Remote Access VPN Design Guide - ASA

Security Business Group
Network Security Technical Marketing Engineering

09 July 2020
## CONTENTS

**Introduction**  
> 3

**Prerequisites**  
> 3

**Problem statement**  
> 3

**Solution overview**  
> 4

**What’s covered in this guide?**  
> 4

**What’s not covered in this guide?**  
> 5

**Design considerations**  
> 5
  - Software platform selection  
> 5
  - Hardware platform selection  
> 6
  - VPN licensing  
> 7
  - VPN protocol selection  
> 10
  - Identity and posture management  
> 11
  - Scaling and resiliency  
> 13
  - Monitoring  
> 15
  - Best practices for optimizing the user experience  
> 19

**Deployment details**  
> 21
  - Example deployment  
> 21
  - Initial setup  
> 21
    - Preparing for ASDM access  
> 21
    - Licensing the device  
> 23
    - Configuring initial device settings  
> 24
    - Configuring SSL settings and certificates  
> 25
    - Configure authentication sources – ISE  
> 31
    - Configure authentication sources – Duo  
> 36
  - Enforcing VPN access via connection profiles and group policies  
> 39
    - Configuring Remote Access VPN using the ASDM Wizard  
> 39
    - Update group policy and connection profile  
> 44
    - Set up AnyConnect Client profile  
> 50
    - Configuring u-turning for VPN internet traffic  
> 53
    - Integrating posture assessment of VPN endpoints and users using ISE posture module  
> 55
    - Configuring and connecting devices  
> 61
Pre-installation steps 61
Using web deployment to provision AnyConnect 61
Pre-deploy and provision AnyConnect Client 62
Connect to VPN using the AnyConnect Client 62
ASA CLI configuration snippet 66

Useful resources 68
Configuration guides 68
Configuration examples 68
Videos 69
Introduction

Remote Access VPN is one of the most significant advances in modern networks, but it also presents a challenge because of the degree of mobility that networks must now support. Users move around wirelessly inside the campus, at home, and on-the-go while expecting the same degree of connectivity that they have plugged in at the office. This guide describes business use cases for mobile users who connect to their organizations with a laptop, smartphone, or tablet device. This guide covers mobile users with secure remote access (RA), the deployment of RA VPN services to either the primary Internet edge firewall or to a standalone RA VPN-specific device, as well as the configuration of the mobile client, to take advantage of this RA VPN infrastructure.

Prerequisites

This guide requires prior knowledge of the following concepts:

➢ Setting up and configuring Adaptive Security Appliances (ASA)
➢ Remote access VPN with TLS, DTLS, and IPsec

Problem statement

An organization’s network must meet many requirements that are sometimes contradictory. The network must be secure and prevent unauthorized access while being open enough to allow users to do their jobs from any location. The increase in user mobility adds to the complexity of network requirements. In the past, a worker might have needed laptop connectivity while at the office or home. Today, a worker needs access to the network from a smartphone while traveling, from a laptop while at a customer’s or partner’s office, or from both while sitting in the local coffee shop. Although providing this access is a primary requirement for the network, other requirements, such as ease of use and security, have not been relaxed.

Remote access connectivity should support:

• A wide variety of endpoint devices.
• Seamless access to the internal network and public data resources from managed and BYOD devices.
• Authentication and policy control that integrates with the authentication resources in use by the organization.
• Cryptographic security to prevent the exposure of sensitive data to unauthorized parties who accidentally or intentionally intercept the data.
Solution overview

The Cisco AnyConnect Secure Mobility Client is used to connect remote users to a primary site Cisco ASA Firewall. A well-designed VPN remote access network needs to be tolerant of the most common failure types. A single-site design that includes only a firewall pair using static default routing to the Internet provides resiliency.

An often-overlooked component of access is the ease of use. If a user has to check whether a secure connection is needed for a mobile device and entering their credentials repeatedly to enable a secure connection, they may bypass the solution. A solution must be highly integrated and seamless so that it doesn’t significantly affect users’ productivity. Therefore, utilizing platform automation prevents users from either forgetting to follow procedures or to specifically try to bypass them. This design enables the following network and security capabilities:

- **User authentication**: The AnyConnect client requires all remote access users to authenticate before negotiating a secure connection.
- **Differentiated access**: The remote access VPN configuration provides different access policies depending on assigned user roles and client posture status.
- **Strong encryption for data privacy**: The Advanced Encryption Standard (AES) GCM cipher with a key length of 256 bits encrypts user data. Additional ciphers are also supported.
- **Hashing for data integrity**: The Secure Hash Standard 2 (SHA-2) cryptographic hash function with up to 512-bit message digest ensures that data is not modified during transit.
- **Split-tunneling**: The Cisco AnyConnect client uses the split-tunnel feature to control what traffic is encrypted and what can be transmitted in clear text to limit the load on the VPN headend.
- **Device resiliency**: The Cisco ASA firewall supports failover between the active and standby units of a resilient firewall pair in the event of a hardware failure.
- **Internet link resiliency**: The configuration in the AnyConnect client profile includes a backup server reachable through the secondary ISP for automatic switchover if the primary server is not reachable.
- **Web Deployment**: Easy deployment of VPN and other modules and their associated profiles, which allows easy VPN client distribution and setup.
- **Always-on VPN**: The Trusted Network Detection capability of the Cisco AnyConnect client determines if a mobile device is on a trusted internal network or an untrusted external network. If the device is on an untrusted network, the client automatically tries to establish a VPN connection to the primary site. The user needs to provide authentication, but no other intervention is required. If the user disconnects, no other network access is permitted.
- **Advanced Malware and DNS protection**: The AnyConnect AMP and Umbrella modules provide on-client protection for both protected and direct internet traffic.
- **VPN Load Balancing**: A remote-client configuration using two or more ASAs connected to the same network to handle remote sessions, can be configured to share their session load. Load balancing directs session traffic to the least loaded device, thus distributing the load among all devices to make efficient use of system resources and provide increased performance and availability.

What’s covered in this guide?

This guide provides information about the following topics:

- AnyConnect client-based remote access VPN
• Design and implementation best practices on the ASA

What’s not covered in this guide?

This guide does not provide information about the following topics:

• Clientless and third-party RA VPN
• RA VPN on FTD

Design considerations

Software platform selection

With Cisco firewalls, you have the option of running ASA or FTD. Consider the following factors before choosing between them:

➢ VPN feature set: ASA-only supported features.

<table>
<thead>
<tr>
<th>Unsupported RA VPN features on FTD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clientless VPN</td>
</tr>
<tr>
<td>Third-party VPN clients</td>
</tr>
<tr>
<td>EzVPN</td>
</tr>
<tr>
<td>Deployment of AnyConnect Modules</td>
</tr>
<tr>
<td>AnyConnect Customization and</td>
</tr>
<tr>
<td>Localization support</td>
</tr>
<tr>
<td>AnyConnect Custom Attributes</td>
</tr>
<tr>
<td>SAML, TACACS, Kerberos</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
</tr>
<tr>
<td>VPN Local CA</td>
</tr>
</tbody>
</table>

• Firewall deployment model: If using the Firewall as a dedicated RA VPN headend, ASA software is recommended since it provides better performance than FTD on the same hardware.

