ISE Posture met FlexVPN configureren

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren Netwerkdiagram Configuratie DNS-server IOS XE initiële configuratie Identiteitsbewijs configureren IKEv2 configureren AnyConnect-configuratie van clientprofiel **ISE-configuratie** Configuratie van beheers- en CPP-certificaten Een lokale gebruiker op ISE maken Voeg de FlexVPN-HUB toe als een RADIUS-client Configuratie van clientprovisioning Postbeleid en -voorwaarden Clientprovisioningportal configureren Verificatieprofielen en -beleid configureren Verifiëren Problemen oplossen

Inleiding

Dit document geeft een voorbeeld van hoe u een IOS XE head-end voor toegang op afstand kunt configureren met een houding waarbij AnyConnect IKEv2 en EAP-Message Digest 5 (EAP-MD5) verificatiemethode wordt gebruikt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FlexVPN Remote Access (RA) VPN-configuratie op IOS XE
- AnyConnect-clientconfiguratie (AC)
- Poststroom op Identity Services Engine (ISE) 2.2 en hoger
- Configuratie van posteringscomponenten op ISE
- Configuratie van DNS-server op Windows Server 2008 R2

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco CSR 1000V-router met IOS XE 16.8 [Fuji]
- AnyConnect-clientversie 4.5.030/40, actief op Windows 7
- Cisco ISE 2.3
- Windows 2008 R2-server

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Om te verzekeren dat de opgelegde maatregelen van de netwerkveiligheid relevant en effectief blijven, staat Cisco ISE u toe om veiligheidsmogelijkheden op om het even welke clientmachine te valideren en te onderhouden die het beschermde netwerk betreden. Door gebruik te maken van postbeleid dat is ontworpen om te verzekeren dat de meest up-to-date beveiligingsinstellingen of toepassingen beschikbaar zijn op clientmachines, kan de Cisco ISE-beheerder ervoor zorgen dat elke client-machine die toegang heeft tot het netwerk voldoet aan de gedefinieerde beveiligingsnormen voor netwerktoegang en blijft voldoen aan deze normen. De rapporten over de naleving van de Post bieden Cisco ISE een momentopname van het nalevingsniveau van de clientmachine op het moment van inloggen van de gebruiker, evenals elke keer dat er een periodieke herbeoordeling plaatsvindt.

De post kan worden vertegenwoordigd door drie hoofdelementen:

- 1. ISE als een beleidsconfiguratiedistributie en besluitvormingspunt. Vanuit het oogpunt van de beheerder van ISE, vormt u posteringsbeleid (aan welke precieze voorwaarden moet worden voldaan om een apparaat aan te merken als een bedrijfsconforme), het leveringsbeleid van de cliënt (welke software van de agent moet worden geïnstalleerd op welk soort apparaten) en het autorisatiebeleid (aan welke rechten moet worden toegekend, hangt af van hun posterstatus).
- 2. Network Access device (NAD) als beleidshandhavingspunt. Aan de NAD-zijde worden werkelijke autorisatiebeperkingen toegepast op het moment van gebruikersverificatie. ISE als beleidspunt biedt vergunningparameters zoals toegangscontrolelijst (ACL). Traditioneel worden, om positie te kunnen innemen, NAD's verplicht om verandering van autorisatie (CoA) te ondersteunen om de gebruiker na de status van het eindpunt opnieuw te authentiseren. Om te beginnen met ISE 2.2 NAD's zijn niet vereist om omleiding te ondersteunen.

Opmerking: Routers die IOS XE uitvoeren ondersteunen omleiding niet. Opmerking: IOS XEsoftware moet voorzien zijn van oplossingen voor de volgende defecten om CoA met ISE volledig operationeel te maken:

CSCve16269 IKEv2 CoA werkt niet met ISE

CSCvi90729 IKEv2 CoA werkt niet met ISE (cacaodruk=TRUE in plaats van waar) 3. Agent-software als punt van gegevensverzameling en interactie met eindgebruiker. Agent

ontvangt informatie over postvereisten van ISE en verstrekt rapport aan ISE over de status

van vereisten. Dit document is gebaseerd op AnyConnect ISE Posture Module die de enige is die houding volledig ondersteunt zonder omleiding.

Postflow zonder omleiding is zeer goed gedocumenteerd in artikel "<u>ISE Posture Style Vergelijking</u> <u>voor Pre en Post 2.2</u>", paragraaf "Postflow in ISE 2.2".

AnyConnect ISE Posture Module-provisioning met FlexVPN kan op 2 verschillende manieren worden uitgevoerd:

• Handmatig - de module is handmatig op de werking van de klant geïnstalleerd via het AnyConnect-pakket dat beschikbaar is op het Cisco-softwaredownloadoptieportal: <u>https://software.cisco.com/download/home/283000185</u>.

Aan de volgende voorwaarden moet worden voldaan voor de posterijen met handmatige ISEposteringsmodule:

1. Domain Name Server (DNS) moet FQDN-**inschrijving** (Full Qualified Domain Name) (FQDN) in.**cisco.com** to Policy Service Nodes (PSN's) oplossen. Tijdens de eerste verbindingspoging heeft de postmodule geen informatie over beschikbare PSN's. Ze stuurt zoeksondes naar beschikbare PSN's. FQDN enroll.cisco.com wordt in een van deze speldenprikken gebruikt.

2. **TCP** poort **8905** moet zijn toegestaan voor PSN's IP's. De houding loopt via TCP-poort 8905 in dit scenario.

3. Admin-certificaat op de PSN-knooppunten moet enroll.cisco.com in SAN-omgeving hebben. De verbinding tussen de VPN-gebruiker en het PSN-knooppunt via TCP 8905 wordt beschermd via het Admin-certificaat en de gebruiker krijgt een certificaatwaarschuwing als er geen dergelijke naam "enroll.cisco.com" in het Admin-certificaat van het PSN-knooppunt is.

Opmerking: Volgens <u>RFC6125</u> moeten GN's van certificaten worden genegeerd indien er SAN-waarden zijn opgegeven. Het betekent dat we ook GN's van Admin-certificaat in SAN-gebieden moeten toevoegen.

 Automatische provisioning via Client Provisioning Portal (CPP) - de module wordt gedownloed en geïnstalleerd vanaf de ISE door directe toegang tot CPP via portal FQDN.
 Aan de volgende voorwaarden moet worden voldaan voor de posterijen met automatische ISE Posture Module-voorzieningen:

1. DNS moet FQDN van CPP aan Policy Service Nodes (PSN's) IP's oplossen.

2. **TCP-poorten 80, 443 en CPP-poort (standaard 8443)** moeten zijn toegestaan voor IP's van VPN's. De client moet CPP FQDN rechtstreeks openen via HTTP (wordt herbestemd voor HTTPS) of HTTPS. Dit verzoek wordt naar de CPP-haven (standaard 8443) verwezen en dan gaat de houding via die poort.

3. Admin- en CPP-certificaten op de PSN-knooppunten moeten CPP FQDN in SAN-veld hebben. De verbinding tussen de VPN-gebruiker en het PSN-knooppunt via TCP 443 wordt beschermd door Admin-certificaat en de verbinding op CPP-poort wordt beschermd door het CPP-certificaat.

Opmerking: Volgens <u>RFC6125</u> moeten GN's van certificaten worden genegeerd indien er

SAN-waarden zijn opgegeven. Dit betekent dat we ook moeten toevoegen aan de GN's van Admin- en CPP-certificaten in SAN-gebieden van overeenkomstige certificaten.

Opmerking: Als de ISE-software geen oplossing voor <u>CSCvj76466</u> bevat, zal de houding of de clientprovisioning alleen werken als de client of de klant provisioning worden uitgevoerd op dezelfde PSN waarop de client was geauthentiseerd.

In geval van postuur met FlexVPN omvat de stroom de volgende stappen:

1. Gebruiker sluit op de FlexVPN-hub aan met AnyConnect-client.

2. ISE stuurt access-Accept naar de FlexVPN-hub met de naam ACL die moet worden toegepast voor het beperken van de toegang.

3 bis. Eerste verbinding met Handmatige voorziening - ISE postmodule ontdekt beleidsserver die de sonde naar enroll.cisco.com stuurt via TCP-poort 8905. Als een succesvol resultaat zijn de downloads van de postermodule ingesteld posteringsprofiel en werkt de module voor naleving aan de clientkant bij.

Tijdens de volgende verbinding zal de ISE postmodule ook Namen en IPs gebruiken die in de Lijst van het Startpunt van de Vraag van het postprofiel voor de detectie van de beleidsserver zijn gespecificeerd.

3 ter. Eerste verbinding met automatische provisioning - client opent CPP via FQDN. Als een succesvol resultaat wordt Network Setup Assistant gedownload op het werkstation van de klant en dan downloads en installeert het ISE Posture-module, ISE-nalevingsmodule en postprofiel.

Tijdens de volgende verbinding zal de ISE postmodule Namen en IPs gebruiken die in de Lijst van het Startpunt van de Vraag van het postprofiel voor de detectie van de beleidsserver zijn gespecificeerd.

