Erweitertes VPN-Setup auf dem CVR100W VPN-Router

Ziel

Ein Virtual Private Network (VPN) wird verwendet, um Endpunkte in verschiedenen Netzwerken über ein öffentliches Netzwerk wie das Internet miteinander zu verbinden. Diese Funktion ermöglicht Remote-Benutzern, die sich nicht im lokalen Netzwerk befinden, eine sichere Verbindung zum Netzwerk über das Internet herzustellen.

In diesem Artikel wird die Konfiguration von Advanced VPN auf dem CVR100W VPN-Router erläutert. Eine grundlegende VPN-Konfiguration finden Sie im Artikel *Basic VPN Setup (Grundlegendes VPN-Setup) auf dem CVR100W VPN-Router*.

Anwendbare Geräte

·CVR100W VPN-Router

Softwareversion

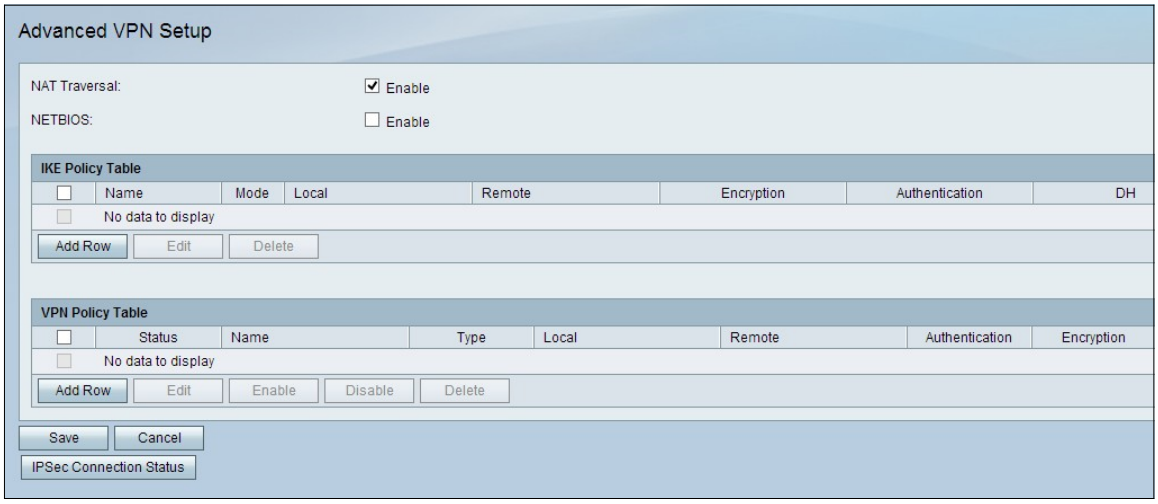
·1.0.1.19

Erweiterte VPN-Einrichtung

Ersteinstellungen

In diesem Verfahren wird erläutert, wie die ursprünglichen Einstellungen für das erweiterte VPN-Setup konfiguriert werden.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **VPN > Advanced VPN Setup aus**. Die Seite *Advanced VPN Setup* wird geöffnet:



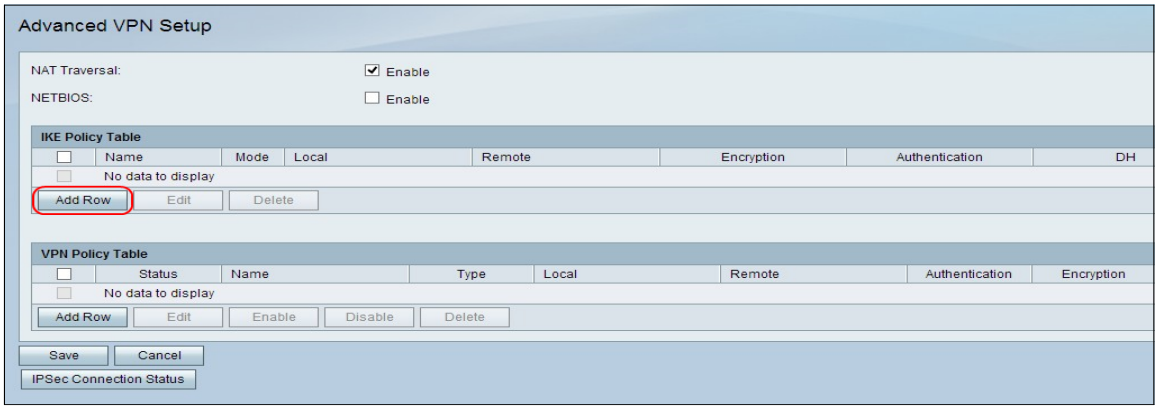
Schritt 2: (Optional) Um Network Address Translation (NAT) Traversal für die VPN-Verbindung zu aktivieren, aktivieren Sie im Feld NAT Traversal das **Kontrollkästchen Enable (Aktivieren)**. NAT Traversal ermöglicht die Herstellung einer VPN-Verbindung zwischen

Gateways, die NAT verwenden. Wählen Sie diese Option aus, wenn Ihre VPN-Verbindung über ein NAT-fähiges Gateway verläuft.

