Configuring SSL VPN on the Cisco ISA500 Security Appliance

This application note describes how to configure SSL VPN on the Cisco ISA500 security appliance. This document includes these topics:

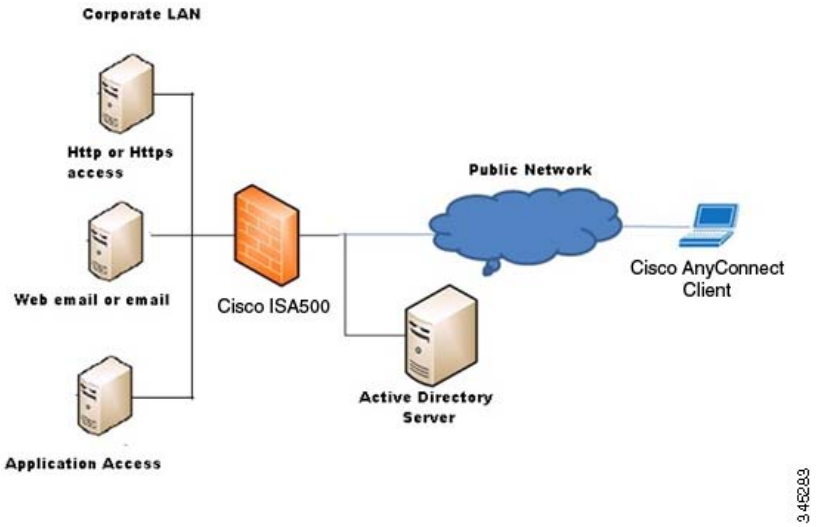
Overview

Secure Socket Layer (SSL) Virtual Private Network (VPN) technology allows a remote user to connect securely from anywhere on the Internet to an internal corporate network by using an SSL VPN client. In this document, the SSL VPN client used is the Cisco AnyConnect client.

With SSL VPN and the AnyConnect client, personal computers, Cisco SPA525G phones, and handheld devices (such as IPhone, iPad, and so forth) can connect to the SSL VPN gateway (ISA500) for remote access.

This document uses the network configuration described in Figure 1. As illustrated, the remote user connects to the ISA500 IP address with the AnyConnect client. After the user successfully authenticates to the ISA500, they can then use an encrypted secure session for full access to all permitted resources on the corporate network.

Figure 1 ISA500 Network Configuration with AnyConnect Client



Prerequisites

To securely access resources on a private network behind the ISA500, the remote user of the SSL VPN service must have the following:

- User account (login name and password) to access the ISA500 Configuration Utility
- Administrative access to the ISA500 (to initially install the AnyConnect client and to use the full tunnel client feature)
- AnyConnect VPN client (also referred to as the Cisco AnyConnect Secure Mobility client) installed on their workstations. To download the latest client, see: http://www.cisco.com/cisco/software/navigator.html?mdfid=281268793&i=rm.
- Operating system support for the AnyConnect client
  - Microsoft Windows 7, Windows 2000, Windows XP, or Windows Vista
  - Macintosh OS
  - Linux

NOTE You must configure the SSL VPN configuration and the SSL VPN group policies on the ISA500 before a remote user can access resources on the private network.

Configuring the ISA500 for SSL VPN

This section describes how to configure the ISA500 for SSL VPN by using the Remote Access VPN Wizard and how to connect it to the AnyConnect client.

SSL VPN uses tunneling to establish private connections through public networks such as the Internet. VPN supports two types of tunneling modes. Choose one of these modes to configure the ISA500:

- Configuring SSL VPN Full Tunnelling
- Configuring SSL VPN Split Tunneling

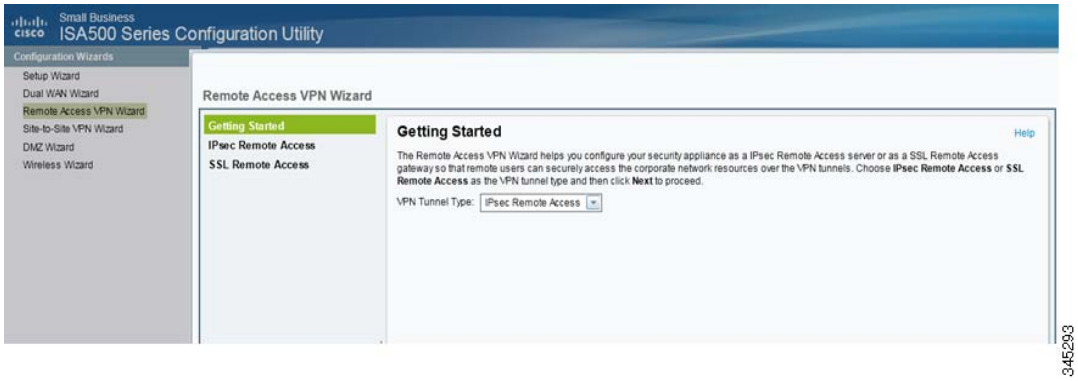
We recommend that you use the Remote Access VPN Wizard the first time that you configure SSL VPN. Afterwards, if you want to modify the SSL VPN configuration and group policies, you can configure them from the **VPN > SSL Remote User Access** pages.

Configuring SSL VPN Full Tunnelling

Full tunnel mode allows remote clients to access both corporate network resources and the Internet through the ISA500. In this mode, all network traffic is routed to the ISA500 through a secure tunnel.

To configure full tunnel mode, follow these steps:

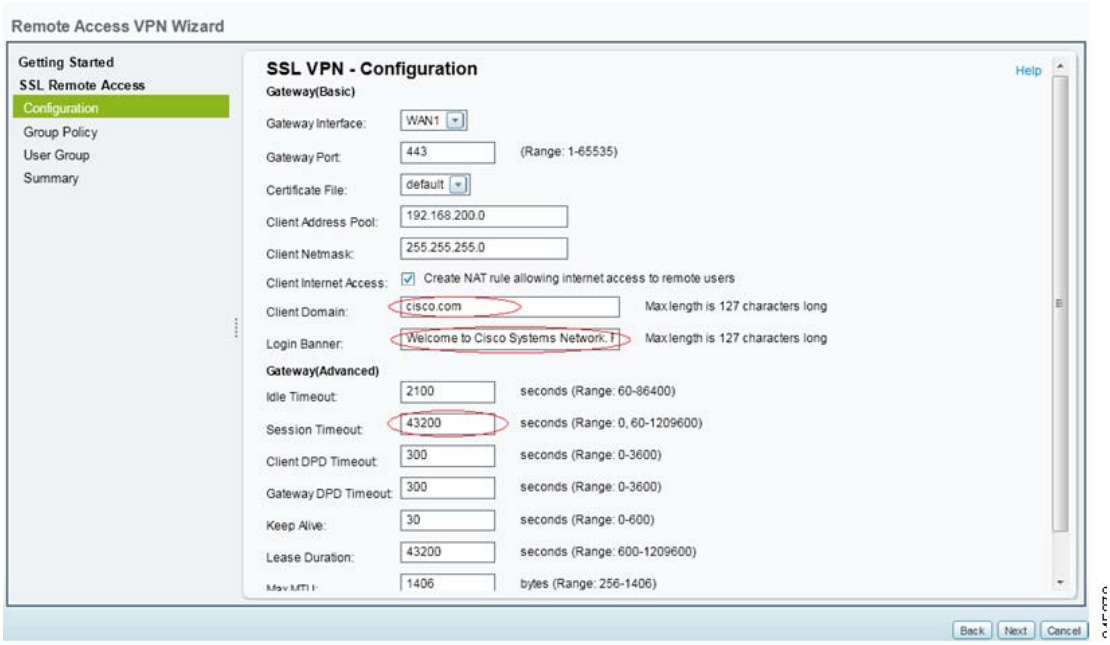
Step 1. From the ISA500 Configuration Utility, choose **Configuration Wizards > Remote Access VPN Wizard.**



Step 2. Choose **SSL Remote Access** from VPN Tunnel Type drop-down menu and click **Next**.

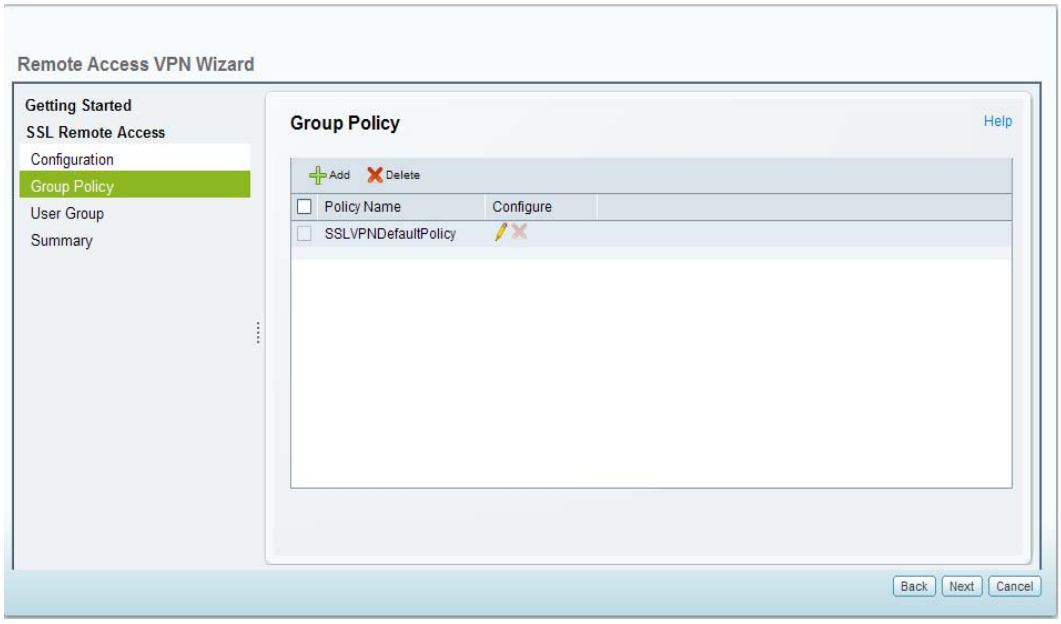
The SSL VPN Configuration window opens and displays the default SSL VPN settings. From this page you can enable or disable the SSL VPN service, and edit or customize the settings.

