

# Configurazione VPN avanzata sul router VPN CVR100W

## Obiettivo

Una rete privata virtuale (VPN) viene utilizzata per connettere gli endpoint di diverse reti tramite una rete pubblica, ad esempio Internet. Questa funzionalità consente agli utenti remoti che non sono connessi a una rete locale di connettersi in modo sicuro alla rete tramite Internet.

Questo articolo spiega come configurare la VPN avanzata sul router VPN CVR100W. Per la configurazione base della VPN, fare riferimento all'articolo [Configurazione base della VPN sul router VPN CVR100W](#).

## Dispositivi interessati

•CVR100W VPN Router

## Versione del software

•1.0.1.19

## Configurazione VPN avanzata

### Impostazioni iniziali

In questa procedura viene illustrato come configurare le impostazioni iniziali dell'installazione VPN avanzata.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **VPN > Advanced VPN Setup**. Viene visualizzata la pagina *Advanced VPN Setup* (Configurazione VPN avanzata):

Advanced VPN Setup

NAT Traversal:  Enable

NETBIOS:  Enable

**IKE Policy Table**

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						

Add Row Edit Delete

**VPN Policy Table**

<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						

Add Row Edit Enable Disable Delete

Save Cancel

IPSec Connection Status

Passaggio 2. (Facoltativo) Per abilitare l'attraversamento NAT (Network Address Translation) per la connessione VPN, selezionare la casella di controllo **Abilita** nel campo Attraversamento NAT. L'attraversamento NAT consente di stabilire una connessione VPN

tra gateway che utilizzano NAT. Scegliere questa opzione se la connessione VPN passa attraverso un gateway abilitato NAT.

Passaggio 3. (Facoltativo) Per abilitare l'invio delle trasmissioni del Network Basic Input/Output System (NetBIOS) tramite la connessione VPN, selezionare la casella di controllo **Abilita** nel campo NETBIOS. NetBIOS consente agli host di comunicare tra loro all'interno di una LAN.

## Impostazioni criteri IKE

IKE (Internet Key Exchange) è un protocollo utilizzato per stabilire una connessione sicura per la comunicazione in una VPN. La connessione protetta stabilita è denominata associazione di protezione (SA, Security Association). In questa procedura viene illustrato come configurare un criterio IKE per la connessione VPN da utilizzare per la sicurezza. Affinché una VPN funzioni correttamente, le policy IKE per entrambi gli endpoint devono essere identiche.

Advanced VPN Setup

NAT Traversal:  Enable

NETBIOS:  Enable

**IKE Policy Table**

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH	
<input type="checkbox"/>	No data to display							
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>						

**VPN Policy Table**

<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>	<input type="button" value="Delete"/>			

Passaggio 1. Nella tabella dei criteri IKE fare clic su **Aggiungi riga** per creare un nuovo criterio IKE. La pagina *Impostazione VPN avanzata* cambia:

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:  ▼

Respondent Mode:  Respondent  
 Auto  Manual

Local ID:  ▼  
 (Hint: 1.2.3.4 or abc.com or @user-defined string or user-defined @ string.)  
 Auto  Manual

Remote ID:  ▼  
 (Hint: 1.2.3.4 or abc.com or @user-defined string or user-defined @ string.)  
 Auto  Manual

Redundancy Remote ID:  ▼  
 (Hint: 1.2.3.4 or abc.com or @user-defined string or user-defined @ string.)

**IKE SA Parameters**

Encryption Algorithm:  ▼

Authentication Algorithm:  ▼

Pre-Shared Key:

Diffie-Hellman (DH) Group:  ▼

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  Seconds (Range: 10 - 999, Default: 10)

DPD Timeout:  Seconds (Range: 30 - 1000, Default: 30)

Passaggio 2. Nel campo Nome criterio immettere un nome per il criterio IKE.

Passaggio 3. Dall'elenco a discesa Modalità di scambio scegliere un'opzione per identificare il funzionamento del criterio IKE.

- Principale: questa opzione consente al criterio IKE di funzionare in modo più sicuro. È più lento della modalità aggressiva. Scegliere questa opzione se è necessaria una connessione VPN più sicura.

- Aggressivo: questa opzione consente alla policy IKE di funzionare più velocemente ma è meno sicura della modalità principale. Scegliere questa opzione se è necessaria una connessione VPN più veloce.

