Konfigurieren von ISE 2.2 IPSEC zur sicheren NAD-Kommunikation (ASA)

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie RADIUS IPSEC zur Sicherung der Kommunikation mit der Cisco Identity Service Engine (ISE) 2.2 - Network Access Device (NAD) konfiguriert und Fehler behoben werden. Der RADIUS-Datenverkehr muss innerhalb des Site-to-Site (LAN-to-LAN) IPSec Internet Key Exchange Version 1 und 2 (IKEv1 und IKEv2)-Tunnels zwischen Adaptive Security Appliance (ASA) und ISE verschlüsselt werden. Dieses Dokument behandelt nicht den Konfigurationsteil für AnyConnect SSL VPN.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- ISE
- Cisco ASA
- Allgemeine IPSec-Konzepte
- Allgemeine RADIUS-Konzepte

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ASA der Serie 5515-X mit Softwareversion 9.4(2)11
- Cisco Identity Service Engine Version 2.2
- Windows 7 Service Pack 1

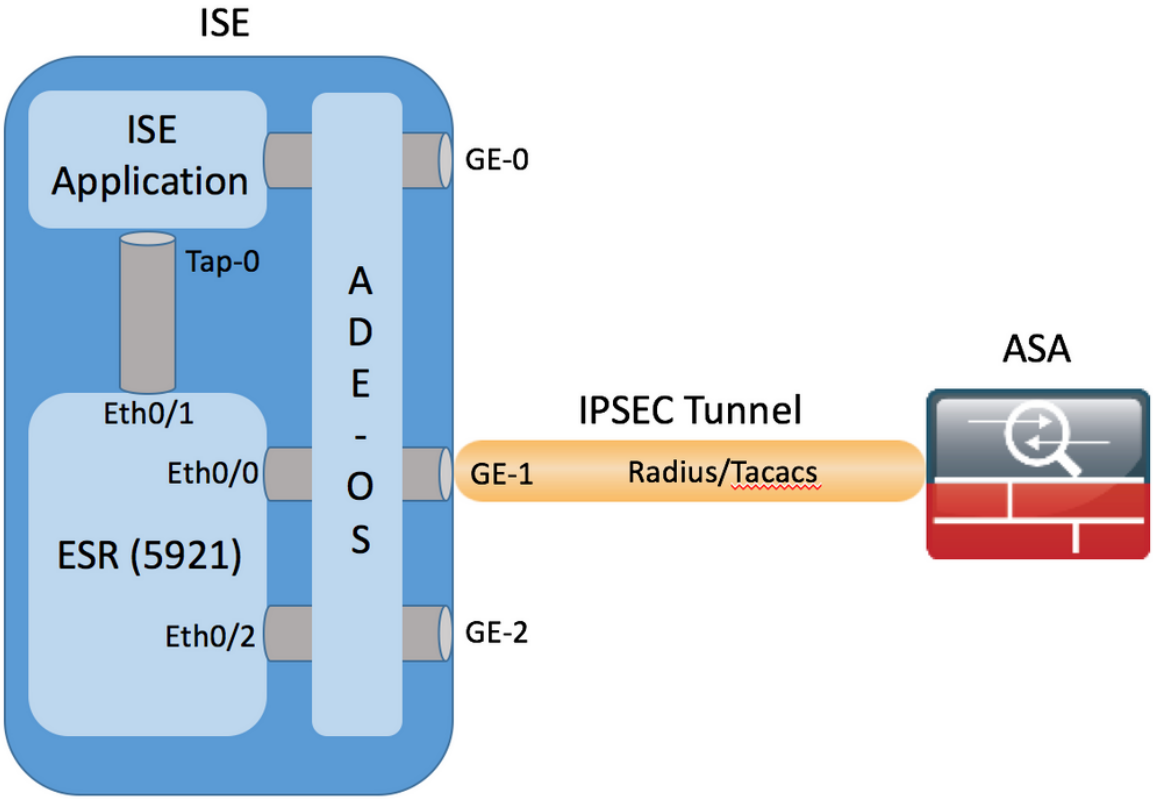
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Ziel ist es, Protokolle zu sichern, die unsichere MD5-Hash-, Radius- und TACACS-Protokolle mit IPSec verwenden. Berücksichtigen Sie dabei Folgendes:

- Die Cisco ISE unterstützt IPSec im Tunnel- und Transportmodus.
- Wenn Sie IPSec auf einer Cisco ISE-Schnittstelle aktivieren, wird zwischen der Cisco ISE und der NAD ein IPSec-Tunnel erstellt, um die Kommunikation zu sichern.
- Sie können einen vorinstallierten Schlüssel definieren oder X.509-Zertifikate für die IPSec-Authentifizierung verwenden.
- IPSec kann an Eth1- bis Eth5-Schnittstellen aktiviert werden. Sie können IPSec auf nur einer Cisco ISE-Schnittstelle pro PSN konfigurieren.

