AnyConnect sobre IKEv2 ao ASA com AAA e certificado de autenticação

Índice

Introdução

Este documento descreve como conectar um PC a uma ferramenta de segurança adaptável de Cisco (ASA) com o uso do IPsec de AnyConnect (IKEv2) assim como certificate e autenticação do Authentication, Authorization, and Accounting (AAA).

> Nota: O exemplo que é fornecido neste documento descreve somente as partes relevantes que são usadas a fim obter uma conexão IKEv2 entre o ASA e o AnyConnect. Um exemplo da configuração direta não é fornecido. O Network Address Translation (NAT) ou a configuração de lista de acesso não são descritos nem são exigidos neste documento.

Prepare para a conexão

Esta seção descreve os perparations que são exigidos antes que você possa conectar seu PC ao ASA.

Certificados com EKU apropriado

Éimportante notar que mesmo que não se exija para a combinação ASA e de AnyConnect, o RFC

exige que os Certificados estenderam o uso chave (EKU):

- O certificado para o ASA deve conter o server-**AUTH** EKU.
- O certificado para o PC deve conter o cliente-**AUTH** EKU.

  Nota: Um IOS Router com a revisão do software recente pode colocar EKU em Certificados.

Configuração no ASA

Esta seção descreve as configurações ASA que são exigidas antes que a conexão ocorra.

> Nota: O Cisco Adaptive Security Device Manager (ASDM) permite que você crie a configuração básica com somente alguns cliques. Cisco recomenda que você o usa a fim evitar erros.

Configuração do crypto map

Está aqui um exemplo de configuração do 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
```

Propostas do IPsec

Está aqui um exemplo de configuração da proposta do IPsec:

```
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
```

Políticas IKEv2

Está aqui um exemplo de configuração da política IKEv2:

```
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
```

Serviços de cliente e certificado

Você deve permitir serviços de cliente e Certificados na relação correta, que é a interface externa neste caso. Está aqui um exemplo de configuração:

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

> Nota: O mesmo ponto confiável é atribuído igualmente para o secure sockets layer (SSL), que é pretendido e exigido.

Permita o perfil de AnyConnect

Você deve permitir o perfil de AnyConnect no ASA. Está aqui um exemplo de configuração:

```
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
```

Username, Grupo-política, e grupo de túneis

Está aqui um exemplo de configuração para um username, uma grupo-política, e um grupo de túneis básicos no 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
```

