AnyConnect über IKEv2 zu ASA mit AAA- und Zertifikatsauthentifizierung

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie einen PC mithilfe von AnyConnect IPsec (IKEv2) und Authentifizierung, Autorisierung und Abrechnung (AAA) mit einer Cisco Adaptive Security Appliance (ASA) verbinden.

> **Hinweis**: Im in diesem Dokument gezeigten Beispiel werden nur die relevanten Teile beschrieben, die für die Herstellung einer IKEv2-Verbindung zwischen ASA und AnyConnect verwendet werden. Ein vollständiges Konfigurationsbeispiel wird nicht bereitgestellt. Die Network Address Translation (NAT)- oder die Zugriffslistenkonfiguration werden in diesem Dokument weder beschrieben noch erforderlich.

Für die Verbindung vorbereiten

In diesem Abschnitt werden die erforderlichen Vorgänge beschrieben, bevor Sie Ihren PC mit der ASA verbinden können.

Zertifikate mit ordnungsgemäßem EKU

Es ist zu beachten, dass die Kombination aus ASA und AnyConnect zwar nicht erforderlich ist, für die RFC jedoch die Verwendung von Zertifikaten mit Extended Key Usage (EKU) erforderlich ist:

- Das Zertifikat für die ASA muss das **Server-Auth** EKU enthalten.

- Das Zertifikat für den PC muss das **client-auth** EKU enthalten.

  Hinweis: Ein IOS-Router mit der aktuellen Softwareversion kann EKUs auf Zertifikate platzieren.

Konfiguration auf der ASA

In diesem Abschnitt werden die ASA-Konfigurationen beschrieben, die vor dem Eintreten der Verbindung erforderlich sind.

> **Hinweis**: Mit dem Cisco Adaptive Security Device Manager (ASDM) können Sie die Basiskonfiguration mit nur wenigen Klicks erstellen. Cisco empfiehlt die Verwendung, um Fehler zu vermeiden.

Konfiguration der Crypto Map

Hier eine Beispielkonfiguration für eine Crypto Map:

```
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-Angebote

Hier ein Beispiel für eine IPsec-Angebotskonfiguration:

```
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-Richtlinien

Nachfolgend finden Sie ein IKEv2-Richtlinienbeispiel für die Konfiguration:

```
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
```

Clientdienste und Zertifikat

Sie müssen Clientdienste und Zertifikate auf der richtigen Schnittstelle aktivieren, also in diesem Fall auf der externen Schnittstelle. Hier ein Beispiel für eine Konfiguration:

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

> **Hinweis**: Derselbe Vertrauenspunkt wird auch Secure Sockets Layer (SSL) zugewiesen, was beabsichtigt und erforderlich ist.

AnyConnect-Profil aktivieren

Sie müssen das AnyConnect-Profil auf der ASA aktivieren. Hier ein Beispiel für eine Konfiguration:

```
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
```

Benutzername, Gruppenrichtlinie und Tunnelgruppe

Im Folgenden finden Sie ein Beispiel für eine grundlegende Konfiguration für einen Benutzernamen, eine Gruppenrichtlinie und eine Tunnelgruppe auf der 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-Profil

