Cisco IOS SSL VPN Smart Tunnels Support

Smart Tunnels Support is a Secure Socket Layer (SSL) VPN feature used to instruct TCP-based client applications that use the winsock library to direct all traffic through the SSL tunnel established between a local relay process and the SSL VPN gateway. The SSL VPN is also known as WebVPN.

- Finding Feature Information, on page 1
- Prerequisites for Cisco IOS SSL VPN Smart Tunnels Support, on page 1
- Restrictions for Cisco IOS SSL VPN Smart Tunnels Support, on page 2
- Information About Cisco IOS SSL VPN Smart Tunnels Support, on page 2
- How to Configure Cisco IOS SSL VPN Smart Tunnels Support, on page 3
- Configuration Examples for Cisco IOS SSL VPN Smart Tunnels Support, on page 11
- Additional References, on page 12
- Feature Information for Cisco IOS SSL VPN Smart Tunnels Support, on page 13

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Cisco IOS SSL VPN Smart Tunnels Support

- The operating system of the host must be a 32-bit version of Microsoft Windows Vista or Windows XP or Windows 2000.
- The web browser must be enabled with ActiveX or Javascript.
- A headend gateway address must be added in the Trusted Site Zone for Microsoft Windows Vista users with smart tunnel or port forwarding.
- The Messaging Application Programming Interface (MAPI) protocol must be used for Microsoft Outlook Exchange communication and an AnyConnect VPN client for remote users.

- Administrative privileges are required to configure the Smart Tunnels Support feature on the router in thin-client access mode.

Restrictions for Cisco IOS SSL VPN Smart Tunnels Support

- Smart tunnels do not support split tunneling, Cisco Secure Desktop, private socket libraries, and MAPI proxy.
- Smart tunnels must not be started in two different web browsers simultaneously.
- Applications only with the winsock dll library such as Remote Desktop, VNCviewer, Outlook Express, Outlook Web Access (OWA), Secure Shell (SSH) using Putty, Telnet, FTP, and others are supported.

Information About Cisco IOS SSL VPN Smart Tunnels Support

SSL VPN Overview

Cisco IOS SSL VPN provides SSL VPN remote-access connectivity for any internet web browser that supports SSL encryption. The SSL VPN feature extends secure enterprise network access to any authorized user by providing remote-access connectivity to corporate resources from any location with internet service.

Cisco IOS SSL VPN also provides remote-access connectivity from noncorporate-owned machines such as home computers and internet kiosks.

SSL VPN delivers the following three modes of SSL VPN access:

- Clientless--Clientless mode provides secure access to private web resources and web content. This mode is useful for accessing content found in web browsers, databases, and online tools that employ a web interface.
- Thin-client (port-forwarding Java applet)--Thin-client mode extends the capability of the cryptographic functions of the web browser to enable remote access to TCP-based applications such as Post Office Protocol version 3 (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Telnet, and SSH.
- Full tunnel client--Full tunnel client mode offers extensive application support through its dynamically downloaded Cisco AnyConnect VPN Client (next-generation SSL VPN Client) for SSL VPN. Full tunnel client mode delivers a lightweight, centrally configured, and easy-to-support SSL VPN tunneling client that provides network layer access to any application virtually.

For more information about SSL VPN, see the *Cisco IOS SSL VPN Configuration Guide*.

SSL VPN Smart Tunnels Support Overview

A smart tunnel is a connection between a TCP-based application and a private site using a clientless (browser based) SSL VPN session, where the SSL VPN gateway works as a pathway and as a proxy server. The Smart Tunnels Support feature is based on the method of modifying an existing default behavior of a TCP-based application that accesses internal resources using SSL VPN.

Unlike port forwarding, a smart tunnel does not require a user connection to the local application and the local port. Instead, the SSL VPN Smart Tunnels Support package is delivered and deployed on the client using ActiveX and Java applets. When you launch the Smart Tunnels Support feature on the browser, the ActiveX or Java applet stored on the SSL VPN headend gateway is delivered to the client through HTTP. The client web browser launches the applet and installs the smart tunnel library. This process results in starting the smart tunnel session to relay application data.

