Configurazione della configurazione VPN (Virtual Private Network) avanzata su un router RV130 o RV130W

Obiettivo

Una VPN (Virtual Private Network) è una connessione protetta stabilita all'interno di una rete o tra reti. Le VPN consentono di isolare il traffico tra host e reti specificati dal traffico di host e reti non autorizzati. Una VPN da sito a sito (da gateway a gateway) connette intere reti tra loro, mantenendo la sicurezza tramite la creazione di un tunnel su un dominio pubblico noto anche come Internet. Ogni sito ha bisogno solo di una connessione locale alla stessa rete pubblica, così risparmiando denaro su lunghe linee affittate private.

Le VPN sono vantaggiose per le aziende in quanto sono altamente scalabili, semplificano la topologia di rete e migliorano la produttività riducendo i tempi e i costi di viaggio per gli utenti remoti.

IKE (Internet Key Exchange) è un protocollo utilizzato per stabilire una connessione sicura per la comunicazione in una VPN. Questa connessione protetta è denominata associazione di protezione (SA, Security Association). È possibile creare criteri IKE per definire i parametri di sicurezza da utilizzare nel processo, ad esempio l'autenticazione del peer, gli algoritmi di crittografia e così via. Affinché una VPN funzioni correttamente, le policy IKE per entrambi gli endpoint devono essere identiche.

In questo articolo viene illustrato come configurare la configurazione VPN avanzata su un router RV130 o RV130W, che descrive le impostazioni dei criteri IKE e dei criteri VPN.

Dispositivi interessati

RV130
RV130W

Versione del software

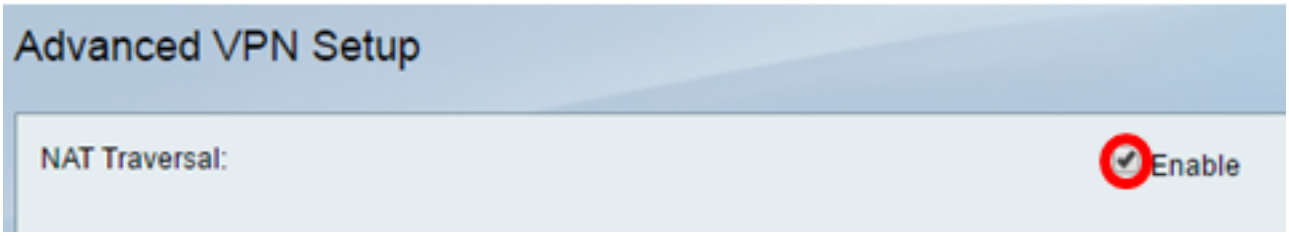
•1.0.3.22

Configura installazione VPN avanzata

Aggiungi/Modifica impostazioni criteri IKE

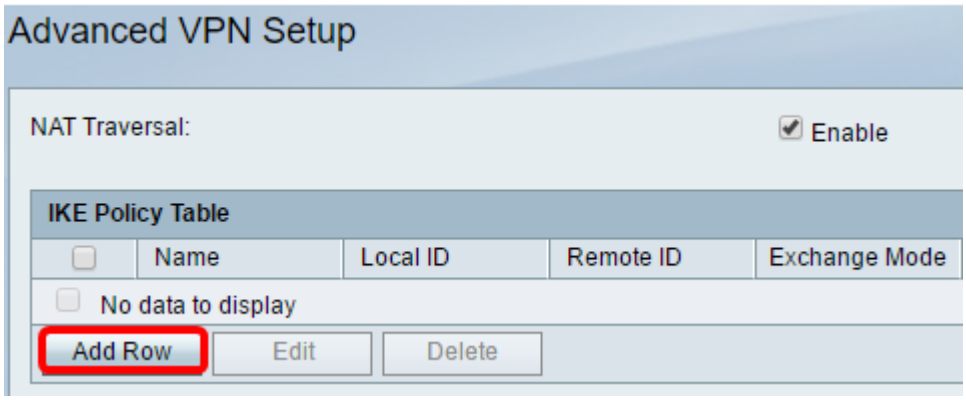
Passaggio 1. Accedere all'utility basata sul Web e scegliere **VPN > IPSec VPN da sito a sito >Advanced VPN Setup**.

Passaggio 2. (Facoltativo) Selezionare la casella di controllo **Abilita** in NAT Traversal per abilitare Network Address Translation (NAT) Traversal per la connessione VPN. NAT Traversal consente di stabilire una connessione VPN tra gateway che utilizzano NAT. Scegliere questa opzione se la connessione VPN passa attraverso un gateway abilitato NAT.



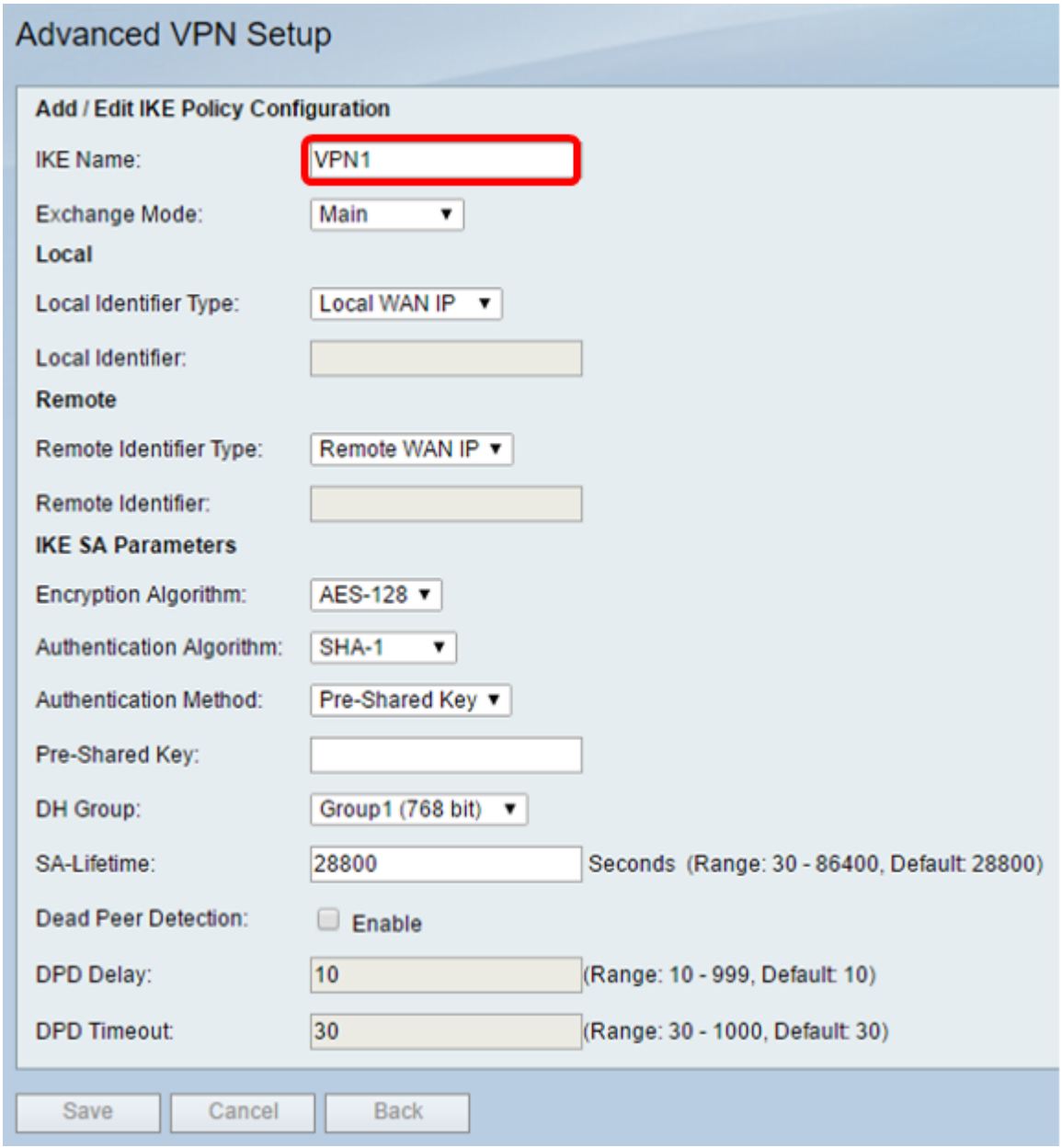
Passaggio 3. Nella tabella dei criteri IKE fare clic su **Aggiungi riga** per creare un nuovo criterio IKE.

Nota: Se sono state configurate le impostazioni di base, la tabella seguente conterrà le impostazioni VPN di base create. È possibile modificare un criterio IKE esistente selezionando la casella di controllo corrispondente al criterio e facendo clic su **Modifica**. La pagina Impostazione VPN avanzata cambia:



Passaggio 4. Nel campo *Nome IKE* immettere un nome univoco per il criterio IKE.

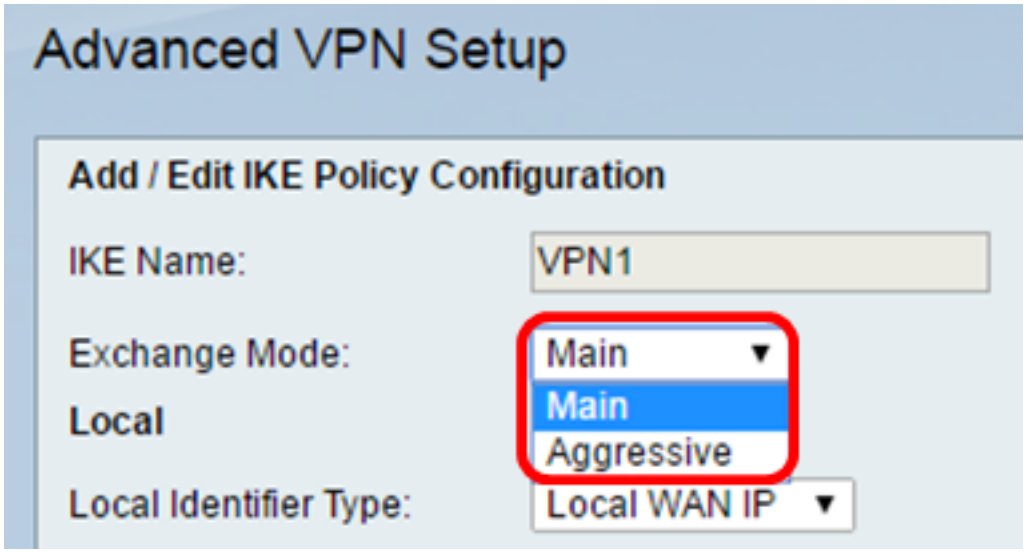
Nota: Se sono state configurate le impostazioni di base, il nome della connessione creata viene impostato come nome IKE. Nell'esempio, il nome IKE scelto è VPN1.



Passaggio 5. Dall'elenco a discesa Modalità scambio, scegliere un'opzione.

- Principale: questa opzione consente al criterio IKE di negoziare il tunnel VPN con un livello di sicurezza superiore rispetto alla modalità aggressiva. Fare clic su questa opzione se una connessione VPN più sicura ha la priorità su una velocità di negoziazione.
- Aggressivo: questa opzione consente al criterio IKE di stabilire una connessione più veloce ma meno sicura rispetto alla modalità principale. Fare clic su questa opzione se una connessione VPN più veloce ha la priorità su una protezione elevata.

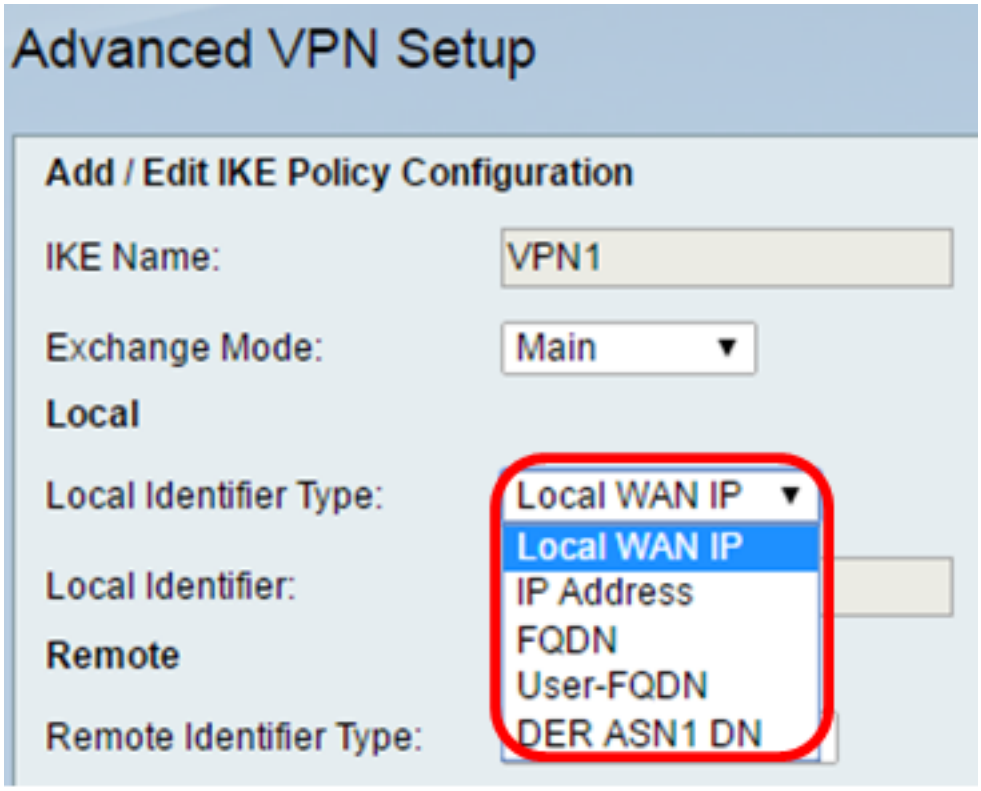
Nota: Nell'esempio viene scelto Principale.



