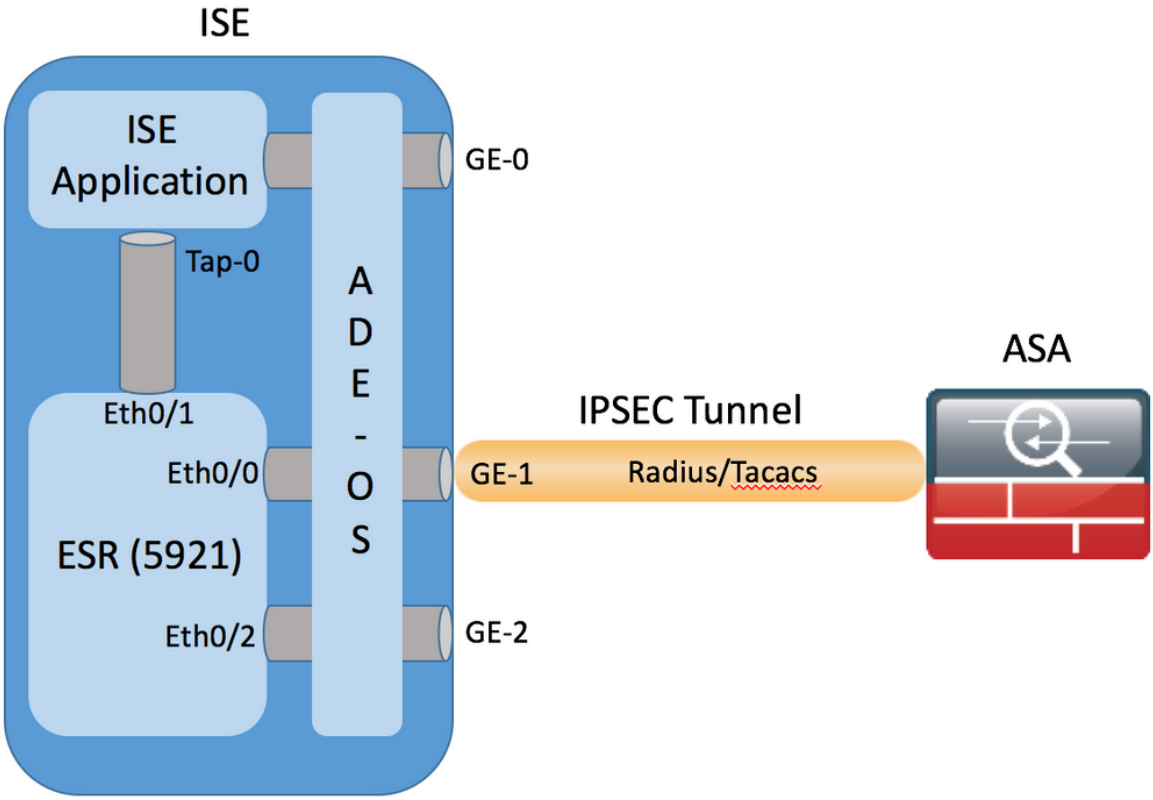
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

والهدف هو تأمين البروتوكولات التي تستخدم تجزئة MD5 غير الآمنة و RADIUS و TACACS مع IPSec. خذ هذا 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 أو إستخدام شهادات X.509 لمصادقة IPSec.
- يمكن تمكين IPSec على ETH1 من خلال واجهات ETH5. أنت يستطيع شكلت IPSec على فقط واحد cisco ISE قارن لكل PSN.

بنية ISE IPSec



بمجرد إستلام الحزم المشفرة بواسطة GE-1 ISE interface ESR واعتراضها على واجهة ETH0/0.

```
interface Ethernet0/0
 description e0/0->connection to external NAD
 ip address 10.48.26.170 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 no ip route-cache
 crypto map radius
```

يقوم ESR بفك تشفيرها ووقوا 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:

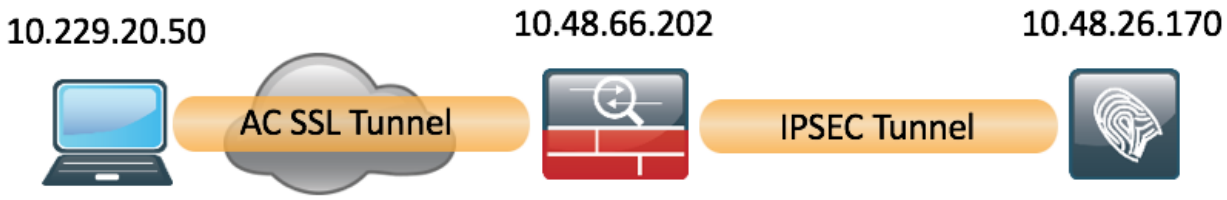
```
ISE22-1ek/admin# show interface | b tap0
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 10.1.1.2  netmask 255.255.255.252  broadcast 10.1.1.3
       inet6 fe80::6c2e:37ff:fe5f:b609  prefixlen 64  scopeid 0x20<link>
       ether 6e:2e:37:5f:b6:09  txqueuelen 500  (Ethernet)
       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
```

التكوين

يوضح هذا القسم كيفية إكمال تكوينات ASA CLI و ISE.