Passaggio 4. (Facoltativo) Per abilitare la modalità Rispondente, selezionare la casella di controllo **Rispondente**. Se la modalità rispondente è abilitata, il router VPN CVR100W può ricevere solo la richiesta VPN dall'endpoint VPN remoto.

Passaggio 5. Nel campo ID locale, fare clic sul pulsante di opzione desiderato per identificare come specificare l'ID locale.

- Auto - Questa opzione assegna automaticamente l'ID locale.

- Manuale - Questa opzione viene utilizzata per assegnare manualmente l'ID locale.

Passaggio 6. (Facoltativo) Dall'elenco a discesa ID locale, scegliere il metodo di identificazione desiderato per la rete locale.

- Indirizzo IP: questa opzione identifica la rete locale tramite un indirizzo IP pubblico.
- FQDN: questa opzione utilizza un nome di dominio completo (FQDN) per identificare la rete locale.

Passaggio 7. (Facoltativo) Nel campo ID locale, immettere l'indirizzo IP o il nome del dominio. La voce dipende dall'opzione scelta al passo 6.

Passaggio 8. Nel campo ID remoto, fare clic sul pulsante di opzione desiderato per identificare come specificare l'ID remoto.

- Auto - Questa opzione assegna automaticamente un ID remoto.
- Manuale - Questa opzione viene utilizzata per assegnare manualmente un ID remoto

Passaggio 9. (Facoltativo) Dall'elenco a discesa ID remoto, scegliere il metodo di identificazione desiderato per la rete remota.

- Indirizzo IP: questa opzione identifica la rete remota tramite un indirizzo IP pubblico.
- FQDN: questa opzione utilizza un nome di dominio completo (FQDN) per identificare la rete remota.

Passaggio 10. (Facoltativo) Nel campo ID remoto, immettere l'indirizzo IP o il nome del dominio. La voce dipende dall'opzione scelta nel passaggio 9.

Passaggio 11. Nel campo ID remoto ridondanza, fare clic sul pulsante di opzione desiderato per identificare come specificare l'ID remoto di ridondanza. L'ID remoto di ridondanza è un ID remoto alternativo utilizzato per configurare il tunnel VPN nel gateway remoto.

- Auto - Questa opzione assegna automaticamente l'ID remoto di ridondanza.
- Manuale - Questa opzione viene utilizzata per assegnare manualmente l'ID remoto di ridondanza.

Passaggio 12. (Facoltativo) Dall'elenco a discesa ID remoto ridondanza, scegliere il metodo di identificazione desiderato per la rete di ridondanza.

- Indirizzo IP: questa opzione identifica la rete remota di ridondanza tramite un indirizzo IP pubblico.
- FQDN: questa opzione utilizza un nome di dominio completo (FQDN) per identificare la rete remota ridondante.

Passaggio 13. (Facoltativo) Nel campo ID remoto ridondanza, immettere l'indirizzo IP o il nome di dominio. La voce dipende dall'opzione scelta al passo 12.

IKE SA Parameters	
Encryption Algorithm:	AES-128 ▼
Authentication Algorithm:	SHA-1 ▼
Pre-Shared Key:	1234abcd
Diffie-Hellman (DH) Group:	Group1 (768 bit) ▼
SA-Lifetime:	3600 Seconds (Range: 30 - 86400, Default: 3600)
Dead Peer Detection:	<input checked="" type="checkbox"/> Enable
DPD Delay:	10 Seconds (Range: 10 - 999, Default: 10)
DPD Timeout:	30 Seconds (Range: 30 - 1000, Default: 30)

Passaggio 14. Dall'elenco a discesa Algoritmo di crittografia, scegliere un'opzione per negoziare l'associazione di sicurezza (SA).

- DES: lo standard DES (Data Encryption Standard) utilizza una chiave a 56 bit per la crittografia dei dati. DES è obsoleto e deve essere utilizzato se un solo endpoint supporta DES.
- 3DES: lo standard 3DES (Triple Data Encryption Standard) esegue il DES tre volte, ma le dimensioni della chiave variano da 168 a 112 bit e da 112 a 56 bit, a seconda dell'arrotondamento di DES eseguito. 3DES è più sicuro di DES e AES.
- AES-128 — Advanced Encryption Standard con chiave a 128 bit (AES-128) utilizza una chiave a 128 bit per la crittografia AES. AES è più veloce e sicuro rispetto a DES. Alcuni tipi di hardware rendono 3DES più veloce. AES-128 è più veloce ma meno sicuro di AES-192 e AES-256.
- AES-192 - AES-192 utilizza una chiave a 192 bit per la crittografia AES. AES-192 è più lento ma più sicuro di AES-128 e AES-192 è più veloce ma meno sicuro di AES-256.
- AES-256 - AES-256 utilizza una chiave a 256 bit per la crittografia AES. AES-256 è più lento ma più sicuro di AES-128 e AES-192.