In this example, the **Client Domain**, **Login Banner,** and **Session Timeout** values were modified. The session timeout value (shown as 43200 seconds) is equivalent to 12 hours. For detailed descriptions of these fields, see Basic Configuration Settings, page 14.



Step 3. Click **Next** to continue to the Group Policy configuration page.

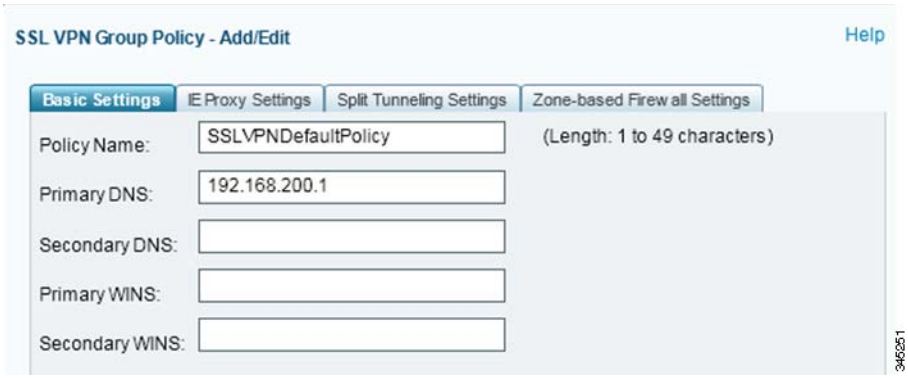
By default, the ISA500 uses the default policy **SSLVPNDefaultPolicy**. You can also create and customize your own policy by clicking **Add**.



Step 4. Click the pencil icon next to the default policy to open the Group Policy configuration settings.

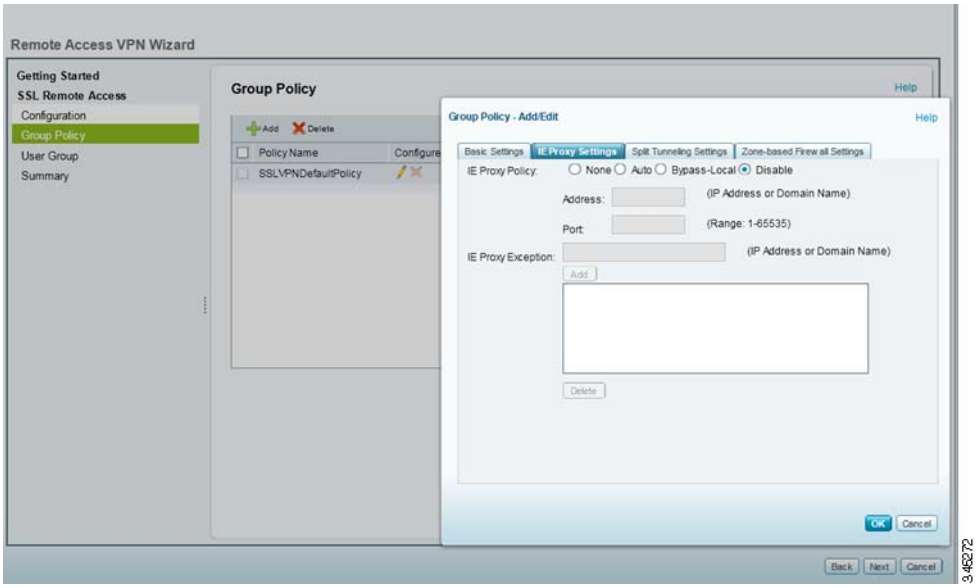
As shown here, the Primary DNS value is automatically populated with the default ISA500 IP address (this field is required). When the ISA500 IP address uses the Primary DNS, the remote clients sets this IP address as the DNS server address on its outgoing SSL VPN interface and sends any DNS queries to the ISA500. The ISA500 resolves these queries by using the DNS server IP address configured on the WAN settings.

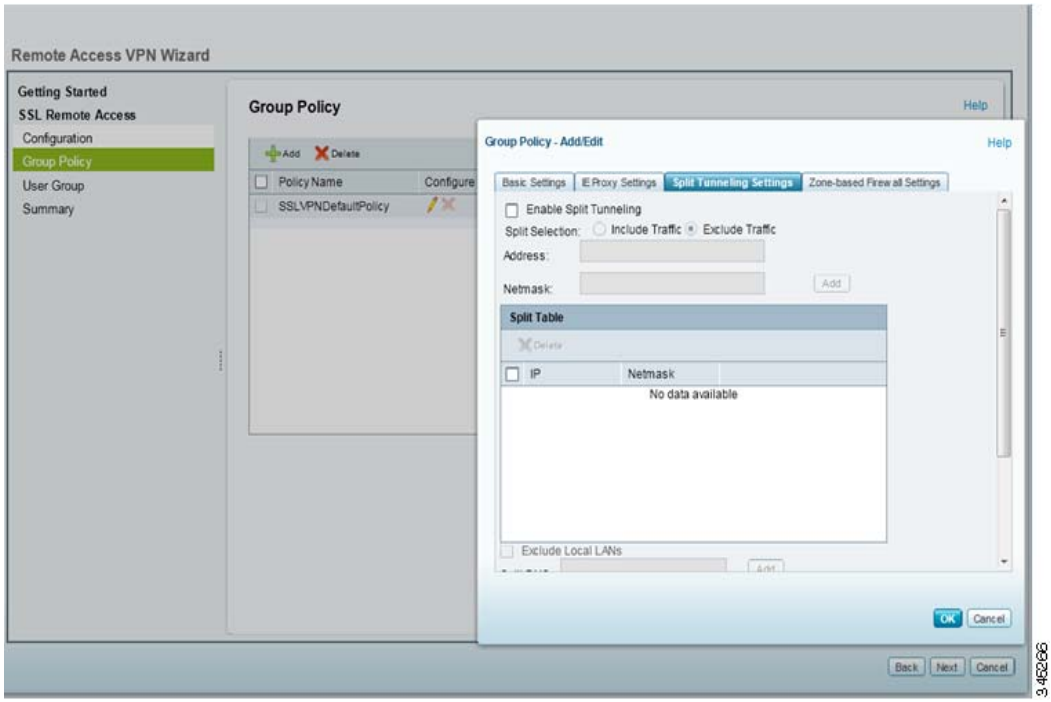
If desired, you can change the Primary DNS value to the DNS IP address of the corporate network. Optionally, you can configure a secondary DNS server and a primary and secondary WIN server.



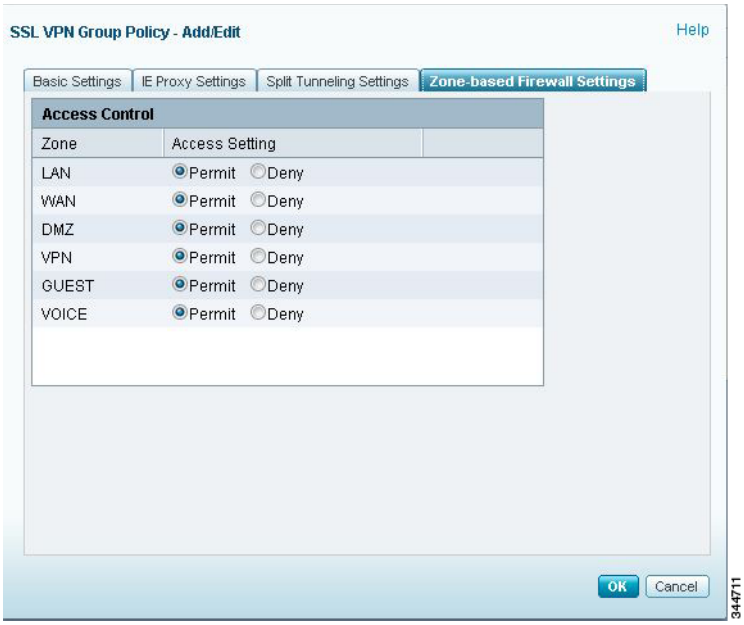
Step 5. Configure the IE Proxy, Split Tunneling, and Zone based Firewall settings.

In this example, the IE Proxy Policy and Split Tunneling settings are disabled. If desired, you can enable the proxy and specify several Internet Explorer (MSIE) proxies for the client's computers. When enabled, Internet Explorer on the client computer is automatically configured with these settings.