الرسم التخطيطي للشبكة

تستخدم المعلومات الواردة في هذا المستند إعداد الشبكة التالي:



تكوين ASA

تكوين واجهات ASA

إذا لم يتم تكوين واجهة/واجهات ASA، فتأكد من تكوين عنوان IP واسم الواجهة ومستوى الأمان على الأقل:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 100
 ip address 10.48.66.202 255.255.254.0
```

تكوين نهج IKEv1 وتمكين IKEv1 على الواجهة الخارجية

دخلت in order to شكلت الإنترنت أمن اقتران ومفاتيح إدارة بروتوكول (ISAKMP) سياسة ل ال IKEv1 توصيل، ال **crypto ikev1 سياسة <priority>** أمر:

```
crypto ikev1 policy 20
 authentication pre-share
 encryption aes
 hash sha
 group 5
```

```
lifetime 86400
```

ملاحظة: توجد مطابقة لسياسة IKEv1 عندما تحتوي كل النهجين على قيم معلمات Diffie-Hellman و تجزئة والتشفير والمصادقة. بالنسبة ل IKEv1، يجب أيضا أن يحدد نهج النظير البعيد فترة بقاء أقل من أو تساوي فترة البقاء في النهج الذي يرسله البادئ. وإذا كانت فترات الحياة غير متطابقة، يستخدم ASA فترة الحياة الأقصر.

يجب تمكين IKEv1 على الواجهة التي تنهي VPN قفل. بشكل نموذجي، هذه هي الواجهة الخارجية (أو *العامة*). دخلت in order to تمكين IKEv1، **أدخل الأمر crypto ikev1 enable <interface-name>** في وضع التكوين العام:

```
crypto ikev1 enable outside
```

تكوين مجموعة النفق (ملف تعريف اتصال شبكة LAN إلى شبكة LAN)

بالنسبة لأي نفق من شبكة LAN إلى شبكة LAN، يكون هناك ملف تعريف الاتصال وهو *مجموعة النفق-ipSec* تشكيل **IPsec-l2l**. دخلت in order to شكلت ال IKEv1 مفاتيح مدرب، أستعمل الأمر:

```
tunnel-group 10.48.26.170 type ipsec-l2l
tunnel-group 10.48.26.170 ipsec-attributes
 ikev1 pre-shared-key Krakow123
```

تكوين قائمة التحكم في الوصول لحركة مرور VPN ذات الاهتمام

يستخدم ASA قوائم التحكم في الوصول (ACLs) للتمييز بين حركة المرور التي يجب حمايتها باستخدام تشفير IPSec وحركة المرور التي لا تتطلب الحماية. وهو يحمي الحزم التي تطابق إدخالات التحكم في الوصول (ACE) المسموح بها وتضمن أن الحزم الصادرة التي تطابق محرك التحكم في التطبيق (ACE) المسموح به تحتوي على حماية.

```
access-list 101 extended permit ip host 10.48.66.202 host 10.48.26.170
```

ملاحظة: تستخدم قائمة التحكم في الوصول لحركة مرور VPN عناوين IP المصدر والوجهة بعد ترجمة عنوان الشبكة (NAT). حركة المرور الوحيدة المشفرة في هذه الحالة هي حركة مرور البيانات بين ASA و ISE.

تكوين مجموعة تحويل IKEv1

مجموعة تحويل IKEv1 هي مجموعة من بروتوكولات الأمان والخوارزميات التي تحدد الطريقة التي تحمي بها البيانات من خلال ASA. أثناء مفاوضات "اقتران أمان IPSec (SA)"، يجب على مجموعة ASA النظارة تحديد مجموعة تحويل أو اقتراح مماثل لكل من النظارة. ثم يطبق ASA مجموعة التحويل أو الاقتراح المتطابق لإنشاء SA الذي يحمي تدفقات البيانات في قائمة الوصول لخرائط التشفير تلك.

دخلت in order to شكلت ال IKEv1 تحويل مجموعة، **أدخل الأمر crypto ipSec ikev1 transform-set**:

```
crypto ipsec ikev1 transform-set SET2 esp-aes esp-sha-hmac
```

تكوين خريطة تشفير وتطبيقها على واجهة

تحدد خريطة التشفير سياسة IPSec التي سيتم التفاوض عليها في IPSec SA وتتضمن:

- قائمة وصول لتحديد الحزم التي يسمح بها اتصال IPSec وتحميها
- تعريف النظير
- عنوان محلي لحركة مرور IPSec
- مجموعات تحويل IKEv1

فيما يلي مثال:

```
crypto map MAP 20 match address 101
crypto map MAP 20 set peer 10.48.26.170
crypto map MAP 20 set ikev1 transform-set SET2
```

يمكنك بعد ذلك تطبيق خريطة التشفير على الواجهة:

```
crypto map MAP interface outside
```

التكوين النهائي ASA

فيما يلي التكوين النهائي على ASA:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.48.66.202 255.255.254.0
!
!
access-list 101 extended permit ip host 10.48.66.202 host 10.48.26.170
!
crypto ipsec ikev1 transform-set SET2 esp-aes esp-sha-hmac
!
crypto map MAP 20 match address 101
crypto map MAP 20 set peer 10.48.26.170
crypto map MAP 20 set ikev1 transform-set SET2
crypto map MAP interface outside
```

تكوين ISE

تكوين عنوان IP على ISE

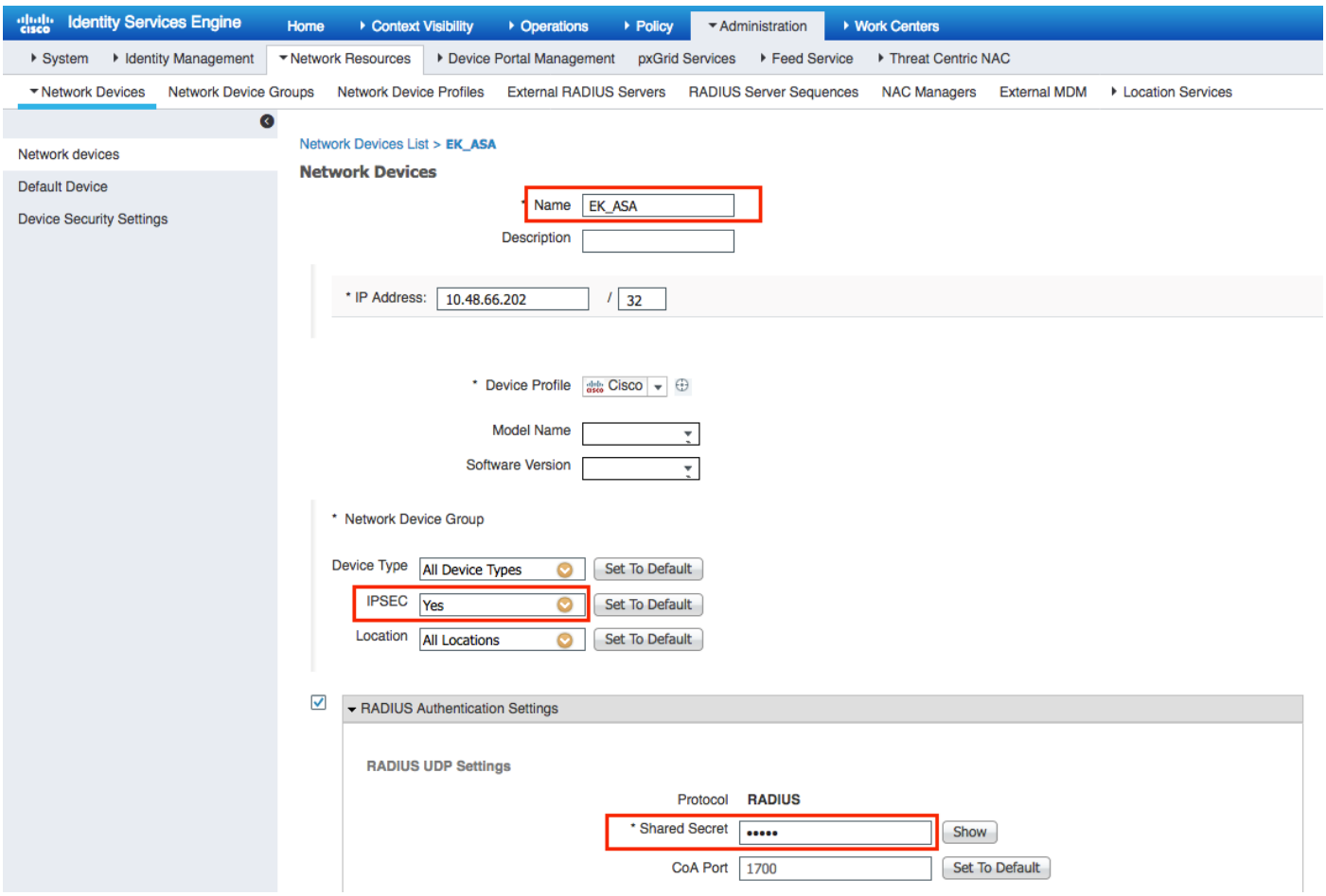