Im Folgenden finden Sie ein Beispielprofil mit den entsprechenden **fett** dargestellten Teilen:

```
<?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 einige wichtige Hinweise zu diesem Konfigurationsbeispiel:

- Wenn Sie das Profil erstellen, muss die HostAddress mit dem Zertifikatsnamen (CN) des Zertifikats übereinstimmen, das für IKEv2 verwendet wird. Geben Sie den Befehl **crypto ikev2 remote-access trustpoint** ein, um dies zu definieren.

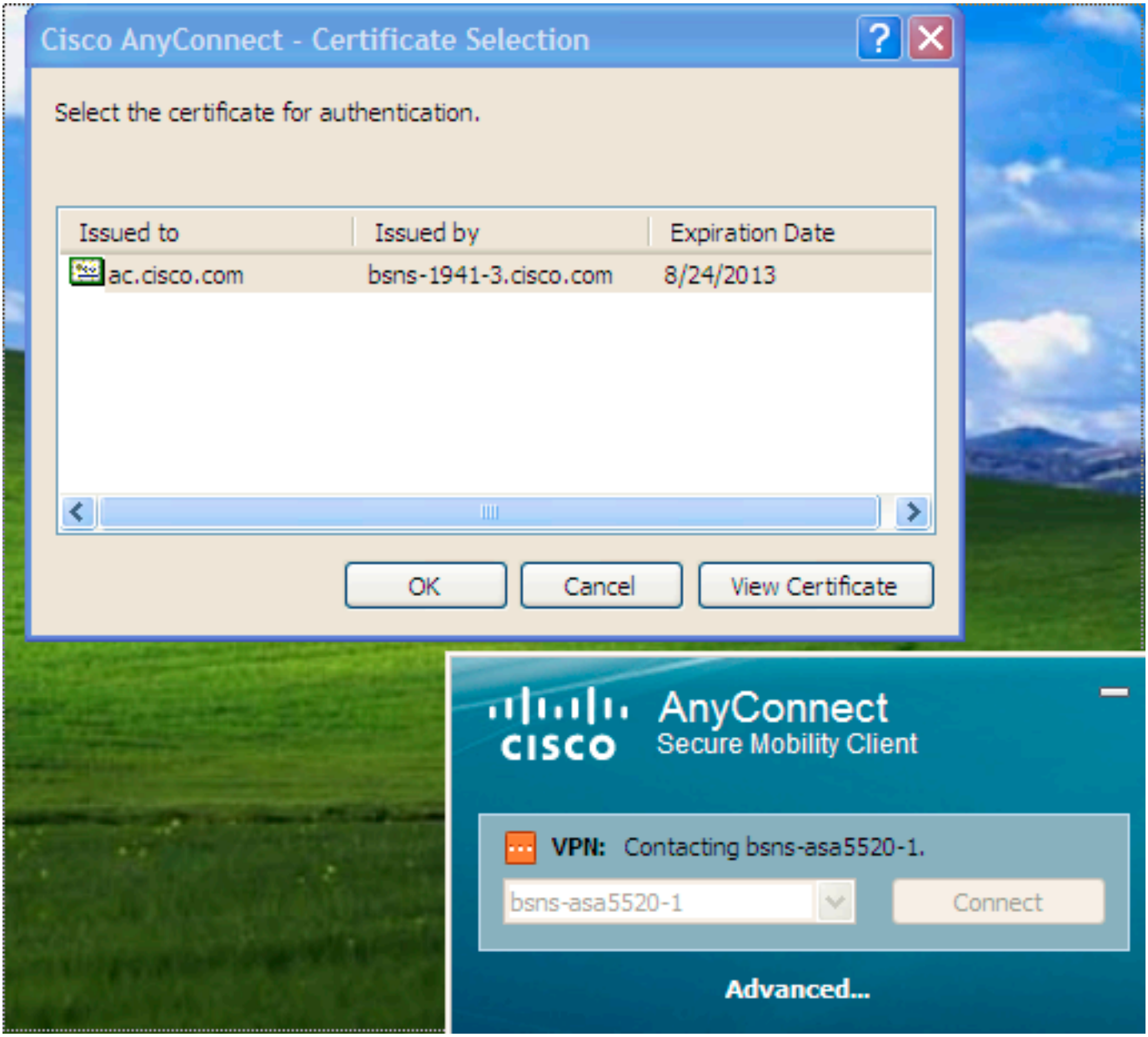
- Die UserGroup muss mit dem Namen der Tunnelgruppe übereinstimmen, der die IKEv2-Verbindung zugewiesen wird. Wenn sie nicht übereinstimmen, schlägt die Verbindung häufig fehl, und die Debug-Meldungen weisen auf eine Diffie-Hellman (DH)-Gruppenungleichheit oder ein ähnliches falsches Negativ hin.

Verbindung herstellen

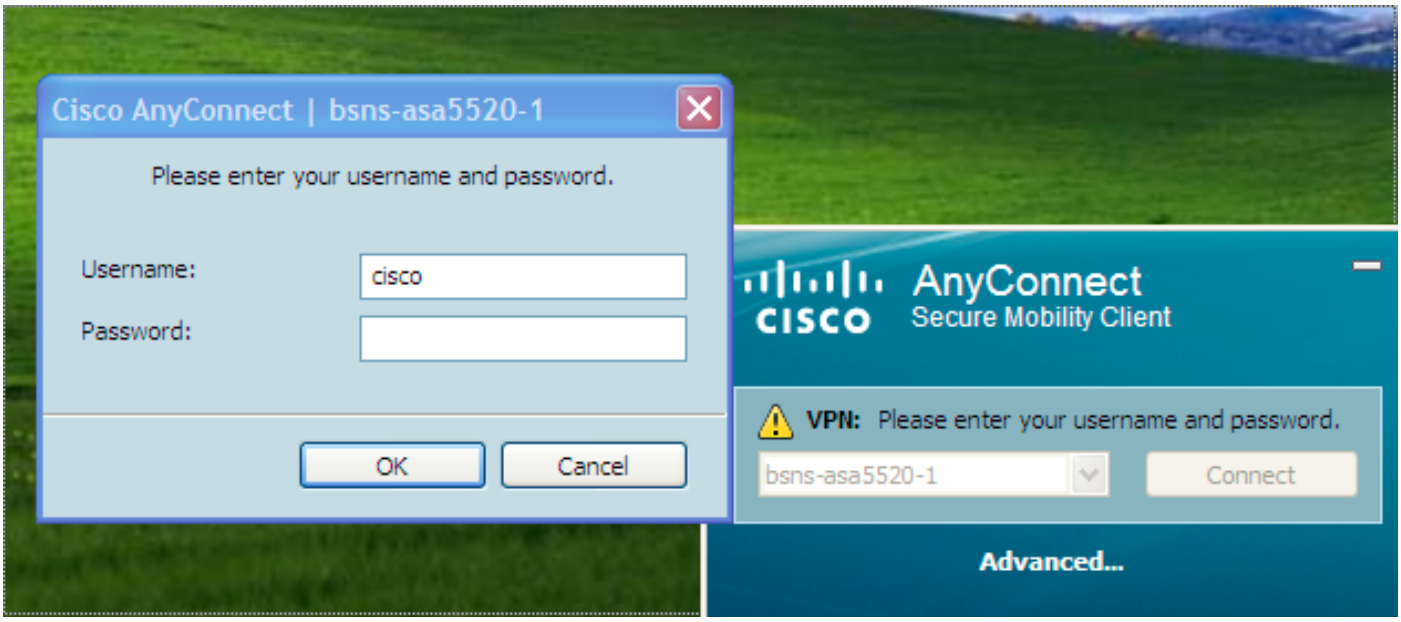