• The ASA software version used depends on the importance of stability or feature velocity. The current recommendations are:
  ▪ ASA 9.8(4.latest) for longevity
  ▪ ASA 9.12(2.latest) for feature velocity
  ▪ Subscribe to release notifications here: software.cisco.com

• Always use the latest AnyConnect client version available for download.
Hardware platform selection

- The most important factors for selecting a VPN headend are:
- The maximum number of concurrent users connecting – this affects licensing and the worst-case encrypted throughput that you will see on the Firewall.
  - The average expected throughput consumed per user is typically a range from 0.3 – 1 Mbps/user, depending on how much traffic is tunneled.

With these two factors, you can then determine the overall VPN throughput you need and compare that with the firewall-encrypted throughput. These values are available on the firewall datasheets.

- Each firewall model has a limit on the number of concurrent RA VPN sessions supported, as shown in the following table:

<table>
<thead>
<tr>
<th>Firewall Model</th>
<th>Maximum # of sessions supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASAv5</td>
<td>50</td>
</tr>
<tr>
<td>FP 1010</td>
<td>75</td>
</tr>
<tr>
<td>FP 1120</td>
<td>150</td>
</tr>
<tr>
<td>ASAv10, 5512, 5515</td>
<td>250</td>
</tr>
<tr>
<td>ASA 5516</td>
<td>300</td>
</tr>
<tr>
<td>FP 1140</td>
<td>400</td>
</tr>
<tr>
<td>ASAv30, 5525</td>
<td>750</td>
</tr>
<tr>
<td>FP 1150</td>
<td>800</td>
</tr>
<tr>
<td>FP 2110</td>
<td>1500</td>
</tr>
<tr>
<td>ASA 5545</td>
<td>2500</td>
</tr>
<tr>
<td>FP 2120</td>
<td>3500</td>
</tr>
<tr>
<td>ASA 5555, 5585 (SSP 10, SSP 20)</td>
<td>5000</td>
</tr>
<tr>
<td>FP 2130</td>
<td>7500</td>
</tr>
<tr>
<td>ASAv50, 5585 (SSP 40, SSP 60), ASA-SM, FP 2140, 4110</td>
<td>10000</td>
</tr>
<tr>
<td>FP 4115, 4120, SM-24</td>
<td>15000</td>
</tr>
<tr>
<td>FP 4125, 4140, 4145, 4150, SM-36, SM-40, SM-44, SM-48, SM-56</td>
<td>20000</td>
</tr>
</tbody>
</table>

- In general, ASA software running on Firepower hardware has better capacity than ASA hardware.
- Plan to have at least two VPN firewalls to provide resiliency in RA VPN services.
VPN licensing

With AnyConnect Release 4.x, Cisco introduced a new AnyConnect licensing model based on a unique user term-based licensing model. The two simple licensing tiers are AnyConnect Plus and AnyConnect Apex.

<table>
<thead>
<tr>
<th>AnyConnect Plus</th>
<th>AnyConnect Apex</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device or system VPN (including VPN Phone)</td>
<td>All Plus features as well as the other features in this column</td>
</tr>
<tr>
<td>Third-party IPsec IKEv2 remote access VPN clients (non-AnyConnect client)</td>
<td>Network Visibility Module</td>
</tr>
<tr>
<td>Per-application VPN</td>
<td>Unified endpoint compliance and remediation (posture) (Identity Services Engine Apex is required and licensed separately)</td>
</tr>
<tr>
<td>Cloud Web Security and Web Security Appliance</td>
<td>Suite B or next-generation encryption (including third-party IPsec IKEv2 remote VPN clients)</td>
</tr>
<tr>
<td>Cisco Umbrella Roaming (Umbrella Roaming services are licensed separately)</td>
<td>Clientless (browser-based) VPN connectivity</td>
</tr>
<tr>
<td>Network Access Manager</td>
<td>ASA multi-context mode remote access</td>
</tr>
<tr>
<td>Cisco AMP for Endpoints Enabler (AMP for Endpoints is licensed separately)</td>
<td>SAML authentication</td>
</tr>
</tbody>
</table>

**NOTE:** There is a third form of AnyConnect License – VPN Only, which is a perpetual license tied to a specific headend device. VPN Only licenses are most applicable to environments wanting to use AnyConnect exclusively for remote access VPN services but with high or unpredictable total user counts. For further details, refer to the [AnyConnect Ordering Guide](#).

- Licensing on ASA Hardware:
  - Licensing is [PAK based](#).
  - Apart from the above AnyConnect licenses, enable [strong encryption](#) on the ASA.

  - Licensing on ASAv and Firepower Hardware:
    - Licensing is [Smart Software licensed](#).
    - Apart from the above AnyConnect licenses, enable [strong encryption](#) on the ASA.

  - Failover units do not require the same license on each unit. If you have licenses on both units, they combine into a single running failover license.

  - Cluster units do not require the same license on each unit. Typically, you buy a license only for the control unit; data units inherit the control license. If you have licenses on multiple units, they combine into a single running ASA cluster license.

  - Multiple context mode requires the AnyConnect Apex license. Moreover, in multiple context mode, this license must be applied to each unit in a failover pair; the license is not aggregated.

  - View license information on the ASA (see below):
ASA5506-X# show version

Cisco Adaptive Security Appliance Software Version 9.13(1)
SSP Operating System Version 2.7(1.107)
Device Manager Version 7.13(1)

Compiled on Mon 23-Sep-19 09:28 PDT by builders
System image file is "disk0:asa9-13-1-ibff-k8.SPA"
Config file at boot was "startup-config"

ASA5506-X up 10 days 6 hours

Hardware: ASA5506, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4 cores)
Internal ATA Compact Flash, 8000MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB

Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1)
Number of accelerators: 1

1: Ext: GigabitEthernet1/1 : address is 84b8.0276.92ac, irq 255
2: Ext: GigabitEthernet1/2 : address is 84b8.0276.92ad, irq 255
3: Ext: GigabitEthernet1/3 : address is 84b8.0276.92ae, irq 255
4: Ext: GigabitEthernet1/4 : address is 84b8.0276.92af, irq 255
5: Ext: GigabitEthernet1/5 : address is 84b8.0276.92b0, irq 255
6: Ext: GigabitEthernet1/6 : address is 84b8.0276.92b1, irq 255
7: Ext: GigabitEthernet1/7 : address is 84b8.0276.92b2, irq 255
8: Ext: GigabitEthernet1/8 : address is 84b8.0276.92b3, irq 255
9: Int: Internal-Data1/1 : address is 84b8.0276.92ab, irq 255
10: Int: Internal-Data1/2 : address is 0000.0001.0002, irq 0
11: Int: Internal-Control1/1 : address is 0000.0001.0001, irq 0
12: Int: Internal-Data1/3 : address is 0000.0001.0003, irq 0
13: Ext: Management1/1 : address is 84b8.0276.92ab, irq 0
14: Int: Internal-Data1/4 : address is 0000.0100.0001, irq 0

The Running Activation Key feature: 2 security contexts exceed the limit on the platform, reduced to 0 security contexts.

