在IKEv2的AnyConnect对与AAA和证书验证的ASA

目录

简介

本文描述如何连接PC到思科可适应安全工具(ASA)有使用的AnyConnect IPsec (IKEv2)以及证书和验证、授权和统计(AAA)验证。

> **注意**：在本文提供的示例描述使用为了获取ASA和AnyConnect之间的一IKEv2连接仅的相关部分。没有提供完全配置示例。网络地址转换(NAT)或访问控制列表配置在本文没有描述也没有要求。

准备连接

此部分描述要求的perparations，在您能连接您的PC到ASA前。

与适当的EKU的证书

请注意，即使没有为ASA和AnyConnect组合要求， RFC要求证书扩展了密钥用法(EKU) ：

- ASA的证书必须包含服务器**验证**EKU。

- PC的证书必须包含客户端**验证**EKU。

  注意：有最新软件版本的一个IOS路由器能放置在证书上的EKUs。

在ASA的配置

此部分描述要求的ASA配置，在连接发生前。

> **注意**：Cisco Adaptive Security Device Manager (ASDM)允许您创建与仅一些点击的基本配置。思科建议您使用它为了避免错误。

加密映射配置

这是加密映射配置示例：

```
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建议

这是IPsec建议配置示例：

```
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策略

这是IKEv2策略配置示例：

```
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
```

客户端服务和证书

您必须启用客户端服务和证书在正确接口，在这种情况下是外部接口。这是配置示例：

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

注意：同样信任点为安全套接字协议层(SSL)也分配，打算并且要求。

Enable (event) AnyConnect配置文件

您必须启用在ASA的AnyConnect配置文件。这是配置示例：

```
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
```

用户名、组政策和隧道群

这是一基本用户名、组政策和隧道群的一配置示例ASA的：

```
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配置文件

这是与在**粗体**显示的相关部分的一示例配置文件：

