Remote Access VPN Wizard on ISA500 Series Integrated Security Appliance

Objective

The Remote Access VPN wizard allows an administrator to configure the ISA500 Series Integrated Security Appliance as either an Internet Protocol Security (IPsec) Remote Access server or as a Secure Sockets Layer (SSL) Remote Access gateway. These two security methods encrypt data for Virtual Private Network (VPN) connections. The Remote Access VPN wizard compiles the main settings for these methods into one convenient location in the ISA500 Series Configuration Utility. This article explains how to configure the Remote Access VPN Wizard on the ISA500 Series Integrated Security Appliances.

Applicable Devices

• ISA500 Series Integrated Security Appliances

Software Version

• v1.1.14

Remote Access VPN Wizard Settings

ISA500 Series Integrated Security Appliance supports both Internet Protocol Security (IPsec) Remote Access server and Secure Sockets Layer (SSL). Choose the appropriate method as per scenario:

• IP Sec VPN — IPsec is a protocol suite that operates at the Internet Layer of the Internet Protocol Suite (TCP/IP) and authenticates and encrypts IP packets sent and received through a VPN connection. IPsec offers more security features than SSL. Use IPsec for a VPN connection if a few clients need VPN access and security is strongly needed.

• SSL VPN — SSL encrypts data at Application Layer and uses the same at the Transport Layer of the Internet Protocol Suite (TCP/IP). SSL is quicker to configure than IPsec but lacks some of the security features that are in IPsec. Use SSL if many VPN clients need to access a VPN connection, with the use of web browser without any special client software.

Configure with IPsec Remote Access

This procedure explains how to configure settings for IPsec Remote Access in the Remote Access VPN Wizard.

Step 1. Log in to the ISA500 Series Configuration Wizard, and choose Configuration Wizards > Remote Access VPN Wizard. The Getting Started page opens:
The *Getting Started* page allows you to choose which type of VPN tunnel to use.

Step 2. From the VPN Tunnel Type drop-down list, choose **IPsec Remote Access**.

Step 3. Click **Next**. The *IPsec Group Policy* page appears:

![IPsec Group Policy](image)

The *IPsec Group Policy* page allows you to configure group policy settings such as the name and IKE authentication method.

Step 4. In the Group Name field, enter a name to identify the IPsec group policy.

Step 5. In the IKE Authentication Method field, click a radio button.

- Pre-shared Key — This option requires VPN clients to authenticate themselves with a pre-shared key.

- Certificate — This option requires VPN clients to authenticate themselves with digital certificates.
Step 6. (Optional) If you chose Pre-shared Key in Step 5, enter the pre-shared key to use to authenticate clients in the Pre-shared Key field.

Step 7. (Optional) If you chose Certificate in Step 5, choose a local certificate to use to authenticate clients. The local certificate for the ISA500 Series Integrated Security Appliance should be the peer certificate on the client host.

Step 8. (Optional) If you chose Certificate in Step 5, choose a peer certificate to use to authenticate clients. The peer certificate for the ISA500 Series Integrated Security Appliance should be the local certificate on the client host.

Step 9. Click Next. The WAN page appears:

The WAN page allows you to turn on and off WAN failover and select the WAN interface through which the VPN tunnel occurs.

Step 10. In the WAN Failover field, click a radio button.

- On — This option redirects the VPN traffic to a secondary WAN interface if the primary WAN interface fails.
- Off — This option does not redirect the VPN traffic to a secondary WAN interface if the primary WAN interface fails.

Step 11. From the WAN Interface drop-down list, choose a WAN interface to use to send and receive VPN traffic.

Step 12. Click Next. The Network page appears:
The *Network* page allows you to configure settings for how the VPN clients are assigned IP addresses.

**Step 13.** In the Network field, click a radio button.

- **Client** — This option assigns VPN clients IP addresses that are not part of the VPN server network IP address space. Remote VPN clients have access to the VPN server network, but hosts that are directly connected to the server network cannot access the VPN clients. For this option, enter the first IP address of the client IP address range in the Start IP field, and enter the last IP address of the client range in the End IP field.

- **NEM** — Network Extension Mode (NEM) assigns VPN clients IP addresses from the IP address range of the VPN server network through the use of DHCP. These client addresses are completely routable to the server network, and hosts that are directly connected to the server network can access the VPN clients.

**Step 14.** (Optional) If you chose Client in Step 13, enter the first address of the client IP address range in the Start IP field.

**Step 15.** (Optional) If you chose Client in Step 13, enter the last address of the client IP address range in the End IP field.