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited perpetual
Maximum VLANs                     : 5              perpetual
Inside Hosts                      : Unlimited perpetual
Failover                         : Disabled       perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Carrier                           : Disabled       perpetual
AnyConnect Premium Peers          : 50             86 days
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 10             perpetual
Total VPN Peers                   : 50             perpetual
AnyConnect for Mobile             : Enabled        86 days
AnyConnect for Cisco VPN Phone    : Enabled        86 days
Advanced Endpoint Assessment      : Enabled        86 days
Shared License                    : Disabled       perpetual
Total TLS Proxy Sessions          : 2              perpetual
Botnet Traffic Filter             : Disabled       perpetual
Cluster                          : Disabled       perpetual
ASA5506-X# show vpn-sessiondb license-summary

VPN Licenses and Configured Limits Summary

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
<th>Capacity</th>
<th>Installed</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect Premium</td>
<td>ENABLED</td>
<td>50</td>
<td>50</td>
<td>NONE</td>
</tr>
<tr>
<td>AnyConnect Essentials</td>
<td>DISABLED</td>
<td>50</td>
<td>0</td>
<td>NONE</td>
</tr>
<tr>
<td>Other VPN (Available by Default)</td>
<td>ENABLED</td>
<td>10</td>
<td>10</td>
<td>NONE</td>
</tr>
<tr>
<td>Shared License Server</td>
<td>DISABLED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shared License Participant</td>
<td>DISABLED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AnyConnect for Mobile</td>
<td>ENABLED(Requires Premium or Essentials)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced Endpoint Assessment</td>
<td>ENABLED(Requires Premium)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AnyConnect for Cisco VPN Phone</td>
<td>ENABLED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN-3DES-AES</td>
<td>ENABLED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN-DES</td>
<td>ENABLED</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VPN Licenses Usage Summary

<table>
<thead>
<tr>
<th>Feature</th>
<th>All</th>
<th>Peak</th>
<th>Eff.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect Premium</td>
<td>50</td>
<td>50</td>
<td>100%</td>
</tr>
<tr>
<td>AnyConnect Client</td>
<td>50</td>
<td>50</td>
<td>100%</td>
</tr>
<tr>
<td>Other VPN</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>L2TP Clients</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VPN protocol selection

The Cisco AnyConnect client connects to the ASA firewall using either TLS, DTLS (UDP 443), or IKEv2 protocols. A typical VPN connection will have the following stages:

- **Parent Tunnel**
  - Main VPN Session created.
  - Essentially a cookie to allow the ASA to keep track of a session across hibernation or network connectivity issues.
  - Kept alive till either idle timeout or max connect timeout are reached. SSL keepalives used to monitor tunnel.

- **TLS Tunnel**
  - Established next.
  - In the case of DTLS/IKEv2 tunnels, control plane transactions continue to take place across this tunnel.
  - TLS uses TCP port 443.
  - DPD used to monitor tunnel.

- **DTLS/IPSec Tunnel**
  - When fully established, all data packets are transmitted through this tunnel.
  - In the case of DTLS tunnels, TLS tunnel is a fallback in case of DTLS disruption.
  - DPD or IPSec keepalives used to monitor tunnel.

- TLS versions supported: 1.0, 1.1, and 1.2
- DTLS versions supported: 1.0, 1.1, and 1.2
- Performance for the same sized traffic is ranked: IKEv2 > DTLS > TLS. When sizing for DTLS, factor in a 50% decrease in rated throughput
- GCM-based ciphers have about twice the throughput of CBC ciphers
- TLS 1.0 and 1.1 are being deprecated by major OS and browser companies by March 2020
- ASA Release 9.4(1) or higher, no longer supports all SSLv3 keywords and SSLv3
Identity and posture management

The RA VPN solution on ASA provides support for multiple protocols and mechanisms by which incoming users can be authenticated and provided with differentiated access. The following table gives a quick overview of supported functionality.

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Authorization</th>
<th>Accounting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>✓ User or group-based</td>
<td>✓</td>
</tr>
<tr>
<td>RADIUS</td>
<td>ASA and IETF RADIUS Authorization attributes</td>
<td>✓</td>
</tr>
<tr>
<td>LDAP</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Certificates</td>
<td>Use DAP or combine with another AAA protocol</td>
<td></td>
</tr>
<tr>
<td>SAML</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>TACACS</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Kerberos</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>SDI</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Multi-Factor Authentication (MFA)** is one of the most effective methods to provide reliable authenticated access. The ASA RA VPN solution works with multiple vendors, including Duo MFA.

Duo MFA provides the following integration options:

1. **ASA SSL VPN using SAML**: Choose this option for the best end-user experience for ASA. With this configuration, end-users experience the interactive Duo Prompt when using the Cisco AnyConnect Client for VPN. The interactive MFA prompt gives users the ability to view all available authentication device options and select one to use, self-enroll new or replacement 2FA devices, and manage their own registered devices. Primary authentication and Duo MFA occur at the identity provider, not at the ASA itself.

2. **ASA SSL VPN using RADIUS**: Choose this option for ASA and AnyConnect deployments that do not meet the minimum product version requirements for SAML SSO. With this configuration, end-users receive an automatic push or phone call for multi-factor authentication after submitting their primary credentials using the AnyConnect Client or clientless SSL VPN via a browser. Users may append a different factor selection to their password entry.

3. **ASA SSL VPN using LDAPS**: When using this option with the clientless SSL VPN, end-users experience the interactive Duo Prompt in the browser. The AnyConnect client does not show the Duo Prompt but instead adds a second password field to the regular AnyConnect login screen where the user enters the word “push” for Duo Push, the word “phone” for a phone call, or enters a one-time passcode. This method does not support IP-based network policies or device health requirements.
Another aspect to consider during design is provisioning for **end-user posture assessment**, which allows enforcement of an endpoint's compliance for things like antivirus, antispyware, and firewall software installed on the host. Options for posture assessment include:

1. **Dynamic Access Policy (DAP with HostScan):** Local on-box solution that leverages the AnyConnect Posture Module that performs posture assessment and remediation.
2. **ISE Posture:** Solution provided with integration to ISE that leverages the ISE posture module that performs posture assessment and remediation.
3. **Duo Device Health Application:** A solution provided with integration to Duo that performs assessment only.

<table>
<thead>
<tr>
<th>Cisco ASA HostScan-based Posture</th>
<th>Cisco Identity Services Engine Posture</th>
<th>Cisco Duo Device Health Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Posture validation and remediation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Provisioned by ASA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Dynamic Access Policies enforce policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Uses OPSWAT v4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ OPSWAT libraries are uploaded directly as part of the HostScan package</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Also, supported on Firepower with ASA image only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Posture validation and remediation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Replaced the legacy NAC agent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Provisioned by ISE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Downloadable ACL (DAACL) pushed to ASA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ One agent for wired, wireless, and VPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Uses OPSWAT v3 and v4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ OPSWAT libraries are available through a feed service or uploaded directly to ISE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Stealth Mode option</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Posture validation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Provisioned by Duo</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Uses a client agent to scan and assess client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Health application policies enforce posture checks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

You can configure the security appliance to apply user attributes obtained from a RADIUS/LDAP authentication/authorization server, and user attributes set in group policies on the security appliance, or both. The security appliance aggregates attributes received from both sources and applies them to the user policy. DAP attributes take precedence for conflicts between server and group policy attributes.