Passaggio 6. Selezionare un'opzione dall'elenco a discesa Local Identifier Type per identificare o specificare l'ISAKMP (Internet Security Association and Key Management Protocol) del router locale. Le opzioni sono:

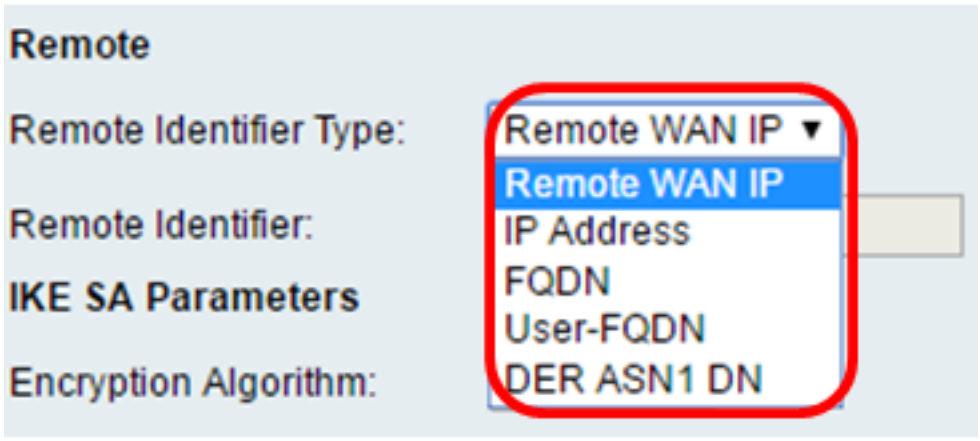
- IP WAN locale: il router utilizza l'IP della WAN (Wide Area Network) locale come identificatore principale. Questa opzione consente la connessione tramite Internet. Se si sceglie questa opzione, il campo *Local Identifier* riportato di seguito non sarà disponibile.
- Indirizzo IP: facendo clic su questo pulsante è possibile immettere un indirizzo IP nel campo *Identificatore locale*.
- FQDN: un nome di dominio completo (FQDN) o il nome di dominio, ad esempio http://www.example.com, consente di immettere il nome di dominio o l'indirizzo IP nel campo *Identificatore locale*.
- FQDN utente: questa opzione corrisponde a un indirizzo di posta elettronica dell'utente, ad esempio user@email.com. Immettere un nome di dominio o un indirizzo IP nel campo *Identificatore locale*.
- DN DER ASN1 - Questa opzione è un tipo di identificatore per il nome distinto (DN) che utilizza le regole di codifica distinto Sintassi astratta Notazione uno (DER ASN1) per trasmettere le informazioni. Questo si verifica quando il tunnel VPN è associato a un certificato utente. Se si sceglie questa opzione, immettere un nome di dominio o un indirizzo IP nel campo *Identificatore locale*.

Nota: Nell'esempio, viene scelto Local WAN IP.



Passaggio 7. Selezionare un'opzione dall'elenco a discesa Tipo di identificatore remoto per identificare o specificare l'ISAKMP (Internet Security Association and Key Management Protocol) del router remoto. Le opzioni sono Remote WAN IP, IP Address, FQDN, User FQDN e DER ASN1 DN.

Nota: Nell'esempio, viene scelto Remote WAN IP.



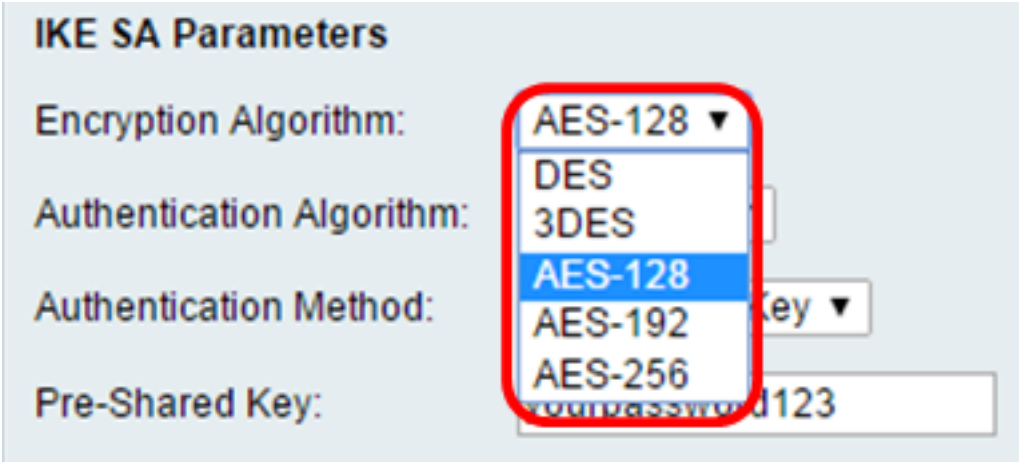
Passaggio 8. Scegliere un'opzione dall'elenco a discesa Algoritmo di crittografia.

- DES — Data Encryption Standard (DES) è un vecchio metodo di crittografia a 56 bit che non è molto sicuro, ma potrebbe essere necessario per garantire la compatibilità con le versioni precedenti.
- 3DES — Triple Data Encryption Standard (3DES) è un semplice metodo di crittografia a 168 bit utilizzato per aumentare le dimensioni della chiave, in quanto i dati vengono crittografati tre volte. Ciò garantisce una maggiore sicurezza rispetto a DES ma una minore sicurezza rispetto a 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. In generale,

AES è anche più veloce e più sicuro di 3DES. AES-128 è l'algoritmo di crittografia predefinito ed 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 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.

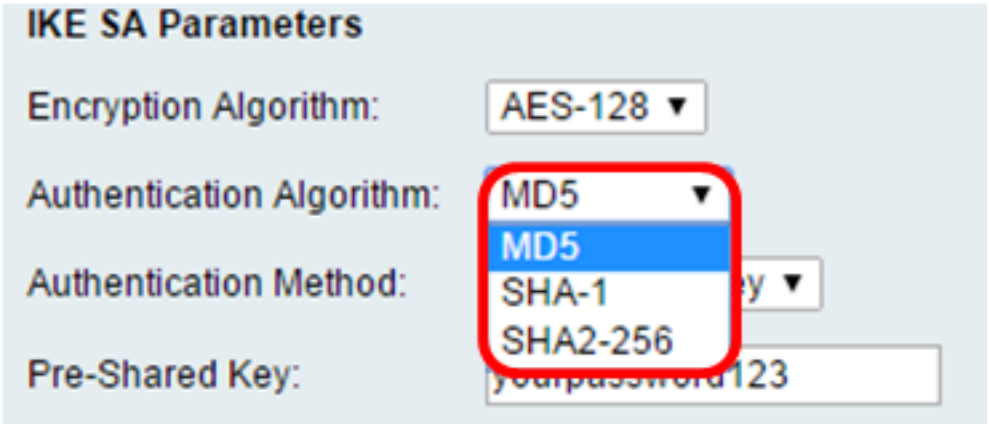
Nota: Nell'esempio, è selezionato AES-128.



Passaggio 9. Dall'elenco a discesa Algoritmo di autenticazione, scegliere una delle seguenti opzioni:

- MD5 — Message Digest 5 (MD5) è un algoritmo di autenticazione che 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: la funzione SHA-1 (Secure Hash Function 1) utilizza un valore hash a 160 bit per l'autenticazione. SHA-1 è più lento ma più sicuro di MD5. SHA-1 è l'algoritmo di autenticazione predefinito ed è più veloce ma meno sicuro di SHA2-256.
- SHA2-256 — L'algoritmo 2 per l'hash sicuro con un valore hash a 256 bit (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.

Nota: In questo esempio, viene scelto MD5.

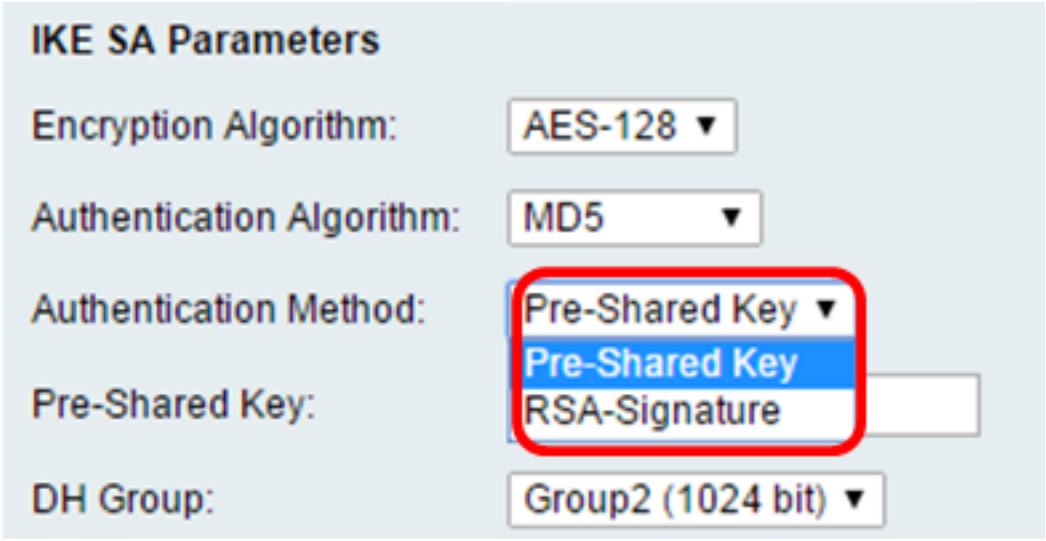


Passaggio 10. Nell'elenco a discesa Metodo di autenticazione scegliere una delle opzioni seguenti:

- Chiave già condivisa - Questa opzione richiede una password condivisa con il peer IKE.
- Firma RSA: questa opzione utilizza i certificati per autenticare la connessione. Se questa

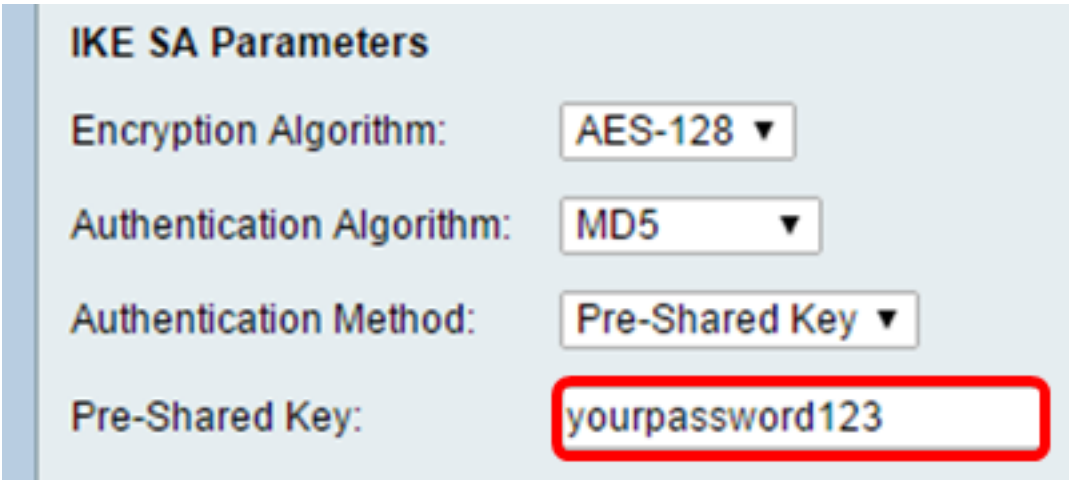
opzione è selezionata, il campo Chiave già condivisa è disattivato. Andare al passo 12.

