Introduction

Clientless SSL VPN (WebVPN) allows a user to securely access resources on the corporate LAN from anywhere with an SSL–enabled Web browser. The user first authenticates with a WebVPN gateway which then allows the user access to pre–configured network resources. WebVPN gateways can be configured on Cisco IOS® routers, Cisco Adaptive Security Appliances (ASA), Cisco VPN 3000 Concentrators, and the Cisco WebVPN Services Module for the Catalyst 6500 and 7600 Routers.

Secure Socket Layer (SSL) Virtual Private Network (VPN) technology can be configured on Cisco devices in three main modes: Clientless SSL VPN (WebVPN), Thin–Client SSL VPN (Port Forwarding), and SSL VPN Client (SVC) mode. This document demonstrates the configuration of the WebVPN on Cisco IOS routers.

Refer to Thin–Client SSL VPN (WebVPN) IOS Configuration Example with SDM in order to learn more about the Thin–Client SSL VPN.

Refer to SSL VPN Client (SVC) on IOS with SDM Configuration Example in order to learn more about the SSL VPN Client.

SSL VPN runs on these Cisco Router platforms:

- Cisco 870, 1811, 1841, 2801, 2811, 2821 and 2851 series routers
- Cisco 3725, 3745, 3825, 3845, 7200 and 7301 series routers
Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- An advanced image of Cisco IOS Software Release 12.4(6)T or later
- One of the Cisco router platforms listed in the Introduction

Components Used

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

- Cisco 3825 router
- Advanced Enterprise software image – Cisco IOS Software Release 12.4(9)T
- Cisco Router and Security Device Manager (SDM) – version 2.3.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command. The IP addresses used in this example are taken from RFC 1918 addresses which are private and not legal to use on the Internet.

Network Diagram

This document uses this network setup:

![Network Diagram Image]

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Preconfiguration Tasks

Before you begin, complete these tasks:

1. Configure a host name and domain name.
2. Configure the router for SDM. Cisco ships some routers with a preinstalled copy of SDM.

If the Cisco SDM is not already loaded on your router, you can obtain a free copy of the software from Software Download (registered customers only). You must have a CCO account with a service contract. For detailed information on the installation and configuration of SDM, refer to Cisco Router and Security Device Manager.

3. Configure the correct date, time, and time zone for your router.

**Configure WebVPN on Cisco IOS**

You can have more than one WebVPN gateway associated with a device. Each WebVPN gateway is linked to only one IP address on the router. You can create more than one WebVPN context for a particular WebVPN gateway. To identify individual contexts, provide each context with a unique name. One policy group can be associated with only one WebVPN context. The policy group describes which resources are available in a particular WebVPN context.

Complete these steps in order to configure WebVPN on Cisco IOS:

1. Configure the WebVPN Gateway
2. Configure the Resources Allowed for the Policy Group
3. Configure the WebVPN Policy Group and Select the Resources
4. Configure the WebVPN Context
5. Configure the User Database and Authentication Method

**Step 1. Configure the WebVPN Gateway**

Complete these steps in order to configure the WebVPN Gateway:

1. Within the SDM application, click **Configure**, and then click **VPN**.
2. Expand **WebVPN**, and choose **WebVPN Gateways**.
3. Click **Add**.

The Add WebVPN Gateway dialog box appears.
4. Enter values in the Gateway Name and IP Address fields, and then check the Enable Gateway check box.
5. Check the Redirect HTTP Traffic check box, and then click OK.
6. Click Save, and then click Yes to accept the changes.

Step 2. Configure the Resources Allowed for the Policy Group

In order to make it easier to add resources to a policy group, you can configure the resources before you create the policy group.

Complete these steps in order to configure the resources allowed for the policy group:

1. Click Configure, and then click VPN.
2. Choose **WebVPN**, and then click the **Edit WebVPN** tab.

**Note:** WebVPN allows you to configure access for HTTP, HTTPS, Windows file browsing through the Common Internet File System (CIFS) protocol, and Citrix.
3. Click **Add**.

The Add WebVPN Context dialog box appears.
4. Expand **WebVPN Context**, and choose **URL Lists**.
5. Click **Add**.

The Add URL List dialog box appears.

6. Enter values in the URL List Name and Heading fields.
7. Click **Add**, and choose **Website**.
This list contains all the HTTP and HTTPS Web servers that you want to be available for this WebVPN connection.