ISE IPSec-Architektur



Sobald verschlüsselte Pakete von der GE-1 ISE-Schnittstelle empfangen werden, werden sie vom ESR auf der Eth0/0-Schnittstelle abgefangen.

```
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
```

ESR entschlüsselt sie und führt die Adressumwandlung gemäß vorkonfigurierten NAT-Regeln durch. Ausgehende RADIUS-/TACACS-Pakete (in Richtung NAD) werden in Ethernet0/0-Schnittstellenadresse umgewandelt und anschließend verschlüsselt.

```
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
```

Pakete, die für eine Eth0/0-Schnittstelle an RADIUS/TACACS-Ports bestimmt sind, sollten über die Eth0/1-Schnittstelle an die interne Adresse der ISE, die 10.1.1.2-IP-Adresse, weitergeleitet werden. ESR-Konfiguration von 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
```

ISE-Konfiguration der internen Tap-0-Schnittstelle:

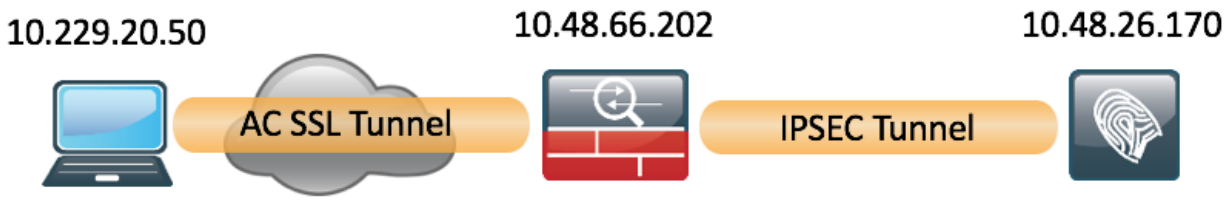
```
ISE22-1ek/admin# show interface | b tap0
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 10.1.1.2  netmask 255.255.255.252  broadcast 10.1.1.3
       inet6 fe80::6c2e:37ff:fe5f:b609  prefixlen 64  scopeid 0x20<link>
       ether 6e:2e:37:5f:b6:09  txqueuelen 500  (Ethernet)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

Konfigurieren

In diesem Abschnitt wird beschrieben, wie die ASA CLI- und ISE-Konfigurationen abgeschlossen werden.

Netzwerkdiagramm

Die Informationen in diesem Dokument verwenden die folgende Netzwerkeinrichtung:



ASA-Konfiguration

Konfigurieren der ASA-Schnittstellen

Wenn die ASA-Schnittstelle bzw. -Schnittstellen nicht konfiguriert sind, stellen Sie sicher, dass Sie mindestens die IP-Adresse, den Schnittstellennamen und die Sicherheitsstufe konfigurieren:

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

Konfigurieren der IKEv1-Richtlinie und Aktivieren von IKEv1 an der externen Schnittstelle

Um die Internet Security Association and Key Management Protocol (ISAKMP)-Richtlinien für die IKEv1-Verbindungen zu konfigurieren, geben Sie den **Befehl crypto ikev1 policy <priority>** ein:

```
crypto ikev1 policy 20
 authentication pre-share
 encryption aes
 hash sha
 group 5
 lifetime 86400
```

> **Hinweis:** Eine Übereinstimmung der IKEv1-Richtlinien ist vorhanden, wenn beide Richtlinien der beiden Peers dieselben Parameterwerte für Authentifizierung, Verschlüsselung, Hash und Diffie-Hellman enthalten. Für IKEv1 muss die Remote-Peer-Richtlinie in der Richtlinie, die der Initiator sendet, auch eine Lebensdauer unter oder gleich der Lebensdauer angeben. Wenn die Lebensdauer nicht identisch ist, verwendet die ASA die kürzere Lebensdauer.

