Configurazione della configurazione VPN (Virtual Private Network) avanzata sul firewall RV110W

Obiettivo

La rete privata virtuale (VPN) utilizza la rete pubblica, o Internet, per stabilire una rete privata per comunicare in modo sicuro. Uno IKE (Internet Key Exchange) è un protocollo che stabilisce una comunicazione sicura tra due reti. Viene usata per scambiare una chiave prima dei flussi di traffico, il che assicura l'autenticità di entrambe le estremità del tunnel VPN.

Per comunicare correttamente tra loro, entrambe le estremità della VPN devono seguire lo stesso criterio VPN.

Questo documento spiega come aggiungere un profilo IKE e configurare i criteri VPN sul router wireless RV110W.

Dispositivi interessati

RV110W

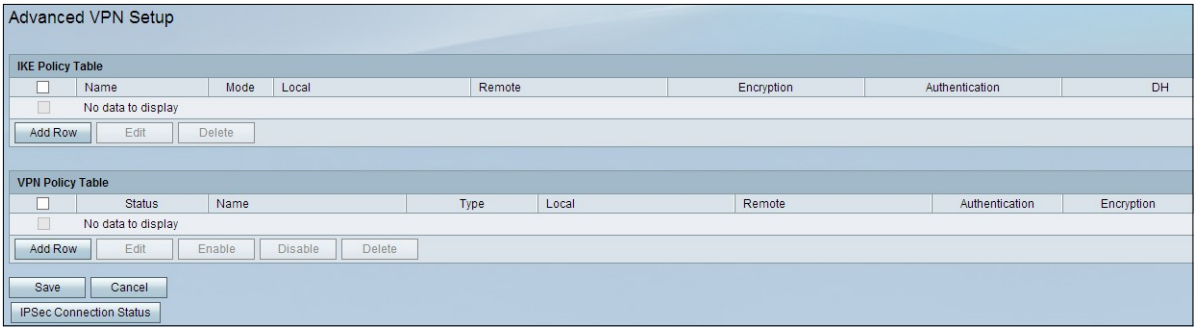
Versione del software

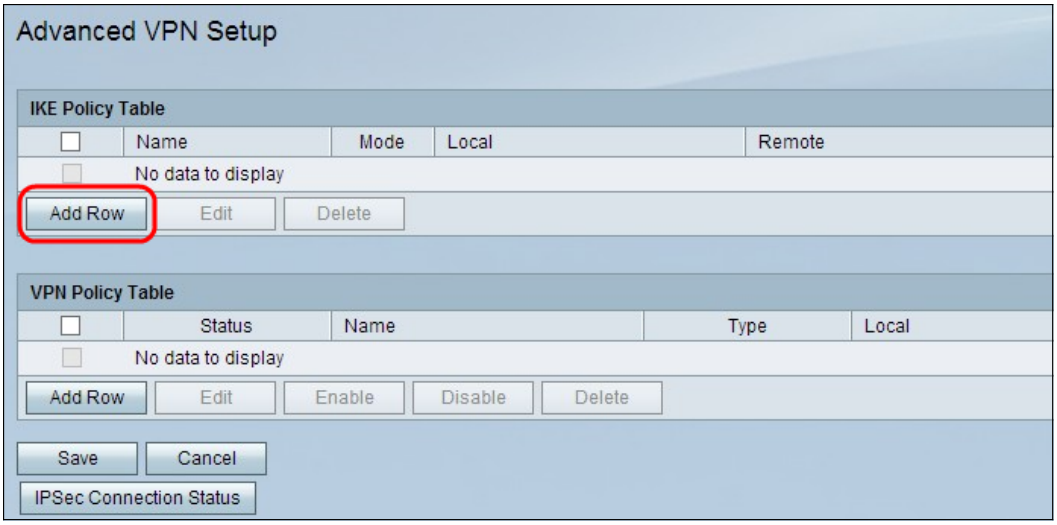
•1.2.0.9

Impostazioni criteri IKE

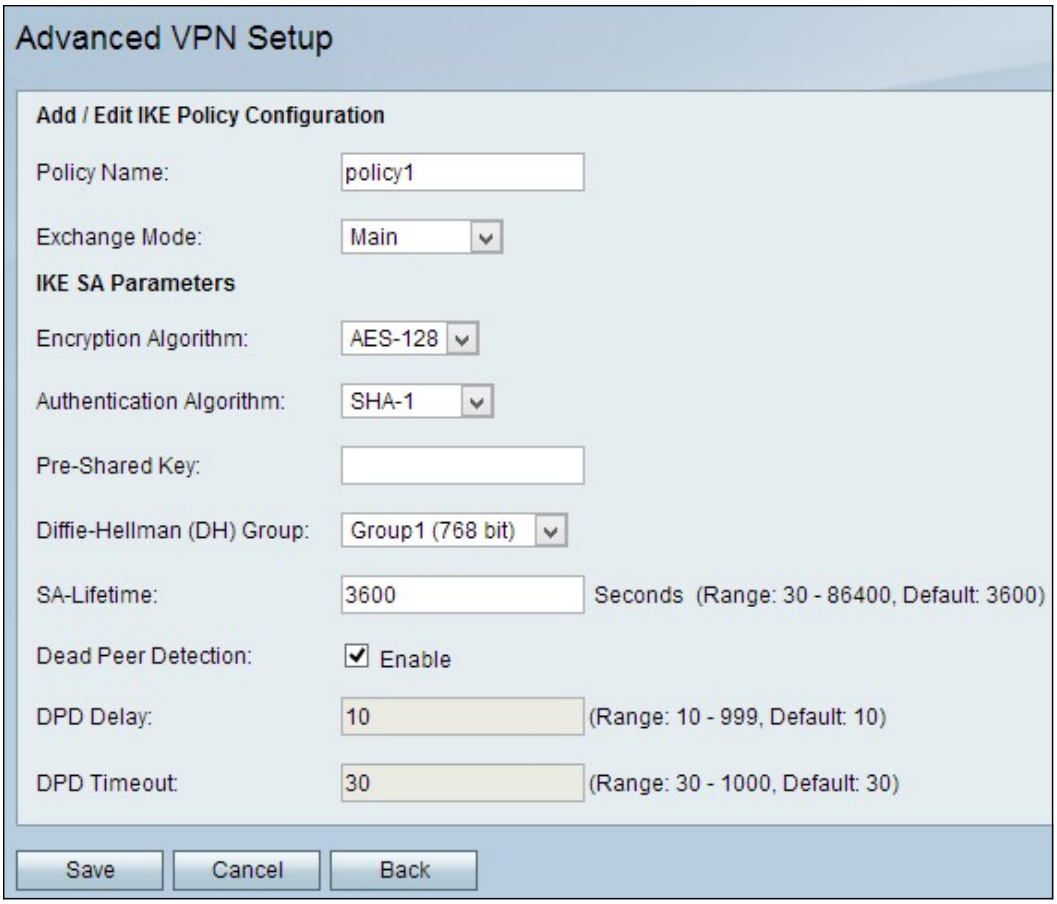
IKE (Internet Key Exchange) è un protocollo utilizzato per stabilire una connessione sicura per la comunicazione in una VPN. Questa connessione sicura stabilita è denominata associazione di sicurezza (SA, Security Association). In questa procedura viene illustrato come configurare un criterio IKE per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

