IPSec/L2TP/PPTP/PPP on the CAS (Deprecated)

These features are deprecated and will be removed in future releases.

This chapter discusses how to configure the encryption mechanisms supported by the CAS.

- Overview, page 7-1
- Configure IPSec Encryption, page 7-3
- Configure L2TP Encryption, page 7-6
- Configure PPTP Encryption, page 7-7
- Configure PPP, page 7-8
- Example Windows L2TP/IPSec Setup, page 7-9

This chapter describes how to configure secure tunnels between users and the CAS. If you require support for a larger VPN base, Cisco NAC Appliance allows you to deploy a VPN concentrator in front of the Clean Access Server. In this case, see Chapter 8, “Integrating with Cisco VPN Concentrators” for details.

Overview

The Clean Access Server itself supports secure Virtual Private Network (VPN) connections between the Clean Access Server (CAS) and end user devices. The CAS supports VPN connections via PPTP, L2TP/IPSec or native IPSec clients. You can use Windows 2000, Windows XP, or other Pre-Shared Key VPN clients to use this feature. Note that each Clean Access Server supports the following number of concurrent VPN connections:

- IPSec—no limit is in place
- PPTP—64 tunnels
- L2TP—64 tunnels
Overview

Figure 7-1 Encrypted Connections

The Clean Access Server acts as an endpoint for the following encryption mechanisms:

- IPSec (IP Security)
- L2TP
- PPTP

You can use encryption whether the Clean Access Server is running in Real-IP/NAT Gateway mode or Virtual Gateway (bridge) mode.

User computers must have the appropriate client software. When configuring the client software, the user should set up the untrusted interface address of the Clean Access Server as the VPN gateway. For L2TP and PPTP, the user will need to provide the password for the PPP tunnel. For more information, see Configure PPP, page 7-8.

Note

Devices allowed in the MAC filter list cannot establish VPN connections to the Clean Access Server (CAS). Only users logging in via web login or Clean Access agent can establish VPN connections to the CAS.

Enable VPN Policies

First, enable VPN policies for both the Clean Access Server and the user role. Then, perform the protocol-specific configuration described in the following sections.

1. Go to Device Management > CCA Servers > List of Servers, click the Manage button for the Clean Access Server, then go to Network > IPSec.
2. For the VPN Policy for Clean Access Server option, choose either Optional or Enforce. Note that the Clean Access Server supports the following number of concurrent VPN connections:
   - IPSec—no limit is placed
   - PPTP—64 tunnels
   - L2TP—64 tunnels

3. From User Management > User Roles > List of Roles, click the Edit icon next to the user role for which you want to enable encryption.

   ![User Management > User Roles](image)


4. In the Edit form that appears, choose either Optional or Enforce for the VPN Policy field, according to what you chose for the Clean Access Server.

5. Click Save Role.

**Configure IPSec Encryption**

The IP Security Protocol (IPSec) is an encryption standard for securing traffic between two computers on a network. IPSec provides significantly better security for wireless users than the mechanism normally associated with wireless networks, WEP. For one thing, WEP uses a shared key, which all users in the network must use. With readily available tools, an intruder can figure out the key, given a large enough data sample. IPSec, on the other hand, uses unique, dynamic keys for data encryption between the client and server.

With the Clean Access Server, you can require users to use IPSec, make it optional, or deny use of IPSec on the network per user role.

To utilize IPSec encryption, users must have IPSec client software on their machines. Many operating systems include an IPSec client. Windows XP, for example, includes the client as a snap-in module.

**To set up IPSec:**

1. Go to Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Network > IPSec.
2. For **VPN Policy for Clean Access Server**, choose either:
   - **Optional** – To make the use of IPSec connections to the Clean Access Server optional, at the client’s discretion.
   - **Enforce** – To require the use of IPSec connections to the Clean Access Server.

3. Configure the following settings for the IPSec policy:
   - **Default IPSec Preshared Key** – Enter the key used to encrypt the data exchanged at the time of authentication negotiation.
   - **Dynamic IPSec Key** – The Dynamic IPSec Key feature must be enabled on both the Clean Access Server and user role. Click **Enable** to give each user a unique, one-time preshared key upon logging in. The user should use this key as the preshared key in their IPSec client to create the IPSec connection.
     
     Leave as **Disable** to have the user use the default preshared key (shared by all users) to create the IPSec connection. The key is given to users in the web logout page (**Figure 7-3**) or Clean Access Agent VPN Info dialog (**Figure 7-4**) after a successful login.
Configure IPSec Encryption

Figure 7-3  IPSec Key—Logout Page for Web Login Users

- **Server Key Life** (default: 450 seconds) – How long the IPSec security association remains active. This should be greater than the Client Rekey Time.
- **Client Rekey Time** (default: 300 seconds) – This value is used by the IPSec client. It specifies how long the IPSec Client will propose that an IPSec SA be allowed to live before being regenerated. Typically, this value is shorter than the Server Key Life and at least 300 seconds.
- **Perfect Forward Secrecy (PFS)** – Enabling PFS (Perfect Forward Secrecy) ensures that the CAS utilizes completely new material when rekeying session keys. Otherwise, rekeys may be derived from material created at the point when the initial server key is created. Enabling PFS ensures that if one key is compromised, no other key is vulnerable due to the compromised key.