To summarize, the VPN permissions policy for user authorization is the aggregate of the DAP access attributes and the group-policy inheritance hierarchy.
The security appliance applies attributes in the following order:

4. **Dynamic Access Policy attributes**: Take precedence over all others.

5. **User attributes**: The AAA server returns these after successful user authentication or authorization.

6. **Group policy attributes**: These attributes come from the group policy associated with the user. You identify the user group policy name in the local database by the vpn-group-policy attribute or from a RADIUS/LDAP server by the value of the RADIUS CLASS attribute (25) in the OU=GroupName. The group policy provides any attributes that are missing from the DAP or user attributes.

7. **Connection profile (tunnel-group) default-group-policy attributes**: These attributes come from the default group policy associated with the connection profile. This group policy provides any attributes that are missing from the DAP, user, or group policy.

8. **System default attributes**: System default attributes provide any values that are missing from the DAP, user, group policy, or connection profile.

**Scaling and resiliency**

With the increase in the number of RA VPN users comes the need for exploring different scalability options. The scalability capabilities available differ based on the requirements of an organization, network setup, and hardware/software limitations. Various options exist:

- **Backup Server**: Configure multiple backup RA VPN servers in the AnyConnect Profile. If the selected RA VPN server is not reachable, the first server in the backup list is selected.

- **Optimal Gateway Selection**: Enabled through the AnyConnect Profile, the Optimal Gateway Selection (OGS) feature determines which gateway has the lowest RTT and connects to that gateway.

- **Active/Standby High Availability**: Provides redundancy by sharing VPN session information between peers.

- **Native VPN Load Balancing**: An ASA feature that allows multiple ASA firewalls to load balance incoming VPN requests based on load, with up to 10 firewalls in a single cluster.

- **VPN Load Balancing using an External Load Balancer**: Leverage either hardware, software, or cloud-based external load balancers to front end VPN connections across multiple ASAs.

- **DNS Load Balancing**: DNS is responsible for load balancing. Note that load balancing may not be equal to each site.
**AnyConnect on an Active/Standby Pair**

**AnyConnect with Native Load Balancing**

**AnyConnect with DNS Load Balancing**
Monitoring

Multiple methods exist for capturing details on RA VPN connections and resource usage. VPN connection details can be directly consumed for tracking AUP and for troubleshooting purposes. The key to successful monitoring of resources by RA VPN, however, lies in understanding which resource elements are affected by performance and scale and in establishing a baseline resource usage to track abnormal device behavior.

➢ **VPN Dashboards:** ASDM, CSM, and CDO are different ASA firewall GUI-based managers that contain robust VPN dashboards and reports for tracking user sessions and device usage.

➢ **Logging with Syslog:** There are specific logging classes used to monitor VPN connections and resource usage: vpn, vpnc, vpnfo, webvpn, auth, sys

➢ **SNMP:** Use the CISCO-REMOTE-ACCESS-MONITOR and CISCO-PROCESS-MIB to monitor RA VPN sessions and device resource usage.

➢ **CLI Monitoring:**

  ▪ **CPU Utilization:** A key traffic usage indicator. Monitor for sustained usage vs. spikes. High DATAPATH usage indicates a high traffic load.

```
show process cpu-usage non-zero
asa# show process cpu-usage non-zero
PC    Thread      5Sec   1Min   5Min   Process
0x0000000019da592  0x00007fffd808b040  0.0%   0.0%   0.5%   Logger
0x00000000844596  0x00007fffd807bd60  0.0%   0.0%   0.1%   CP Processing
0x000000004c0dc8c  0x00007fffd8074960  0.1%   0.1%   0.1%   ARP Thread
-    -          43.8%   43.8%   40.3%   DATAPATH-0-2209
-    -          43.9%   43.8%   40.3%   DATAPATH-1-2210

asa# show cpu usage
CPU utilization for 5 seconds = 88%; 1 minute: 88%; 5 minutes: 82%
```

- **Memory Utilization:** Use `show memory` for initial system memory health assessment. Monitor for lower than baseline conditions.

```
asa# show memory
Free memory: 6800208035 bytes (79%)
Used memory: 1557164032 bytes (21%)
---------------
Total memory: 8589934592 bytes (100%)
```
- **Interface Statistics**: Checks if any drops increase at the time of issue. Clear counters to establish a baseline.

```bash
asa# show interface stats
Interface GigabitEthernet0/0 “outside”, is up, line protocol is up
   Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
   Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
   Input flow control is unsupported, output flow control is off
   MAC address a80c.0dc1.109d, MTU 1500
   IP address unassigned
   469048 packets input, 143676683 bytes, 0 no buffer
   Received 469048 broadcasts, 0 runts, 0 giants
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   0 pause input, 0 resume input
   0 L2 decode drops
   0 packets output, 0 bytes, 0 underruns
   0 pause output, 0 resume output
   0 output errors, 0 collisions, 1 interface resets
   0 late collisions, 0 deferred
   0 input reset drops, 0 output reset drops
   input queue (blocks free curr/low): hardware (503/457)
```
VPN Statistics: The `vpn-sessiondb` command provides a wealth of information about all VPN connections to the box, along with the ability to disconnect sessions.

```plaintext
asa# show vpn-sessiondb
------------------------------------------------------------------------
---
VPN Session Summary
------------------------------------------------------------------------
---
Active : Cumulative : Peak Concur :

Inactive

---

---

AnyConnect Client            :    100 :       1280 :         202 :
SSL/TLS/DTLS               :    100 :       1280 :         202 :
----------------------------

Total Active and Inactive    :    100             Total Cumulative :
1280

Device Total VPN Capacity    :   5000
```

Device Total VPN Capacity    :   5000
Cisco Endpoint Security Analytics: Cisco Endpoint Security Analytics (CESA) Built on Splunk analyzes endpoint telemetry generated by the Network Visibility Module (NVM) built into the Cisco AnyConnect Secure Mobility Client. CESA Built on Splunk is Splunk Enterprise software that is tuned to analyze NVM telemetry produced by endpoints to detect a variety of endpoint-specific security risks and breaches, such as:

- Finding unapproved or blocked list SaaS and client applications
- Detecting data theft and data loss
- Discovering day-zero malware and conduct threat hunting
- Identifying endpoints trying to evade security scanning or disable client-side security software
- Monitoring pertinent activity and behavior of endpoints when they are not attached to the network, such as in zero-trust deployments
- Creating endpoint software application and process allowed lists
- Performing endpoint asset inventory or OSs, user accounts, device manufacturers/model, and software under IT management on the network

You can find more details at the following URLs:

- Cisco Endpoint Security Analytics Built on Splunk:

- Cisco Endpoint Security Analytics (CESA) Built on Splunk Quickstart POV Kit & Deployment Guide:
Best practices for optimizing the user experience

Dynamic split tunneling

Dynamic split tunneling was designed to enhance the current split-tunneling options. Beyond the static IP-based inclusions or exclusions typically used to define split tunneling, the dynamic split tunneling inclusions or exclusions address scenarios where traffic pertaining to a specific service needs to be excluded from or included in the VPN tunneling. You can configure a distinct split tunneling setting for each IP protocol.