**Step 16.** Check the **Create NAT rule to allow internet access to remote users** to allow remote users to access the Internet through the Internet connection of the ISA500 Series Integrated Security Appliance.

**Step 17.** Click **Next**. The *Access Control* page appears:
The Access Control page allows you to permit and deny access to VPN clients for specific zones.

Step 18. For each zone, click a radio button.

- Permit — This option grants remote users access to the zone.
- Deny — This option denies remote users access to the zone.

Step 19. Click Next. The DNS/WINS page appears:

The DNS/WINS page allows you to configure addresses for the DNS and WINS servers used by the VPN tunnel.

Step 20. In the Primary DNS Server field, enter the IP address of the primary Domain Name System (DNS) server. A DNS server translates domain names to static IP addresses to be used by computer networks. DNS works independent of operating systems.

Step 21. In the Secondary DNS Server field, enter the IP address of the secondary DNS server.
Step 22. In the Primary WINS Server field, enter the IP address of the primary Windows Internet Name Service (WINS) server. A WINS server translates domain names to dynamic IP addresses to be used by computer networks. WINS primarily only works on Microsoft clients and Microsoft networks.

Step 23. In the Secondary WINS Server field, enter the IP address of the secondary Windows Internet Name Service (WINS) server.

Step 24. In the Default Domain field, enter the domain name that the VPN clients use.

Step 25. Click **Next**. The **Backup Server** page appears:

The **Backup Server** page allows you to configure addresses for backup servers who will take over the VPN tunnel in the event that the main server fails.

Step 26. In the Backup Server 1 field, enter the domain name or IP address of the primary backup server through which the VPN clients connect to the network when the regular VPN server fails.

Step 27. In the Backup Server 2 field, enter the domain name or IP address of the secondary backup server through which the VPN clients connect to the network when the regular VPN server and the primary backup server fail.

Step 28. In the Backup Server 3 field, enter the domain name or IP address of the tertiary backup server through which the VPN clients connect to the network when the regular VPN server, the primary backup server, and the secondary backup server fail.

Step 29. Click **Next**. The **Split Tunnel** page appears:
The Split Tunnel page allows you to configure settings for Split Tunneling and Split DNS for the VPN tunnel.

Step 30. In the Split Tunnel field, click a radio button.

- On — This option enable split tunneling and split DNS. Split Tunneling allows a VPN client to access the VPN server network but still use the Internet connection of the VPN client to access the Internet. This setup creates less traffic on the VPN server network but allows the VPN client to bypass the VPN server Internet firewall rules. Split DNS allows VPN clients to access web pages only available within the VPN server network.

- Off — This option disables split tunneling and split DNS.
Step 31. Split Tunneling only directs traffic from the VPN client to the VPN server when the VPN client sends traffic to a specific range or ranges of IP addresses. All other traffic from the VPN client is sent to the normal Internet connection of the VPN client. In the IP address field, enter the subnet network IP address of the subnet that receives the VPN client tunnel traffic.

Step 32. In the Netmask field, enter the subnet mask for the IP address entered above.

Step 33. Click **Add** to add the subnet to the list of recipient subnets.

Step 34. Repeat Steps 31 to 33 for each recipient subnet that you want to add.
Step 35. When the VPN client sends traffic to a domain name, Split DNS examines the destination domain name of the traffic. If the domain name is on the list of specified domain names, the traffic is redirected to the DNS server within the VPN server network. All other traffic is sent to the normal DNS server (i.e. the ISP DNS server). In the Domain name field, enter a domain name for traffic that is to be redirected to the DNS server of the VPN server network.

Step 36. Repeat Step 35 for each domain name that you want to add.

Step 37. Click Next. The Group Policy Summary page appears:
The *Group Policy Summary* page displays the current settings configured for the group policies.

Step 38. Click **Next**. The *IPsec Remote Access - User Group* page appears:

The *IPsec Remote Access - User Group* page allows you to configure settings for VPN users and groups of users.

Step 39. In the table, click **Add** to add a new user group, or click the edit icon (pencil icon) to edit an existing user group. The *User Group - Add/Edit* window appears.

Step 40. Click the Group Settings tab.
Step 41. In the Name field, enter a name for the user group.

Step 42. In the Web Login field, click a radio button.
- Disable — This option does not allow a VPN client to access the ISA500 Series Configuration Utility.
- Read Only — This option allows VPN clients to view the ISA500 Series Configuration Utility but not make changes to configuration.
- Administrator — This option allows VPN clients to view and edit the ISA500 Series Configuration Utility.

Step 43. From the SSL VPN drop-down list, choose a SSL VPN policy to use.