يجب تكوين العنوان على الواجهة ge1-GE5 من واجهة سطر الأوامر، التي تم دعم ge0.

```
interface GigabitEthernet 1
 ip address 10.48.26.170 255.255.255.0
 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 على **إضافة**. تأكد من تكوين الاسم وعنوان IP والسر المشترك. لإنهاء نفق IPSec من NAD، ثم حدد **نعم** مقابل مجموعة أجهزة شبكة IPSec.

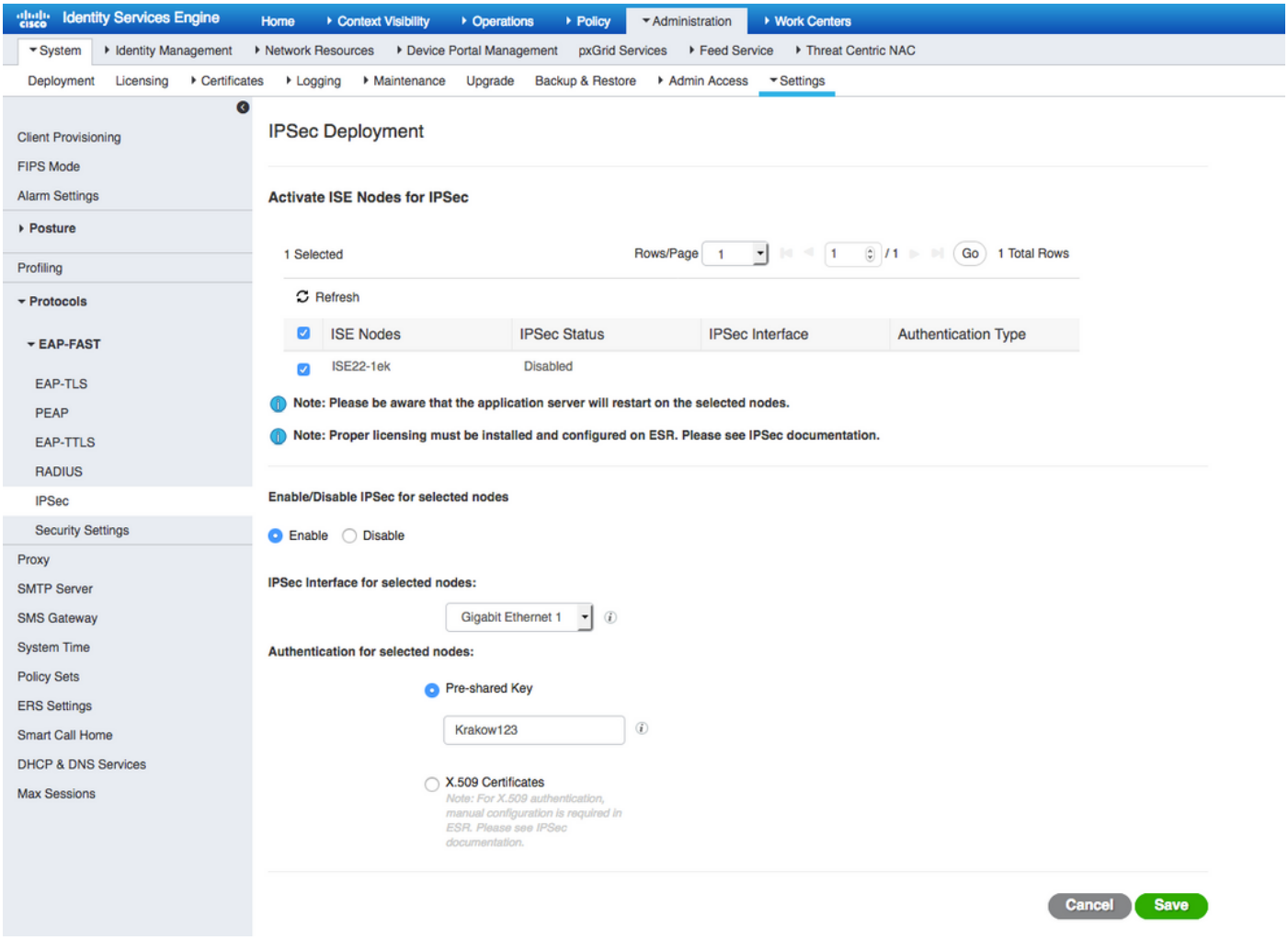


وبمجرد إضافة NAD، يجب إنشاء مسار إضافي على محرك خدمات الهوية (ISE) لضمان مرور بيانات RADIUS عبر محرك أقراص ESR ويتم تشفيرها:

```
ip route 10.48.66.202 255.255.255.255 gateway 10.1.1.1
```

تمكين IPSec على ISE

انتقل إلى **إدارة > نظام > إعدادات**. انقر فوق **Radius** وفوق **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 نوع 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 بتكوين التشفير التالي:

```
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
```

نظرا لأن ASA ال يدعم تجزئة SHA256، يلزم إجراء تكوين إضافي على ESR لمطابقة سياسات IKEv1 للمرحلتين الأولى والثانية من IPsec. تكوين سياسة ISAKMP ومجموعة عمليات التحويل، لمطابقة تلك التي تم تكوينها على ASA:

```
crypto isakmp policy 30
 encr aes
 authentication pre-share
 group 5
!
crypto ipsec transform-set radius-3 esp-aes esp-sha-hmac
 mode tunnel
!
crypto dynamic-map MVPN-dynmap 10
 set transform-set radius radius-2 radius-3
```

تأكد من أن ESR لديه مسار لإرسال الحزم المشفرة:

```
ip route 0.0.0.0 0.0.0.0 10.48.26.1
```

التحقق من الصحة

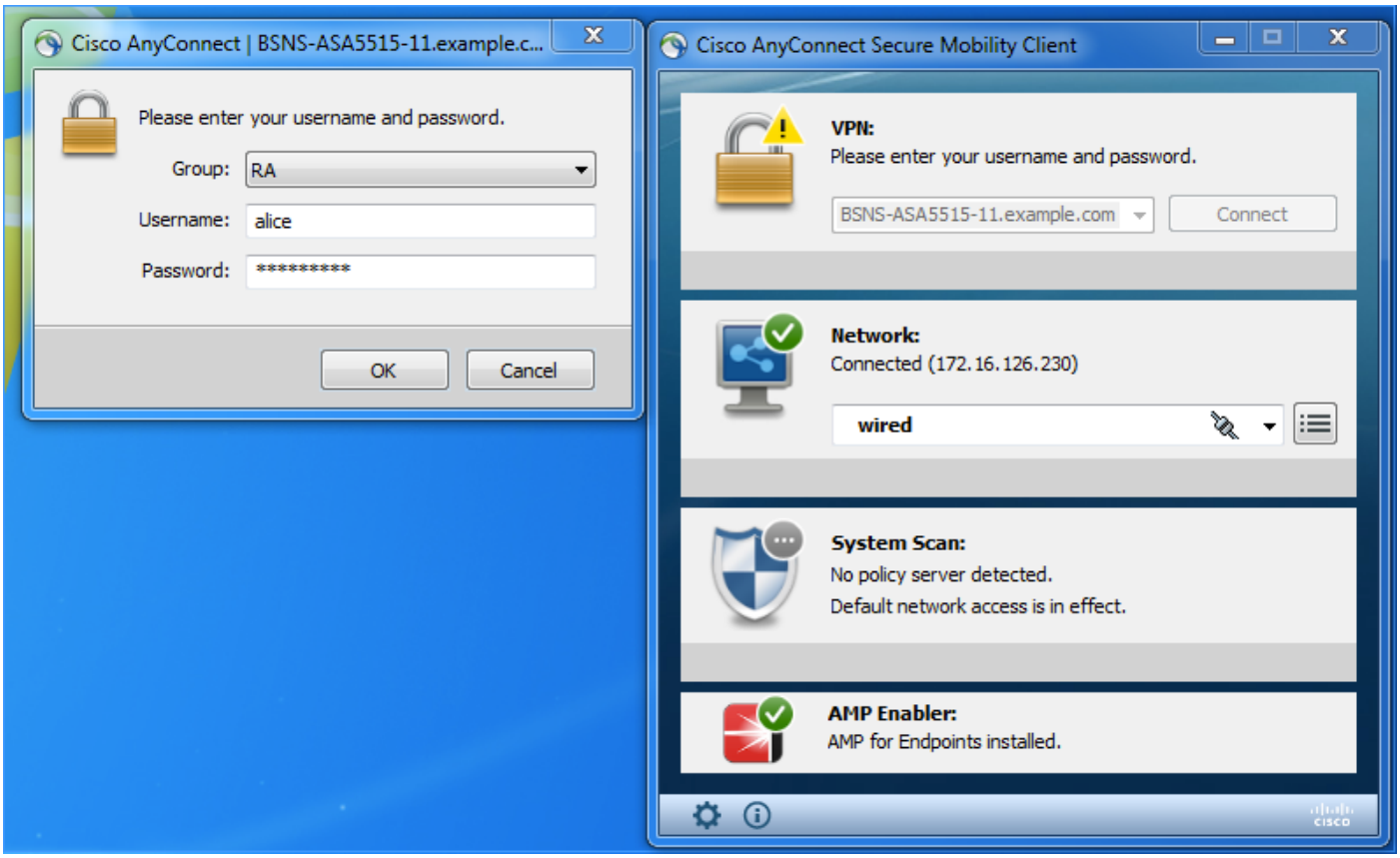
ASA

قبل اتصال عملاء AnyConnect، الذي يحتوي ASA على جلسة تشفير:

```
BSNS-ASA5515-11# sh cry isa sa

There are no IKEv1 SAs
```

```
There are no IKEv2 SAs
BSNS-ASA5515-11# sh cry ipsec sa

There are no ipsec sas
BSNS-ASA5515-11#
```

يتصل العميل عبر عميل AnyConnect VPN، عند إستخدام مصدر مصادقة ISE 2.2.



يرسل ASA حزمة RADIUS، والتي تؤدي إلى تشغيل إنشاء جلسة VPN، ما إن النفق يكون فوق التالي ينتج يرى على ASA ويؤكد أن المرحلة 1 من النفق يكون فوق:

```
BSNS-ASA5515-11# sh cry isa sa

IKEv1 SAs:

  Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 10.48.26.170
   Type    : L2L             Role    : initiator
   Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
BSNS-ASA5515-11#
```

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

```
BSNS-ASA5515-11# sh cry ipsec sa
interface: outside
   Crypto map tag: MAP, seq num: 20, local addr: 10.48.66.202

     access-list 101 extended permit ip host 10.48.66.202 host 10.48.26.170
```

```
      local ident (addr/mask/prot/port): (10.48.66.202/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port): (10.48.26.170/255.255.255.255/0/0)
      current_peer: 10.48.26.170


      #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
      #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.48.66.202/0, remote crypto endpt.: 10.48.26.170/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 5BBE9F07
      current inbound spi : 068C04D1

   inbound esp sas:
     spi: 0x068C04D1 (109839569)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 323584, crypto-map: MAP
        sa timing: remaining key lifetime (kB/sec): (4373999/3558)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x0000003F
   outbound esp sas:
     spi: 0x5BBE9F07 (1539219207)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 323584, crypto-map: MAP
        sa timing: remaining key lifetime (kB/sec): (4373999/3558)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

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
10.48.26.170    10.48.66.202    QM_IDLE           1012 ACTIVE MVPN-profile

IPv6 Crypto ISAKMP SA

ise-esr5921#
```

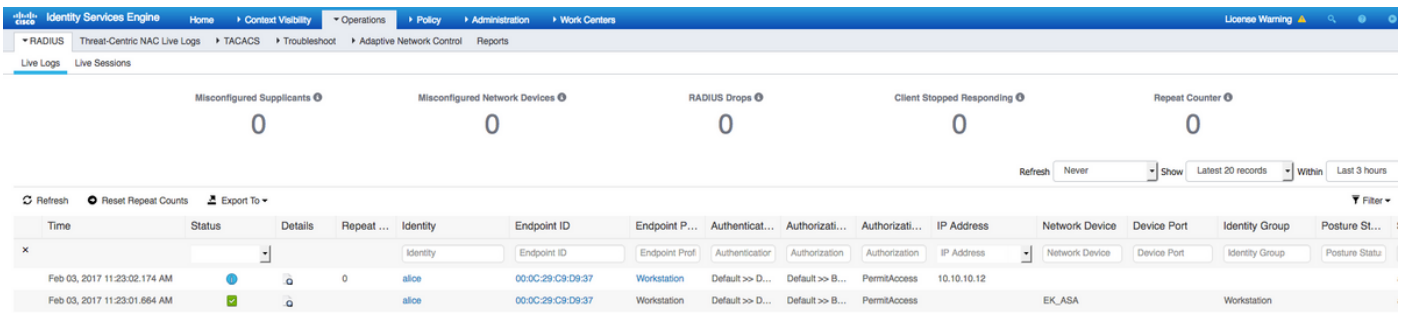
تكون المرحلة 2 قيد التشغيل، ويتم تشفير الحزم وفك تشفيرها بنجاح:

```
ise-esr5921#sh cry ipsec sa

interface: Ethernet0/0
```

```
 Crypto map tag: radius, local addr 10.48.26.170

protected vrf: (none)
local  ident (addr/mask/prot/port): (10.48.26.170/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.48.66.202/255.255.255.255/0/0)
current_peer 10.48.66.202 port 500
  PERMIT, flags={}
 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
 #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.: 10.48.26.170, remote crypto endpt.: 10.48.66.202
  plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
  current outbound spi: 0x68C04D1(109839569)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
   spi: 0x5BBE9F07(1539219207)
     transform: esp-aes esp-sha-hmac ,
     in use settings ={Tunnel, }
     conn id: 31, flow_id: SW:31, sibling_flags 80000040, crypto map: radius
     sa timing: remaining key lifetime (k/sec): (4259397/3508)
     IV size: 16 bytes
     replay detection support: Y
     Status: ACTIVE(ACTIVE)