Perfil de AnyConnect

Está aqui um perfil do exemplo com as partes relevantes mostradas em **corajoso**:

```
<?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>
<HostName>bsns-asa5520-1</HostName>
<HostAddress>bsns-asa5520-1.cisco.com</HostAddress>
<UserGroup>AC</UserGroup>
<PrimaryProtocol>IPsec</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

Estão aqui algumas observações importantes sobre este exemplo de configuração:

- Quando você cria o perfil, o host address deve combinar o nome do certificado (CN) no certificado que é usado para IKEv2. Incorpore o comando **cripto do ponto confiável do acesso remoto ikev2** a fim definir isto.

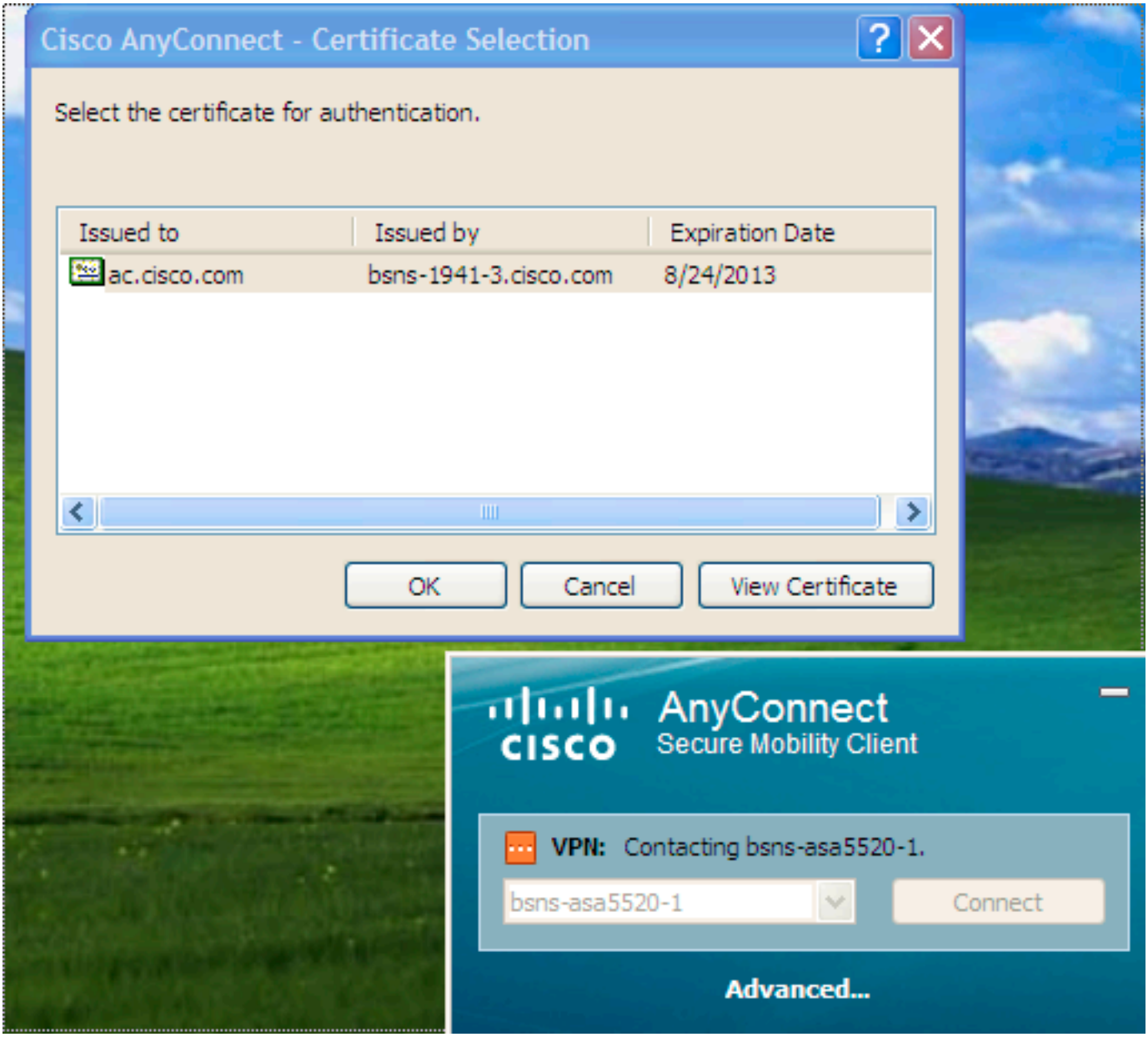
- O grupo de utilizadores deve combinar o nome do tunnelgroup a que a conexão IKEv2 cai. Se não combinam, a conexão falha frequentemente e debuga indicam uma má combinação do grupo do Diffie-Hellman (DH) ou um falso negativo similar.