Step 44. In the IPsec Remote Access field, click a radio button.
- Enable — This option uses IPsec to allow the user group remote access to the VPN server network.
- Disable — This option does not use IPsec to allow the user group remote access to the VPN server network.

Step 45. In the Captive Portal field, click a radio button.
- Enable — This option directs a VPN client to the captive portal after the VPN connection is established.
- Disable — This option does not direct a VPN client to the captive portal after the VPN connection is established.

Step 46. Click the Membership tab.
Note: Perform Steps 47 through 50 if you want to create a new user for the group; otherwise, skip to Step 51.

Step 47. In the User Name field, enter a name for a new user.

Step 48. In the Password field, enter a password for a new user.

Step 49. In the Password Confirm field, re-enter the password.

Step 50. Click Create. The new user is added to the User list.

Step 51. To add a user to the user group, click and select the user to add in the User list, and click ->. The user appears in the Membership list.

Step 52. To remove a user from the user group, click and select the user to remove in the Membership list, and click <-. The user appears in the User list field.

Step 53. Click Ok. The IPsec Remote Access - User Group page re-appears.

Step 54. Click Next. The IPsec Remote Access - Summary page appears:
The *IPsec Remote Access - Summary* page displays all configuration made for IPsec Remote Access.

Step 55. Click **Finish**. The Remote Access VPN Wizard is finished.

**Configure with SSL Remote Access**

This procedure explains how to configure settings for SSL Remote Access in the Remote Access VPN Wizard.

Step 1. Log in to the ISA500 Series Configuration Wizard, and choose **Configuration Wizards > Remote Access VPN Wizard**. The *Getting Started* page opens:

The *Getting Started* page allows you to choose which type of VPN tunnel to use.

Step 2. From the VPN Tunnel Type drop-down list, choose **SSL Remote Access**.

Step 3. Click **Next**. The *SSL VPN - Configuration* page appears:
The SSL VPN - Configuration page allows you to configure settings for the SSL VPN connection such as network addresses and timeout limits.

Step 4. From the Gateway Interface drop-down list, choose a WAN interface through which the VPN traffic passes.
Step 5. In the Gateway Port field, enter a port on which that SSL operates.

Step 6. From the Certificate File drop-down list, choose a certificate to authenticate VPN clients.
Step 7. In the Client Address Pool, enter a network IP address for the client pool of address.

Step 8. In the Client Netmask, enter the subnet mask for the client pool of address.

Step 9. Check the **Create NAT rule allowing internet access to remote users** check box to allow VPN clients to access the Internet through the Internet connection of the VPN server.
Step 10. In the Client Domain field, enter a domain name for the VPN clients to use.

Step 11. In the Login Banner field, enter a message that is displayed on the VPN client login page.

Step 12. In the Idle Timeout field, enter how long in seconds a VPN session can remain idle before dropped.

Step 13. In the Session Timeout field, enter how long in seconds a VPN session lasts even if active. A value of 0 indicates that the session is never dropped when active.

Step 14. In the Client DPD Timeout field, enter how long in seconds a VPN session lasts once a VPN client becomes unresponsive.

Step 15. In the Gateway DPD Timeout field, enter how long in seconds a VPN session lasts once a VPN gateway becomes unresponsive.

Step 16. In the Keep Alive field, enter how often in seconds the VPN server checks the VPN session.

Step 17. In the Lease Duration field, enter how often in seconds a VPN client sends an IP address lease renewal request.
Step 18. In the Max MTU field, enter the Maximum Transfer Unit (MTU) for the VPN session.

Step 19. In the Rekey Interval field, enter how often in seconds the encryption key is changed.

Step 20. Click Next. The Group Policy page appears. The Group Policy page allows you to configure settings for group policies such as basic settings, proxies, split tunneling, and zone access.

Step 21. Click the Basic Settings tab.

Step 22. To add a group policy, click Add, or click the edit icon (pencil icon) to edit an a policy. The Group Policy - Add/Edit window appears:

Step 23. In the Policy Name field, enter a name for the group policy.

Step 24. In the Primary DNS Server field, enter the IP address of the primary Domain Name System (DNS) server. A DNS server translates domain names to static IP addresses to be used by computer networks. DNS works independent of operating systems.

Step 25. In the Secondary DNS Server field, enter the IP address of the secondary DNS server.

Step 26. In the Primary WINS Server field, enter the IP address of the primary Windows Internet Name Service (WINS) server. A WINS server translates domain names to dynamic
IP addresses to be used by computer networks. WINS primarily only works on Microsoft clients and Microsoft networks.