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0x68C04D1(109839569)
     transform: esp-aes esp-sha-hmac ,
     in use settings ={Tunnel, }
     conn id: 32, flow_id: SW:32, sibling_flags 80000040, crypto map: radius
     sa timing: remaining key lifetime (k/sec): (4259397/3508)
     IV size: 16 bytes
     replay detection support: Y
     Status: ACTIVE(ACTIVE)

  outbound ah sas:

  outbound pcp sas:
```

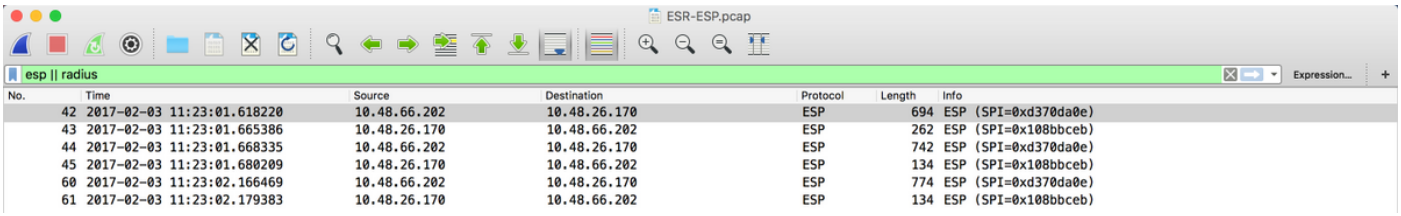
محرك خدمات كشف الهوية (ISE)

تشير المصادقة المباشرة إلى مصادقة PAP_ASCII العادية:

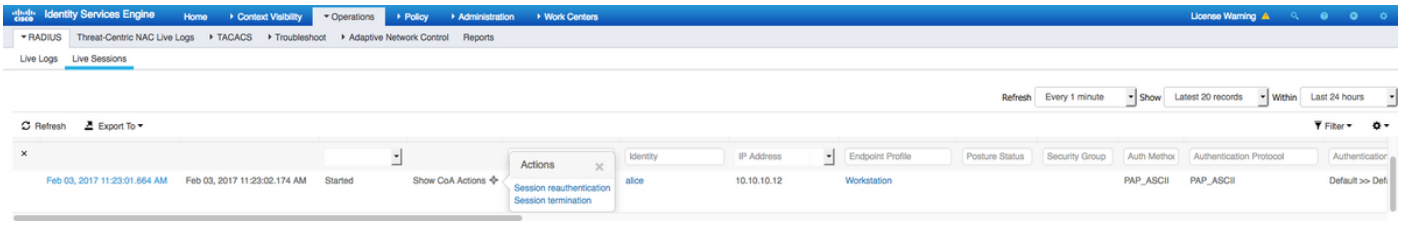


عمليات الالتقاط التي تم التقاطها على واجهة GE1 من ISE والتي تمت تصفيتها

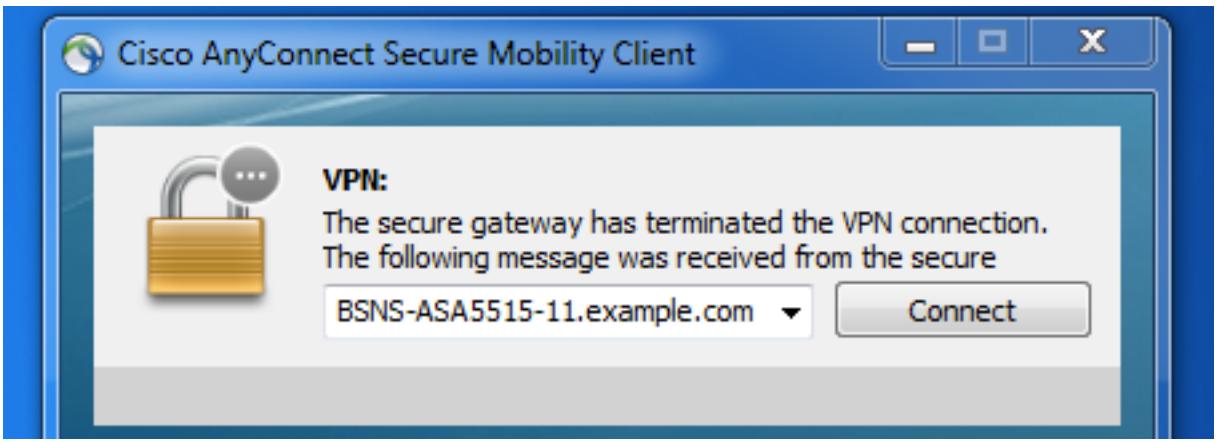
باستخدام ESP أو RADIUS، تؤكد أن ال يوجد RADIUS في نص واضح، ويتم تشفير جميع حركات مرور البيانات:



من الممكن أيضا إرسال حزم مشفرة من ISE - تغيير التفويض (CoA) - بمجرد تشغيل النفق:



في هذا المثال، تم إصدار إنهاء جلسة العمل، ونتيجة لذلك تم قطع اتصال عميل VPN:



استكشاف الأخطاء وإصلاحها

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

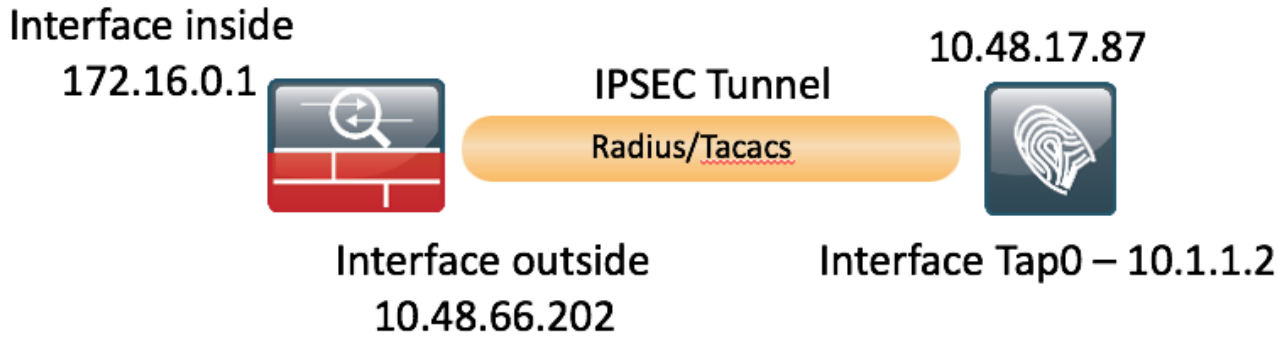
عمليات تصحيح أخطاء IOS IKEv2 لشبكة VPN من موقع إلى موقع مع PSKs أستكشاف أخطاء وإصلاحها TechNote

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 FlexVPN (DVTI إلى خريطة التشفير) بين NAD و ISE 2.2

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



تكوين FlexVPN مستقيم إلى الأمام. يمكن العثور على مزيد من التفاصيل هنا:

http://www.cisco.com/c/en/us/support/docs/security/flexvpn/116008-flexvpn-nge-config-00.html

تكوين ASA