Nota: In questo esempio viene scelta la chiave già condivisa.



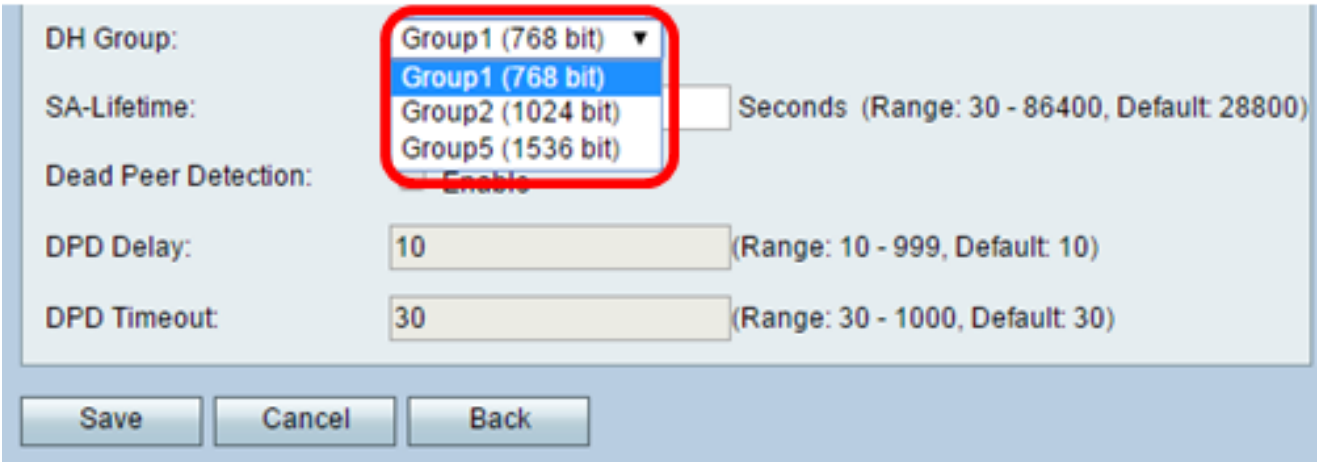
Passaggio 11. Nel campo *Chiave già condivisa*, immettere una password con una lunghezza compresa tra 8 e 49 caratteri.

Nota: Nell'esempio viene utilizzata la password 123.

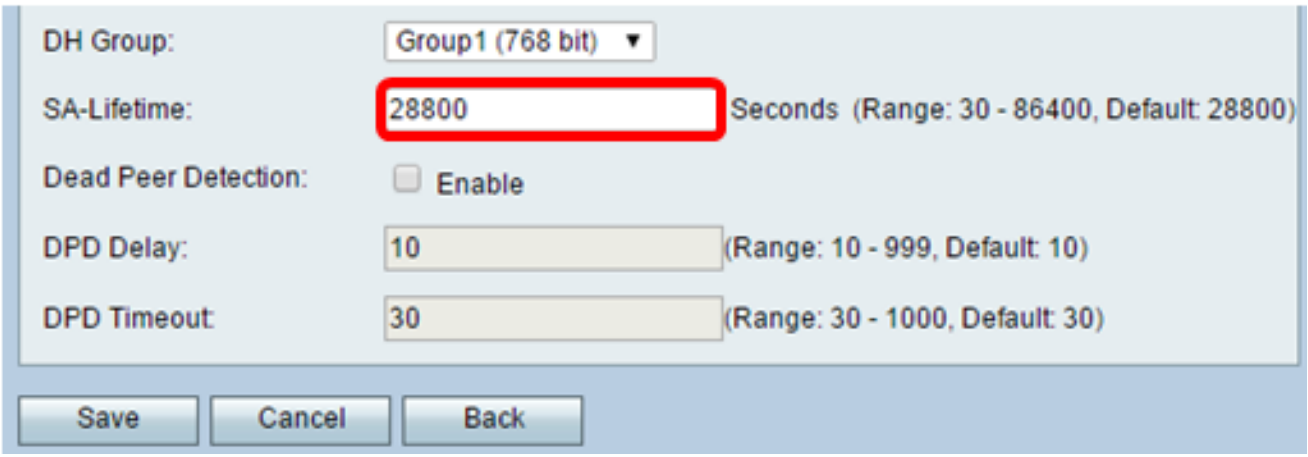


Passaggio 12. Dall'elenco a discesa Gruppo DH, scegliere l'algoritmo di gruppo Diffie-Hellman (DH) utilizzato da IKE. Gli host di un gruppo DH possono scambiare le chiavi senza essere a conoscenza gli uni degli altri. Maggiore è il numero di bit del gruppo, migliore sarà la sicurezza.

Nota: In questo esempio viene scelto Gruppo1.

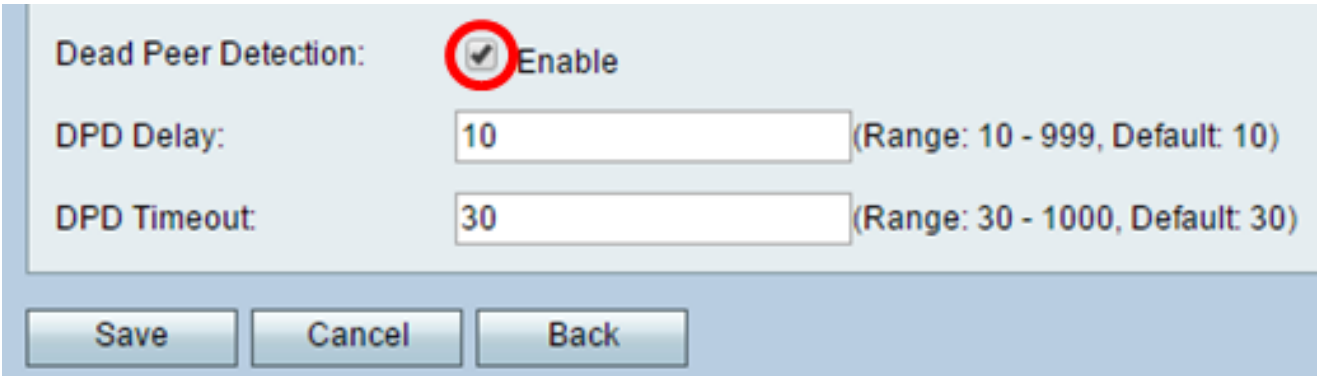


Passaggio 13. Nel campo *SA-Lifetime* (Durata SA), immettere la durata in secondi di un'associazione di sicurezza per la VPN prima che venga rinnovata. L'intervallo è compreso tra 30 e 86400 secondi. Il valore predefinito è 28800.



Passaggio 14. (Facoltativo) Selezionare la casella di controllo **Abilita** rilevamento peer inattivi per abilitare il rilevamento peer inattivi (DPD). Il DPD controlla i peer IKE per verificare se un peer ha smesso di funzionare o è ancora attivo. Se il peer viene rilevato come inattivo, il dispositivo elimina l'associazione di protezione IPsec e IKE. La DPD impedisce lo spreco di risorse di rete su peer inattivi.

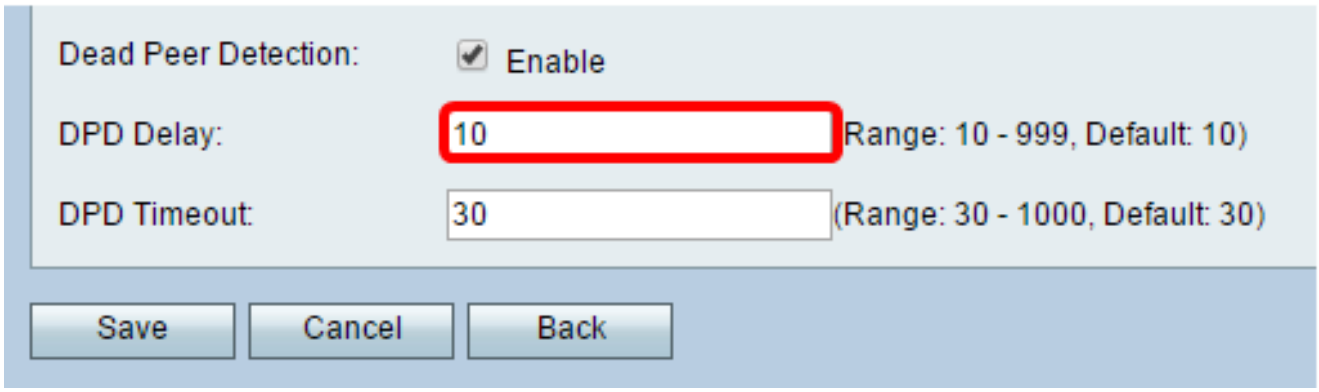
Nota: Se non si desidera abilitare Dead Peer Detection, andare al passo 17.



Passaggio 15. (Facoltativo) Se è stato abilitato DPD nel passaggio 14, immettere la frequenza (in secondi) con cui il peer viene controllato per verificare l'attività nel campo *Ritardo DPD*.

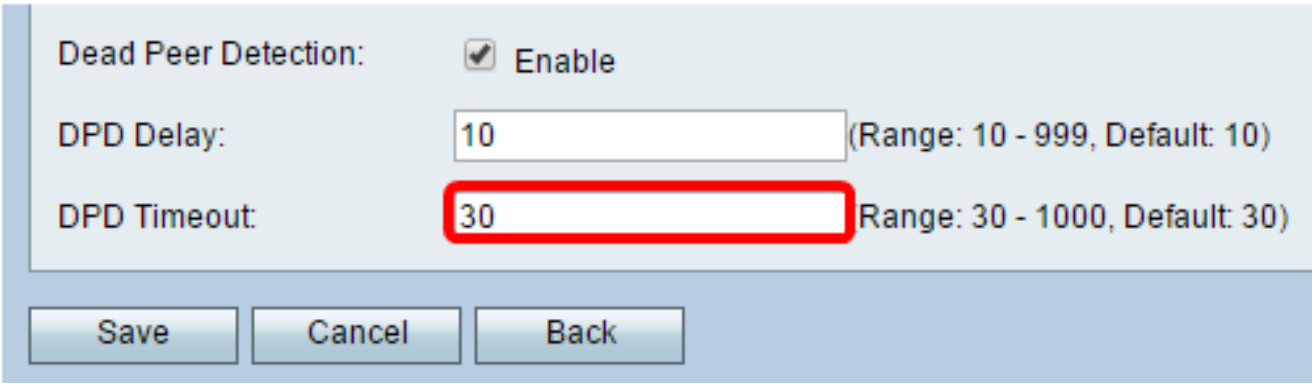
Nota: Il ritardo DPD è l'intervallo in secondi tra i messaggi consecutivi di DPD R-U-LÌ. I

messaggi DPD R-U-THERE vengono inviati solo quando il traffico IPsec è inattivo. Il valore predefinito è 10.