Sie müssen IKEv1 auf der Schnittstelle aktivieren, die den VPN-Tunnel terminiert. In der Regel handelt es sich hierbei um die externe (oder *öffentliche*) Schnittstelle. Um IKEv1 zu aktivieren, geben Sie den Befehl **crypto ikev1 enable**<interface-name> im globalen Konfigurationsmodus ein:

```
crypto ikev1 enable outside
```

Konfigurieren der Tunnelgruppe (LAN-zu-LAN-Verbindungsprofil)

Bei einem LAN-zu-LAN-Tunnel ist der Verbindungsprofiltyp **ipsec-l2l**. Um den vorinstallierten IKEv1-Schlüssel zu konfigurieren, geben Sie den Konfigurationsmodus *tunnel-group ipsec-attribute ein*:

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

Konfigurieren der ACL für den VPN-Datenverkehr von Interesse

Die ASA verwendet Zugriffskontrolllisten (ACLs), um den Datenverkehr, der mit IPSec-Verschlüsselung geschützt werden soll, von dem Datenverkehr zu unterscheiden, der keinen Schutz erfordert. Sie schützt die ausgehenden Pakete, die mit einer zugelassenen Application Control Engine (ACE) übereinstimmen, und stellt sicher, dass die eingehenden Pakete, die einem ACE entsprechen, geschützt sind.

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

> **Hinweis:** Eine ACL für VPN-Datenverkehr verwendet die Quell- und Ziel-IP-Adressen nach Network Address Translation (NAT). Der einzige verschlüsselte Datenverkehr ist in diesem Fall der Datenverkehr zwischen ASA und ISE.

Konfigurieren des IKEv1-Transformationssatzes

Ein IKEv1-Transformationssatz ist eine Kombination aus Sicherheitsprotokollen und Algorithmen, die festlegen, wie die ASA Daten schützt. Bei Verhandlungen mit der IPSec Security Association (SA) müssen die Peers einen Transformationssatz oder einen Transformationsvorschlag identifizieren, der für beide Peers gleich ist. Die ASA wendet dann den übereinstimmenden Transformationssatz oder das zugehörige Angebot an, um eine SA zu erstellen, die die Datenflüsse in der Zugriffsliste für diese Crypto Map schützt.

Um den IKEv1-Transformationssatz zu konfigurieren, geben Sie den Befehl **crypto ipsec ikev1 transformation-set ein**:

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

Konfigurieren einer Kryptozuordnung und Anwenden auf eine Schnittstelle

Eine Crypto Map definiert eine IPSec-Richtlinie, die in der IPSec SA ausgehandelt wird, und umfasst Folgendes:

- Eine Zugriffsliste, um die Pakete zu identifizieren, die die IPSec-Verbindung zulässt und schützt.
- Peer-Identifizierung
- Eine lokale Adresse für den IPSec-Datenverkehr
- Die IKEv1-Transformationssätze

Hier ein Beispiel:

```
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
```

Sie können dann die Crypto Map auf die Schnittstelle anwenden:

```
crypto map MAP interface outside
```

ASA - Endgültige Konfiguration

Die endgültige Konfiguration für die ASA ist wie folgt:

```
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
```

ISE-Konfiguration

Konfigurieren der IP-Adresse für die ISE

Die Adresse muss auf der Schnittstelle GE1-GE5 von der CLI konfiguriert werden. GE0 wird nicht unterstützt.