Passaggio 15. Dall'elenco a discesa Authentication Algorithm (Algoritmo di autenticazione), scegliere un'opzione per autenticare l'installazione VPN.

- MD5 — Message-Digest Algorithm 5 (MD5) utilizza un valore hash a 128 bit per l'autenticazione. MD5 è meno sicuro ma più veloce di SHA-1 e SHA2-256.
- SHA-1: SHA-1 (Secure Hash Algorithm 1) utilizza un valore hash a 160 bit per l'autenticazione. SHA-1 è più lento ma più sicuro di MD5 e SHA-1 è più veloce ma meno sicuro di SHA2-256.
- SHA2-256 — Secure Hash Algorithm 2 (SHA2-256) utilizza un valore hash a 256 bit per l'autenticazione. SHA2-256 è più lento ma sicuro di MD5 e SHA-1.

Passaggio 16. Nel campo Chiave già condivisa immettere una chiave già condivisa utilizzata dal criterio IKE.

Passaggio 17. Dall'elenco a discesa Gruppo Diffie-Hellman (DH), scegliere il gruppo DH utilizzato da IKE. Gli host di un gruppo DH possono scambiarsi le chiavi senza essere a conoscenza gli uni degli altri. Più alto è il numero di bit del gruppo, più sicuro è il gruppo.

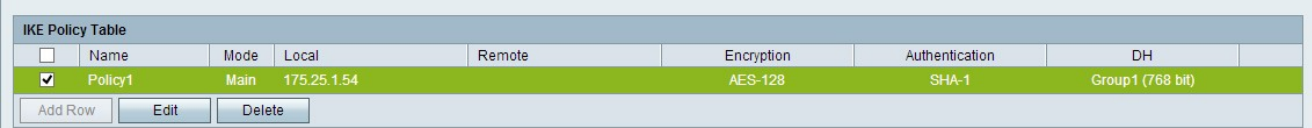
Passaggio 18. Nel campo Durata SA, immettere la durata (in secondi) dell'associazione di sicurezza (SA) per la VPN prima del rinnovo dell'SA.

Passaggio 19. (Facoltativo) Per abilitare Dead Peer Detection (DPD), selezionare la casella di controllo **Enable** nel campo Dead Peer Detection. DPD viene utilizzato per monitorare i peer IKE per verificare se un peer non funziona più. La DPD impedisce lo spreco di risorse di rete su peer inattivi.

Passaggio 20. (Facoltativo) Per indicare la frequenza con cui il peer viene controllato per l'attività, immettere l'intervallo di tempo (in secondi) nel campo Ritardo DPD. Questa opzione è disponibile se DPD è abilitato nel passaggio 19.

Passaggio 21. (Facoltativo) Per indicare il tempo di attesa prima che un peer inattivo venga eliminato, immettere il tempo di attesa (in secondi) nel campo Timeout DPD. Questa opzione è disponibile se DPD è abilitato nel passo 19.

Passaggio 2. Fare clic su **Salva**. Viene visualizzata nuovamente la pagina originale *Advanced VPN Setup*.



<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input checked="" type="checkbox"/>	Policy1	Main	175.25.1.54		AES-128	SHA-1	Group1 (768 bit)

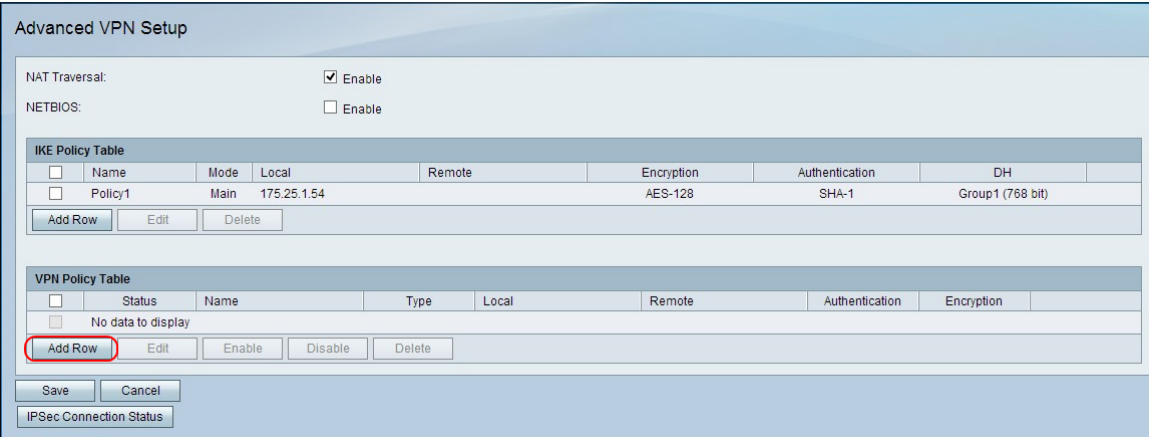
Buttons: Add Row, Edit, Delete

Passaggio 23. (Facoltativo) Per modificare un criterio IKE nella tabella dei criteri IKE, selezionare la casella di controllo corrispondente al criterio. Quindi fare clic su **Modifica**, modificare i campi obbligatori e fare clic su **Salva**.

Passaggio 24. (Facoltativo) Per eliminare un criterio IKE nella tabella dei criteri IKE, selezionare la casella di controllo relativa al criterio e fare clic su **Elimina**. Quindi fare clic su **Salva**.

## Impostazioni criteri VPN

In questa procedura viene illustrato come configurare un criterio VPN per la connessione VPN da utilizzare. Affinché una VPN funzioni correttamente, i criteri VPN per entrambi gli endpoint devono essere identici.



Advanced VPN Setup

NAT Traversal:  Enable

NETBIOS:  Enable

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	Policy1	Main	175.25.1.54		AES-128	SHA-1	Group1 (768 bit)

Buttons: Add Row, Edit, Delete

<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						

Buttons: Add Row, Edit, Enable, Disable, Delete

Buttons: Save, Cancel

IPSec Connection Status

Passaggio 1. Nella tabella Criteri VPN, fare clic su **Aggiungi riga** per creare un nuovo criterio VPN. La pagina *Impostazione VPN avanzata* cambia:

### Advanced VPN Setup

**Add / Edit VPN Policy Configuration**

Policy Name:

Policy Type:

Remote Endpoint:   (Hint: 1.2.3.4 or abc.com)

Redundancy Endpoint:  Enable   (Hint: 1.2.3.4 or abc.com)

Rollback enable

**Local Traffic Selection**

Local IP:

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

**Remote Traffic Selection**

Remote IP:

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

**Auto Policy Parameters**

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

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group:  Enable

Select IKE Policy:

**Add / Edit VPN Policy Configuration**

Policy Name:

Policy Type:  ▼

Remote Endpoint:  ▼

(Hint: 1.2.3.4 or abc.com)

Redundancy Endpoint:  Enable

▼

(Hint: 1.2.3.4 or abc.com)

Rollback enable

Passaggio 2. Nel campo Nome criterio, immettere un nome per il criterio VPN.

Passaggio 3. Dall'elenco a discesa Tipo di criterio, scegliere un'opzione per identificare la modalità di generazione delle impostazioni del tunnel VPN.

- Criterio manuale - Questa opzione consente di configurare le chiavi per la crittografia e l'integrità dei dati.
- Criteri automatici: questa opzione utilizza criteri IKE per l'integrità dei dati e gli scambi di chiavi di crittografia.

Passaggio 4. Dall'elenco a discesa Remote Endpoint, scegliere un'opzione per specificare come assegnare manualmente l'ID remoto.

- Indirizzo IP: questa opzione identifica la rete remota tramite un indirizzo IP pubblico.
- FQDN: questa opzione utilizza un nome di dominio completo (FQDN) per identificare la rete remota.

Passaggio 5. Nel campo di immissione testo sotto l'elenco a discesa Remote Endpoint, immettere l'indirizzo IP pubblico o il nome di dominio dell'indirizzo remoto.

Passaggio 6. (Facoltativo) Per abilitare la ridondanza, selezionare la casella di controllo **Abilita** nel campo Endpoint ridondanza. L'opzione endpoint ridondanza consente al router VPN CVR100W di connettersi a un endpoint VPN di backup quando la connessione VPN primaria non riesce.