4. Postmodule start controles op de naleving en stuurt de resultaten van de controle naar de ISE.

5. Als de status van de client voldoet, verstuurt ISE access-Accept naar de FlexVPN-hub met de naam ACL-naam: deze moet worden toegepast op een conforme client.

6. Cliënt krijgt toegang tot het netwerk.

Meer informatie over het postproces vindt u in document "<u>ISE Posture Style Vergelijking voor Pre</u> <u>en Post 2.2</u>".

Configureren

Netwerkdiagram



VPN-gebruiker krijgt alleen toegang tot de server (10.0.10) als hij de status heeft die compatibel is.

Configuratie DNS-server

In dit document wordt Windows Server 2008 R2 als DNS-server gebruikt.

Stap 1. Voeg host (A) record toe voor enroll.cisco.com, waarbij wordt gewezen op de IP van PSN:

File Action Wew Help	Server Manager				
Server Manager (PUSTYUGO-DC-1) Server Manager (PUSTYUGO-DC-1) Active Directory Certificate Services Active Directory Certificate Services Active Directory Comain Services DisS Server (IS) Persward Lookup Zones Diss Configuration Encoded from the services B Configuration Diss Server (IIS) Fedures Configuration Configuration Encoded from the services Diss Server (IS) Diss Server Security Zones Diss Server Security Zones Diss Server (IS) <p< td=""><td>File Action View Help</td><td></td><td></td><td></td><td></td></p<>	File Action View Help				
Server Manager (PUSTVUGO-DC-1) enroll.cisco.com 3 record(3) Roles Active Directory Donain Services D Active Directory Donain Services Sarat of Authority (SOA) D DKS Server Forward Lookp Zones E enroll.cisco.com Earnel E enroll.cisco.com Forward Lookp Zones E enroll.cisco.com Earnel E enroll.cisco.com Forward Lookp Zones E enroll.cisco.com Forwarders E confloade powerse Forwarders E configuration Forwarders E configuration Forwarders E configuration Forwarders E configuration Forwarder	🗢 🔿 🖄 📷 💥 🖬 🗟 🔽 📷 🗄 🗑				
OK Cancel Apply	Server Manager (PUSTYUGO-DC-1) Roles Active Directory Certificate Services DHC Server DVS DVS DVS DVS DVS DVS Forward Lookup Zones Reverse Lookup Zones Web Server (IIS) Features Diagnostics Configuration Storage	enroll.cisco.com 3 record(s) Name (same as parent folder) (same as parent folder) (same as parent folder)	Type Start of Authority (SOA) Name Server (NS) Host (A)	Data [12], pustyugo- pustyugo-dc-1 10.48.30.127	enroll.cisco.com Properties ? X Host (A)

Stap 2. Add Host (A) record voor CPP FQDN (cpp.voorbeeld.com gebruikt in dit voorbeeld) met aandacht voor IP van PSN:

🚆 Server Manager				
File Action View Help				
🗢 🔿 🔁 🔐 💥 🖹 🖻 🕄				
Server Manager (PUSTYUGO-DC-1)	example.com 6 record(s)			
🖃 🔐 Roles	Name	Туре	Data	cpp Properties
Gring Active Directory Certificate Services	(same as parent folder)	Start of Authority (SOA)	[13], pustyugo	
Active Directory Domain Dervices	(same as parent folder)	Name Server (NS)	pustyugo-dc-1	Host (A) Security
DNS Server	Срр	Host (A)	10.48.30.127	Host (uses parent domain if left blank):
	flexvpn-hub	Host (A)	10.48.71.183	
E EPUSTYUGO-DC-1	pustyugo-ise23-1	Host (A)	10.48.30.127	1895
🕀 🔝 Global Logs	pustyugo-ise23-2	Host (A)	10.48.30.128	Fully gualified domain name (FQDN):
E Forward Lookup Zones				cpp.example.com
	1			
eproll.cisco.com	1			IP address:
example.com	1			10.48.30.127
🕀 👔 📁 🖬 👘	1			
E 🛐 BERNER	1			Update associated pointer (PTH) record
E 👔 🚽	1			
Reverse Lookup Zones Gonditional Forwarders	1			
Web Server (IIS)	1			
🕀 📷 Features	1			
🗉 🚋 Diagnostics	1			
🗉 🏬 Configuration	1			
🕀 🔚 Storage	1			
	1			
	1			
	1			
				UK Lancel Apply
			-	

IOS XE initiële configuratie

Identiteitsbewijs configureren

De router zal certificaat gebruiken om zichzelf voor de AnyConnect-client te authenticeren. Het routercertificaat dient te worden vertrouwd door het besturingssysteem van de gebruiker om waarschuwing tijdens de fase van de verbindingsinrichting te voorkomen.

Het identiteitsbewijs kan op een van de volgende manieren worden verstrekt:

Opmerking: Het gebruik van zelfgetekende certificaten wordt niet ondersteund door IKEv2 FlexVPN.

Optie 1 - Het configureren van een certificeringsinstantie (CA) server op de router

Opmerking: Een CA-server kan op dezelfde IOS-router of een andere router worden gemaakt. In dit artikel wordt CA op dezelfde router gecreëerd.

Opmerking: U moet tijd aan NTP server synchroniseren voordat CA server kan worden ingeschakeld.

Opmerking: De gebruiker kan de authenticiteit van dit certificaat niet controleren en dus worden de gebruikersgegevens niet beschermd tegen aanvallen van mensen in het midden, tenzij het CA-certificaat handmatig wordt geverifieerd en ingevoerd in de machine van de gebruiker voordat de verbinding wordt ingesteld.

Stap 1. Generate RSA keys voor de CA server:

FlexVPN-HUB(config)# crypto key generate rsa label ROOT-CA modulus 2048 Stap 2. RSA-toetsen genereren voor identiteitsbewijs:

FlexVPN-HUB(config)# crypto key generate rsa label FLEX-1 modulus 2048
Verificatie:

FlexVPN-HUB# show crypto key mypubkey rsa

---- output truncated -----

Key name: ROOT-CA Key type: RSA KEYS Storage Device: private-config Usage: General Purpose Key Key is not exportable. Redundancy enabled. Key Data: 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101 00C01F04 E0AF3AB8 97CED516 3B31152A 5C3678A0 829A0D0D 2F46D86C 2CBC9175 ----- output truncated ----- output truncated ----- Key name: FLEX-1 Key type: RSA KEYS Storage Device: private-config Usage: General Purpose Key Key is not exportable. Redundancy enabled. Key Data: 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101 009091AE 4185DC96 4F561F7E 506D56E8 240606D0 CC16CC5E E4E24EEB 1664E42C ----- output truncated

Stap 3. Configuratie van de CA:

ip http server crypto pki server ROOT-CA issuer-name cn=ROOT-CA.example.com hash sha256 lifetime certificate 1095 lifetime ca-certificate 3650 eku server-auth no shutdown

Verificatie:

FlexVPN-HUB# show crypto pki server

Certificate Server ROOT-CA: Status: enabled State: enabled Server's configuration is locked (enter "shut" to unlock it) Issuer name: cn=ROOT-CA.example.com CA cert fingerprint: A5522AAB 1410E645 667F0D70 49AADA45 Granting mode is: auto Last certificate issued serial number (hex): 3 CA certificate expiration timer: 18:12:07 UTC Mar 26 2021 CRL NextUpdate timer: 21:52:55 UTC May 21 2018 Current primary storage dir: nvram: Database Level: Minimum - no cert data written to storage

Stap 4. Het vertrouwenspunt configureren:

```
interface loopback 0
ip address 10.10.10.10 255.255.255.255
crypto pki trustpoint FLEX-TP-1
enrollment url http://10.10.10.10.80
fqdn none
subject-name cn=flexvpn-hub.example.com
revocation-check none
rsakeypair FLEX-1
```

Stap 5. Verifieer de CA:

```
FlexVPN-HUB(config)#crypto pki authenticate FLEX-TP-1
Certificate has the following attributes:
      Fingerprint MD5: A5522AAB 1410E645 667F0D70 49AADA45
     Fingerprint SHA1: F52EAB1A D39642E7 D8EAB804 0EB30973 7647A860
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
Stap 6. Voer router in aan CA:
FlexVPN-HUB(config) #crypto pki enroll FLEX-TP-1
2
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
 For security reasons your password will not be saved in the configuration.
 Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: cn=flexvpn-hub.example.com
% The fully-qualified domain name will not be included in the certificate
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose FLEX-TP-1' commandwill show the fingerprint.
May 21 16:16:55.922: CRYPTO_PKI: Certificate Request Fingerprint MD5: 80B1FAFD 35346D0F
D23F6648 F83F039B
May 21 16:16:55.924: CRYPTO_PKI: Certificate Request Fingerprint SHA1: A8401EDE 35EE4AF8
46C4D619 8D653BFD 079C44F7
Controleer hangende certificaatverzoeken op de CA en controleer of de vingerafdruk overeenkomt
met:
```

FlexVPN-HUB#show crypto pki server ROOT-CA requests Enrollment Request Database:

Subordinate CA certificate requests: ReqID State Fingerprint SubjectName

RA certificate requests:

 ReqID
 State
 Fingerprint
 SubjectName

 Router
 certificates
 requests:

 ReqID
 State
 Fingerprint
 SubjectName

 1
 pending
 80B1FAFD35346D0FD23F6648F83F039B
 cn=flexvpn-hub.example.com

Stap 7. Verleent het certificaat met behulp van de juiste ReqID:

FlexVPN-HUB#crypto pki server ROOT-CA grant 1

Wacht tot de router opnieuw om het certificaat vraagt (volgens deze configuratie zal het 10 keer per minuut controleren). Zoeken naar syslog-bericht:

May 21 16:18:56.375: %PKI-6-CERTRET: Certificate received from Certificate Authority Controleer of het certificaat is geïnstalleerd:

```
FlexVPN-HUB#show crypto pki certificates FLEX-TP-1
Certificate
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: General Purpose
Issuer:
  cn=ROOT-CA.example.com
Subject:
  Name: flexvpn-hub.example.com
  cn=flexvpn-hub.example.com
Validity Date:
  start date: 16:18:16 UTC May 21 2018
  end date: 18:12:07 UTC Mar 26 2021
Associated Trustpoints: FLEX-TP-1
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
  cn=ROOT-CA.example.com
Subject:
  cn=ROOT-CA.example.com
Validity Date:
  start date: 18:12:07 UTC Mar 27 2018
  end date: 18:12:07 UTC Mar 26 2021
Associated Trustpoints: FLEX-TP-1 ROOT-CA
Storage: nvram:ROOT-CAexamp#1CA.cer
```

Optie 2 - extern ondertekende certificering importeren

FlexVPN-HUB(config)# crypto pki import FLEX-TP-2 pkcs12 ftp://cisco:cisco@10.48.30.130/ password cisco123 % Importing pkcs12... Address or name of remote host [10.48.30.130]? Source filename [FLEX-TP-2]? flexvpn-hub.example.com.p12 Reading file from ftp://cisco@10.48.30.130/flexvpn-hub.example.com.p12! [OK - 4416/4096 bytes] % The CA cert is not self-signed. % Do you also want to create trustpoints for CAs higher in % the hierarchy? [yes/no]: May 21 16:55:26.344: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named FLEX-TP-2 has been generated or imported yes CRYPTO_PKI: Imported PKCS12 file successfully. FlexVPN-HUB(config)# May 21 16:55:34.396: %PKI-6-PKCS12IMPORT_SUCCESS: PKCS #12 Successfully Imported. FlexVPN-HUB(config)#

IKEv2 configureren

Stap 1. Configuratie van RADIUS-server en CoA:

```
aaa group server radius FlexVPN-AuthC-Server-Group-1
server-private 10.48.30.127 key Cisco123
server-private 10.48.30.128 key Cisco123
```

```
aaa server radius dynamic-author
client 10.48.30.127 server-key Cisco123
client 10.48.30.128 server-key Cisco123
server-key Cisco123
auth-type any
```

Stap 2: Verificatie en autorisatielijsten configureren:

aaa new-model aaa authentication login FlexVPN-AuthC-List-1 group FlexVPN-AuthC-Server-Group-1 aaa authorization network FlexVPN-AuthZ-List-1 local aaa accounting update newinfo aaa accounting network FlexVPN-Accounting-List-1 start-stop group FlexVPN-AuthC-Server-Group-1 Stap 3. Creëer het vergunningenbeleid van ikev2:

```
crypto ikev2 authorization policy FlexVPN-Local-Policy-1
pool FlexVPN-Pool-1
dns 10.48.30.104
netmask 255.255.255.0
def-domain example.com
```

Stap 4. Maak IKEv2-profiel:

```
crypto ikev2 profile FlexVPN-IKEv2-Profile-1
match identity remote key-id example.com
identity local dn
authentication local rsa-sig
authentication remote eap query-identity
pki trustpoint FLEX-TP-2
dpd 60 2 on-demand
aaa authentication eap FlexVPN-AuthC-List-1
aaa authorization group eap list FlexVPN-AuthZ-List-1 FlexVPN-Local-Policy-1
aaa authorization user eap cached
aaa accounting eap FlexVPN-Accounting-List-1
virtual-template 10
```

Stap 5. Maak een transformatieset en ipsec-profiel:

```
crypto ipsec transform-set FlexVPN-TS-1 esp-aes esp-sha-hmac
mode tunnel
crypto ipsec profile FlexVPN-IPsec-Profile-1
set transform-set FlexVPN-TS-1
set ikev2-profile FlexVPN-IKEv2-Profile-1
```

Stap 6. Maak een virtuele sjabloon-interface:

interface Virtual-Template10 type tunnel
ip unnumbered GigabitEthernet3
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
Stap 7. Maak een lokale pool:

ip local pool FlexVPN-Pool-1 10.20.30.100 10.20.30.200

Stap 8. Maak ACL om toegang voor niet-conforme klanten te beperken. Tijdens een onbekende posterstatus dienen ten minste deze machtigingen te worden verstrekt:

- DNS-verkeer
- Verkeer naar ISE PSN's via de poorten 80, 443 en 8905
- Verkeer naar ISE PSN's waarop CPP-portal FQD wijst
- Verkeersservers naar herstelservers indien nodig

Dit is een voorbeeld van ACL zonder verbeteringsservers, expliciet ontkennen voor 10.0.0/24 netwerk wordt toegevoegd voor zichtbaarheid, bestaat impliciet "ontkennen ip elke"in het eind van ACL:

```
ip access-list extended DENY_SERVER
permit udp any any eq domain
permit tcp any host 10.48.30.127 eq 80
permit tcp any host 10.48.30.127 eq 443
permit tcp any host 10.48.30.127 eq 8443
permit tcp any host 10.48.30.127 eq 8905
permit tcp any host 10.48.30.128 eq 80
permit tcp any host 10.48.30.128 eq 443
permit tcp any host 10.48.30.128 eq 8443
permit tcp any host 10.48.30.128 eq 8905
deny ip any 10.0.00 0.0.255
```

Stap 9. Maak ACL om toegang voor conforme klanten toe te staan:

ip access-list extended PERMIT_ALL
 permit ip any any
Stap 10. Split-tunnelconfiguratie (optioneel)

Standaard zal al het verkeer via VPN worden geleid. Om alleen tunnelverkeer te maken naar de gespecificeerde netwerken, kunt u deze specificeren in het vak ikev2 autorisatiebeleid. Het is mogelijk om meerdere verklaringen toe te voegen of standaard toegang-lijst te gebruiken.

crypto ikev2 authorization policy FlexVPN-Local-Policy-1 route set remote ipv4 10.0.0.0 255.0.0.0

Stap 11. Internettoegang voor externe klanten (optioneel)

U kunt de NAT-vertaling configureren als u wilt dat de uitgaande verbindingen van de klanten voor

externe toegang naar de hosts in het internet NAT-ed zijn naar het wereldwijde IP-adres van de router:

ip access-list extended NAT
permit ip 10.20.30.0 0.0.0.255 any
ip nat inside source list NAT interface GigabitEthernet1 overload extended
interface GigabitEthernet1
ip nat outside

interface Virtual-Template 10
ip nat inside

AnyConnect-configuratie van clientprofiel

Het clientprofiel configureren met behulp van de AnyConnect Profile Editor. profielen van Any Connect Security mobiele client op Windows 7 en 10 worden opgeslagen in **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile**.

Stap 1. Schakel de optie Captive Portal Detectie uit. Als de http server niet is uitgeschakeld op de FlexVPN-hub, zal AnyConnect-detectie in gevangenschap de verbinding mislukken. Merk op dat CA server niet zal werken zonder HTTP server.

🔉 AnyConnect Profile Editor -	VPN	
File Help		
VPN	Preferences (Part 1) Profile:\Cisco AnyConnect Se	cure Mobility Client\Profile\FLEXVPN.xml
Gertificate Pinning Certificate Matching Certificate Enrollment	Use Start Before Logon	☑ User Controllable
Server List	Certificate Store Windows All macOS All	 ▼
	Certificate Store Overnoe Auto Connect On Start Minimize On Connect	✓ User Controllable✓ User Controllable
	Local Lan Access Disable Captive Portal Detection Auto Reconnect	User Controllable
	Auto Reconnect Behavior ReconnectAfterResume	User Controllable

Stap 2. Configuratie van de serverlijst:

AnyConnect Profile Editor File Help	- VPN	
VPN	Server List Profile:\Cisco AnyConnect Secure Mobility Client\Profile\FLEXVPN.xml	
Backup Servers Certificate Inning Certificate Enrollment Mobile Policy Server List	Server List Entry Server Load Balancing Servers SCEP Mobile Certificate Pinning Primary Server a. Display Name (required) FLEXVPN FQDN or IP Address User Group b. ffexvpn-hub.example.com Group URL Badkup Servers Host Address Host Address Add Move Up Move Up Move Up Delete	d.
	OK Cancel	

- Geef een naam op.
- Voer FQDN-of IP-adres van de FlexVPN-hub in.
- Selecteer IPsec als Primair Protocol.
- Schakel het selectieteken "ASA gateway" uit en specificeer EAP-MD5 als Auth Methode. Voer IKE Identity in precies het zelfde als in de IKEv2 profielconfiguratie op de FlexVPN-hub (in dit voorbeeld wordt het IKEv2-profiel ingesteld met de opdracht "match Identity Remote keyid.com", zodat we voorbeeld.com als IKE Identity moeten gebruiken).

Stap 3. Sla het profiel op in **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile** en start het AC opnieuw.

Het XML-equivalent van het profiel:

```
<CertificateStoreOverride>false</CertificateStoreOverride>
       <ProxySettings>Native</ProxySettings>
       <AllowLocalProxyConnections>false</AllowLocalProxyConnections>
       <AuthenticationTimeout>12</AuthenticationTimeout>
       <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
       <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
       <LocalLanAccess UserControllable="true">false</LocalLanAccess>
       <DisableCaptivePortalDetection
UserControllable="false">true</DisableCaptivePortalDetection>
       <ClearSmartcardPin UserControllable="true">false</ClearSmartcardPin>
       <IPProtocolSupport>IPv4, IPv6</IPProtocolSupport>
       <AutoReconnect UserControllable="false">true
           <AutoReconnectBehavior
UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
       </AutoReconnect>
       <AutoUpdate UserControllable="false">true</AutoUpdate>
       <RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
       <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
       <WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
       <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
       <PPPExclusion UserControllable="false">Automatic
           <PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
       </PPPExclusion>
       <EnableScripting UserControllable="false">false</EnableScripting>
       <EnableAutomaticServerSelection UserControllable="true">false
           <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
           <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
       </EnableAutomaticServerSelection>
       <RetainVpnOnLogoff>false
       </RetainVpnOnLogoff>
       <AllowManualHostInput>true</AllowManualHostInput>
   </ClientInitialization>
   <ServerList>
       <HostEntry>
           <HostName>FLEXVPN</HostName>
           <HostAddress>flexvpn-hub.example.com</HostAddress>
           <PrimaryProtocol>IPsec
               <StandardAuthenticationOnly>true
                   <AuthMethodDuringIKENegotiation>EAP-MD5</AuthMethodDuringIKENegotiation>
                   <IKEIdentity>example.com</IKEIdentity>
               </StandardAuthenticationOnly>
           </PrimaryProtocol>
       </HostEntry>
   </ServerList>
</AnyConnectProfile>
```

ISE-configuratie

Configuratie van beheers- en CPP-certificaten

Opmerking: Door op het Admin-certificaat te drukken, wordt het knooppunt waarop het certificaat is gewijzigd, opnieuw gestart.

Stap 1. Ga naar Beheer -> Systeem -> Certificaten -> Verzoeken voor certificaatsignalering, klik op Generate certificaatsignaleringsaanvragen (CSR):

dentity Services Engine	Home Context Visibility	Operations Policy	✓ Administration								
	Network Resources Device	e Portal Management pxGri	d Services Feed Se	ervice Threat Centric NAC							
Deployment Licensing - Certificate	Deployment Licensing -Certificates + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings										
G											
▼ Certificate Management	Certificate Signing Req	uests									
System Certificates	Generate Certificate Signing	Requests (CSR)									
Trusted Certificates	A Certificate Signing Request	s (CSRs) must be sent to and	signed by an external au	thority. Click "export" to downloa	d one or more CSR	s so that they may be					
OCSP Client Profile	bind to bind the request to the	ne signed certificate issued by	that authonity. Once a CS	ort is bound, it will be removed in	iom uns iist.						
Certificate Signing Requests	🔎 View 🔹 Export 🔀 De	Bind Certificate									
Certificate Periodic Check Setti	Friendly Name		Certificate Subject	Key Length	Portal group tag	Timestamp					
Certificate Authority				No data	available						

Stap 2. Selecteer in de geopende pagina het gewenste PSN-knooppunt, vul de gewenste velden in en voeg FQDN van het knooppunt toe, enroll.cisco.com, cpp.voorbeeld.com en IP-adres van het knooppunt in SAN-velden en klik op **Generate**:

dentity Services Engine	Home	tions Policy Administration	▶ Work Centers
▼System ► Identity Management	Network Resources Device Portal Mar	agement pxGrid Services + Feed Services	ervice
Deployment Licensing - Certificate	es Logging Maintenance Upgrad	e Backup & Restore Admin Acce	ess > Settings
0	Usage		
▼ Certificate Management	Certificate(s) will be used for Mul	ti-Use	Λ You can use a single certificate for multiple services, but
System Certificates			should obtain individual certificates specifically for each
Trusted Certificates		2	Portals, EAP, and pxGrid).
OCSP Client Profile	Allow Wildcard Certificates	U	
Certificate Signing Requests	Node(s)		
Certificate Periodic Check Setti	Generate CSR's for these Nodes:		
Certificate Authority	Node	CSR Friendly Name	e
	✓ pustyugo-ise23-1	pustyugo-ise23-1#M	ulti-Use
	pustyugo-ise23-2	pustyugo-ise23-2#M	lulti-Use
	Subject		
	Common Name (CN) \$F(DDN\$	()
	Organizational Unit (OU) TAG	5	()
	Organization (O) Cis-		(I)
	City (L)		
	State (ST)		
	Country (C)		

Subject Alternative Name (SAN)	DNS Name	pustyugo-ise23-1.example.com	_	÷	
	DNS Name	enroll.cisco.com	_	+	
	DNS Name	cpp.example.com	_	+	
	IP Address 🔹	10.48.30.127] —		i
* Key type	RSA 💌 🕧				
* Key Length	2048				
* Digest to Sign With	SHA-256				
Certificate Policies					
	Generate				

Opmerking: Als u in deze stap **Multi-Use** selecteert, kunt u ook hetzelfde certificaat voor Portal gebruiken.

Klik in het venster Exporteren om de CSR in pem-indeling naar het lokale werkstation op te slaan:





×

Stap 3. Ring de CSR met vertrouwde CA en haal het certificaatbestand van de CA evenals de volledige keten van CA-certificaten (Root and Intermediate) in.

Stap 4. Ga naar **Beheer -> Systeem -> Certificaten -> Vertrouwde certificaten**, klik op **Importeren**. Klik op het volgende scherm op **Kies bestand** en selecteer **Root CA** certificaatbestand, vul indien nodig Friendly name en Description in en selecteer nodig **Trusted For** Opties en klik op **Indienen**:



Herhaal deze stap voor alle tussencertificaten in de keten als er een is.

Stap 5. Ga terug naar Administratie -> Systeem -> Certificaten -> Verzoeken om certificaten te verzenden, selecteer de gewenste CSR en klik op Bind-certificaat:



Stap 6. Klik op de geopende pagina op **Kies bestand**, selecteer het certificaatbestand dat van de CA is ontvangen, en voer indien nodig een familienaam in en selecteer **Gebruik: Admin (Gebruik: Portal** kan hier ook worden geselecteerd als de CSR is gemaakt met **multi-use**) en klik op **Indienen**:

dentity Services Engine	Home	Operations Policy	 Administration 	▶ Work Centers				
▼System ► Identity Management	Network Resources Device	Portal Management pxGrid	Services Feed Se	rvice				
Deployment Licensing Certificat	es	Upgrade • Backup & Re	store Admin Acce	ss > Settings				
0								
▼ Certificate Management	Bind CA Signed Certificat	te						
System Certificates	* Certificate	File Choose File Signed C	SR.cer					
Trusted Certificates								
OCSP Client Profile	Friendly N	ame pustyugo-ise23-1 Admin						
Certificate Signing Requests	Validate Certificate Extension	ns 🗆 🛈						
Certificate Periodic Check Setti	Validate certificate Extension							
Certificate Authority	lie	- 200						
	05	age						
	Admin: Use certificate to authenticate the ISE Admin Portal							
		protocols that use SSL/TLS tunneling						
	RADIUS DTLS: Use certificate for the RADSec server							
	pxGrid : Use certificate for the pxGrid Controller							
		Portal: Use for portal						
		Submit Cancel						

Stap 7. Klik in de waarschuwing op **Ja** om de invoer te voltooien. Het knooppunt waarop het Admin-certificaat is gewijzigd, wordt opnieuw gestart:

vice F) ortal	Management pyCrid Convises - L Torest Contris NAC	
ince		Enabling Admin role for this certificate will cause an application server restart on the selected node.	
icat		Note: Make sure required Certificate Chain is imported under Trusted Certificates	
icate	_	No Yes	

Herhaal de stappen voor het wijzigen van CPP certificaat als u besloot om afzonderlijk certificaat voor portal te gebruiken. Selecteer in Stap 6 **Gebruik: Portal** en klik op **Inzenden:**



Herhaal de stappen voor alle PSN's in ISE-implementatie.

Een lokale gebruiker op ISE maken

Opmerking: Met EAP-MD5-methode worden alleen lokale gebruikers ondersteund op ISE.