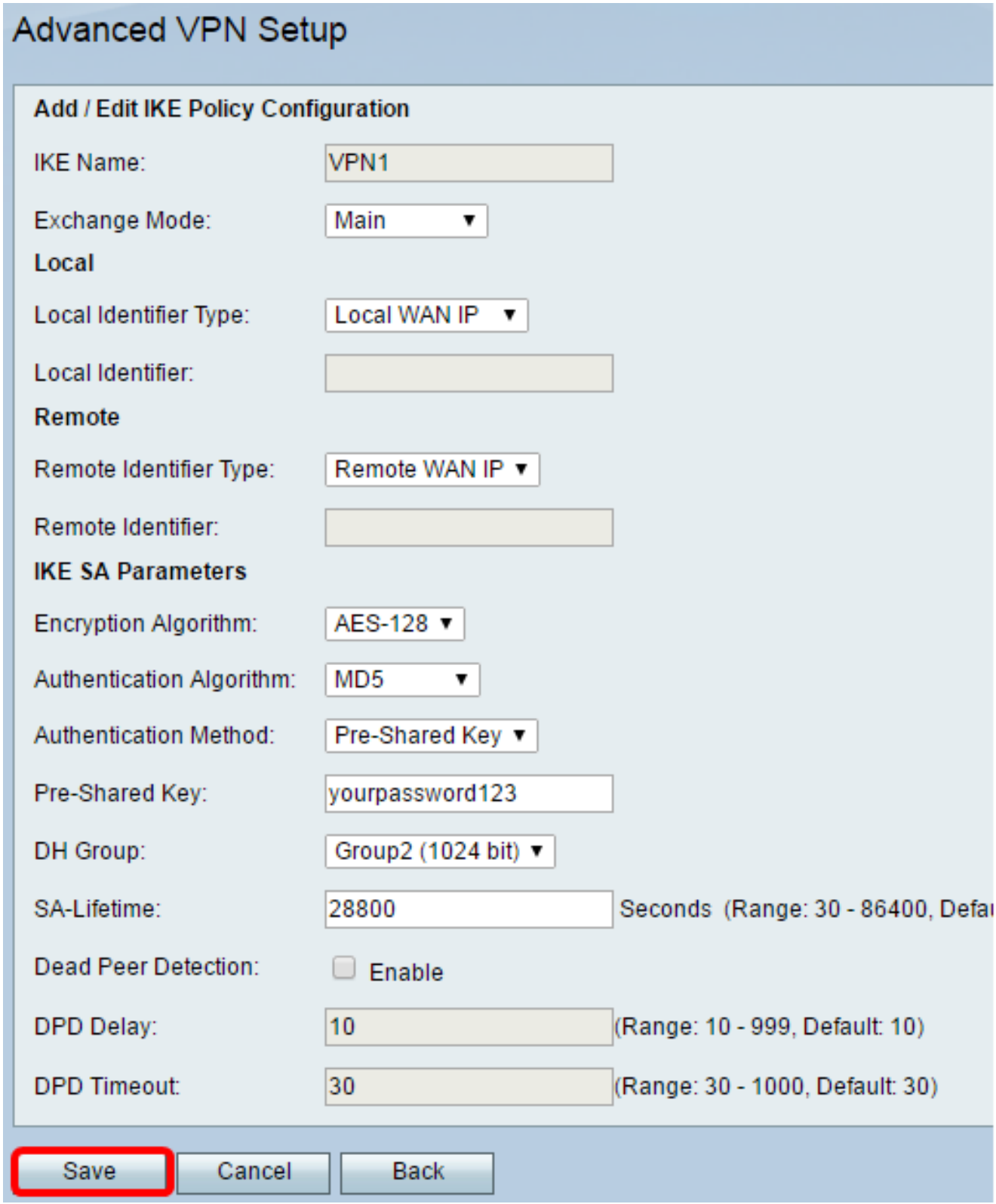


Passaggio 16. (Facoltativo) Se nel passaggio 14 è stato abilitato DPD, immettere il numero di secondi di attesa prima che un peer inattivo venga eliminato nel campo *Timeout DPD*.

Nota: Tempo massimo di attesa del dispositivo per la ricezione di una risposta al messaggio DPD prima che il peer venga considerato inattivo. Il valore predefinito è 30.



Passaggio 17. Fare clic su **Salva**.



Nota: Viene visualizzata di nuovo la pagina Impostazione VPN avanzata.

Èora necessario configurare correttamente le impostazioni dei criteri IKE sul router.

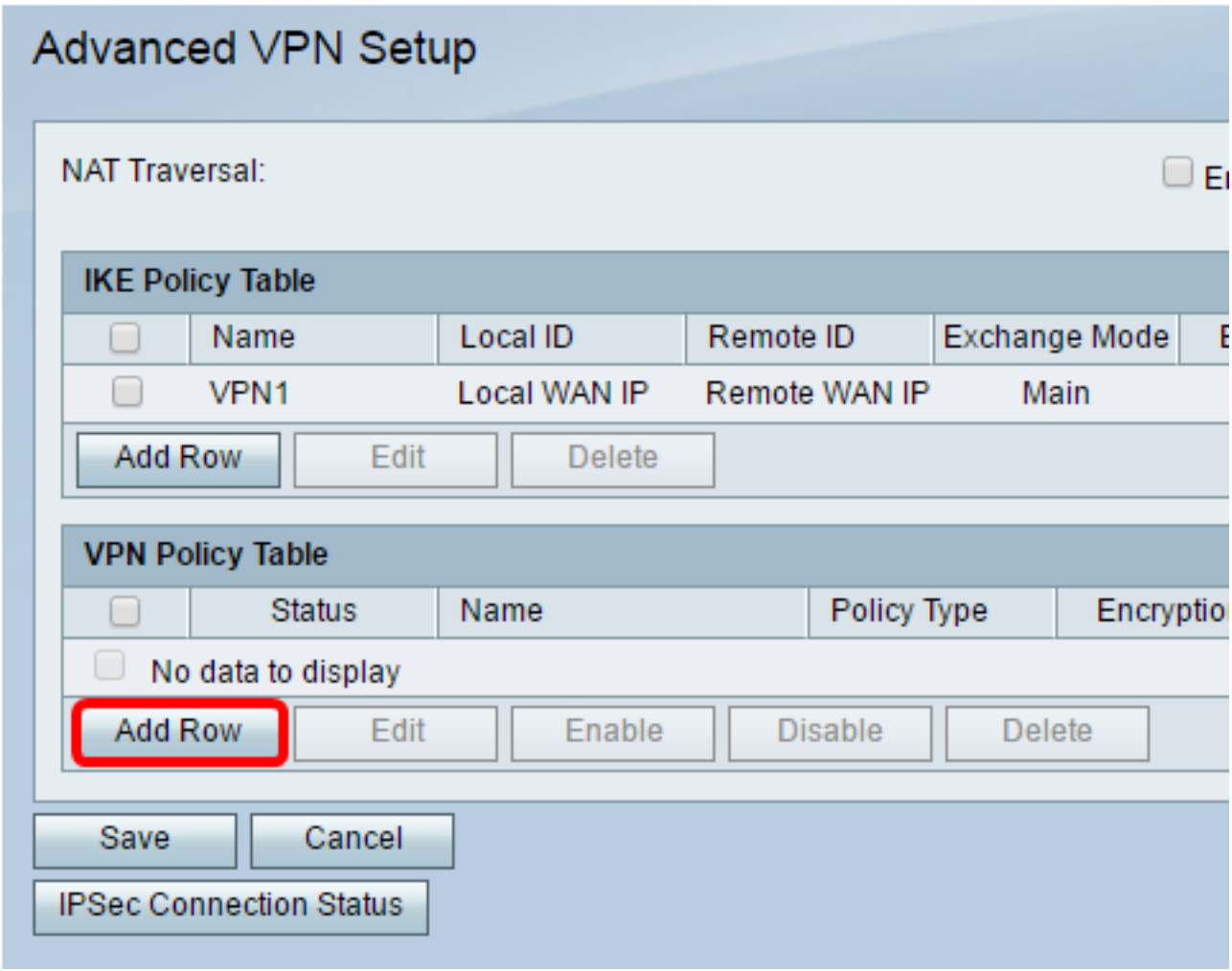
Configura impostazioni criteri VPN

Nota:per il corretto funzionamento di una VPN, i criteri VPN per entrambi gli endpoint devono essere identici.

Passaggio 1. Nella tabella Criteri VPN, fare clic su **Aggiungi riga** per creare un nuovo criterio

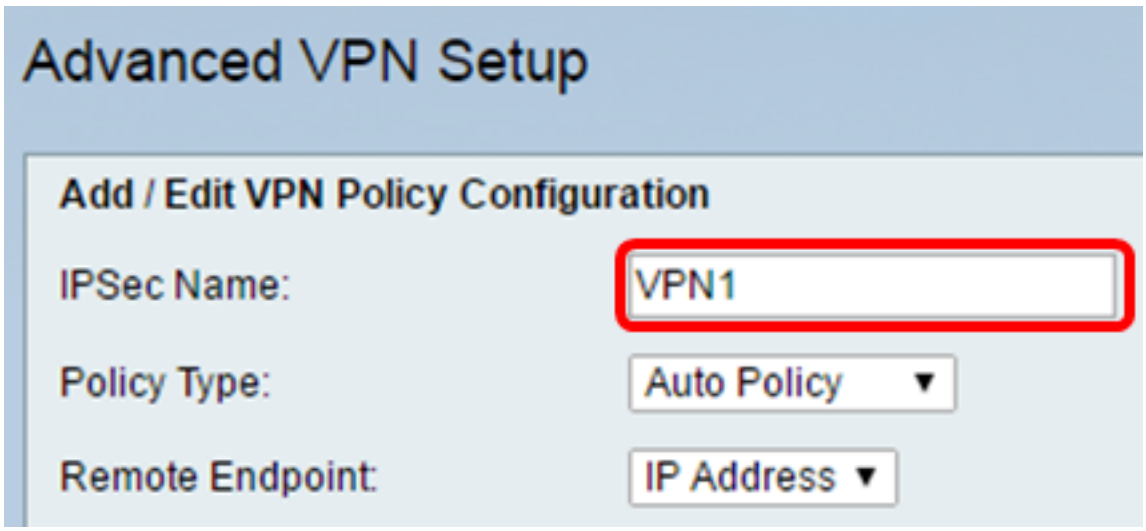
VPN.

Nota: È inoltre possibile modificare un criterio VPN selezionando la relativa casella di controllo e facendo clic su **Modifica**. Viene visualizzata la pagina Configurazione VPN avanzata:



Passaggio 2. Nel campo *IPSec Name* (Nome IPSec) dell'area Add/Edit VPN Configuration (Aggiungi/Modifica configurazione VPN), immettere un nome per il criterio VPN.

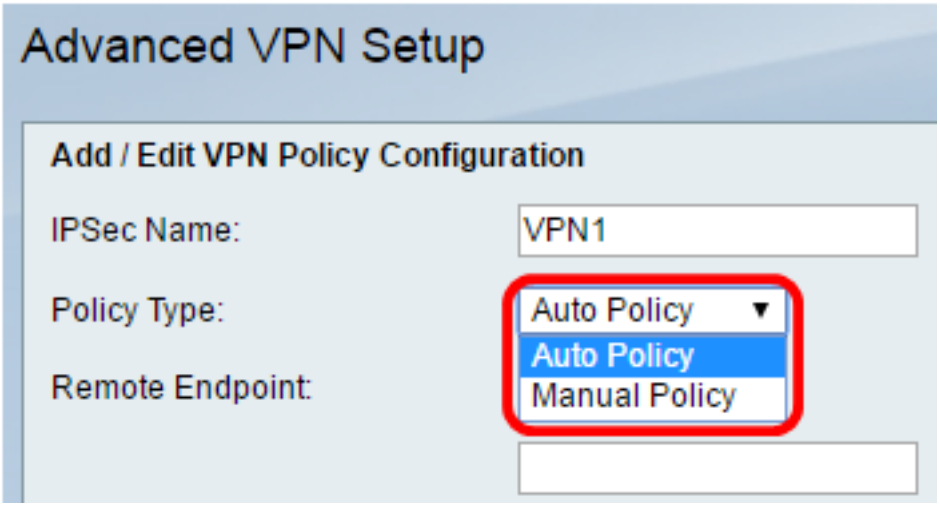
Nota: Nell'esempio viene utilizzato VPN1.



Passaggio 3. Dall'elenco a discesa Tipo di criterio, scegliere un'opzione.

- Criterio manuale - Questa opzione consente di configurare manualmente le chiavi per la crittografia dei dati e l'integrità del tunnel VPN. Se questa opzione è selezionata, le impostazioni di configurazione nell'area Parametri criteri manuali sono attivate. Continuare la procedura fino a Selezione traffico remoto. Fare clic qui per conoscere i passaggi.
- Criteri automatici: i parametri dei criteri vengono impostati automaticamente. Questa opzione utilizza un criterio IKE per l'integrità dei dati e gli scambi di chiavi di crittografia. Se questa opzione è selezionata, le impostazioni di configurazione nell'area Parametri criteri automatici sono attivate. Fare clic qui per conoscere i passaggi. Verificare che il protocollo IKE esegua automaticamente la negoziazione tra i due endpoint VPN.

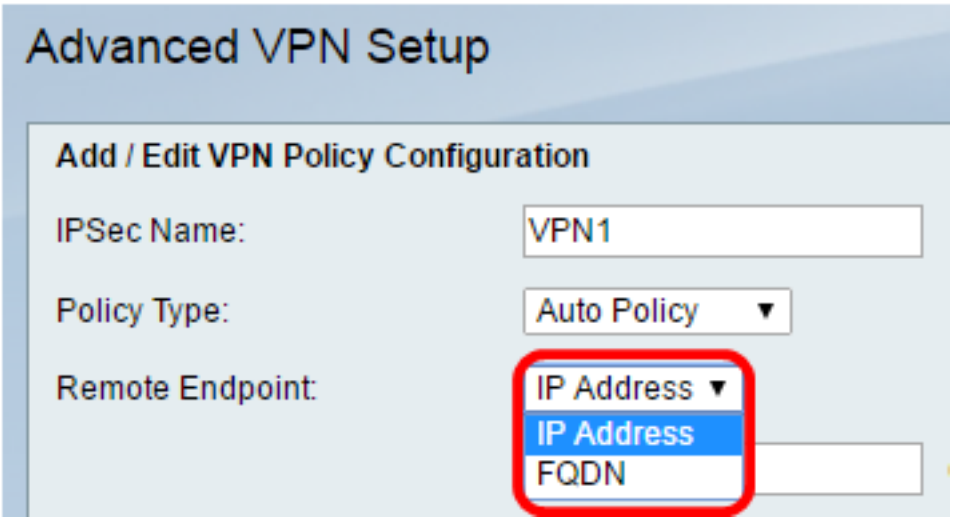
Nota: In questo esempio, viene scelto Criterio automatico.



Passaggio 4. Dall'elenco a discesa Remote Endpoint, scegliere un'opzione.

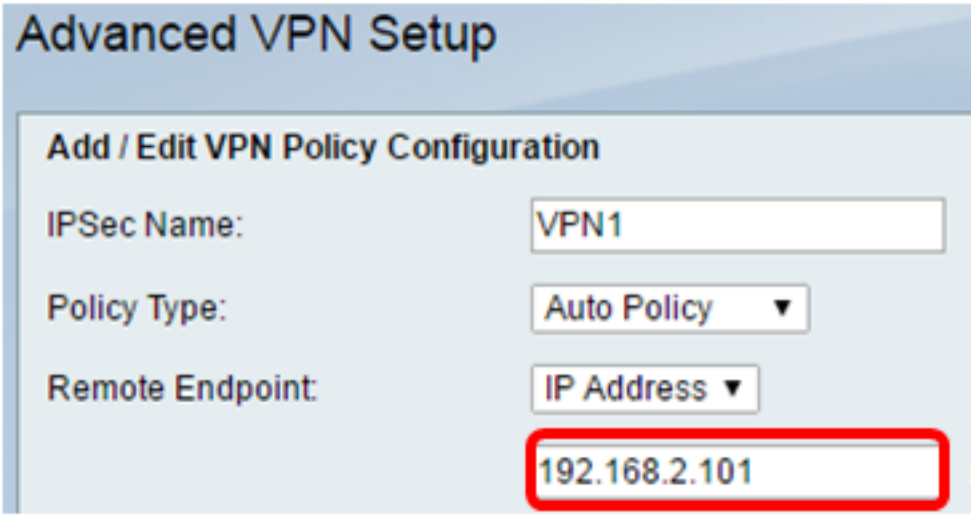
- Indirizzo IP - Questa opzione identifica la rete remota tramite un indirizzo IP pubblico.
- FQDN: nome di dominio completo per un computer, un host o Internet specifico. L'FQDN è costituito da due parti: il nome dell'host e il nome del dominio. Questa opzione può essere abilitata solo quando è selezionata l'opzione **Criteri automatici** nel passo 3.

Nota: Nell'esempio, viene scelto IP Address (Indirizzo IP).



Passaggio 5. Nel campo *Endpoint remoto*, immettere l'indirizzo IP pubblico o il nome di dominio dell'indirizzo remoto.

Nota: nell'esempio viene usato 192.168.2.101.

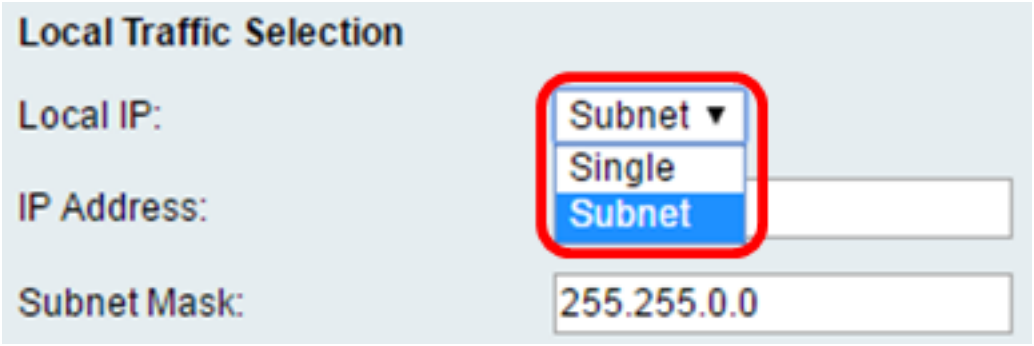


Passaggio 6. (Facoltativo) Selezionare la casella di controllo **NetBios Enabled** per abilitare l'invio delle trasmissioni NetBIOS (Network Basic Input/Output System) tramite la connessione VPN. NetBIOS consente agli host di comunicare tra loro all'interno di una LAN (Local Area Network).

Passaggio 7. Dall'elenco a discesa Local IP nell'area Local Traffic Selection (Selezione traffico locale), selezionare un'opzione.

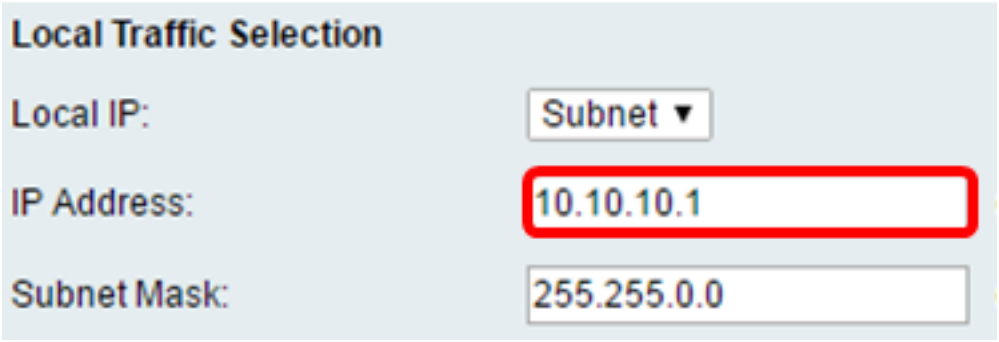
- Singolo — limita il criterio a un host.
- Subnet: consente agli host all'interno di un intervallo di indirizzi IP di connettersi alla VPN.

Nota: Nell'esempio riportato di seguito, viene scelto Subnet.



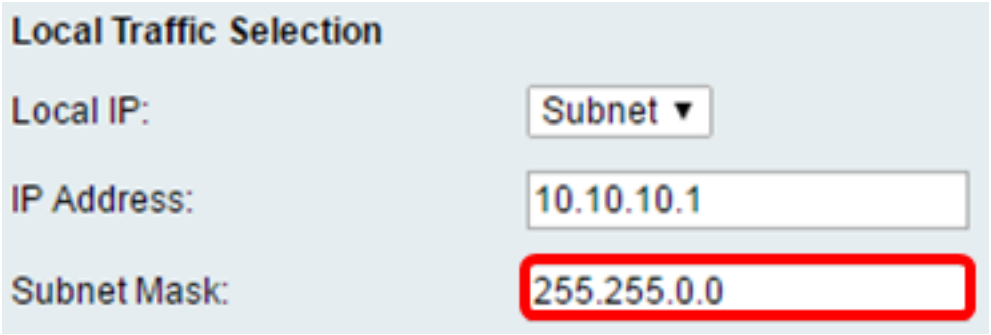
Passaggio 8. Nel campo Indirizzo IP, immettere l'indirizzo IP dell'host o della subnet locale.

Nota: Nell'esempio, viene usato l'indirizzo IP della subnet locale 10.10.10.1.



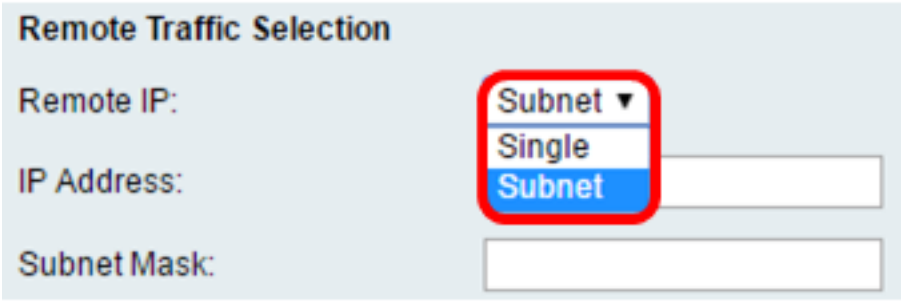
Passaggio 9. (Facoltativo) Se nel Passaggio 7 è selezionato Subnet mask, immettere la subnet mask del client nel Campo *Subnet mask*. Il campo Subnet mask viene disabilitato se si sceglie Single nel passaggio 1.

Nota: Nell'esempio viene usata la subnet mask 255.255.0.0.



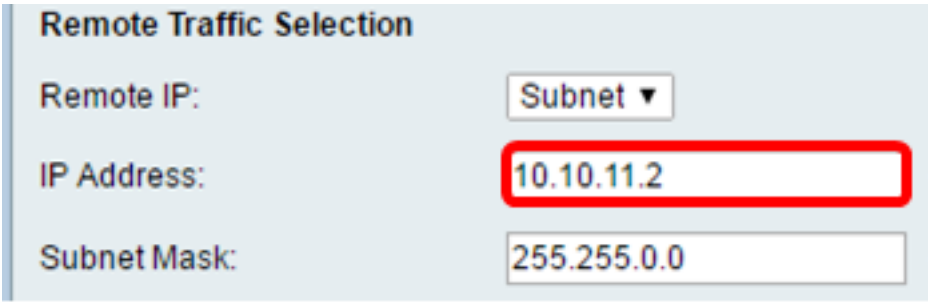
Passaggio 10. Dall'elenco a discesa Remote IP (IP remoto) nell'area Remote Traffic Selection (Selezione traffico remoto), selezionare un'opzione.

- Singolo — limita il criterio a un host.
- Subnet: consente agli host all'interno di un intervallo di indirizzi IP di connettersi alla VPN.
  Nota: Nell'esempio riportato di seguito, viene scelto Subnet.



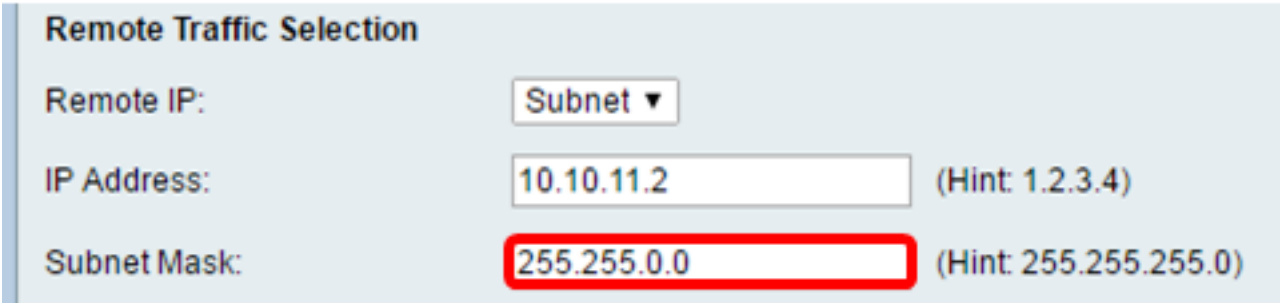
Passaggio 11. Immettere l'intervallo di indirizzi IP dell'host che farà parte della VPN nel campo *Indirizzo IP*. Se si è selezionato **Single** (Singolo) al punto 10, immettere un indirizzo IP.

Nota: Nell'esempio seguente viene utilizzato 10.10.11.2.



Passaggio 12. (Facoltativo) Se **Subnet** è selezionato nel passaggio 10, immettere la subnet mask dell'indirizzo IP della subnet nel campo *Subnet mask*.

Nota: Nell'esempio seguente viene utilizzato 255.255.0.0.

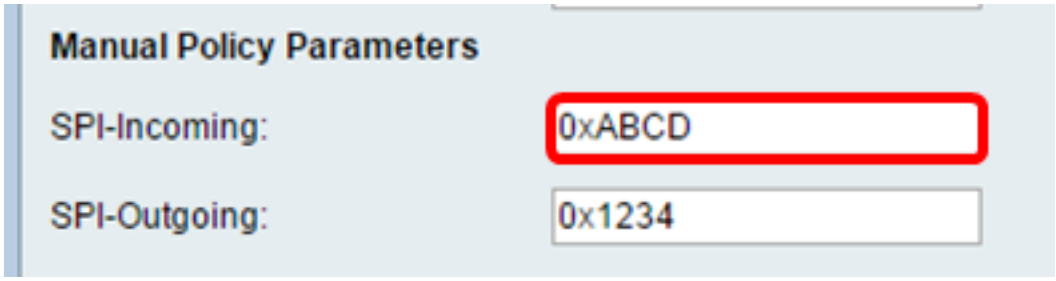


Criteri manuali Parametri

Nota: questi campi possono essere modificati solo se si sceglie **Criteri manuali**.