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

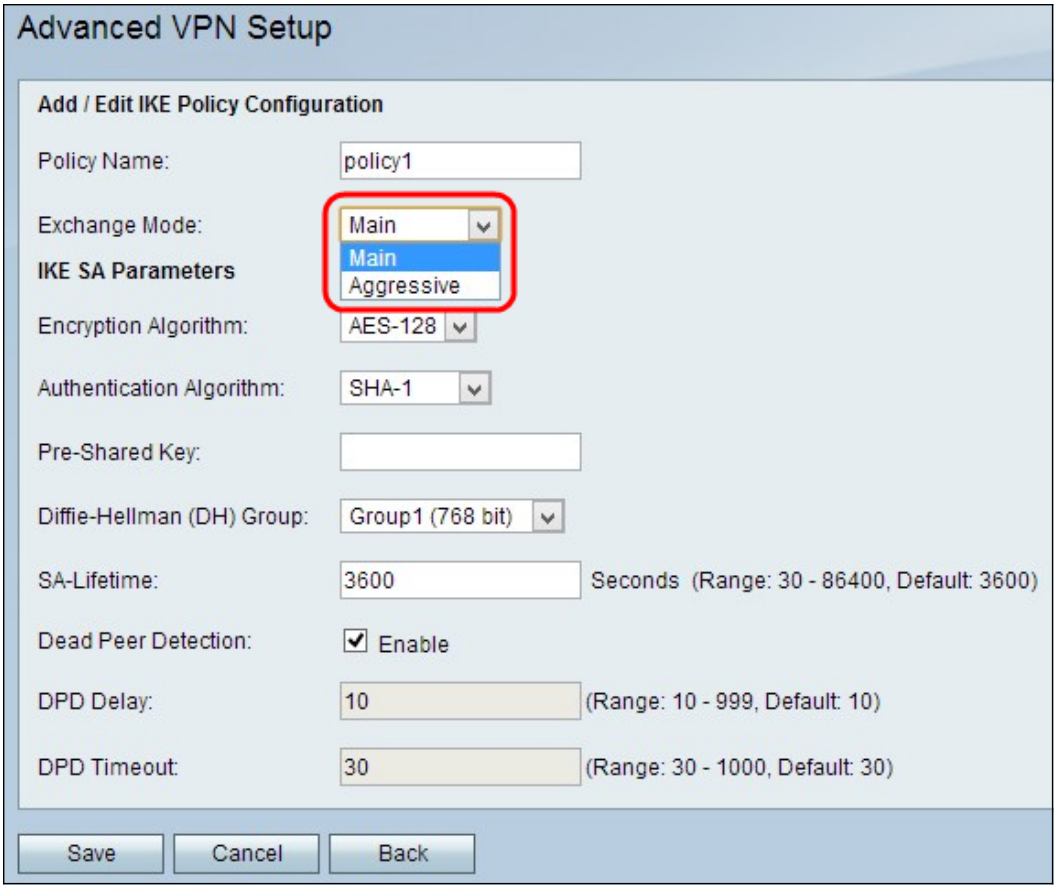




Passaggio 2. Fare clic su **Aggiungi riga** per creare un nuovo criterio IKE. Viene visualizzata la pagina *Advanced VPN Setup* (Configurazione VPN avanzata):



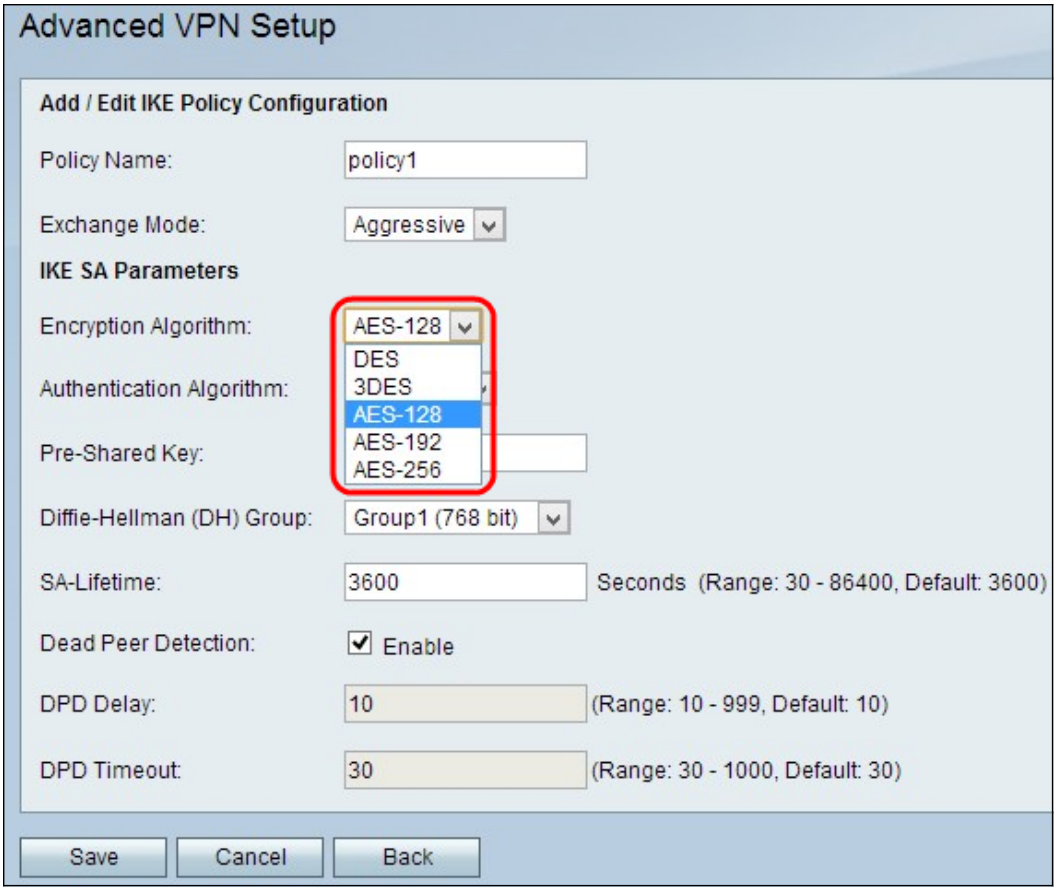
Passaggio 3. Nel campo *Nome criterio* immettere un nome per il criterio IKE da identificare facilmente.



Passaggio 4. Scegliere un'opzione dall'elenco a discesa *Modalità scambio*:

·Principale: consente al criterio IKE di funzionare in modo più sicuro ma più lento rispetto alla modalità aggressiva. Scegliere questa opzione se è necessaria una connessione VPN più sicura.

·Aggressivo: consente al criterio IKE di funzionare più velocemente ma in modo meno sicuro rispetto alla modalità principale. Scegliere questa opzione se è necessaria una connessione VPN più veloce.



Passaggio 5. Scegliere un algoritmo dall'elenco a discesa *Algoritmo di crittografia*:

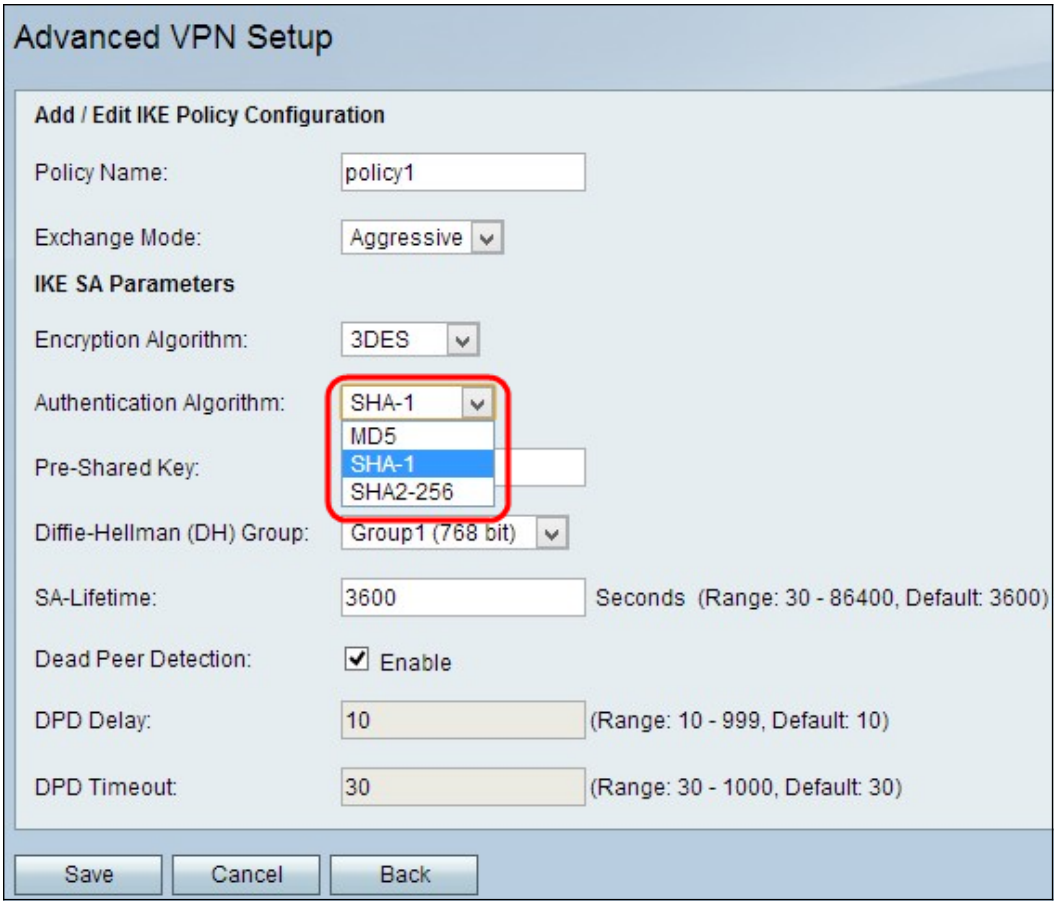
·DES: lo standard DES (Data Encryption Standard) utilizza una chiave a 56 bit per la crittografia dei dati. DES è obsoleto e deve essere utilizzato solo se un endpoint supporta solo DES.

·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. In generale, AES è anche più veloce ma meno sicuro rispetto a 3DES, ma 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.

