

AnyConnect sobre IKEv2 al ASA con el AAA y la autenticación certificada

Contenido

[Introducción](#)

[Prepárese para la conexión](#)

[Certificados con el ECU apropiado](#)

[Configuración en el ASA](#)

[Configuración de la correspondencia de criptografía](#)

[Ofertas del IPSec](#)

[Directivas IKEv2](#)

[Servicios al cliente y certificado](#)

[Perfil de AnyConnect del permiso](#)

[Nombre de usuario, Grupo-directiva, y grupo de túnel](#)

[Perfil de AnyConnect](#)

[Haga la conexión](#)

[Verificación en el ASA](#)

[Advertencias conocidas](#)

Introducción

Este documento describe cómo conectar un PC con un dispositivo de seguridad adaptante de Cisco (ASA) con el uso del IPSec de AnyConnect (IKEv2) así como certificarlo y el autenticación del Authentication, Authorization, and Accounting (AAA).

Nota: El ejemplo que se proporciona en este documento describe solamente a las partes pertinentes que se utilizan para obtener una conexión IKEv2 entre el ASA y el AnyConnect. Un ejemplo de la configuración total no se proporciona. El Network Address Translation (NAT) o la configuración de la lista de acceso no se describe ni se requiere en este documento.

Prepárese para la conexión

Esta sección describe los preparaciones que se requieren antes del usted puede conectarse su PC al ASA.

Certificados con el ECU apropiado

Es importante observar que aunque no se requiere para la combinación ASA y de AnyConnect, el RFC requiere que los Certificados hayan ampliado el uso dominante (EKU):

- El certificado para el ASA debe contener el EKU del servidor-**auth**.
- El certificado para el PC debe contener el EKU del cliente-**auth**.

Nota: Un router IOS con la revisión del software reciente puede colocar EKUs sobre los Certificados.

Configuración en el ASA

Esta sección describe las configuraciones ASA se requieren que antes de que ocurra la conexión.

Nota: El Cisco Adaptive Security Device Manager (ASDM) permite que usted cree la configuración básica con solamente algunos tecleos. Cisco recomienda que usted lo utiliza para evitar los errores.

Configuración de la correspondencia de criptografía

Aquí está un ejemplo de configuración de la correspondencia de criptografía:

```
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
```

Ofertas del IPSec

Aquí está un ejemplo de configuración de la oferta del 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
```

Directivas IKEv2

Aquí está un ejemplo de configuración de la directiva 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
```

Servicios al cliente y certificado

Usted debe habilitar los Servicios al cliente y los Certificados en la interfaz correcta, que es la interfaz exterior en este caso. Aquí está un ejemplo de configuración:

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

Nota: El mismo trustpoint también se asigna para Secure Sockets Layer (SSL), se piensa y se requiere que.

Perfil de AnyConnect del permiso

Usted debe habilitar el perfil de AnyConnect en el ASA. Aquí está un ejemplo de configuración:

```
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
```

Nombre de usuario, Grupo-directiva, y grupo de túnel

Aquí está un ejemplo de configuración para un nombre de usuario, una grupo-directiva, y un grupo de túnel básicos en el 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

