Introduction

This document describes the basic configuration of a Cisco IOS Router as an AnyConnect SSLVPN Headend.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Internetwork Operating System (IOS)
- AnyConnect Secure Mobility Client
- General Secure Sockets Layer (SSL) Operation

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 892W Router running 15.3(3)M5
Licensing Information for Different IOS Versions

- The securityk9 feature set is required to use the SSLVPN features, regardless of which IOS version is used.
- IOS 12.x - the SSLVPN feature is integrated into all 12.x images that start with 12.4(6)T which have at least a security license (ie. advsecurityk9, adventerprisek9, and so on).
- IOS 15.0 - earlier versions require an LIC file to be installed on the router which will allow for 10, 25, or 100 user connections. Right to Use* licenses were implemented in 15.0(1)M4
- IOS 15.1 - earlier versions require an LIC file to be installed on the router which will allow for 10, 25, or 100 user connections. Right to Use* licenses were implemented in 15.1(1)T2, 15.1(2)T2, 15.1(3)T, and 15.1(4)M1
- IOS 15.2 - all 15.2 versions offer Right to Use* licenses for SSLVPN
- IOS 15.3 and beyond - earlier versions offer Right to Use* licenses. Starting in 15.3(3)M, the SSLVPN feature is available after you boot into a securityk9 technology-package

For RTU licensing, an evaluation license will be enabled when the first webvpn feature is configured (that is, webvpn gateway GATEWAY1) and the End User License Agreement (EULA) has been accepted. After 60 days, this evaluation license becomes a permanent license. These licenses are honor based and require a paper license to be purchased in order to use the feature. Additionally, rather than being limited to a certain number of uses, the RTU allow for the maximum number of simultaneous connections which the router platform can support concurrently.

Significant Software Enhancements

These bugs IDs resulted in significant features or fixes for AnyConnect:

- CSCti89976: Added support for AnyConnect 3.x to IOS
- CSCtx38806: Fix for BEAST Vulnerability, Microsoft KB2585542

Configure

Step 1. Confirm License is Enabled

The first step when AnyConnect is configured on an IOS Router headend is to confirm that the license has been correctly installed (if applicable) and enabled. Refer to the licensing information in the previous section for the licensing specifics on different versions. It depends on the version of code and platform whether show license lists an SSL_VPN or securityk9 license. Regardless of the version and license, the EULA will need to be accepted and the license will show as Active.

Step 2. Upload and Install AnyConnect Secure Mobility Client Package on Router

To upload an AnyConnect image to the VPN headend serves two purposes. Firstly, only operating systems which have AnyConnect images present on the AnyConnect headend will be permitted to connect. For example, Windows clients require a Windows package to be installed on the headend, Linux 64-bit clients require a Linux 64-bit package, and so on. Secondly, the
AnyConnect image installed on headend will automatically be pushed down to the client machine upon connection. Users that connect for the first time will be able to download the client from the web portal and users that return will be able to upgrade, provided the AnyConnect package on the headend is newer than what is installed on their client machine.

AnyConnect packages can be obtained through the AnyConnect Secure Mobility Client section of the [Cisco Software Downloads website](https://www.cisco.com/c/en/us/support/downloads/). While there are many options available, the packages which are to be installed on the headend will be labeled with the operating system and Head-end deployment (PKG). AnyConnect packages are currently available for these operating system platforms: Windows, Mac OS X, Linux (32-bit), and Linux 64-bit. Note that for Linux, there are both 32 and 64-bit packages. Each operating system requires the proper package to be installed on the headend in order for connections to be permitted.

Once the AnyConnect package has been downloaded, it can be uploaded to the Router's flash with the `copy` command via TFTP, FTP, SCP, or a few other options. Here is an example:

```
After you copy the AnyConnect image to the flash of the Router, it must be installed via command line. Multiple AnyConnect packages can be installed when you specify a sequence number at the end of the installation command; this will allow for the Router to act as headend for multiple client operating systems. When you install the AnyConnect package, it will also move it to the `flash:/webvpn/` directory if it was not copied there initially.
```

On versions of code which were released before 15.2(1)T, the command to install the PKG is slightly different.

### Step 3. Enable the http Server on the Router

### Step 4. Generate RSA Keypair and Self-Signed Certificate

When you configure SSL or any feature which implements Public Key Infrastructure (PKI) and digital certificates, a Rivest-Shamir-Adleman (RSA) keypair is required for the signing of the certificate. The follow command will generate an RSA keypair which will then be used when the self-signed PKI certificate is generated. When you make use of a modulus of 2048 bits, it is not a requirement, it is recommended to use the largest modulus available for enhanced security and compatibility with the AnyConnect client machines. To use a descriptive label is also recommended as it will allow for ease of key management. The key generation can be confirmed with the `show crypto key mypubkey rsa` command.

**Note:** As there are many security risks associated with making RSA keys exportable, the recommended practice is to ensure keys are configured to be not exportable which is the default. The risks that are involved when you make the RSA keys exportable are discussed in the this document: [Deploying RSA Keys Within a PKI](https://www.cisco.com/c/en/us/support/security/rsa-key-generator-documents.html).

Once the RSA keypair has successfully been generated, a PKI trustpoint must be configured with our router's information and RSA keypair. The Common Name (CN) in the Subject-Name should be configured with the IP address or Full Qualified Domain Name (FQDN) which users use to connect to the AnyConnect gateway; in this example, the clients use the FQDN of fdenofa-SSLVPN.cisco.com when they attempt to connect. While it is not mandatory, when you correctly
enter in the CN, it helps reduce the number of certificate errors that are prompted at login.

**Note**: Rather than using a self-signed certificate generated by the router, it is possible to use a certificate issued by a third-party CA. This can be done via a few different methods as discussed in this document: Configuring Certificate Enrollment for a PKI.

After the trustpoint has been correctly defined, the router must generate the certificate by using the `crypto pki enroll` command. With this process, it is possible to specify a few other parameters such as serial number and IP address. However, this is not required. The certificate generation can be confirmed with the `show crypto pki certificates` command.

**Step 5. Configure Local VPN User Accounts**

While it is possible to use an external Authentication, Authorization, and Accounting (AAA) server, for this example local authentication is used. These commands will create a user name VPNUSER and also create an AAA authentication list named SSLVPN_AAA.

**Step 6. Define Address Pool and Split Tunnel Access List to be Used by Clients**

A local IP address pool must be created in order for AnyConnect client adapters to obtain an IP address. Ensure you configure a large enough pool to support the maximum number of simultaneous AnyConnect client connections.

By default, AnyConnect will operate in full tunnel mode which means that any traffic generated by the client machine will be sent across the tunnel. As this is typically not desirable, it is possible to configure an Access Control List (ACL) which then defines traffic which should or should not be sent across the tunnel. As with other ACL implementations, the implicit deny at the end eliminates the need for an explicit deny; therefore, it is only necessary to configure permit statements for the traffic which should be tunneled.

**Step 7. Configure the Virtual-Template Interface (VTI)**

**Dynamic VTIs** provide an on-demand separate Virtual-Access interface for each VPN session that allows highly secure and scalable connectivity for remote-access VPNs. The DVTI technology replaces dynamic crypto maps and the dynamic hub-and-spoke method that helps establish tunnels. Because DVTIs function like any other real interface they allow for more complex Remote Access deployment because they support QoS, firewall, per-user attributes and other security services as soon as the tunnel is active.

```
interface Loopback0
  ip address 172.16.1.1 255.255.255.255
!
interface Virtual-Template 1
  ip unnumbered Loopback0
```

**Step 8. Configure WebVPN Gateway**

The WebVPN Gateway is what defines the IP address and port(s) which will be used by the
AnyConnect headend, as well as the SSL encryption algorithm and PKI certificate which will be presented to the clients. By default, the Gateway will support all possible encryption algorithms, which vary depending on the IOS version on the router.

```bash
interface Loopback0
  ip address 172.16.1.1 255.255.255.255

interface Virtual-Template 1
  ip unnumbered Loopback0
```

**Step 9. Configure WebVPN Context and Group Policy**

The WebVPN Context and Group Policy define some additional parameters which will be used for the AnyConnect client connection. For a basic AnyConnect configuration, the Context simply serves as a mechanism used to call the default Group Policy which will be used for AnyConnect. However, the Context can be used to further customize the WebVPN splash page and WebVPN operation. In the defined Policy Group, the SSLVPN_AAA list is configured as the AAA authentication list which the users are a member of. The `functions svc-enabled` command is the piece of configuration which allows users to connect with the AnyConnect SSL VPN Client rather than just WebVPN through a browser. Lastly, the additional SVC commands define parameters which are relevant only to SVC connections: svc address-pool tells the Gateway to handout addresses in the ACPool to the clients, svc split include defines the split tunnel policy per ACL 1 defined above, and svc dns-server defines the DNS server which will be used for domain name resolution. With this configuration, all DNS queries will be sent to the specified DNS server. The address which is received in the query response will dictate whether or not the traffic is sent across the tunnel.

```bash
webvpn context SSL_Context
gateway SSLVPN_Gateway
inservice
policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  functions svc-enabled
  svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
  svc split include acl 1
  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```

**Step 10 (Optional). Configure a Client Profile**

Unlike on ASAs, Cisco IOS does not have a built-in GUI interface that can assist admins in creating the client profile. The AnyConnect client profile needs to be created/edited separately with the Stand-Alone Profile Editor.

**Tip**: Look for anyconnect-profileeditor-win-3.1.03103-k9.exe

Follow these steps to have the Router deploy the profile:

1. Upload it to IOS Flash using ftp/tftp
2. Use this command to identify the profile that was just uploaded:

   ```bash
   webvpn context SSL_Context
   gateway SSLVPN_Gateway
   inservice
   policy group SSL_Policy
   ```
aaa authentication list SSLVPN_AAA
functions svc-enabled
svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
svc split include acl 1
svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy

Tip: On IOS versions older than 15.2(1)T, this command needs to be used:
webvpn import svc profile <profile_name> flash:<profile.xml>

3. Under the context, use this command to link the profile to that context:

   1. webvpn context SSL_Context
gateway SSLVPN_Gateway
inservice
policy group SSL_Policy
   aaa authentication list SSLVPN_AAA
   functions svc-enabled
   svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
   svc split include acl 1
   svc dns-server primary 8.8.8.8
   virtual-template 1
default-group-policy SSL_Policy

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Verify

Once the configuration is complete, when you access the Gateway address and port via browser, it will return to the WebVPN splash page.
After you log in, the WebVPN home page is displayed. From here, click **Tunnel Connection (AnyConnect)**. When Internet Explorer is used, ActiveX is utilized to push down and install the AnyConnect client. If it is not detected, Java will be used instead. All other browsers use Java immediately.
Once the installation is completed, AnyConnect will automatically attempt to connect to the WebVPN Gateway. As a self-signed certificate is being used for the Gateway to identify itself, multiple certificate warnings will appear during the connection attempt. These are expected and must be accepted for the connection to continue. To avoid these certificate warnings, the self-signed certificate being presented must be installed in trusted certificate store of the client machine, or if a third-party certificate is being used then the Certificate Authority certificate must be in trusted certificate store.

When the connection completes negotiation, click on the gear icon in the lower left of AnyConnect will display some advanced information about the connection. On this page it is possible to view some connection statistics and route details attained from the split tunnel ACL in the Group Policy configuration.

Here is the final running-configuration result from the configuration steps:
Troubleshoot

There are a few common components to check for when you troubleshoot AnyConnect connection issues:

- As the client must present a certificate, it is a requirement that the certificate specified in the WebVPN Gateway be valid. To issue a `show crypto pki certificate` will show information that pertains to all certificates on the router.
- Whenever a change is made to the WebVPN configuration, it is a best practice to issue a no inservice and inservice on both the Gateway and Context. This will ensure the changes take effect properly.
- As mentioned earlier, it is a requirement to have an AnyConnect PKG for each client operating system which will connect to this Gateway. For example, Windows clients require a Windows PKG, Linux 32-bit clients require a Linux 32-bit PKG, and so on.
- When you consider both the AnyConnect client and browser-based WebVPN utilize SSL, to be able to access the WebVPN splash page generally indicates that AnyConnect will be able to connect (assume that the pertinent AnyConnect configuration is correct).

Cisco IOS offers some various debug webvpn options which can be used to troubleshoot a failing connections. This is the output generated from debug webvpn aaa, debug wevpn tunnel, and show webvpn session upon a successful connection attempt:

webvpn context SSL_Context
gateway SSLVPN_Gateway
inservice
policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  functions svc-enabled
  svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
  svc split include acl 1
  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy

Related Information

- SSL VPN Configuration Guide, Cisco IOS Release 15M&T
- AnyConnect VPN (SSL) Client on IOS Router with CCP Configuration Example