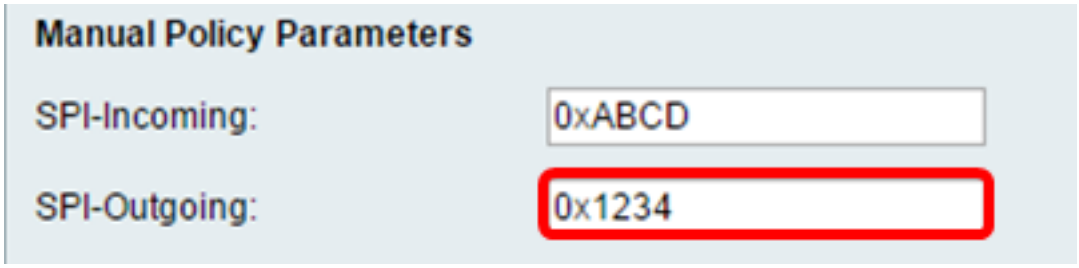
Passaggio 1. Nel campo *SPI-Incoming*, immettere da tre a otto caratteri esadecimali per il tag Security Parameter Index (SPI) per il traffico in entrata sulla connessione VPN. Il tag SPI viene utilizzato per distinguere il traffico di una sessione dal traffico di altre sessioni.

Nota: Nell'esempio, viene usato 0xABCD.



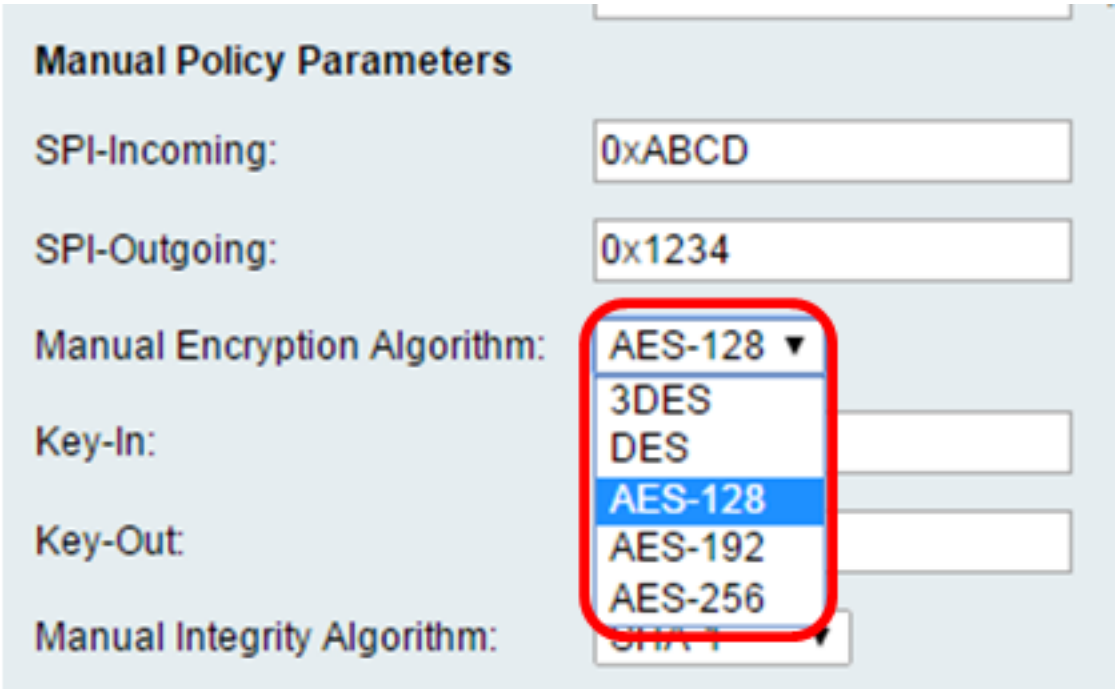
Passaggio 2. Nel campo *SPI-Outgoing*, immettere da tre a otto caratteri esadecimali per il tag SPI per il traffico in uscita sulla connessione VPN.

Nota: Nell'esempio viene usato 0x1234.



Passaggio 3. Dall'elenco a discesa Manual Encryption Algorithm, scegliere un'opzione. Le opzioni sono DES, 3DES, AES-128, AES-192 e AES-256.

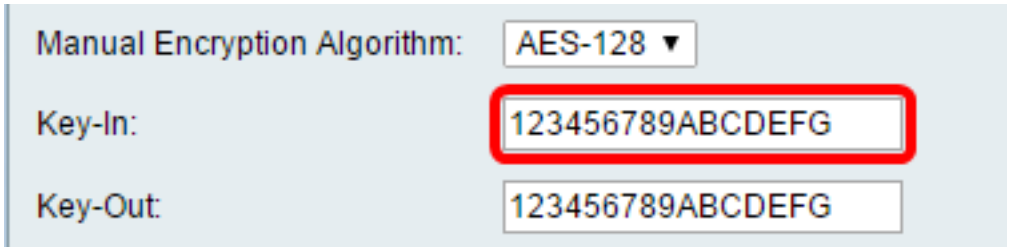
Nota: Nell'esempio, viene scelto AES-128.



Passaggio 4. Nel campo *Chiave in ingresso*, immettere una chiave per il criterio in ingresso. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 3.

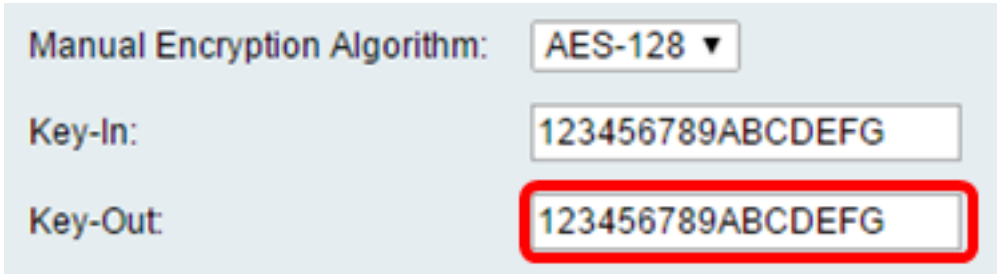
- DES utilizza un tasto a 8 caratteri.
- 3DES utilizza un tasto di 24 caratteri.
- AES-128 utilizza un tasto a 16 caratteri.
- AES-192 utilizza un tasto di 24 caratteri.
- AES-256 utilizza un tasto di 32 caratteri.

Nota: Nell'esempio viene utilizzato 123456789ABCDEFG.



Passaggio 5. Nel campo *Esclusione* immettere una chiave per il criterio in uscita. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 3.

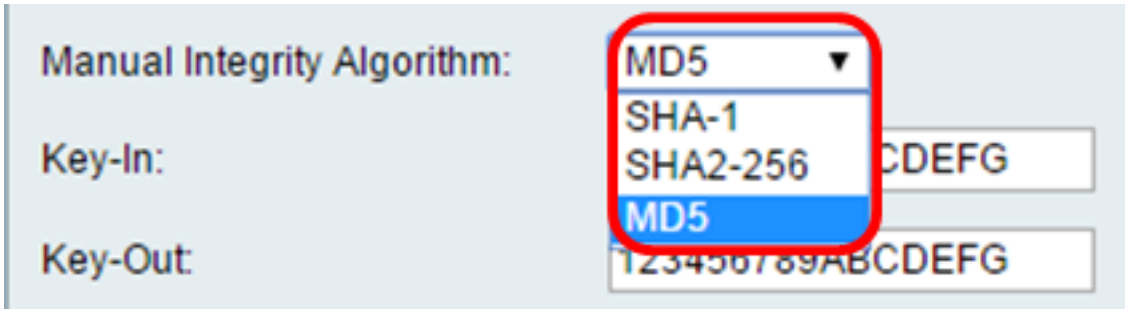
Nota: Nell'esempio viene utilizzato 123456789ABCDEFG.



Passaggio 6. Dall'elenco a discesa Manual Integrity Algorithm, scegliere un'opzione.

- MD5: utilizza un valore hash a 128 bit per l'integrità dei dati. MD5 è meno sicuro ma più veloce rispetto a SHA-1 e SHA2-256.
- SHA-1: utilizza un valore hash a 160 bit per l'integrità dei dati. SHA-1 è più lento ma più sicuro di MD5 e SHA-1 è più veloce ma meno sicuro di SHA2-256.
- SHA2-256: utilizza un valore hash a 256 bit per l'integrità dei dati. SHA2-256 è più lento ma sicuro di MD5 e SHA-1.

Nota: In questo esempio, viene scelto MD5.



Passaggio 7. Nel *campo Chiave in ingresso*, immettere una chiave per il criterio in ingresso. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 6.

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

Nota: Nell'esempio viene utilizzato 123456789ABCDEFG.

Passaggio 8. Nel *campo Esclusione*, immettere una chiave per il criterio in uscita. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 6.

Nota: Nell'esempio viene utilizzato 123456789ABCDEFG.

Autoo Parametri dei criteri

Nota: prima di creare un criterio VPN automatico, assicurarsi di creare il criterio IKE in base al quale si desidera creare il criterio VPN automatico. Questi campi possono essere modificati solo se nel passaggio 3 è stata selezionata l'opzione **Criterio automatico**.

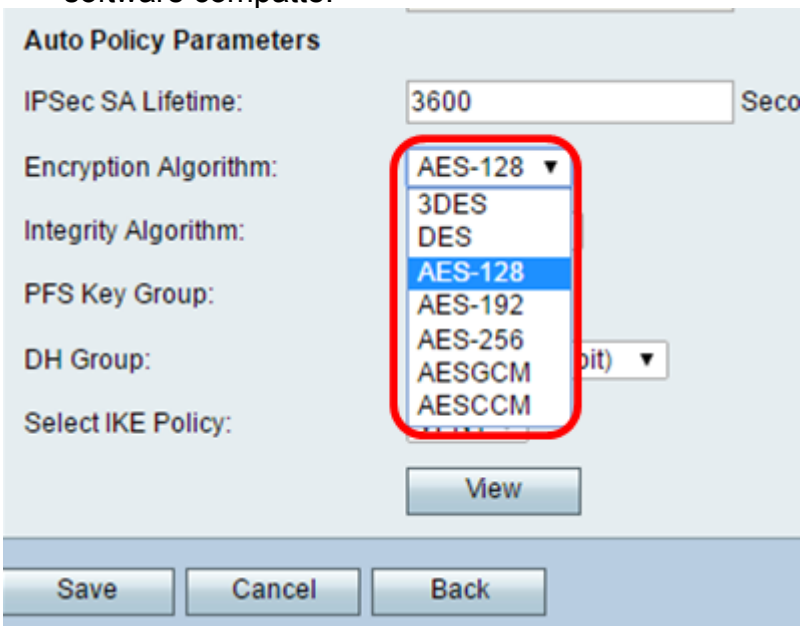
Passaggio 1. Nel *campo IPSec SA-Lifetime*, immettere la durata in secondi dell'associazione di protezione prima del rinnovo. L'intervallo è compreso tra 30 e 86400. Il valore predefinito è 3600.

Passaggio 2. Dall'elenco a discesa Algoritmo di crittografia, scegliere un'opzione. Le opzioni sono:

Nota: Nell'esempio, viene scelto AES-128.

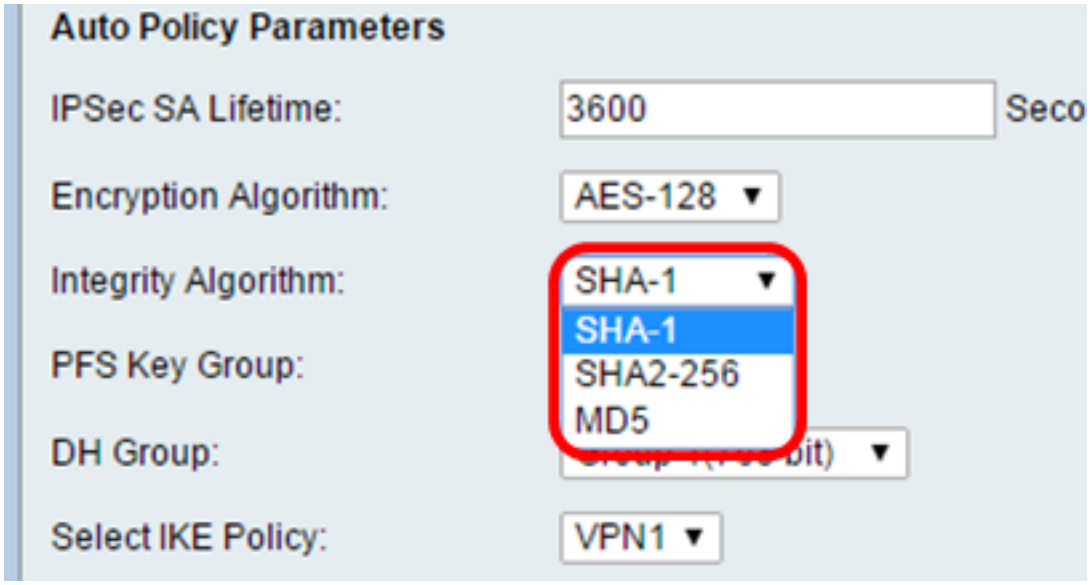
- DES: un metodo di crittografia a 56 bit meno recente che non è molto sicuro, ma che potrebbe essere necessario per garantire la compatibilità con le versioni precedenti.
- 3DES: un semplice metodo di crittografia a 168 bit utilizzato per aumentare le dimensioni della chiave poiché esegue la crittografia dei dati tre volte. Ciò garantisce una maggiore sicurezza rispetto a DES ma una minore sicurezza rispetto a AES.