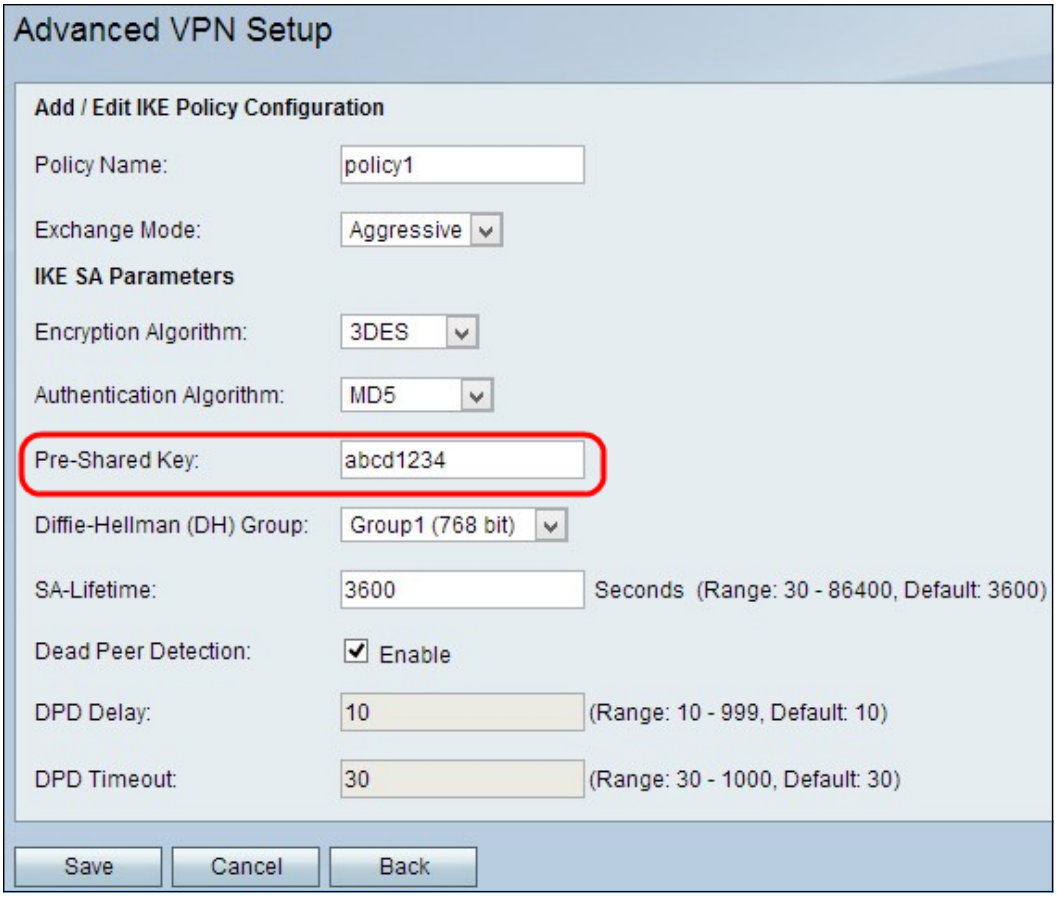


Passaggio 6. Scegliere l'autenticazione desiderata dall'elenco a discesa *Authentication Algorithm*:

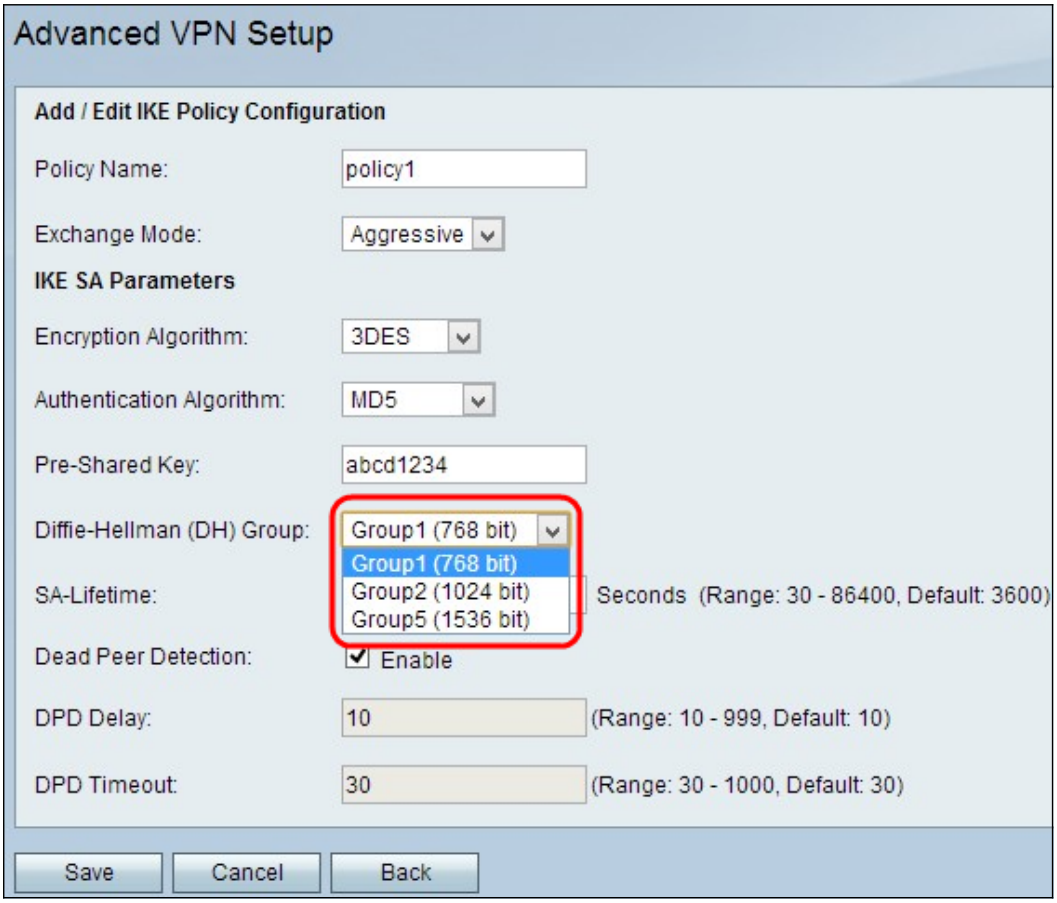
·MD5 — Message-Digest Algorithm 5 (MD5) utilizza un valore hash a 128 bit per l'autenticazione. MD5 è meno sicuro ma più veloce rispetto a SHA-1 e SHA2-256.

·SHA-1: la funzione Secure Hash 1 (SHA-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 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 sicuro di MD5 e SHA-1.



Passaggio 7. Nel campo *Chiave già condivisa*, immettere una chiave già condivisa utilizzata dal criterio IKE.

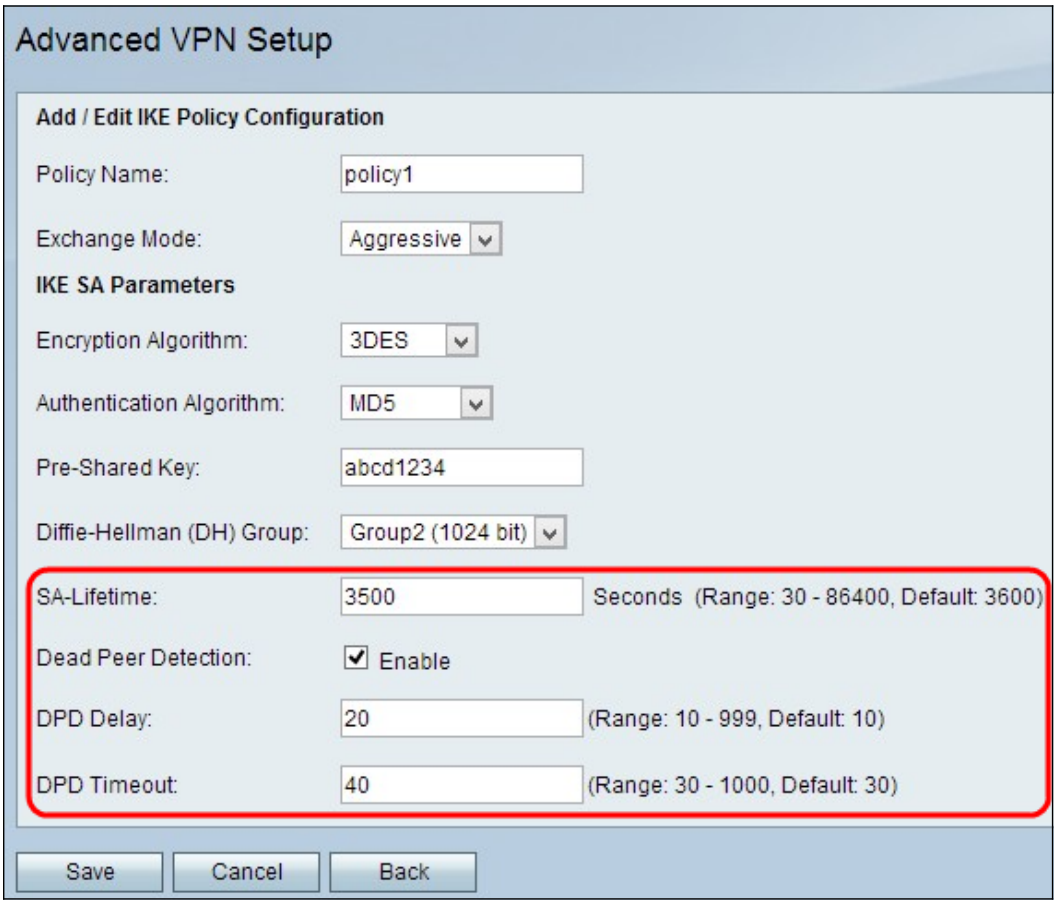


Passaggio 8. Dall'elenco a discesa *Gruppo Diffie-Hellman (DH)*, scegliere il gruppo DH utilizzato da IKE. Gli host di un gruppo DH possono scambiarsi le chiavi senza essere a conoscenza gli uni degli altri. Più alto è il numero di bit del gruppo, più sicuro è il gruppo.

