IKEv2를 통해 ASA에 AAA 및 인증서 인증을 통한 AnyConnect

목차

소개

이 문서에서는 AnyConnect IPsec(IKEv2)을 사용하여 PC를 Cisco ASA(Adaptive Security Appliance)에 연결하는 방법과 인증서 및 AAA(Authentication, Authorization, and Accounting) 인증을 설명합니다.

> **참고:**이 문서에서 제공되는 예제는 ASA와 AnyConnect 간의 IKEv2 연결을 얻기 위해 사용되는 관련 부품만 설명합니다.전체 컨피그레이션 예는 제공되지 않습니다.이 문서에서는 NAT(Network Address Translation) 또는 액세스 목록 컨피그레이션에 대해 설명하거나 필요하지 않습니다.

연결 준비

이 섹션에서는 PC를 ASA에 연결하기 전에 필요한 작업에 대해 설명합니다.

적절한 EKU가 있는 인증서

ASA와 AnyConnect 조합에 필요하지 않지만 RFC에서는 인증서에 EKU(Extended Key Usage)가 있어야 합니다.

- ASA의 인증서에는 **서버 인증 EKU가** 포함되어야 합니다.
- PC에 대한 인증서에는 **클라이언트 인증 EKU가** 포함되어야 합니다.

참고:최신 소프트웨어 버전이 있는 IOS 라우터는 EKU를 인증서에 배치할 수 있습니다.

ASA의 컨피그레이션

이 섹션에서는 연결이 발생하기 전에 필요한 ASA 컨피그레이션에 대해 설명합니다.

참고: Cisco ASDM(Adaptive Security Device Manager)에서는 몇 번의 클릭만으로 기본 컨피그레이션을 생성할 수 있습니다.Cisco에서는 실수를 방지하기 위해 이 기능을 사용하는 것이 좋습니다.

암호화 맵 컨피그레이션

다음은 암호화 맵 예제 컨피그레이션입니다.

```
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 제안

다음은 IPsec 제안 컨피그레이션의 예입니다.

```
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 정책

다음은 IKEv2 정책 예제 컨피그레이션입니다.

```
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
```

클라이언트 서비스 및 인증서

이 경우 외부 인터페이스인 올바른 인터페이스에서 클라이언트 서비스와 인증서를 활성화해야 합니다.다음은 컨피그레이션의 예입니다.

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

> **참고:**SSL(Secure Sockets Layer)에도 동일한 신뢰 지점이 할당되며, 이는 의도된 필수 사항입니다.

AnyConnect 프로파일 활성화

ASA에서 AnyConnect 프로파일을 활성화해야 합니다.다음은 컨피그레이션의 예입니다.

```
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
```

사용자 이름, 그룹 정책 및 터널 그룹

다음은 ASA의 기본 사용자 이름, group-policy 및 tunnel-group 컨피그레이션의 예입니다.

```
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 프로파일

다음은 관련 부품이 **굵게** 표시된 예제 프로필입니다.

