مادختساب IKEv2 إلى ASA عبر AnyConnect مصادقة الشهادة و AAA

المحتويات

المقدمة

يوضح هذا المستند كيفية توصيل جهاز كمبيوتر بجهاز أمان قابل للتكيف (ASA) من Cisco باستخدام مصادقة AnyConnect IPsec (IKEv2) بالإضافة إلى الشهادة والمصادقة والتفويض والمحاسبة (AAA).

ملاحظة: يوضح المثال الوارد في هذا المستند الأجزاء ذات الصلة فقط التي يتم إستخدامها للحصول على اتصال IKEv2 بين ASA و AnyConnect. لم يتم توفير مثال تكوين كامل. لم يتم وصف تكوين ترجمة عنوان الشبكة (NAT) أو قائمة الوصول أو أنه مطلوب في هذا المستند.

التحضير للاتصال

يصف هذا القسم العمليات المطلوبة قبل أن تتمكن من توصيل جهاز الكمبيوتر الخاص بك ب ASA.

الشهادات التي تحتوي على EKU مناسب

من المهم ملاحظة أنه على الرغم من أنه غير مطلوب لمجموعة ASA و AnyConnect، يتطلب RFC أن تحتوي الشهادات على إستخدام موسع للمفتاح (EKU):

- يجب أن تحتوي الشهادة الخاصة ب ASA على EKU الخاص **بوحدة مصادقة الخادم**.
- يجب أن تحتوي شهادة الكمبيوتر على EKU **client-auth**.

ملاحظة: يمكن لموجه IOS مع مراجعة البرامج الأخيرة وضع وحدات EKU على الشهادات.

تشكيل على ال ASA

يصف هذا القسم تكوينات ASA المطلوبة قبل حدوث الاتصال.

ملاحظة: يسمح لك مدير أجهزة حلول الأمان المعدلة (ASDM) من Cisco بإنشاء التكوين الأساسي ببضع نقرات فقط. توصي Cisco باستخدامه لتجنب الأخطاء.

تكوين خريطة التشفير

فيما يلي تكوين مثال على خريطة التشفير:

```
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
```

مقترحات IPsec

فيما يلي تكوين مثال اقتراح 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
```

سياسات IKEv2

فيما يلي تكوين مثال سياسة 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
```

خدمات العملاء والشهادة

يجب تمكين خدمات العملاء والشهادات على الواجهة الصحيحة، وهي الواجهة الخارجية في هذه الحالة. هنا مثال على التكوين:

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

ملاحظة: يتم أيضا تعيين نقطة الثقة نفسها لطبقة مآخذ التوصيل الآمنة (SSL)، والتي يتم إعدادها وتطلبها.

تمكين ملف تعريف AnyConnect

يجب تمكين ملف تعريف AnyConnect على ASA. هنا مثال على التكوين:

```
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
```

اسم المستخدم، وسياسة المجموعة، ومجموعة النفق

هنا مثال تكوين لاسم مستخدم أساسي، و group-policy، و tunnel-group على 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
```

ملف تعريف AnyConnect

فيما يلي ملف تعريف يتضمن الأجزاء ذات الصلة الموضحة **بأحرف داكنة**:

```
<?"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/>
```

فيما يلي بعض الملاحظات المهمة حول مثال التكوين هذا:

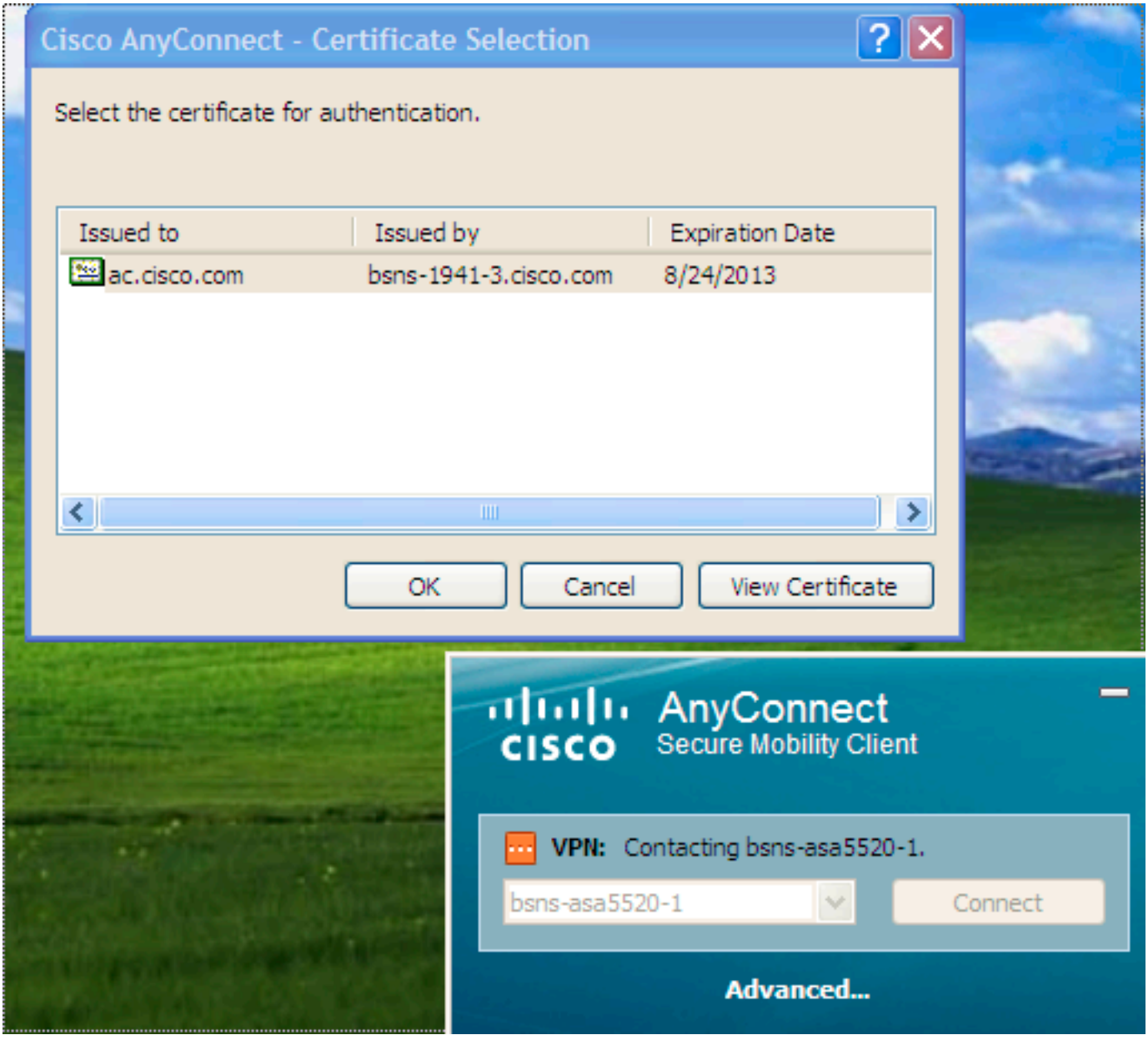
- عندما تقوم بإنشاء التوصيف، يجب أن يطابق HostAddress اسم الشهادة (CN) في الشهادة التي تستخدم ل IKEv2. أدخل الأمر **crypto ikev2 remote-access trustPoint** لتحديد هذا الأمر.
- يجب أن تتطابق UserGroup مع اسم Tunnelgroup الذي يقع عليه اتصال IKEv2. إذا لم تكن متطابقة، يفشل التوصيل غالبا وتشير الأخطاء إلى عدم تطابق مجموعة Diffie-Hellman (DH) أو خطأ سلبي مماثل.

إجراء الاتصال

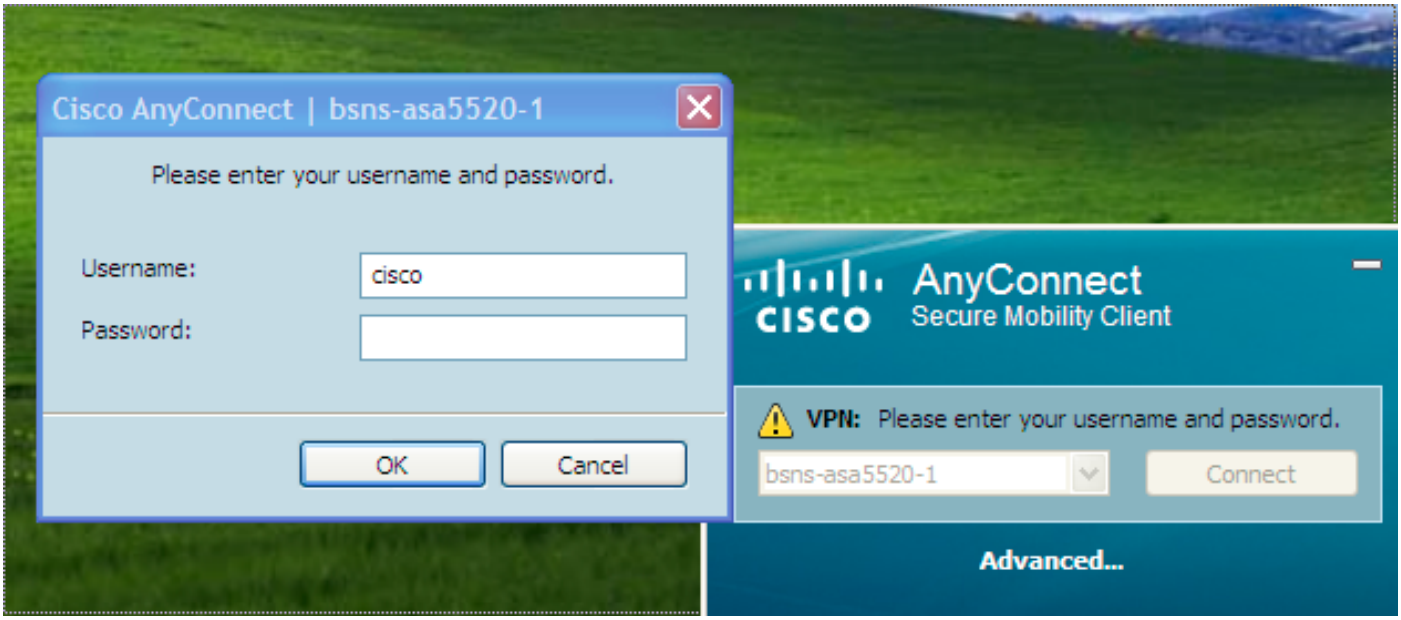
يصف هذا القسم الاتصال من كمبيوتر إلى ASA عندما يكون ملف التعريف موجودا بالفعل.

ملاحظة: المعلومات التي تدخلها في واجهة المستخدم الرسومية (GUI) للاتصال هي قيمة <HostName> التي تم تكوينها في ملف تعريف AnyConnect. في هذه الحالة، يتم إدخال **BSNS-asa5520-1**، وليس اسم المجال المؤهل بالكامل (FQDN).

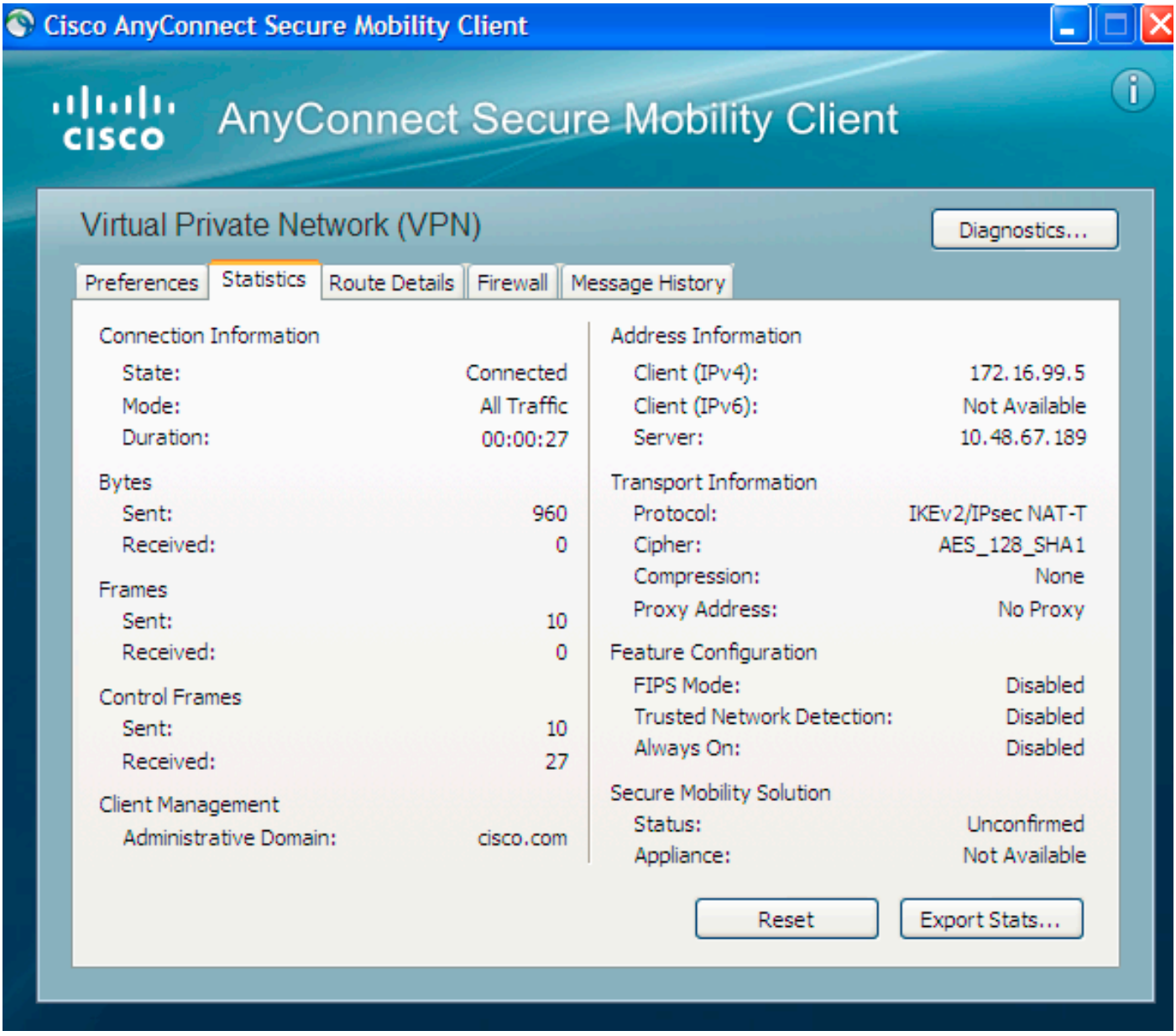
عند محاولة الاتصال لأول مرة من خلال AnyConnect، تطلب منك البوابة تحديد الشهادة (في حالة تعطيل تحديد الشهادة التلقائي):



أنت ينبغي بعد ذلك دخلت ال username وكلمة:



بمجرد قبول اسم المستخدم وكلمة المرور، ينجح الاتصال ويمكن التحقق من إحصائيات AnyConnect:



التحقق من ASA

أدخل هذا الأمر على ASA للتحقق من إستخدام الاتصال ل IKEv2 وكذلك المصادقة والتفويض والمحاسبة (AAA) ومصادقة الشهادة:

```
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
```

المحاذير المعروفة

هذه هي المحاذير المعروفة والقضايا المتعلقة بالمعلومات الموضحة في هذا المستند:

- يجب أن تكون نقاط ثقة IKEv2 و SSL هي نفسها.
- cisco يوصي أن يستعمل أنت ال FQDN بما أن ال CN ل ال ASA جانب شهادة. تأكد من أنك تشير إلى نفس

FQDN ل <HostAddress> في ملف تعريف AnyConnect.

- تذكر إدراج قيمة <HostName> من ملف تعريف AnyConnect عند التوصيل.

- حتى في تكوين IKEv2، عند اتصال AnyConnect ب ASA، فإنه يقوم بتنزيل ملفات التعريف والتحديثات الثنائية عبر SSL، ولكن ليس IPsec.

- يستخدم اتصال AnyConnect عبر IKEv2 إلى ASA EAP-AnyConnect، وهي آلية خاصة تتيح تنفيذ أكثر بساطة.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).