For example, you can enable dynamic split include tunneling for IPv4 (such as IPv4 split include and dynamic split include domains). You can also enable dynamic split exclude tunneling for IPv6 (such as IPv6 tunnel-all and dynamic split exclude domains). Additionally, AnyConnect release 4.6 added an enhanced dynamic split tunneling, where both dynamic split exclude and dynamic split include domains are specified for enhanced domain name matching.

This feature is extremely useful in optimizing VPN bandwidth usage by excluding high bandwidth and SAAS-based applications.

QoS

RA VPN traffic can be policed pre-encryption and post-decryption by matching based on tunnel-group and the flow IP destination. Additionally, the ASA preserves the TOS bits after encryption allowing QoS Prioritization on post-encrypted traffic.
Crypto acceleration bias

ASA and Firepower platforms come with multiple Crypto cores, which are used for both IPSec and TLS/SSL. Some platforms equally allocate cores between IPSec and SSL. While other platforms, using "crypto engine accelerator-bias SSL/IPsec/balanced," configure the allocation of cores to either IPsec or SSL or balanced. The option of allocating cores is available only on specific platforms.

FTD running on FPR9300 and FPR4100 allows configuration of the Crypto Engine Bias using flex config, to provide a marginal VPN throughput performance improvement. Note that the latest Firepower models do not support the Crypto Engine Bias. For further details, see the table below:

<table>
<thead>
<tr>
<th>Platform</th>
<th>FTD Default</th>
<th>FTD User Configurable</th>
<th>ASA Default</th>
<th>ASA User Configurable</th>
<th>Other Variations</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPR9300, SM24, SM36, SM48</td>
<td>Balanced</td>
<td>Through Flex-Config, but marginal improvement</td>
<td>Balanced</td>
<td>Available</td>
<td>SSL/IPSEC</td>
</tr>
<tr>
<td>FPR41x0</td>
<td>Balanced</td>
<td>Through Flex-Config, but marginal improvement</td>
<td>Balanced</td>
<td>Available</td>
<td>SSL/IPSEC</td>
</tr>
<tr>
<td>FPR1000, FPR2100, FPR41x5, FPR9300, SM40, SM44, SM56</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>ASA 5545-X &amp; 5555-X</td>
<td>IPSec</td>
<td>Available</td>
<td>IPSec</td>
<td>Available</td>
<td>Balanced/SSL</td>
</tr>
<tr>
<td>ASA5506, 5508, 5516, 5525-X</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

*Balanced—Equally distributes cryptographic hardware resources (Admin/SSL and IPsec cores)
Deployment details

Example deployment

This deployment covers the following RA VPN Scenario:

➢ DTLS-based AnyConnect client connecting to an ASA headend.
➢ Two-factor user authentication using ISE RADIUS and Duo LDAPS.
➢ An authenticated user authorized to access either Engineering or Sales resources based on AD group membership (integration with ISE).
➢ ISE Posture ensures enabling the Windows auto-update feature before network access.

Versions used:

➢ ASAv running 9.13 and ASDM 7.13
➢ AnyConnect Client running 4.8.3052
➢ AnyConnect ISE Compliance Module 4.3.1250
➢ ISE running 2.6

Initial setup

This section provides instructions for setting up ASDM to manage the security appliance, configuring basic settings, and adding users.

Preparing for ASDM access

To use ASDM, perform the following steps:

1. Use an Ethernet cable to connect the MGMT interface to a switch or hub. To this same switch, connect a PC that will run ASDM to configure the security appliance.
   
   **NOTE:** You can use other interfaces for ASDM access if you choose.

2. Configure the PC to use DHCP to obtain an IP address automatically from the security appliance. It can then communicate with the security appliance and the Internet as well as run ASDM for configuration and management tasks.
   
   **NOTE:** Alternatively, you can assign a static IP address to your PC by selecting an address in the 192.168.45.0 subnet. Valid addresses are 192.168.45.10 through 192.168.45.12, with a mask of 255.255.255.0 and a default route of 192.168.45.1. When you connect other devices to any of the inside ports, make sure that they do not have the same IP address. The MGMT interface of the adaptive security appliance is assigned the IP address 192.168.45.1 by default, so this address is unavailable.

3. Check the LINK LED on the MGMT interface.
When a connection is established, the LINK LED interface on the adaptive security appliance, and the corresponding LINK LED on the switch or hub are solid green.


5. Click one of the available options: Install ASDM Launcher or Run ASDM.

6. Follow the instructions to launch ASDM according to the option you chose. The Cisco ASDM-IDM Launcher displays.

7. Leave the username and password fields empty and click OK. The main ASDM window displays.

8. To see the commands that ASDM sends to the security appliance, in the toolbar at the top of the main ASDM screen, go to Tools > Preferences > General tab and click the Preview commands before sending them to the device checkbox.
Licensing the device

The ASA can be licensed using the PAK or Smart Licensing method, depending on the platform in use. Remote Access VPN headends require the Strong Encryption and AnyConnect licenses, find further details here.

NOTE: If using Smart Licensing, the ASA will use the management interface by default to reach out to https://tools.cisco.com
Configuring initial device settings

Use the following steps to leverage the Startup wizard on the ASDM for this purpose:

1. From Wizards > Startup Wizard, click the Modify existing configuration radio button.
2. The Startup Wizard walks you through configuring:
   - The hostname, domain name and enable password
   - Interfaces, including setting the inside and outside interface IP addresses and enabling interfaces
   - Static routes
   - The DHCP server
Configuring SSL settings and certificates

1. Configure the SSL Settings at either of the following locations:
   - Configuration > Device Management > Advanced > SSL Settings
   - Configuration > Remote Access VPN > Advanced > SSL Settings

   ![SSL Settings Configuration](image)

   **NOTE**: SSLv3 was deprecated in ASA 9.4. Cisco recommends using the most secure ciphers and protocols for both VPN and management access. Ensure that the TLS session is as secure or more secure than the DTLS session by using an equal or higher version of TLS than DTLS.

2. Digital certificates provide digital identification for authentication. Cisco does not recommend the use of a self-signed certificate because a user could inadvertently configure a browser to trust a certificate from a rogue server. It is also inconvenient for users to have to respond to a security warning when it connects to the secure gateway. It is recommended to use trusted third-party CAs to issue SSL certificates to the ASA for this purpose.

4. Define a trustpoint name and then select the **Add a new identity certificate** radio button. For the Key Pair, click **New**.

   - Choose the **Key Type** - RSA or ECDSA.
   - Click the **Enter new key pair name** radio button. Identify the key pair name in a distinct way for recognition purposes.
   - Choose the **Key Size**. Also, if you use RSA, choose **General Purpose for Usage**.
   - Click **Generate Now** to create the key pair.
5. To define the Certificate Subject DN, click Select, and configure the attributes listed in this table:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN</td>
<td>FQDN (Full Qualified Domain Name) that will be used for connections to your firewall. For example, webvpn.cisco.com</td>
</tr>
<tr>
<td>OU</td>
<td>Department Name</td>
</tr>
<tr>
<td>O</td>
<td>Company Name (Avoid using Special Characters)</td>
</tr>
<tr>
<td>C</td>
<td>Country Code (2 Letter Code without Punctuation)</td>
</tr>
<tr>
<td>ST</td>
<td>State (Must be spelled out completely. For example, North Carolina)</td>
</tr>
<tr>
<td>L</td>
<td>City</td>
</tr>
<tr>
<td>EA</td>
<td>Email Address</td>
</tr>
</tbody>
</table>

To configure these attributes, select an attribute from the Attribute drop-down list, enter the value, and click Add.