Stap 1. Ga naar Beheer -> Identificatiebeheer -> Identificaties -> Gebruikers, klik op Toevoegen.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
▶ System ▼ Identity Management	Network Resources	
◄ Identities Groups External Identity	Sources Identity Source Sequences	
G	Network Assess Users	
Users	Network Access Users	
Latest Manual Network Scan Results	✓ Edit ♣Add BChange Status Change Status Export ▼ X Delete	
	Status Name Description First Name Last Name Email Address User Iden	ntity Groups Admin
	No data avail	able

Stap 2. Voer in de geopende pagina een gebruikersnaam, wachtwoord en andere benodigde informatie in en klik op **Indienen**.

cisco	Identi	ty Servio	es E	ngine	Hom	ne 🕨	Context	t Visibility	▶ Op	erations	▶ Policy	▼Ad	ministration	• V	Vork Centers
 Syst 	tem 🗖	- Identity	Manag	gement	Network	vork Reso	urces	Device	e Portal M	anagement	pxGrid	Services	Feed Ser	rvice	Threat Centric NAC
✓ Iden	tities	Groups	Ext	ernal Iden	tity Sour	ices Id	entity S	ource Sequ	uences	 Settings 					
				G											
Users					Net	Netwo	ess Use	ers List > N	lew Netw	ork Access	User				
Latest M	Ianual N	letwork S	can R	esults		netwo		233 0321							
						* Name	vpnuse	er							
						Status	🗹 E	nabled 👻]						
						Email									
						• Pass	vords								
						Passwo	rd Type	Inter	nal Users		Ŧ				
								Passw	vord			Re-Enter	Password		
						* Login	Passwo	rd •••••				•••••			Generate Password (i)
						Enable	Passwo	rd							Generate Password ()
					-	- Ilser	Inform	ation							
						Final Ma		adon			_				
						FIRST Na	.me								
						Last Na	me								
						Acco	int Op	tions							
								Descr	ription						h
						Change	passwo	ord on next	t login	ן					
						Acco	unt Dis	able Poli	icy						
						🗆 Di	sable ac	count if da	te exceed	is 2018-0	7-27		(7777)	y-mm-d	(bt
						 User 	Groups	5							
										<u> </u>					
						II ALL_A	COUNT	rs (default))	♥					
						Submit	Canc	el							

Voeg de FlexVPN-HUB toe als een RADIUS-client

Stap 1. Ga naar werkcentra -> Uitstellen -> Netwerkapparaten, klik op Toevoegen.

cisco Identity S	ervices Engine	Home	Context Visibility	Operations	▶ Policy	Administration	✓ Work Centers	
 Network Access 	Guest Access	TrustSec	BYOD Profiler	▼ Posture	Device Admin	nistration + Pas	siveID	
Overview Netw	ork Devices + Clie	nt Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports + Settings	
Network Devic	es							
🥖 Edit 🛛 🕂 Add	Duplicate 🔐 I	import 🛛 🔂 Exp	ort 🕑 Generate PA	Delete				
Name	 IP/Mask 	Profile Name	9	Location		Туре		Description
								No data available

Stap 2. Voer in de geopende pagina Apparaatnaam, IP-adres, andere benodigde informatie in, controleer het aankruisvakje "RADIUS-verificatie-instellingen", voer Gedeeld geheim in en klik op **Indienen** onder op de pagina.

uluilu cisco	Identity Services Engine	Home ► Context Vis	ibility 🕨 K	Operations	▶ Policy	Administration	✓ Work Centers		
Net	work Access	TrustSec BYOD	Profiler	▼ Posture	Device Admi	nistration Pa	ssiveID		
Overv	iew Network Devices + Clie	ent Provisioning	lements Po	osture Policy	Policy Sets	Troubleshoot	Reports Setting	s	
Networ	k Devices List > New Network D ork Devices	* Name FlexVPN-HUB Description FlexVPN HUB							
11									
	IP Address ▼ * IP : 1	0.48.71.183		/ 32					
O IP	IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected * Device Profile								
	Ма	odel Name	-						
	Softwa	re Version	•						
*	Network Device Group								
	Location All Locations	Set To Default							
	IPSEC Is IPSEC Device	Set To Default							
D	evice Type All Device Types	Set To Default							
•	→ RADIUS Authentication Setting	JS							
	RADIUS UDP Settings								
		Protocol	RADIUS						
		- Snared Secret	•••••		Show				
		ose second snared secret			Show				
		CoA Port	1700		Set T	o Default			
	RADIUS DTLS Settings (i)								
		DTLS Required	(i)						
		Shared Secret	radius/dtls		(j)				
		CoA Port	2083		Set T	o Default			
	Issuer C	JA OF ISE Certificates for CoA	Select if rec	quired (optiona	al)	• (i)			
		Dino iname							
	General Settings								
		Enable KeyWrap	i						
	* ****	* Key Encryption Key			Show				
	^ Mes	Key Input Format			Show				
_		ivey input i onliat							
	TACACS Authentication Setting	gs							
	 SNMP Settings 								
	 Advanced TrustSec Settings 								
Cubr	vit Cancol								

Configuratie van clientprovisioning

Dit zijn de stappen om AnyConnect-configuratie voor te bereiden.

Stap 1. Het pakket kan worden gedownload. Elk pakket zelf is niet beschikbaar voor direct download van ISE dus voordat u begint, zorg ervoor dat AC op uw PC beschikbaar is. Deze link kan worden gebruikt voor het downloaden van AC - <u>http://cisco.com/go/anyconnect</u>. In dit document wordt anyconnect-win-4.5.05030-web-implementatie-k9.pkg pakket gebruikt.

Stap 2. Om het AC-pakket naar ISE te uploaden, **navigeer** naar **werkcentra -> Post-up -> Clientprovisioning ->** resources en klik op **Add**. Kies **de middelen van de Agent van lokale schijf**. Kies in het nieuwe venster **Cisco Provided Packages**, klik op **Bestand kiezen** en selecteer ACpakket op uw PC.

cisco Identity Services Engine	Home Context Visibility		ministration - Work Centers		
Network Access Guest Access	TrustSec BYOD Profile	er Posture Device Administra	tion PassiveID		
Overview Network Devices - Clie	nt Provisioning Policy Elements	Posture Policy Policy Sets Tr	oubleshoot Reports + Setting	S	
Client Provisioning Policy	Agent Resources From Local Dis Agent Resources From Lo	sk > Agent Resources From Local Disk OCal Disk			
Resources	5				
Client Provisioning Portal	Category	Cisco Provided Packages Choose File anyconnectploy	▼ (j) k9.pkg		
		▼ AnyConnect Uploaded Resou	'Ces		
		Name	▲ Туре	Version	Description
		AnyConnectDesktopWindows 4.5.503	AnyConnectDesktopWindows	4.5.5030.0	AnyConnect Secure Mobility Clien
	Submit Cancel				

Klik op Inzenden om de import te voltooien. Controleer de verpakking en druk op Bevestig.

Stap 3. De nalevingsmodule moet aan ISE worden geüpload. Op dezelfde pagina (Workcenters -> Posture -> Client Provisioning -> Resources) klik op Add en kies Agent-bronnen van Cisco-site. In een lijst met resources moet u een nalevingsmodule controleren en op Save. Voor dit document Er wordt een module voor naleving van AnyConnect-nalevingsmodule voor Windows 4.3.50.0 gebruikt.

Dov	vnload Remote Resources		×
	Name 🔺	Description	
	AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Wir	h
	AnyConnectComplianceModuleOSX 3.6.11682.2	AnyConnect OS X Compliance Module 3.6.11682.2	
	AnyConnectComplianceModuleOSX 4.3.29.0	AnyConnect OSX Compliance Module 4.3.29.0	
	AnyConnectComplianceModuleWindows 3.6.11682.2	AnyConnect Windows Compliance Module 3.6.11682.2	
\checkmark	AnyConnectComplianceModuleWindows 4.3.50.0	AnyConnect Windows Compliance Module 4.3.50.0	
	CiscoTemporalAgentOSX 4.5.02036	Cisco Temporal Agent for OSX With CM: 4.2.1019.0 Works wi	
	CiscoTemporalAgentWindows 4.5.02036	Cisco Temporal Agent for Windows With CM: 4.2.1226.0 Work	
	ComplianceModule 3.6.11510.2	NACAgent ComplianceModule v3.6.11510.2 for Windows	
	MACComplianceModule 3.6.11510.2	MACAgent ComplianceModule v3.6.11510.2 for MAC OSX	
	MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.	
	MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12,	
	MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Mac OsX 1.0.0.18 (ISE 1.1	
	MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Mac OsX 1.0.0.21 (for ISE	
	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE	
	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE	
	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for Mac OsX 1.0.0.30 (for ISE	
		۱. Electric de la construcción de l	
For	AnyConnect software, please download from http://cisco.com/go/anyc	onnect. Use the "Agent resource from local disk" add option,	

to import into ISE

٣

Save Cancel

Stap 4. Nu moet een AC-profiel worden gemaakt. Klik op Add en kies NAC agent of Any Connectpostelprofiel.

cisco Identity Services Engine	Home ► Context Visibility	Operations Policy	Administration	✓ Work Centers
Network Access Guest Access	TrustSec BYOD Profiler	▼ Posture → Device Admin	nistration + Pass	iveID
Overview Network Devices - Clier	t Provisioning Policy Elements	Posture Policy Policy Sets	Troubleshoot F	Reports
Client Provisioning Policy	ISE Posture Agent Profile Settings	> New Profile		
Resources	Posture Agent Profile Settings			
Client Provisioning Portal	A. AnyConnect AnyConnect Ac-4.5-Posture Description:			
	Agent Behavior			

- Kies het type van het profiel. AnyConnect moet voor dit scenario worden gebruikt.
- Naam profiel opgeven. Navigeren in het gedeelte Protocol van profiel naar Posture

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	* <u>a.</u>	need to be blank by default to force admin to enter a value. "*" means agent will connect to all
Call Home List	pustyugo-ise23-1.exampl b .	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.

