



# Cisco Secure Client - AnyConnect 5.1 for Red Hat Enterprise Linux 8.2 CC Configuration Guide

**Version:** 0.3

**Date:** February 15, 2024

## Table of Contents

Document Introduction .....	3
Introduction.....	5
Audience.....	5
Purpose.....	5
Document References.....	5
TOE Overview .....	6
Operational Environment .....	6
Excluded Functionality .....	7
Procedures and Operational Guidance for IT Environment .....	8
Preparative Procedures and Operational Guidance for the TOE .....	16
Cisco Secure Client Profiles .....	17
Cisco Secure Client Stand-Alone Profile Editor .....	17
Cisco Secure Client Local Policy .....	18
Configure Certificates.....	18
Start Cisco Secure Client.....	20
Operational Guidance for the TOE.....	21
Establish a VPN Connection.....	21
Integrity Verification .....	22
Monitor and Troubleshoot .....	22
Exiting Secure Client .....	22
Cryptographic Support .....	22
Trusted Updates.....	23
Obtaining Documentation and Submitting a Service Request .....	23
Contacting Cisco.....	23

## Document Introduction

Prepared By:  
Cisco Systems, Inc.  
170 West Tasman Dr.  
San Jose, CA 95134

This document provides Guidance to IT personnel for the TOE, Cisco Secure Client - AnyConnect 5.1 for Red Hat Enterprise Linux 8.2. This Guidance document includes instructions to successfully install the TOE in the Operational Environment, instructions to manage the security of the TSF, and instructions to provide a protected administrative capability.

### Revision History

Version	Date	Change
0.1	July 25, 2023	Initial Version
0.2	November 14, 2023	Updates
0.3	February 15, 2024	Updates for Check-out

## Document Introduction

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2024 Cisco Systems, Inc. All rights reserved.

## Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Secure Client - AnyConnect 5.1 for Red Hat Enterprise Linux 8.2 TOE, as it was certified under Common Criteria. The Cisco Secure Client - AnyConnect 5.1 for Red Hat Enterprise Linux 8.2 may be referenced below by the related acronym e.g. VPN Client or simply the TOE.

## Audience

This document is written for administrators installing and configuring the TOE. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, and understand your network topology and the protocols that the devices in your network can use, that you are a trusted individual, and that you are trained to use the operating systems on which you are running your network.

## Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining Cisco Secure Client operations. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

## Document References

This section lists the Cisco Systems documentation that is also a portion of the Common Criteria Configuration Item (CI) List. The documents used are shown below in Table 1. Throughout this document, the guides will be referred to by the “#”, such as [1].

**Table 1 Cisco Documentation**

#	Title	Link
1	Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1	<a href="https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-1.html">https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-1.html</a>
2	Release Notes for Cisco Secure Client (including AnyConnect), Release 5.1	<a href="https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/release/notes/release-notes-cisco-secure-client-5-1.html">https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/release/notes/release-notes-cisco-secure-client-5-1.html</a>

## TOE Overview

The TOE is the Cisco Secure Client - AnyConnect 5.1 for Red Hat Enterprise Linux 8.2 (herein after referred to as the VPN client, or the TOE). The Cisco Secure Client - AnyConnect 5.1 for Red Hat Enterprise Linux 8.2 TOE provides remote users with secure IPsec (IKEv2) VPN connections to the Cisco 5500 Series Adaptive Security Appliance (ASA) VPN Gateway allowing installed applications to communicate as though connected directly to the enterprise network.

## Operational Environment

The TOE requires the following IT Environment Components when the TOE is configured in its evaluated configuration:

**Table 2. Operational Environment Components**

Component	Usage/Purpose/Description
Certificate Authority	The Certification Authority provides the TOE with valid certificates. The CA also provides the TOE with a method to check the certificate revocation status of the VPN Gateway.
Red Hat Enterprise Linux 8.2	The Red Hat Enterprise Linux 8.2 platform provides an execution platform for the TOE to run. Red Hat Enterprise Linux 8.2 has been evaluated for conformance with the Protection Profile for Operating Systems v4.2.1 and listed on the NIAP Product Compliant List (PCL).
ASA 5500-X series VPN Gateway	The Cisco ASA 5500-X with software version 9.2.2 or later functions as the head-end VPN Gateway. The Cisco Secure Client TOE communicates only with the Cisco ASA 5500-X Series Gateway.

Introduction

<p>ASDM Management Platform</p>	<p>The ASDM 7.7 or later operates from any of the following operating systems:</p> <ul style="list-style-type: none"> <li>■ Windows 7, 8, 10</li> <li>■ Windows Server 2008, 2012, 2012 R2, 2016 and Server 2019</li> <li>■ Apple OS X 10.4 or later</li> </ul> <p>Note that that ASDM software is installed on the ASA appliance and the management platform is used to connect to the ASA and run the ASDM. The only software installed on the management platform is a Cisco ASDM Launcher.</p>
---------------------------------	--

The underlying OS platform provides some of the security functionality required in [MOD\_VPNC\_V2.4] , and is denoted using the phrase “TOE Platform” in this document.

The Cisco Secure Client TOE uses network hardware resources on the OS platform to send and receive encrypted packets. The TOE does not access sensitive information repositories or other hardware resources.

References in this document to “ASA” refer to a VPN Gateway

### Excluded Functionality

The functionality listed below is not included in the evaluated configuration.

**Table 3. Excluded Functionality and Rationale**

Function Excluded	Rationale
Non-FIPS 140-2 mode of operation	The TOE includes FIPS mode of operation. The FIPS modes allows the TOE to use only approved cryptography. FIPS mode of operation must be enabled in order for the TOE to be operating in its evaluated configuration.
SSL Tunnel with DLTS tunneling options	[MOD_VPNC_V2.4] only permits IPsec VPN tunnel.

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the claimed Protection Profiles.

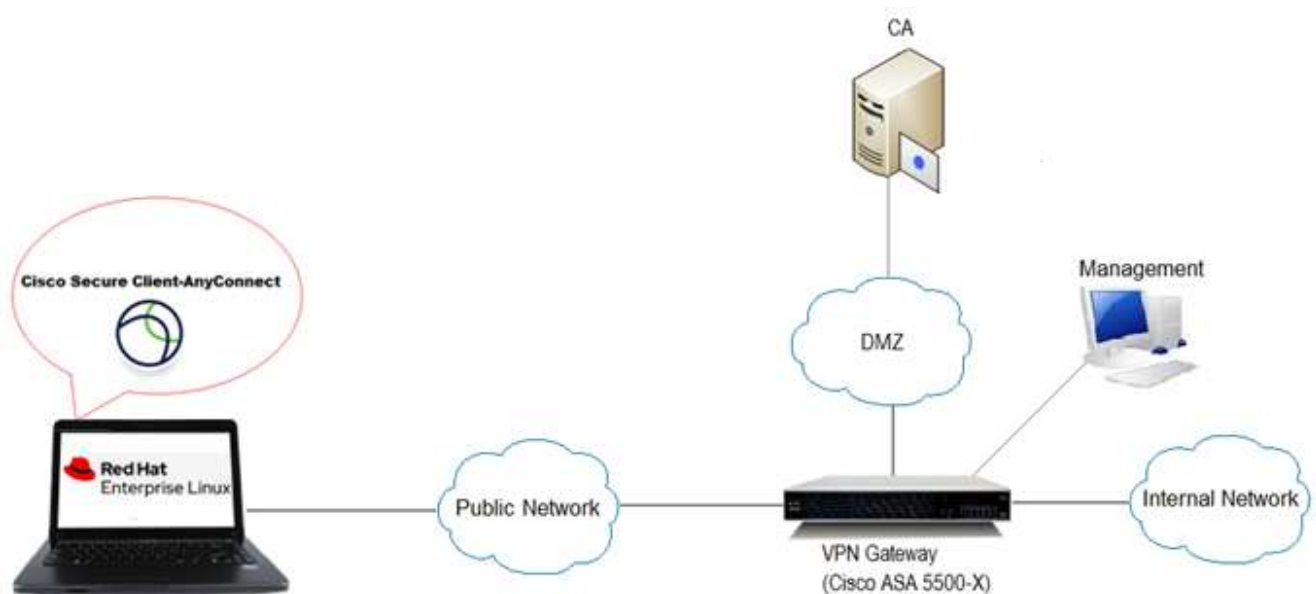
## Procedures and Operational Guidance for IT Environment

To operate in its evaluated configuration, the TOE requires a minimum one (1) Certificate Authority (CA), one (1) VPN Gateway, and one (1) Red Hat Enterprise Linux 8.2 platform.

To resemble customer PKI environments, a two-tier CA solution using an Offline Root CA and an Enterprise Subordinate CA employing Microsoft 2012 R2 Certificate Authority (CA) will be referenced in this section. Other CA products in place of Microsoft may be used.

A Root CA is configured as a standalone (Workgroup) server while the Subordinate CA is configured as part of a Microsoft domain with Active Directory services enabled. See figure 1 below.

**Figure 1. TOE and Environment**



The Subordinate CA issues X.509 digital certificates and provides a Certificate Revocation List (CRL) to the TOE Platform and VPN Gateway.

Alternatively, one (1) single root Enterprise CA could be deployed.

- Install and Configure a Certificate Authority

If using a Microsoft two-tier CA solution, install and configure a Root (GRAYCA) and Enterprise Subordinate Certificate Authority (GRAYSUBCA1) in accordance with the guidance from the vendor. The following is a step-by-step guide for the configuration of Microsoft Active Directory Certificate Services:

<http://technet.microsoft.com/en-us/library/cc772393%28v=ws.10%29.aspx>

It is assumed both the Offline Root CA (GRAYCA) certificate and the Enterprise Subordinate CA (GRAYSUBCA1) certificates depicted in figure 1 are installed and trusted to ensure a trusted certificate chain is established. If using a CA from a vendor other than Microsoft, follow that vendor's CA installation guidance.



Regardless of the CA product used, the ECDSA and RSA certificates on the ASA MUST have the following Key Usage and Extended Key Usage properties:

- o Key Usage: Digital Signature, Key Agreement
- o EKU: IP security IKE intermediate, IP end security system

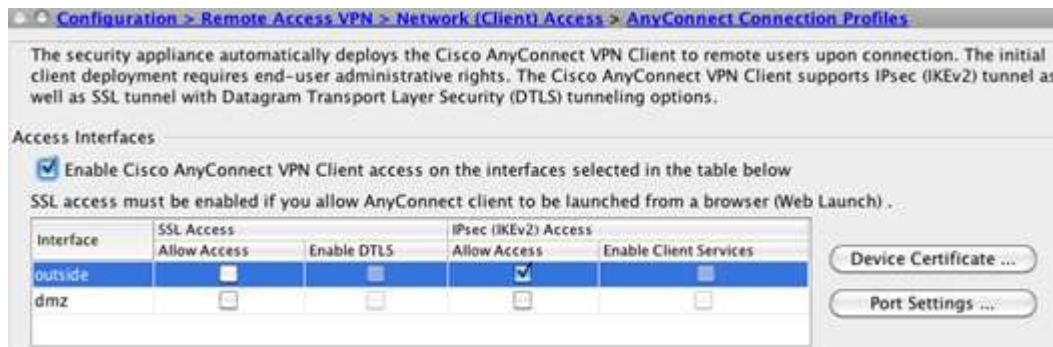
The Subject Alternative Name (SAN) fields within ECDSA and RSA certificates on the ASA MUST match the connection information specified within the Cisco Secure Client profile on the client.

■ Install and Configure a VPN Gateway

Install Cisco ASA 9.1 (or later), optionally with ASDM, in accordance with installation guides and release notes appropriate for the versions to be installed. ASDM allows the ASA to be managed from a graphical user interface. Alternatively, if the administrator prefers, equivalent command line (CLI) configuration steps could be used.

Configuration Note: As there are parameters managed by the ASA, the Gateway Administrator must follow the steps in this section to ensure the TOE is in its evaluated configuration.

- o Enable AnyConnect and IKEv2 on the ASA. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles and select Enable Cisco AnyConnect checkbox and Allow Access under IKEv2.



- o On the AnyConnect Connection Profiles page mentioned above, select Device Certificate. Ensure Use the same device certificate... is NOT checked and select the EC ID certificate under the ECDSA device certificate. Then select Ok.



- o Create IKEv2 crypto policy using the algorithms permitted in the Common Criteria evaluated configuration. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Policies and add an IKEv2 policy.

Select Add and enter 1 for the highest priority. The range is 1 to 65535, with 1 the highest priority.

Encryption:

AES	Specifies AES-CBC with a 128-bit key encryption for ESP.
AES-256	Specifies AES-CBC with a 256-bit key encryption for ESP.
AES-GCM-128	Specifies AES Galois Counter Mode 128-bit encryption
AES-GCM-256	Specifies AES Galois Counter Mode 256-bit encryption

D-H Group: Choose the Diffie-Hellman group identifier. This is used by each IPsec peer to derive a shared secret, without transmitting it to each other. Valid Selections are: 19, 20

PRF Hash - Specify the PRF used for the construction of keying material for all of the cryptographic algorithms used in the SA. Valid selections are: sha256 and sha384

In this example configuration select:

Priority: **1**

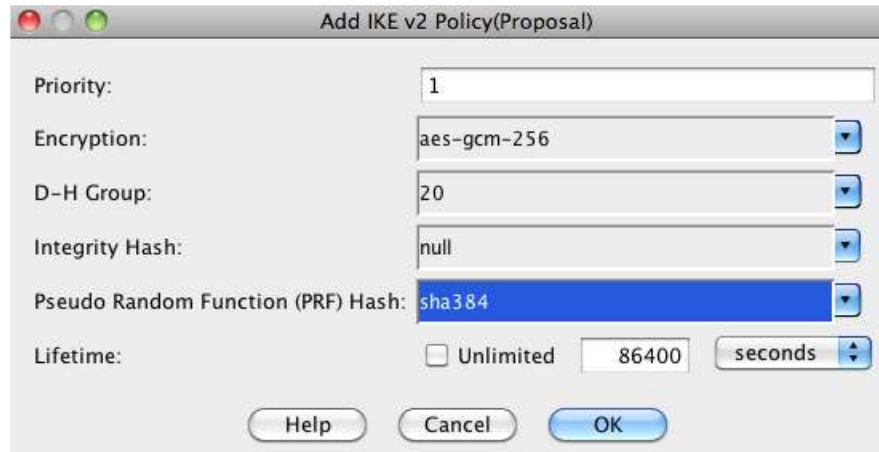
**AES Galois Counter Mode (AES-GCM) 256-bit encryption:** When GCM is selected, it precludes the need to select an integrity algorithm. This is because the authenticity capabilities are built into GCM, unlike CBC (Cipher-Block Chaining).

Diffie-Hellman **Group: 20**

Integrity Hash: **Null**

PRF Hash: **sha384**

Lifetime: **86400**



The screenshot shows a dialog box titled "Add IKE v2 Policy(Proposal)". It contains the following fields and values:

- Priority: 1
- Encryption: aes-gcm-256
- D-H Group: 20
- Integrity Hash: null
- Pseudo Random Function (PRF) Hash: sha384
- Lifetime:  Unlimited, 86400, seconds

At the bottom of the dialog are three buttons: Help, Cancel, and OK.

Select **Ok**.

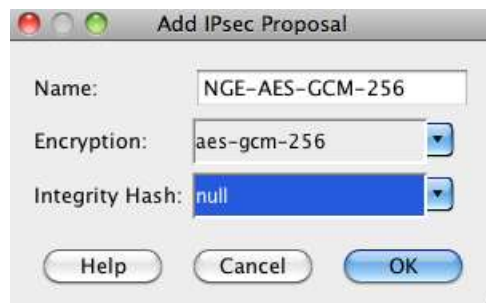
**Administrator Note:** Use of any Additional Encryption, DH-Group, Integrity or PRF Hash not listed above is not evaluated.

**Administrator Note:** The advanced tab displays the IKE strength enforcement parameter. Ensure the Security Association (SA) Strength Enforcement parameter is checked. This ensures that the strength of the IKEv2 encryption cipher is higher than the strength of its child IPsec SA's encryption ciphers. Higher strength algorithms will be downgraded.

The CLI equivalent is: `crypto ipsec ikev2 sa-strength-enforcement`

- o Create an IPSEC proposal. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IPsec Proposals (Transform Sets) and add an IKEv2 IPsec Proposal. then select Ok.

In the example below the name used is NGE-AES-GCM-256 with AES-GCM-256 for encryption and Null for the Integrity Hash:

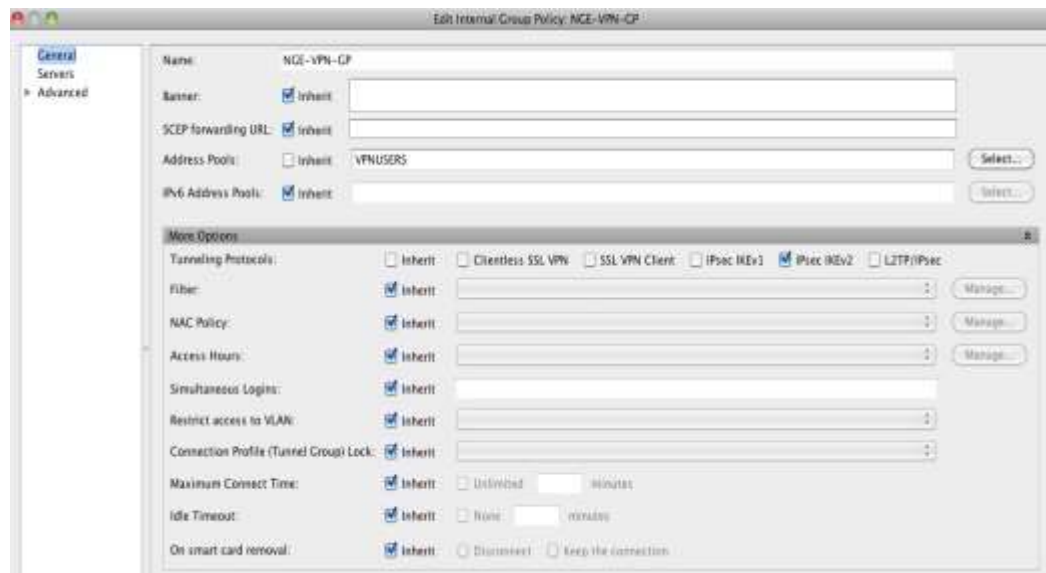


- o Create a dynamic crypto map, select the IPsec proposal and apply to the outside interface. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps. Select Add, select the outside interface and the IKEv2 proposal. Click the Advanced Tab. Ensure the following:
  - Enable NAT-T —Enables NAT Traversal (NAT-T) for this policy
  - Security Association Lifetime Setting — is set to 8 hours (28800 seconds)
- o Create an address pool VPNUSERS that will be assigned to VPN users. Address pools contain the following fields:
  - Name—Specifies the name assigned to the IP address pool.
  - Starting IP Address—Specifies the first IP address in the pool.
  - Ending IP Address—Specifies the last IP address in the pool.
  - Subnet Mask—Selects the subnet mask to apply to the addresses in the pool.

In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools and add an IP pool specifying the above fields and then select Ok.

Add a group policy that will apply the desired settings to the VPN users. Group Policies lets you manage AnyConnect VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs stored either internally on the ASA device. Configuring the VPN group policy lets users inherit attributes that you have not configured at the individual group or username level. By default, VPN users have no group policy association. The group policy information is used by VPN tunnel groups and user accounts. In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > Group Policies and Add an internal group policy. Ensure the VPN tunnel protocol is set to IKEv2 and the IP pool created above is referenced in the policy by de-selecting the Inherit check box and selecting the appropriate setting. Relevant DNS, WINS and domain names can also be added in the policy in the Servers section.

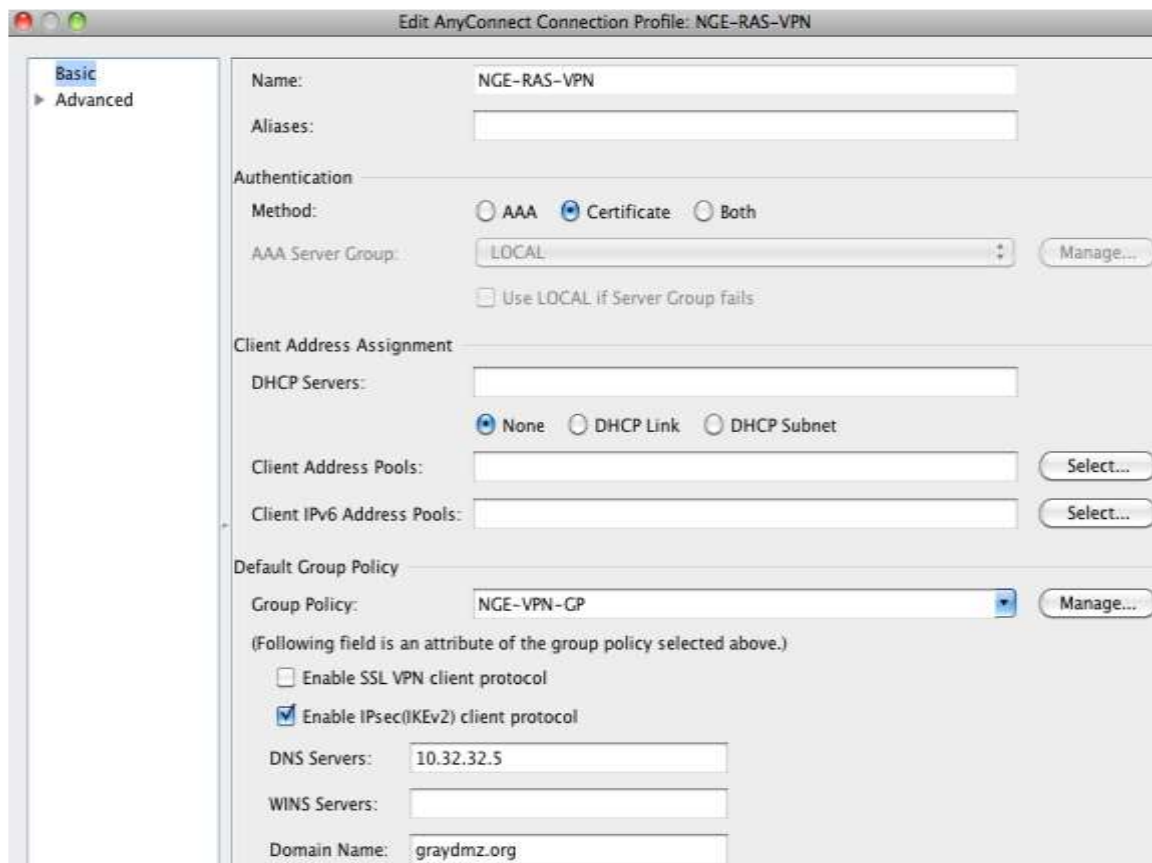
Refer to example group policy NGE-VPN-GP below:



- o Create a tunnel group name. A tunnel group contains tunnel connection policies for the IPsec connection. A connection policy can specify authentication, authorization, and accounting servers, a default group policy, and IKE attributes.

In ASDM, go to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles. At the bottom of the page under Connection Profiles, select Add.

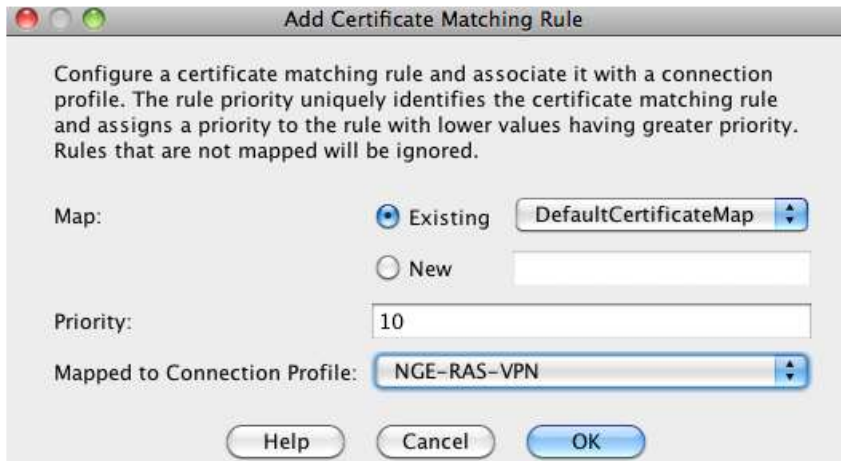
In the example below the tunnel group name NGE-VPN-RAS is used.



The configuration references Certificate authentication, the associated group policy NGE-VPN-GP and Enable IPsec (IKEv2). DNS and domain name can also be added here. Also ensure only IPsec is used by **not** checking the enable SSL VPN Client Protocol.

- o Create a certificate map, mapping the NGE VPN users to the VPN tunnel group that was previously created. The certificate map will be applied to the AC users. In this scenario, the Subordinate CA common name was matched to ensure an incoming TOE platform request with an EC certificate issued from the Subordinate CA will be mapped to the appropriate tunnel group that was previously created. VPN users that are not issued a certificate from the EC CA will fall back to the default tunnel groups and fail authentication and will be denied access.

In ASDM, go to Configuration > Remote Access VPN > Advanced > Certificate to AnyConnect and Clientless SSL VPN Connection Profile Maps. Under Certificate to Connection Profile Maps select Add. Choose the existing DefaultCertificateMap with a priority of 10 and reference the NGE-RAS-VPN tunnel group.



In ASDM, go to Configuration > Remote Access VPN > Advanced > Certificate to AnyConnect and Clientless SSL VPN Connection Profile Maps. Under Mapping Criteria select Add. Select Issuer for field, Common Name (CN) for component, Contains for Operator, and then select Ok.



Ensure to select APPLY on the main page and SAVE the configuration.

- o Configure ASA to accept VPN connections from the AnyConnect VPN client, use the AnyConnect VPN Wizard. This wizard configures IPsec (IKEv2) VPN protocols for remote network access. Refer to the instructions here:

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/asdm710/vpn/asdm-710-vpn-config/vpn-wizard.html#ID-2217-0000005b>

## Preparative Procedures and Operational Guidance for the TOE

To install Cisco Secure Client - AnyConnect 5.1 for Red Hat Enterprise Linux 8.2 follow the steps below:

1. Ensure the Linux Requirements are met. Refer to [Cisco Secure Client Support for Linux](#) in [2].
2. Download the Cisco Secure Client for Linux TOE software from [https://software.cisco.com/software/cswws/platform/home?locale=en\\_US#](https://software.cisco.com/software/cswws/platform/home?locale=en_US#) into a directory on the TOE platform. Ensure the RPM package is downloaded and the version is 5.1.
3. Navigate to the folder where you have downloaded the Cisco Secure Client for Linux TOE RPM Package.
4. The initial download is a gzip archive, which must be unzipped. The command 'gunzip filename' will extract the contents to the same directory in which the initial file is located.
5. The extracted file is a tarball archive (multiple files packed into one), which also must be uncompressed. The command 'tar -xvf filename' will extract the contents to the same directory in which the initial file is located.
6. The Cisco Secure Client for Linux RPM installation package is digitally signed. The Linux platform is used to verify the digital signature prior to installation. The Linux Administrator must import the public key by entering the following command:

```
rpm --import CiscoSystemsInc.pgp
```

7. The Linux Administrator must run the following commands for the Linux platform to verify the digital signatures on the Cisco Secure Client and DART RPM packages:

```
rpm -K cisco-secure-client-vpn-5.1.03072-1.x86_64.rpm
```

```
rpm -K cisco-secure-client-dart-5.1.03072-1.x86_64.rpm
```

If the output for either says "digests signatures OK" you may proceed with the installation. If the output says "digests SIGNATURES NOT OK" you must not proceed. Please contact Cisco Technical Support for further assistance.

8. To install the Cisco Secure Client for Linux RPM package enter the following:

```
rpm -i cisco-secure-client-vpn-5.1.03072-1.x86_64.rpm
```

The installation should complete.

9. To install the optional DART RPM package enter the following:

```
rpm -i cisco-secure-client-dart-5.1.03072-1.x86_64.rpm
```

After installation the Administrator must follow the steps below to place the TOE in the evaluated configuration:



## Cisco Secure Client Profiles

Cisco Secure Client features and settings are enabled in profiles. Profiles are created using the profile editors. A form of the profile editor exists integrated with the ASDM tool. This form of the Profile editor is used when the ASA is used to centrally manage profiles globally for all Cisco Secure Client users.

To add a new client profile to the ASA from ASDM:

Open ASDM and select Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile

There is also a standalone version of the profile editors for Linux that you can use as an alternative to the profile editors integrated with ASDM. Users with sudo privileges can manage or modify their own profiles.

For initial configuration of the TOE, Secure Client profiles must either be:

- Created using the profile editors integrated with ASDM and exported to a local or remote Linux host computer where the Cisco Secure Client resides. For this option refer to the Exporting an Cisco Secure Client Profile function within ASDM.
- Created using standalone version of the Profile Editor. See section below.

## Cisco Secure Client Stand-Alone Profile Editor

To use the standalone version of the Profile Editor, change directory to `‘/opt/cisco/secureclient/vpn/profile’`

Using a standard editor such as vi, edit the `myvpn.xml` file. The name of the Group Policy on the ASA Gateway MUST match the name of the .xml file in the location above, or profile mismatch errors will occur.

Populate the contents of the XML file using the example below.

```
<?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>
    <CertificateStoreMac>All</CertificateStoreMac>
    <CertificateStoreOverride>false</CertificateStoreOverride>
    <ProxySettings>Native</ProxySettings>
    <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
    <AuthenticationTimeout>30</AuthenticationTimeout>
    <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
    <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
    <LocalLanAccess UserControllable="true">false</LocalLanAccess>
    <DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
    <ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
    <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
    <AutoReconnect UserControllable="false">true
      <AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
    </AutoReconnect>
    <SuspendOnConnectedStandby>false</SuspendOnConnectedStandby>
    <AutoUpdate UserControllable="false">true</AutoUpdate>
    <RSA SecurIDIntegration UserControllable="false">Automatic</RSA SecurIDIntegration>
    <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
    <LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
    <WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
    <LinuxVPNEstablishment>LocalUsersOnly</LinuxVPNEstablishment>
    <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
    <PPPEExclusion UserControllable="false">Disable
      <PPPEExclusionServerIP UserControllable="false"></PPPEExclusionServerIP>
    </PPPEExclusion>
    <EnableScripting UserControllable="false">false</EnableScripting>
    <EnableAutomaticServerSelection UserControllable="false">false
      <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
  </ClientInitialization>
</AnyConnectProfile>
```

## Preparative Procedures and Operational Guidance for the TOE

```

        <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
    </EnableAutomaticServerSelection>
    <RetainVpnOnLogoff>>false</RetainVpnOnLogoff>
    </RetainVpnOnLogoff>
    <CaptivePortalRemediationBrowserFailover>>false</CaptivePortalRemediationBrowserFailover>
    <AllowManualHostInput>>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
    <HostEntry>
        <HostName>Example Org</HostName>
        <HostAddress>vpn.example.com</HostAddress>
        <PrimaryProtocol>IPsec
            <StandardAuthenticationOnly>false
            </StandardAuthenticationOnly>
        </PrimaryProtocol>
    </HostEntry>
</ServerList>
</AnyConnectProfile>

```

The Primary Protocol (IPsec) and Standard Authentication (false) values above in bold are mandatory.

Replace the contents of HostName and HostAddress with values for your organization. The HostAddress section specifies configuration of the reference identifier for the VPN Gateway peer. During IKE phase 1 authentication, the Secure Client App compares the reference identifier to the identifier presented by the VPN Gateway. If the Secure Client App determines they do not match, authentication will not succeed.

## Cisco Secure Client Local Policy

Changed directory to `/opt/cisco/secureclient`. This directory will contain the **AnyConnectLocalPolicy.xml** file. The AnyConnectLocalPolicy.xml is an XML file on the client containing security settings. This file is not deployed or managed by the ASA VPN Gateway.

Using a standard editor such as vi, edit the **AnyConnectLocalPolicy.xml** file. The following settings must be set to True:

```

<ExcludeFirefoxNSSCertStore>true</ExcludeFirefoxNSSCertStore>
<FipsMode>true</FipsMode>
<StrictCertificateTrust>true</StrictCertificateTrust>
<OCSPRevocation>true</OCSPRevocation>

```

Strict Certificate Trust prevents users the ability to accept a certificate that could not be successfully verified.

Additional information on these settings can be found in [The Cisco Secure Client Local Policy](#) section of [1].

After making change to FIPS mode, you will need to restart the vpn agent daemon:

```
systemctl restart vpnagentd
```

## Configure Certificates

Cisco Secure Client requires an X.509 certificate and associated private key. Certificates are stored on the Linux file system in a folder within the user's home folder (e.g. /home/user1): `/home/user1/.cisco/certificates/client`.

The private key for the certificate is stored under: `/home/user1/.cisco/certificates/client/private`

Note the following requirements:

## Preparative Procedures and Operational Guidance for the TOE

- All certificate files must end with the extension .pem.
- All private key files must end with the extension .key.
- A client certificate and its corresponding private key must have the same filename. For example: client.pem and client.key.

1. By default, the path for installing client certificate and the private key is not present. In the user's home directory (e.g., /home/user1) execute the following command:

```
mkdir -p .cisco/certificates/client/private/
```

2. At the top level of the home directory, (i.e. /home/user1), generate a RSA or ECDSA private key.

To generate a RSA key enter:

```
openssl genrsa -out ../cisco/certificates/client/private/client.key 2048
```

To generate a ECDSA key enter:

```
openssl ecparam -name prime256v1 -genkey -out ../cisco/certificates/client/private/client.key
```

3. Generate the Certificate Signing Request (CSR) for the Linux Client Certificate

```
openssl req -sha256 -days 730 -new -key ../cisco/certificates/client/private/client.key -out ../cisco/certificates/client/client.csr
```

You will be prompted to supply the following attributes: Country Name, State or Province Name, Locality, Organization, Organizational Unit, Common Name, and email address (optional). You may also provide extra attributes when prompted.

4. The generated **client.csr** is used to request a CA to issue a user identity certificate for the Linux client.
5. Once the certificate is issued by CA, copy the certificate to the following location under the user's home directory.

```
/home/user1/.cisco/certificates/client/client.pem
```

The CA Administrator should provide the user identify certificate in PEM format.

6. The CA Administrator must also provide the Linux Administrator with the chain of CA certificates each in PEM format. The CA certificates need to be stored under one of the following locations:

- a. For individual users, store the CA certificates under:

```
/home/user1/.cisco/certificates/ca
```

- b. To provide trusted CA certificates for all users on the machine that use Cisco Secure Client, store the CA certificates under:

```
/opt/.cisco/certificates/ca/
```

## Start Cisco Secure Client

1. To start, click on the Cisco Secure Client App on the Desktop.



Alternatively, you may open a terminal window and run **'gtk-launch cisco-secureclient'** or enter the following command at the CLI: **'/opt/cisco/secureclient/bin/vpnui'**.

## Operational Guidance for the TOE

### Establish a VPN Connection

1. Once Cisco Secure Client is launched, Click the Statistics Tab and the Details button. Ensure FIPS Mode is Enabled.
2. Click the VPN tab and ensure the status at the bottom of the window says “Ready to Connect”.
3. The VPN tab prompts for a “Connect to” address. If you did not provide a FQDN of your Gateway server in the profile editor, you must supply one.



4. Click Connect.

The Administrator should note the following PROTECT, BYPASS, and DISCARD rules regarding the use of IPsec in Cisco Secure Client:

- PROTECT

Entries for PROTECT are configured through remote access group policy on the ASA using ASDM. For PROTECT entries, the traffic flows through the IPsec VPN tunnel provided by the TOE. No configuration is required for the TOE tunnel all traffic. The administrator optionally could explicitly set this behavior with the command in their Group Policy: `split-tunnel-policy tunnelall`

- BYPASS

The TOE supports BYPASS operations (when split tunneling has been explicitly permitted by Remote Access policy). When split tunneling is enabled, the ASA VPN Gateway pushes a list of network segments to the TOE to PROTECT. All other traffic travels unprotected without involving the TOE thus bypassing IPsec protection.

Split tunneling is configured in a Network (Client) Access group policy. The administrator has the following options:

Excludespecified: Exclude only networks specified by `split-tunnel-network-list`

Tunnelspecified: Tunnel only networks specified by `split-tunnel-network list`

Refer to the "About Configuring Split Tunneling for AnyConnect Traffic" section in the [VPN ASDM configuration guide](#) and see steps provided in the "Configure Split-Tunneling for AnyConnect Traffic" section.

After making changes to the group policy in ASDM, be sure the group policy is associated with a Connection Profile in Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy.

BYPASS SPD entries are provided by the host platform through implicit network traffic permit rules. No configuration is required on the TOE platform to allow it to pass this traffic.

- DISCARD

DISCARD rules are performed exclusively by the TOE platform. There is no administrative interface for specifying a DISCARD rule.

## Integrity Verification

Integrity verification is performed each time the Cisco Secure Client app is loaded. A self-test is performed to verify the digital signature on the TOE's executable files. If the integrity verification fails to successfully complete, the GUI will not load, rendering the app unusable. The Linux log file will contain a CERTIFICATE\_ERROR\_SIGN\_VERIFY\_FAILED message.

If the integrity verification is successful, the app GUI will load and operate normally. The Linux log file will contain a 'code-signing verification succeeded' message.

## Monitor and Troubleshoot

Refer to the [Troubleshoot Cisco Secure Client](#) section of [1].

## Exiting Secure Client

Exiting Secure Client terminates the current VPN connection and stops all VPN processes. Use this action sparingly. Other apps or processes on your device may be using the current VPN connection and exiting Cisco Secure Client may adversely affect their operation.

To exit, click Disconnect from the Secure Client applet.

## Cryptographic Support

The TOE provides cryptography in support of IPsec with ESP symmetric cryptography for bulk AES encryption/decryption and SHA-2 algorithm for hashing. In addition the TOE provides the cryptography to support Elliptic-Curve Diffie-Hellman key exchange and derivation function used in the IKEv2 and ESP protocols. Instructions to configure cryptographic functions are described in the "Procedures and Operational Guidance for IT Environment" section of this document. The TOE operates in IPsec tunnel mode without any configuration needed, and the TOE does not support IPsec transport mode.

## Trusted Updates

This section provides instructions for securely accepting the TOE and any subsequent TOE updates. “Updates” are a new version of the TOE.

TOE versioning can be queried by the user by clicking the ‘About’ button which will display version information.

The administrator can check for software updates at Cisco Software Central which is available at:

[https://software.cisco.com/software/cswws/platform/home?locale=en\\_US#](https://software.cisco.com/software/cswws/platform/home?locale=en_US#)

Customers can also subscribe to the Cisco Notification Service allows users to subscribe and receive important information regarding product updates. Full information is provide in the Cisco Security Vulnerability Policy available at:

[https://tools.cisco.com/security/center/resources/security\\_vulnerability\\_policy.html](https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html)

When there is an update for Cisco Secure Client, the process to update is the same as a new installation. Refer to steps 1 – 9 on pages 12-13 of this document.

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). The RSS feeds are a free service.

## Contacting Cisco

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).