**NOTE:** Some third-party vendors require particular attributes to issue an identity certificate. If unsure of the required attributes, check with the vendor for details.
6. After adding the appropriate values, click OK. The Add Identity Certificate dialog box displays with the Certificate Subject DN field populated. Click Advanced.
   - In the FQDN field, enter the FQDN that is used to access the device from the Internet. Click OK.
   - Leave the Enable CA flag in basic constraints extension option checked. Certificates without the CA flag now cannot be installed on the ASA as CA certificates by default. The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate. Bypass this requirement by unchecking the option.

7. Click OK, and then click Add Certificate. A prompt displays to save the CSR to a file on the local machine.
8. Install the SSL certificate on the ASA with either ASDM or using the CLI:
   ▪ Import the CA and identity certificate separately in PEM format, OR
   ▪ Import the PKCS12 file (base64 encoded for CLI) in which the identity certificate, CA certificate, and
     private key are bundled.

   **NOTE:** If the CA provides a CA certificate chain, only install the immediate intermediate CA certificate in the hierarchy
   on the trustpoint used to generate the CSR. The Root CA certificate and any other intermediate CA certificates can be
   installed in new trustpoints.

   The installation steps given assume that the CA provides a PEM-encoded (.pem, .cer, .crt) identity certificate and CA
   certificate bundle.


   ![Install Certificate](image)

10. Open the PEM-encoded certificate in a text editor and copy and paste the base64 CA certificate provided by the
    third-party vendor into the text field. Then click Install certificate.

12. Select the Identity Certificate created previously. Click **Install**.

![Install Identity Certificate](image)

Either click the **Install from a file** radio button and choose the PEM-encoded Identity certificate or open the PEM-encoded certificate in a text editor and copy and paste the base64 Identity certificate provided by the third-party vendor into the text field.

13. Click Add Certificate.

14. Navigate to **Configuration > Remote Access VPN > Advanced > SSL Settings**. Under **Certificates**, select the interface that is used to terminate WebVPN sessions. This example uses the outside interface. Click **Edit**. In the **Certificate** drop-down list, choose the newly installed certificate.

![Select SSL Certificate](image)

15. Click **OK**. Click **Apply** to use the new certificate for all Remote Access VPN sessions that terminate on the interface specified.
Configure authentication sources – ISE
This section is optional but recommended for a remote access VPN deployment. This example uses RADIUS as the protocol for authentication, authorization, and accounting. You can find the initial setup and deployment of ISE (which is beyond the scope of this guide) at the following URL:


1. Navigate to the Cisco Identity Services Engine (ISE) web console.
2. In Administration > Identity Management > External Identity Sources > Active Directory, click the Active Directory domain. Select Groups.
3. Click Add > Select Groups from Directory. Locate and add the required groups. Click Save.
4. Navigate to Administration > Network Resources > Network Devices and click Add. Enter the ASA connection details. Keep a note of the RADIUS Shared Secret.


Name = Engineering_Access
Access Type = ACCESS_ACCEPT
DACL: Permit_Engineering

Name: Sales_Access
Access Type = ACCESS_ACCEPT
DACL: Permit_Sales
7. Navigate to Policy > Policy Sets and click the + symbol. Create a policy set for VPN users.

8. Navigate back to the ASDM and select Remote Access VPN > AAA/Local Users > AAA Server Groups > Add.
   a. Enter the RADIUS Server group name. Click OK.
   b. Highlight the newly created AAA server group and click Add in the lower half of the configuration panel.
c. Enter the details shown in the following table (default values not listed):

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Interface through which the ISE server is reachable</td>
</tr>
<tr>
<td>Server Name or IP Address</td>
<td>ISE Server IP address (PSN node)</td>
</tr>
<tr>
<td>Timeout</td>
<td>Set to 60 seconds (for Duo in next section)</td>
</tr>
<tr>
<td>Authentication/Accounting Port</td>
<td>1645/1646 or 1812/1813</td>
</tr>
<tr>
<td>Server Secret Key</td>
<td>Same as that used in ISE Network Device</td>
</tr>
</tbody>
</table>

d. Click OK and then Apply.

9. Highlight the server and click Test to confirm connectivity.
Configure authentication sources – Duo

When using this option with clientless SSL VPN, end-users experience the interactive Duo Prompt in the browser. The AnyConnect client does not show the Duo Prompt, but instead adds a second password field to the regular AnyConnect login screen where the user enters the word “push” for Duo Push, the word “phone” for a phone call, or a one-time passcode. This section assumes the presence of a Duo Account (Duo Account) with the Cisco ASA SSL VPN Application added in.

1. Download the DigiCert High Assurance EV Root CA and DigiCert SHA2 High Assurance Server CA certificates from the DigiCert site.
2. Navigate to Remote Access VPN > Certificate Management > CA Certificates and install the CA certificates from the previous step.
   a. Enter the LDAP Server group name. Select LDAP for Protocol, and then click OK.

![Image of Add AAA Server Group window]

b. Highlight the newly created AAA server group and click Add in the lower half of the configuration panel.
c. Enter the details (default values are not listed) in the following table:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Interface through which the ISE server is reachable</td>
</tr>
<tr>
<td>Server Name or IP Address</td>
<td>Your API hostname (i.e., api-XXXXXXXX.duosecurity.com)</td>
</tr>
<tr>
<td>Timeout</td>
<td>60 seconds</td>
</tr>
<tr>
<td>Enable LDAP over SSL</td>
<td>Checked</td>
</tr>
<tr>
<td>Base DN</td>
<td>dc=INTEGRATION_KEY,dc=duosecurity,dc=com</td>
</tr>
<tr>
<td>Naming Attribute(s)</td>
<td>cn</td>
</tr>
<tr>
<td>Login DN</td>
<td>dc=INTEGRATION_KEY,dc=duosecurity,dc=com</td>
</tr>
</tbody>
</table>
d. Click **OK** and then click **Apply**.

4. Highlight the server and click **Test** to confirm connectivity.
Enforcing VPN access via connection profiles and group policies

Configuring Remote Access VPN using the ASDM Wizard
The ASDM provides different wizards for the quick configuration of various ASA features.

1. Navigate to the Menu bar and select **Wizards > VPN Wizards > AnyConnect VPN Wizard**. Click **Next**.

2. Enter the **Connection Profile name** and select the **VPN Access Interface**. Click **Next**.
3. Enable the VPN protocols (SSL or IPsec, or both) to be used, and from the Device Certificate drop-down, select the certificate created previously. Click Next.

4. Click Add to upload the AnyConnect client image. Upload the latest image for the client OS in use directly into the ASA from the local client machine using ASDM. As an alternative, upload images to the ASA flash from Tools > File Management. Click Next.
5. Select the **Primary AAA Server Group**. This example uses the ISE server group created earlier. Click **Next**.

