AnyConnect over IKEv2 su ASA con autenticazione AAA e certificato

Sommario

Introduzione

In questo documento viene descritto come connettere un PC a una appliance Cisco Adaptive Security (ASA) con l'uso di AnyConnect IPsec (IKEv2) e con l'autenticazione AAA (Certificate and Authentication, Authorization, and Accounting).

> **Nota:** Nell'esempio riportato in questo documento vengono descritte solo le parti rilevanti per ottenere una connessione IKEv2 tra l'appliance ASA e AnyConnect. Non viene fornito un esempio di configurazione completo. La configurazione NAT (Network Address Translation) o dell'elenco degli accessi non è descritta né richiesta in questo documento.

Preparazione connessione

In questa sezione vengono descritti i preparativi necessari per connettere il PC all'appliance ASA.

Certificati con EKU appropriato

Èimportante notare che anche se non è richiesto per l'appliance ASA e la combinazione di AnyConnect, la RFC richiede che i certificati abbiano l'utilizzo esteso della chiave (EKU):

- Il certificato per l'ASA deve contenere l'EKU **server-auth**.
- Il certificato per il PC deve contenere l'EKU di **autenticazione client**.

Nota: Un router IOS con la recente revisione software può inserire gli EKU nei certificati.

Configurazione sull'appliance ASA

In questa sezione vengono descritte le configurazioni ASA necessarie prima della connessione.

Nota: Cisco Adaptive Security Device Manager (ASDM) consente di creare la configurazione di base con pochi clic del mouse. Cisco consiglia di utilizzarlo per evitare errori.

Configurazione mappa crittografica

Di seguito è riportata la configurazione di un esempio di mappa crittografica:

```
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
```

Proposte IPSec

Di seguito è riportata una configurazione di esempio della proposta 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
```

Criteri IKEv2

Di seguito è riportata una configurazione di esempio del criterio 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
```

Servizi e certificati client

Ènecessario abilitare i servizi client e i certificati sull'interfaccia corretta, che in questo caso è l'interfaccia esterna. Di seguito è riportato un esempio di configurazione:

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

> **Nota:** Lo stesso trust point viene assegnato anche per SSL (Secure Sockets Layer), che è previsto e obbligatorio.

Abilita profilo AnyConnect

Ènecessario abilitare il profilo AnyConnect sull'appliance ASA. Di seguito è riportato un esempio di configurazione:

```
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
```

Nome utente, Criteri di gruppo e Tunnel-Group

Di seguito è riportato un esempio di configurazione per un nome utente di base, un gruppo di criteri e un gruppo di tunnel sull'appliance 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
```

Profilo AnyConnect

Di seguito è riportato un profilo di esempio con le parti interessate mostrate in **grassetto**:

```
<?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>
```

Di seguito sono riportate alcune note importanti su questo esempio di configurazione:

- Quando si crea il profilo, l'indirizzo host deve corrispondere al nome del certificato (CN) sul certificato utilizzato per IKEv2. Immettere il comando **crypto ikev2 remote-access trustpoint** per definire questa condizione.

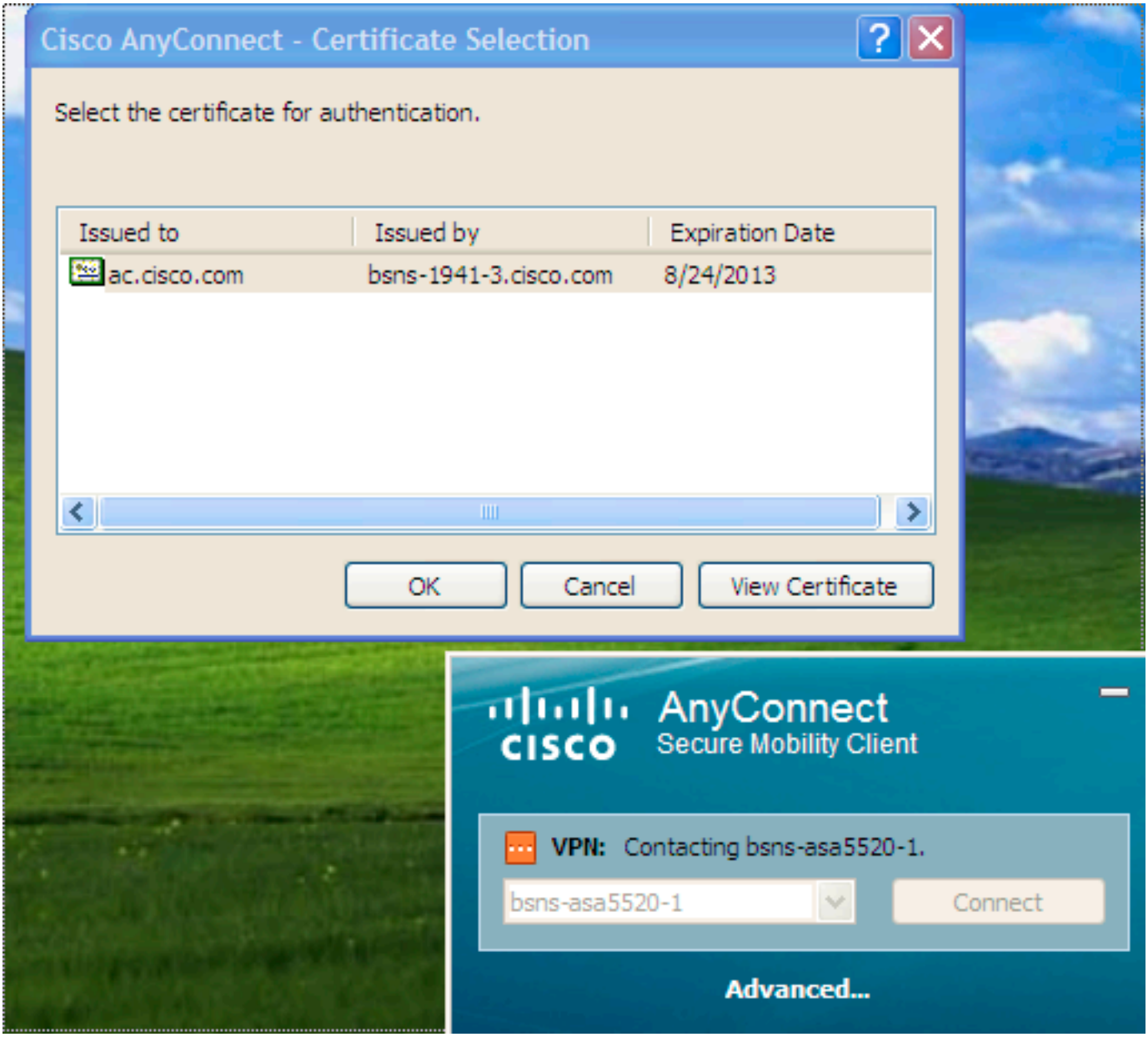
- Il gruppo di utenti deve corrispondere al nome del gruppo di tunnel a cui appartiene la connessione IKEv2. Se non corrispondono, la connessione spesso non riesce e i debug indicano una mancata corrispondenza del gruppo Diffie-Hellman (DH) o un falso negativo simile.

Crea connessione

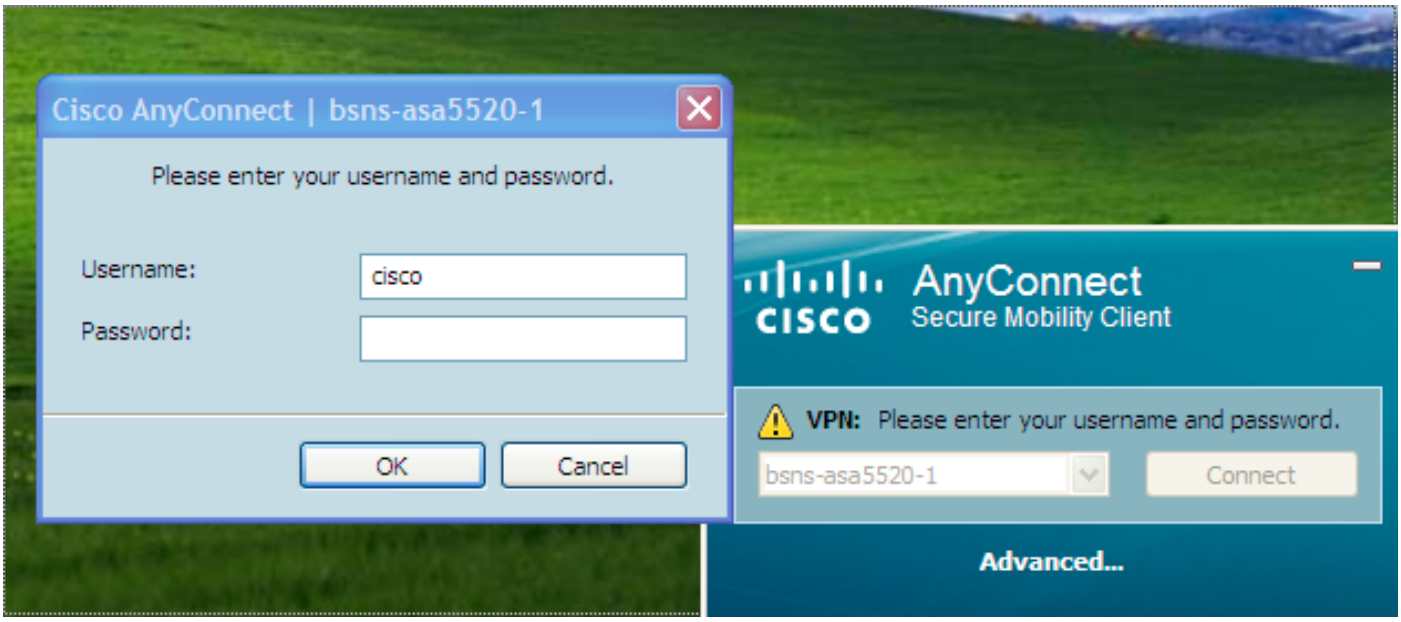
In questa sezione viene descritta la connessione da PC ad ASA quando il profilo è già presente.

> **Nota:** Le informazioni immesse nella GUI per la connessione sono il valore <HostName> configurato nel profilo AnyConnect. In questo caso, viene immesso **bsns-asa5520-1**, non il nome di dominio completo (FQDN).

Al primo tentativo di connessione tramite AnyConnect, il gateway chiede di selezionare il certificato (se la selezione automatica dei certificati è disabilitata):

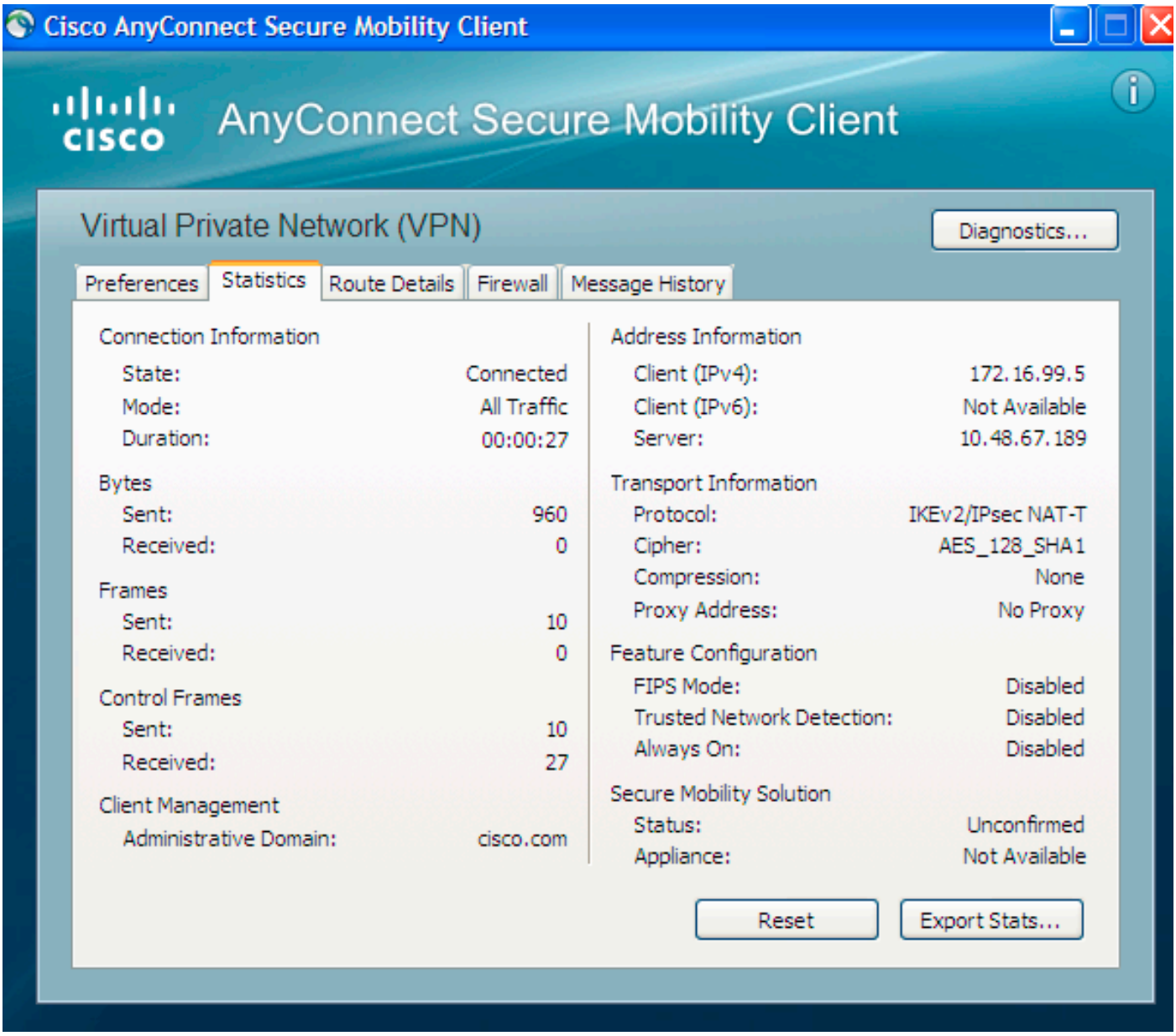


Immettere il nome utente e la password:



Dopo aver accettato il nome utente e la password, la connessione viene stabilita e le statistiche di

AnyConnect possono essere verificate:



Verifica sull'ASA

Immettere questo comando sull'appliance ASA per verificare che la connessione utilizzi sia l'autenticazione IKEv2 sia l'autenticazione AAA e dei certificati:

```
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
```

Avvertenze note

Di seguito sono riportati gli avvertimenti e i problemi noti relativi alle informazioni descritte nel presente documento:

- I trust point IKEv2 e SSL devono essere uguali.
- Cisco consiglia di utilizzare l'FQDN come CN per i certificati lato ASA. Verificare di fare riferimento allo stesso FQDN per <HostAddress> nel profilo AnyConnect.
- Ricordarsi di inserire il valore <HostName> dal profilo AnyConnect quando si esegue la connessione.
- Anche nella configurazione IKEv2, quando AnyConnect si connette all'ASA, scarica gli aggiornamenti binari e dei profili su SSL, ma non su IPsec.
- La connessione AnyConnect su IKEv2 all'appliance ASA utilizza EAP-AnyConnect, un meccanismo proprietario che consente un'implementazione più semplice.