·Gruppo 1 - 768 bit: la chiave con il livello di protezione più basso e il gruppo di autenticazione con il livello di protezione più basso. Ma serve meno tempo per calcolare le chiavi IKE. Questa opzione è preferibile se la velocità della rete è bassa.

·Gruppo 2 - 1024 bit: la chiave di livello superiore e il gruppo di autenticazione più sicuro. Ma ha bisogno di un po' di tempo per calcolare le chiavi IKE.

·Gruppo 5 - 1536 bit: rappresenta la chiave con il livello di protezione più elevato e il gruppo di autenticazione più sicuro. È necessario più tempo per calcolare i tasti IKE. È preferibile se la velocità della rete è elevata.



Passaggio 9. Nel campo *Durata SA* immettere la durata (in secondi) di un'associazione di protezione per la VPN prima del rinnovo dell'associazione di protezione.

Passaggio 10. (Facoltativo) Selezionare la casella di controllo **Abilita** nel campo *Dead Peer Detection* (Rilevamento peer morti) per abilitare Dead Peer Detection (Rilevamento peer morti). Deed Peer Detection esegue il monitoraggio dei peer IKE per verificare se un peer non funziona più. Dead Peer Detection impedisce lo spreco di risorse di rete su peer inattivi.

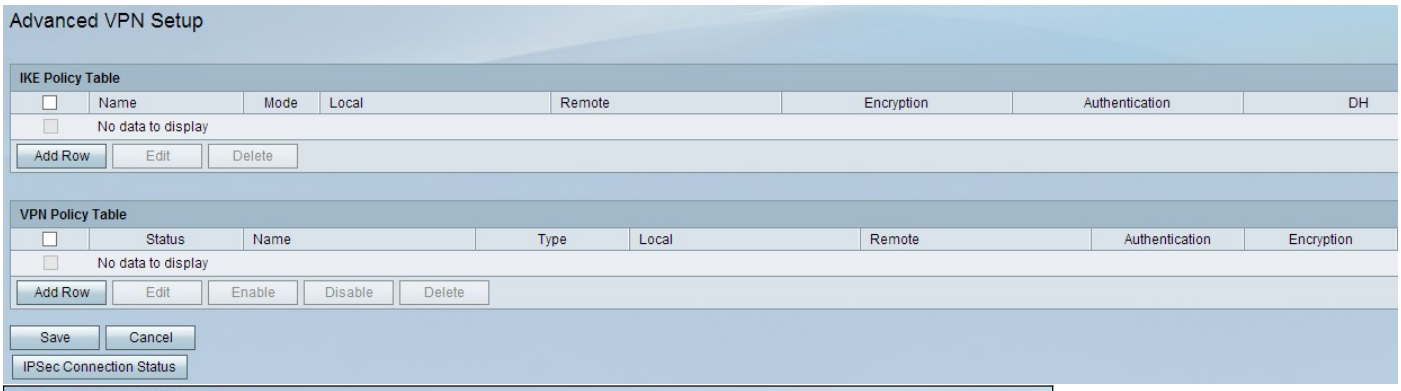
Passaggio 11. (Facoltativo) Se nel passaggio 9 è stato abilitato Deed Peer Detection, immettere la frequenza (in secondi) con cui il peer viene controllato per verificare l'attività nel campo *Deed Peer Delay*.

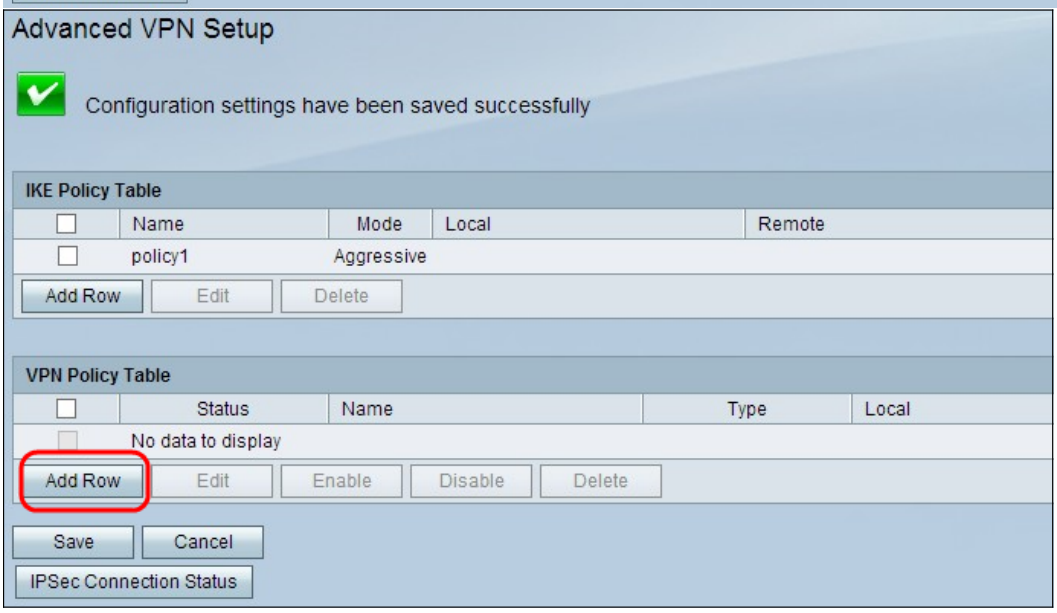
Passaggio 12. (Facoltativo) Se nel passaggio 9 è stato abilitato Deed Peer Detection, immettere il numero di secondi di attesa prima che un peer inattivo venga eliminato nel campo Deed Peer Detection Timeout.

Passaggio 13. Fare clic su **Salva** per applicare tutte le impostazioni.

