AnyConnect over IKEv2 naar ASA met AAA en certificaatverificatie

Inhoud

Inleiding

Dit document beschrijft hoe u een PC aan een Cisco adaptieve security applicatie (ASA) kunt aansluiten bij het gebruik van AnyConnect IPsec (IKEv2) evenals verificatie, autorisatie en accounting (AAA) verificatie.

> Opmerking: Het voorbeeld in dit document beschrijft alleen de relevante onderdelen die worden gebruikt om een IKEv2-verbinding tussen de ASA en AnyConnect te verkrijgen. Er is geen volledig configuratievoorbeeld beschikbaar. De configuratie van het netwerkadresomzetting (NAT) of de toegangslijst wordt in dit document niet beschreven of vereist.

Bereid het voor op de verbinding

In dit gedeelte worden de specificaties beschreven die vereist zijn voordat u uw pc op de ASA kunt aansluiten.

Certificaten met juiste EKU

Het is belangrijk om op te merken dat, ook al is dit niet nodig voor de ASA and AnyConnect-combinatie, RFC vereist dat certificaten Extended Key Gebruik (EKU) hebben:

- Het certificaat voor de ASA moet de **server-auth** EKU bevatten.

- Het certificaat voor de PC moet de **client-auth** EKU bevatten.

  Opmerking: Een IOS router met de recente softwareherziening kan EKU's op certificaten plaatsen.

Configuratie van de ASA

In dit gedeelte worden de ASA-configuraties beschreven die vereist zijn voordat de verbinding plaatsvindt.

> Opmerking: Met Cisco Adaptieve Security Devices Manager (ASDM) kunt u de basisconfiguratie met slechts een paar klikken maken. Cisco raadt u aan deze te gebruiken om fouten te voorkomen.

Configuratie van versleuteling

Hier is een crypto kaart voorbeeldconfiguratie:

```
crypto dynamic-map DYN 1 set pfs group1
crypto dynamic-map DYN 1 set ikev2 ipsec-proposal secure
crypto dynamic-map DYN 1 set reverse-route
crypto map STATIC 65535 ipsec-isakmp dynamic DYN
crypto map STATIC interface outside
```

IPsec-voorstellen

Hier is een IPsec-voorbeeldconfiguratie:

```
crypto ipsec ikev2 ipsec-proposal secure
 protocol esp encryption aes 3des
 protocol esp integrity sha-1
crypto ipsec ikev2 ipsec-proposal AES256-SHA
 protocol esp encryption aes-256
 protocol esp integrity sha-1
```

IKEv2-beleid

Hier is een IKEv2 beleidsvoorbeeldconfiguratie:

```
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5 2
prf sha
 lifetime seconds 86400
crypto ikev2 policy 10
 encryption aes-192
 integrity sha
group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 20
```

```
 encryption aes
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 30
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 40
 encryption des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
```

Clientservices en -certificaat

U moet clientservices en -certificaten op de juiste interface inschakelen, wat in dit geval de externe interface is. Hier is een voorbeeldconfiguratie:

```
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint OUTSIDE
ssl trust-point OUTSIDE outside
```

> Opmerking: Hetzelfde punt wordt ook toegewezen voor Secure Socket Layer (SSL), dat bedoeld en vereist is.

AnyConnect-profiel inschakelen

U moet het AnyConnect-profiel op de ASA inschakelen. Hier is een voorbeeldconfiguratie:

```
webvpn
 enable outside
anyconnect image disk0:/anyconnect-win-3.0.5080-k9.pkg 1 regex "Windows NT"
anyconnect profiles Anyconnect disk0:/anyconnect.xml
 anyconnect enable
tunnel-group-list enable
```