Step 27. In the Secondary WINS Server field, enter the IP address of the secondary Windows Internet Name Service (WINS) server.

Step 28. Click the IE Proxy Settings tab.

Step 29. In the IE Proxy Policy field, click a radio button for Microsoft Internet Explorer proxy settings.

- None — This option does not require the browser to use any proxy settings with the remote user.
- Auto — This option has the browser automatically detect proxy settings on the remote user.
- Bypass-Local — This option enables the browser to bypass proxy settings on the remote user.
- Disable — This option disables the Internet Explorer proxy settings.

Note: If you chose Auto or Bypass-Local from Step 28, perform Steps 29 through 31; otherwise, skip to Step 32.
Step 30. In the Address field, enter an IP address or domain name for the proxy server to use.

Step 31. In the Port field, enter the port number that the proxy server uses.

Step 32. To add an IP address or domain name that does not go through the proxy server, enter the IP address or domain name in the IE Proxy Exception field, and click Add.

Note: To remove an IP address or domain name from the exception list, click the IP address or domain name in the exception list, and click Delete.

Step 33. Click the Split Tunneling Settings tab.

Split Tunneling allows some of the remote client traffic to be transported outside the SSL VPN tunnel based on the destination addresses of the traffic.
Step 34. To enable Split Tunneling and Split DNS, check the **Enable Split Tunneling** check box.

Step 35. In the Split Selection field, click a radio button.

- Include Traffic — This option directs specified addresses through the VPN tunnel.
- Exclude Traffic — This option directs specified addresses through the WAN or ISP connection of the VPN client and not the VPN tunnel. For this option, the Exclude Local LANs feature must be enabled on Cisco AnyConnect Secure Mobility clients.
Step 36. In the Address field, enter the IP address to either include or exclude from the VPN Tunnel.

Step 37. In the Netmask field, enter the subnet mask for the IP address.

Step 38. Click Add. The IP address and Netmask are added to the Split Table.

Step 39. (Optional) If you chose Exclude Traffic in Step 34, check the Exclude Local LANs check box to allow the remote client to communicate with its local LAN devices without the use of the tunnel.
Step 40. To use a DNS server within the VPN, enter the DNS server IP address or domain name in the Split DNS field, and click **Add**.

**Note:** To delete a DNS server, click a DNS server in the Split DNS list, and click **Delete**.

Step 41. Click the Zone-based Firewall Settings tab.
Step 42. To grant the VPN client access to a zone on the VPN server network, click **Permit** for the zone. To deny the VPN client access to a zone on the VPN server network, click **Deny** for the zone.

Step 43. Click **Ok**. The *Group Policy* page re-appears.

Step 44. Click **Next**. The *User Group* page appears:

Step 45. To add a new user group, click **Add**. To edit an user group, click the edit icon (pencil icon) for the group to edit. The *User Group - Add/Edit* window appears.
Step 46. In the Name field, enter a name for the user group.

Step 47. In the Web Login field, click a radio button.

- **Disable** — This option does not allow the remote client to access the ISA500 Series Configuration Utility.

- **Read Only** — This option allows the remote client to access the ISA500 Series Configuration Utility but not to make changes.

- **Administrator** — This option allows the remote client to access the ISA500 Series Configuration Utility and to make changes.

Step 48. From the SSL VPN drop-down list, choose a policy to use for the group, or choose **Disable** to not use a policy.

Step 49. In the Cisco IPsec VPN field, click a radio button.

- **Enable** — This option use IPsec to allow the user group remote access to the VPN server network.

- **Disable** — This option does not use IPsec to allow the user group remote access to the VPN server network.

Step 50. In the Captive Portal field, click a radio button.

- **Enable** — This option directs a VPN client to the captive portal when the VPN connection is made.

- **Disable** — This option does not direct a VPN client to the captive portal when the VPN connection is made.

Step 51. Click the Membership tab.
Note: Perform Steps 52 through 55 if you want to create a new user for the group; otherwise, skip to Step 56.

Step 52. Enter the user name in the User Name field.

Step 53. In the Password field, enter a password for the new user.

Step 54. In the Password Confirm field, re-type the password for the new user.

Step 55. Click Create.

Step 56. To add a user to the user group, click the user to add in the User list, and click ->. The user appears in the Membership list.

Step 57. To remove a user from the user group, click the user to remove in the Membership list, and click <-. The user appears in the User list field.

Step 58. Click Ok. The User Group page reappears.

Step 59. Click Next. The SSL VPN summary page appears. The SSL VPN summary displays the configuration made for the SSL VPN connection.
Step 60. Click **Finish**. The Remote Access VPN Wizard is finished.