6. Skipping this step is an option for this example since SAML authentication is not used. However, enabling LOCAL authentication is recommended as a fallback AAA mechanism should access to ISE fail. Check the option **Use LOCAL if Server Group fails**. Click **Next**.
7. The VPN address pool is specified in this step, assuming the use of a locally-defined IP address pool. Using a DHCP server assigned address requires adding it after completing the wizard configuration in the Connection Profile. Click New. Enter the Pool Name, Starting and Ending IP Address and Subnet Mask. Click Next.

8. Enter the DNS Servers, WINS Servers, and Domain Name details. Click Next.
9. In most cases, the VPN traffic requires an exemption from NAT. Check the option ‘Exempt VPN traffic from network address translation.’ Select the Inside interface and local network for exemption from NAT. Click Next.

10. Click Next.

11. Inspect the VPN deployment details, and if correct, click Finish.
Update group policy and connection profile


2. From the General tab, select the Tunneling protocol as SSL VPN Client.
3. From the **Servers** tab, enter the DNS/WINS server IP address and Default Domain Name.

4. Under **Advanced > Split Tunneling**, specify the **DNS resolution behavior** and **split-tunnel network list**. If using ISE posture assessment, tunnel all or split-exclude is recommended.
5. Under **Advanced > AnyConnect Client > Custom Attributes**, add a **dynamic split-exclude list** to exclude high bandwidth applications like WebEx and SAAS applications like Office 365 from being tunneled. The domains specified here are wildcard domains by default and support any child domains under it.
6. While the wizard completes most of the AnyConnect Connection Profile configuration, additional configurations are required. Navigate to Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles. Select the connection profile created and click Edit.

8. Under **Advanced > Accounting**, select the **ISE server** as the Accounting Server.
9. Under Advanced > Group Alias/Group URL, add a group-URL for the ASA FQDN. Click OK and then Apply.
Set up AnyConnect Client profile

Use the AnyConnect Client profile to enable client-side functionality. These profiles contain configuration settings for the core client VPN functionality and the optional client modules Network Access Manager, ISE posture, customer experience feedback, and Web Security. The ASA deploys the profiles during AnyConnect installation and updates.

1. Navigate to Remote Access VPN > Network (Client) Access > Group Policies. Click Add and enter the profile name. Select the group-policy under Group Policy. Click OK.
2. Edit the newly created profile. **Under Preferences (Part 2), change the Authentication Timeout to 120 seconds (for Duo).**
3. Under the **Server** tab, enter the **Server Display Name** and the **device FQDN** used for VPN accessed. Click **OK**.
Configuring u-turning for VPN internet traffic
In this example, since we are tunneling most traffic, internet traffic needs to be u-turned on the outside interface.

1. To enable u-turning on the outside interface, navigate to Device Setup > Interface Settings > Interfaces and click the Enable traffic between two or more hosts connected to the same interface checkbox.
2. Add a NAT statement to allow for VPN traffic to be NAT’d to the outside interface IP address. Navigate to **Firewall > NAT Rules** and click **Add Network Object NAT Rule**. Enter the object name, object type, VPN pool, NAT type, and translated address. Click **OK**.
Integrating posture assessment of VPN endpoints and users using ISE posture module

The AnyConnect Secure Mobility Client offers a VPN Posture (HostScan) Module and an ISE Posture Module. Both provide the Cisco AnyConnect Secure Mobility Client with the ability to assess an endpoint's compliance for things like antivirus, antispyware, and firewall software installed on the host. You can then restrict network access until the endpoint is in compliance or can elevate local user privileges so they can establish remediation practices. In this example, we use the ISE Posture module. ISE Posture performs a client-side evaluation. The client receives the posture requirement policy from the headend, performs the posture data collection, compares the results against the policy, and sends the assessment results back to the headend. Even though ISE determines whether or not the endpoint is compliant, it relies on the endpoint's evaluation of the policy.

NOTE: This assumes that you have completed the Configure Authentication Sources – ISE section.

1. Navigate to the ISE portal and move to Policy > Policy Elements > Results > Client Provisioning > Resources. Add the latest ISE Compliance Module and AnyConnect Package.
2. Create an ISE Posture Agent Profile with **Server Name Rules** set to *.* Use the **Server Name Rules** field to specify the domain on which the compliance server should exist, if the end machine connects to multiple domains with overlapping IP addresses.

3. Create an ISE Posture Configuration file with the previously uploaded AnyConnect Image and ISE Compliance Module. Reference the newly created ISE Posture Agent Profile.
4. Create an Authorization Profile for the Unknown posture state.

5. Navigate to Policy > Policy Elements > Conditions > Posture and create a posture condition. In this example, we are using the predefined AutoUpdateCheck under Service Condition.
6. Navigate to Policy > Policy Elements > Results > Posture > Requirements to link the Posture condition to the requirement.

7. Navigate to Policy > Posture Policy and create a new Posture policy to map the requirement.

8. Navigate to Policy > Client Provisioning and configure the provisioning rules. These are the rules that decide the type of agent to provision.

9. Navigate to Policy > Policy Sets and modify the existing authorization profiles to reflect the posture status.
10. On the ASDM, navigate to **Remote Access VPN > AAA/Local Users > AAA Server Groups**. Select the ISE RADIUS Server group and click **Edit**. Under ISE Policy Enforcement, click the **Enable dynamic authorization** checkbox.
11. Navigate to Remote Access VPN > Advanced > ACL Manager. Click Add > Add ACL and enter the same name as the ISE redirect access-list name.

12. Select the newly created access-list and click Add > Add ACE. Add the following ACEs:
   a. Deny DNS traffic
   b. Deny traffic to the ISE server (PSN)
   c. Deny ICMP traffic
   d. Permit all traffic
Configuring and connecting devices

Pre-installation steps

To minimize user prompts during the AnyConnect client setup, make sure the certificate data on the client PCs and the security appliance match:

➢ If you are using a Certificate Authority (CA) for certificates on the security appliance, choose one previously configured as a trusted CA on client machines.

➢ If you are using a self-signed certificate on the security appliance, be sure to install it as a trusted root certificate on clients. This procedure varies by browser.

➢ Make sure the Common Name (CN) in security appliance certificates matches the name clients use to connect to it. By default, the security appliance certificate CN field is its IP address. If clients use a DNS name, change the CN field on the security appliance certificate to that name.

➢ Add the ASA to the list of trusted sites in Internet Explorer

➢ Under certain conditions, AnyConnect hides (locks down) the Internet Explorer Tools > Internet Options > Connections tab. When exposed, this tab lets the user set proxy information. Hiding this tab prevents the user from intentionally or unintentionally circumventing the tunnel. The tab lockdown setting reverses upon disconnect.

Using web deployment to provision AnyConnect

Without a previously installed client, remote users enter into their browser the IP address or DNS name of the interface configured to accept SSL VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, users must enter the URL in the form https://<address>.

After the user enters the URL, the browser connects to that interface and displays the login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as requiring the client, it loads the client that matches the operating system of the remote computer. After loading, the client installs and configures itself, establishes a secure SSL connection and either remains or uninstalls itself (depending on the security appliance configuration) when the connection terminates.

In the case of a previously installed client, when the user authenticates, the security appliance examines the revision of the client and upgrades the client as necessary.

This method of provisioning requires administrative privileges on the client machine only during install but not upgrades or module installs.
Pre-deploy and provision AnyConnect Client

AnyConnect can be predeployed using SMS, by manually distributing files for end-users to install, or by making an AnyConnect file archive available for users to access.