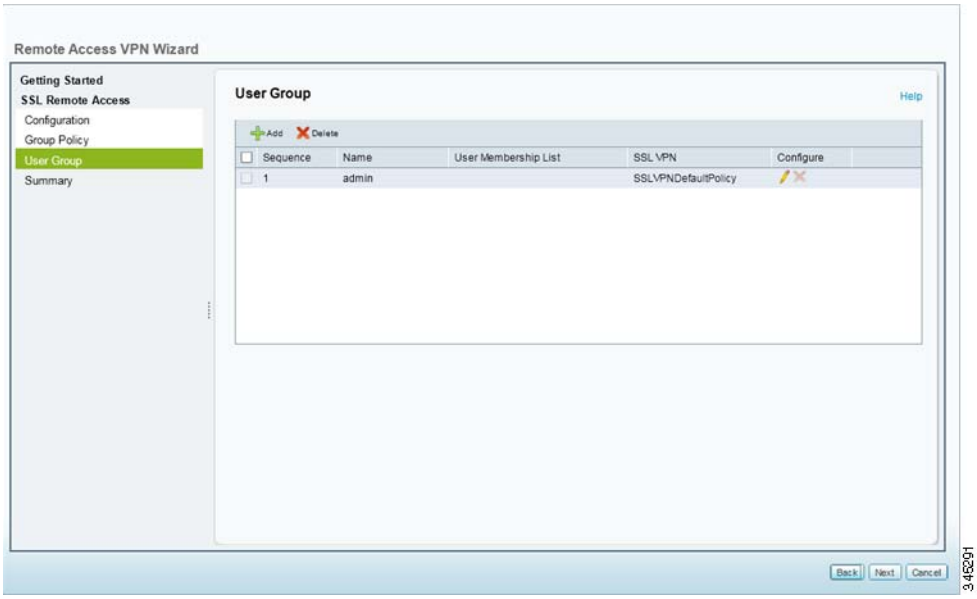
By default, the remote clients can access all resources on all ISA500 interfaces. However, if desired, you can control user access by permitting or denying access to a particular zone.

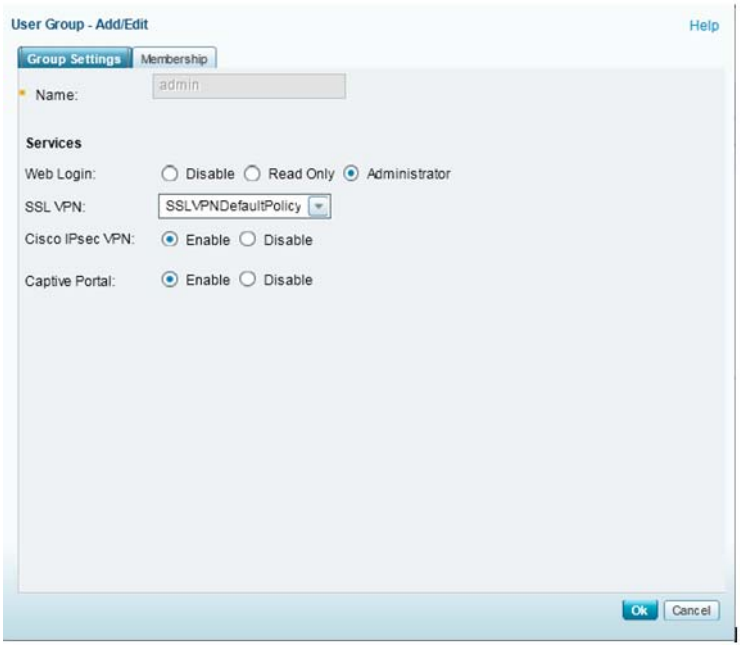


Step 6. Click **OK** when you are finished.

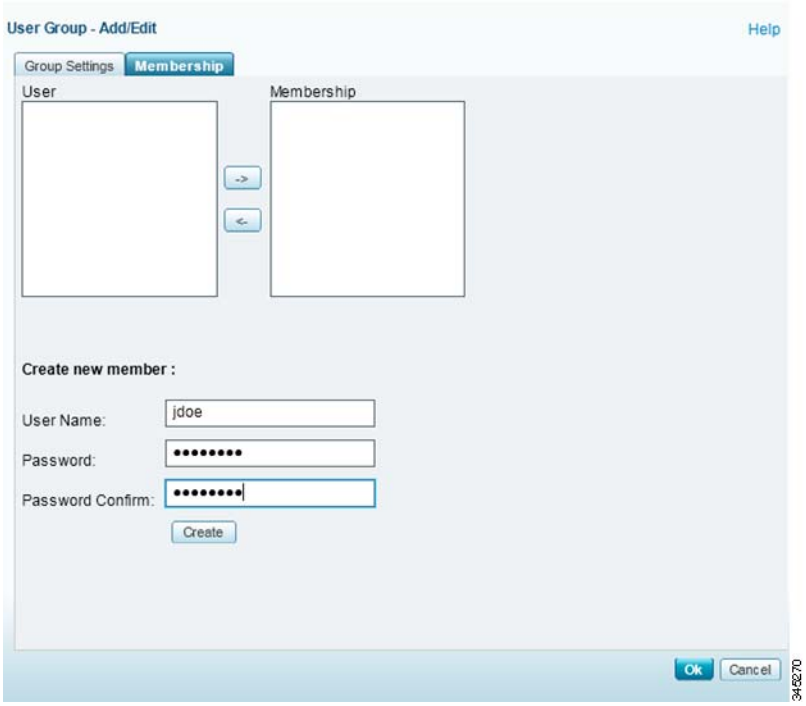
Step 7. From the Group Policy page, click **Next** to configure the users and user groups for the SSL VPN remote clients on the local database. In this example, we used the default user group **admin** and created user accounts under that group on the local database.

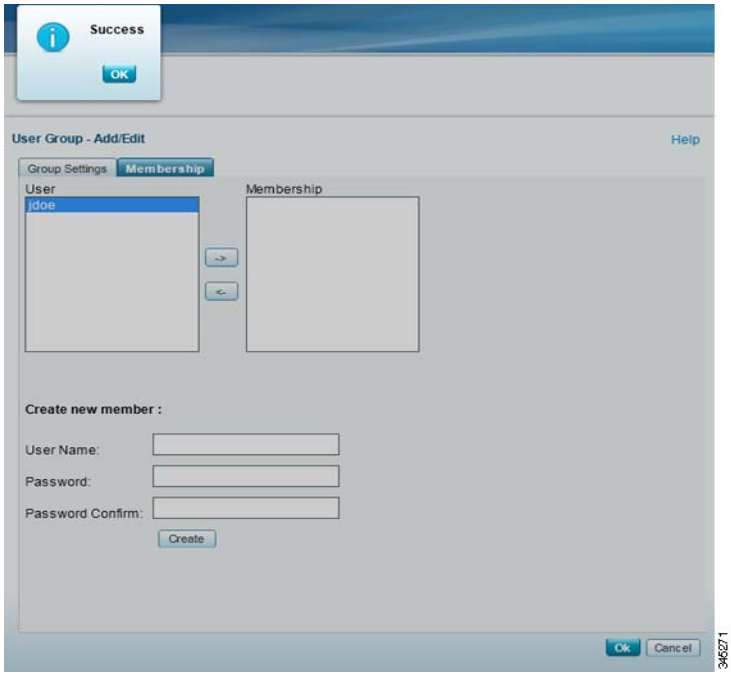
To add your own user groups, click **Add**. You can also configure user accounts on an Active Directory or RADIUS server. For more information see the “Configuring the ISA500 for Active Directory/LDAP and RADIUS Authentication” application note at: www.cisco.com/go/isa500resources.



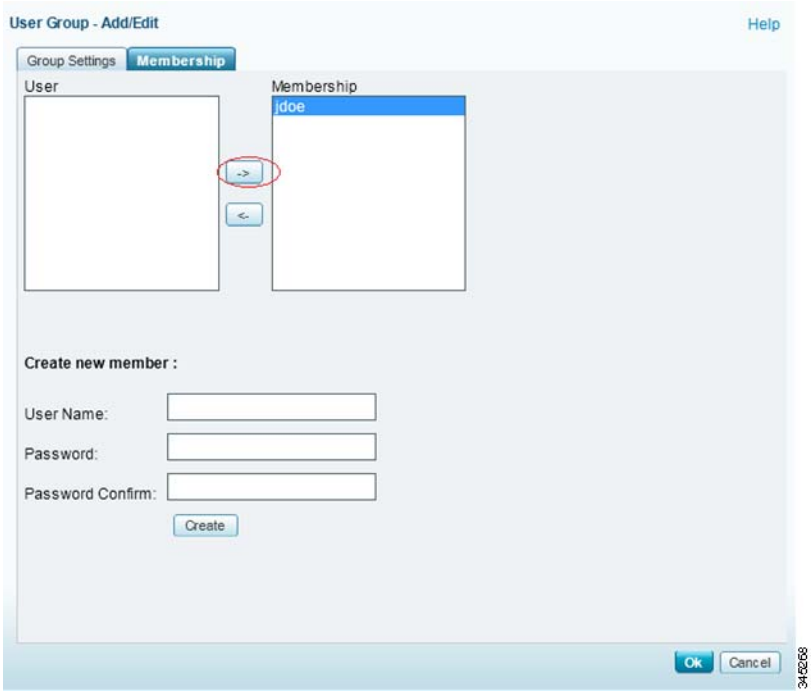


a. Click the **Membership** tab to create a new user account for the remote client. Enter the **User Name** and **Password** and then click **Create**. In this example, we created a user named **jdoe**.



