There are so many custom applications or some applications that require the users to be on the same network as the internal network as opposed to clientless ssl vpn so we use AnyConnect SSL full tunnel VPN or IPSec on Anyconnect or IPSec on legacy cisco vpn client.

**AnyConnect SSL VPN Client:**

*Using the client for a "full" tunnel*

**Review of "when" we would use this option**

**Implementing AnyConnect based on requirements**

**Requirements:**

New Admin user needs full interactive access to both the ASA and internal network devices

**Solution:** AnyConnect Client

**Properties:**

- Connection profile: admin-con-profile
- group: admin-group
- admin-user-1 address from pool: 10.0.0.51-100
- admin-user-1 tunnel only to 10.0.0.0/24

---

**Requirements:**

New Admin user needs full interactive access to both the ASA and internal network devices

**Solution:** AnyConnect Client

**Properties:**

- Connection profile: admin-con-profile
- group: admin-group
- admin-user-1 address from pool: 10.0.0.51-100
- admin-user-1 tunnel only to 10.0.0.0/24

Split tunnel (don't send the traffic over the SSL VPN unless it is destined for the corporate network), so rest of the traffic including the Internet traffic doesn't go across the SSL VPN.

Or we can tunnel everything except the local subnet of the client.

By default it is a full tunnel.
The following CLI commands are generated based on the changes you made to the ASA configuration.

```
ip local pool 10-pool 192.168.51.0 192.168.100.0 mask 255.255.255.0
group-policy admin-group internal

group-policy admin-group attributes
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Just-10
address-pools value 10-pool
```

In the configuration for the AnyConnect Connection Profile, the following fields are set:

- **Name:** admin-con-profile
- **Address:** (admin-con-profile-all)
- **Authentication:** AAA
- **AAA Server Groups:** LOCAL
- **Client Address Assignment:**
- **DHCP Servers:**
- **Client Address Pools:** 10-pool
- **Client IPv6 Address Pools:**
- **Default Group Policy:** admin-group
- **Group Policy:**

The fields are set as follows:

- **Enable SSL VPN client protocol:**
- **Enable IPsec (IKEv2) client protocol:**
- **DHCP Servers:** 10.0.0.10
- **DNS Servers:**
- **WINS Servers:**
- **Domain Name:** CITINuggets.com
The following CLI commands are generated based on the configuration:

```plaintext
group-policy admin-group
vpn-tunnel-protocol ssp-client
dns-server value 10.0.0.40
win-server none
default-domain value CBINugget.com
exit
bypass-group admin-con-profile type remote-access
tunnel-group admin-con-profile general-attributes
default-group-policy admin-group
address-pool 10-pool
tunnel-group admin-con-profile webvpn-attributes
group-alias admin-con-profile-alias enable
```
DTLS is on by default, and also uses port 443.

username admin-user password T3UhLVJ1JQxkwk7 encrypted privilege 15
username admin-user attributes

Add AnyConnect Client Image
AnyConnect Image: disk0:anyconnect-win-3.0.13332.0.png

Add
Delete

Enable AnyConnect Client Access
AnyConnect Client access cannot be enabled without a designated AnyConnect image
Would you like to designate an AnyConnect image?
Yes
No

Add
Delete
Save
Refresh
Add
Delete

Interface
SSL Access
Ipsec (IKEv2) Access
Enable Access
Enable DTLS
Enable Client Services

Add
Delete
Match Case

Configuration > Remote Access VPN > Network Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administration. AnyConnect VPN Client supports IKEv2 (IKEv2) tunnel as well as SSL tunnel, with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).

Access Interfaces

Add
Delete
Match Case

Configuration > Remote Access VPN > Network Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administration. AnyConnect VPN Client supports IKEv2 (IKEv2) tunnel as well as SSL tunnel, with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).

Access Interfaces

Add
Delete
Match Case

Configuration > Remote Access VPN > Network Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administration. AnyConnect VPN Client supports IKEv2 (IKEv2) tunnel as well as SSL tunnel, with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).

Access Interfaces

Add
Delete
Match Case
ASAl# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : admin-user
Assigned IP : 10.0.0.51
Protocol : AnyConnect-Parent SSL-Tunnel
License : AnyConnect Premium
Encryption : RC4
Bytes Tx : 16503
Group Policy : admin-group
Duration : 0h:04m:21s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A

Index : 2
Public IP : 192.168.1.20
Hashing : SHA1
Bytes Rx : 18766
Tunnel Group : admin-con-profile

ASAl#