If an application is configured with the Smart Tunnels Support feature, all new instances of the application are hooked and the traffic passes through the SSL VPN gateway. By default, the browser launching the smart tunnel is hooked automatically. The Smart Tunnels Support feature provides better performance than plug-ins.

How to Configure Cisco IOS SSL VPN Smart Tunnels Support

Configuring a Smart Tunnel List and Adding Applications

Configuring the smart tunnel list and adding the applications to the list on the router with administrative privileges creates a tunnel with the listed applications.

Before you begin

Before you can configure the SSL VPN Smart Tunnels Support feature, the virtual gateway must be configured and enabled. This gateway configuration specifies the IP address, port number, and trustpoint for the SSL VPN. Enabling the virtual gateway enables the SSL VPN service.

An SSL VPN virtual context must be configured to associate the virtual SSL VPN gateway with the configured features. For more information on SSL VPN gateway configuration and associating the context, see the *Cisco IOS SSL VPN Configuration Guid*e.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **smart-tunnel list** *name*
5. **appl** *display-name appl-name* **windows**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**webvpn context** *name* **Example:** `Router(config)# webvpn context sslgw`	Enters WebVPN context configuration mode to configure the SSL VPN context.
Step 4	**smart-tunnel list** *name* **Example:** `Router(config-webvpn-context)# smart-tunnel list st1`	Configures smart tunneling and enters WebVPN smart tunnel configuration mode to configure the applications for tunneling.
Step 5	**appl** *display-name appl-name* **windows** **Example:** `Router(config-webvpn-smart-tunnel)# appl ssh putty.exe windows`	Specifies the applications that are to be directed into the smart tunnel. • Multiple applications can be directed to the tunnel using this command.
Step 6	**end** **Example:** `Router(config-webvpn-smart-tunnel)# end`	Exits WebVPN smart tunnel configuration mode.

What to Do Next

An SSL VPN policy group configuration must be defined for the smart tunnel. Proceed to task in the Configuring a Group Policy for Smart Tunnels Support task.

Configuring a Group Policy for Smart Tunnels Support

The group policy configuration with administrative privileges on a router defines the group policy, associates the gateway, and enables the context to the smart tunnel list defined in the WebVPN context configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **smart-tunnel list** *name*
6. **exit**
7. **default-group-policy** *name*
8. **gateway** *name* [**domain** *name* | **virtual-host** *name*]
9. **inservice**

10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**webvpn context** *name* **Example:** `Router(config)# webvpn context sslgw`	Enters WebVPN context configuration mode to configure the SSL VPN context.
Step 4	**policy group** *name* **Example:** `Router(config-webvpn-context)# policy group new`	Enters WebVPN group policy configuration mode to configure a group policy.
Step 5	**smart-tunnel list** *name* **Example:** `Router(config-webvpn-group)# smart-tunnel list st1`	Configures a smart tunnel list for different applications in WebVPN group policy configuration mode.
Step 6	**exit** **Example:** `Router(config-webvpn-group)# exit`	Exits WebVPN group policy configuration mode.
Step 7	**default-group-policy** *name* **Example:** `Router(config-webvpn-context)# default-group-policy new`	Associates a group policy with a WebVPN context configuration. • This command is configured to attach a policy group to the WebVPN context when multiple group policies are defined under the context. • This policy will be used as default, unless an authentication, authorization, and accounting (AAA) server forces an attribute that specifically requests another group policy.
Step 8	**gateway** *name* [**domain** *name* | **virtual-host** *name*] **Example:**	Associates a WebVPN gateway with a WebVPN context.

	Command or Action	Purpose
	`Router(config-webvpn-context)# gateway sslgw`	• The gateway configured is associated with the WebVPN context in this configuration step.
Step 9	**inservice** **Example:** `Router(config-webvpn-context)# inservice`	Enables a WebVPN context configuration. • The context is put "in service" by entering this command. However, the context is not operational until it is associated with an enabled SSL VPN gateway.
Step 10	**end** **Example:** `Router(config-webvpn-context)# end`	Exits WebVPN context configuration mode.

Troubleshooting Tips

Use the **debug webvpn http** command to debug tunnels in Cisco IOS software.