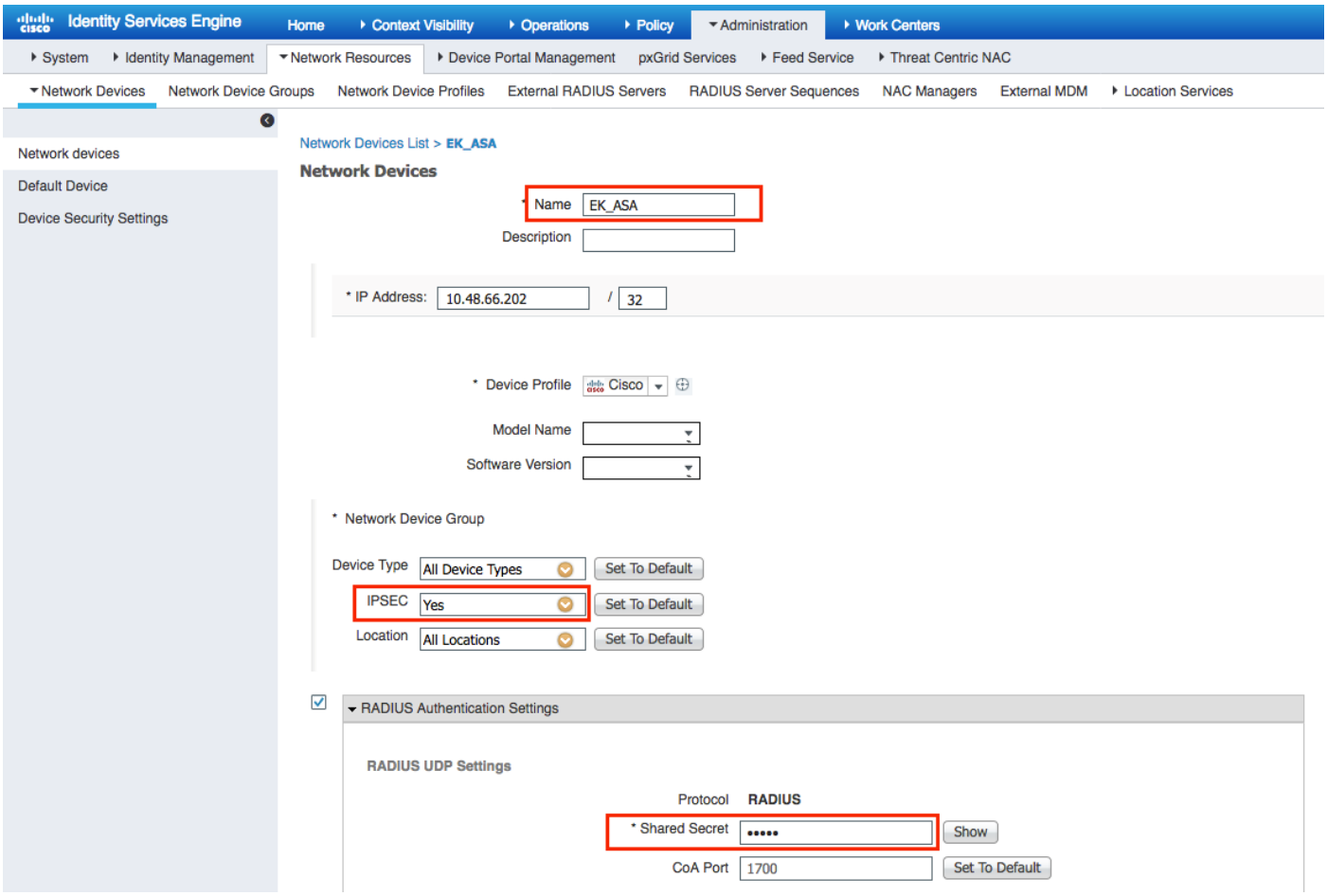
```
interface GigabitEthernet 1
```

```
ip address 10.48.26.170 255.255.255.0
ipv6 address autoconfig
ipv6 enable
```

Hinweis: Die Anwendung wird neu gestartet, nachdem die IP-Adresse auf der Schnittstelle konfiguriert wurde:
% Durch Ändern der IP-Adresse können ISE-Services neu gestartet werden.
Fahren Sie mit der Änderung der IP-Adresse fort? J/N [N]: J

Hinzufügen von NAD zur IPSec Group auf der ISE

Navigieren Sie zu **Administration > Network Resources > Network Devices**. Klicken Sie auf **Hinzufügen**. Stellen Sie sicher, dass der Name, die IP-Adresse und der gemeinsame geheime Schlüssel konfiguriert sind. Um den IPSec-Tunnel von der NAD zu beenden, wählen Sie **JA** gegen die IPSEC-Netzwerkgerätegruppe aus.



