Advanced VPN Setup on the CVR100W VPN Router

Objective

A Virtual Private Network (VPN) is used to connect endpoints on different networks together over a public network, such as the Internet. This feature allows remote users who are away from a local network to securely connect to the network over the Internet.

This article explains how to configure Advanced VPN on the CVR100W VPN Router. For basic VPN setup, refer to the article *Basic VPN Setup on the CVR100W VPN Router*.

Applicable Devices

- CVR100W VPN Router

Software Version

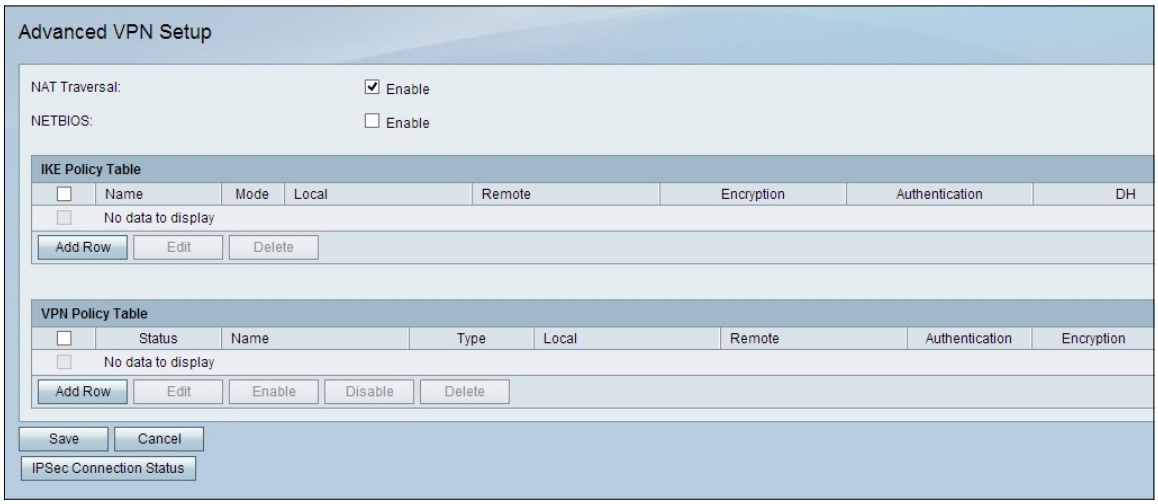
- 1.0.1.19

Advanced VPN Setup

Initial Settings

This procedure explains how to configure the initial settings of the Advanced VPN Setup.

Step 1. Log in to the web configuration utility and choose **VPN > Advanced VPN Setup**. The *Advanced VPN Setup* page opens:



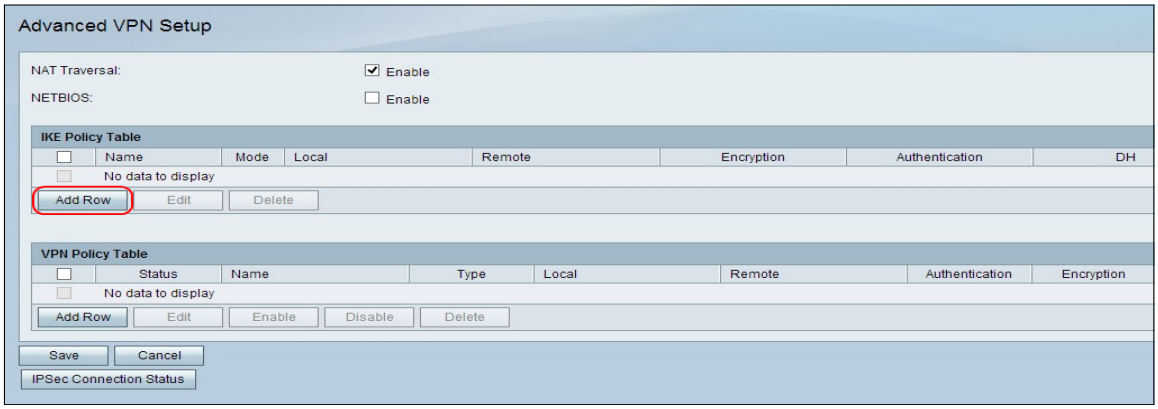
Step 2. (Optional) To enable Network Address Translation (NAT) Traversal for the VPN connection, check the **Enable** check box in the NAT Traversal field. NAT Traversal enables a VPN connection to be made between gateways that utilize NAT. Choose this option if your VPN connection passes through a NAT-enabled gateway.

Step 3. (Optional) To enable Network Basic Input/Output System (NetBIOS) broadcasts to

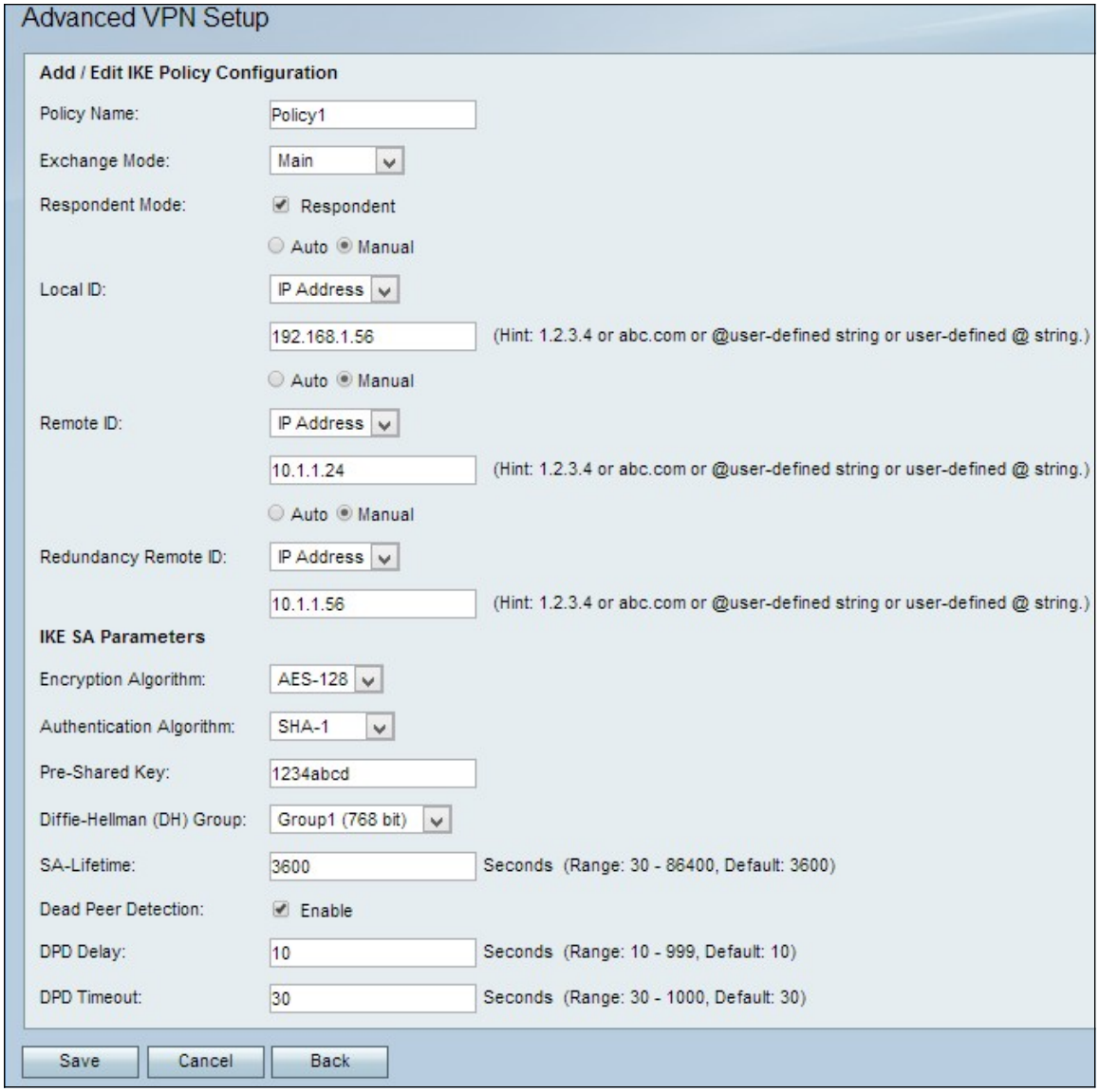
be sent through the VPN connection, check the **Enable** check box in the NETBIOS field. NetBIOS enables hosts to communicate with each other within a LAN.

IKE Policy Settings

Internet Key Exchange (IKE) is a protocol used to establish a secure connection for communication in a VPN. This established secure connection is called a Security Association (SA). This procedure explains how to configure an IKE policy for the VPN connection to use for security. For a VPN to function properly, the IKE policies for both end points should be identical.



Step 1. In the IKE Policy Table, click **Add Row** to create a new IKE policy. The *Advanced VPN Setup* page changes:



Step 2. In the Policy Name field, enter a name for the IKE policy.

Step 3. From the Exchange Mode drop-down list, choose an option to identify how the IKE policy operates.

- Main — This option allows the IKE policy to operate more securely. It is slower than aggressive mode. Choose this option if a more secure VPN connection is needed.
- Aggressive — This option allows the IKE policy to operate faster but it is less secure than main mode. Choose this option if a faster VPN connection is needed.

Step 4. (Optional) To enable the Respondent Mode, check the **Respondent** check box. If the Respondent Mode is enabled the CVR100W VPN Router can only receive the VPN request from the remote VPN endpoint.

Step 5. In the Local ID field, click on the desired radio button to identify how to specify the Local ID.

- Auto — This option automatically assigns Local ID.
- Manual — This option is used to manually assign Local ID.

Step 6. (Optional) From the Local ID drop-down list, choose the desired identification method for the local network.

- IP Address — This option identifies the local network by a public IP address.
- FQDN — This option uses a Fully Qualified Domain Name (FQDN) to identify the local network.

Step 7. (Optional) In the Local ID field, enter either the IP Address or the domain name. The entry is dependent on the option chosen in Step 6.

Step 8. In the Remote ID field, click on the desired radio button to identify how to specify the Remote ID.

- Auto — This option automatically assigns Remote ID.
- Manual — This option is used to manually assign Remote ID

Step 9. (Optional) From the Remote ID drop-down list, choose the desired identification method for the remote network.

- IP Address — This option identifies the remote network by a public IP address.
- FQDN — This option uses a Fully Qualified Domain Name (FQDN) to identify the remote network.

Step 10. (Optional) In the Remote ID field, enter either the IP Address or the domain name. The entry is dependent on the option chosen in Step 9.

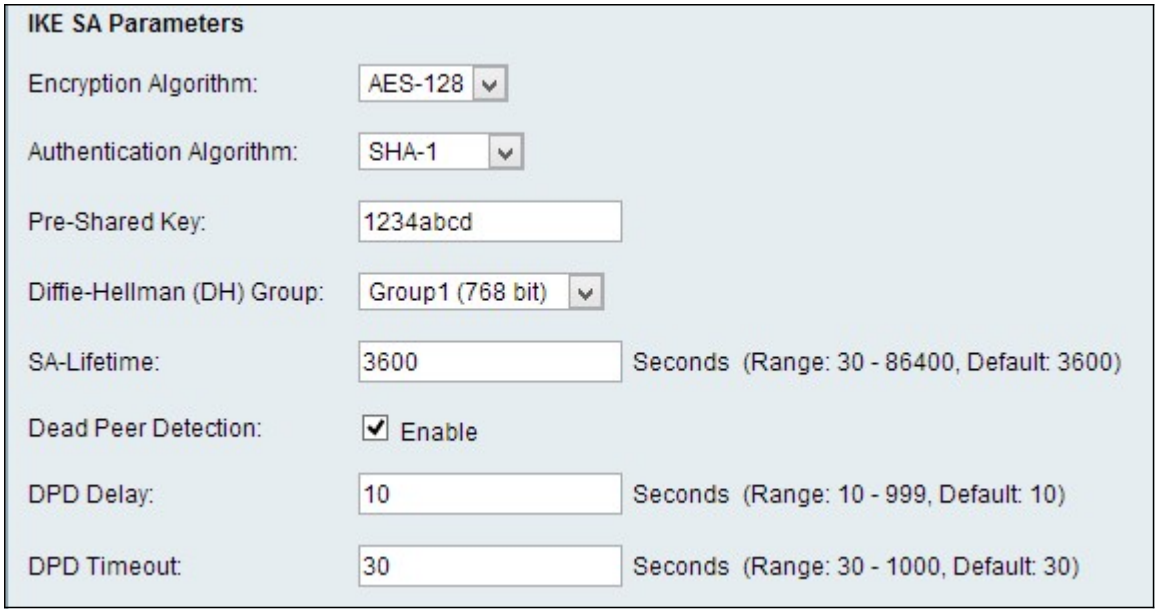
Step 11. In the Redundancy Remote ID field, click on the desired radio button to identify how to specify the Redundancy Remote ID. The Redundancy Remote ID is an alternative Remote ID used to setup the VPN tunnel at the remote gateway.

- Auto — This option automatically assigns Redundancy Remote ID.
- Manual — This option is used to manually assign Redundancy Remote ID.

Step 12. (Optional) From the Redundancy Remote ID drop-down list, choose the desired identification method for the redundancy network.

- IP Address — This option identifies the redundancy remote network by a public IP address.
- FQDN — This option uses a Fully Qualified Domain Name (FQDN) to identify the redundancy remote network.

Step 13. (Optional) In the Redundancy Remote ID field, enter either the IP Address or the domain name. The entry is dependent on the option chosen in Step 12.



Step 14. From the Encryption Algorithm drop-down list, choose an option to negotiate the Security Association (SA).

- DES — Data Encryption Standard (DES) uses a 56-bit key size for data encryption. DES is outdated and should be used if one endpoint only supports DES.
- 3DES — Triple Data Encryption Standard (3DES) performs DES three times but varies the key size from 168 bits to 112 bits and from 112 bits to 56 bits depending on the round of DES performed. 3DES is more secure than DES and AES.
- AES-128 — Advanced Encryption Standard with 128-bit key (AES-128) uses a 128-bit key for AES encryption. AES is faster and more secure than DES. Some types of hardware enable 3DES to be faster. AES-128 is faster but less secure than AES-192 and AES-256.
- AES-192 — AES-192 uses a 192-bit key for AES encryption. AES-192 is slower but more secure than AES-128, and AES-192 is faster but less secure than AES-256.
- AES-256 — AES-256 uses a 256-bit key for AES encryption. AES-256 is slower but more secure than AES-128 and AES-192.

Step 15. From the Authentication Algorithm drop-down list, choose an option to authenticate the VPN header.

- MD5 — Message-Digest Algorithm 5 (MD5) uses a 128-bit hash value for authentication. MD5 is less secure but it is faster than SHA-1 and SHA2-256.
- SHA-1 — Secure Hash Algorithm 1 (SHA-1) uses a 160-bit hash value for authentication. SHA-1 is slower but more secure than MD5, and SHA-1 is faster but less secure than SHA2-256.
- SHA2-256 — Secure Hash Algorithm 2 (SHA2-256) uses a 256-bit hash value for authentication. SHA2-256 is slower but secure than MD5 and SHA-1.

Step 16. In the Pre-Shared Key field, enter a preshared key that the IKE policy uses.

Step 17. From the Diffie-Hellman (DH) Group drop-down list, choose the DH group the IKE utilizes. Hosts in a DH group can exchange keys without knowledge of each other. The higher the group bit number, the more secure the group is.

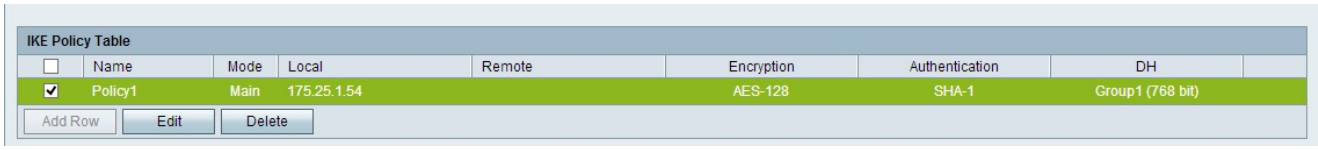
Step 18. In the SA-Lifetime field, enter how long (in seconds) the Security Association (SA) for the VPN lasts before the SA is renewed.

Step 19. (Optional) To enable Dead Peer Detection (DPD), check the **Enable** check box in the Dead Peer Detection field. DPD is used to monitor IKE peers to check if a peer has ceased to function. DPD prevents the waste of network resources on inactive peers.

Step 20. (Optional) To indicate how often the peer is checked for activity, enter the time interval (in seconds) in the DPD Delay field. This option is available if DPD is enabled in Step 19.

Step 21. (Optional) To indicate how long to wait before an inactive peer is dropped, enter how long (in seconds) in the DPD Timeout field. This option is available if DPD is enabled in Step 19.

Step 22. Click **Save**. The original *Advanced VPN Setup* page re-appears.

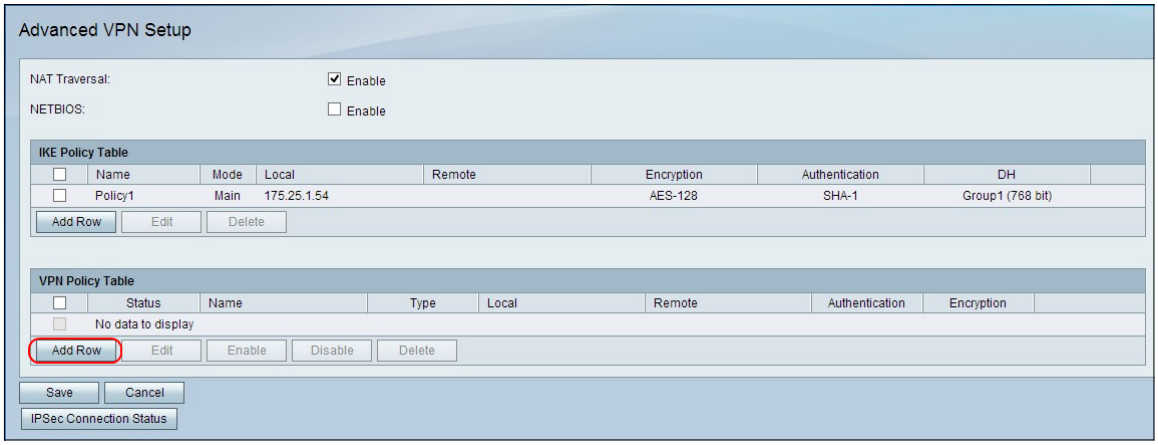


Step 23. (Optional) To edit an IKE policy in the IKE Policy Table, check the check box for the policy. Then click **Edit**, edit the required fields, and click **Save**.

Step 24. (Optional) To delete an IKE policy in the IKE Policy Table, check the check box for the policy and click **Delete.** Then click **Save**.

VPN Policy Settings

This procedure explains how to configure a VPN policy for the VPN connection to use. For a VPN to function properly, the VPN policies for both end points should be identical.



Step 1. In the VPN Policy Table, click **Add Row** to create a new VPN policy. The *Advanced VPN Setup* page changes:

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type: Auto Policy

Remote Endpoint: IP Address

(Hint: 1.2.3.4 or abc.com)

Redundancy Endpoint: Enable

IP Address

(Hint: 1.2.3.4 or abc.com)

Rollback enable

Local Traffic Selection

Local IP: Single

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP: Single

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming: 0x

SPI-Outgoing: 0x

Encryption Algorithm: AES-128

Key-In:

Key-Out:

Integrity Algorithm: SHA-1

Key-In:

Key-Out:

Auto Policy Parameters

SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1

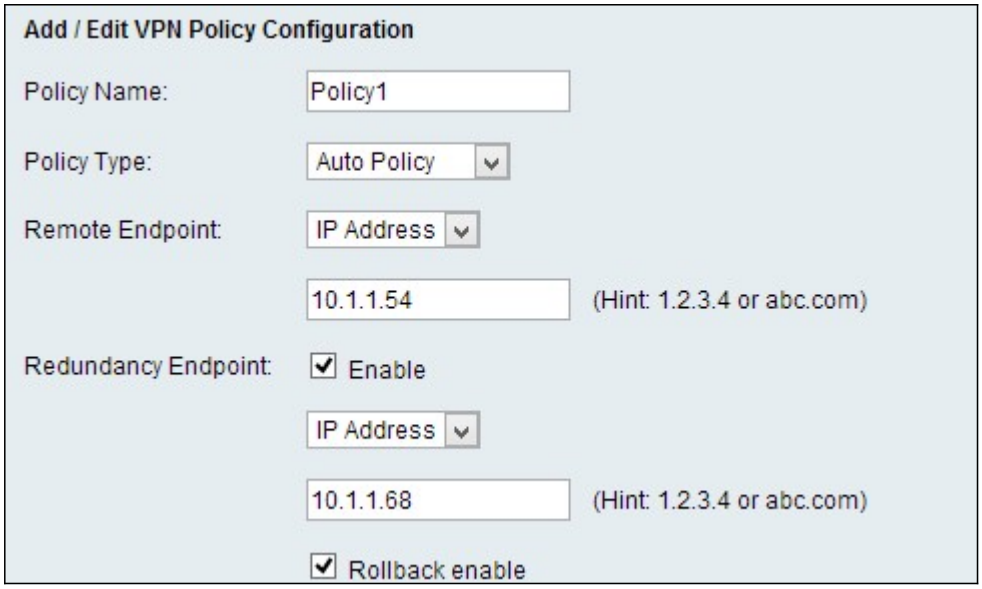
PFS Key Group: Enable

DH-Group 1(768 bit)

Select IKE Policy: Policy1

View

Save Cancel Back



Step 2. In the Policy Name field, enter a name for the VPN policy.

Step 3. From the Policy Type drop-down list, choose an option to identify how the settings of the VPN tunnel are generated.

- Manual Policy — This option allows you configure the keys for data encryption and integrity.
- Auto Policy — This option uses an IKE policy for data integrity and encryption key exchanges.

Step 4. From the Remote Endpoint drop-down list, choose an option to specify how to manually assign the Remote ID.

- IP Address — This option identifies the remote network by a public IP address.
- FQDN — This option uses a Fully Qualified Domain Name (FQDN) to identify the remote network.

Step 5. In the text-entry field below the Remote Endpoint drop-down list, enter either the public IP address or domain name of the remote address.

Step 6. (Optional) To enable redundancy, check the **Enable** check box in the Redundancy Endpoint field. The redundancy endpoint option enables the CVR100W VPN Router to connect to a backup VPN endpoint when the primary VPN connection fails.

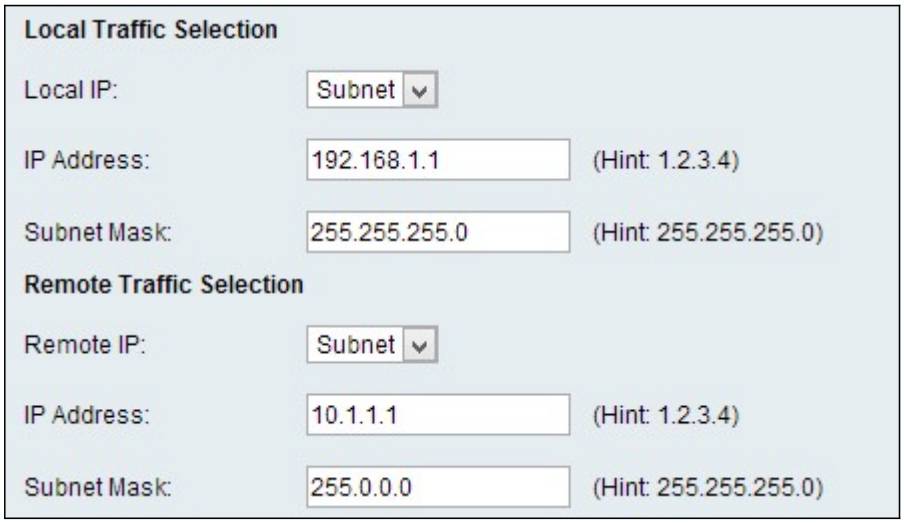
Step 7. (Optional) To manually assign the Redundancy ID, choose an option from the Redundancy Endpoint drop-down list.

- IP Address — This option identifies the redundancy remote network by a public IP address.
- FQDN — This option uses a Fully Qualified Domain Name (FQDN) to identify the redundancy remote network.

Step 8. (Optional) To enter the redundancy address, in the text-entry field below the Redundancy Endpoint drop-down list, enter either the public IP address or domain name.

Step 9. (Optional) To enable rollback, check the **Rollback enable** check box. This option

enables automatic switching from the backup VPN connection to the primary VPN connection when the primary VPN connection has recovered from a failure.



Step 10. From the Local IP drop-down list, choose an option to identify which hosts are affected by the policy.

- Single — This option uses a single host as the local VPN connection point.
- Subnet — This option uses a subnet of the local network as the local VPN connection point.

Step 11. In the IP Address field, enter the host or subnet IP address of the local subnet or host.

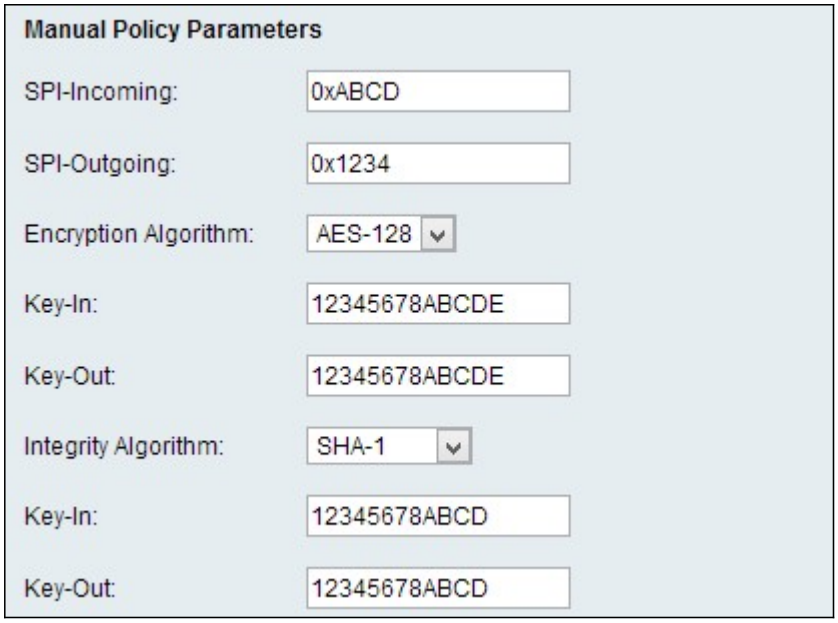
Step 12. (Optional) If the Subnet option is chosen in Step 10, enter the subnet mask for the local subnet in the Subnet Mask field.

Step 13. From the Remote IP drop-down list, choose an option to identify which hosts are affected by the policy.

- Single — This option uses a single host as the remote VPN connection point.
- Subnet — This option uses a subnet of the remote network as the remote VPN connection point.

Step 14. In the IP Address field, enter the host or subnet IP address of the remote subnet or host.

Step 15. (Optional) If the Subnet option is chosen in Step 13, enter the subnet mask for the remote subnet in the Subnet Mask field.



Note: If the Manual Policy option is chosen in Step 3, perform Step 16 through Step 23; otherwise, skip to Step 24.

Step 16. In the SPI-Incoming field, enter three to eight hexadecimal characters for Security Parameter Index (SPI) tag for incoming traffic on the VPN connection. The SPI tag is used to distinguish the traffic of one session from the traffic of other sessions. The incoming SPI on one side of the tunnel should be the outgoing SPI of the other side of the tunnel.

Step 17. In the SPI-Outgoing field, enter three to eight hexadecimal characters for SPI tag for outgoing traffic on the VPN connection. The SPI tag is used to distinguish the traffic of one session from the traffic of other sessions. The outgoing SPI on one side of the tunnel should be the incoming SPI of the other side of the tunnel.

Step 18. From the Encryption Algorithm drop-down list, choose an option to negotiate the Security Association (SA).

- DES — Data Encryption Standard (DES) uses a 56-bit key size for data encryption. DES is outdated and should be used if one endpoint only supports DES.

- 3DES — Triple Data Encryption Standard (3DES) performs DES three times but varies the key size from 168 bits to 112 bits and from 112 bits to 56 bits depending on the round of DES performed. 3DES is more secure than DES and AES.

- AES-128 — Advanced Encryption Standard with 128-bit key (AES-128) uses a 128-bit key for AES encryption. AES is faster and more secure than DES. Some types of hardware enable 3DES to be faster. AES-128 is faster but less secure than AES-192 and AES-256.

- AES-192 — AES-192 uses a 192-bit key for AES encryption. AES-192 is slower but more secure than AES-128, and AES-192 is faster but less secure than AES-256.

- AES-256 — AES-256 uses a 256-bit key for AES encryption. AES-256 is slower but more secure than AES-128 and AES-192.

Step 19. In the Key-In field, enter a key for the inbound policy. The key length depends on the algorithm chosen in Step 18.

- DES uses a 8 character key.

- 3DES uses a 24 character key.
- AES-128 uses a 12 character key.
- AES-192 uses a 24 character key.
- AES-256 uses a 32 character key.

Step 20. In the Key-Out field, enter a key for the outgoing policy. The key length depends on the algorithm chosen in Step 18. The key length depends on the algorithm chosen in Step 18.

- DES uses a 8 character key.
- 3DES uses a 24 character key.
- AES-128 uses a 12 character key.
- AES-192 uses a 24 character key.
- AES-256 uses a 32 character key.

Step 21. From the Integrity Algorithm drop-down list, choose an option to authenticate the VPN header.

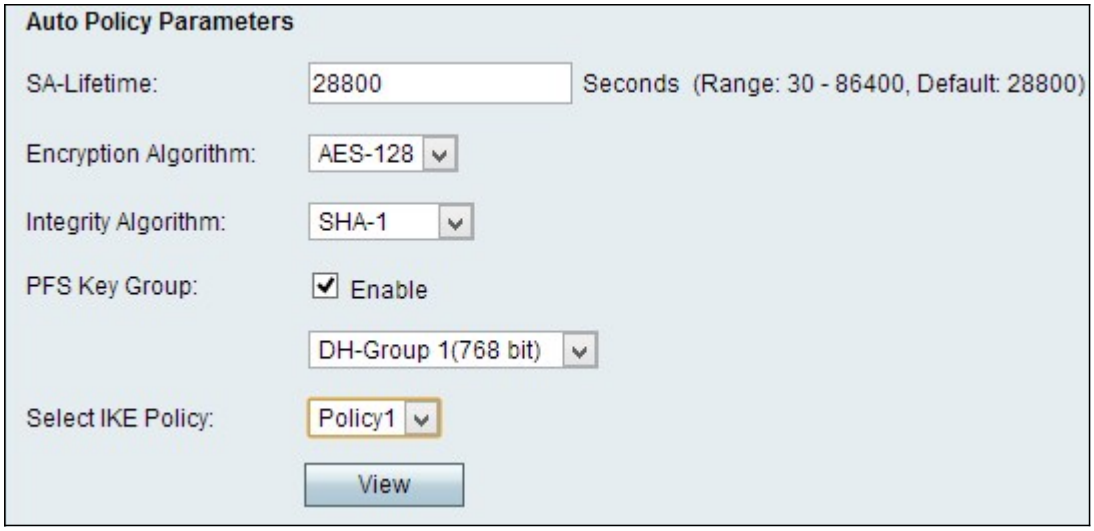
- MD5 — Message-Digest Algorithm 5 (MD5) uses a 128-bit hash value for authentication. MD5 is less secure but faster than SHA-1 and SHA2-256.
- SHA-1 — Secure Hash Algorithm 1 (SHA-1) uses a 160-bit hash value for authentication. SHA-1 is slower but more secure than MD5, and SHA-1 is faster but less secure than SHA2-256.
- SHA2-256 — Secure Hash Algorithm 2 (SHA2-256) uses a 256-bit hash value for authentication. SHA2-256 is slower but more secure than MD5 and SHA-1.