In diesem Abschnitt wird die Verbindung zwischen PC und ASA beschrieben, wenn das Profil bereits vorhanden ist.

> **Hinweis**: Die Informationen, die Sie in die GUI eingeben, um eine Verbindung herzustellen, sind der **<HostName>**-Wert, der im AnyConnect-Profil konfiguriert ist. In diesem Fall wird **bsns-asa5520-1** eingegeben, nicht der vollständige vollqualifizierte Domänenname (Fully Qualified Domain Name, FQDN).

Beim ersten Verbindungsversuch über AnyConnect werden Sie vom Gateway aufgefordert, das Zertifikat auszuwählen (wenn die automatische Zertifikatauswahl deaktiviert ist):

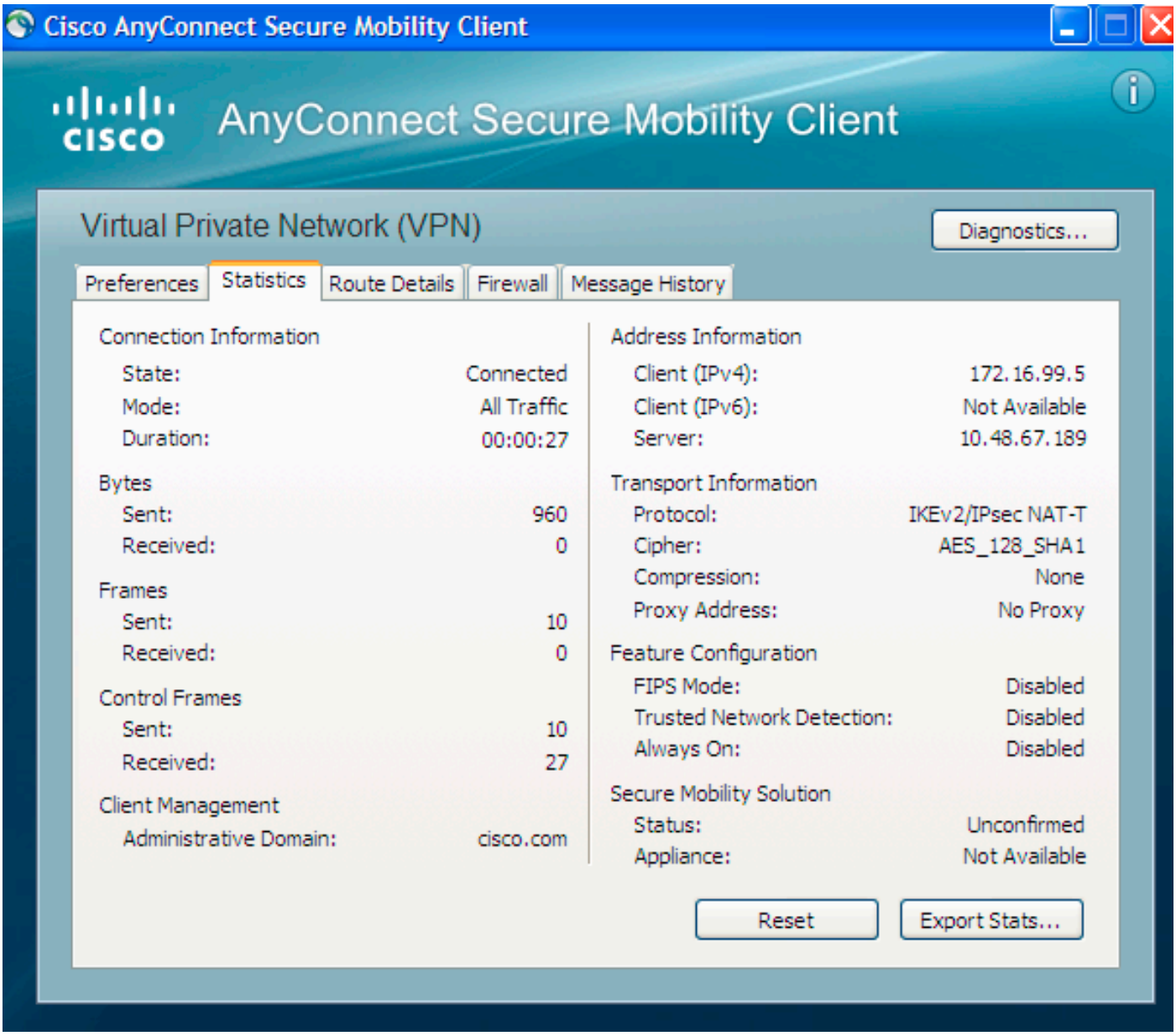


Geben Sie dann den Benutzernamen und das Kennwort ein:



Sobald der Benutzername und das Kennwort akzeptiert wurden, ist die Verbindung erfolgreich,

und die AnyConnect-Statistiken können überprüft werden:



Überprüfung auf ASA

Geben Sie diesen Befehl auf der ASA ein, um zu überprüfen, ob die Verbindung IKEv2 sowie AAA und Zertifikatsauthentifizierung verwendet:

```
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
```

Bekannte Einwände

Dies sind die bekannten Probleme und Probleme im Zusammenhang mit den in diesem Dokument beschriebenen Informationen:

- Die IKEv2- und SSL-Vertrauenspunkte müssen identisch sein.
- Cisco empfiehlt, den FQDN als CN für ASA-seitige Zertifikate zu verwenden. Stellen Sie sicher, dass Sie im AnyConnect-Profil auf denselben FQDN für die <HostAddress> verweisen.
- Denken Sie daran, den <HostName>-Wert aus dem AnyConnect-Profil einzufügen, wenn Sie eine Verbindung herstellen.
- Selbst in der IKEv2-Konfiguration lädt AnyConnect, wenn eine Verbindung zur ASA hergestellt wird, Profil- und Binäraktualisierungen über SSL herunter, nicht aber über IPsec.
- Die AnyConnect-Verbindung über IKEv2 zur ASA nutzt EAP-AnyConnect, einen proprietären Mechanismus, der die Implementierung vereinfacht.