```
hostname BSNS-ASA5515-11
domain-name example.com

ip local pool POOL 10.10.10.10-10.10.10.100 mask 255.255.255.0
!
interface GigabitEthernet0/0
 nameif outside
 security-level 100
 ip address 10.48.66.202 255.255.254.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.0.1 255.255.255.0
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network POOL
 subnet 10.10.10.0 255.255.255.0
object network ISE
 host 10.48.17.86
object network ISE22
 host 10.1.1.2
object network INSIDE-NET
 subnet 172.16.0.0 255.255.0.0
access-list 101 extended permit ip host 172.16.0.1 host 10.1.1.2
access-list OUT extended permit ip any any
nat (inside,outside) source static INSIDE-NET INSIDE-NET destination static ISE22 ISE22
nat (outside,outside) source dynamic POOL interface
nat (inside,outside) source dynamic any interface
access-group OUT in interface outside
route outside 0.0.0.0 0.0.0.0 10.48.66.1 1

aaa-server ISE22 protocol radius
 authorize-only
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE22 (inside) host 10.1.1.2
 key *****
```

```
crypto ipsec ikev2 ipsec-proposal SET
 protocol esp encryption aes
 protocol esp integrity sha-1
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map DMAP 1 set ikev1 transform-set SET
crypto map MAP 10 ipsec-isakmp dynamic DMAP
crypto map MAP 20 match address 101
crypto map MAP 20 set peer 10.48.17.87
crypto map MAP 20 set ikev2 ipsec-proposal SET
crypto map MAP interface outside
crypto ikev2 policy 10
 encryption aes
 integrity sha256
 group 2
 prf sha256
 lifetime seconds 86400
crypto ikev2 enable outside
management-access inside
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-4.4.00243-webdeploy-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 error-recovery disable
group-policy GP-SSL internal
group-policy GP-SSL attributes
 vpn-tunnel-protocol ssl-client
tunnel-group RA type remote-access
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group ISE22
 accounting-server-group ISE22
 default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
 group-alias RA enable
tunnel-group 10.48.17.87 type ipsec-l2l
tunnel-group 10.48.17.87 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

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

- يتم إنشاء نفق VPN باستخدام DVTI على ESR بجانب ASA وخريطة التشفير على ASA، مع قدرة التكوين أعلى ASA على إنشاء حزمة RADIUS التي تم إنشاؤها من الواجهة الداخلية، والتي ستضمن قائمة الوصول الصحيحة للتشفير لتشغيل إنشاء جلسة VPN.
- لاحظ أنه في هذه الحالة يجب تعريف ASA NAD على ISE مع عنوان IP للواجهة الداخلية.

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).