- AES-128: utilizza una chiave a 128 bit per la crittografia AES. AES è più veloce e sicuro rispetto a DES. In generale, AES è anche più veloce e più sicuro di 3DES. AES-128 è più veloce ma meno sicuro di AES-192 e AES-256.
- AES-192: utilizza una chiave a 192 bit per la crittografia AES. AES-192 è più lento ma più sicuro di AES-128 e più veloce ma meno sicuro di 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.
- AESGCM — Advanced Encryption Standard Galois Counter Mode è una modalità di crittografia a blocchi con autenticazione generica. L'autenticazione GCM utilizza operazioni particolarmente adatte all'implementazione efficiente nell'hardware, rendendola particolarmente interessante per le implementazioni ad alta velocità o per le implementazioni in un circuito compatto ed efficiente.
- AESCCM — Advanced Encryption Standard Counter con modalità CBC-MAC è una modalità di crittografia a blocchi autenticata generica. CCM è adatto per l'utilizzo in implementazioni software compatte.

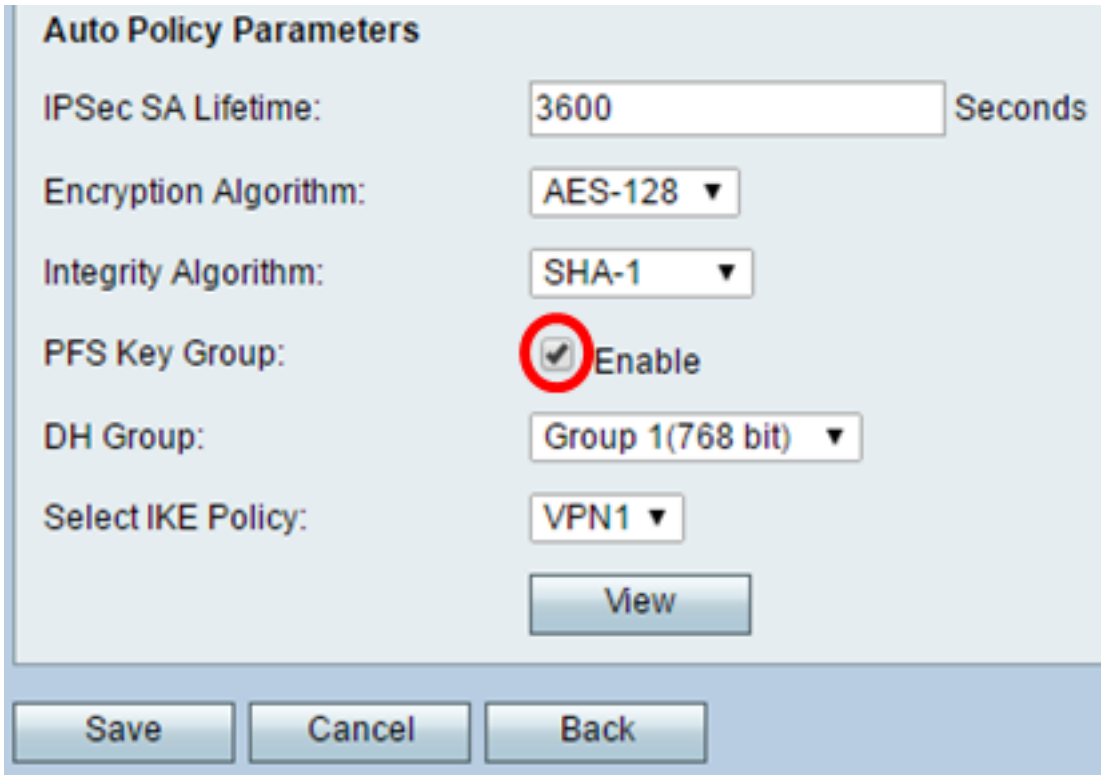


Passaggio 3. Dall'elenco a discesa Algoritmo di integrità, scegliere un'opzione. Le opzioni sono MD5, SHA-1 e SHA2-256.

Nota: Nell'esempio viene scelto SHA-1.

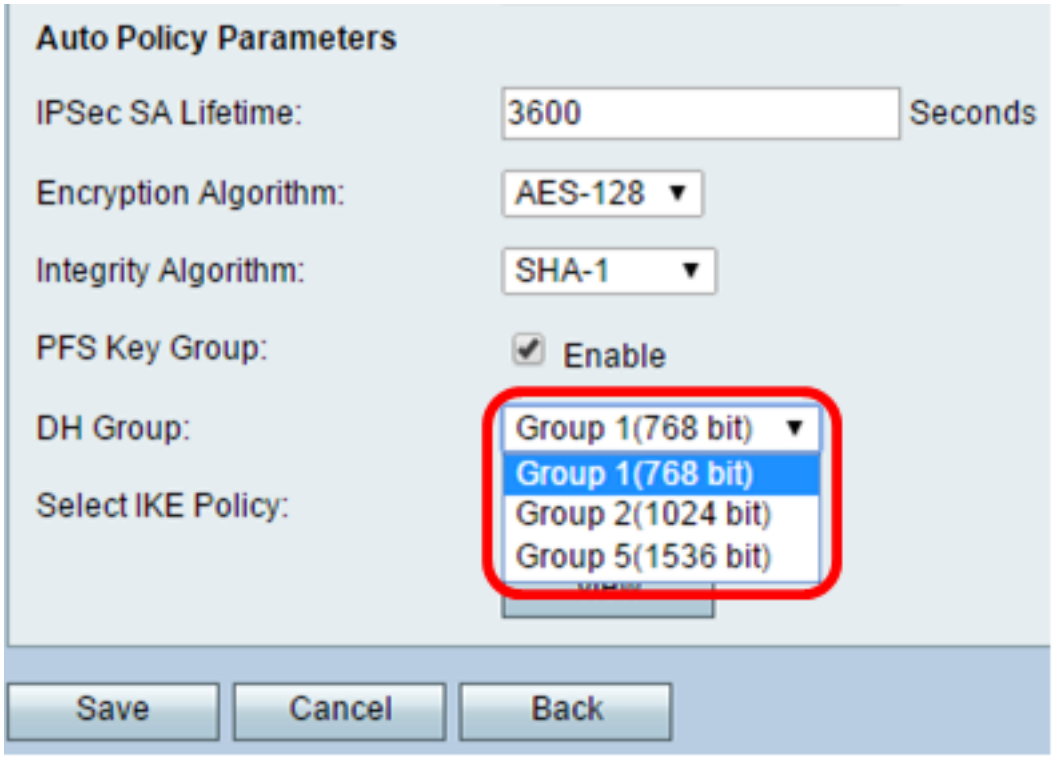


Passaggio 4. Selezionare la casella di controllo **Abilita** nel gruppo di chiavi PFS per abilitare PFS (Perfect Forward Secrecy). PFS aumenta la sicurezza della VPN, ma rallenta la velocità di connessione.



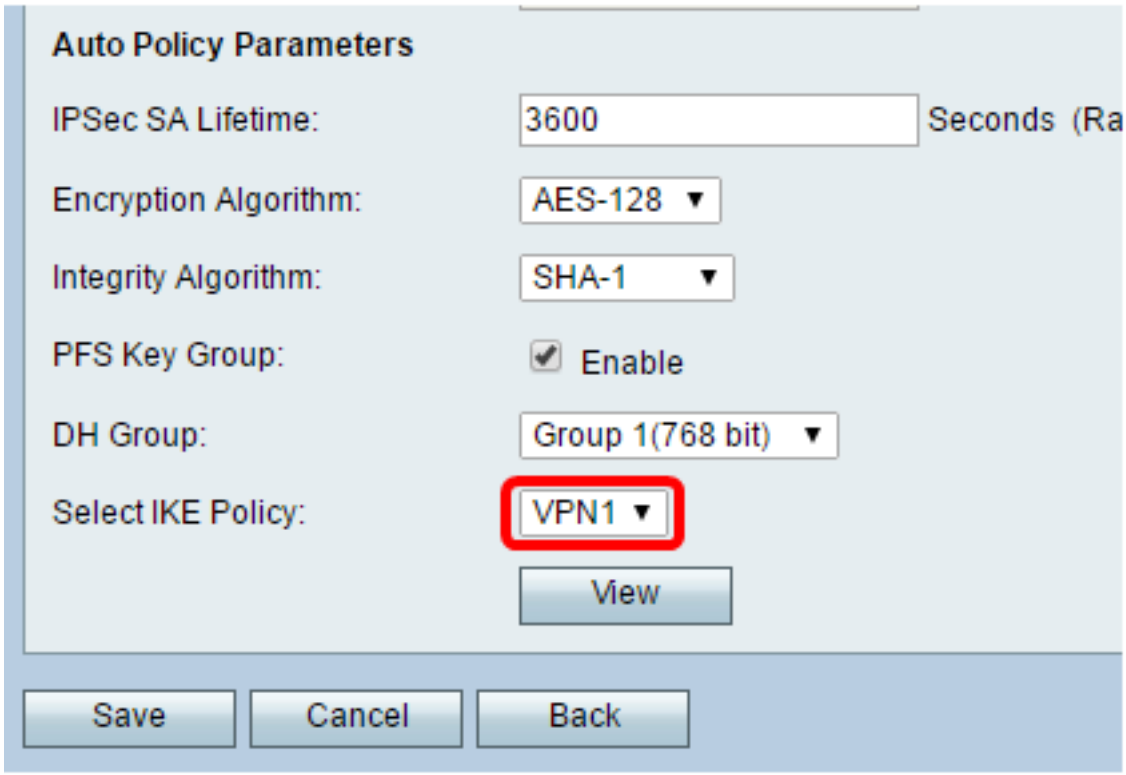
Passaggio 5. (Facoltativo) Se si è scelto di abilitare PFS nel passaggio 4, scegliere un gruppo DH a cui unirsi dall'elenco a discesa Gruppo DH. Più alto è il numero di gruppo, migliore sarà la sicurezza.

Nota: Per questo esempio, viene scelto Gruppo 1.

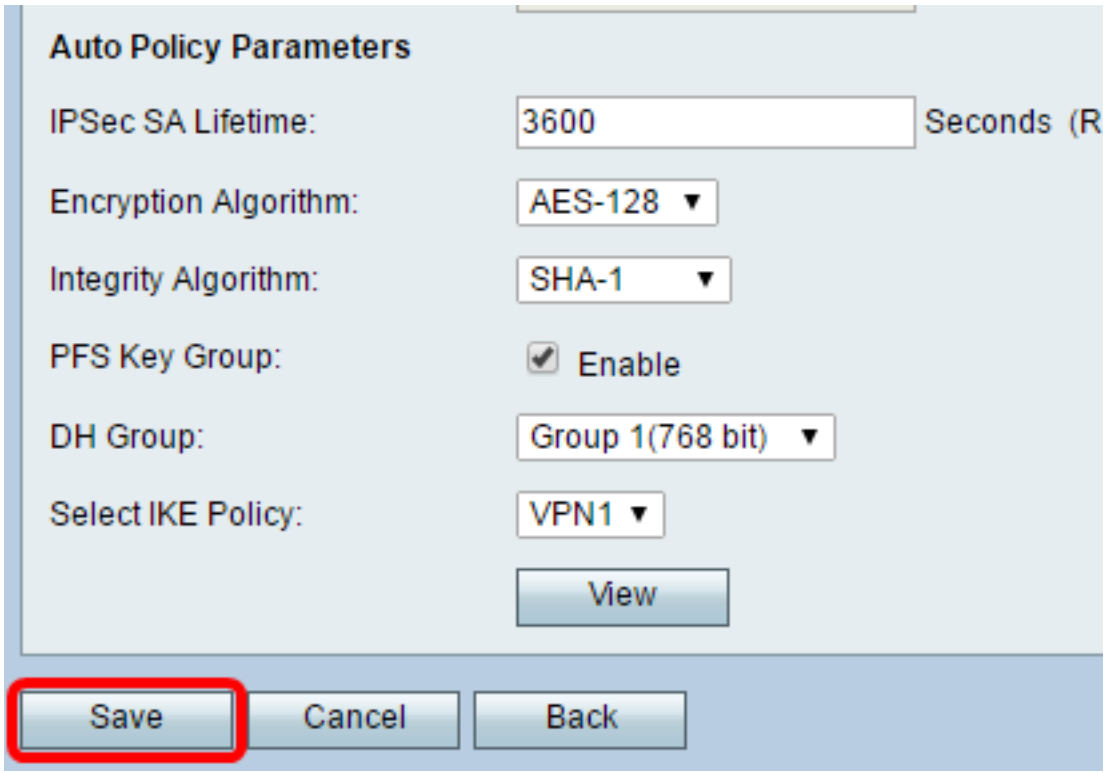


Passaggio 6. Dall'elenco a discesa Seleziona criterio IKE scegliere il criterio IKE da utilizzare per il criterio VPN.

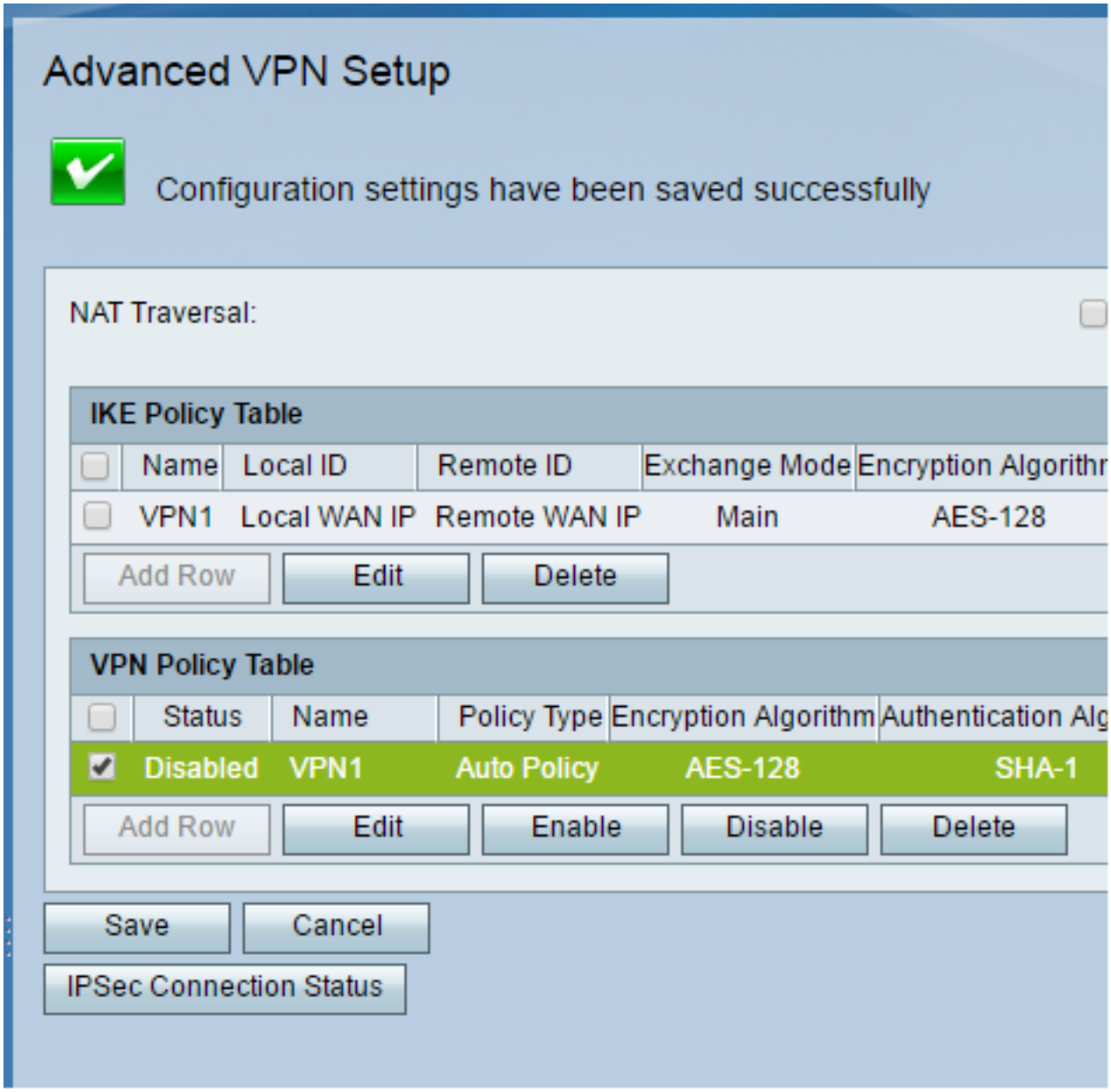
Nota: In questo esempio è stato configurato un solo criterio IKE, pertanto verrà visualizzato un solo criterio.



Passaggio 7. Fare clic su **Salva**.

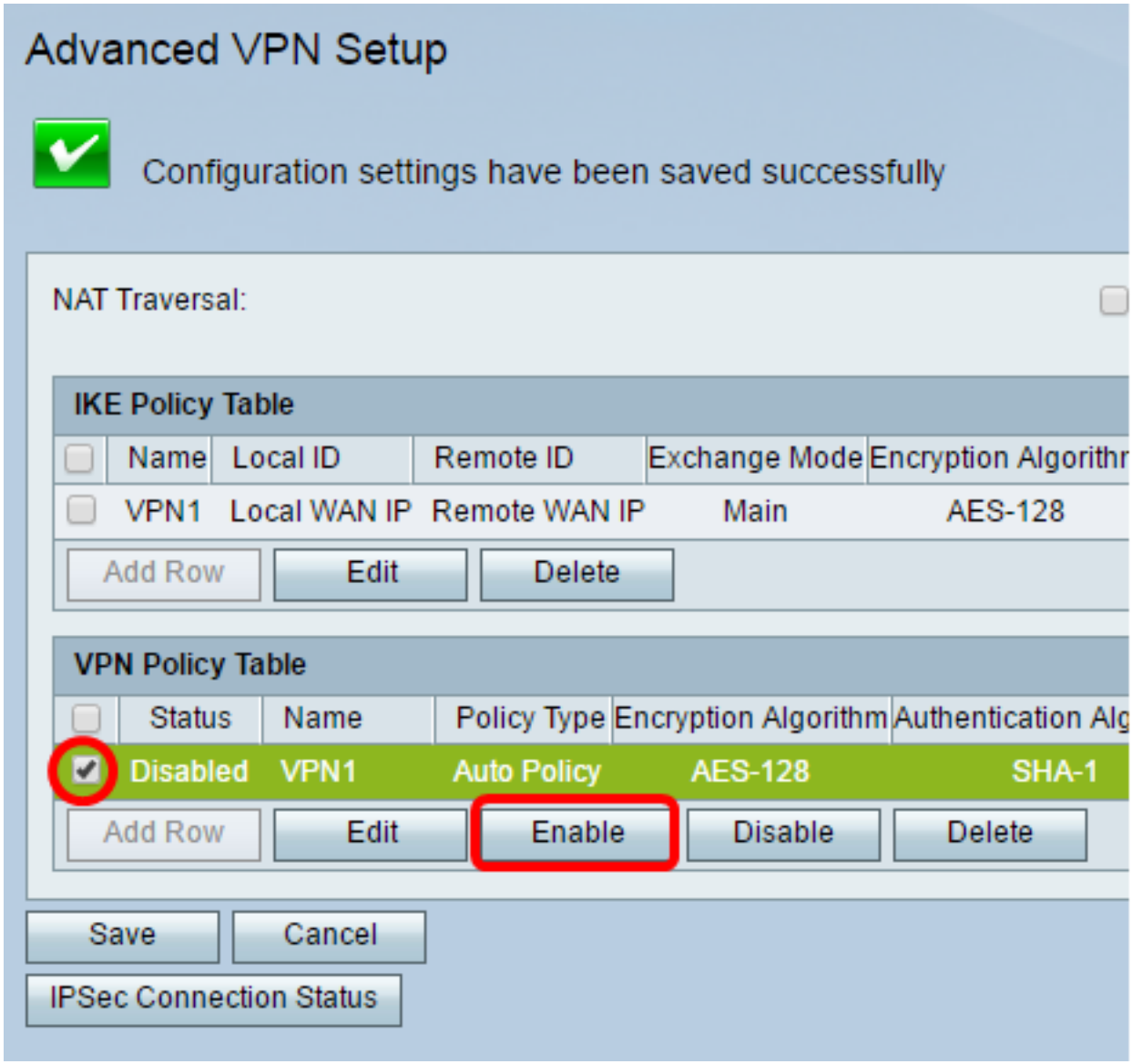


Nota: Viene visualizzata di nuovo la pagina Impostazione VPN avanzata. Viene visualizzato un messaggio di conferma del corretto salvataggio delle impostazioni di configurazione.

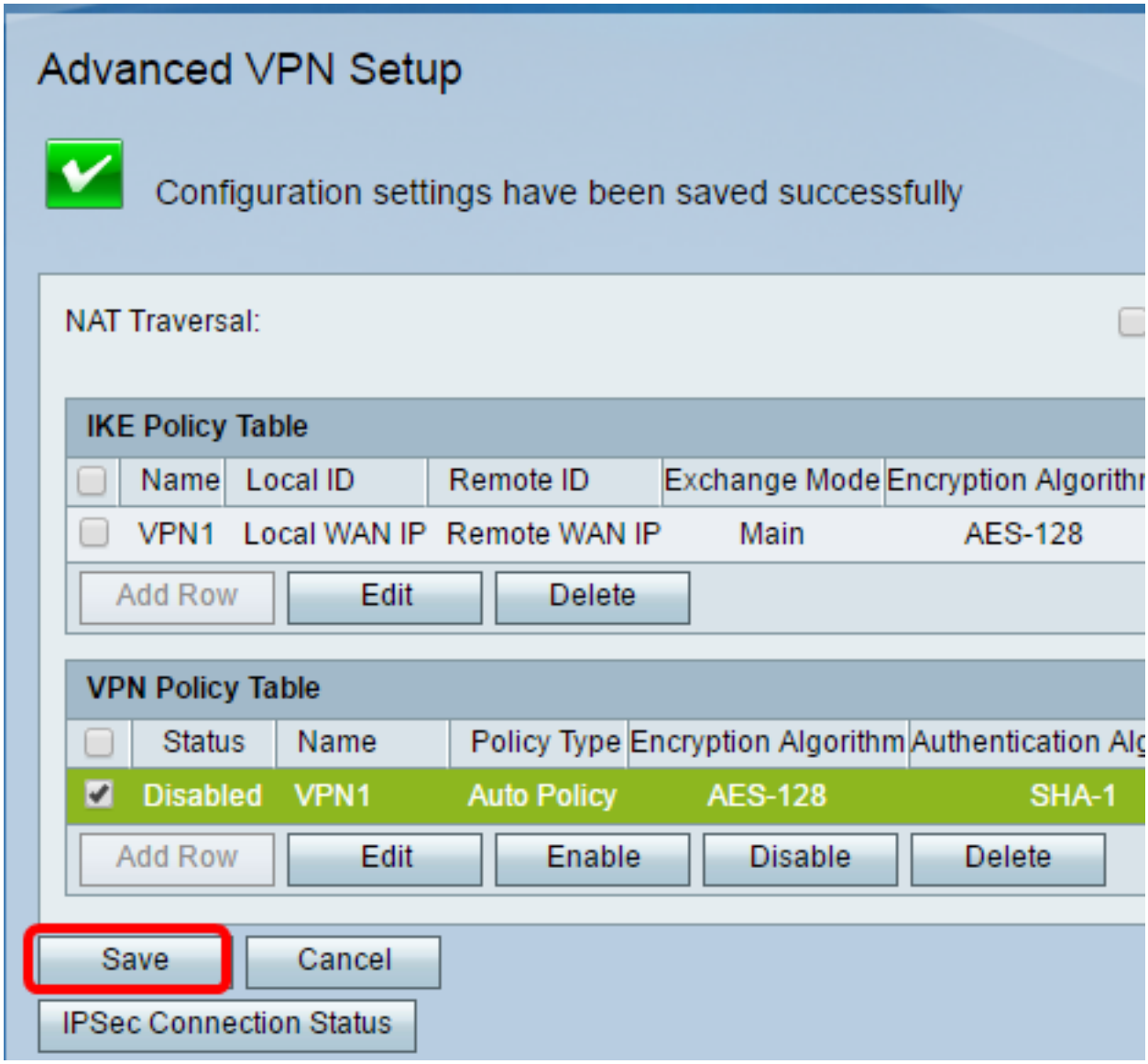


Passaggio 8. Sotto la tabella Criteri VPN, selezionare una casella di controllo per scegliere una VPN e fare clic su **Abilita**.

Nota: I criteri VPN configurati sono disabilitati per impostazione predefinita.



Passaggio 9. Fare clic su **Salva**.



Èora necessario configurare correttamente un criterio VPN sul router RV130 o RV130W.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).