What to Do Next

Configuring the Smart Tunnels Support on the router ends the configuration activity of an administrator. Once the client logs in to the SSL VPN enabled web browser after a router is configured with a smart tunnel, the user must enable smart tunneling by installing ActiveX or Java applet with settings. Proceed to the Enabling a Smart Tunnel with the Client Web Browser, on page 6 for more information.

Enabling a Smart Tunnel with the Client Web Browser

An SSL VPN enabled client web browser automatically launches the ActiveX or Java applet to install the smart tunnel. This process enables the smart tunnel session to relay data.

Before you begin

Smart tunnels support must be configured on the router before enabling it on the client's web browser.

SUMMARY STEPS

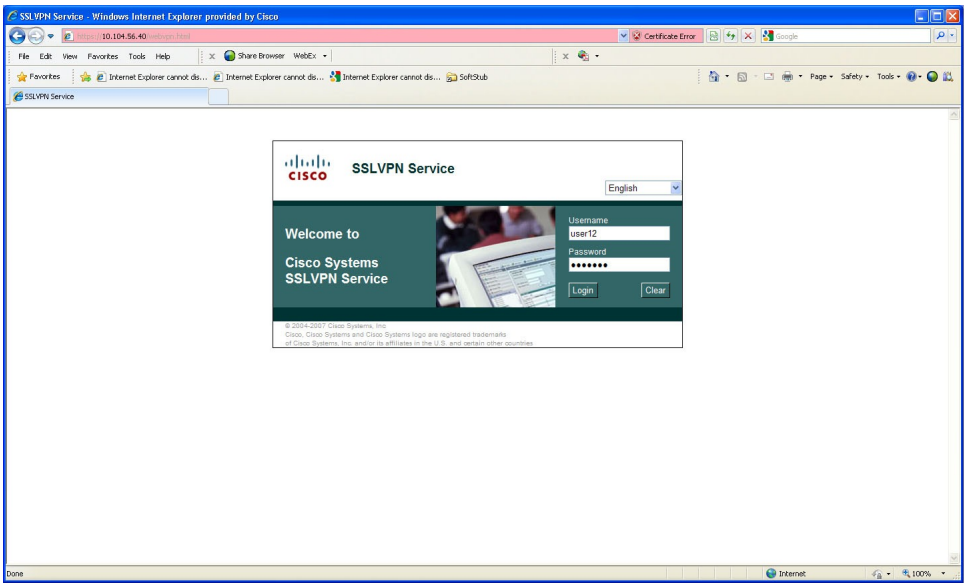
1. Log in to the application using the username and the password.
2. To enable smart tunneling, click the **Start** button present for the Smart Tunnel Application.
3. To proceed with the installation, click **Run**.
4. To proceed with the settings, click **Yes**.
5. To proceed with the settings, click **Run**.
6. To proceed with the settings, click **Run**.
7. To allow your data to pass through the specified IP address, click **Yes**.

DETAILED STEPS

Step 1 Log in to the application using the username and the password.

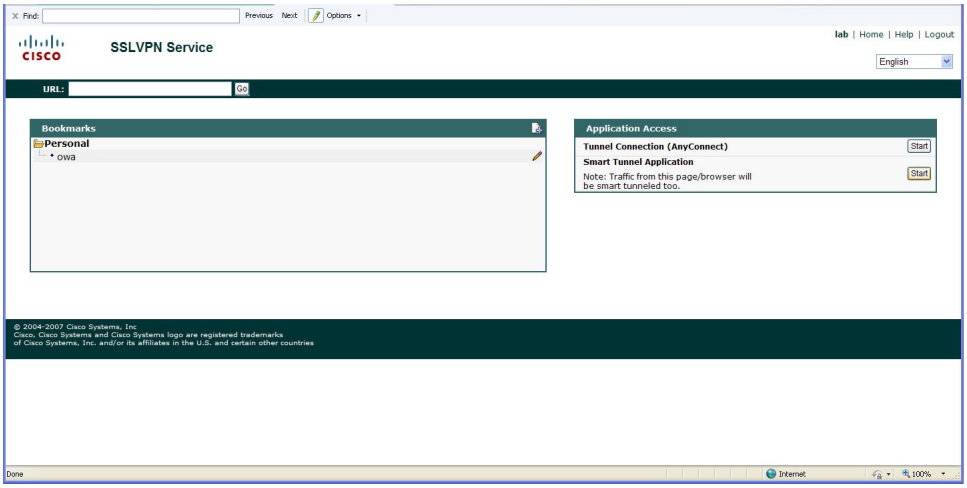
The figure below is an example of an SSL VPN Service login window.