Step 22. In the Key-In field, enter a key for the inbound policy. The key length depends on the algorithm chosen in Step 21.

- MD5 uses a 16 character key.
- SHA-1 uses a 20 character key.
- SHA2-256 uses a 32 character key.

Step 23. In the Key-Out field, enter a key for the outgoing policy. The key length depends on the algorithm chosen in Step 21. The key length depends on the algorithm chosen in Step 21.

- MD5 uses a 16 character key.
- SHA-1 uses a 20 character key.
- SHA2-256 uses a 32 character key.



Note: If you chose Auto Policy in Step 3, perform Step 24 through Step 29; otherwise, skip to Step 31.

Step 24. In the SA-Lifetime field, enter how long in seconds the SA lasts before renewal.

Step 25. From the Encryption Algorithm drop-down list, choose an option to negotiate the Security Association (SA).

- DES — Data Encryption Standard (DES) uses a 56-bit key size for data encryption. DES is outdated and should be used if one endpoint only supports DES.
- 3DES — Triple Data Encryption Standard (3DES) performs DES three times but varies the key size from 168 bits to 112 bits and from 112 bits to 56 bits depending on the round of DES performed. 3DES is more secure than DES and AES.
- AES-128 — Advanced Encryption Standard with 128-bit key (AES-128) uses a 128-bit key for AES encryption. AES is faster and more secure than DES. Some types of hardware enable 3DES to be faster. AES-128 is faster but less secure than AES-192 and AES-256.
- AES-192 — AES-192 uses a 192-bit key for AES encryption. AES-192 is slower but more secure than AES-128, and AES-192 is faster but less secure than AES-256.
- AES-256 — AES-256 uses a 256-bit key for AES encryption. AES-256 is slower but more secure than AES-128 and AES-192.

Step 26. From the Integrity Algorithm drop-down list, choose an option to authenticate the VPN header.

- MD5 — Message-Digest Algorithm 5 (MD5) uses a 128-bit hash value for authentication. MD5 is less secure but faster than SHA-1 and SHA2-256.
- SHA-1 — Secure Hash Algorithm 1 (SHA-1) uses a 160-bit hash value for authentication. SHA-1 is slower but more secure than MD5, and SHA-1 is faster but less secure than SHA2-256.
- SHA2-256 — Secure Hash Algorithm 2 (SHA2-256) uses a 256-bit hash value for authentication. SHA2-256 is slower but secure than MD5 and SHA-1.

Step 27. Check the **Enable** check box in the PFS Key Group field to enable Perfect Forward Secrecy (PFS). PFS increases the VPN security, but slows the speed of connection.

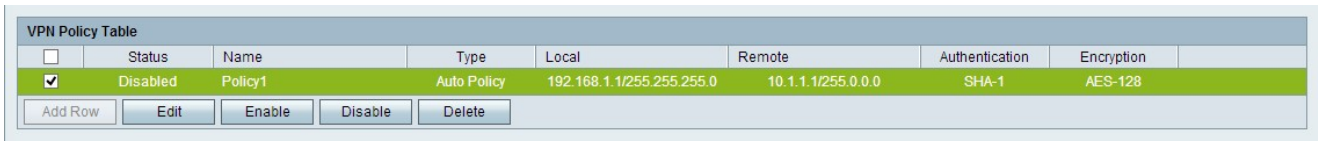
Step 28. (Optional) If you chose to enable PFS in Step 27, choose a Diffie-Hellman (DH) group to join from the drop-down list, below the PFS Key Group field. The higher the group number is, the more secure the group is.

Step 29. From the Select IKE Policy drop-down list, choose which IKE policy to use for the VPN policy.

Step 30. (Optional) If you click **View**, you are directed to the IKE configuration section of the *Advanced VPN Setup* page.

Step 31. Click **Save**. The original *Advanced VPN Setup* page re-appears.

Step 32. Click **Save**.



Step 33. (Optional) To edit a VPN policy in the VPN Policy Table, check the check box for the policy. Then click **Edit**, edit the required fields, and click **Save**.

Step 34. (Optional) To delete a VPN policy in the VPN Policy Table, check the check box for the policy, click **Delete**, and then click **Save**.