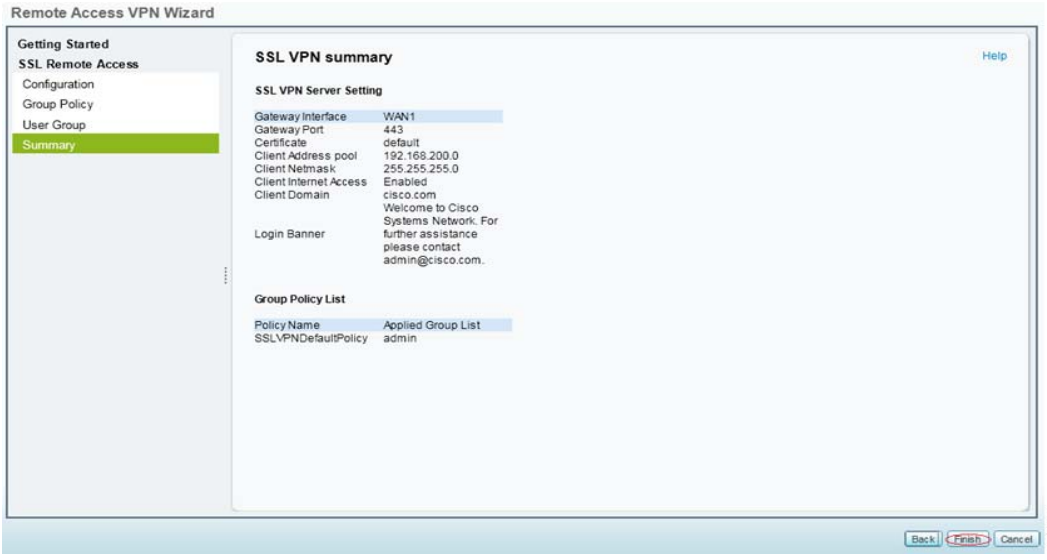


Step 8. Click the right arrow to add **jdoe** as a member to the user group **admin**.



Step 9. Create more user accounts as needed and then click **OK** to save your settings.

Step 10. Click **Next** to continue to the SSL VPN summary page. Verify that the information is correct and then click **Finish** to save the configuration.



Configuring SSL VPN Split Tunneling

SSL VPN split tunnelling allows specific traffic to be routed outside of the AnyConnect client tunnel. You can configure network traffic to be either included (resolved by the SSL VPN tunnel), or excluded (resolved through the ISP or the WAN connection).

To configure split tunneling mode, follow these steps:

Step 1. For steps 1 though 5, follow the same steps as those in Configuring SSL VPN Full Tunnelling, page 2. In this example the IE Proxy settings are left unchanged. For more about the proxy settings feature see page 6.

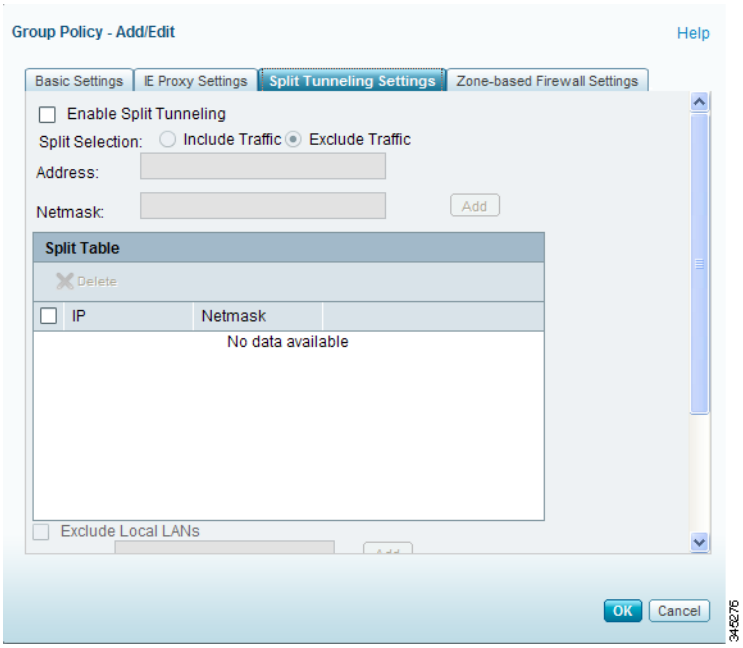
Step 2. Click the **Split Tunneling Settings** tab to configure the policy.

a. Check the box to enable Split Tunneling.

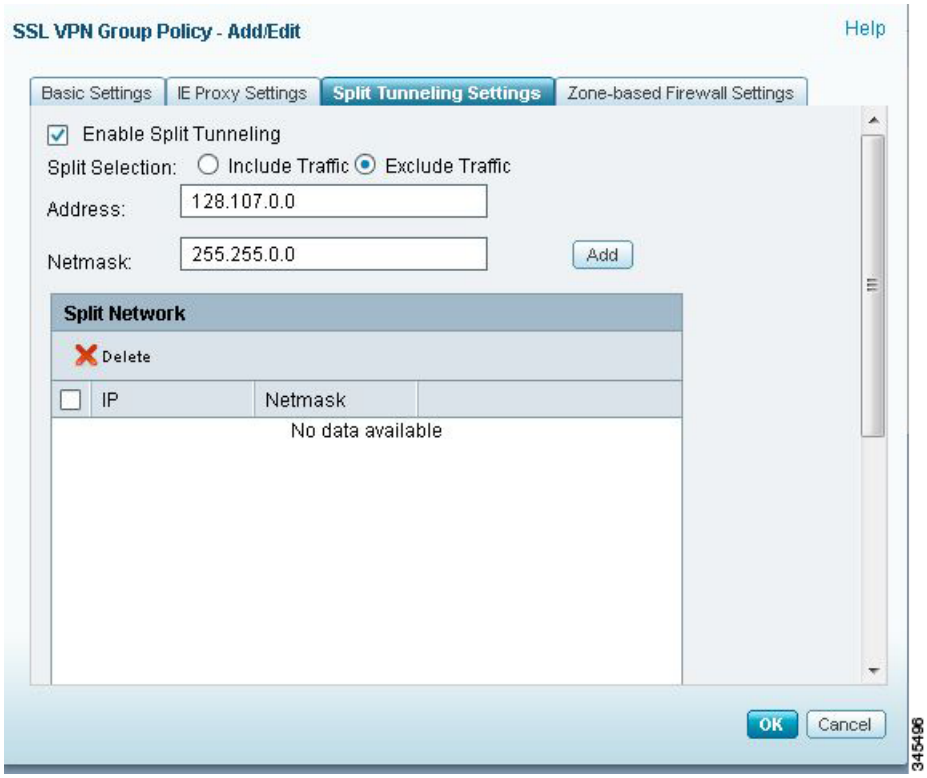
In this example, the **Exclude Traffic** option is enabled. With this option all network traffic on the remote client (except for those networks added to exclude traffic) is routed to the ISA500 and the excluded traffic is routed to the ISP.

If you select **Include Traffic**, all network traffic on the remote client (except for those networks added to include traffic) is routed to the ISP and the included traffic is routed to the ISA500.

NOTE You can select either the Include Traffic or Exclude Traffic option for the group policy but not both.



b. Enter the **Address** and **Netmask** for the traffic that you want to exclude when routing traffic to the ISA500 and then click **Add**.



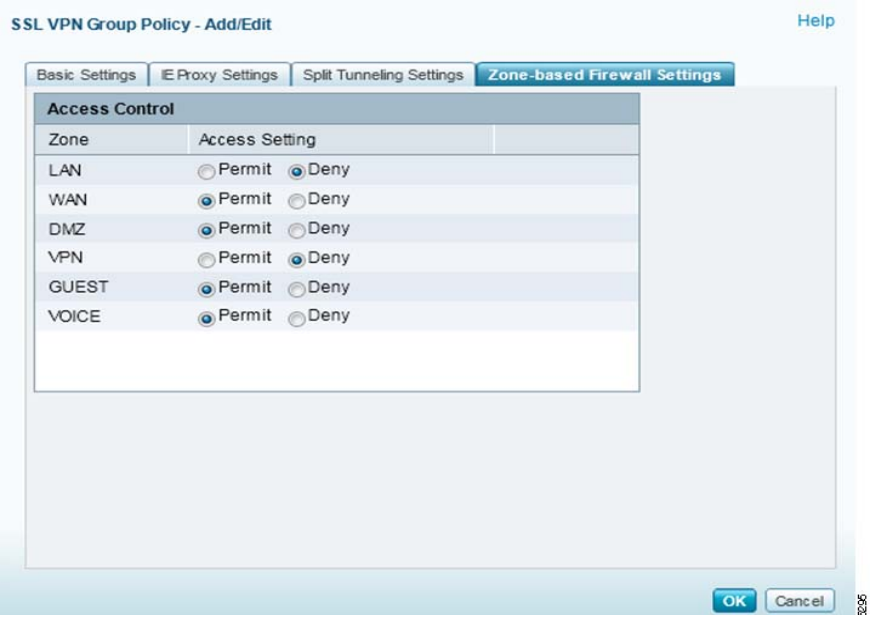
c. Check the **Exclude Local LANs** box to exclude the remote clients local LAN from traffic that is resolved by ISA500. When enabled, traffic routed to the hosts on the same LAN as the remote client is routed directly to the hosts (instead of sent to the ISA500 to route back on same secure tunnel).

d. Enter the **DNS server IP address** in the Split DNS field and click **Add**. The DNS server resolves domain names when traffic is sent to the excluded networks.

Step 3. Click **OK** to save your settings.

Step 4. Click the **Zone-based Firewall Settings** tab.

By default, the remote clients can access resources on all of the ISA500 interfaces. You can control this access by changing the Access Setting for a particular zone to Permit or Deny. In this example, the firewall is configured to deny LAN and VPN access to the remote client.