Note: It is recommended that a separate profile be created for Windows and OSX deployments

Submit Cancel	

- Specificeer de regels voor servernaam. Dit veld kan niet leeg zijn. Het veld kan FQDN bevatten met jokerteken dat de verbinding met de postuur van de module beperkt tot PSNs vanuit een geschikte naamruimte. Doe sterren als een FQDN zou moeten worden toegestaan.
- Naam en IP's die hier zijn gespecificeerd, zijn in gebruik tijdens fase 2 van postontdekking (zie stap 14 van "<u>Postflow in ISE 2.2</u>" sectie). U kunt namen scheiden door komma even goed poortnummer toe te voegen na FQDN/IP met behulp van colon.

Stap 5. Maak AC-configuratie. navigeren naar **werkcentra -> Post -> Clientprovisioning -> Bronnen** en klik op **Add** en selecteer vervolgens **AnyConnect Configuration**.



- Selecteer het AC-pakket.
- Geef de naam van de AC-configuratie op.
- Kies de versie van de nalevingsmodule.
- Selecteer in de vervolgkeuzelijst het configuratieprofiel voor de AC-houding.

Stap 6. Het leveringsbeleid van de cliënt configureren. Navigeer naar **werkcentra -> Postering -> Clientprovisioning**. In het geval van een startconfiguratie kunt u lege waarden invullen in beleid dat standaard wordt weergegeven. Als u beleid aan bestaande posteringsconfiguratie moet toevoegen, navigeer dan naar beleid dat hergebruikt kan worden en kies **Duplicate boven** of **Duplicaat hieronder.** Er kan ook een nieuw Brand-beleid worden gecreëerd.

Dit is het voorbeeld van het in het document gebruikte beleid.

the title to the title of the t	ne	Operations + Policy + Administr	vation Vork Centers			License Warning 🔺	ৎ 🛛 🔞
Network Access Guest Access Trus	ustSec + BYOD + Profiler	Posture Posture	PassiveID				
Overview Network Devices - Client Provis	isioning Policy Elements	Posture Policy Policy Sets Troublest	noot Reports + Settings				
0							
Client Provisioning Policy Clie	ent Provisioning Policy						
Resources For A							
Client Provisioning Portal	Native Supplicant Configuration.	wizaro profile and/or wizaro. Urag and drop	rules to change the order.				
	Rule Name	Identity Groups	Operating Systems	Other Conditions	Results		
II.	🖉 💌 Windows	If Any 💠 and	Windows All 🔶 and	Condition(s)	AnyConnect 🗢		
					Agent Configuration		^
					Agent: AnyConnect Configuration]	
					Native Supplicant Configuration		
					Config Wizard Choose a Config Wizard O		
					Wizard Profile: Choose a Wizard Profile		-
					4		•

Kies uw AC-configuratie in het resulterende gedeelte.

Postbeleid en -voorwaarden

Eenvoudige postcontrole wordt gebruikt. ISE is ingesteld om de aanwezigheid van bestand C:\TEST.txt aan de kant van het eindapparaat te controleren. Reallife scenario's kunnen veel gecompliceerder zijn, maar de algemene configuratiestappen zijn hetzelfde.

Stap 1. Maak de posteringsconditie. De posterijen bevinden zich in **de werkcentra -> Postdiensten** -> **Beleidselementen -> Voorwaarden**. Kies het type postconditie en klik op **Toevoegen**. Geef de benodigde informatie op en klik op **Opslaan**. Hieronder vindt u een voorbeeld van de staat van de dienst die moet controleren of het bestand C:\TEST.txt bestaat.

cisco Identity Services Engine	Home ► Context V	/isibility I Operations	Policy →	Administration	✓ Work Centers
Network Access Guest Access	TrustSec BYOD	► Profiler ▼Posture	Device Adminis	stration	iveID
Overview Network Devices + C	ient Provisioning Policy	Elements Posture Policy	Policy Sets	Troubleshoot	Reports • Settings
 Conditions Hardware Attributes Condition Application Firewall Condition Anti-Malware Anti-Malware Anti-Spyware Anti-Virus Compound Dictionary Simple Dictionary Compound Disk Encryption 	File Conditions List > T File Condition * Name Description * Operating System Compliance Module * File Type * File Path * File Operator	TEST_txt TEST_txt Windows All Any version FileExistence ABSOLUTE_PATH Exists	▼ (i) ▼ ▼ ▼	C:\TEST.txt	
File					
Patch Management					
Service					
USB					

Stap 2.Configuratie van de eisen voor de houding. Navigeren in op **werkcentra -> Post ->** Beleidselementen -> Vereisten. Dit is een voorbeeld voor het bestaan van bestand TEST.txt:



Kies uw posteringsconditie in een nieuw vereiste en geef een corrigerende actie op.

Stap 3. Plaats het beleid. Navigeren in op **werkcentra -> Posture -> Posture Policy**. Hieronder vind je een voorbeeld van het beleid dat voor dit document is gebruikt. Beleidsbeleid heeft een "Bestaan van een bestand"-vereiste toegewezen als verplicht en heeft geen andere voorwaarden toegewezen.

A Mahardi Januara - A Guard Januara - A Tarabéta - A Bullet - Bandara - A Bundara - A Bandara	()
► Network Access ► Guest Access ► Frustsec ► BYOD ► Promer ▼ Posture ► Device Administration ► PassivelD	
Overview Network Devices + Client Provisioning + Policy Elements Posture Policy Sets Troubleshoot Reports + Settings	
Bestung Bellion	
POSITIE POINTY Define the Positive Policy by configuring rules based on operating system and/or other conditions.	
•	
Status Rule Name Identity Groups Operating Systems Compliance Module Posture Type Other Conditions Requirements	
✓ ▼ File Policy II Any → and Windows All ↓ and Lx or later ▲ and AnyConnect ↓ and (Optional) Dictionar ↓ Ibin File Existance ↓ Ibin	

Clientprovisioningportal configureren

Voor houding zonder omleiding moet de configuratie van de klant provisioningportal worden aangepast. Navigeren in **naar werkcentra -> Posture -> Clientprovisioning -> Clientprovisioningportal** U kunt de standaardindeling gebruiken of uw eigen portal maken.

Identity Services Engine Home Context Visibility Operations Policy Administration Vork Centers
Network Access Guest Access TrustSec BYOD Profiler ▼Posture Device Administration PassiveID
Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings
0
Client Provisioning Policy
Resources Portal Settings
Client Provisioning Portal HTTPS port.* 8443 (8000 - 8999)
Allowed Interfaces:* For PSNs Using Physical Interfaces For PSNs with Bonded Interfaces Configured Gigabit Ethernet 0 Gigabit Ethernet 1 Gigabit Ethernet 2 Gigabit Ethernet 2 Gigabit Ethernet 2 Gigabit Ethernet 3 Gigabit Ethernet 4 Gigabit Ethernet 5 Certificate group tag: * Default Portal Certificate Group * Configure certificates at: Authentication method: * All_User_ID_Stores * a.
Compute autrentication methods at: Administration > Identify Management > Identify Source Sequences
Configure authorized groups User account with Super admin privilege or ERS admin privilege will have access to the portal
Available Chosen Available Chosen AD: AD: Builtin/Administrators AD: Users/Domain Computers AD: Users/VPN User Employee GROUP_ACCOUNTS (default) OWN_ACCOUNTS (d
★ Choose all X Clear all
Fully qualified domain name (FQDN): cpp.example.com
Idle timeout: 10 1-30 (minutes)

Deze instellingen moeten in de poortconfiguratie worden bewerkt voor een scenario zonder omleiding:

- Specificeer in Verificatie Identity Source Sequence die moet worden gebruikt als SSO geen sessie voor de gebruiker kan vinden.
- Afhankelijk van de geselecteerde Identity Source Sequence list van beschikbare groepen is bevolkt. Hier moet u groepen selecteren die zijn geautoriseerd voor inloggen.
- FQDN van client provisioningportal moet worden gespecificeerd. Deze FQDN moet kunnen worden opgelost voor IP's van ISE PSN's. Gebruikers dienen geïnstrueerd te worden om de FQDN in de webbrowser te specificeren tijdens de eerste poging tot verbinding.