Gebruikersnaam, groepsbeleid en tunnelgroep

Hier is een voorbeeldconfiguratie voor een basale gebruikersnaam, groepsbeleid en tunnelgroep op de ASA:

```
group-policy GroupPolicy_AC internal
group-policy GroupPolicy_AC attributes
 dns-server value 4.2.2.2
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
default-domain value cisco.com
webvpn
anyconnect profiles value Anyconnect type user
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15
tunnel-group AC type remote-access
tunnel-group AC general-attributes
```

```
address-pool VPN-POOL
 default-group-policy GroupPolicy_AC
tunnel-group AC webvpn-attributes
 authentication aaa certificate
 group-alias AC enable
 group-url https://bsns-asa5520-1.cisco.com/AC enable
 without-csd
```

AnyConnect-profiel

Hier is een voorbeeldprofiel met de desbetreffende delen in **vet weergegeven**:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation=
 "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false
 </AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="true">Automatic
 </RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
</ClientInitialization>
<ServerList>
<HostEntry>




        bsns-asa5520-1
<HostAddress>bsns-asa5520-1.cisco.com</HostAddress>
<UserGroup>AC</UserGroup>
<PrimaryProtocol>IPsec</PrimaryProtocol>
```

```
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

Hier zijn een paar belangrijke opmerkingen over dit configuratievoorbeeld:

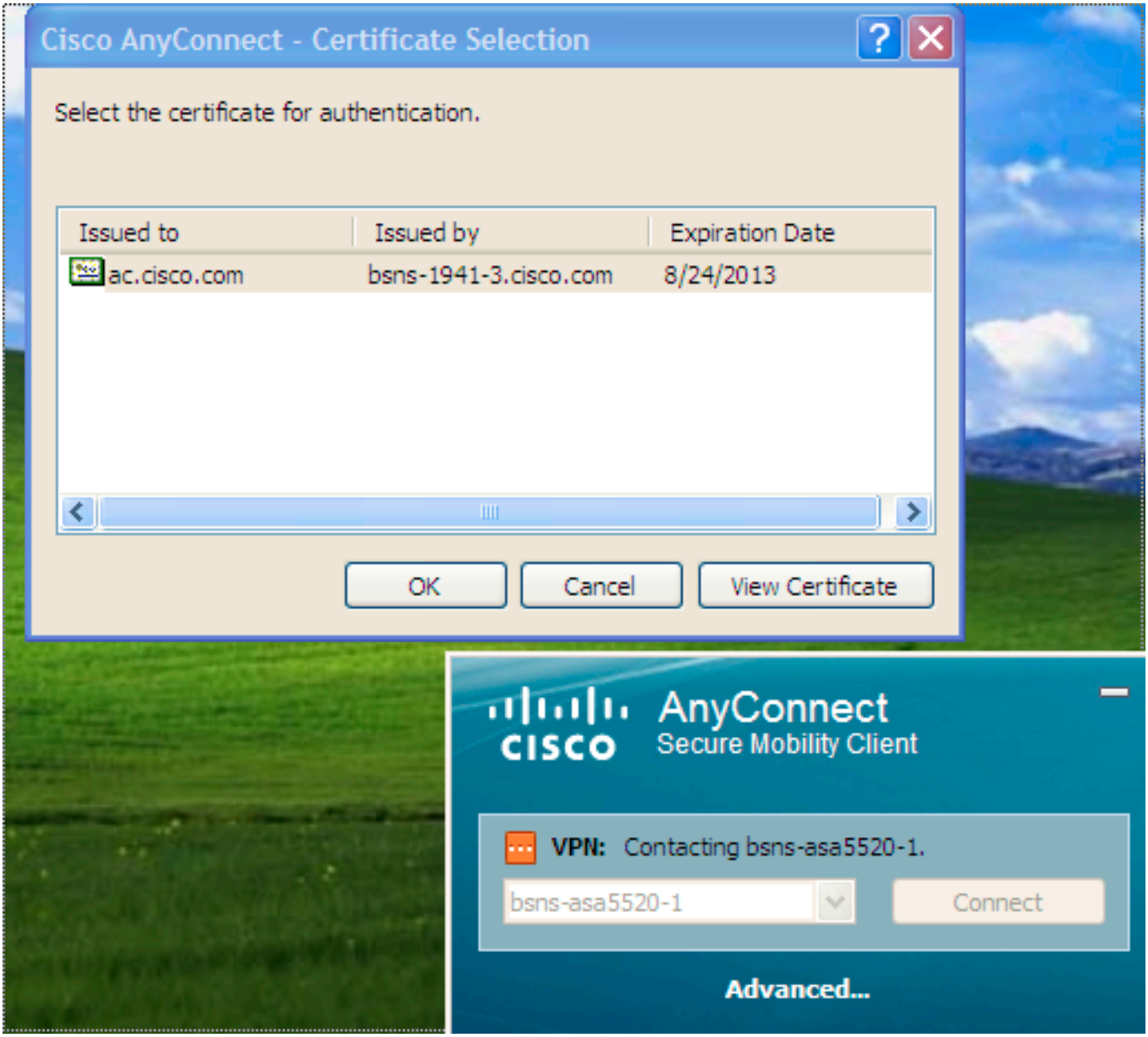
- Wanneer u het profiel maakt, moet het HostAddress overeenkomen met de certificaatnaam (GN) op het certificaat dat wordt gebruikt voor IKEv2. Voer de opdracht **crypto ikev2** externe **access** trustpoint in om dit te definiëren.
- De UserGroup moet de naam van de tunnelgroep overeenkomen waarop de IKEv2-verbinding valt. Als ze niet overeenkomen, faalt de verbinding vaak en de debugs duiden op een Diffie-Hellman (DH) groep mismatch of een vergelijkbaar vals negatief.