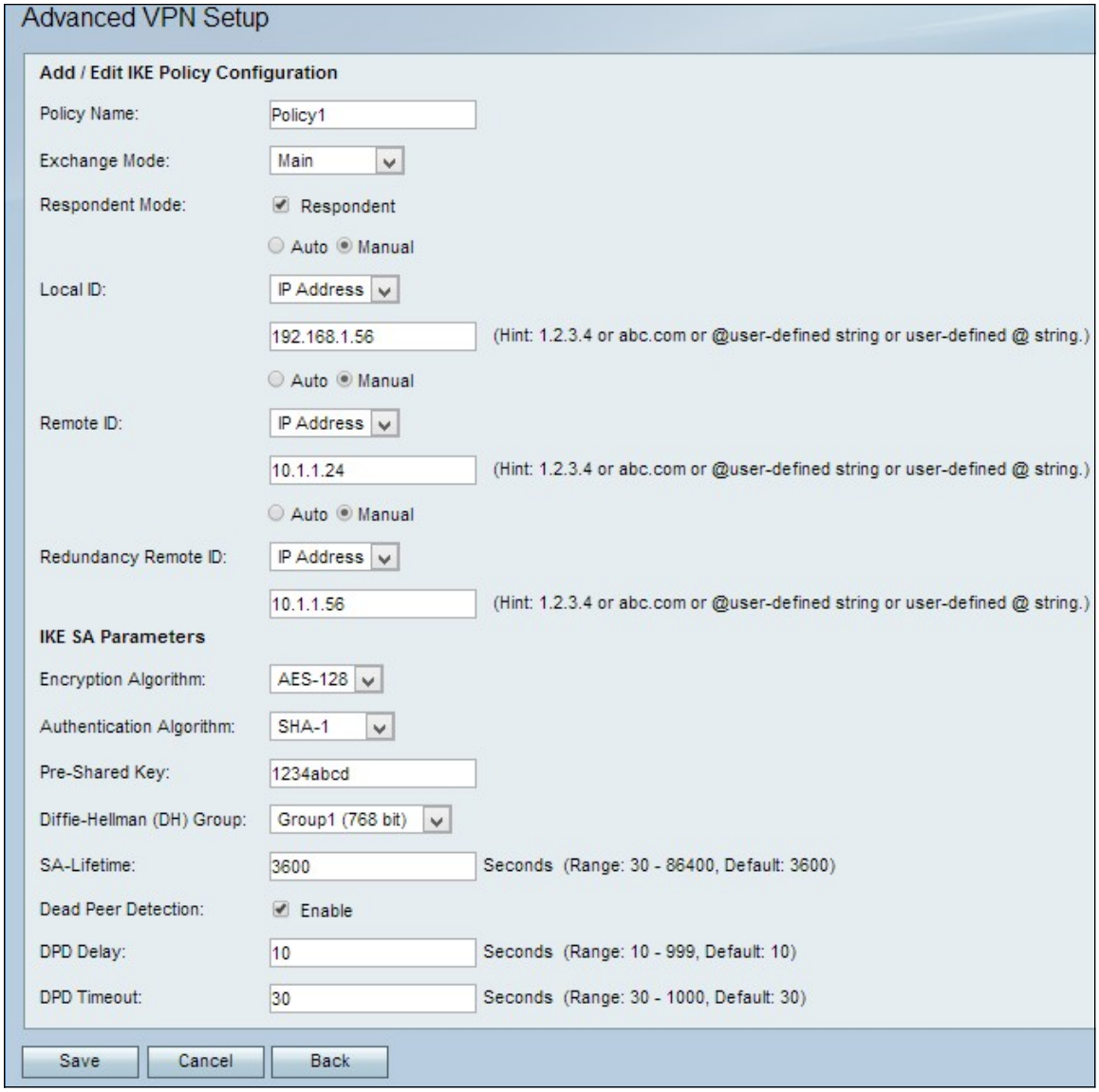
Schritt 3: (Optional) Um das Senden von NetBIOS-Broadcasts (Network Basic Input/Output System) über die VPN-Verbindung zu aktivieren, aktivieren Sie im Feld NETBIOS das Kontrollkästchen **Enable (Aktivieren)**. NetBIOS ermöglicht Hosts die Kommunikation untereinander in einem LAN.

IKE-Richtlinieneinstellungen

Internet Key Exchange (IKE) ist ein Protokoll, das verwendet wird, um eine sichere Verbindung für die Kommunikation in einem VPN herzustellen. Diese etablierte sichere Verbindung wird als Security Association (SA) bezeichnet. In diesem Verfahren wird erläutert, wie Sie eine IKE-Richtlinie für die VPN-Verbindung konfigurieren, die für die Sicherheit verwendet wird. Damit ein VPN ordnungsgemäß funktioniert, müssen die IKE-Richtlinien für beide Endpunkte identisch sein.



Schritt 1: Klicken Sie in der IKE-Richtlinientabelle auf **Zeile hinzufügen**, um eine neue IKE-Richtlinie zu erstellen. Die Seite *Advanced VPN Setup* wird wie folgt geändert:



Schritt 2: Geben Sie im Feld Policy Name (Richtlinienname) einen Namen für die IKE-Richtlinie ein.

Schritt 3: Wählen Sie aus der Exchange Mode-Dropdown-Liste eine Option aus, um festzulegen, wie die IKE-Richtlinie funktioniert.

·Main (Hauptmodus): Mit dieser Option kann die IKE-Richtlinie sicherer arbeiten. Er ist langsamer als aggressiver Modus. Wählen Sie diese Option aus, wenn eine sicherere VPN-Verbindung erforderlich ist.

·Aggressive (Aggressiv): Mit dieser Option kann die IKE-Richtlinie schneller ausgeführt werden, ist jedoch weniger sicher als der Hauptmodus. Wählen Sie diese Option aus, wenn eine schnellere VPN-Verbindung erforderlich ist.

Schritt 4: (Optional) Um den Teilnehmermodus zu aktivieren, aktivieren Sie das Kontrollkästchen **Teilnehmer**. Wenn der Antwortmodus aktiviert ist, kann der CVR100W VPN-Router nur die VPN-Anforderung vom Remote-VPN-Endpunkt empfangen.

Schritt 5: Klicken Sie im Feld Lokale ID auf das gewünschte Optionsfeld, um anzugeben, wie die lokale ID angegeben wird.

·Auto (Automatisch): Diese Option weist die lokale ID automatisch zu.

·Manual (Manuell) - Diese Option wird verwendet, um eine lokale ID manuell zuzuweisen.

Schritt 6: (Optional) Wählen Sie aus der Dropdown-Liste Local ID (Lokale ID) die gewünschte Identifizierungsmethode für das lokale Netzwerk aus.

·IP Address (IP-Adresse): Diese Option identifiziert das lokale Netzwerk anhand einer öffentlichen IP-Adresse.