Verificatieprofielen en -beleid configureren

De initiële toegang voor de cliënt wanneer de status van postuur niet beschikbaar is, moet worden beperkt. Dit kan op verschillende manieren worden bereikt:

- Straal filter-ID met deze eigenschap kunnen ACL die lokaal op NAD is gedefinieerd, aan de gebruiker met onbekende status worden toegewezen. Aangezien dit een standaard RFCeigenschap is, zou deze benadering goed moeten werken voor alle verkopers van NAD.
- Cisco:cisco-av-paar = ip:interface-configuratie zeer gelijkend op Straal filter-ID, ACL lokaal gedefinieerd op NAD kan aan de gebruiker met onbekende status worden toegewezen. Voorbeeld van de configuratie:

cisco-av-pair = ip:interface-configuratie=ip access-groep DENY_SERVER in

Stap 1. Het vergunningprofiel configureren.

Zoals gebruikelijk zijn twee vergunningsprofielen vereist. Ten eerste moeten alle beperkingen van de toegang tot het netwerk bevatten. Dit profiel kan worden toegepast op de authenticaties waarvoor de posterstatus niet gelijk is aan de conforme. Het tweede vergunningprofiel kan slechts toegang tot de vergunning bevatten en kan worden aangevraagd voor een sessie met een poststatus die gelijk is aan de conforme.

Om een autorisatieprofiel te maken, navigeer naar **werkcentra -> Posture -> Beleidselementen ->** Verificatieprofielen.

Voorbeeld van een beperkt toegangsprofiel met een radiofilter-ID:

cisco Identity Services Engine	Home	Operations Policy Adr	ninistration Vork Centers					
Network Access Guest Access	TrustSec BYOD Profile	r Posture Device Administrati	on PassiveID					
Overview Network Devices + Clier	nt Provisioning Policy Elements	Posture Policy Policy Sets Trou	ubleshoot Reports + Settings					
0								
	Authorization Profiles > LIMITED_ACCESS							
Hardware Attributes Condition	* Name LIM	ITED ACCESS						
Application	Description							
Firewall Condition	* Access Type	ESS ACCEDT						
Anti-Malware	ACC	ESS_ACCEPT						
Anti-Spyware	Network Device Profile	Cisco 👻 🕀						
Anti-Virus	Service Template							
Compound	Track Movement)						
Dictionary Simple	Passive Identity Tracking							
Dictionary Compound								
Disk Encryption								
File	- Common Tasks							
Patch Management								
Registry	DACL Name							
Service								
USB	ACL (Filter-ID)	DENY_SERVER	.in					
Remediations	_							
Requirements	Security Group							
Allowed Protocols								
Authorization Profiles	U VEAN							
Downloadable ACLs								
	- Advanced Attributes Se	ttings						
	Auvaliceu Attributes Se	tungs						
	Select an item	○ =	○ - +					
	▼ Attributes Details							
	Access Type = ACCESS_ACCEP	т						
	Filter-ID = DENY_SERVER.in							

Voorbeeld van beperkt toegangsprofiel met cisco-av-paar:

alialia cisco	Identi	ity Ser	vices Eng	jine	Home	Context Visibili	ity i	 Operations 	▶ Policy	Administration	▼ Wor	k Centers		
Net	work Ac	cess	Guest A	Access	TrustSec	+ BYOD + F	Profiler	✓ Posture	Device Admi	nistration + Pa	ssiveID			
Overv	view N	Network	Devices	Clie	nt Provisioning	- Policy Elem	nents	Posture Policy	Policy Sets	Troubleshoot	Reports	 Settings 	3	
				G										
- Cond	litions				Authorizati	on Profiles > LIM	IITED_A	ACCESS						
Hard	lware At	tributes	Condition		Autionz	* Name	LIMIT	ED ACCESS						
Appl	ication					Description		LD_ACCE35						_
Firev	wall Con	dition				* Access Tupe								11
Anti-	Malware	е				Access Type	ACCES	5S_ACCEPT	Ŧ					
Anti-	Spywar	е			Network	Device Profile	ditte Cit	sco 💌 🕀						
Anti-	Virus				s	ervice Template								
Com	pound				1	Frack Movement								
Dicti	onary Si	imple			Passive I	dentity Tracking								
Dicti	onary C	ompour	nd		1 0001101	dentry meeting								
Disk	Encrypt	tion												
File						and the state								
Patc	h Manaş	gement			▼ Comr	non Tasks								
Regi	istry					L Name								
Serv	ice													
USB	1				AC	L (Filter-ID)								
Reme	diation	s												
Require	ments				Sec	urity Group								
Allowed	Protoco	ols			_									
Authoriz	zation Pr	rofiles			U VLA	AN								
Downlo	adable /	ACLs												
								-						
					▼ Adva	nced Attribute	es Setti	ings						
						-1					1 .			
					II Cisco:	cisco-av-pair		= lip:in	nterface-config=	ip access-g 💟]— +			
					▼ Attrib	outes Details								
					Access T	ype = ACCESS_4	ACCEPT							
					cisco-av-	-pair = ip:interfac	ce-config	g=ip access-gro	up DENY_SERVI	ER in				

Voorbeeld van onbeperkt toegangsprofiel met Radius filter-ID:

cisco Identity Services Engine	Home → Context Visibility → Operations → Policy → Administration work Centers
Network Access Guest Access	TrustSec BYOD Profiler Posture Device Administration PassiveID
Overview Network Devices + Clie	nt Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings
G	* Name UNLIMITED_ACCESS
- Conditions	Description
Hardware Attributes Condition	* Access Type ACCESS_ACCEPT
Application	Network Device Profile 📾 Cisco 💌 🕀
Firewall Condition	Service Template
Anti-Malware	
Anti-Spyware	Track Movement
Anti-Virus	Passive Identity Tracking
Compound	
Dictionary Simple	
Dictionary Compound	▼ Common Tasks
Disk Encryption	
File	DACL Name
Patch Management	
Registry	
Service	Security Group
USB	
Remediations	VLAN
Requirements	
Allowed Protocols	
Authorization Profiles	▼ Advanced Attributes Settings
Downloadable ACLs	
	Select an item 📀 =
	✓ Attributes Details
	Access Type = ACCESS_ACCEPT Filter-ID = PERMIT_ALL.in

Voorbeeld van onbeperkt toegangsprofiel met cisco-av-paar:

uluiu cisco	Identity Ser	vices Eng	jine	Home	Context Visibility	 Operations 	▶ Policy	Administration	▼ Wor	k Centers		
Net	work Access	 Guest A 	Access	TrustSec	► BYOD ► Pro	ofiler Posture	Device Adm	inistration + Pa	ssiveID			
Overv	riew Networ	k Devices	Clier	nt Provisioning	- Policy Element	nts Posture Policy	Policy Sets	Troubleshoot	Reports	 Settings 		
			G		* Name	UNLIMITED_ACCESS	6					
- Cond	litions				Description						1	
Harr	lwaro Attributo	e Condition			* Access Type	ACCESS_ACCEPT	*					
Anni	ication	5 Condition		Network	Device Profile	deb Cieco - @						
Fire	vall Condition											
Anti-	Malware			S	ervice Template	0						
Anti-	Souware			т	rack Movement							
Anti-	Minus			Passive I	dentity Tracking	1						
Com	nound											
Dicti	onary Simple											
Dicti	onary Compou	nd		▼ Comr	non Tasks							
Disk	Encryption											
File	2.1019.0011				L Name							
Pate	h Managemen	t										
Regi	istry			AC	L (Filter-ID)							
Serv	ice											
USB				Sec	urity Group							
> Domo	adiations				N I							
P Refire	sulduona				uv.							
Require	ments											
Allowed	I Protocols			- Adup	need Attributes	Cottings						_
Authoriz	zation Profiles				nced Attributes	Settings						
Downlo	adable ACLs			Eisco:	risco-av-nair	🚫 = linti	nterface-config=	in access-o				
				:: [Ciscold	cioco-av-pair	= [ipii	nterrace-comig-	ip accessigni 🦭				
					outes Details	CEDT						
				cisco-av-	pair = ip:interface	-config=ip access-gr	DUP PERMIT_ALL	Lin				

Stap 2. Het vergunningenbeleid instellen. Gedurende deze stap dienen twee autorisatiebeleid te worden opgezet. Een om een eerste authentificatieaanvraag te koppelen met een onbekende status en een tweede om volledige toegang toe te wijzen na een succesvol postuur proces.

Het is een voorbeeld van eenvoudig toelatingsbeleid in dit geval:

✓ Auth	orization	Policy (12)							
٠	Status	Rule Name	Condit	ins	Results Profiles Security Groups				
Searc	1								
	ø	Unknown_Compliance_Redirect	AND	Network_Access_Authentication_Passed Compliance_Unkinoum_Devices	+LIMITED_ACCESS	Select from list	55	٥	
	0	NonCompliant_Devices_Redirect	AND	Network_Access_Authentication_Passed Non_Compliant_Devices	*LIMITED_ACCESS	Select from list	3	٥	
	ø	Compliant_Devices_Access	AND	Network_Access_Authentication_Passed Compliant_Devices	+ UNLIMITED_ACCESS	Select from list	30	٥	

De configuratie van het verificatiebeleid maakt geen deel uit van dit document, maar u dient er rekening mee te houden dat de authenticatie succesvol moet zijn voordat de verwerking van het autorisatiebeleid begint.