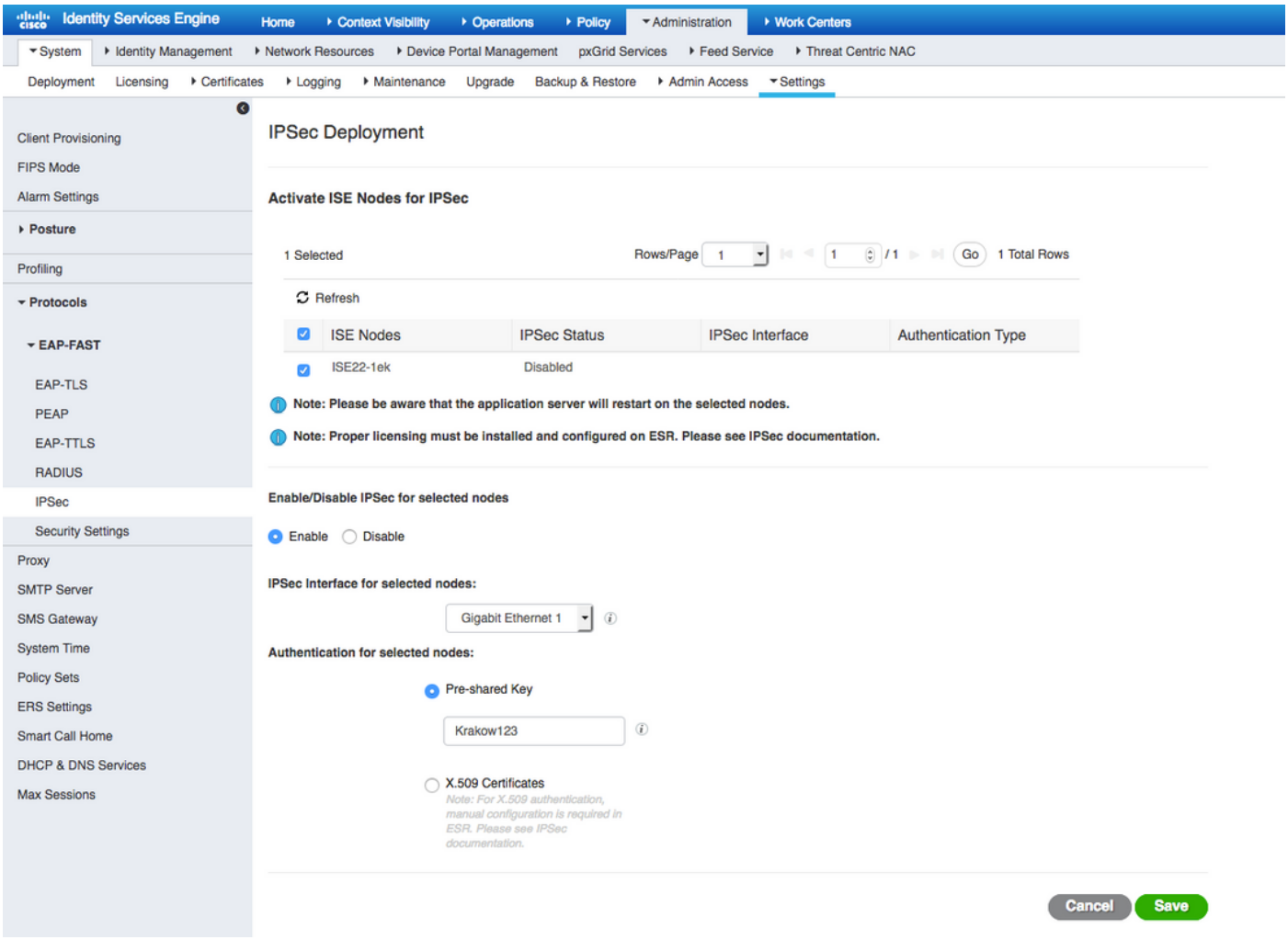
Nach dem Hinzufügen der NAD sollte auf der ISE eine zusätzliche Route erstellt werden, um sicherzustellen, dass der RADIUS-Datenverkehr den ESR durchläuft und verschlüsselt wird:

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

IPSEC auf ISE aktivieren

Navigieren Sie zu **Administration > System > Settings**. Klicken Sie auf **Radius** und weiter auf **IPSEC**. Wählen Sie PSN (Single/Multiple/All) aus, wählen Sie Enable (Aktivieren) aus, wählen Sie

Interface (Schnittstelle) und Select Authentication Method (Authentifizierungsverfahren auswählen) aus. Klicken Sie auf **Speichern**. Dienste werden zu diesem Zeitpunkt auf dem ausgewählten Knoten neu gestartet.



Beachten Sie, dass nach dem Neustart der Services die ISE-CLI-Konfiguration eine konfigurierte Schnittstelle ohne IP-Adresse und einen deaktivierten Zustand anzeigt, da der ESR (Embedded Services Router) die Kontrolle über die ISE-Schnittstelle übernimmt.

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

Nach dem Neustart der Services wird die ESR-Funktionalität aktiviert. Um sich bei ESR anzumelden, geben Sie esr in die Befehlszeile ein:

```
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#
```

ESR wird mit der folgenden Verschlüsselungskonfiguration geliefert:

```
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
```

Da die ASA die sha256-Hashing-Abstimmung nicht unterstützt, ist eine zusätzliche Konfiguration des ESR erforderlich, um die IKEv1-Richtlinien für die 1. und 2. Phase von IPSEC zu erfüllen. Konfigurieren Sie die isakmp-Richtlinie und den Transformationssatz, um die auf der ASA konfigurierten zu erfüllen:

```
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
```

Stellen Sie sicher, dass die ESR über eine Route zum Senden verschlüsselter Pakete verfügt:

```
ip route 0.0.0.0 0.0.0.0 10.48.26.1
```