Passaggio 7. (Facoltativo) Per assegnare manualmente l'ID di ridondanza, scegliere un'opzione dall'elenco a discesa Endpoint ridondanza.

- Indirizzo IP: questa opzione identifica la rete remota di ridondanza tramite un indirizzo IP pubblico.
- FQDN: questa opzione utilizza un nome di dominio completo (FQDN) per identificare la rete remota ridondante.

Passaggio 8. (Facoltativo) Per immettere l'indirizzo di ridondanza, nel campo di immissione testo sotto l'elenco a discesa Endpoint di ridondanza, immettere l'indirizzo IP pubblico o il nome di dominio.



Passaggio 9. (Facoltativo) Per abilitare il rollback, selezionare la casella di controllo **Abilita rollback**. Questa opzione abilita il passaggio automatico dalla connessione VPN di backup alla connessione VPN primaria quando la connessione VPN primaria viene ripristinata da un errore.

Local Traffic Selection		
Local IP:	<input type="text" value="Subnet"/>	
IP Address:	<input type="text" value="192.168.1.1"/>	(Hint: 1.2.3.4)
Subnet Mask:	<input type="text" value="255.255.255.0"/>	(Hint: 255.255.255.0)
Remote Traffic Selection		
Remote IP:	<input type="text" value="Subnet"/>	
IP Address:	<input type="text" value="10.1.1.1"/>	(Hint: 1.2.3.4)
Subnet Mask:	<input type="text" value="255.0.0.0"/>	(Hint: 255.255.255.0)

Passaggio 10. Dall'elenco a discesa IP locale, scegliere un'opzione per identificare gli host interessati dal criterio.

- Singolo: questa opzione utilizza un singolo host come punto di connessione VPN locale.
- Subnet: questa opzione utilizza una subnet della rete locale come punto di connessione VPN locale.

Passaggio 11. Nel campo Indirizzo IP, immettere l'indirizzo IP dell'host o della subnet locale.

Passaggio 12. (Facoltativo) Se nel passaggio 10 è stata scelta l'opzione Subnet mask, immettere la subnet mask per la subnet locale nel campo Subnet mask.

Passaggio 13. Dall'elenco a discesa IP remoto, scegliere un'opzione per identificare gli host interessati dal criterio.

- Singolo: questa opzione utilizza un singolo host come punto di connessione VPN remota.
- Subnet: questa opzione utilizza una subnet della rete remota come punto di connessione VPN remota.

Passaggio 14. Nel campo Indirizzo IP, immettere l'indirizzo IP dell'host o della subnet remota.

Passaggio 15. (Facoltativo) Se si sceglie l'opzione Subnet nel passaggio 13, immettere la subnet mask per la subnet remota nel campo Subnet mask.

Manual Policy Parameters	
SPI-Incoming:	<input type="text" value="0xABCD"/>
SPI-Outgoing:	<input type="text" value="0x1234"/>
Encryption Algorithm:	<input type="text" value="AES-128"/> ▼
Key-In:	<input type="text" value="12345678ABCDE"/>
Key-Out:	<input type="text" value="12345678ABCDE"/>
Integrity Algorithm:	<input type="text" value="SHA-1"/> ▼
Key-In:	<input type="text" value="12345678ABCD"/>
Key-Out:	<input type="text" value="12345678ABCD"/>

**Nota:** Se nel passo 3 è stata scelta l'opzione Criteri manuali, eseguire i passi da 16 a 23; in caso contrario, andare al [passo 24](#).

Passaggio 16. Nel campo SPI-Incoming, immettere da tre a otto caratteri esadecimali per il tag Security Parameter Index (SPI) per il traffico in entrata sulla connessione VPN. Il tag SPI viene utilizzato per distinguere il traffico di una sessione dal traffico di altre sessioni. Il SPI in entrata su un lato del tunnel deve essere il SPI in uscita sull'altro lato del tunnel.

Passaggio 17. Nel campo SPI-In uscita, immettere da tre a otto caratteri esadecimali per il tag SPI per il traffico in uscita sulla connessione VPN. Il tag SPI viene utilizzato per distinguere il traffico di una sessione dal traffico di altre sessioni. L'indice SPI in uscita su un lato del tunnel deve essere l'indice SPI in entrata sull'altro lato del tunnel.