Figure 1: Login Window



The figure below shows the SSL VPN Service main window displayed after logging in to the application.

Figure 2: SSL VPN Service Main Window



The Smart Tunnel Application is displayed in the Application Access area of the window.

Step 2 To enable smart tunneling, click the **Start** button present for the Smart Tunnel Application.

A security warning related to the ActiveX installation is displayed when the user clicks the Start button of the Smart Tunnel Application. The figure below shows the security warning dialog box.

Figure 3: ActiveX Security Warning

Step 3 To proceed with the installation, click **Run**.

A certificate verification warning is displayed after ActiveX is installed. The figure below shows the certificate verification warning dialog box.

Figure 4: Certificate Verification Warning

Step 4 To proceed with the settings, click **Yes**.

Note This certificate verification warning can be avoided if the administrator configures the appropriate certificate.

A hostname mismatch warning is displayed after the certificate verification error is overridden. The figure below shows the hostname mismatch warning dialog box.

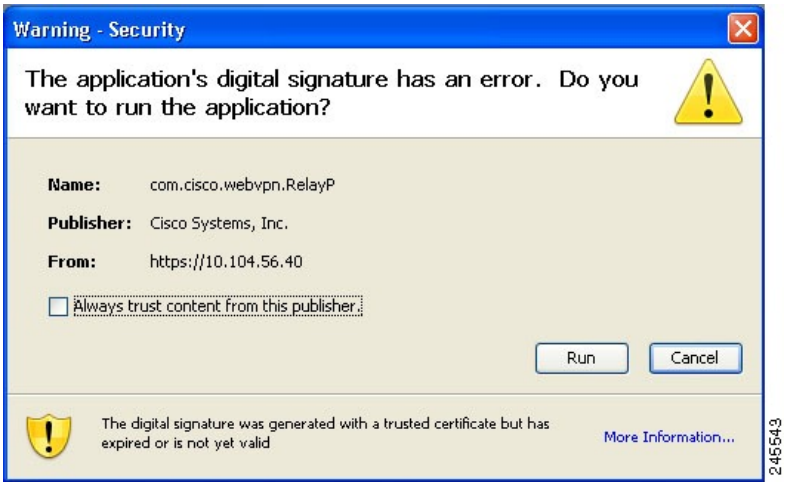
Figure 5: Hostname Mismatch Warning

Step 5 To proceed with the settings, click **Run**.

Note This hostname mismatch warning can be avoided if the administrator configures the appropriate hostname.

An application signature error warning is displayed after overriding the hostname mismatch warning. The figure below shows the digital signature warning dialog box.

Figure 6: Application Digital Signature Warning



Step 6 To proceed with the settings, click **Run**.

A data pass-through message is displayed after the digital signature error is overridden. The figure below shows the data pass-through dialog box.

Figure 7: Data Pass-through Message

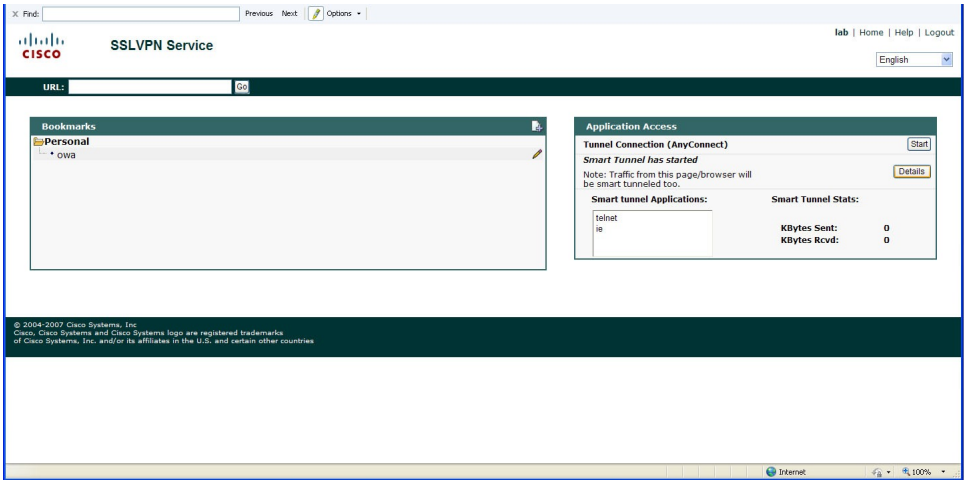
Step 7 To allow your data to pass through the specified IP address, click **Yes**.