Aquí está un perfil del ejemplo con las partes pertinentes mostradas en intrépido:

```

<?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>
<PPPEExclusion UserControllable="false">Disable
<PPPEExclusionServerIP UserControllable="false"></PPPEExclusionServerIP>
</PPPEExclusion>
<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>

Aquí están algunas NOTAS IMPORTANTES sobre este ejemplo de configuración:

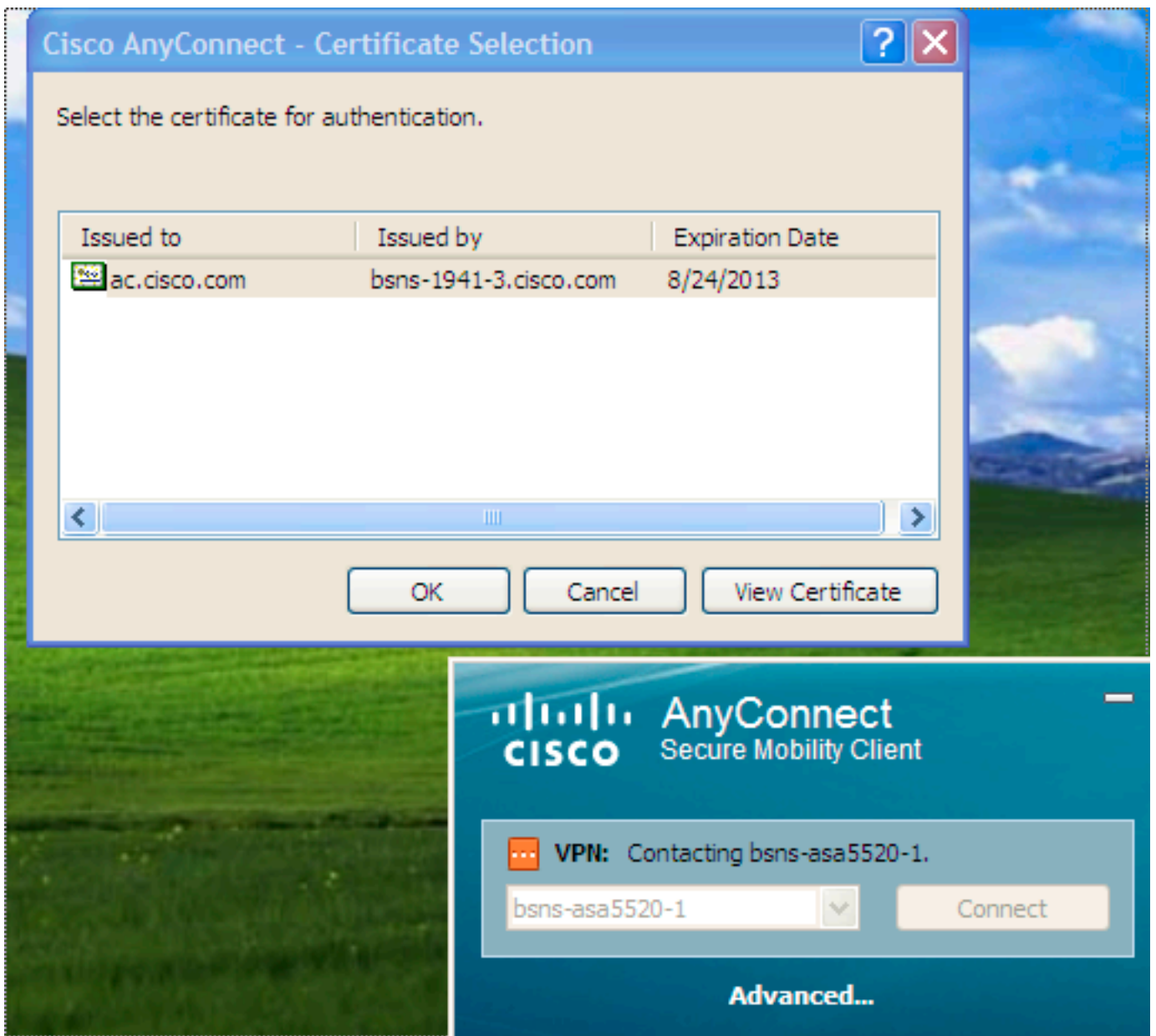
- Cuando usted crea el perfil, el host address debe hacer juego el nombre del certificado (CN) en el certificado que se utiliza para IKEv2. Ingrese el comando **crypto del trustpoint del acceso remoto ikev2** para definir esto.
- El grupo de usuarios debe hacer juego el nombre del tunnelgroup al cual la conexión IKEv2 cae. Si no hacen juego, la conexión falla a menudo y los debugs indican una discordancia del grupo del Diffie-Hellman (DH) o una negativa falsa similar.