When creating a file archive to install AnyConnect, the directory structure of the archive must match the directory structure of the files installed on the client.

This method of provisioning requires administrative privileges on the client machine.

Connect to VPN using the AnyConnect Client

This example makes use of a Windows 10 workstation that has the AnyConnect VPN Client and ISE Posture module installed.

1. Open AnyConnect from the Start Menu. Because the AnyConnect profile is present on the client machine (\Program Data\Cisco\Cisco AnyConnect Secure Mobility Client\Profile), the Connect To field is populated with the ASA’s FQDN. Click Connect.
2. Enter the AD username and password in the **Username** and **Password** fields. Enter push (or phone/SMS) in the **Second Password** field. Click **OK**. Duo prompts your associated device.

3. The ISE Posture module will run its compliance check. In this example, it checks if the AutoUpdate service is running. A successful check results in a compliant status.
4. Verify connection details on the client and ASA.
ASA CLI configuration snippet

ip local pool VPN_Pool 172.16.50.1-172.16.50.30 mask 255.255.255.0

object network ISE
group ISE host 192.168.1.20
object network VPN_Pool
subnet 172.16.50.0 255.255.255.0

access-list split-tunnel standard permit 172.16.20.0 255.255.255.128
access-list split-tunnel standard permit host 192.168.1.20
access-list split-tunnel standard permit host 72.163.1.80
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any object ISE
access-list redirect extended deny icmp any any
access-list redirect extended permit ip any any
access-list Remote-Management standard permit host 192.168.1.77

nat (inside,outside) source static NETWORK_OBJ_172.16.20.0_25 NETWORK_OBJ_172.16.20.0_25 destination static NETWORK_OBJ_172.16.50.0_27 NETWORK_OBJ_172.16.50.0_27 no-proxy-arp route-lookup

object network VPN_Pool
nat any,any dynamic interface

aaa server ISE_RADIUS_Server protocol radius
dynamic-authorization
aaa server ISE_RADIUS_Server (management) host 192.168.1.20
timeout 60
key *****

aaa server Duo_LDAPS_Server protocol ldap
aaa server Duo_LDAPS_Server (management) host api-29acc4f3.duosecurity.com
timeout 60
server-port 636
ldap-base-dn dc=DI9ER61FT6EV44KHKNOR,dc=duosecurity,dc=com
ldap-naming-attribute cn
ldap-login-password *****
ldap-login-dn dc=DI9ER61FT6EV44KHKNOR,dc=duosecurity,dc=com
ldap-over-ssl enable
server-type auto-detect
crypto ca trustpoint RAVPN_TrustPoint
enrollment terminal
fqdn ciscoasa.therndlab.com
subject-name CN=ciscoasa.therndlab.com,O=Cisco Systems,C=US
keypair RAVPN_Keypair
crl configure
crypto ca trustpoint ASDM_TrustPoint0
enrollment terminal
crl configure
crypto ca trustpoint ASDM_TrustPoint1
enrollment terminal
crl configure
crypto ca trustpoint ASDM_TrustPoint2
enrollment terminal
crl configure
ssl server-version tlsv1.2 dtlsv1.2
ssl trust-point RAVPN_TrustPoint outside
ssl trust-point RAVPN_TrustPoint inside
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
no x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/anyconnect-win-4.8.03052-webdeploy-k9.pkg 1
anyconnect profiles ACProfile disk0:/acprofile.xml
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable
anyconnect-custom-data dynamic-split-exclude-domains Office365Applications office.com
anyconnect-custom-data dynamic-split-exclude-domains Office365Applications office365.com
anyconnect-custom-data dynamic-split-exclude-domains Office365Applications outlook.com
anyconnect-custom-data dynamic-split-exclude-domains Office365Applications sharepoint.com
anyconnect-custom-data dynamic-split-exclude-domains Office365Applications live.com
anyconnect-custom-data dynamic-split-exclude-domains Office365Applications microsoftonline.com
anyconnect-custom-data dynamic-split-exclude-domains Office365Applications onedrive.com
anyconnect-custom-data dynamic-split-exclude-domains Office365Applications microsoft.com
anyconnect-custom-data dynamic-split-exclude-domains Office365Applications onedrive.sfx.ms
anyconnect-custom-data dynamic-split-exclude-domains Office365Applications sharepointonline.com
anyconnect-custom-data dynamic-split-exclude-domains Office365Applications lync.com
anyconnect-custom-data dynamic-split-exclude-domains Office365Applications skype.com
anyconnect-custom-data dynamic-split-exclude-domains Office365Applications webex.com
anyconnect-custom-data dynamic-split-exclude-domains Office365Applications ciscospark.com
anyconnect-custom-data dynamic-split-exclude-domains Office365Applications wbx2.com
group-policy "GroupPolicy_Remote VPN" internal
group-policy "GroupPolicy_Remote VPN" attributes
wins-server value 192.168.1.3
dns-server value 192.168.1.3
vpn-tunnel-protocol ssl-client
split-tunnel-policy excludespecified
split-tunnel-network-list value Remote-Management
default-domain value therndlab.com
split-dns value therndlab.com
split-tunnel-all-dns enable
anyconnect-custom-data dynamic-split-exclude-domains value Office365Applications
webvpn
anyconnect profiles value ACProfile type user
dynamic-access-policy-record DfIAccessPolicy
username admin password ***** pbkdf2 privilege 15
tunnel-group "Remote VPN" type remote-access
tunnel-group "Remote VPN" general-attributes
address-pool VPN_Pool
authentication-server-group ISE_RADIUS_Server LOCAL
secondary-authentication-server-group Duo_LDAPS_Server use-primary-username
accounting-server-group ISE_RADIUS_Server
default-group-policy "GroupPolicy_Remote VPN"
tunnel-group "Remote VPN" webvpn-attributes
group-alias "Remote-VPN" enable
group-url https://ciscoasa.therndlab.com enable
without-cid anyconnect
Useful resources

Configuration guides

➢ Duo: https://duo.com/docs/cisco#cisco-asa-with-anyconnect

Configuration examples

➢ Office 365 URLs and IP address ranges: https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges
➢ ASA Remote Access VPN with OCSP Verification under Microsoft Windows 2012 and OpenSSL:

➢ ASA Version 9.2.1 VPN Posture with ISE Configuration Example:

➢ ASA Version 9.2 VPN SGT Classification and Enforcement Configuration Example:

➢ Configure AnyConnect Management VPN Tunnel on ASA:

➢ Install and Configure AnyConnect NVM 4.7.x or Later and Related Splunk Enterprise Components for CESA:


➢ Configure AnyConnect Secure Mobility Client for Linux using Client Certificate Authentication on an ASA:

Videos

➢ AnyConnect Configuration with ASAv: https://youtu.be/7PkpzPbjC8E
➢ ASA VPN Load Balancing: https://youtu.be/ha4UqZZK74k
➢ Wild card certificates for ASA RA VPN: https://youtu.be/yK-Rnmg5ugw
➢ Deploy AnyConnect with Umbrella Roaming Module and Trusted Network Detection: https://youtu.be/qNMcljlepFU
➢ AnyConnect RA VPN using SAML authentication with DUO and LDAP authorization: https://youtu.be/Ku0mvU9XS94