ActiveX is installed and the Smart Tunnel application is displayed on the web browser.

Smart Tunnel Application Statistics Display

The statistics of the applications that are tunneled through the Smart Tunnel application are also displayed. The figure below shows a typical web browser with smart tunnel statistics.

Figure 8: Smart Tunnel Application Statistics



Note The statistics displayed for the Smart Tunnel application on the web browser and the statistics displayed on the router for the **show webvpn smart-tunnel stats** command are always different.

Always log out of the SSL VPN Smart Tunnel Support enabled browser after performing the required tasks to avoid problems in accessing the application in the future.

Troubleshooting Tips

To enable smart tunnel logging, navigate to the temp folder of the respective system user and execute the following files:

- rundll32.exe
- relay.dll
- SetDbgLogLevel *xy* (where *x* is 0 or 1, *y* specifies the log level within 1-6 range. The default value is 2).

Configuration Examples for Cisco IOS SSL VPN Smart Tunnels Support

Example Configuring a Smart Tunnel List and Adding Applications

The following example shows how to configure the Cisco IOS SSL VPN Smart Tunnels Support feature on a router:

```
enable
 configure terminal
  webvpn context sslgw
  smart-tunnel list st1
   appl ssh putty.exe windows
   appl ie iexplore.exe windows
   end
```

Example Configuring a Group Policy for Smart Tunnels Support

The following example shows how to configure the group policy for the Cisco IOS SSL VPN Smart Tunnels Support feature:

```
enable
 configure terminal
  webvpn context sslgw
  policy group new
   smart-tunnel list st1
   exit
  default-group-policy new
  gateway sslgw
  inservice
  end
```

Example Verifying the Smart Tunnel Configuration

The following is sample output from the **show webvpn policy**command that can be used to verify smart tunnel list configuration:

```
Router# show webvp policy group new context sslgw

WV: group policy = new ; context = sslgw
      idle timeout = 2100 sec
      session timeout = Disabled
      port forward name = "pflist"
      smart tunnel list name = "stlist"
      functions =
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keepalive interval = 30 sec
      SSLVPN Full Tunnel mtu size = 1406 bytes
      keep sslvpn client installed = disabled
      rekey interval = 3600 sec
```

```
      rekey method =
      lease duration = 43200 sec
```

The following sample output from the **show webvpn stats** command with the **smart-tunnel** and **context** keywords displays smart tunnel statistics:

```
Router# show webvpn stats smart-tunnel context name
WebVPN context name : manmeet
Smart tunnel statistics:
  Client                                Server
    proc pkts               : 0          proc pkts                : 0
    proc bytes              : 0          proc bytes               : 0
    cef pkts                  : 0          cef pkts                 : 0
    cef bytes               : 0          cef bytes                : 0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands	*Cisco IOS Security Command Reference*
SSL VPN feature guide	SSL VPN
SSL VPN Remote user guide	SSL VPN Remote User Guide
SSL VPN configuration guide	*Cisco IOS SSL VPN Configuration Guide*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco IOS SSL VPN Smart Tunnels Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Cisco IOS SSL VPN Smart Tunnels Support

Feature Name	Releases	Feature Information
Cisco IOS SSL VPN Smart Tunnels Support	15.1(3)T	Smart Tunnels Support is an SSL VPN related feature used to instruct TCP-based client applications to direct all traffic through the SSL tunnel established between a local relay process and the SSL VPN gateway. In Cisco IOS Release 15.1(3)T, this feature was introduced. The following commands were introduced or modified: **appl**(webvpn), **smart-tunnel list**.