Verifiëren

De basiscontrole van de stroom kan bestaan uit drie hoofdstappen:

Stap 1. RA VPN-sessieverificatie op de FlexVPN-HUB:

```
show crypto session username vpnuser detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
Interface: Virtual-Access1
Profile: FlexVPN-IKEv2-Profile-1
Uptime: 00:04:40
Session status: UP-ACTIVE
Peer: 7.7.7.7 port 60644 fvrf: (none) ivrf: (none)
    Phase1_id: example.com
    Desc: (none)
 Session ID: 20
 IKEv2 SA: local 5.5.5.5/4500 remote 7.7.7.7/60644 Active
        Capabilities:DNX connid:1 lifetime:23:55:20
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.20.30.107
      Active SAs: 2, origin: crypto map
       Inbound: #pkts dec'ed 499 drop 0 life (KB/Sec) 4607933/3320
       Outbound: #pkts enc'ed 185 drop 0 life (KB/Sec) 4607945/3320
show crypto ikev2 sa detail
IPv4 Crypto IKEv2 SA
Tunnel-id Local
                               Remote
                                                     fvrf/ivrf
                                                                           Status
        5.5.5.5/4500 7.7.7.7/60644 none/none
1
                                                                           READY
    Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: RSA, Auth
verify: EAP
    Life/Active Time: 86400/393 sec
    CE id: 1010, Session-id: 8
     Status Description: Negotiation done
    Local spi: 54EC006180B502D8 Remote spi: C3B92D79A86B0DF8
    Local id: cn=flexvpn-hub.example.com
    Remote id: example.com
                                Remote req msg id: 19
Remote next mag
     Remote EAP id: vpnuser
    Local next msg id: 0
Local next msg id: 0
Local req queued: 0
    Local req msg id: 0
                                     Remote req queued: 19
    Local window: 5
                                     Remote window:
                                                         1
    DPD configured for 60 seconds, retry 2
    Fragmentation not configured.
     Dynamic Route Update: disabled
    Extended Authentication configured.
    NAT-T is detected outside
    Cisco Trust Security SGT is disabled
     Assigned host addr: 10.20.30.107
     Initiator of SA : No
```

IPv6 Crypto IKEv2 SA

Stap 2. Verificatie van verificatiesnelheid (radius Live Logs):

	Time	Status	Details	Identity	Posture Status	Endpoint ID	Authentication P	Authorization Policy	Authorization Profiles	IP Address
×				Identity	Posture Status	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
3.	Jun 07, 2018 07:40:01.378 PM		ò		Compliant	7.7.7.7			UNLIMITED_ACCESS	
2.	Jun 07, 2018 07:39:59.345 PM	0	Q	vpnuser	Compliant	7.7.7.7	Default >> Default	Default >> Unknown_Compliance	LIMITED_ACCESS	10.20.30.112
1.	Jun 07, 2018 07:39:22.414 PM	~	0	vpnuser	NotApplicable	7.7.7.7	Default >> Default	Default >> Unknown_Compliance	LIMITED_ACCESS	

- Eerste authenticatie. Voor deze stap kan het u interesseren welke autorisatieprofiel is toegepast. Indien een onverwacht vergunningprofiel is toegepast, onderzoek dan naar een gedetailleerd verslag van de authenticatie. U kunt dit rapport openen door in de kolom Details op vergroot glas te klikken. U kunt eigenschappen in gedetailleerd authentificatierapport vergelijken met voorwaarde in vergunningbeleid die u verwacht te matchen.
- 2. Sessiegegevens wijzigen, in dit geval is de status van de voorbeeldsessie gewijzigd van NietToepasselijk naar Compliant.
- 3. COA naar netwerktoegangsapparaat. Als de COA heeft gefaald, kunt u een gedetailleerd rapport openen om de reden te onderzoeken. De meest voorkomende problemen met COA zijn: COA timeout - in zo'n geval is ofwel PSN die een verzoek heeft verstuurd niet ingesteld als een COA client aan de NAD of is COA request ergens op weg gedropt.COA-negatieve ACK - geeft aan dat COA door NAD is ontvangen, maar om een of andere reden kan COAoperatie niet worden bevestigd. Voor dit scenario moet in een gedetailleerd verslag meer gedetailleerde uitleg worden gegeven.

Aangezien IOS XE gebaseerde router als NAD voor dit voorbeeld gebruikt is, kunt u geen verder authentificatieverzoek voor de gebruiker zien. Dit gebeurt door het feit dat ISE COA-toets voor IOS XE gebruikt waardoor VPN-service interuptie wordt vermeden. In een dergelijk scenario bevat de COA zelf nieuwe vergunningsparameters, zodat herauthenticatie niet nodig is.

Stap 3.Controleer het rapport van het bedrijf - navigeer naar **bewerkingen -> Rapporten ->** Rapporten -> Endpoint en gebruikers -> Beoordeling van de positie per eindpunt.

dentity Services Engine	Home	 Context Visibility 	← Operations Po	licy ▶ Adm	inistration		License Warning 🔺 🔍	0 0 ¢
RADIUS Threat-Centric NAC Live	e Logs	TACACS + Troublesh	Noot Adaptive Network	Control Re	ports			
▼ Reports	Post	ure Assessment by	Endpoint 🕄				+ My Reports Z Export	To • O Schedule
▶ Audit	From	2018-06-07 00:00:00.0 to	2018-06-07 19:52:48.0					
Device Administration	Repor	ts exported in last 7 days	0					
Diagnostics							▼ Filter ▼	CRefresh O-
✓ Endpoints and Users		Logged At	Status	Details	PRA Action	Identity	Endpoint ID	IP Address
Authentication Summary	×	Today 🔻	×			Identity	Endpoint ID	
Client Provisioning		2018-06-07 19:39:59.3	45 🗹	Q	N/A	vpnuser	50:00:00:03:00:00	10.20.30.112
Current Active Sessions		2018-06-07 19:38:14.0	53 🖌	Q	N/A	vpn	50:00:00:03:00:00	10.20.30.111
External Mobile Device M		2018-06-07 19:35:03.1	72 😵	0	N/A	vpnuser	50:00:00:03:00:00	10.20.30.110
Manual Certificate Provisi		2018-06-07 19:29:38.7	61 🔽	Q	N/A	vpn	50:00:00:03:00:00	10.20.30.109
PassiveID		2018-06-07 19:26:52.6	57 🔽	0	N/A	vpnuser	50:00:00:03:00:00	10.20.30.108
Posture Assessment by C		2018-06-07 19:17:17.9	06	à	N/A	vpnuser	50:00:00:03:00:00	10.20.30.107
Posture Assessment by E	4							•
Profiled Endpoints Summ							Rows/Page 6 • I I	6 Total Rows

U kunt voor elke specifieke gebeurtenis van hier gedetailleerd rapport openen om bijvoorbeeld te controleren tot welke sessie-ID dit rapport behoort, welke precieze posteringsvereisten door ISE zijn geselecteerd voor het eindpunt en voor elke vereiste de status van een goede positie.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te

lossen.

1. IKEv2-apparaten om zich te verzamelen bij het uiteinde:

```
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 internal
debug crypto ikev2 error
```

2. AAA-debugs voor de toewijzing van lokale en/of externe eigenschappen:

```
debug aaa authorization
debug aaa authentication
debug aaa accounting
debug aaa coa
debug radius authentication
debug radius accounting
```

- 3. DART van de AnyConnect-client.
- 4. Voor problemen oplossen bij posteringsproces moeten deze ISE-onderdelen zijn ingeschakeld in debug op de ISE-knooppunten waar een posteringsproces kan plaatsvinden:client-webapp: onderdeel dat verantwoordelijk is voor het leveren van agentia. Doel van het logbestand is te gast.log en ise-psc.log.guestacess component verantwoordelijk voor client-provisioning portal, samengesteld en sessie eigenaar lookup (wanneer het verzoek tot verkeerde PSN leidt). Bestandslogbestand gaste.log.bevoorrading component verantwoordelijk voor de verwerking van clientprovisioningbeleid. Doel logbestand gastarge.log.Positie alle met postuur samenhangende gebeurtenissen. Doel logbestand ise-psc.log
- 5. Voor problemen oplossen aan clientzijde kunt u gebruiken: AnyConnect.txt Dit bestand is te vinden in de DART-bundel en te gebruiken voor het oplossen van VPN.acisensa.log-In geval van een storing in de cliëntenvoorziening wordt dit bestand aangemaakt in dezelfde map waarin NSA is gedownload (downloads folder voor Windows normaal); AnyConnect_ISEPosture.txt Dit bestand is te vinden in de DART-bundel in map Cisco AnyConnect ISE Posture Module. Alle informatie over ISE PSN ontdekking en algemene stappen van poststroom worden in dit bestand ingelogd.