·FQDN - Diese Option identifiziert das lokale Netzwerk mithilfe eines FQDN (Fully Qualified Domain Name).

Schritt 7: (Optional) Geben Sie im Feld Local ID (Lokale ID) entweder die IP-Adresse oder den Domänennamen ein. Der Eintrag hängt von der in Schritt 6 ausgewählten Option ab.

Schritt 8: Klicken Sie im Feld Remote ID (Remote-ID) auf das gewünschte Optionsfeld, um anzugeben, wie die Remote-ID angegeben wird.

·Auto (Automatisch): Diese Option weist die Remote-ID automatisch zu.

·Manual (Manuell): Diese Option wird verwendet, um die Remote-ID manuell zuzuweisen.

Schritt 9: (Optional) Wählen Sie in der Dropdown-Liste Remote ID (Remote-ID) die gewünschte Identifikationsmethode für das Remote-Netzwerk aus.

·IP Address (IP-Adresse): Diese Option identifiziert das Remote-Netzwerk über eine öffentliche IP-Adresse.

·FQDN - Diese Option identifiziert das Remote-Netzwerk mithilfe eines FQDN (Fully Qualified Domain Name).

Schritt 10: (Optional) Geben Sie im Feld Remote ID (Remote-ID) entweder die IP-Adresse oder den Domänennamen ein. Der Eintrag hängt von der Option ab, die in Schritt 9 gewählt wurde.

Schritt 11: Klicken Sie im Feld Redundancy Remote ID (Redundanz-Remote-ID) auf das gewünschte Optionsfeld, um anzugeben, wie die Redundanz-Remote-ID angegeben wird. Die Redundanz-Remote-ID ist eine alternative Remote-ID, die zum Einrichten des VPN-Tunnels am Remote-Gateway verwendet wird.

·Auto (Automatisch): Diese Option weist Redundanz-Remote-ID automatisch zu.

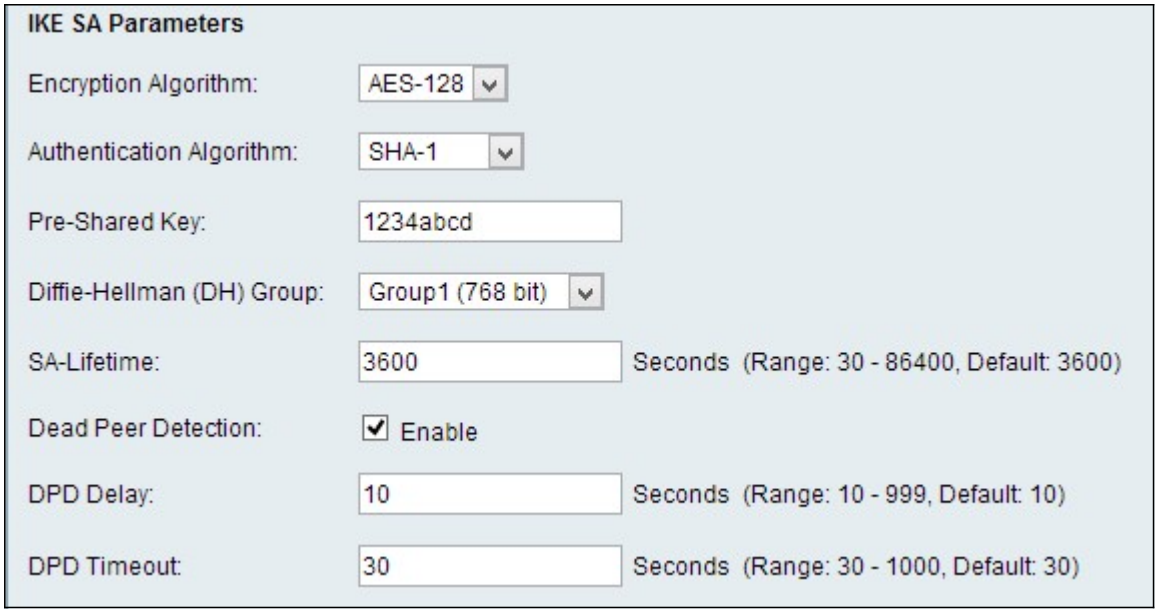
·Manual (Manuell): Mit dieser Option wird die Remote-ID der Redundanz manuell zugewiesen.

Schritt 12: (Optional) Wählen Sie aus der Dropdown-Liste Redundancy Remote ID (Redundanz-Remote-ID) die gewünschte Identifikationsmethode für das Redundanznetzwerk aus.

·IP Address (IP-Adresse): Diese Option identifiziert das redundante Remote-Netzwerk über eine öffentliche IP-Adresse.

·FQDN: Diese Option verwendet einen FQDN (Fully Qualified Domain Name), um das redundante Remote-Netzwerk zu identifizieren.

Schritt 13: (Optional) Geben Sie im Feld Redundancy Remote ID (Remote-ID für Redundanz) entweder die IP-Adresse oder den Domänennamen ein. Der Eintrag hängt von der in Schritt 12 ausgewählten Option ab.



Schritt 14: Wählen Sie in der Dropdown-Liste Verschlüsselungsalgorithmus eine Option aus, um die Security Association (SA) auszuhandeln.

·DES - Data Encryption Standard (DES) verwendet eine 56-Bit-Schlüsselgröße für die Datenverschlüsselung. DES ist veraltet und sollte verwendet werden, wenn nur ein Endpunkt DES unterstützt.

·3DES - Der Triple Data Encryption Standard (3DES) führt DES dreimal durch, variiert jedoch die Schlüssellänge zwischen 168 Bit und 112 Bit und zwischen 112 Bit und 56 Bit, je nach der DES-Runde. 3DES ist sicherer als DES und AES.

·AES-128 - Advanced Encryption Standard mit 128-Bit-Schlüssel (AES-128) verwendet einen 128-Bit-Schlüssel für AES-Verschlüsselung. AES ist schneller und sicherer als DES. Einige Hardwaretypen ermöglichen eine schnellere 3DES-Verarbeitung. AES-128 ist schneller, aber weniger sicher als AES-192 und AES-256.