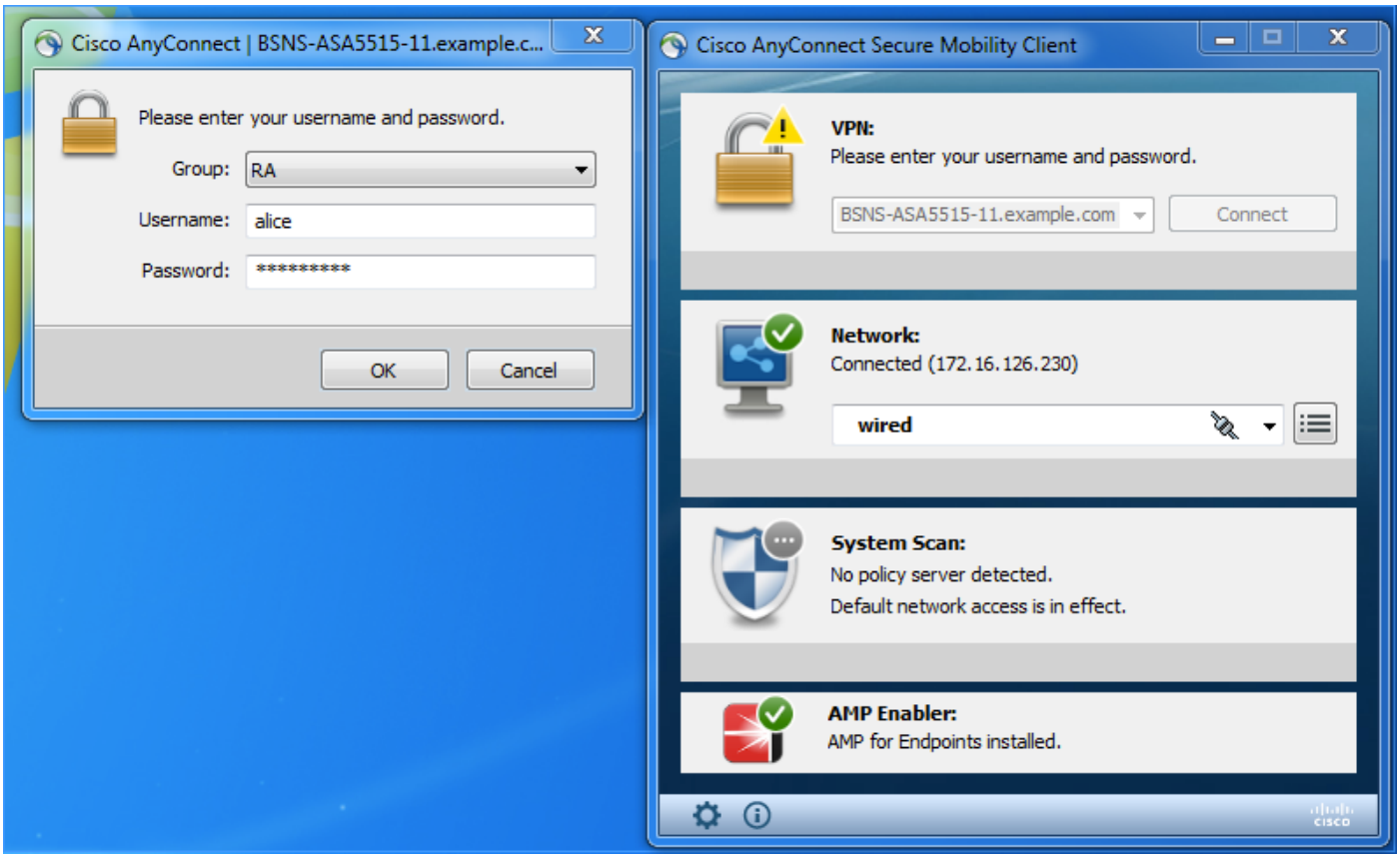
Überprüfen

ASA

Bevor AnyConnect-Clients eine Verbindung herstellen, hat die ASA keine Krypto-Sitzung:

```
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#
```

Der Client stellt über den AnyConnect VPN-Client eine Verbindung her, da ISE 2.2 als Authentifizierungsquelle verwendet wird.



ASA sendet ein Radius-Paket, das die Einrichtung von VPN-Sitzungen auslöst, sobald der Tunnel aktiv ist, die folgende Ausgabe auf der ASA angezeigt wird und bestätigt, dass Phase 1 des Tunnels aktiv ist:

```
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#
```

Phase 2 ist aktiv, und die Pakete werden verschlüsselt und entschlüsselt:

```
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

Die gleichen Ausgaben können für ESR überprüft werden, Phase 1 ist aktiv:

```
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
```

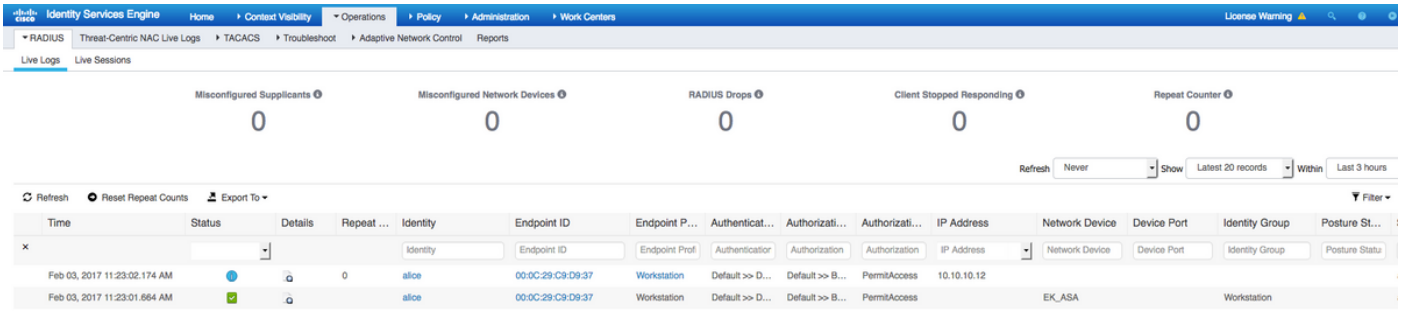
```
ise-esr5921#
```

Phase 2 ist aktiv, Pakete werden verschlüsselt und erfolgreich entschlüsselt:

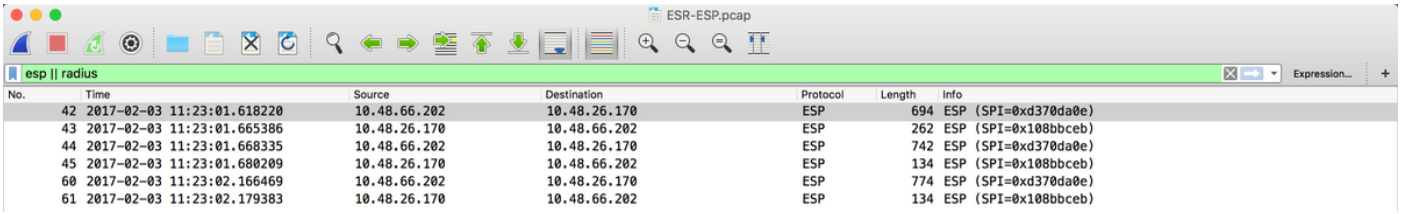
```
ise-esr5921#sh cry ipsec sa