Step 5. Click **OK** when you are finished.

Step 6. Configure the user accounts for the SSL VPN remote clients on the local database. Follow the same steps as those for configuring full tunnel mode on page 7.

Basic Configuration Settings

This section describes the basic settings required for an SSL VPN Configuration. You can configure these settings from the Remote Access VPN Wizard or from the **VPN > SSL Remote User Access > SSL VPN Configuration** page.

- **Gateway Interface**: The WAN port through which SSL VPN connection requests are sent to the ISA500. By default, WAN1 (mandatory) is the only available interface and is the only option that appears in the Gateway Interface drop-down menu.
  - For a WAN load balancing configuration, choose either WAN1 or WAN2 depending on your network.
  - For a WAN failover configuration, always choose the primary WAN (WAN1) as the gateway interface.

    NOTE If a failover occurs, the SSL VPN service restarts and uses the standby WAN as the gateway interface.
- **Gateway Port**: By default, SSL VPN operates on port number 443. If desired, you can change the port number to a user-defined value. When configuring the port, the SSL VPN client must enter the entire address pair as *Gateway IP Address:Gateway Port Number* to connect to the ISA500.

  In this example, the AnyConnect client uses the default SSL VPN port and the ISA500 IP address 220.0.0.1.

  In this example, the ISA500 IP address 220.0.0.1 is the same as before, but the SSL VPN port was changed to 10000.

- **Certificate file**: File used to authenticate remote users who try to access the corporate network through the SSL VPN tunnels. You can choose either the default certificate file or import one of your choice.
- **Client Address Pool**: Private network address from which the host IP address is assigned to the remote access client. The IP address range must not overlap with other IP addresses on the local network.
- **Client Netmask**: Netmask address for the network address chosen for the client's address pool. Valid netmask addresses are 255.255.255.0, 255.255.255.128 and 255.255.255.192.

  The following table shows the network address range for different network addresses. This example assumes that the maximum number of clients connected to the ISA500 is 50.

Network IP Address	Netmask	Beginning Host Address	Ending Host Address	SSL VPN Gateway IP Address
10.10.10.0	255.255.255.0	10.10.10.2	10.10.10.51	10.10.10.1
172.16.10.0	255.255.255.128	172.16.10.130	172.16.10.179	172.16.10.129
192.168.10.0	255.255.255.192	192.168.10.194	192.168.10.243	192.168.10.193

- **Client Internet Access**: Automatically creates advanced NAT rules to allow SSL VPN clients to access the Internet over the SSL VPN tunnels. This option is enabled by default.
- **Client Domain**: Changes the default text to the domain name of choice given to the SSL VPN address space.
- **Login Banner**: Text entered in the login banner field that appears after a remote user authenticates to the SSL VPN server. You can change the default banner text to whatever you want. For example: Welcome to *xyz* company. For assistance contact admin@xyz.com.

Connecting the AnyConnect Client to the ISA500

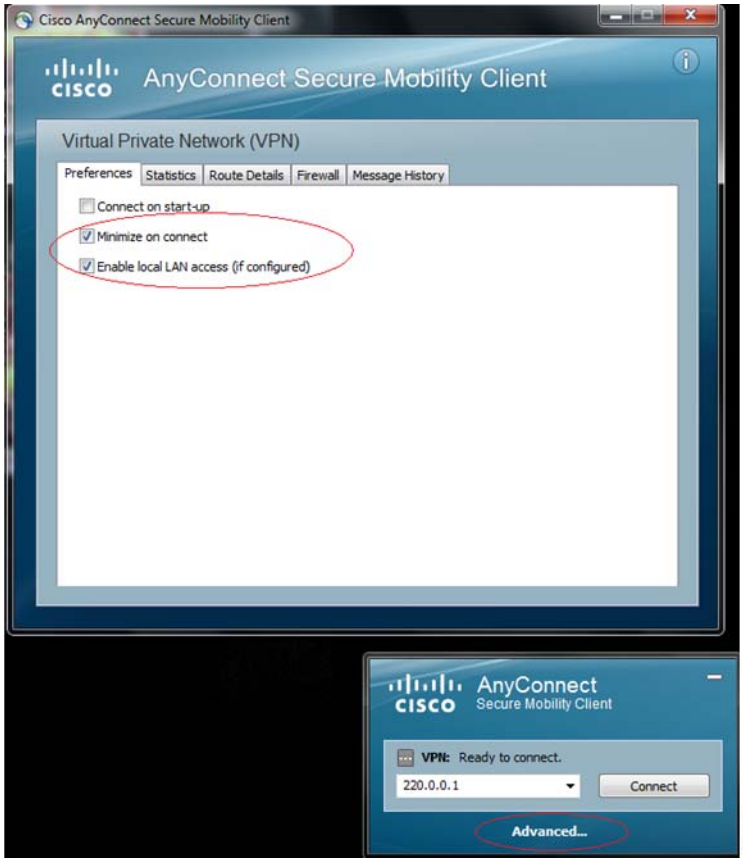
After you configure the ISA500 for SSL VPN, you can set up the connection to the AnyConnect client. This client establishes the SSL VPN tunnels and provides users with a secure VPN connection to the ISA500.

Make sure that the user has already installed the AnyConnect client installed on their workstations. To download the latest client, see: http://www.cisco.com/cisco/software/navigator.html?mdfid=281268793&i=rm.

Follow these steps to connect the client to the ISA500. In this example, we used the Cisco AnyConnect Secure Mobility Client v3.0.2052 on a Windows 7 computer.

Step 1. Launch the AnyConnect client.

Step 2. From the AnyConnect Secure Mobility Client window, click the **Advanced** link.



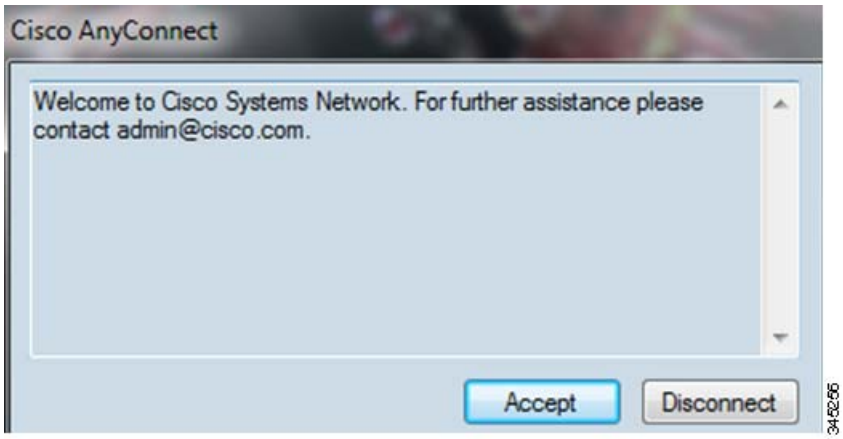
Step 3. Under Preferences, check the **Enable local LAN access** box. You must select this option if you enabled it in the Split Tunneling settings as described on page 11. If this option is disabled, the local LAN to which the remote client belongs will not be excluded from routing packets to the ISA500.

Step 4. Choose the ISA500 WAN address in the AnyConnect dialog box and click **Connect**.

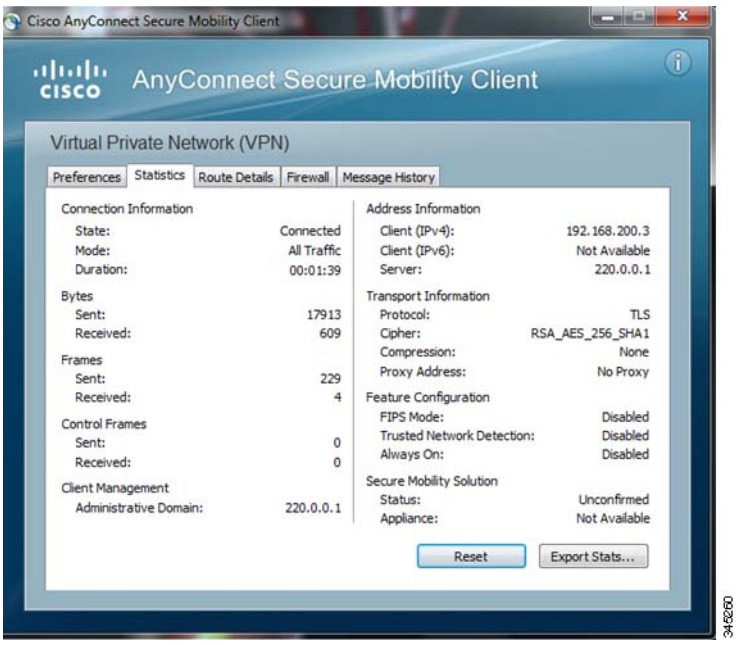
Step 5. Enter the remote client's **Username** and **Password** and click **OK**.