Faça a conexão

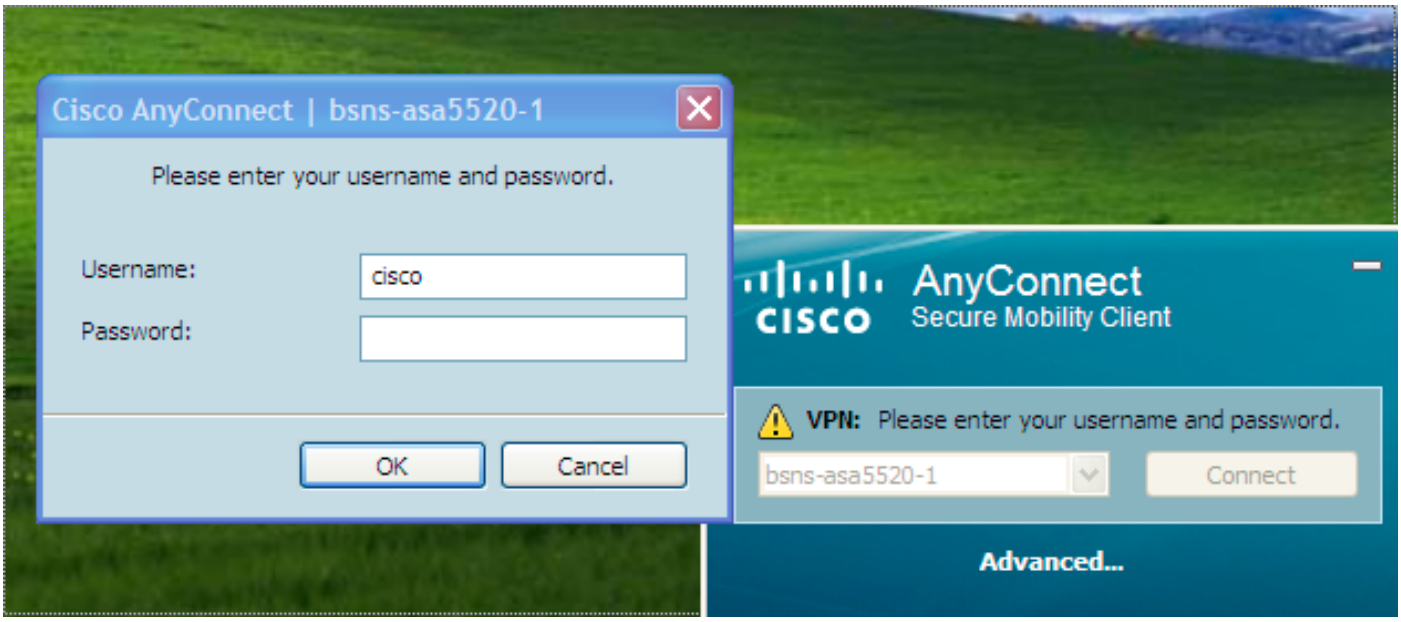
Esta seção descreve a conexão PC-à-ASA quando o perfil está já atual.

> Nota: A informação que você entra no GUI a fim conectar é o valor do **<hostname>** que é configurado no perfil de AnyConnect. Neste caso, **bsns-asa5520-1** é incorporado, não o nome de domínio totalmente qualificado completo (FQDN).

Quando você tenta primeiramente conectar com AnyConnect, o gateway alerta-o selecionar o certificado (se a seleção automática do certificado é desabilitada):

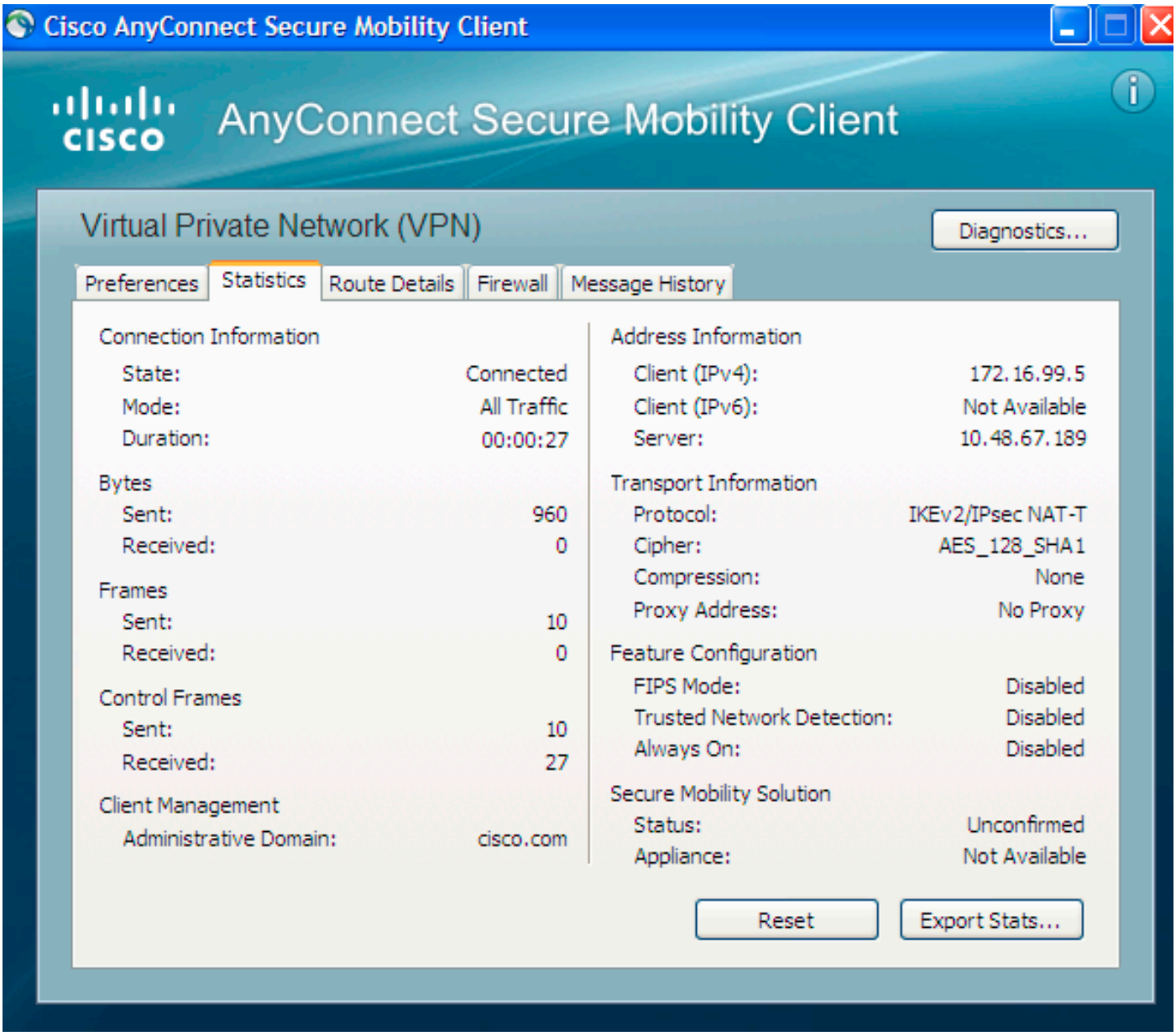


Você deve então incorporar o nome de usuário e senha:



Uma vez que o nome de usuário e senha é aceitado, a conexão é bem sucedida e as estatísticas

de AnyConnect podem ser verificadas:



Verificação no ASA

Incorpore este comando no ASA a fim verificar que a conexão usa IKEv2 assim como AAA e certificado de autenticação:

```
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
```

Caveats conhecidos

Estas são as advertências conhecidas e as edições que são relacionadas à informação que é descrita neste documento:

- Os pontos confiáveis IKEv2 e SSL devem ser os mesmos.
- Cisco recomenda que você usa o FQDN como o CN para os Certificados do ASA-lado. Assegure-se de que você proveja o mesmo FQDN para o <HostAddress> no perfil de AnyConnect.
- Recorde introduzir o valor do <hostname> do perfil de AnyConnect quando você conecta.
- Mesmo na configuração IKEv2, quando AnyConnect conecta ao ASA, transfere o perfil e atualizações binárias sobre o SSL, mas não IPsec.
- A conexão de AnyConnect sobre IKEv2 ao ASA usa o EAP-AnyConnect, um mecanismo proprietário que permita uma aplicação mais simples.