```
<?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>
```

이 컨피그레이션 예에 대한 몇 가지 중요한 참고 사항은 다음과 같습니다.

- 프로필을 만들 때 HostAddress는 IKEv2에 사용되는 인증서의 CN(Certificate Name)과 일치해야 합니다. 이를 정의하려면 **crypto ikev2 remote-access trustpoint** 명령을 입력합니다.

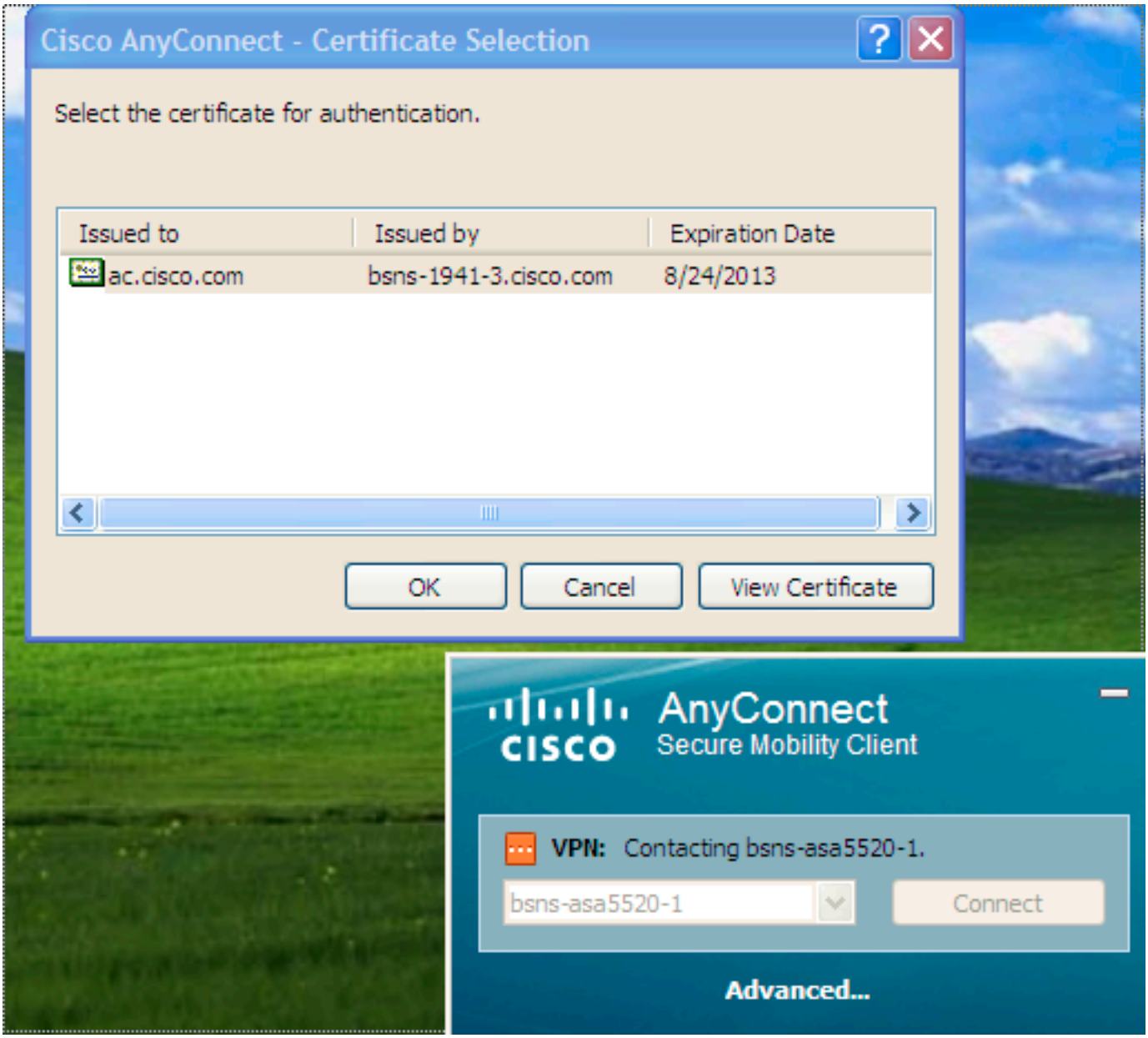
- UserGroup은 IKEv2 연결이 속하는 터널 그룹의 이름과 일치해야 합니다.일치하지 않으면 연결이 실패하는 경우가 많고 디버그가 DH(Diffie-Hellman) 그룹 불일치 또는 이와 유사한 false 음수를 나타냅니다.

연결 만들기

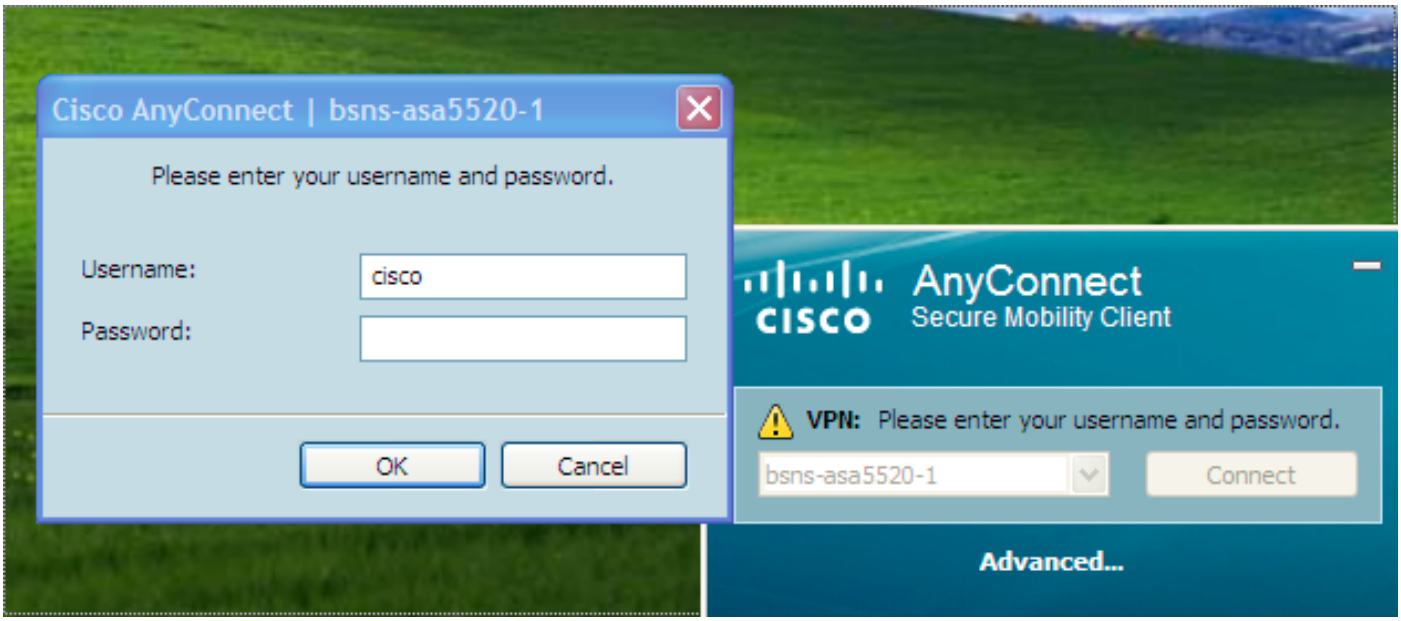
이 섹션에서는 프로파일이 이미 있는 경우 PC-ASA 연결에 대해 설명합니다.

> **참고:**연결하기 위해 GUI에 입력하는 정보는 AnyConnect 프로필에 구성된 <HostName> 값입니다.이 경우 **bsns-asa5520-1**은 전체 FQDN(Fully Qualified Domain Name)이 아니라 입력됩니다.

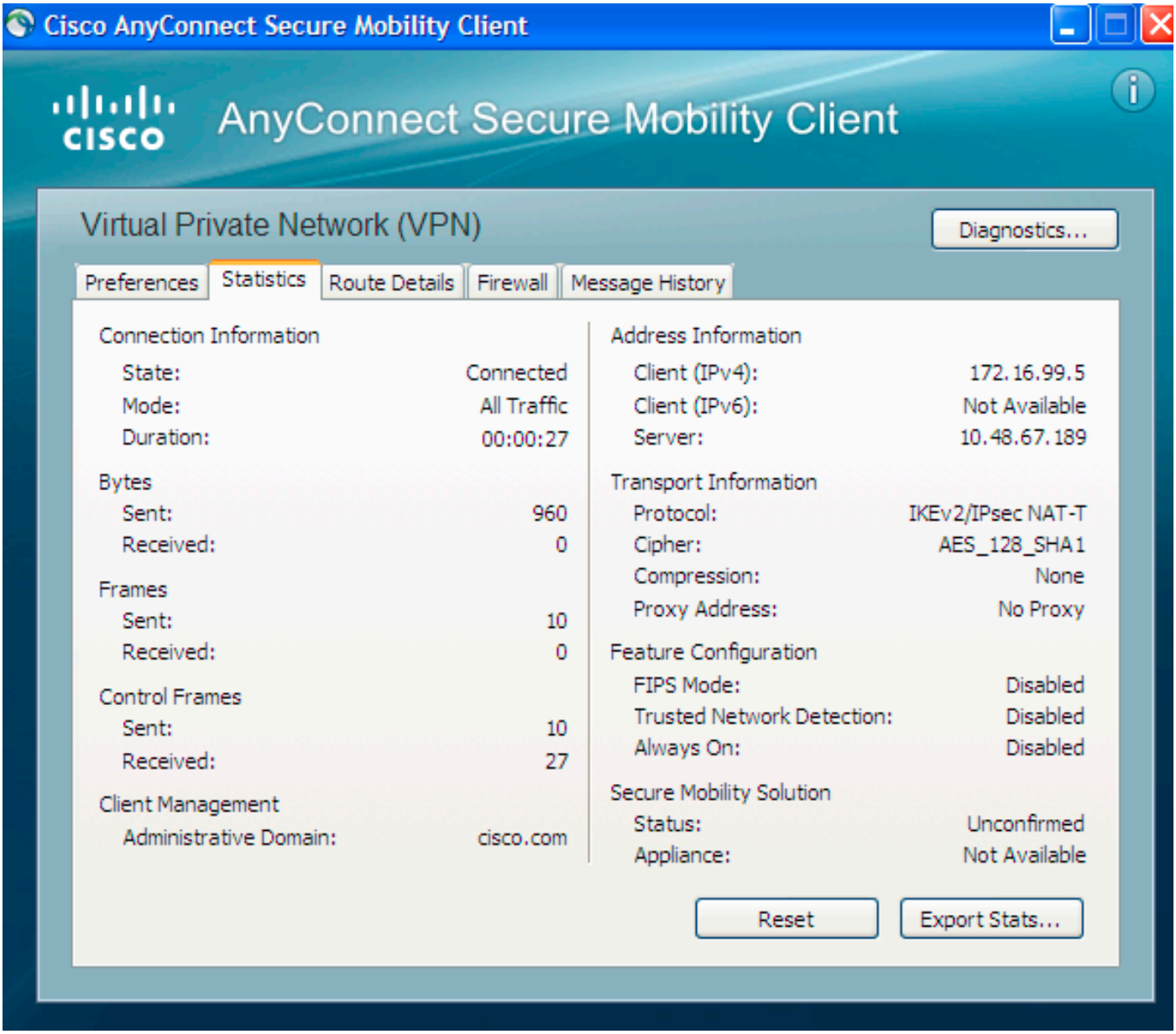
AnyConnect를 통해 처음 연결을 시도하면 게이트웨이가 인증서를 선택하라는 메시지를 표시합니다(자동 인증서 선택이 비활성화된 경우).



그런 다음 사용자 이름과 비밀번호를 입력해야 합니다.



사용자 이름 및 비밀번호가 수락되면 연결에 성공하고 AnyConnect 통계를 확인할 수 있습니다.



ASA에서 확인

연결에서 IKEv2뿐 아니라 AAA 및 인증서 인증을 사용하는지 확인하려면 ASA에서 이 명령을 입력합니다.

```
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
```

알려진 주의 사항

다음은 이 문서에서 설명한 정보와 관련된 알려진 주의 사항 및 문제입니다.

- IKEv2 및 SSL 신뢰 지점은 동일해야 합니다.

- ASA 측 인증서의 CN으로 FQDN을 사용하는 것이 좋습니다.AnyConnect 프로파일의 <HostAddress>에 대해 동일한 FQDN을 참조하는지 확인합니다.

- 연결할 때 AnyConnect 프로파일에서 <HostName> 값을 삽입해야 합니다.

- IKEv2 컨피그레이션에서도 AnyConnect가 ASA에 연결되면 SSL을 통해 프로필 및 이진 업데이트를 다운로드하지만 IPsec은 다운로드하지 않습니다.

- IKEv2를 통한 ASA로의 AnyConnect 연결은 더 간단하게 구현할 수 있는 독점적인 메커니즘인 EAP-AnyConnect를 사용합니다.