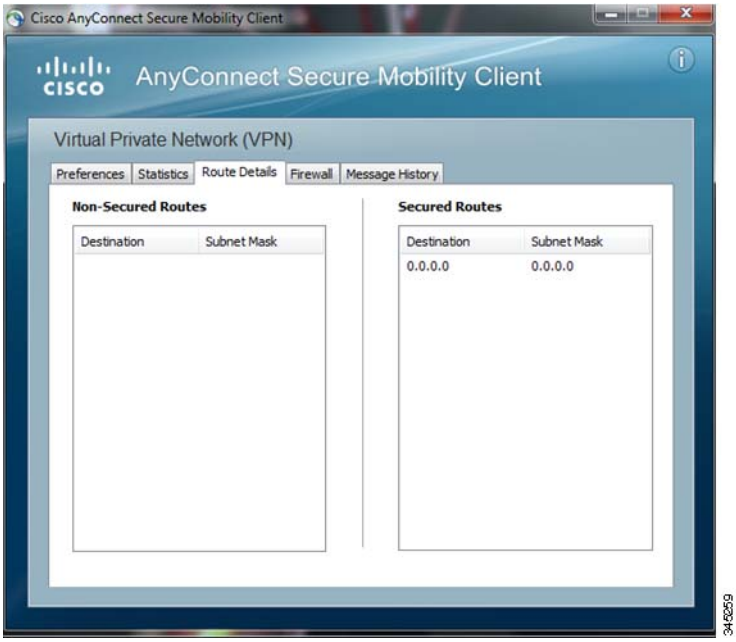
The banner text message appears and prompts the remote user to **Accept** the connection. The SSL VPN connection is then established.

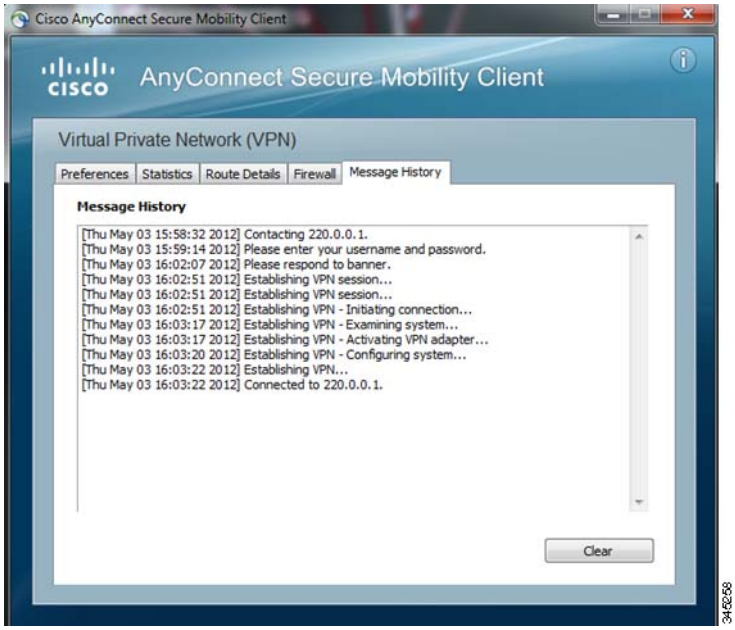
NOTE If you receive an error message or if the connection fails, see Troubleshooting, page 26 for more information.



You can view the connection status and other details about the VPN from the AnyConnect VPN status pages. These pages show the status, routing, and client connection information for the VPN.



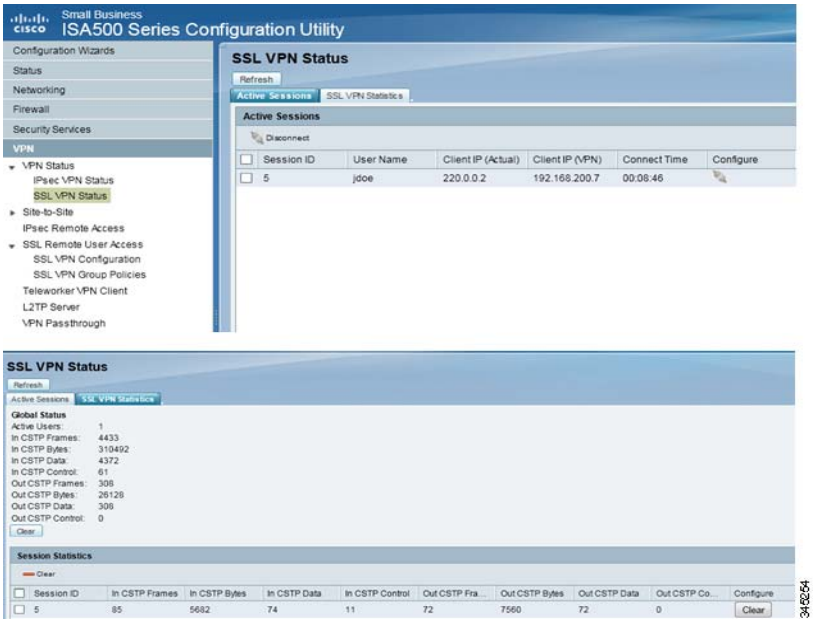




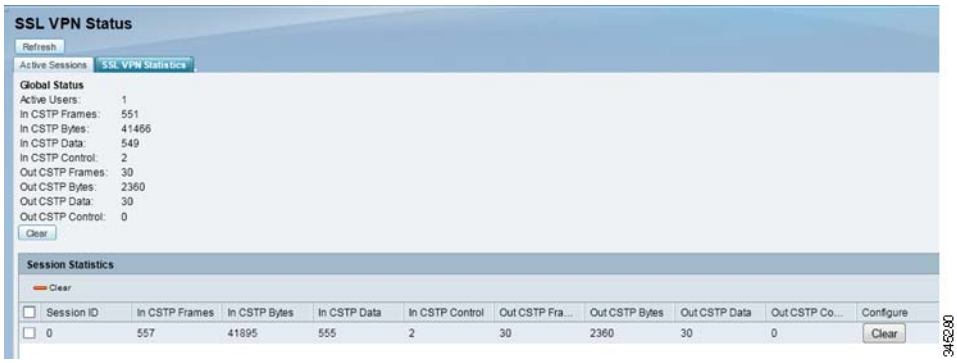
Verifying the SSL VPN Connection

You can use the ISA500 SSL VPN Status page to view the information for all active VPN sessions. This page is automatically updated every 10 seconds.

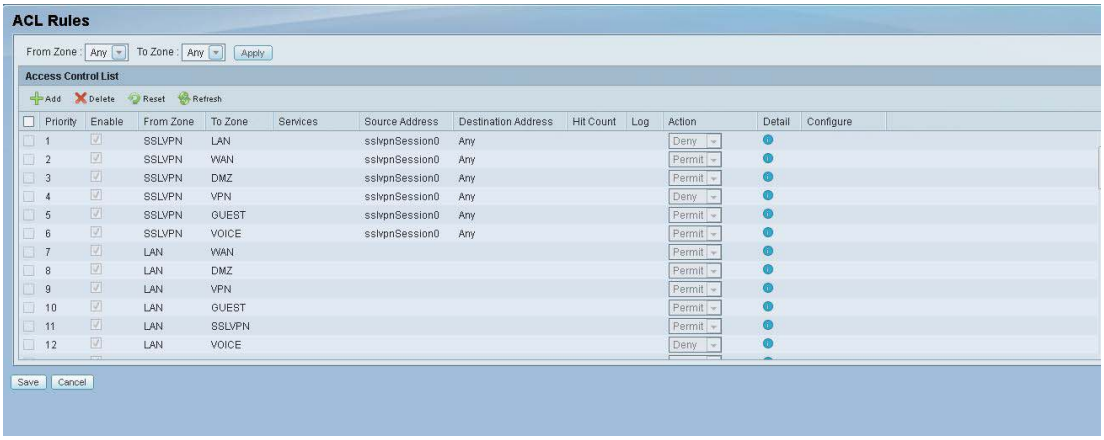
Step 1. To verify the SSL VPN connection, choose **VPN > SSL VPN Status.**



Step 2. Click the **SSL VPN Statistics** tab to view the traffic statistics.



After the SSL VPN session is established, a dynamic access control list (ACL) is added to the ISA500 firewall based on the Zone-based Firewall settings that you configured on page 12.



Configuring Advanced Settings

This section provides information on using the advanced features on the ISA500. It includes the following:

- Advanced Configuration Settings
- Configuring the Cisco SPA525G with the ISA500
- Configuring Content Filtering Policies

Advanced Configuration Settings

These are the advanced (optional) configuration settings that are available for SSL VPN. You can configure these settings from the **Remote Access VPN Wizard** or from the **VPN > SSL Remote User Access > SSL VPN Configuration** page.