De verbinding maken

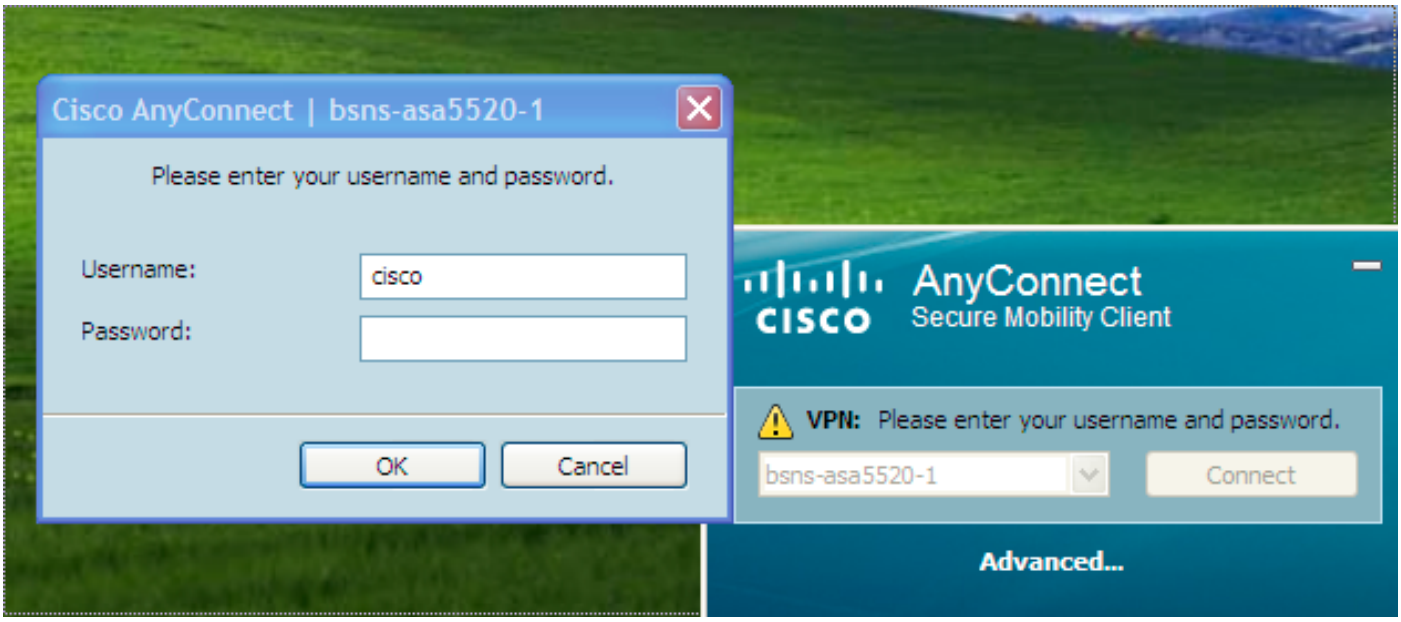
In dit gedeelte wordt de PC-to-ASA verbinding beschreven wanneer het profiel al aanwezig is.

> Opmerking: De informatie die u in de GUI invoert om verbinding te maken, is de <HostName>-waarde die in het AnyConnect-profiel wordt ingesteld. In dit geval wordt **bsns-asa5520-1** ingevoerd, niet de volledige FQDN-naam (Full Qualified Domain Name, FQDN).

Wanneer u voor het eerst probeert verbinding te maken met AnyConnect, wordt u gevraagd het certificaat te selecteren (indien automatische selectie van het certificaat is uitgeschakeld):

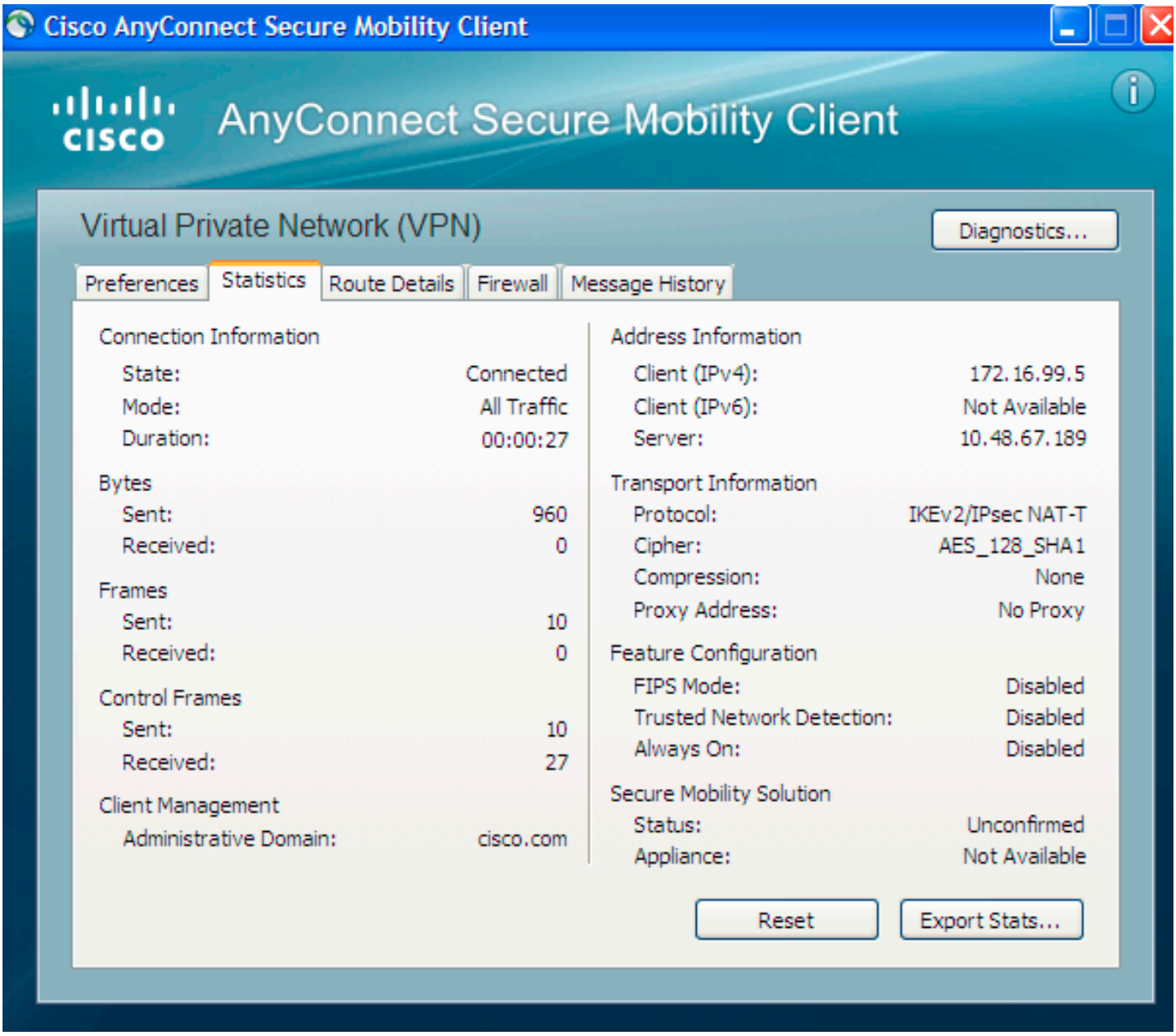


U moet vervolgens de gebruikersnaam en het wachtwoord invoeren:



Zodra de gebruikersnaam en het wachtwoord zijn geaccepteerd, is de verbinding succesvol en

kunnen de AnyConnect-statistieken worden geverifieerd:



Verificatie van ASA

Voer deze opdracht in op de ASA om te controleren of de verbinding IKEv2 evenals AAA en certificatie gebruikt:

```
bsns-asa5520-1# show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed
Username : cisco Index : 6
Assigned IP : 172.16.99.5 Public IP : 1.2.3.4
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : AES256 AES128 Hashing : none SHA1 SHA1
Bytes Tx : 0 Bytes Rx : 960
Pkts Tx : 0 Pkts Rx : 10
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_AC Tunnel Group : AC
Login Time : 15:45:41 UTC Tue Aug 28 2012
Duration : 0h:02m:41s
```

```
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1
AnyConnect-Parent:
Tunnel ID : 6.1
Public IP : 1.2.3.4
Encryption : none Auth Mode : Certificate and userPassword
 Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client Type : AnyConnect
Client Ver : 3.0.08057
IKEv2:
Tunnel ID : 6.2
UDP Src Port : 60468 UDP Dst Port : 4500
Rem Auth Mode: Certificate and userPassword
 Loc Auth Mode: rsaCertificate
 Encryption : AES256 Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86238 Seconds
PRF : SHA1 D/H Group : 5
Filter Name :
Client OS : Windows
IPsecOverNatT:
Tunnel ID : 6.3
Local Addr : 0.0.0.0/0.0.0.0/0/0
Remote Addr : 172.16.99.5/255.255.255.255/0/0
Encryption : AES128 Hashing : SHA1\
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 28638 Seconds
Rekey Int (D): 4608000 K-Bytes Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Bytes Tx : 0 Bytes Rx : 960
Pkts Tx : 0 Pkts Rx : 10
```

gekende Caveats

Dit zijn de bekende voorbehouden en kwesties die te maken hebben met de informatie die in dit document wordt beschreven:

- De IKEv2 en SSL trustpoints moeten hetzelfde zijn.
- Cisco raadt u aan om FQDN als GN te gebruiken voor de ASA-zijcertificaten. Zorg ervoor dat u dezelfde FQDN voor het <HostAddress> in het AnyConnect-profiel hebt geraadpleegd.
- Vergeet niet de waarde <HostName> in het AnyConnect-profiel in te voeren wanneer u verbinding maakt.
- Zelfs in de IKEv2 configuratie, wanneer AnyConnect met de ASA verbonden is, downloads het profiel en de binaire updates via SSL, maar niet IPsec.
- De AnyConnect-verbinding via IKEv2 naar de ASA maakt gebruik van EAP-AnyConnect, een eigen mechanisme dat een eenvoudiger implementatie mogelijk maakt.