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:
```

ISE

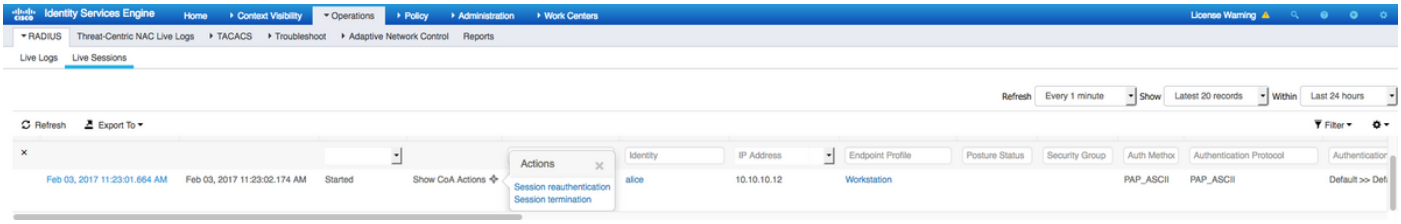
Die Live-Authentifizierung bezeichnet die reguläre PAP_ASCII-Authentifizierung:



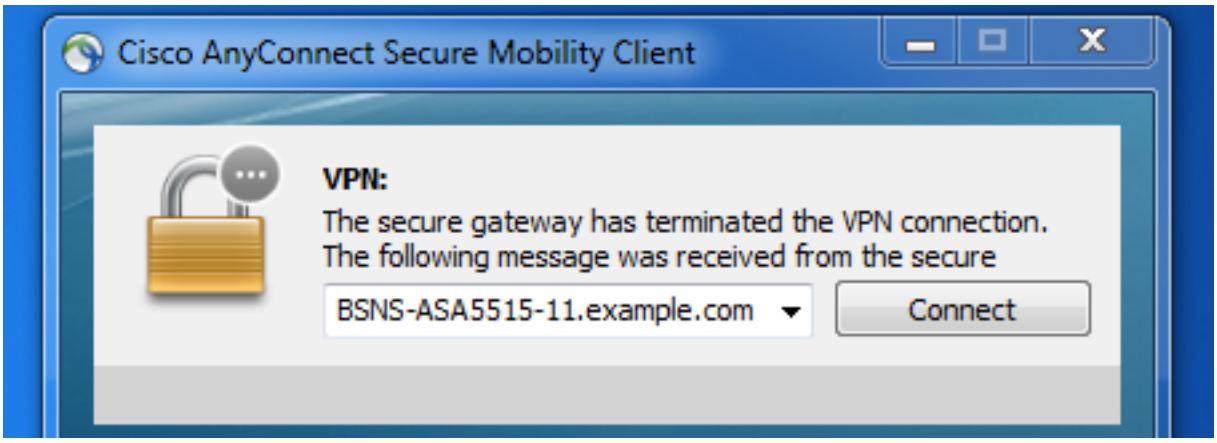
In GE1-Schnittstellen der ISE erfasste und mit ESP oder Radius gefilterte Aufnahmen bestätigen, dass kein Radius im Klartext vorhanden ist und der gesamte Datenverkehr verschlüsselt ist:



Es ist auch möglich, verschlüsselte Pakete von der ISE - Change of Authorization (CoA) - zu senden, sobald der Tunnel betriebsbereit ist:



In diesem Beispiel wurde die Sitzungsbeendigung ausgegeben, und der VPN-Client wurde getrennt. Dies hatte zur Folge:



Fehlerbehebung

Zur Fehlerbehebung bei IPSEC-Problemen kann eine gängige VPN-Fehlerbehebungstechnik verwendet werden. Nachstehend finden Sie hilfreiche Dokumente:

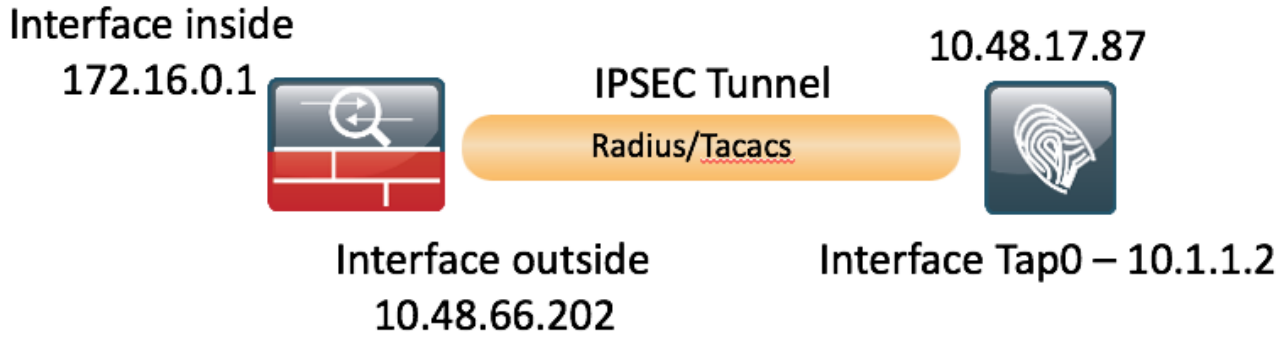
[IOS IKEv2 Debugs für Site-to-Site-VPN mit PSKs Fehlerbehebung Technischer Hinweis]

[ASA IKEv2 Debugs für Site-to-Site-VPN mit PSKs]

[IPsec-Fehlerbehebung: Verwenden von Debugbefehlen]

Konfigurieren von FlexVPN Site-to-Site (DVTI zu Crypto Map) zwischen NAD und ISE 2.2

RADIUS-Datenverkehr kann auch mit FlexVPN geschützt werden. Im folgenden Beispiel wird die folgende Topologie verwendet:



Die FlexVPN-Konfiguration ist sofort einsatzbereit. Weitere Informationen finden Sie hier:

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

ASA-Konfiguration

```
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 *****
```

ESR-Konfiguration auf 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
```

Überlegungen zum FlexVPN-Design

- Der VPN-Tunnel wird mithilfe von DVTI auf der ESR-Seite und Crypto Map auf der ASA-Seite erstellt. Die oben angegebene Konfiguration ermöglicht die Generierung des Radius-Pakets, das von der internen Schnittstelle stammt. Dadurch wird sichergestellt, dass die richtige Zugriffsliste für die Verschlüsselung erstellt wird, um die Einrichtung von VPN-Sitzungen auszulösen.
- Beachten Sie, dass in diesem Fall ASA NAD auf ISE mit interner Schnittstellen-IP-Adresse definiert werden sollte.