- **Idle Timeout**: Timeout value in seconds that the SSL VPN session remains idle after the ISA500 terminated the session. The default value is 2100 seconds.
- **Session Timeout**: Timeout value in seconds that a SSL VPN session can remain active. Set this value to a larger value to avoid terminating the session. The default value is 0 seconds, which keeps the SSL VPN session always active.
- **Client DPD Timeout**: Dead Peer Detection (DPD) allows detection and termination of inactive SSL VPN sessions. This timeout is configured on the remote client during the SSL VPN tunnel set up. If the session is nonresponsive for the period of the timeout value, the remote client will terminate the session. The default value is 300 seconds.
- **Gateway DPD Timeout**: If the SSL VPN session is unresponsive more than twice the amount of the DPD timeout value, the ISA500 will terminate the session. The default value is 300 seconds.
- **Keep Alive**: Timeout set on the remote client. A timeout interval periodically sends the Keep Alive packets to the ISA500 to indicate that it is active. The default value is 30 seconds.
- **Lease Duration**: Amount of time after which the SSL VPN client must send an IP address lease renewal request to the server. The default value is 43200 seconds.
- **Max MTU**: Maximum transmission unit for the session. The default value is 1406 bytes.
- **Rekey Interval**: Time interval for which the remote client negotiates with the ISA500 to rekey the session key. The default value is 3600 seconds

Configuring the Cisco SPA525G with the ISA500

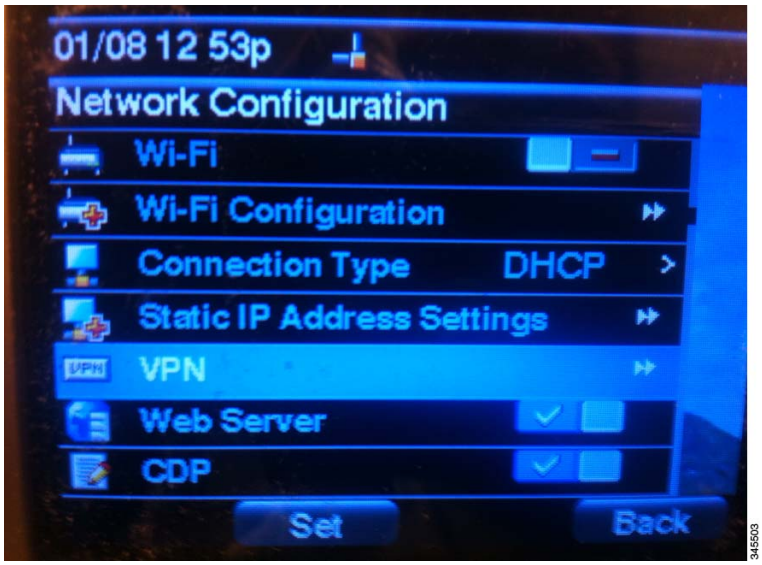
You can create a secure VPN connection between the ISA500 and the Cisco SPA525G phone. The SPA525G has an embedded SSL VPN client that can be used to establish SSL VPN connections to the ISA500.

Step 1. Log on to the SPA525G configuration utility.

Step 2. Click the **Information and Settings** button.

Step 3. Choose number 3 **Network Configuration**.

Step 4. Click the **VPN** option.



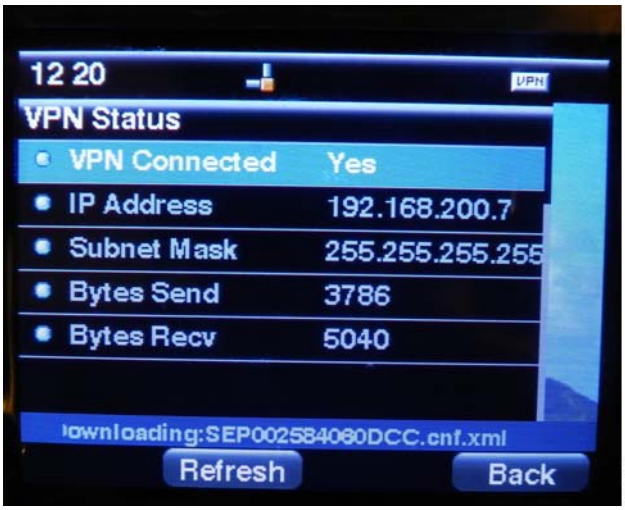
Step 5. Enter the **VPN Server**, **User Name,** and **Password** under VPN Settings. Leave the Tunnel Group field blank.

Step 6. Check the **Connect on Bootup** box to establish a VPN connection every time that the phone boots up.

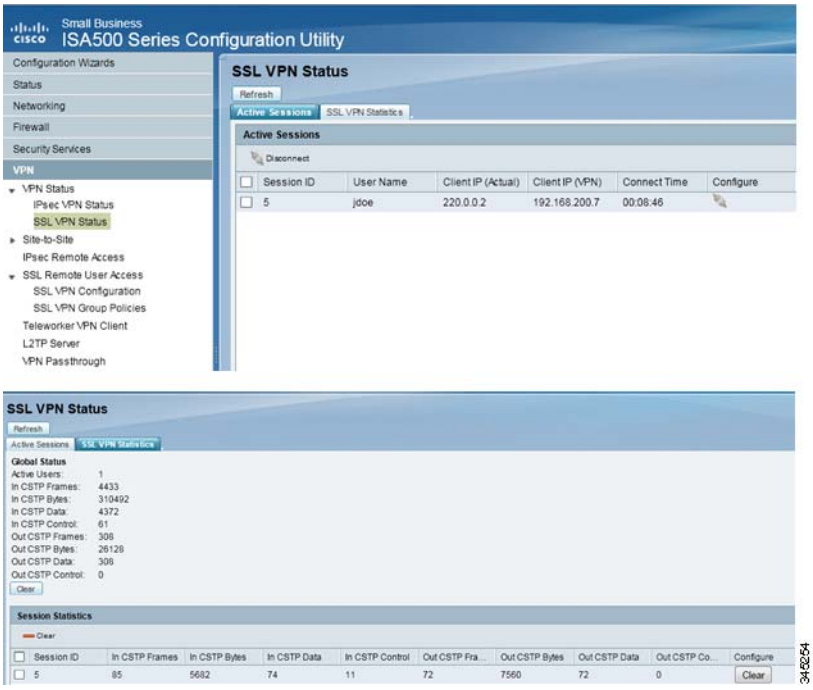
Step 7. Click **Set** to save your settings.

Step 8. Check the **Enable Connection** box to establish the SSL VPN connection.

The VPN connection is successful.



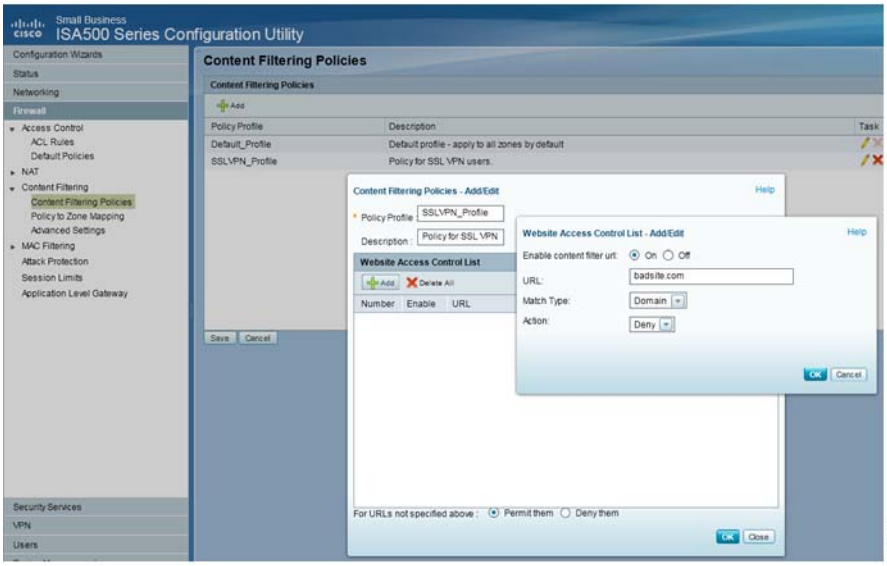
You can also verity the connection from the ISA500 Configuration Utility by choosing **VPN > VPN Status > SSL VPN Status**. This example shows that the SSL VPN session is now active.



Configuring Content Filtering Policies

You can configure content filtering policies on the ISA500 to specify which websites to block or allow on your network.

Step 1. Choose **Firewall > Content Filtering > Content Filtering Policies**.



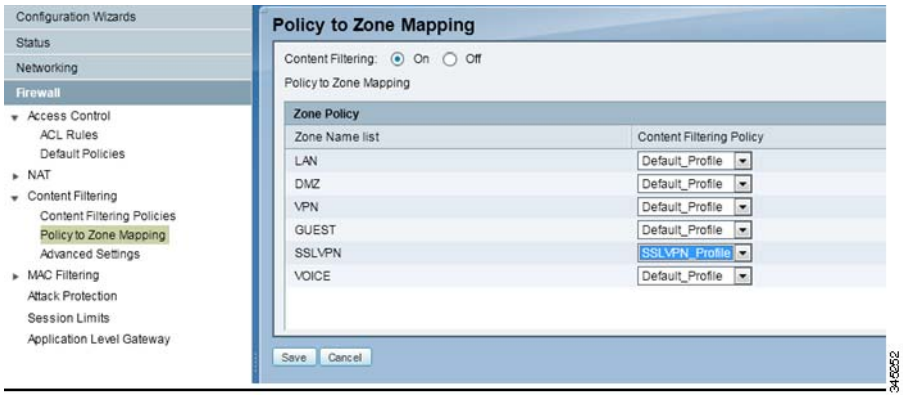
Step 2. Click **Add** to create a new policy profile.

Step 3. In the Content Filtering Policies page, click **Add**

Step 4. Under the Website Access Control List, specify the website URLs that you want to allow or block.

Step 5. Click **OK** to save the new profile.

Step 6. To map the content filtering policy profile to the SSL VPN zone, choose **Content Filtering > Policy to Zone Mapping**. Choose the content filtering policy for the SSL VPN zone and click **Save**.



Troubleshooting

The following is a list of problems that might occur when AnyConnect client fails to connect to the ISA500:

- WAN Connection is Down
- Remote Client Cannot Reach the ISA500 WAN Interface
- Wrong Username and Password Combination
- Active Directory or RADIUS Server is Unresponsive
- Accessibility Issues

NOTE If logging is enabled on the ISA500, you can use the information in the syslogs for troubleshooting purposes. See Troubleshooting Using Log Files, page 28.