```
<?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>
```

这是关于此配置示例的一些重要提示：

- 当您创建配置文件时，主机地址必须匹配验证名称(CN)在使用IKEv2的证书。输入**crypto ikev2远程访问信任点**命令为了定义此。
- 用户组必须匹配IKEv2连接落tunnelgroup的名称。如果他们不配比，连接经常发生故障，并且

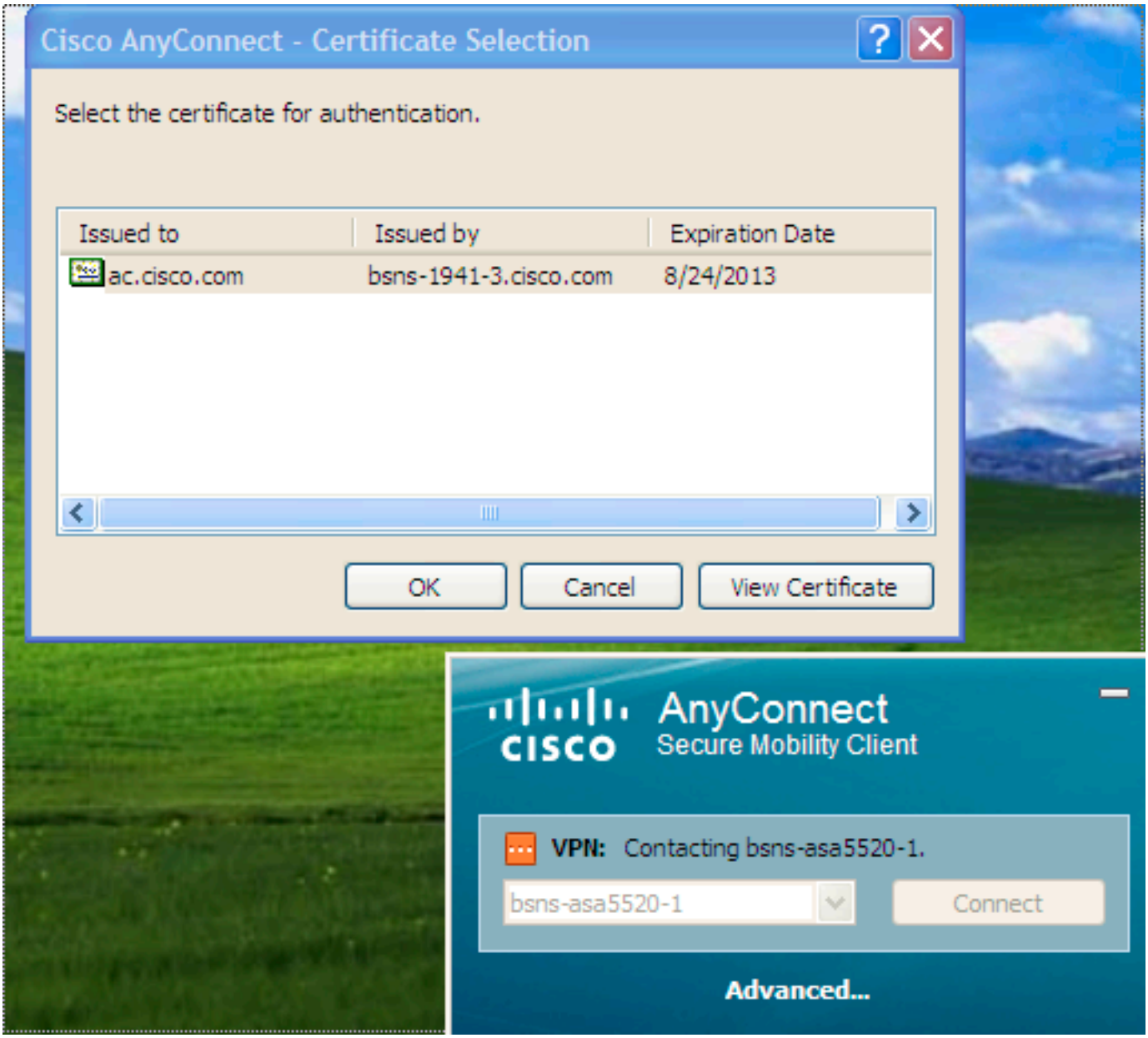
调试指示一Diffie-Hellman (DH)组不匹配或相似的假攻击。

建立联系

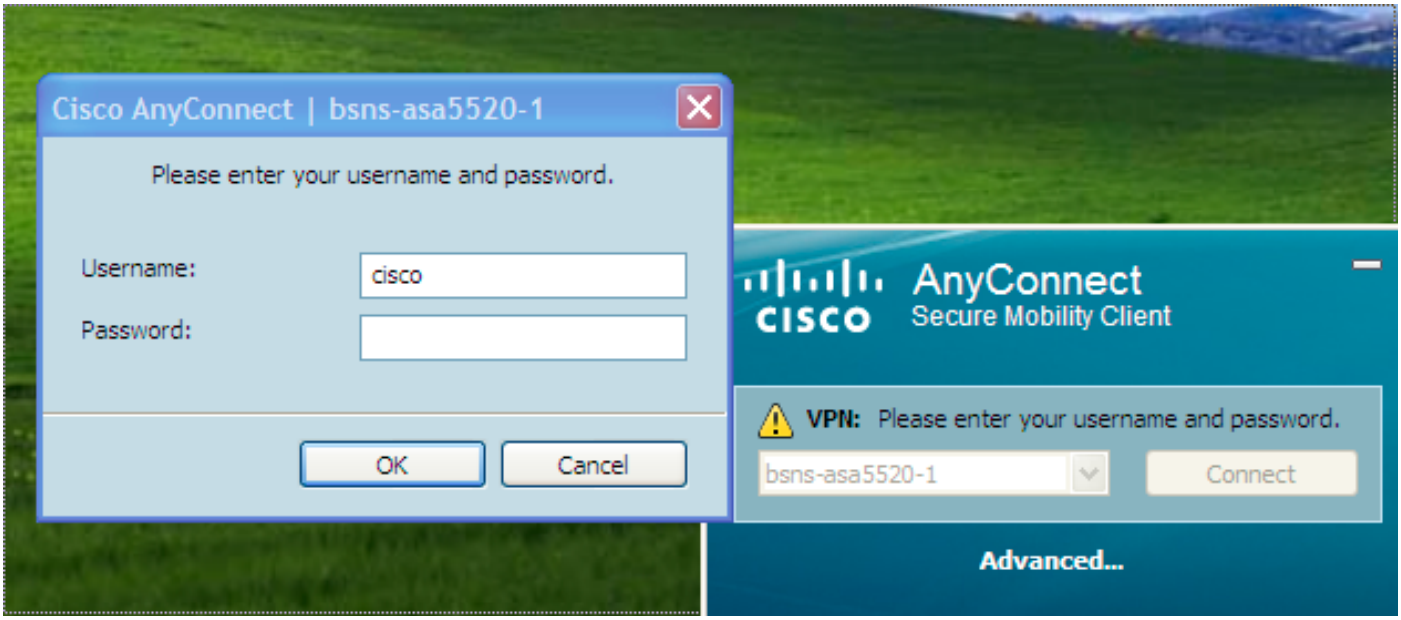
当配置文件已经存在时，此部分描述个人计算机对ASA连接。

> **注意**：信息您输入到GUI为了连接是在AnyConnect配置文件配置的<hostname>值。在这种情况下， **bsns-asa5520-1没有**被输入，没有完整完全合格的域名(FQDN)。

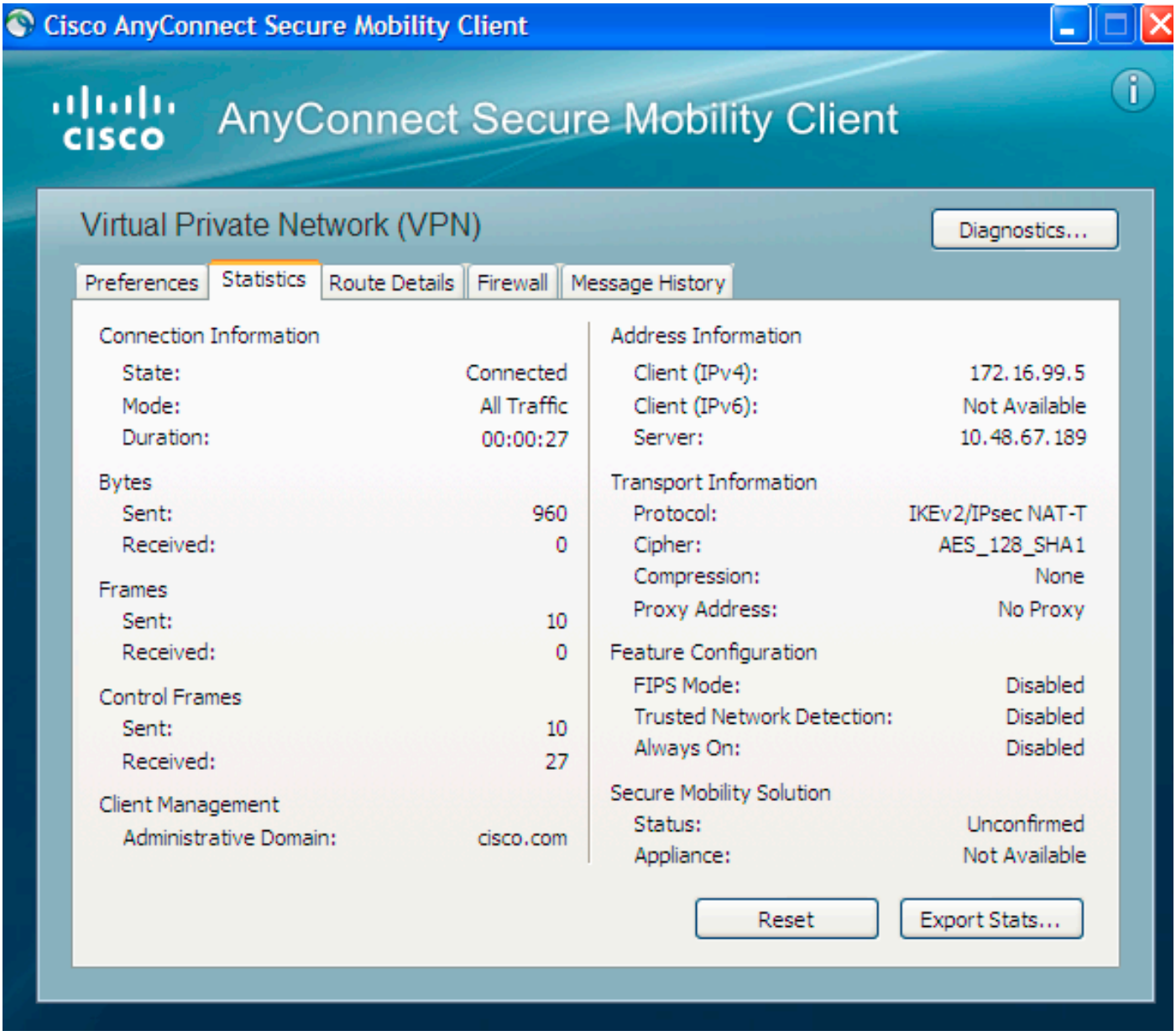
当您连接的第一次尝试通过AnyConnect，网关提示您选择证书(如果自动证书选择禁用)：



您必须然后输入用户名和密码：



一旦用户名和密码接受，连接是成功的，并且AnyConnect统计信息可以验证：



在ASA的验证

输入此on命令ASA为了验证连接使用IKEv2以及AAA和证书验证：

```
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
```

已知问题说明

这些是与信息涉及在本文描述的已知问题说明和问题：

- IKEv2和SSL信任点必须是相同的。

- 思科建议您使用FQDN作为CN ASA旁拉证书。保证您参考<HostAddress>的同样FQDN AnyConnect配置文件。
- 当您连接时，请切记插入从AnyConnect配置文件的<hostname>值。
- 在IKEv2配置里，当AnyConnect连接对ASA时，它下载在SSL的不是配置文件和二进制更新，但是IPsec。
- 在IKEv2的AnyConnect连接对ASA使用EAPAnyConnect，允许更加简单的实施的所有权机制。