·AES-192 - AES-192 verwendet einen 192-Bit-Schlüssel für die AES-Verschlüsselung. AES-192 ist langsamer, aber sicherer als AES-128, und AES-192 ist schneller, aber weniger sicher als AES-256.

·AES-256 - AES-256 verwendet einen 256-Bit-Schlüssel für die AES-Verschlüsselung. AES-256 ist langsamer, aber sicherer als AES-128 und AES-192.

Schritt 15: Wählen Sie in der Dropdown-Liste Authentication Algorithm (Authentifizierungsalgorithmus) eine Option zur Authentifizierung des VPN-Headers.

·MD5 — Message-Digest Algorithm 5 (MD5) verwendet einen 128-Bit-Hashwert für die Authentifizierung. MD5 ist weniger sicher, aber schneller als SHA-1 und SHA2-256.

·SHA-1 - Secure Hash Algorithm 1 (SHA-1) verwendet für die Authentifizierung einen 160-Bit-Hashwert. SHA-1 ist langsamer, aber sicherer als MD5, und SHA-1 ist schneller, aber weniger sicher als SHA2-256.

·SHA2-256 - Secure Hash Algorithm 2 (SHA2-256) verwendet einen 256-Bit-Hash-Wert für die Authentifizierung. SHA2-256 ist langsamer, aber sicher als MD5 und SHA-1.

Schritt 16: Geben Sie im Feld Pre-Shared Key (Vorinstallierter Schlüssel) einen vorinstallierten Schlüssel ein, den die IKE-Richtlinie verwendet.

Schritt 17: Wählen Sie aus der Dropdown-Liste Diffie-Hellman (DH) Group (DH-Gruppe) die DH-Gruppe aus, die von IKE verwendet wird. Hosts in einer DH-Gruppe können Schlüssel austauschen, ohne einander zu kennen. Je höher die Bitnummer der Gruppe, desto sicherer ist die Gruppe.

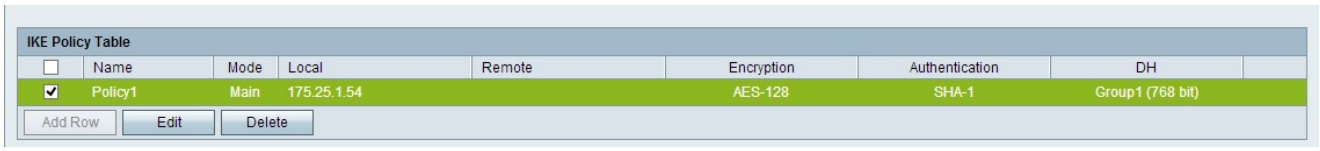
Schritt 18: Geben Sie im Feld SA-Lifetime (SA-Lifetime) ein, wie lange (in Sekunden) die Security Association (SA) für das VPN dauert, bevor die SA verlängert wird.

Schritt 19: (Optional) Um Dead Peer Detection (DPD) zu aktivieren, aktivieren Sie im Feld Dead Peer Detection (**Dead Peer Detection)** das Kontrollkästchen **Enable (Aktivieren)**. DPD wird zur Überwachung von IKE-Peers verwendet, um zu überprüfen, ob ein Peer nicht mehr funktioniert. DPD verhindert die Verschwendung von Netzwerkressourcen bei inaktiven Peers.

Schritt 20: (Optional) Geben Sie das Zeitintervall (in Sekunden) im Feld "DPD Delay" (DPD-Verzögerung) ein, um anzugeben, wie oft der Peer auf Aktivität überprüft wird. Diese Option ist verfügbar, wenn DPD in Schritt 19 aktiviert ist.

Schritt 21: (Optional) Geben Sie in das Feld Zeitüberschreitung für die DPD an, wie lange (in Sekunden) gewartet werden soll, bis ein inaktiver Peer verworfen wird. Diese Option ist verfügbar, wenn DPD in Schritt 19 aktiviert ist.

Schritt 22: Klicken Sie auf **Speichern**. Die ursprüngliche Seite *Advanced VPN Setup* wird erneut angezeigt.

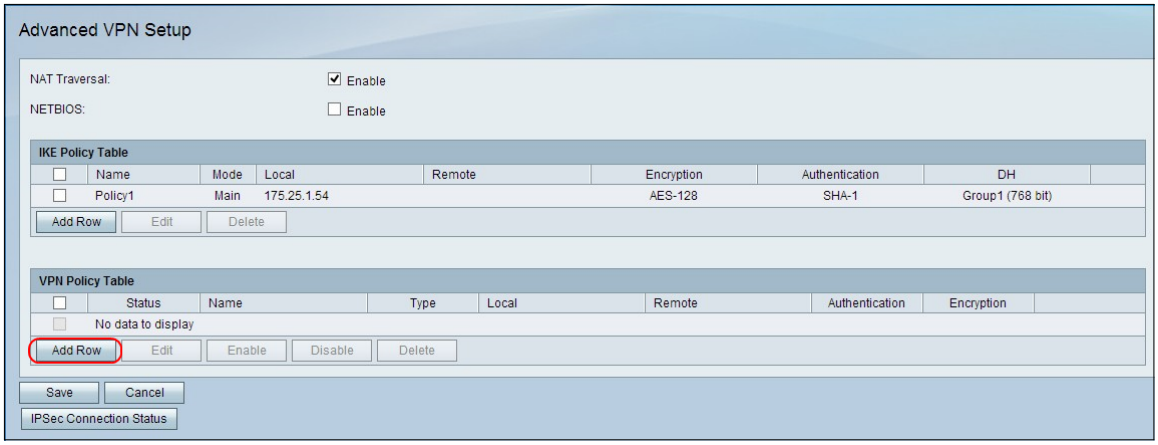


Schritt 23: (Optional) Um eine IKE-Richtlinie in der IKE-Richtlinientabelle zu bearbeiten, aktivieren Sie das Kontrollkästchen für die Richtlinie. Klicken Sie dann auf **Bearbeiten**, bearbeiten Sie die erforderlichen Felder, und klicken Sie auf **Speichern**.

Schritt 24: (Optional) Um eine IKE-Richtlinie in der IKE-Richtlinientabelle zu löschen, aktivieren Sie das Kontrollkästchen für die Richtlinie, und klicken Sie dann auf **Löschen.** Klicken Sie anschließend auf **Speichern**.

VPN-Richtlinieneinstellungen

In diesem Verfahren wird erläutert, wie eine VPN-Richtlinie für die zu verwendende VPN-Verbindung konfiguriert wird. Damit ein VPN ordnungsgemäß funktioniert, müssen die VPN-Richtlinien für beide Endpunkte identisch sein.



Schritt 1: Klicken Sie in der VPN Policy Table (VPN-Richtlinientabelle) auf **Add Row (Zeile hinzufügen)**, um eine neue VPN-Richtlinie zu erstellen. Die Seite *Advanced VPN Setup* wird wie folgt geändert:

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

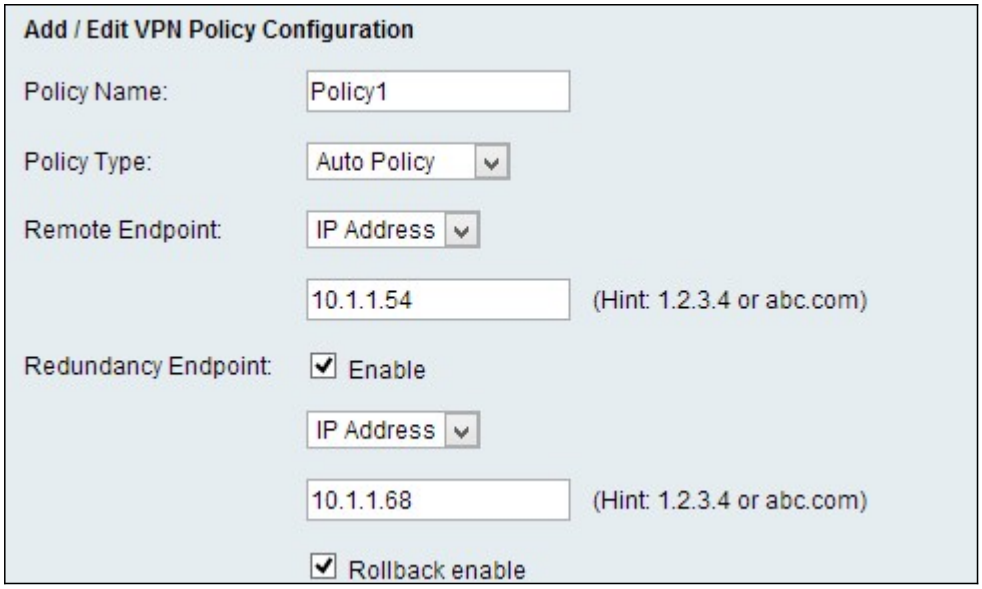
PFS Key Group: Enable

DH-Group 1(768 bit)

Select IKE Policy: Policy1

View

Save Cancel Back



Schritt 2: Geben Sie im Feld Policy Name (Richtlinienname) einen Namen für die VPN-Richtlinie ein.

Schritt 3: Wählen Sie in der Dropdown-Liste Policy Type (Richtlinientyp) eine Option aus, um festzulegen, wie die Einstellungen des VPN-Tunnels generiert werden.

·Manual Policy (Manuelle Richtlinie): Mit dieser Option können Sie die Schlüssel für Datenverschlüsselung und -integrität konfigurieren.

·Auto Policy (Automatische Richtlinie): Diese Option verwendet eine IKE-Richtlinie für Datenintegrität und den Austausch von Verschlüsselungsschlüsseln.

Schritt 4: Wählen Sie in der Dropdown-Liste Remote Endpoint (Remote-Endpunkt) eine Option aus, um anzugeben, wie die Remote-ID manuell zugewiesen wird.

·IP Address (IP-Adresse): Diese Option identifiziert das Remote-Netzwerk über eine öffentliche IP-Adresse.

·FQDN - Diese Option identifiziert das Remote-Netzwerk mithilfe eines FQDN (Fully Qualified Domain Name).

Schritt 5: Geben Sie im Textfeld unter der Dropdown-Liste "Remote Endpoint" entweder die öffentliche IP-Adresse oder den Domänennamen der Remote-Adresse ein.

Schritt 6: (Optional) Um Redundanz zu aktivieren, aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld Redundanz Endpoint. Mit der Endgeräteoption für Redundanz kann der CVR100W VPN-Router bei Ausfall der primären VPN-Verbindung eine Verbindung zu einem Backup-VPN-Endpunkt herstellen.

Schritt 7: (Optional) Um die Redundanz-ID manuell zuzuweisen, wählen Sie eine Option aus der Dropdown-Liste Redundanz Endpoint (Redundanz-Endpunkt) aus.

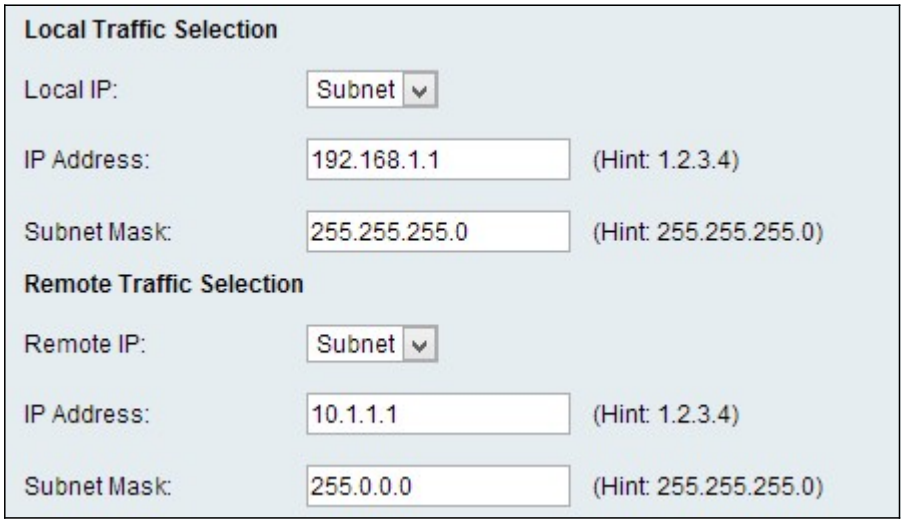
·IP Address (IP-Adresse): Diese Option identifiziert das redundante Remote-Netzwerk über eine öffentliche IP-Adresse.

·FQDN: Diese Option verwendet einen FQDN (Fully Qualified Domain Name), um das redundante Remote-Netzwerk zu identifizieren.

Schritt 8: (Optional) Geben Sie zur Eingabe der Redundanzadresse im Textfeld unter der

Dropdown-Liste Redundanz Endpoint (Redundanzendpunkt) entweder die öffentliche IP-Adresse oder den Domänennamen ein.

Schritt 9: (Optional) Um Rollback zu aktivieren, aktivieren Sie das Kontrollkästchen **Rollback enable**. Diese Option ermöglicht das automatische Switching von der Backup-VPN-Verbindung zur primären VPN-Verbindung, wenn die primäre VPN-Verbindung nach einem Ausfall wiederhergestellt wurde.



Schritt 10: Wählen Sie in der Dropdown-Liste Local IP (Lokale IP) eine Option aus, um zu bestimmen, welche Hosts von der Richtlinie betroffen sind.

·Single (Einzel): Diese Option verwendet einen einzelnen Host als lokalen VPN-Verbindungspunkt.

·Subnetz - Diese Option verwendet ein Subnetz des lokalen Netzwerks als lokalen VPN-Verbindungspunkt.

Schritt 11: Geben Sie im Feld IP-Adresse den Host oder die Subnetz-IP-Adresse des lokalen Subnetzes oder Hosts ein.

Schritt 12: (Optional) Wenn in Schritt 10 die Option Subnet (Subnetz) ausgewählt ist, geben Sie die Subnetzmaske für das lokale Subnetz in das Feld Subnetzmaske ein.

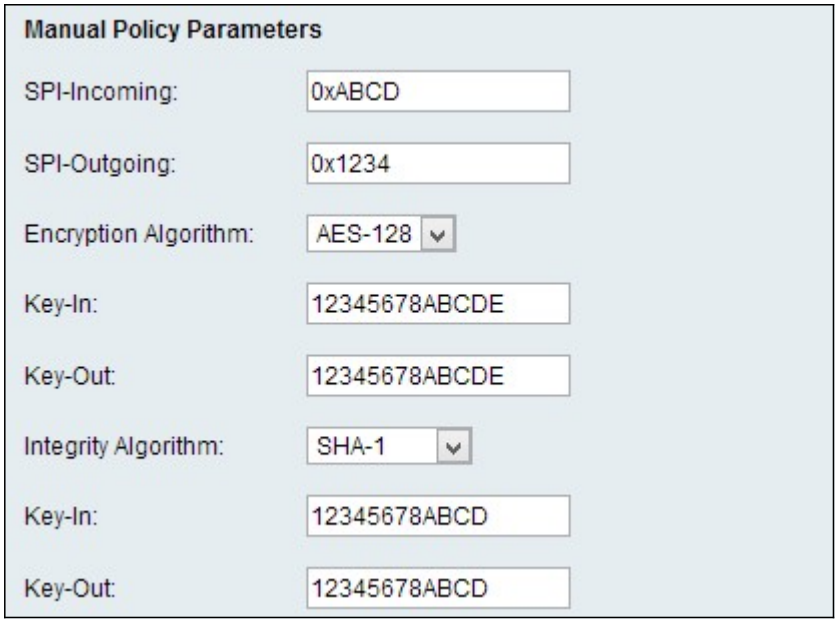
Schritt 13: Wählen Sie in der Dropdown-Liste Remote IP (Remote-IP) eine Option aus, um zu bestimmen, welche Hosts von der Richtlinie betroffen sind.

·Single (Einzel): Diese Option verwendet einen einzelnen Host als Remote-VPN-Verbindungspunkt.

·Subnetz - Diese Option verwendet ein Subnetz des Remote-Netzwerks als Remote-VPN-Verbindungspunkt.

Schritt 14: Geben Sie im Feld IP-Adresse den Host oder die Subnetz-IP-Adresse des Remote-Subnetzes oder -Hosts ein.

Schritt 15: (Optional) Wenn in Schritt 13 die Option Subnet (Subnetz) ausgewählt ist, geben Sie die Subnetzmaske für das Remote-Subnetz in das Feld Subnetzmaske ein.



Hinweis: Wenn Sie in Schritt 3 die Option Manual Policy (Manuelle Richtlinie) auswählen, führen Sie die Schritte 16 bis 23 durch. Fahren Sie andernfalls mit Schritt 24 fort.

Schritt 16: Geben Sie im Feld SPI-Incoming (SPI-Incoming) drei bis acht Hexadezimalzeichen für das SPI-Tag (Security Parameter Index) für eingehenden Datenverkehr an der VPN-Verbindung ein. Der SPI-Tag wird verwendet, um den Datenverkehr einer Sitzung vom Datenverkehr anderer Sitzungen zu unterscheiden. Der eingehende SPI auf der einen Seite des Tunnels sollte der ausgehende SPI auf der anderen Seite des Tunnels sein.

Schritt 17: Geben Sie im Feld SPI-Outgoing (SPI-Ausgang) drei bis acht Hexadezimalzeichen für SPI-Tag für ausgehenden Datenverkehr an der VPN-Verbindung ein. Der SPI-Tag wird verwendet, um den Datenverkehr einer Sitzung vom Datenverkehr anderer Sitzungen zu unterscheiden. Der ausgehende SPI auf der einen Seite des Tunnels sollte der eingehende SPI auf der anderen Seite des Tunnels sein.