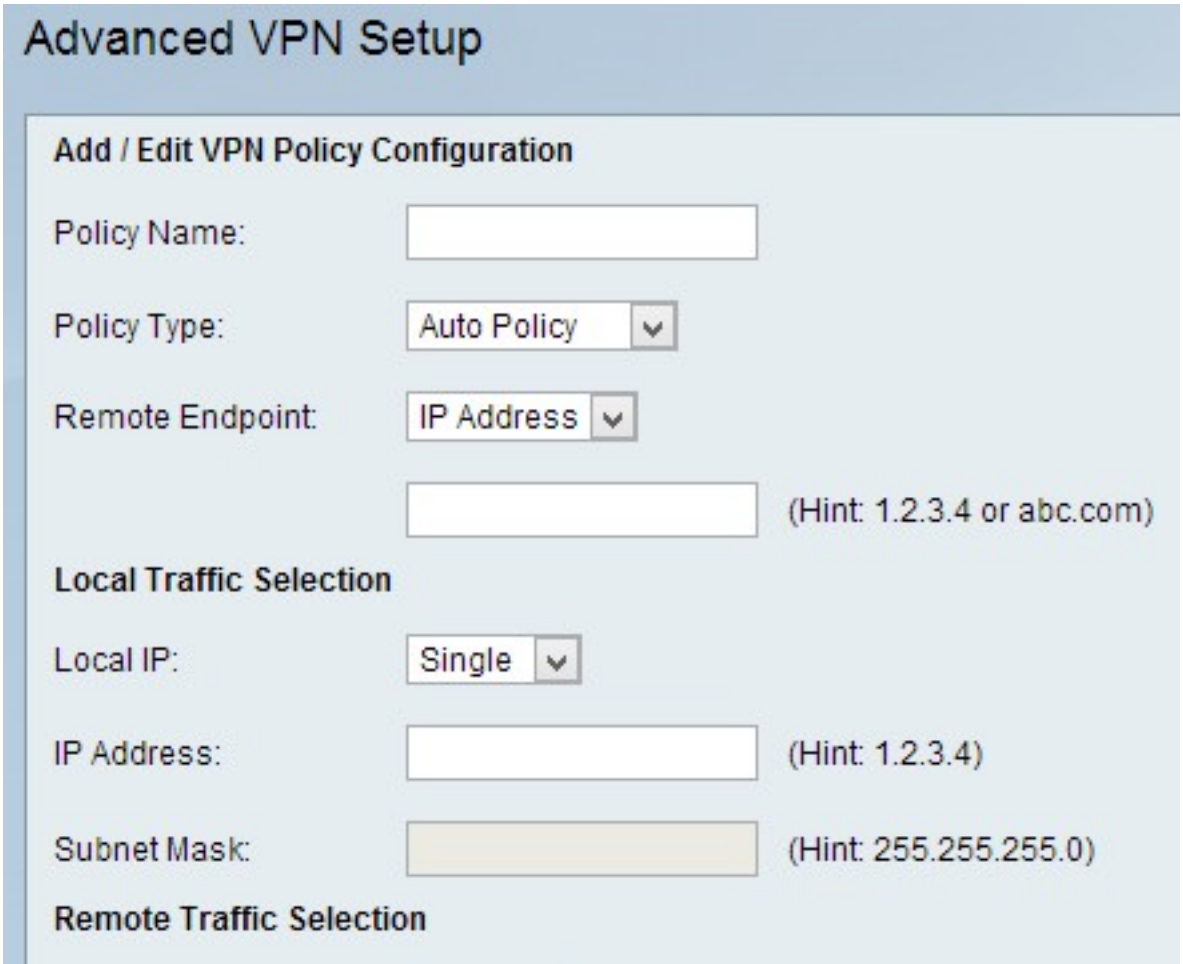
Configurazione criteri VPN

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

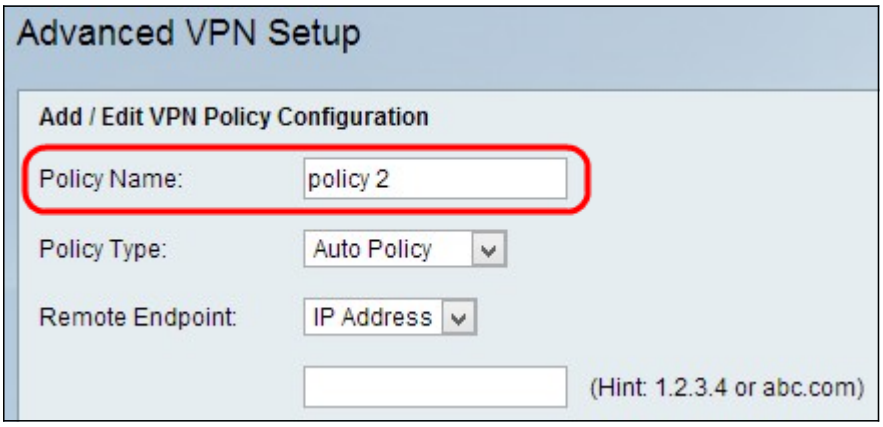




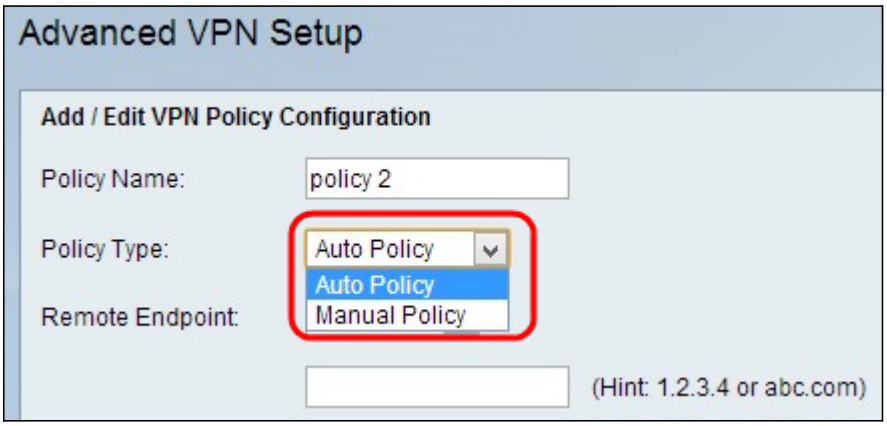
Passaggio 2. Fare clic su **Add** Row (Aggiungi riga) nella *tabella dei criteri VPN*. Viene visualizzata la finestra *Impostazione avanzata criteri VPN*:



Aggiungi/Modifica configurazione criteri VPN



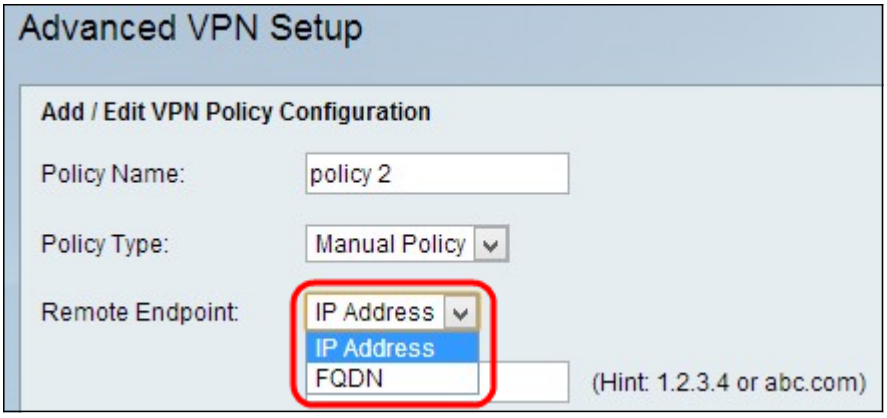
Passaggio 1. Immettere un nome univoco per il criterio nel campo *Nome criterio* per identificarlo facilmente.



Passaggio 2. Scegliere il tipo di criterio appropriato dall'elenco a discesa *Tipo di criterio*.

·Regolazione automatica - I parametri possono essere impostati automaticamente. In questo caso, oltre ai criteri, è necessario che il protocollo IKE (Internet Key Exchange) negozi tra i due endpoint VPN.

·Criterio manuale - In questo caso tutte le impostazioni che includono le impostazioni per le chiavi del tunnel VPN vengono immesse manualmente per ogni endpoint.



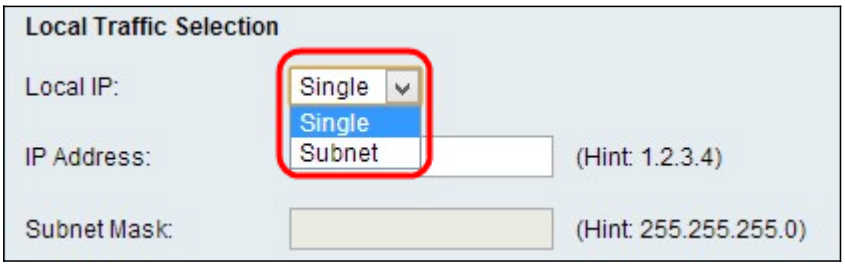
Passaggio 3. Scegliere il tipo di identificatore IP che identifica il gateway nell'endpoint remoto dall'elenco a discesa *Remote Endpoint*.

·Indirizzo IP: indirizzo IP del gateway sull'endpoint remoto. Se si sceglie questa opzione, immettere l'indirizzo IP nel campo.

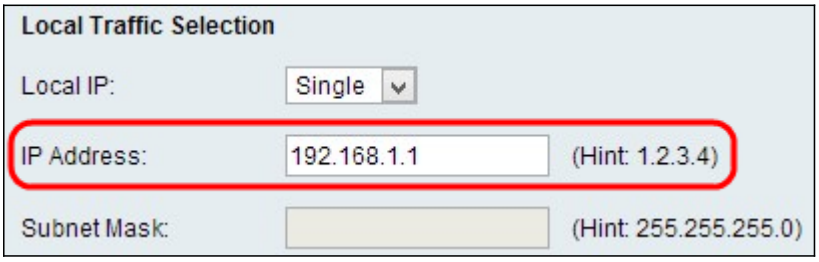
·FQDN (nome di dominio completo): immettere il nome di dominio completo del gateway

sull'endpoint remoto. Se si sceglie questa opzione, immettere il nome di dominio completo nel campo fornito.

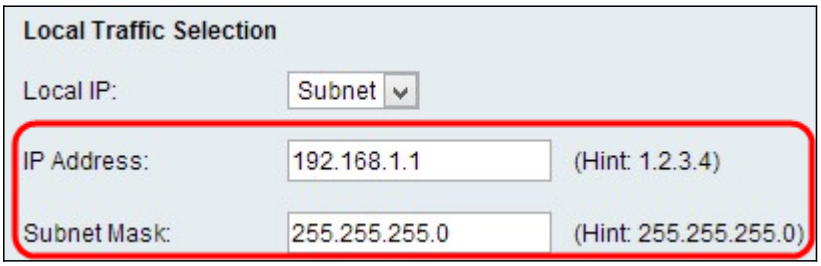
Selezione traffico locale



Passaggio 1. Selezionare il tipo di identificatore che si desidera fornire per l'endpoint dall'elenco a discesa *IP locale*.

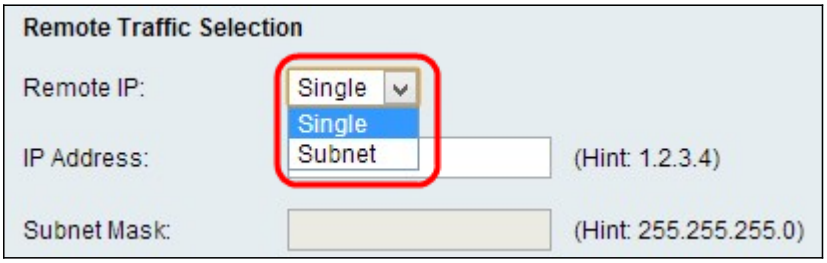


·Singolo: il criterio viene limitato a un host. Se si sceglie questa opzione, immettere l'indirizzo IP nel campo *Indirizzo IP*.



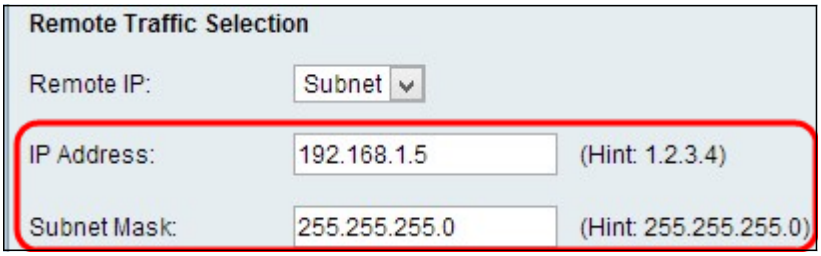
·Subnet: maschera che definisce i limiti di un indirizzo IP. Ciò consente solo agli host della subnet specificata di connettersi alla VPN. Per connettersi a VPN, un computer viene selezionato mediante un'operazione AND logica. Se l'indirizzo IP rientra nello stesso intervallo richiesto, viene selezionato un computer. Se si sceglie questa opzione, immettere l'indirizzo IP e la subnet nei campi Indirizzo IP e Subnet.

Selezione traffico remoto



Passaggio 1. Selezionare il tipo di identificatore da fornire per l'endpoint dall'elenco a discesa *IP locale*:

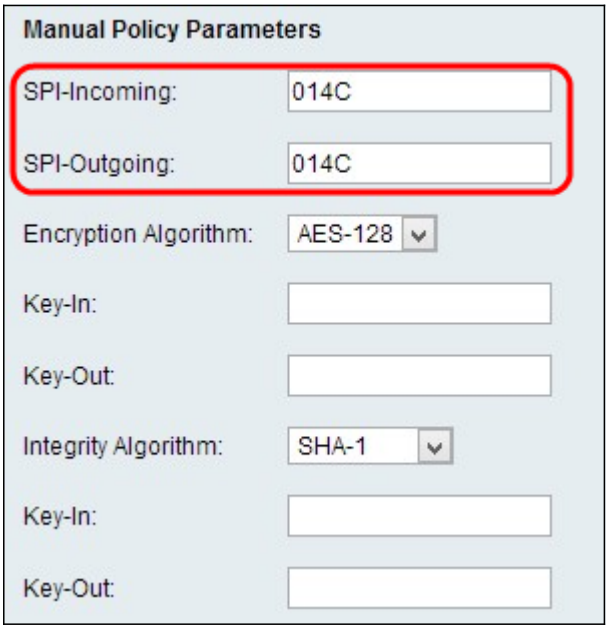
·Singolo: il criterio viene limitato a un host. Se si sceglie questa opzione, immettere l'indirizzo IP nel campo *Indirizzo IP*.



·Subnet: maschera che definisce i limiti di un indirizzo IP. Ciò consente solo agli host della subnet specificata di connettersi alla VPN. Per connettersi a VPN, un computer viene selezionato mediante un'operazione AND logica. Se l'indirizzo IP rientra nello stesso intervallo richiesto, viene selezionato un computer. Se si sceglie questa opzione, immettere l'indirizzo IP e la subnet nei campi Indirizzo IP e Subnet.

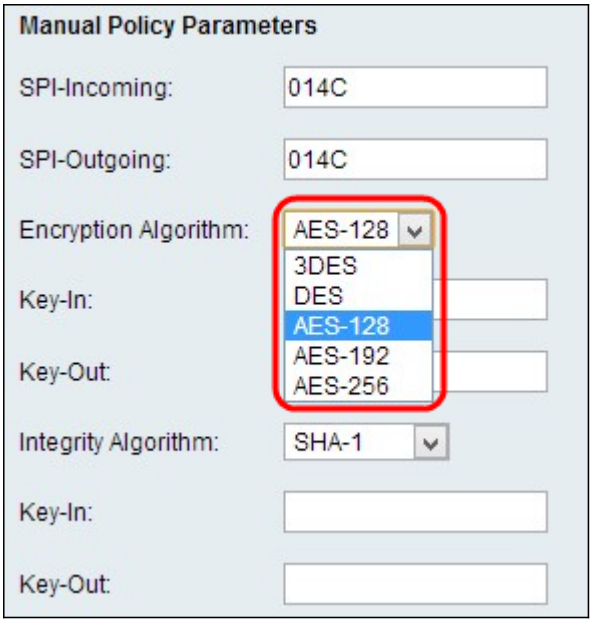
Parametri dei criteri manuali

Per configurare i parametri dei criteri manuali, scegliere **Criteri manuali** dall'elenco a discesa *Tipo di criterio* nel passaggio 2 della sezione *Aggiungi/Modifica configurazione criteri VPN*.



Passaggio 1. Immettere un valore esadecimale compreso tra 3 e 8 nel campo *SPI-Incoming*. Lo Stateful Packet Inspection (SPI) è una tecnologia nota come Deep Packet Inspection. L'interfaccia SPI implementa diverse funzionalità di protezione che consentono di proteggere la rete del computer. Il valore SPI-Incoming corrisponde al valore SPI-Outgoing del dispositivo precedente. Qualsiasi valore è accettabile, a condizione che l'endpoint VPN remoto abbia lo stesso valore nel campo *SPI-Outgoing*.

Passaggio 2. Immettere un valore esadecimale compreso tra 3 e 8 nel campo *SPI-Outgoing*.



Passaggio 3. Scegliere l'algoritmo di crittografia appropriato dall'elenco a discesa Algoritmo di crittografia.

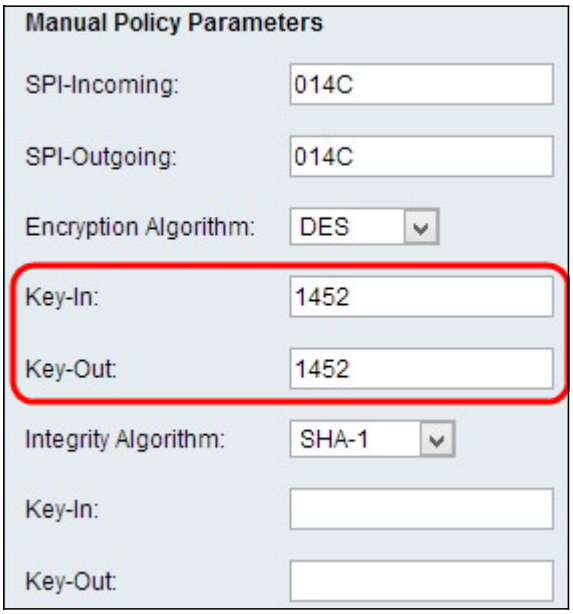
·DES: lo standard DES (Data Encryption Standard) utilizza una chiave a 56 bit per la crittografia dei dati. DES è obsoleto e deve essere utilizzato solo se un endpoint supporta solo DES.

·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 in base all'arrotondamento eseguito dal DES. 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. In generale, AES è anche più veloce ma meno sicuro rispetto a 3DES, ma 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.

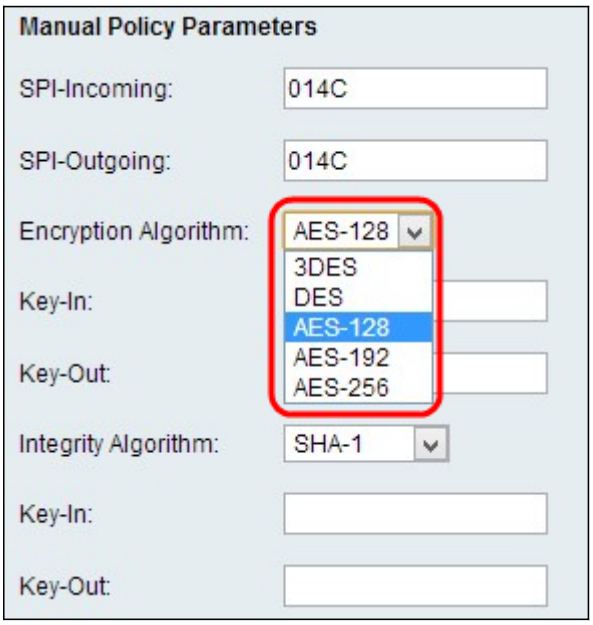
·AES-256 - AES-256 utilizza una chiave a 256 bit per la crittografia AES. AES-256 è più lento ma più sicuro di AES-128 e AES-192.



Passaggio 4. Immettere la chiave di cifratura del criterio in entrata nel campo *Chiave in ingresso*.

La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 3.

Passaggio 5. Immettere la chiave di crittografia del criterio in uscita nel campo *Chiave in uscita*.

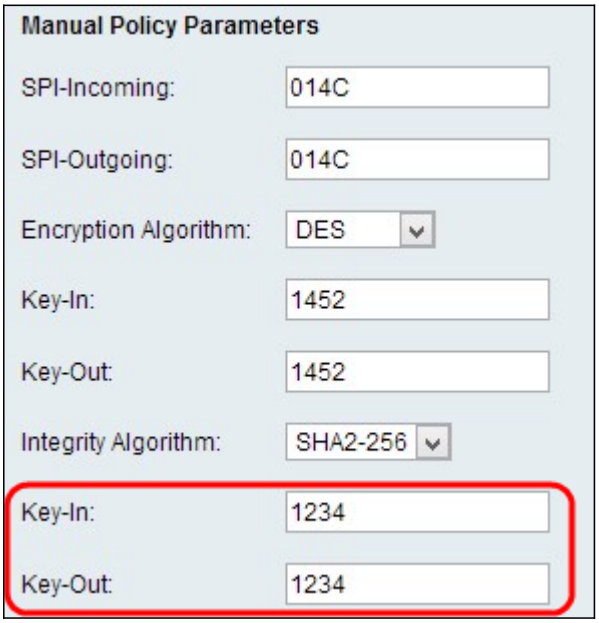


Passaggio 6. Scegliere l'algoritmo di integrità appropriato dall'elenco a discesa *Algoritmo di integrità*. Questo algoritmo verificherà l'integrità dei dati:

·MD5 — Questo algoritmo specifica la lunghezza della chiave a 16 caratteri. MD5 (Message-Digest Algorithm five) non è resistente alle collisioni ed è adatto per applicazioni come i certificati SSL o le firme digitali che si basano su questa proprietà. MD5 comprime qualsiasi flusso di byte in un valore a 128 bit, mentre SHA lo comprime in un valore a 160 bit. MD5 è leggermente più economico da calcolare, tuttavia è una versione precedente dell'algoritmo hash ed è vulnerabile agli attacchi di collisione.

·SHA1 — Secure Hash Algorithm versione 1 (SHA1) è una funzione hash a 160 bit più sicura di MD5, ma richiede più tempo per l'elaborazione.

·SHA2-256 — Questo algoritmo specifica la lunghezza della chiave a 32 caratteri.

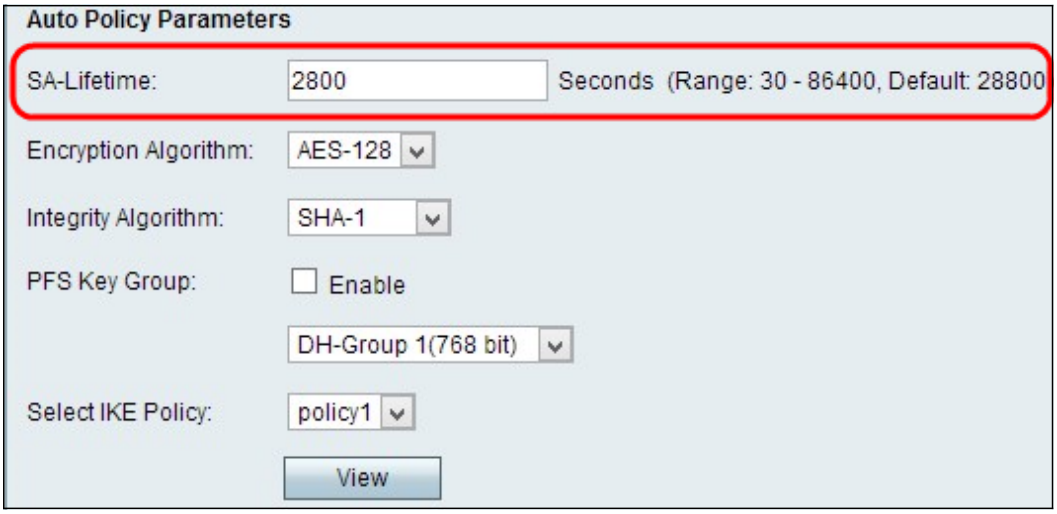


Passaggio 7. Immettere la chiave di integrità (per ESP con modalità Integrità) per il criterio in ingresso. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 6.

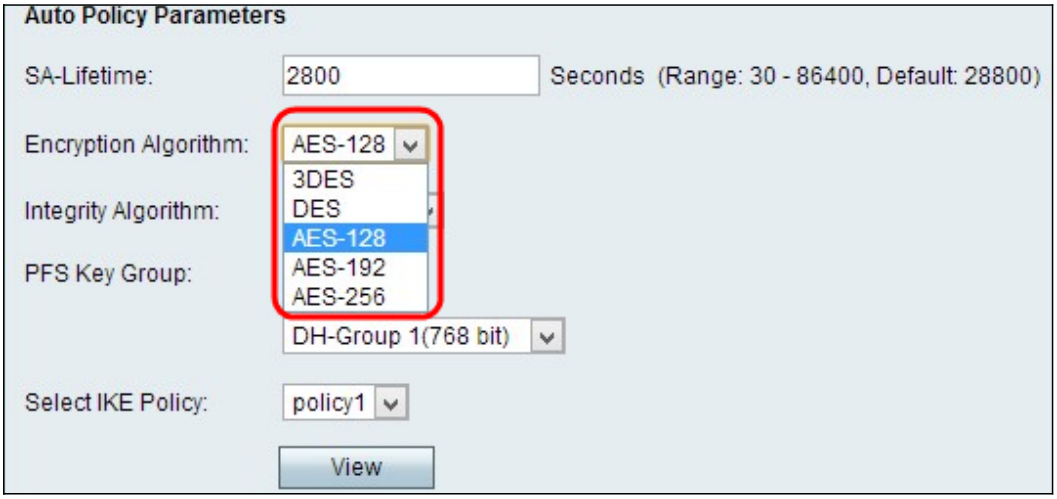
Passaggio 8. Immettere la chiave di integrità del criterio in uscita nel campo Esclusione. Poiché la connessione VPN è impostata per connessioni in uscita verso connessioni in entrata, le chiavi in uscita di un'estremità devono corrispondere alle chiavi in entrata dell'altra estremità.

Nota: Per una connessione riuscita, è necessario che SPI-Incoming e Outgoing, algoritmo di crittografia, algoritmo di integrità e chiavi siano uguali sull'altra estremità del tunnel VPN.

Parametri criteri automatici



Passaggio 1. Immettere la durata dell'associazione di protezione (SA) in secondi nel campo Durata SA. La durata dell'associazione di protezione è la data in cui una chiave ha raggiunto la durata, ogni associazione di protezione associata viene automaticamente rinegoziata.



Passaggio 2. Scegliere l'algoritmo di crittografia appropriato dall'elenco a discesa Algoritmo di crittografia:

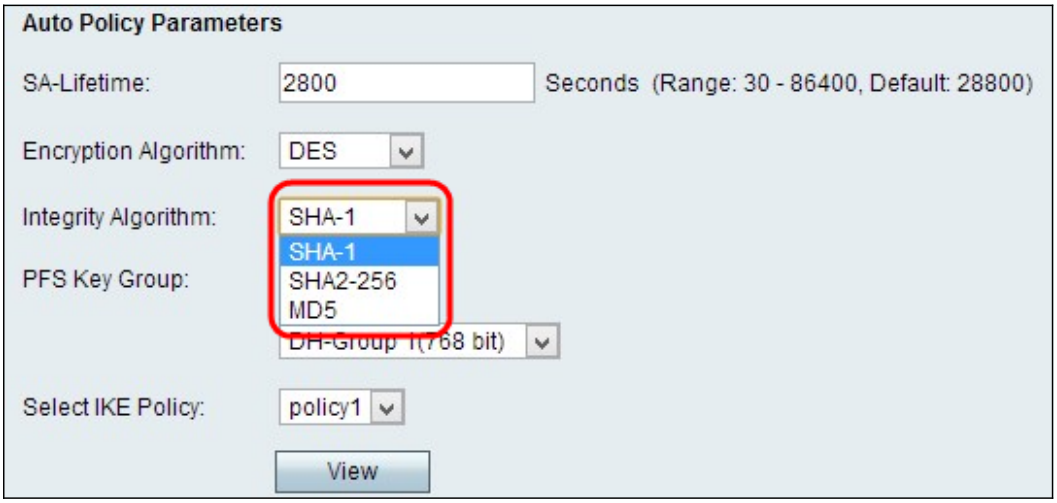
·DES: lo standard DES (Data Encryption Standard) utilizza una chiave a 56 bit per la crittografia dei dati. DES è obsoleto e deve essere utilizzato solo se un endpoint supporta solo DES.

·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 in base all'arrotondamento eseguito dal DES. 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. In generale, AES è anche più veloce ma meno sicuro rispetto a 3DES, ma 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.

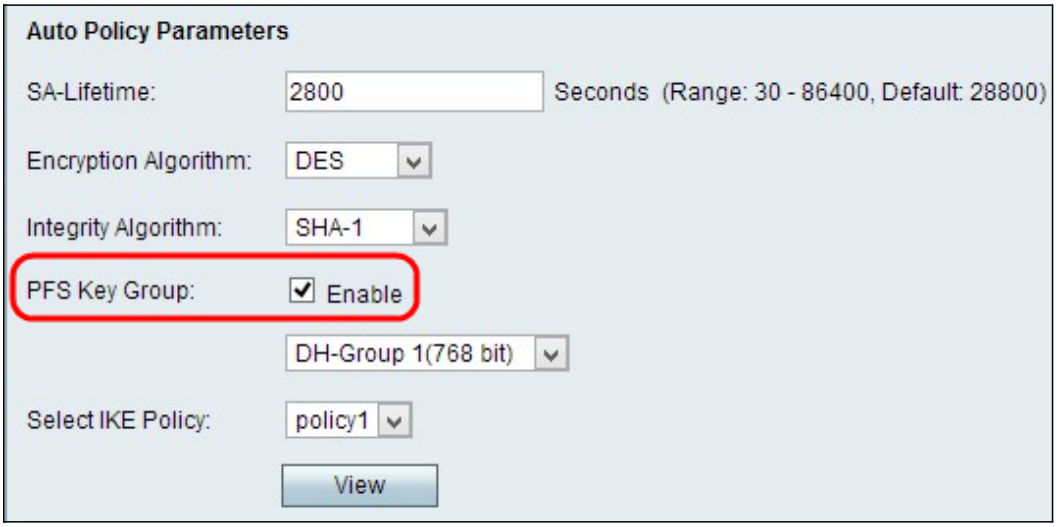


Passaggio 3. Scegliere l'algoritmo di integrità appropriato dall'elenco a discesa Algoritmo di integrità. Questo algoritmo verifica l'integrità dei dati.

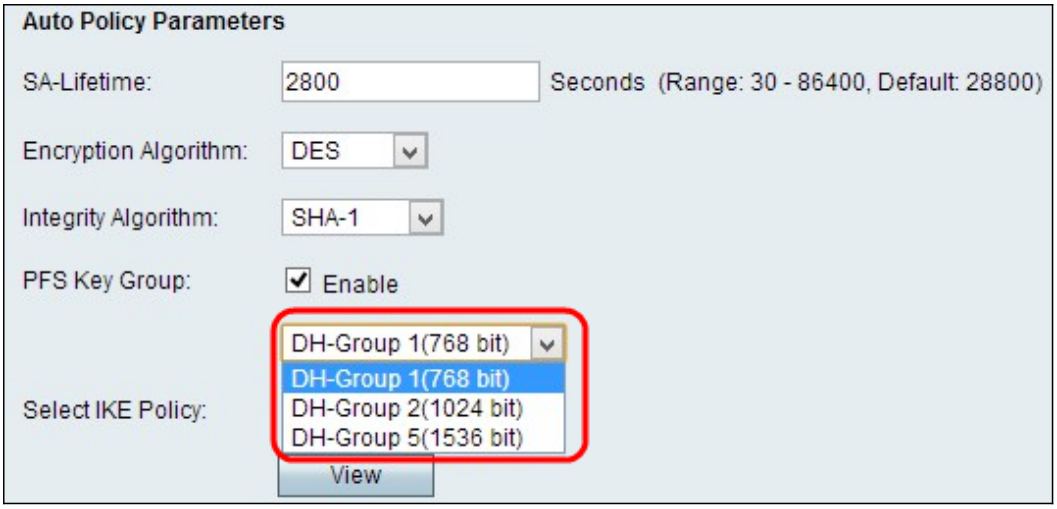
·MD5 — Questo algoritmo specifica la lunghezza della chiave a 16 caratteri. MD5 (Message-Digest Algorithm five) non è resistente alle collisioni ed è adatto per applicazioni come i certificati SSL o le firme digitali che si basano su questa proprietà. MD5 comprime qualsiasi flusso di byte in un valore a 128 bit, mentre SHA lo comprime in un valore a 160 bit. MD5 è leggermente più economico da calcolare, tuttavia è una versione precedente dell'algoritmo hash ed è vulnerabile agli attacchi di collisione.

·SHA1 — Secure Hash Algorithm versione 1 (SHA1) è una funzione hash a 160 bit più sicura di MD5, ma richiede più tempo per l'elaborazione.

·SHA2-256 — Questo algoritmo specifica la lunghezza della chiave a 32 caratteri.



Passaggio 4. (Facoltativo) Selezionare la casella di controllo **Abilita** nel campo *Gruppo di chiavi PFS* per abilitare il segreto di inoltro perfetto, che consente di migliorare la protezione.

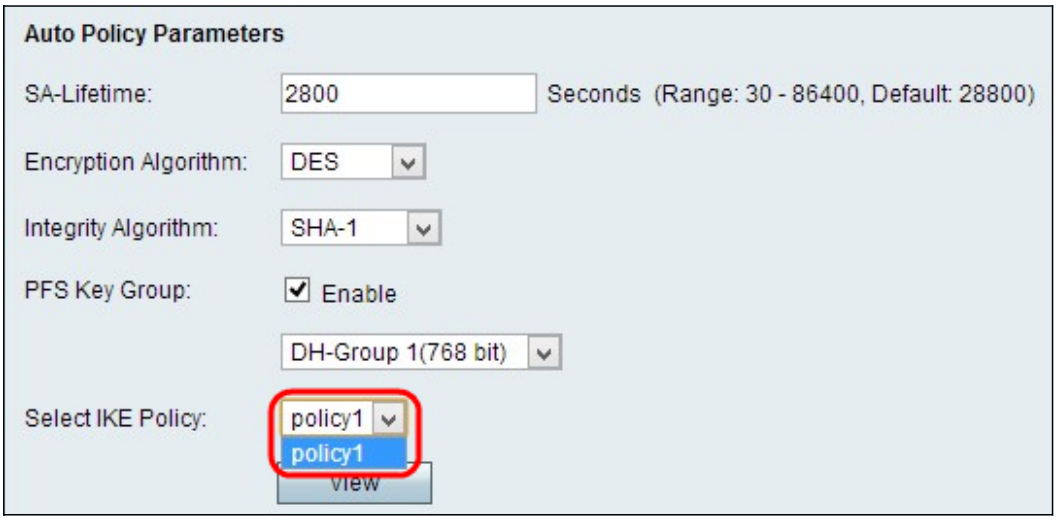


Passaggio 5. Se nel passaggio 4 è stata selezionata l'opzione **Abilita**, scegliere lo scambio di chiavi Diffie-Hellman appropriato dall'elenco a discesa *Gruppo di chiavi PFS*.

·Gruppo 1 - 768 bit: rappresenta la chiave con il livello di protezione più basso e il gruppo di autenticazione più non sicuro. Ma ha bisogno di meno tempo per calcolare le chiavi IKE. È preferibile se la velocità della rete è bassa.

·Gruppo 2 - 1024 bit: rappresenta una chiave di livello superiore e un gruppo di autenticazione più sicuro. Ma ha bisogno di un po' di tempo per calcolare le chiavi IKE.

·Gruppo 5 - 1536 bit: rappresenta la chiave con il livello di protezione più elevato e il gruppo di autenticazione più sicuro. È necessario più tempo per calcolare i tasti IKE. È preferibile se la velocità della rete è elevata.



Passaggio 6. Scegliere il criterio IKE appropriato dall'elenco a discesa *Seleziona criterio IKE*. IKE (Internet Key Exchange) è un protocollo utilizzato per stabilire una connessione sicura per la comunicazione in una VPN. Questa connessione sicura stabilita è denominata associazione di sicurezza (SA, Security Association). Affinché una VPN funzioni correttamente, le policy IKE per entrambi gli endpoint devono essere identiche.

Passaggio 7. Fare clic su **Save** per applicare tutte le impostazioni.

Nota: SA - La durata, l'algoritmo di crittografia, l'algoritmo di integrità, il gruppo di chiavi PFS e i criteri IKE devono essere gli stessi all'altra estremità del tunnel VPN per una connessione riuscita.

Per visualizzare altri articoli sull'RV110W, fare clic qui.