8. In order to add access for Outlook Web Access (OWA), click Add, choose E-mail, and then click OK after you have filled in all the desired fields.

9. In order to allow Windows file browsing through CIFS, you can designate an NetBIOS Name Service (NBNS) server and configure the appropriate shares in the Windows domain in order.

   a. From the WebVPN Context list, choose NetBIOS Name Server Lists.

      b. Click Add.
c. Enter a name for the list, and click **Add**.

d. If applicable, check the **Make This the Master Server** check box.

e. Click **OK**, and then click **OK**.

**Step 3. Configure the WebVPN Policy Group and Select the Resources**

Complete these steps in order to configure the WebVPN policy group and select the resources:

1. Click **Configure**, and then click **VPN**.
2. Expand **WebVPN**, and choose **WebVPN Context**.
3. Choose **Group Policies**, and click **Add**.

The Add Group Policy dialog box appears.
4. Enter a name for the new policy, and check the **Make this the default group policy for context** check box.
5. Click the **Clientless** tab located at the top of the dialog box.
6. Check the **Select** check box for the desired URL List.

7. If your customers use Citrix clients that need access to Citrix servers, check the **Enable Citrix** check box.

8. Check the **Enable CIFS**, **Read**, and **Write** check boxes.

9. Click the **NBNS Server List** drop-down arrow, and choose the NBNS server list that you created for Windows file browsing in Step 2.

10. Click **OK**.

**Step 4. Configure the WebVPN Context**

In order to link the WebVPN gateway, group policy, and resources together, you must configure the WebVPN context. In order to configure the WebVPN context, complete these steps:

1. Choose **WebVPN Context**, and enter a name for the context.
2. Click the Associated Gateway drop-down arrow, and choose an associated gateway.
3. If you intend to create more than one context, enter a unique name in the Domain field to identify this context. If you leave the Domain field blank, users must access the WebVPN with https://IPAddress. If you enter a domain name (for example, Sales), users must connect with https://IPAddress/Sales.
4. Check the Enable Context check box.
5. In the Maximum Number of Users field, enter the maximum number of users allowed by the device license.
6. Click the Default Group policy drop-down arrow, and select the group policy to associate with this context.
7. Click OK, and then click OK.

Step 5. Configure the User Database and Authentication Method

You can configure Clientless SSL VPN (WebVPN) sessions to authenticate with Radius, the Cisco AAA Server, or a local database. This example uses a local database.

Complete these steps in order to configure the user database and authentication method:

1. Click Configuration, and then click Additional Tasks.
2. Expand Router Access, and choose User Accounts/View.
3. Click the **Add** button.

The Add an Account dialog box appears.
4. Enter a user account and a password.
5. Click OK, and then click OK.
6. Click Save, and then click Yes to accept the changes.

Results

The ASDM creates these command-line configurations:

```
ausnml−3825−01
Building configuration...
Current configuration : 4190 bytes
!
! Last configuration change at 17:22:23 UTC Wed Jul 26 2006 by ausnml
! NVRAM config last updated at 17:22:31 UTC Wed Jul 26 2006 by ausnml
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ausnml−3825−01
!
boot−start−marker
boot system flash c3825−adventerprisek9−mz.124−9.T.bin
boot−end−marker
```
no logging buffered
enable secret 5 $1$KbIu$5o8qKYAVpWvyv9YbrJLi/

aaa new-model

aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authorization exec default local

aaa session-id common

resource policy

ip cef

ip domain name cisco.com

voice-card 0
no dspfarm

!--- Self-Signed Certificate Information

crypto pki trustpoint ausnml-3825-01_Certificate
enrollment selfsigned
serial-number none
ip-address none
revocation-check crl
rsakeypair ausnml-3825-01_Certificate_RSAKey 1024

crypto pki certificate chain ausnml-3825-01_Certificate_RSAKey 1024

username admin privilege 15 secret 5 $1$j66N$2xNfhupbAinq3BQZMRzrW0
username ausnml privilege 15 password 7 a5D292421
username fallback privilege 15 password 7 6938CEA4 2E56CDFF CF4F2A01 BCD585C7 D6B01665 595C3413 6B7A7B6C
username austin privilege 15 secret 5 $1$2/SX$ep4fsCpodyeKaRji2mJkX/
username sales_user1 privilege 5 secret 5 $1$s2/SX$ep4fsCpodyeKaRji2mJkX/

interface GigabitEthernet0/0
ip address 192.168.0.37 255.255.255.0
duplex auto
speed auto
media-type rj45

Cisco – Clientless SSL VPN (WebVPN) on Cisco IOS Using SDM Configuration Example
interface GigabitEthernet0/1
 ip address 172.22.1.151 255.255.255.0
duplex auto
 speed auto
 media-type rj45
!
ip route 0.0.0.0 0.0.0.0 172.22.1.1
!
ip http server
 ip http authentication local
 ip http secure-server
 ip http timeout-policy idle 600 life 86400 requests 100
!
control-plane
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 40 0
 privilege level 15
 password 7 071A351A170A1600
 transport input telnet ssh
line vty 5 15
 exec-timeout 40 0
 password 7 001107505D580403
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
!--- The WebVPN Gateway

webvpn gateway WidgetSSLVPNGW1
 hostname ausnml-3825-01
 ip address 192.168.0.37 port 443
 http-redirect port 80
 ssl trustpoint ausnml-3825-01_Certificate
 inservice
!
webvpn context SalesContext
 ssl authenticate verify all
!

!--- Identify resources for the SSL VPN session

url-list "InternalWebServers"
 heading "WidgetWebServers"
 url-text "WidgetWeb" url-value "http://172.22.1.30"
 url-text "OWA" url-value "http://172.22.1.50/exchange"
!
 nbns-list NBNSServers
 nbns-server 172.22.1.30
!

!--- Identify the policy which controls the resources available

policy group policy_1
 url-list "InternalWebServers"
nbns-list "NBNSServers"
 functions file-access
 functions file-browse
 functions file-entry
Verify

Use this section to confirm that your configuration works properly.

Procedure

Complete these procedures in order to confirm your configuration works properly:

- Test your configuration with a user. Enter `https://WebVPN_Gateway_IP_Address` into an SSL–enabled Web browser; where `WebVPN_Gateway_IP_Address` is the IP address of the WebVPN service. After you accept the certificate and enter a user name and password, a screen similar to this image should appear.

- Check the SSL VPN session. Within the SDM application, click the Monitor button, and then click VPN Status. Expand WebVPN (All Contexts), expand the appropriate context, and choose Users.
- Check error messages. Within the SDM application, click the Monitor button, click Logging, and then click the Syslog tab.
- View the running configuration for the device. Within the SDM application, click the Configure button, and then click Additional Tasks. Expand Configuration Management, and choose Config Editor.

Commands

Several `show` commands are associated with WebVPN. You can execute these commands at the command–line interface (CLI) to show statistics and other information. For detailed information about `show` commands, refer to Verifying WebVPN Configuration.
Note: The Output Interpreter Tool (registered customers only) (OIT) supports certain show commands. Use the OIT to view an analysis of show command output.

Troubleshoot

Use this section to troubleshoot your configuration.

Note: Do not interrupt the Copy File to Server command or navigate to a different window while the copying is in progress. Interruption of the operation can cause an incomplete file to be saved on the server.

Note: Users can upload and download the new files using the WebVPN client, but the user is not allowed to overwrite the files in the Common Internet File System (CIFS) on WebVPN using the Copy File to Server command. The user receives this message when the user attempts to replace a file on the server:

Unable to add the file

Procedure

Complete these steps in order to troubleshoot your configuration:

1. Ensure clients disable pop-up blockers.
2. Ensure clients have cookies enabled.
3. Ensure clients use Netscape, Internet Explorer, Firefox, or Mozilla Web browsers.

Commands

Several debug commands are associated with WebVPN. Refer to Using WebVPN Debug Commands for detailed information about these commands.

Note: The use of debug commands can adversely impact your Cisco device. Before you use debug commands, refer to Important Information on Debug Commands.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

<table>
<thead>
<tr>
<th>NetPro Discussion Forums – Featured Conversations for VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Providers: VPN Service Architectures</td>
</tr>
<tr>
<td>Service Providers: Network Management</td>
</tr>
<tr>
<td>Virtual Private Networks: General</td>
</tr>
</tbody>
</table>

Related Information

- Cisco IOS SSLVPN
- Cisco IOS SSLVPN Q&A
- Thin−Client SSL VPN (WebVPN) IOS Configuration Example with SDM