Schritt 18: Wählen Sie in der Dropdown-Liste Verschlüsselungsalgorithmus eine Option aus, um die Security Association (SA) auszuhandeln.

·DES - Data Encryption Standard (DES) verwendet eine 56-Bit-Schlüsselgröße für die Datenverschlüsselung. DES ist veraltet und sollte verwendet werden, wenn nur ein Endpunkt DES unterstützt.

·3DES - Der Triple Data Encryption Standard (3DES) führt DES dreimal durch, variiert jedoch die Schlüssellänge zwischen 168 Bit und 112 Bit und zwischen 112 Bit und 56 Bit, je nach der DES-Runde. 3DES ist sicherer als DES und AES.

·AES-128 - Advanced Encryption Standard mit 128-Bit-Schlüssel (AES-128) verwendet einen 128-Bit-Schlüssel für AES-Verschlüsselung. AES ist schneller und sicherer als DES. Einige Hardwaretypen ermöglichen eine schnellere 3DES-Verarbeitung. AES-128 ist schneller, aber weniger sicher als AES-192 und AES-256.

·AES-192 - AES-192 verwendet einen 192-Bit-Schlüssel für die AES-Verschlüsselung. AES-192 ist langsamer, aber sicherer als AES-128, und AES-192 ist schneller, aber weniger sicher als AES-256.

·AES-256 - AES-256 verwendet einen 256-Bit-Schlüssel für die AES-Verschlüsselung.

AES-256 ist langsamer, aber sicherer als AES-128 und AES-192.

Schritt 19: Geben Sie im Feld Key-In (Schlüsseleingabe) einen Schlüssel für die eingehende Richtlinie ein. Die Schlüssellänge hängt von dem in Schritt 18 gewählten Algorithmus ab.

·DES verwendet einen 8-stelligen Schlüssel.

·3DES verwendet einen 24-stelligen Schlüssel.

·AES-128 verwendet einen 12-stelligen Schlüssel.

·AES-192 verwendet einen 24-stelligen Schlüssel.

·AES-256 verwendet einen 32-stelligen Schlüssel.

Schritt 20: Geben Sie im Feld "Key-Out" (Schlüssel für das Löschen) einen Schlüssel für die ausgehende Richtlinie ein. Die Schlüssellänge hängt von dem in Schritt 18 gewählten Algorithmus ab. Die Schlüssellänge hängt von dem in Schritt 18 gewählten Algorithmus ab.

·DES verwendet einen 8-stelligen Schlüssel.

·3DES verwendet einen 24-stelligen Schlüssel.

·AES-128 verwendet einen 12-stelligen Schlüssel.

·AES-192 verwendet einen 24-stelligen Schlüssel.

·AES-256 verwendet einen 32-stelligen Schlüssel.

Schritt 21: Wählen Sie in der Dropdown-Liste Integrity Algorithm (Integritätsalgorithmus) eine Option zur Authentifizierung des VPN-Headers.

·MD5 — Message-Digest Algorithm 5 (MD5) verwendet einen 128-Bit-Hashwert für die Authentifizierung. MD5 ist weniger sicher, aber schneller als SHA-1 und SHA2-256.

·SHA-1 - Secure Hash Algorithm 1 (SHA-1) verwendet für die Authentifizierung einen 160-Bit-Hashwert. SHA-1 ist langsamer, aber sicherer als MD5, und SHA-1 ist schneller, aber weniger sicher als SHA2-256.

·SHA2-256 - Secure Hash Algorithm 2 (SHA2-256) verwendet einen 256-Bit-Hash-Wert für die Authentifizierung. SHA2-256 ist langsamer, aber sicherer als MD5 und SHA-1.

Schritt 22: Geben Sie im Feld Key-In (Schlüsseleingabe) einen Schlüssel für die eingehende Richtlinie ein. Die Schlüssellänge hängt vom Algorithmus ab, der in Schritt 21 gewählt wurde.

·MD5 verwendet einen 16-stelligen Schlüssel.

·SHA-1 verwendet einen 20-stelligen Schlüssel.

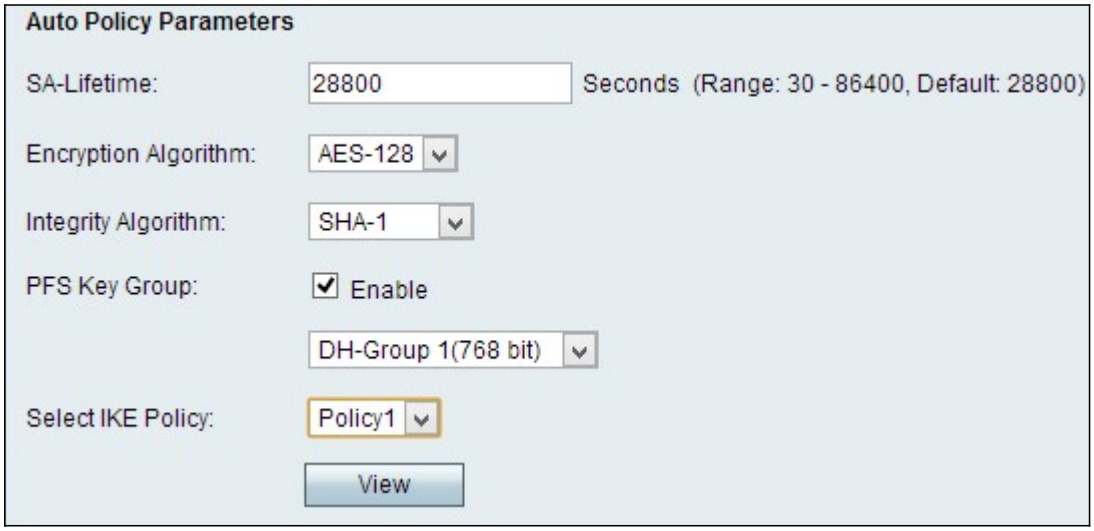
·SHA2-256 verwendet einen 32-stelligen Schlüssel.