Passaggio 18. Dall'elenco a discesa Algoritmo di crittografia, scegliere un'opzione per negoziare l'associazione di sicurezza (SA).

- DES: lo standard DES (Data Encryption Standard) utilizza una chiave a 56 bit per la crittografia dei dati. DES è obsoleto e deve essere utilizzato se un solo endpoint supporta DES.
- 3DES: lo standard 3DES (Triple Data Encryption Standard) esegue il DES tre volte, ma le dimensioni della chiave variano da 168 a 112 bit e da 112 a 56 bit, a seconda dell'arrotondamento di DES eseguito. 3DES è più sicuro di DES e AES.
- AES-128 — Advanced Encryption Standard con chiave a 128 bit (AES-128) utilizza una chiave a 128 bit per la crittografia AES. AES è più veloce e più sicuro di DES. Alcuni tipi di hardware consentono a 3DES di essere più veloce. AES-128 è più veloce ma meno sicuro di AES-192 e AES-256.
- AES-192 - AES-192 utilizza una chiave a 192 bit per la crittografia AES. AES-192 è più lento ma più sicuro di AES-128 e AES-192 è più veloce ma meno sicuro di AES-256.
- AES-256 - AES-256 utilizza una chiave a 256 bit per la crittografia AES. AES-256 è più lento ma più sicuro di AES-128 e AES-192.

Passaggio 19. Nel campo Chiave in ingresso, immettere una chiave per il criterio in ingresso. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 18.

- DES utilizza un tasto a 8 caratteri.
- 3DES utilizza un tasto di 24 caratteri.
- AES-128 utilizza un tasto di 12 caratteri.
- AES-192 utilizza un tasto di 24 caratteri.
- AES-256 utilizza un tasto di 32 caratteri.

Passaggio 20. Nel campo Esclusione, immettere una chiave per il criterio in uscita. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 18. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 18.

- DES utilizza un tasto a 8 caratteri.
- 3DES utilizza un tasto di 24 caratteri.
- AES-128 utilizza un tasto di 12 caratteri.
- AES-192 utilizza un tasto di 24 caratteri.
- AES-256 utilizza un tasto di 32 caratteri.

Passaggio 21. Dall'elenco a discesa Integrity Algorithm, scegliere un'opzione per autenticare l'intestazione VPN.

- MD5 — Message-Digest Algorithm 5 (MD5) utilizza un valore hash a 128 bit per l'autenticazione. MD5 è meno sicuro ma più veloce rispetto a SHA-1 e SHA2-256.
- SHA-1: SHA-1 (Secure Hash Algorithm 1) utilizza un valore hash a 160 bit per l'autenticazione. SHA-1 è più lento ma più sicuro di MD5 e SHA-1 è più veloce ma meno sicuro di SHA2-256.
- SHA2-256 — Secure Hash Algorithm 2 (SHA2-256) utilizza un valore hash a 256 bit per l'autenticazione. SHA2-256 è più lento ma più sicuro di MD5 e SHA-1.

Passaggio 22. Nel campo Chiave in ingresso, immettere una chiave per il criterio in ingresso. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 21.

- MD5 utilizza un tasto a 16 caratteri.
- SHA-1 utilizza un tasto a 20 caratteri.
- SHA2-256 utilizza un tasto a 32 caratteri.

Passaggio 23. Nel campo Esclusione, immettere una chiave per il criterio in uscita. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 21. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 21.

- MD5 utilizza un tasto a 16 caratteri.
- SHA-1 utilizza un tasto a 20 caratteri.
- SHA2-256 utilizza un tasto a 32 caratteri.

**Auto Policy Parameters**

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

Encryption Algorithm:  ▼

Integrity Algorithm:  ▼

PFS Key Group:  Enable

▼

Select IKE Policy:  ▼

**Nota:** Se nel passo 3 è stata scelta l'opzione Criteri automatici, eseguire i passi da 24 a 29; in caso contrario, andare al [passo 31](#).

Passaggio 24. Nel campo Durata SA immettere il numero di secondi che devono trascorrere prima del rinnovo dell'associazione di protezione.

Passaggio 25. Dall'elenco a discesa Algoritmo di crittografia, scegliere un'opzione per negoziare l'associazione di sicurezza (SA).