Note

Enabling PFS may result in slower CAS performance. Use of the legacy IPSec Client enables PFS by default.

Figure 7-4  IPSec Key—Clean Access Agent Users (VPN Info)
Configure L2TP Encryption

The Layer 2 Tunneling Protocol (L2TP) allows PPP frames to be tunneled through the network. L2TP and PPTP are alternatives to IPSec encryption. These formats are widely used due to the availability of client software supporting them.

Unlike IPSec, however, L2TP and PPTP require a dedicated IP address pool. The Clean Access Server uses the address pool to perform address translation of tunnelled traffic (Figure 7-5).

Figure 7-5 L2TP Address Translation

The address pool you use for both L2TP and PPTP pools depends on the Clean Access Server operating mode. Given a Clean Access Server with these interface addresses:

- eth0 (to trusted network): 192.168.151.55
- eth1 (to untrusted, managed network): 10.1.55.1

For Real-IP Gateway and Virtual Gateway, the IP pool must be a valid subnet (routable) on the eth0 side, such as 192.168.151.100–192.168.151.105.

For NAT Gateway, the IP pool can be any private subnet, such as 10.1.70.20–10.1.70.200.

Both L2TP and PPTP are used with PPP (Point-to-Point Protocol). Therefore, to set up L2TP or PPTP you will also need to configure PPP, as described below.

- MSS Clamping (default: 1400 bytes) – A restriction on the Maximum Segment Size (or packet size) of IPSec traffic. MSS Clamping replaces the traditional method of determining the maximum size of transmitted packets, dynamic MTU (maximum transfer unit) discovery. In MTU discovery, hosts negotiate the MTU size by ICMP at the time of data exchange. With MSS, the maximum packet size is predefined, so additional ICMP traffic is not needed.

- MSS Value – If MSS clamping is enabled, the maximum packet size, in bytes.

4. When finished, click Restart IPSec to restart the IPSec service with the new values.

5. Either allow or enforce the use of VPN by choosing the appropriate role policy in the role properties of the user (under User Management > User Roles > Add or Edit).
To set up L2TP:

1. Click the L2TP link in the Network tab to open the form.

**Figure 7-6 L2TP**

2. Click the Enable option.

3. In the L2TP IP Pool field, type the IP address range to be used for the point-to-point connections. Optionally, enter DNS and WIN Server addresses for the pool.

4. In the PPP form, enter the connection password (see Configure PPP, page 7-8) and click Update.

5. Click the Restart L2TP Service button.

Configure PPTP Encryption

Like L2TP, the Point-to-Point Tunneling Protocol (PPTP), allows PPP frames to be tunneled through the network. The actual data is encrypted using a session key and the initial session key is different per user. The session key itself is changed periodically. If configuring PPTP, you must also Configure PPP, page 7-8.

**Note**


To set up PPTP:

1. In the Network tab, click PPTP on the submenu to open the PPTP form.
Configure PPP

Setting up L2TP and PPTP requires configuring PPP (Point-to-Point Protocol). The PPP form (opened by clicking the PPP link in the Network tab) lets you specify the password and user name used to authenticate parties in a point-to-point connection that uses L2TP or PPTP tunneling.

Configure PPP

2. Click the Enable option.
3. In PPTP IP Pool, type the IP address range to use for the point-to-point connections. For information on pool values, see Configure L2TP Encryption, page 7-6.
4. Optionally, type appropriate DNS Server and WIN Server addresses for the pool clients.
5. In the PPP form, enter the connection password (see Configure PPP, page 7-8) and click Update.
6. In the PPTP form, click the restart PPTP service button.
In most cases, the **User Name** value should be an asterisk, which means that any user name is accepted. The password should be the secret key used to authenticate the client participating in the PPP connection. By default, this is **cisco123**. Because the user is typically authenticated through the web login page prior to the establishment of the secure tunnel, you do not need to require unique login names/passwords for the encrypted connection.

- After changing the values in the form, click the **Update** button to save your changes.
- Allow the use of encryption by setting user role VPN policies to **Enforce** or **Optional** (under **User Management > User Roles**).
- In the IPSec form (**Figure 7-2**), set the **VPN Policy for Clean Access Server** to **Enforce** or **Optional**.

### Example Windows L2TP/IPSec Setup

1. From the Start menu on a Windows XP system, right-click My Network Places.
2. Select Properties.
3. In the left window click “Create a new connection.”
4. Click Next in the New Connection Wizard that appears.
5. In the Network Connection Type dialog, choose the second option “Connect to the network at my workplace” and click Next.
6. In the Network Connection dialog, choose Virtual Private Network connection and click Next.
7. In the Connection Name dialog, type a new name for the connection (e.g. test-l2tp) and click Next.
8. In the VPN Server Selection dialog, type the Host name or IP address for the untrusted site (eth1).
9. You can add a shortcut to your desktop or just click Finish.

**VPN Sign In**

1. From the Network Connections window, right-click the new Virtual Private Network connection you just made (test-l2tp), and select Properties.
2. Click the General Tab. Enter the IP address of the Untrusted Interface as the Host name or IP address of destination.
3. Click the Networking Tab.
4. Change the Type of VPN from Automatic to L2TP/IPSEC VPN.

5. Click the Security tab.
6. Click the IPSec Settings button.
7. Enter the user name and the default password “ciscokey” and click OK.

8. Click OK.