Haga la conexión

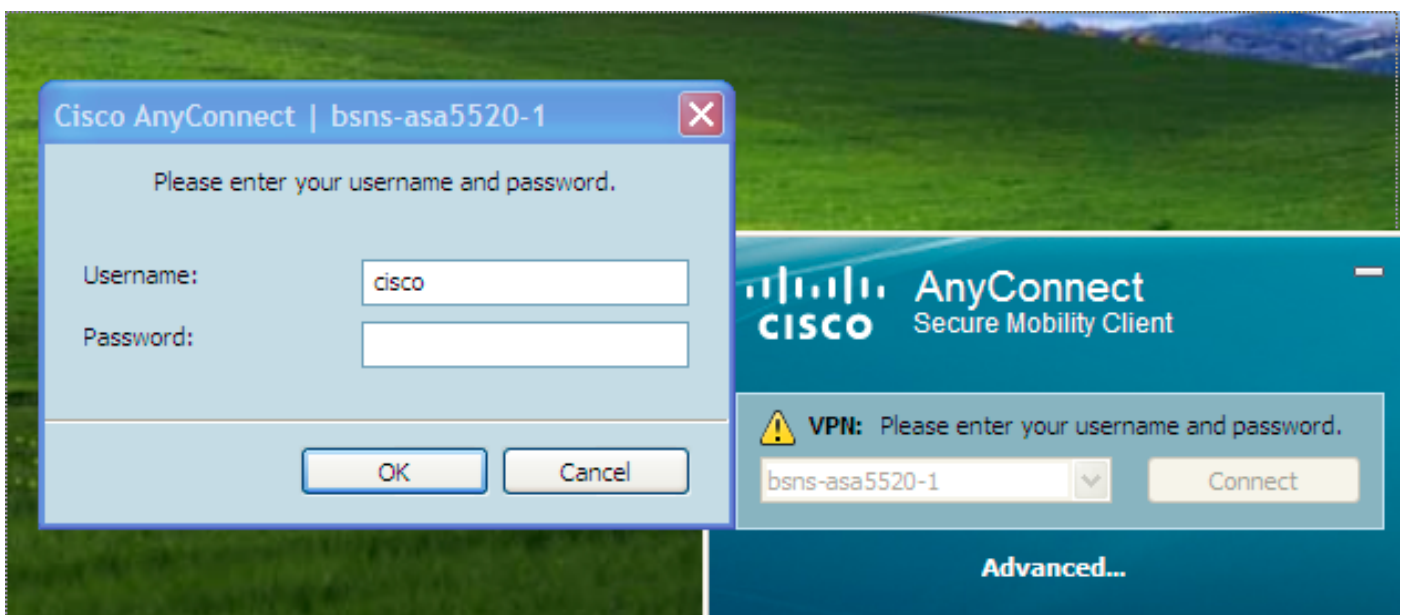
Esta sección describe la conexión PC-a-ASA cuando el perfil está ya presente.

Nota: La información que usted entra en el GUI para conectar es el valor del <hostname> que se configura en el perfil de AnyConnect. En este caso, se ingresa **bsns-asa5520-1**, no el Nombre de dominio totalmente calificado (FQDN) completo (FQDN).

Cuando usted primero intenta conectar con AnyConnect, el gateway le indica a que seleccione el certificado (si se inhabilita la selección automática del certificado):

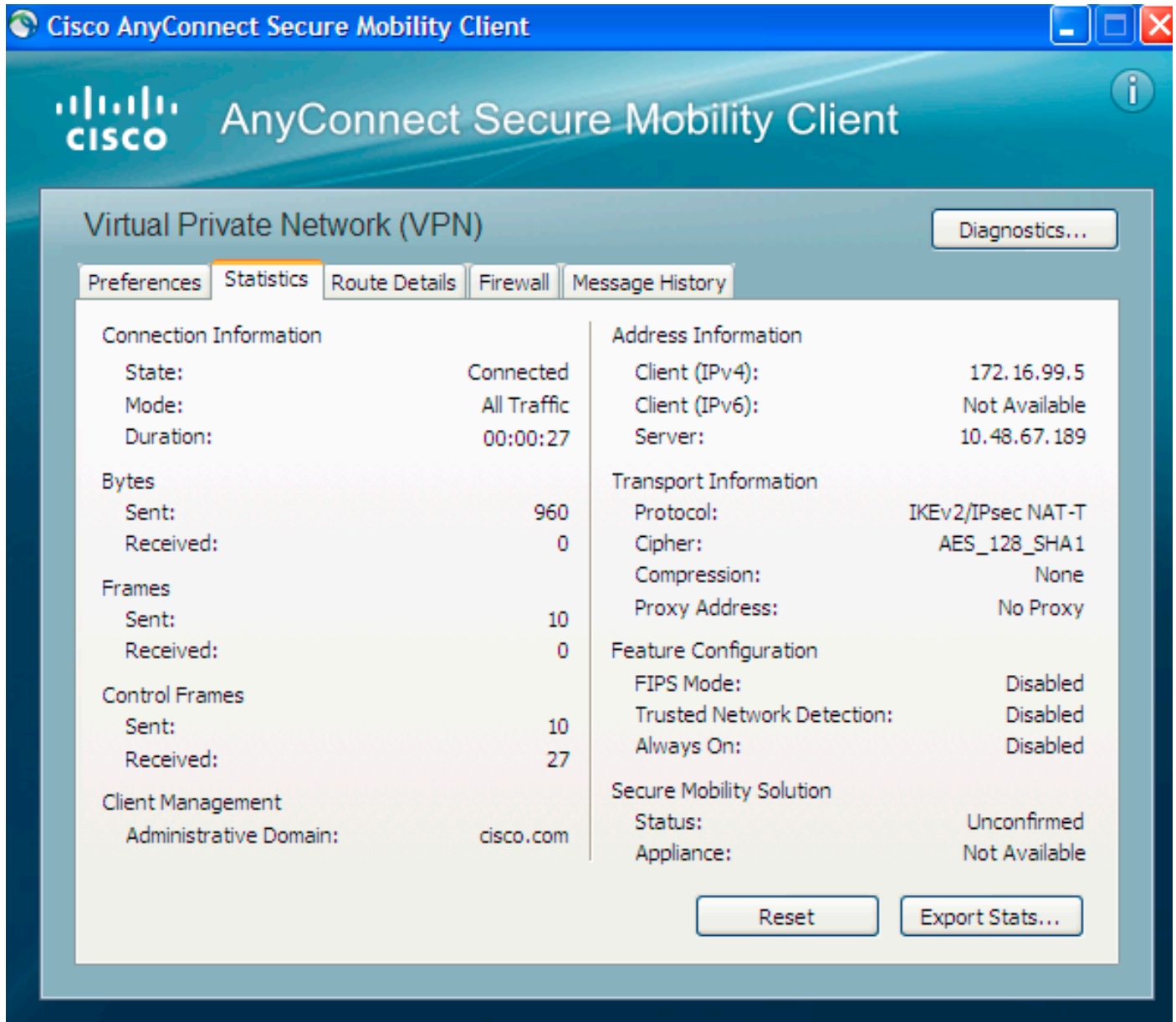


Usted debe entonces ingresar el nombre de usuario y contraseña:



Una vez que se valida el nombre de usuario y contraseña, la conexión es acertada y las

estadísticas de AnyConnect pueden ser verificadas:



Verificación en el ASA

Ingrese este comando en el ASA para verificar que la conexión utiliza IKEv2 así como AAA y autenticación certificada:

```
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

Advertencias conocidas

Éstos son las advertencias conocidas y los problemas que se relacionan con la información que se describe en este documento:

- El IKEv2 y el trustpoints SSL deben ser lo mismo.
- Cisco recomienda que usted utiliza el FQDN como el CN para los Certificados del ASA-lado. Asegúrese de que usted se refiera al mismo FQDN para el <HostAddress> al perfil de AnyConnect.
- Recuerde insertar el valor del <hostname> del perfil de AnyConnect cuando usted conecta.
- Incluso en la configuración IKEv2, cuando AnyConnect conecta con el ASA, descarga el perfil y las actualizaciones binarias sobre el SSL, pero no el IPSec.
- La conexión de AnyConnect sobre IKEv2 al ASA utiliza el EAP-AnyConnect, un mecanismo propietario que permita una implementación más simple.