- DES: lo standard DES (Data Encryption Standard) utilizza una chiave a 56 bit per la crittografia dei dati. DES è obsoleto e deve essere utilizzato se un solo endpoint supporta DES.
- 3DES: lo standard 3DES (Triple Data Encryption Standard) esegue il DES tre volte, ma le dimensioni della chiave variano da 168 a 112 bit e da 112 a 56 bit, a seconda dell'arrotondamento di DES eseguito. 3DES è più sicuro di DES e AES.
- AES-128 — Advanced Encryption Standard con chiave a 128 bit (AES-128) utilizza una chiave a 128 bit per la crittografia AES. AES è più veloce e sicuro rispetto a DES. Alcuni tipi di hardware rendono 3DES più veloce. AES-128 è più veloce ma meno sicuro di AES-192 e AES-256.
- AES-192 - AES-192 utilizza una chiave a 192 bit per la crittografia AES. AES-192 è più lento ma più sicuro di AES-128 e AES-192 è più veloce ma meno sicuro di AES-256.
- AES-256 - AES-256 utilizza una chiave a 256 bit per la crittografia AES. AES-256 è più lento ma più sicuro di AES-128 e AES-192.

Passaggio 26. Dall'elenco a discesa Integrity Algorithm, scegliere un'opzione per autenticare l'intestazione VPN.

- MD5 — Message-Digest Algorithm 5 (MD5) utilizza un valore hash a 128 bit per l'autenticazione. MD5 è meno sicuro ma più veloce rispetto a SHA-1 e SHA2-256.
- SHA-1: SHA-1 (Secure Hash Algorithm 1) utilizza un valore hash a 160 bit per l'autenticazione. SHA-1 è più lento ma più sicuro di MD5 e SHA-1 è più veloce ma meno sicuro di SHA2-256.
- SHA2-256 — Secure Hash Algorithm 2 (SHA2-256) utilizza un valore hash a 256 bit per

l'autenticazione. SHA2-256 è più lento ma sicuro di MD5 e SHA-1.

Passaggio 27. Selezionare la casella di controllo **Abilita** nel campo Gruppo di chiavi PFS per abilitare PFS (Perfect Forward Secrecy). PFS aumenta la sicurezza della VPN, ma rallenta la velocità di connessione.

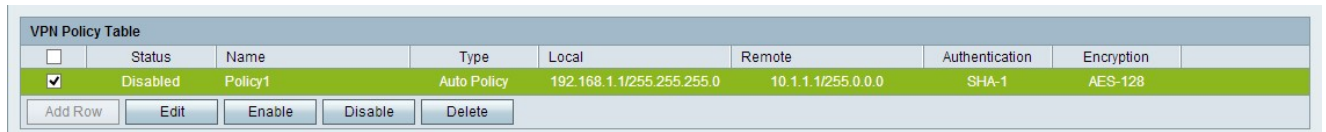
Passaggio 28. (Facoltativo) Se si è scelto di abilitare PFS nel passaggio 27, scegliere un gruppo Diffie-Hellman (DH) da aggiungere dall'elenco a discesa sotto il campo Gruppo di chiavi PFS. Maggiore è il numero di gruppo, più il gruppo è sicuro.

Passaggio 29. Dall'elenco a discesa Seleziona criterio IKE scegliere il criterio IKE da utilizzare per il criterio VPN.

Passaggio 30. (Facoltativo) Se si fa clic su **Visualizza**, si viene indirizzati alla sezione Configurazione IKE della pagina *Configurazione VPN avanzata*.

Passaggio 31. Fare clic su **Salva**. Viene visualizzata nuovamente la pagina originale *Advanced VPN Setup*.

Passaggio 32. Fare clic su **Salva**.



VPN Policy Table								
<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption	
<input checked="" type="checkbox"/>	Disabled	Policy1	Auto Policy	192.168.1.1/255.255.255.0	10.1.1.1/255.0.0.0	SHA-1	AES-128	

Buttons: Add Row, Edit, Enable, Disable, Delete

Passaggio 3. (Facoltativo) Per modificare un criterio VPN nella tabella Criteri VPN, selezionare la casella di controllo corrispondente. Quindi fare clic su **Modifica**, modificare i campi obbligatori e fare clic su **Salva**.

Passaggio 34. (Facoltativo) Per eliminare un criterio VPN nella tabella Criteri VPN, selezionare la casella di controllo del criterio, fare clic su **Elimina**, quindi su **Salva**.