Schritt 23: Geben Sie im Feld "Key-Out" (Schlüssel für das Löschen) einen Schlüssel für die ausgehende Richtlinie ein. Die Schlüssellänge hängt vom Algorithmus ab, der in Schritt 21 gewählt wurde. Die Schlüssellänge hängt vom Algorithmus ab, der in Schritt 21 gewählt wurde.

·MD5 verwendet einen 16-stelligen Schlüssel.

·SHA-1 verwendet einen 20-stelligen Schlüssel.

·SHA2-256 verwendet einen 32-stelligen Schlüssel.



Hinweis: Wenn Sie in Schritt 3 die Option "Auto Policy" (Automatische Richtlinie) ausgewählt haben, führen Sie die Schritte 24 bis 29 aus. Fahren Sie andernfalls mit Schritt 31 fort.

Schritt 24: Geben Sie im Feld SA-Lifetime (SA-Lebensdauer) ein, wie lange die SA-Lebensdauer in Sekunden vor der Verlängerung dauert.

Schritt 25: Wählen Sie in der Dropdown-Liste Verschlüsselungsalgorithmus eine Option aus, um die Security Association (SA) auszuhandeln.

·DES - Data Encryption Standard (DES) verwendet eine 56-Bit-Schlüsselgröße für die Datenverschlüsselung. DES ist veraltet und sollte verwendet werden, wenn nur ein Endpunkt DES unterstützt.

·3DES - Der Triple Data Encryption Standard (3DES) führt DES dreimal durch, variiert jedoch die Schlüssellänge zwischen 168 Bit und 112 Bit und zwischen 112 Bit und 56 Bit, je nach der DES-Runde. 3DES ist sicherer als DES und AES.

·AES-128 - Advanced Encryption Standard mit 128-Bit-Schlüssel (AES-128) verwendet einen 128-Bit-Schlüssel für AES-Verschlüsselung. AES ist schneller und sicherer als DES. Einige Hardwaretypen ermöglichen eine schnellere 3DES-Verarbeitung. AES-128 ist schneller, aber weniger sicher als AES-192 und AES-256.

·AES-192 - AES-192 verwendet einen 192-Bit-Schlüssel für die AES-Verschlüsselung. AES-192 ist langsamer, aber sicherer als AES-128, und AES-192 ist schneller, aber weniger sicher als AES-256.

·AES-256 - AES-256 verwendet einen 256-Bit-Schlüssel für die AES-Verschlüsselung. AES-256 ist langsamer, aber sicherer als AES-128 und AES-192.

Schritt 26: Wählen Sie in der Dropdown-Liste Integrity Algorithm (Integritätsalgorithmus) eine Option zur Authentifizierung des VPN-Headers.

·MD5 — Message-Digest Algorithm 5 (MD5) verwendet einen 128-Bit-Hashwert für die Authentifizierung. MD5 ist weniger sicher, aber schneller als SHA-1 und SHA2-256.

·SHA-1 - Secure Hash Algorithm 1 (SHA-1) verwendet für die Authentifizierung einen 160-Bit-Hashwert. SHA-1 ist langsamer, aber sicherer als MD5, und SHA-1 ist schneller, aber weniger sicher als SHA2-256.

·SHA2-256 - Secure Hash Algorithm 2 (SHA2-256) verwendet einen 256-Bit-Hash-Wert für die Authentifizierung. SHA2-256 ist langsamer, aber sicher als MD5 und SHA-1.

Schritt 27: Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld PFS-Schlüsselgruppe, um Perfect Forward Secrecy (PFS) zu aktivieren. PFS erhöht die VPN-Sicherheit, verlangsamt jedoch die Verbindungsgeschwindigkeit.

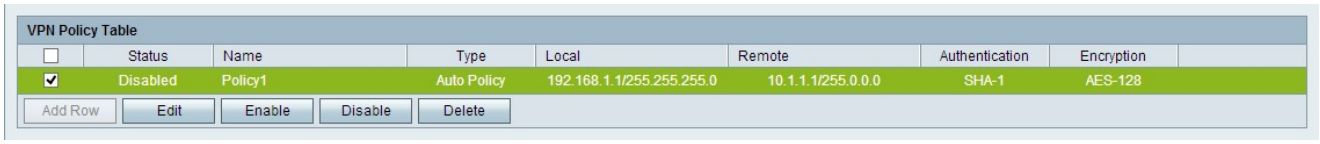
Schritt 28: (Optional) Wenn Sie PFS in Schritt 27 aktiviert haben, wählen Sie in der Dropdown-Liste unterhalb des Felds PFS Key Group (PFS-Schlüsselgruppe) eine Diffie-Hellman (DH)-Gruppe aus, der Sie beitreten möchten. Je höher die Gruppennummer ist, desto sicherer ist die Gruppe.

Schritt 29: Wählen Sie in der Dropdown-Liste Select IKE Policy (IKE-Richtlinie auswählen) aus, welche IKE-Richtlinie für die VPN-Richtlinie verwendet werden soll.

Schritt 30: (Optional) Wenn Sie auf **Ansicht** klicken, werden Sie auf der *Seite* für die *erweiterte VPN-Einrichtung* zum Abschnitt für die IKE-Konfiguration weitergeleitet.

Schritt 31: Klicken Sie auf **Speichern**. Die ursprüngliche Seite *Advanced VPN Setup* wird erneut angezeigt.

Schritt 32: Klicken Sie auf **Speichern**.



Schritt 33: (Optional) Um eine VPN-Richtlinie in der VPN Policy Table zu bearbeiten, aktivieren Sie das Kontrollkästchen für die Richtlinie. Klicken Sie dann auf **Bearbeiten**, bearbeiten Sie die erforderlichen Felder, und klicken Sie auf **Speichern**.

Schritt 34: (Optional) Um eine VPN-Richtlinie in der VPN-Richtlinientabelle zu löschen, aktivieren Sie das Kontrollkästchen für die Richtlinie, klicken Sie auf **Löschen** und klicken Sie dann auf **Speichern**.