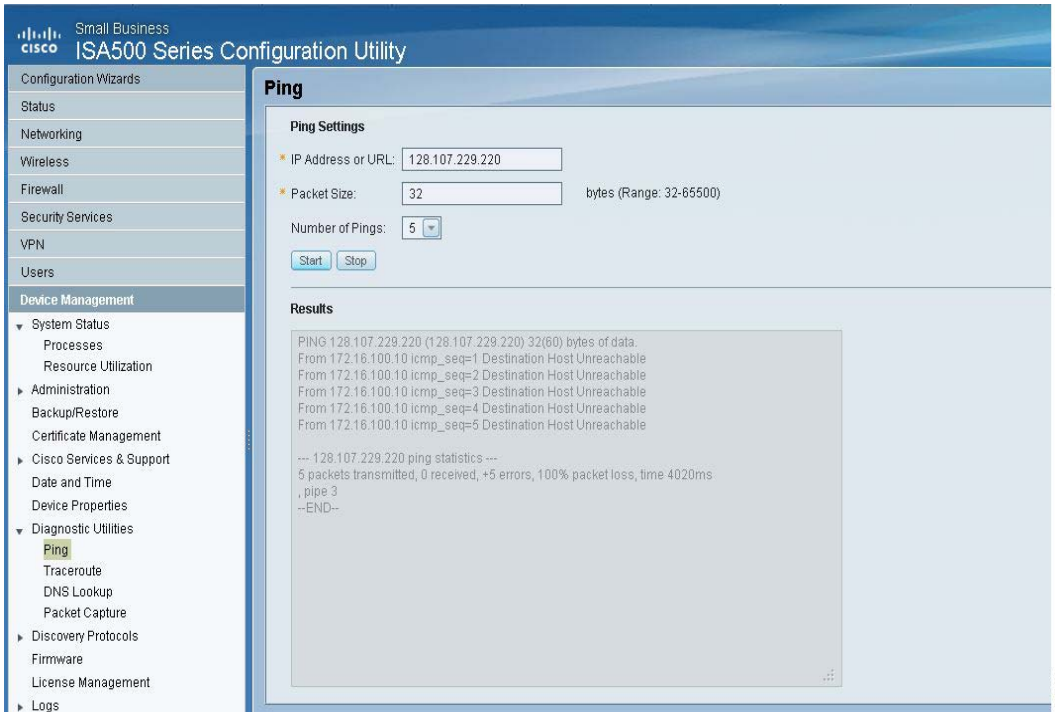
WAN Connection is Down

Verify that your ISA500 is securely connected, or contact your Internet Service Provider (ISP) to resolve the issue.

Remote Client Cannot Reach the ISA500 WAN Interface

Step 1. Uncheck the **Block Ping WAN Interface** option from the **Firewall > MAC Filtering > Attack Protection**. This option is typically used to prevent attackers from discovering your network through ICMP Echo (ping) requests.

Step 2. Use the Diagnostic Utilities (**Device Management >Diagnostic Utilities > Ping**) to check the network connectivity between the remote client and the ISA500. Enter the client's **IP Address** and **Number of Pings** and click **Start**. The results appear in the pane below.



Wrong Username and Password Combination

Check the local database, Active Directory server, or RADIUS server to retrieve or update the username and password.

Active Directory or RADIUS Server is Unresponsive

Check the connectivity between the Active Directory or RADIUS server and the ISA500. Check the logs for more information. See Troubleshooting Using Log Files, page 28.

SSL VPN Session Terminated Due to Idle Timeout or Session Timeout

Increase the idle timeout and session timeout values from the **VPN > Remote User Access > SSL VPN Configuration** page.

Accessibility Issues

These problems might happen if the remote client is unable to reach the resources on ISA500 LAN after the SSL VPN connection is established.

Resources on the ISA500 LAN Not Accessible

Check the connectivity of the hosts on the ISA500 LAN by using the Ping option form the **Device Management >Diagnostic Utilities > Ping** page.

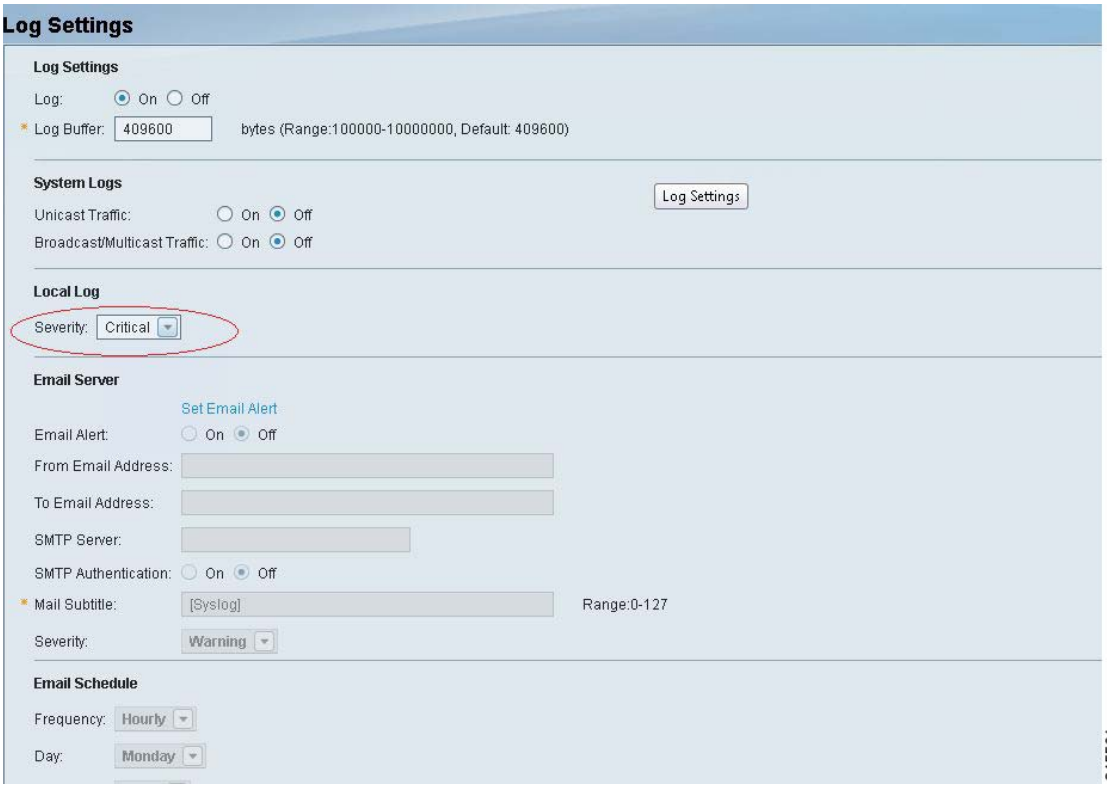
Wrong DNS is Configured

Make sure that the ISA500 IP address is configured as the primary DNS in the Basic Settings tab under **VPN > SSL Remote User Access > SSL VPN Group Policies**. Otherwise, resolve any DNS server issues with the DNS IP address configured on the WAN settings.

Troubleshooting Using Log Files

You can turn on specific VPN logs for more details if problems occur when establishing a VPN connection.

Step 1. To enable logging, choose **Device Management > Logs > Log Settings** and then click **On** to enable the Log feature.

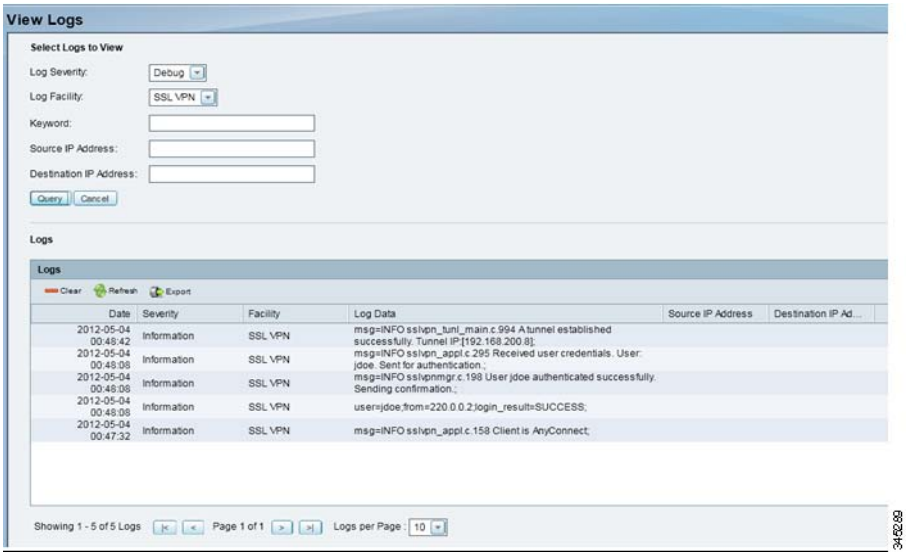


Step 2. Choose the **Severity** level for the events that you want to log and click **Save**. For example: If you select Critical, all logs listed under the Critical, Emergency, and Alert categories are saved to the local syslog.

Step 3. Choose **Log Facilities** and verify that the SSL VPN option is enabled under Local Log. If the syslog server is configured, click the **Remote Log** box.

Step 4. Click **Save** to apply your settings.

Step 5. From the View Logs page, choose **Debug** and **SSL VPN** from the drop-down menus and click **Query**. The log output appears in the Logs table which can then be used for troubleshooting purposes.



For More Information

Product Resources	Location
Product Documentation	www.cisco.com/go/isa500resources
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Firmware Downloads	www.cisco.com/go/isa500software
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb