Configurazione di VPN (Virtual Private Network) da gateway a gateway su serie RV320 e RV325 VPN Router

Obiettivo

Le VPN vengono utilizzate per formare connessioni molto sicure su due endpoint, su Internet pubblico o condiviso, tramite quello che viene chiamato tunnel VPN. In particolare, una connessione VPN da gateway a gateway consente a due router di connettersi in modo sicuro tra loro e al client di un'estremità di apparire logicamente parte della stessa rete remota dell'altra estremità. In questo modo è possibile condividere dati e risorse su Internet in modo più semplice e sicuro. Per stabilire una connessione VPN da gateway a gateway riuscita, è necessario eseguire la configurazione su entrambi i lati della connessione. Lo scopo di questo articolo è quello di guidare l'utente nella configurazione di una connessione VPN da gateway a gateway sulla serie RV32x VPN Router.

Dispositivi interessati

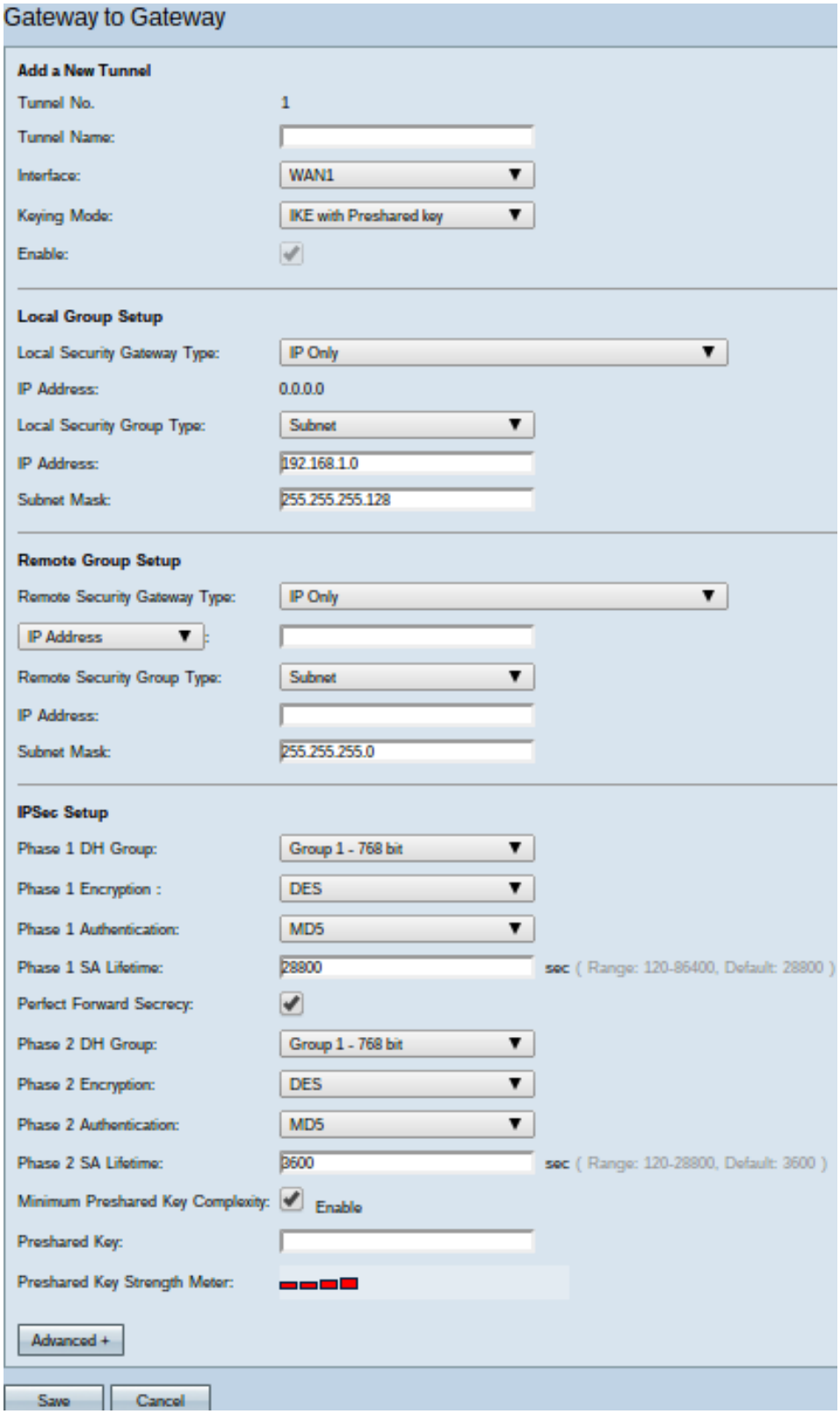
·RV320 Dual WAN VPN Router
· RV325 Gigabit Dual WAN VPN Router

Versione del software

·v1.1.0.09

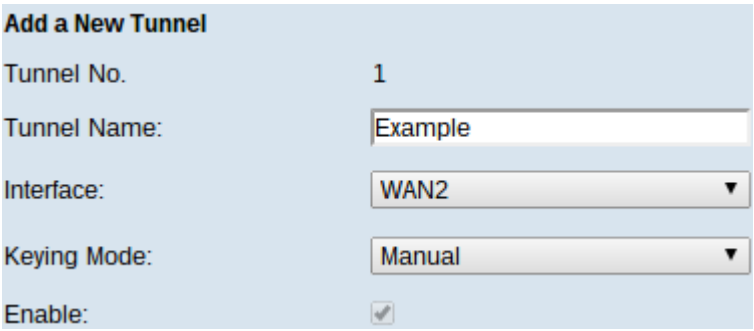
Da gateway a gateway

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **VPN > Gateway to Gateway**. Viene visualizzata la pagina *Gateway to Gateway*:



Affinché la connessione VPN funzioni correttamente, è necessario che i valori IPSec (Internet Protocol Security) su entrambi i lati della connessione siano uguali. Entrambi i lati della connessione devono appartenere a reti LAN (Local Area Network) diverse e almeno uno dei router deve essere identificabile da un indirizzo IP statico o da un nome host DNS dinamico.

Aggiungi nuovo tunnel



·N. tunnel — visualizza il tunnel corrente che verrà creato. Il router supporta 100 tunnel.

Passaggio 1. Immettere un nome per il tunnel VPN nel campo Nome tunnel. Non deve necessariamente corrispondere al nome utilizzato sull'altra estremità del tunnel.

Passaggio 2. Dall'elenco a discesa Interface (Interfaccia), selezionare la porta WAN (Wide Area Network) da utilizzare per il tunnel.

·WAN1: la porta WAN dedicata del router.

·WAN2: la porta WAN2/DMZ del router. Viene visualizzato nel menu a discesa solo se è stato configurato come WAN e non come porta DMZ (Demilitarize Zone).

·USB1: la porta USB1 del router. Funziona solo se alla porta è collegato un dongle USB 3G/4G/LTE.

·USB2: la porta USB2 del router. Funziona solo se alla porta è collegato un dongle USB 3G/4G/LTE.

Passaggio 3. Dall'elenco a discesa Modalità di impostazione chiavi scegliere la protezione del tunnel da utilizzare.

·Manuale - Questa opzione consente di configurare manualmente la chiave anziché negoziarla con l'altro lato della connessione VPN.

·IKE con chiave già condivisa: scegliere questa opzione per abilitare il protocollo IKE (Internet Key Exchange Protocol) che imposta un'associazione di sicurezza nel tunnel VPN. IKE utilizza una chiave già condivisa per autenticare un peer remoto.

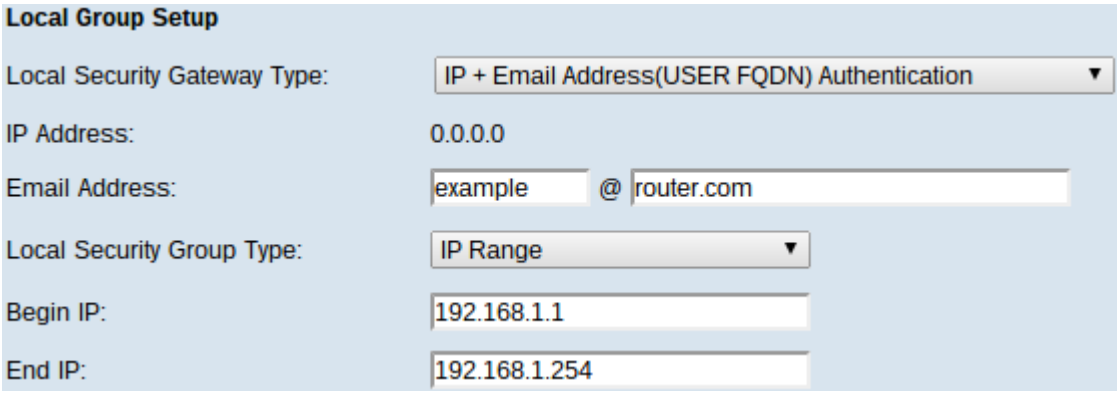
·IKE con certificato: scegliere questa opzione per abilitare il protocollo IKE (Internet Key Exchange) con certificato, che offre un modo più sicuro per generare e scambiare automaticamente le chiavi già condivise in modo da stabilire comunicazioni più autenticate e sicure per il tunnel.

Passaggio 4. Selezionare la casella di controllo Abilita per abilitare il tunnel VPN. Per impostazione predefinita è attivata.

Installazione gruppo locale

Queste impostazioni devono corrispondere alle impostazioni di "Configurazione gruppo remoto" per il router sull'altra estremità del tunnel VPN.

Nota: Se è stata selezionata l'opzione Manuale o IKE con chiave già condivisa dall'elenco a discesa Modalità di impostazione chiavi nel passaggio 3 di Aggiungi nuovo tunnel, avviare dal passaggio 1 e ignorare i passaggi da 2 a 4. Se è stata selezionata l'opzione IKE con certificato, ignorare il passaggio 1.



Passaggio 1. Dall'elenco a discesa Local Security Gateway Type (Tipo di gateway di sicurezza locale) scegliere il metodo per identificare il router per stabilire il tunnel VPN.

·Solo IP: l'accesso al tunnel è possibile solo tramite una rete IP WAN statica. È possibile scegliere questa opzione se solo il router ha un IP WAN statico. L'indirizzo IP statico della WAN è un campo generato automaticamente.

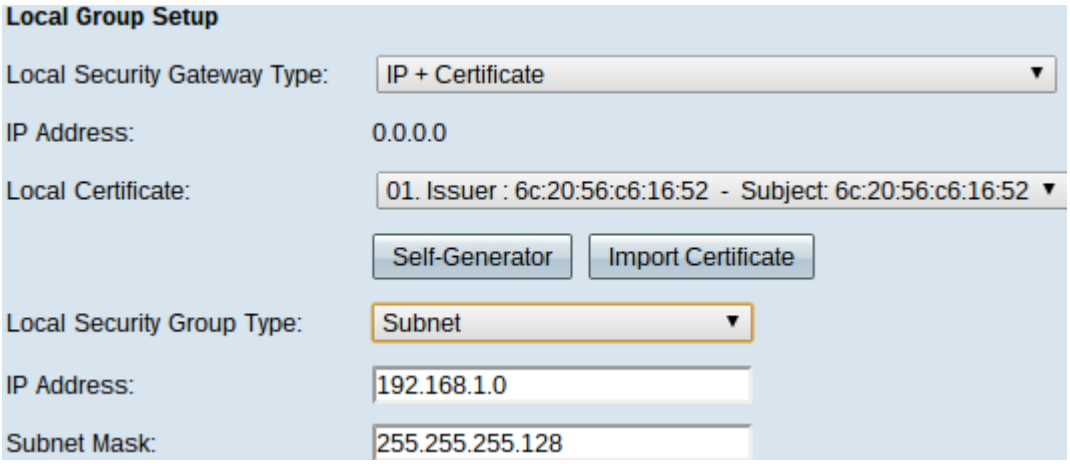
·Autenticazione IP + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP statico e un dominio registrato. Se si sceglie questa opzione, immettere il nome del dominio registrato nel campo Nome dominio. L'indirizzo IP statico della WAN è un campo generato automaticamente.

·Autenticazione IP + indirizzo e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP statico e un indirizzo e-mail. Se si sceglie questa opzione, immettere l'Indirizzo e-mail nel campo Indirizzo e-mail. L'indirizzo IP statico della WAN è un campo generato automaticamente.

·Autenticazione IP dinamico + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP dinamico e un dominio registrato. Se si sceglie questa opzione, immettere il nome del dominio registrato nel campo Nome dominio.

·Autenticazione IP dinamico + indirizzo e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP dinamico e un indirizzo e-mail. Se si sceglie questa opzione, immettere l'Indirizzo e-mail nel campo Indirizzo e-mail.

Nota: Le modifiche seguenti nell'area Installazione gruppo locale vengono modificate quando si utilizza IKE con Certificato.



L'elenco a discesa Tipo di gateway di sicurezza locale non è più modificabile e visualizza IP + certificato. Risorsa LAN che può utilizzare il tunnel.
Il campo Indirizzo IP visualizza l'indirizzo IP WAN del dispositivo. Non è modificabile

dall'utente.

Passaggio 2. Scegliere un certificato dall'elenco a discesa Certificato locale. I certificati offrono una maggiore sicurezza di autenticazione sulle connessioni VPN.

Passaggio 3. (Facoltativo) Fare clic sul pulsante **Self-Generator** per visualizzare la finestra *Generatore di certificati* per configurare e generare certificati.

Passaggio 4. (Facoltativo) Fare clic sul pulsante **Importa certificato** per visualizzare la finestra *Certificato* per visualizzare e configurare i certificati.

Passaggio 5. Dall'elenco a discesa Tipo di gruppo di sicurezza locale scegliere una delle opzioni seguenti:

·Indirizzo IP - Questa opzione consente di specificare un dispositivo che può utilizzare il tunnel VPN. È sufficiente immettere l'indirizzo IP del dispositivo nel campo Indirizzo IP.

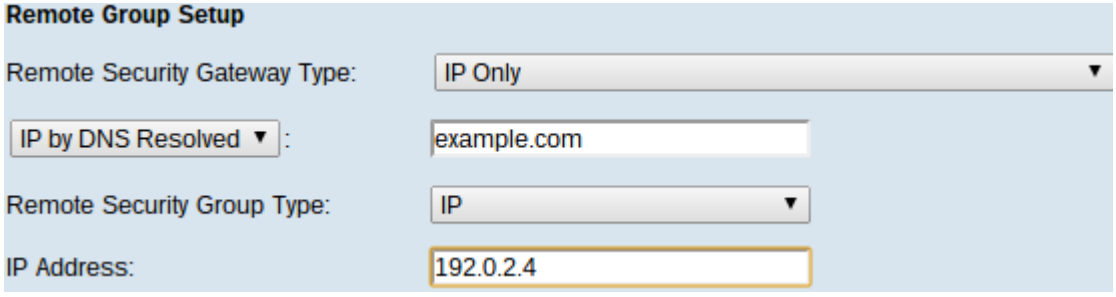
·Subnet: scegliere questa opzione per consentire a tutti i dispositivi che appartengono alla stessa subnet di utilizzare il tunnel VPN. È necessario immettere l'indirizzo IP di rete nel campo Indirizzo IP e la relativa subnet mask nel campo Subnet mask.

·Intervallo IP: scegliere questa opzione per specificare un intervallo di dispositivi che possono usare il tunnel VPN. Immettere il primo indirizzo IP e l'ultimo indirizzo IP dell'intervallo di dispositivi nei campi Inizio IP e Fine IP.

Installazione gruppo remoto

Queste impostazioni devono corrispondere alle impostazioni di "Configurazione gruppo locale" per il router sull'altra estremità del tunnel VPN.

Nota: Se è stata selezionata l'opzione Manuale o IKE con chiave già condivisa dall'elenco a discesa Modalità di impostazione chiavi nel passaggio 3 di Aggiungi nuovo tunnel, avviare dal passaggio 1 e ignorare i passaggi da 2 a 5. In alternativa, se è stata selezionata l'opzione IKE con certificato, ignorare il passaggio 1.



Passaggio 1. Dall'elenco a discesa Tipo di gateway di sicurezza remoto, scegliere il metodo per identificare l'altro router per stabilire il tunnel VPN.

·Solo IP: l'accesso al tunnel è possibile solo tramite una rete IP WAN statica. Se si conosce l'indirizzo IP del router remoto, selezionare Indirizzo IP nell'elenco a discesa sotto il campo Tipo di gateway di sicurezza remoto e immettere l'indirizzo. Scegliere IP da DNS risolto se non si conosce l'indirizzo IP ma si conosce il nome di dominio e immettere il nome di dominio del router nel campo IP da DNS risolto.

·Autenticazione IP + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP statico e un dominio registrato del router. Se si conosce l'indirizzo IP del router

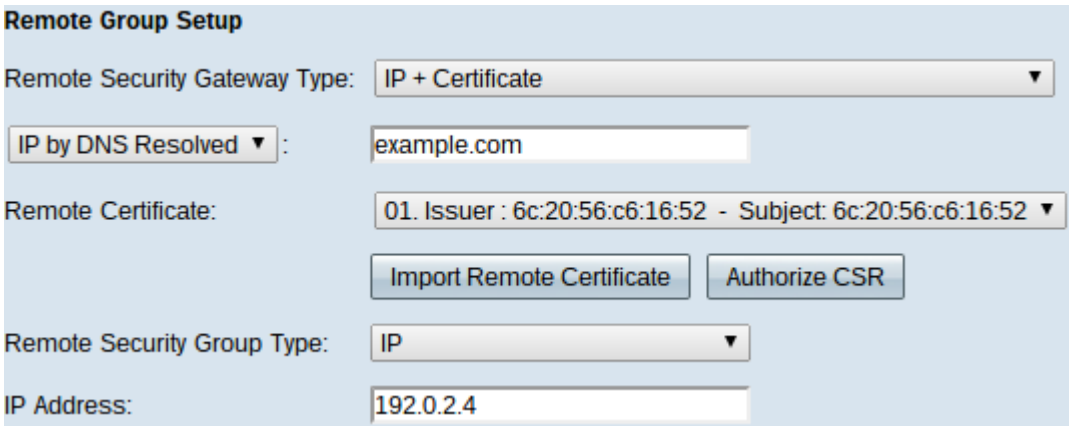
remoto, selezionare Indirizzo IP nell'elenco a discesa sotto il campo Tipo di gateway di sicurezza remoto e immettere l'indirizzo. Scegliere IP da DNS risolto se non si conosce l'indirizzo IP ma si conosce il nome di dominio e immettere il nome di dominio del router nel campo IP da DNS risolto. Se si sceglie questa opzione, immettere il nome del dominio registrato nel campo Nome dominio.

·Autenticazione IP + indirizzo e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP statico e un indirizzo e-mail.Se si conosce l'indirizzo IP del router remoto, scegliere l'indirizzo IP nell'elenco a discesa direttamente sotto il campo Tipo Gateway di sicurezza remota e immettere l'indirizzo. Scegliere IP da DNS risolto se non si conosce l'indirizzo IP ma si conosce il nome di dominio e immettere il nome di dominio del router nel campo IP da DNS risolto. Immettere l'indirizzo di posta elettronica nel campo Indirizzo di posta elettronica.

·Autenticazione IP dinamico + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP dinamico e un dominio registrato. Se si sceglie questa opzione, immettere il nome del dominio registrato nel campo Nome dominio.

·Autenticazione IP dinamico + indirizzo e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP dinamico e un indirizzo e-mail. Se si sceglie questa opzione, immettere l'Indirizzo e-mail nel campo Indirizzo e-mail.
Nota: Se entrambi i router dispongono di indirizzi IP dinamici, NON scegliere IP dinamico + indirizzo e-mail per entrambi i gateway.

Nota: Le modifiche seguenti nell'area Installazione gruppo remoto vengono modificate quando si utilizza IKE con il certificato.



L'elenco a discesa Tipo di gateway di sicurezza remoto non è più modificabile e visualizza IP + certificato. Risorsa LAN che può utilizzare il tunnel.

Passaggio 2. Se si conosce l'indirizzo IP del router remoto, scegliere Indirizzo IP nell'elenco a discesa direttamente sotto il campo Tipo di gateway di sicurezza remoto e immettere l'indirizzo. Scegliere IP da DNS risolto se non si conosce l'indirizzo IP ma si conosce il nome del dominio e immettere il nome di dominio del router remoto nel campo IP da DNS risolto

Passaggio 3. Scegliere un certificato dall'elenco a discesa Certificato remoto. I certificati offrono una maggiore sicurezza di autenticazione sulle connessioni VPN.

Passaggio 4. (Facoltativo) Fare clic sul pulsante **Importa certificato remoto** per importare un nuovo certificato.

Passaggio 5. (Facoltativo) Fare clic sul pulsante **Autorizza CSR** per identificare il certificato con una richiesta di firma digitale.

Passaggio 6. Dall'elenco a discesa Tipo di gruppo di sicurezza locale scegliere una delle opzioni seguenti:

·Indirizzo IP - Questa opzione consente di specificare un dispositivo che può utilizzare il tunnel VPN. È sufficiente immettere l'indirizzo IP del dispositivo nel campo Indirizzo IP.

·Subnet: scegliere questa opzione per consentire a tutti i dispositivi che appartengono alla stessa subnet di utilizzare il tunnel VPN. È necessario immettere l'indirizzo IP di rete nel campo Indirizzo IP e la relativa subnet mask nel campo Subnet mask.

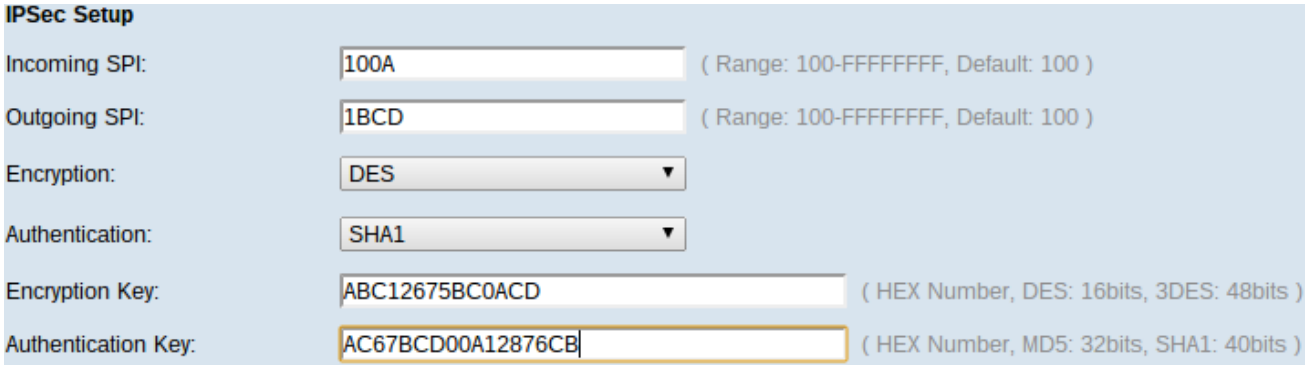
·Intervallo IP: scegliere questa opzione per specificare un intervallo di dispositivi che possono usare il tunnel VPN. Specificare il primo e l'ultimo indirizzo IP dell'intervallo di dispositivi. Nei campi Inizio IP e Fine IP.

Installazione di IPSec

Affinché la crittografia venga configurata correttamente tra le due estremità del tunnel VPN, entrambe devono avere le stesse impostazioni. In questo caso, IPSec crea un'autenticazione protetta tra i due dispositivi. Lo fa in due fasi.

Impostazione IPSec per la modalità di impostazione manuale

Disponibile solo se è stato selezionato Manuale dall'elenco a discesa Modalità di impostazione chiavi nel Passaggio 3 di Aggiunta di un nuovo tunnel. Si tratta di una modalità di protezione personalizzata che consente di generare una nuova chiave di protezione autonomamente e di non negoziarla con la chiave. È la soluzione migliore da utilizzare durante la risoluzione dei problemi e in ambienti statici di piccole dimensioni.



Passaggio 1. Immettere il valore esadecimale univoco per l'indice dei parametri di sicurezza (SPI) in ingresso nel campo SPI in ingresso. L'indice SPI è contenuto nell'intestazione del protocollo ESP (Encapsulating Security Payload) che determina congiuntamente la protezione del pacchetto in ingresso. È possibile immettere da 100 a FFFFFFFF.

Passaggio 2. Inserire il valore esadecimale univoco per SPI nel campo SPI in uscita. SPI è contenuto nell'intestazione ESP che determina congiuntamente la protezione del pacchetto in uscita. È possibile immettere da 100 a FFFFFFFF.

Nota: Per stabilire un tunnel, l'indice SPI in entrata e in uscita devono corrispondere tra loro su entrambe le estremità.

Passaggio 3. Scegliere il metodo di crittografia appropriato dall'elenco a discesa Crittografia. La crittografia consigliata è 3DES. Il tunnel VPN deve utilizzare lo stesso metodo di crittografia per entrambe le estremità.

·DES: DES (Data Encryption Standard) è un vecchio metodo di crittografia a 56 bit, più compatibile con le versioni precedenti, che non è così sicuro come è facile da interrompere.

·3DES: 3DES (Triple Data Encryption Standard) è un semplice metodo di crittografia a 168 bit che consente di aumentare le dimensioni della chiave tramite la crittografia dei dati per tre volte, garantendo una maggiore protezione rispetto a DES.

Passaggio 4. Scegliere il metodo di autenticazione appropriato dall'elenco a discesa Autenticazione. L'autenticazione consigliata è SHA1. Il tunnel VPN deve utilizzare lo stesso metodo di autenticazione per entrambe le estremità.

·MD5 — MD5 (Message Digest Algorithm-5) rappresenta una funzione hash esadecimale a 32 cifre che fornisce protezione ai dati da attacchi dannosi tramite il calcolo del checksum.

·SHA1 — SHA1 (Secure Hash Algorithm versione 1) è una funzione hash a 160 bit più sicura di MD5.

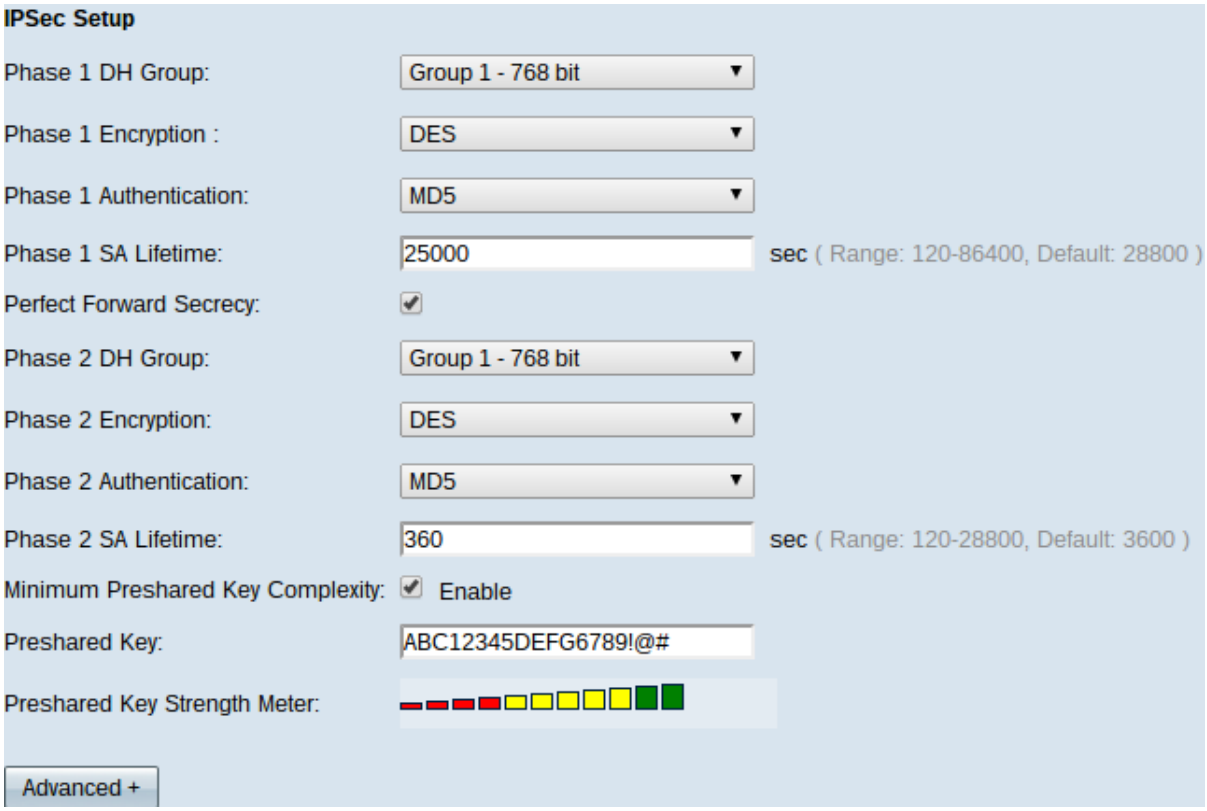
Passaggio 5. Immettere la chiave per crittografare e decrittografare i dati nel campo Chiave di crittografia. Se si sceglie DES come metodo di crittografia al punto 3, immettere un valore esadecimale a 16 cifre. Se si sceglie 3DES come metodo di cifratura al punto 3, immettere un valore esadecimale di 40 cifre.

Passaggio 6. Immettere una chiave già condivisa per autenticare il traffico nel campo Chiave di autenticazione. Se si sceglie MD5 come metodo di autenticazione al punto 4, immettere un valore esadecimale di 32 cifre. Se si sceglie Agente integrità sistema come metodo di autenticazione nel passaggio 4, immettere un valore esadecimale di 40 cifre. Il tunnel VPN deve utilizzare la stessa chiave già condivisa per entrambe le estremità.

Passaggio 7. Fare clic su **Save** per salvare le impostazioni.

Configurazione IPSec per IKE con chiave già condivisa

Disponibile solo se è stato selezionato IKE con chiave già condivisa dall'elenco a discesa Modalità di impostazione chiavi nel passaggio 3 di Aggiungi nuovo tunnel.



Passaggio 1. Scegliere il gruppo DH Fase 1 appropriato dall'elenco a discesa Gruppo DH Fase 1. La fase 1 viene utilizzata per stabilire una associazione di sicurezza logica (SA, Security Association) semplice tra le due estremità del tunnel e supportare la comunicazione di autenticazione protetta. Diffie-Hellman (DH) è un protocollo di scambio chiave di crittografia utilizzato durante la connessione di Fase 1 per condividere una chiave segreta per autenticare la comunicazione.

·Gruppo 1 - 768 bit: rappresenta la chiave con il livello di protezione più alto 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.

·Gruppo 2 - 1024 bit: rappresenta una chiave di livello superiore e un gruppo di autenticazione più sicuro. 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 basso e il gruppo di autenticazione più non sicuro. Richiede meno tempo per calcolare i tasti IKE. È preferibile se la velocità della rete è bassa.

Passaggio 2. Scegliere la crittografia appropriata per la fase 1 per cifrare la chiave dall'elenco a discesa Crittografia fase 1. si consiglia AES-128, AES-192 o AES-256. Il tunnel VPN deve utilizzare lo stesso metodo di crittografia per entrambe le estremità.

·DES: Data Encryption Standard (DES) è un vecchio metodo di crittografia a 56 bit che, al giorno d'oggi, non è molto sicuro.

·3DES: Triple Data Encryption Standard (3DES) è un semplice metodo di crittografia a 168 bit che consente di aumentare le dimensioni della chiave tramite la crittografia dei dati per tre volte, garantendo una maggiore sicurezza rispetto a DES.

·AES-128 — Advanced Encryption Standard (AES) è un metodo di crittografia a 128 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 10 cicli.

·AES-192 — Metodo di crittografia a 192 bit che trasforma il testo normale in testo cifrato

attraverso ripetizioni a 12 cicli.

·AES-256 — È un metodo di crittografia a 256 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 14 cicli.

Passaggio 3. Scegliere il metodo di autenticazione appropriato dall'elenco a discesa Fase 1 Autenticazione. Il tunnel VPN deve utilizzare lo stesso metodo di autenticazione per entrambe le estremità. Si consiglia SHA1.

·MD5 — Message Digest Algorithm-5 (MD5) rappresenta una funzione hash esadecimale a 32 cifre che fornisce protezione ai dati da attacchi dannosi tramite il calcolo del checksum.

·SHA1: una funzione hash a 160 bit più sicura di MD5.

Passaggio 4. Immettere il periodo di tempo in secondi durante il quale il tunnel VPN rimane attivo nel campo Durata ASA fase 1.

Passaggio 5. Selezionare la casella di controllo Perfect Forward Secrecy per proteggere ulteriormente le chiavi. Questa opzione consente di generare una nuova chiave in caso di violazione di una chiave. I dati crittografati vengono compromessi solo tramite la chiave compromessa. In questo modo la comunicazione risulta più sicura e autenticata, poiché protegge altre chiavi anche se compromesse. Si tratta di un'azione consigliata in quanto offre maggiore protezione.

Passaggio 6. Scegliere il gruppo DH Fase 2 appropriato dall'elenco a discesa Gruppo DH Fase 2. La fase 1 viene utilizzata per stabilire una associazione di sicurezza logica (SA, Security Association) semplice tra le due estremità del tunnel e supportare la comunicazione di autenticazione protetta. DH è un protocollo di scambio chiave crittografica utilizzato durante la connessione di fase 1 per condividere la chiave segreta per autenticare la comunicazione.

·Gruppo 1 - 768 bit: rappresenta la chiave con il livello di protezione più alto 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.

·Gruppo 2 - 1024 bit: rappresenta una chiave di livello superiore e un gruppo di autenticazione più sicuro. 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 basso e il gruppo di autenticazione più non sicuro. Richiede meno tempo per calcolare i tasti IKE. È preferibile se la velocità della rete è bassa.

Nota: Poiché non viene generata alcuna nuova chiave, non è necessario configurare il gruppo DH Fase 2 se si deseleziona Segreto inoltro perfetto nel passo 5.

Passaggio 7. Scegliere la crittografia appropriata per la fase 2 per crittografare la chiave dall'elenco a discesa Crittografia fase 2. si consiglia AES-128, AES-192 o AES-256. Il tunnel VPN deve utilizzare lo stesso metodo di crittografia per entrambe le estremità.

·DES: DES è un vecchio metodo di crittografia a 56 bit che non è molto sicuro al giorno d'oggi.

·3DES: 3DES è un semplice metodo di crittografia a 168 bit che consente di aumentare le dimensioni della chiave tramite la crittografia dei dati per tre volte, garantendo una maggiore protezione rispetto a DES.

·AES-128 — AES è un metodo di crittografia a 128 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 10 cicli.

·AES-192 — Metodo di crittografia a 192 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni a 12 cicli.

·AES-256 — È un metodo di crittografia a 256 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 14 cicli.

Passaggio 8. Scegliere il metodo di autenticazione appropriato dall'elenco a discesa Autenticazione fase 2. Il tunnel VPN deve utilizzare lo stesso metodo di autenticazione per entrambe le estremità.

·MD5 — MD5 rappresenta una funzione hash esadecimale a 32 cifre che fornisce protezione ai dati da attacchi dannosi tramite il calcolo del checksum.

·SHA1 — Secure Hash Algorithm versione 1 (SHA1) è una funzione hash a 160 bit più sicura di MD5.

·Null — Non viene utilizzato alcun metodo di autenticazione.

Passaggio 9. Immettere il periodo di tempo in secondi durante il quale il tunnel VPN rimane attivo nel campo Durata SA fase 2.

Passaggio 10. Selezionare la casella di controllo Complessità minima chiave già condivisa se si desidera abilitare il misuratore di affidabilità per la chiave già condivisa.

Passaggio 11. Immettere una chiave condivisa in precedenza tra i peer IKE nel campo Chiave già condivisa. È possibile utilizzare fino a 30 caratteri esadecimali come chiave già condivisa. Il tunnel VPN deve utilizzare la stessa chiave già condivisa per entrambe le estremità.

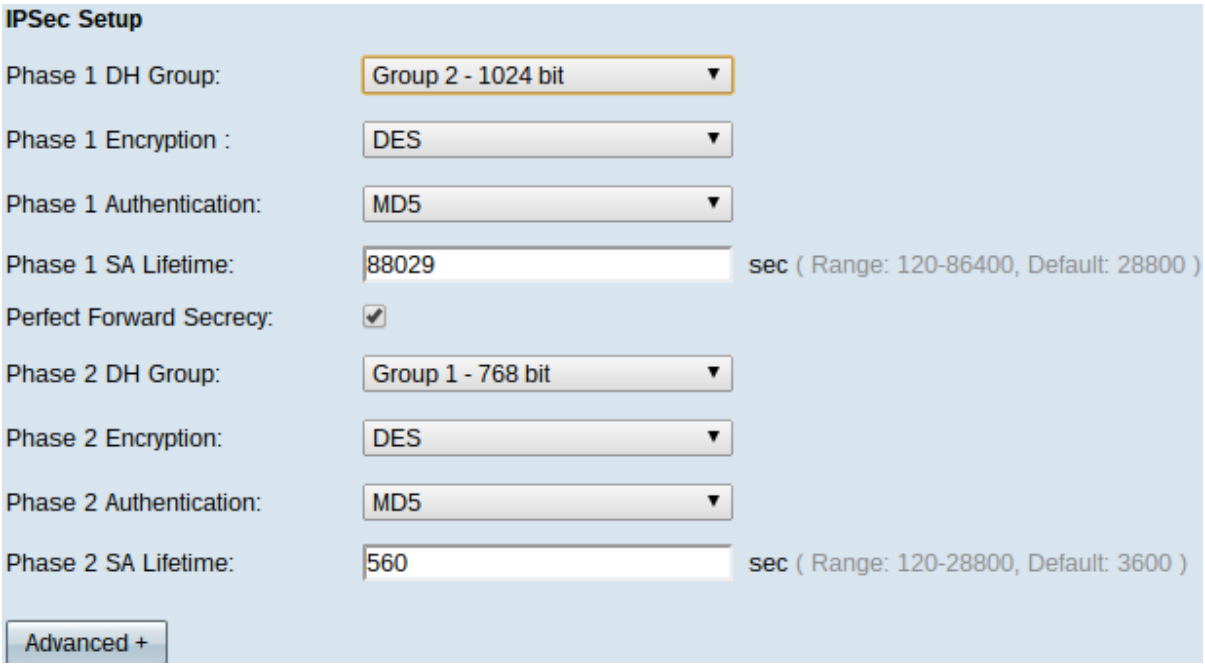
Nota: Si consiglia di modificare frequentemente la chiave già condivisa tra i peer IKE in modo che la VPN resti sicura.

Il misuratore dell'intensità della chiave già condivisa mostra l'intensità della chiave già condivisa attraverso le barre di colore. Il rosso indica una forza debole, il giallo indica una forza accettabile e il verde indica una forza forte.

Passaggio 12. Fare clic su **Save** per salvare le impostazioni.

Installazione IPSec per IKE con certificato

Disponibile solo se IKE con certificato è stato selezionato dall'elenco a discesa Modalità impostazione chiavi nel passaggio 3 di Aggiungi nuovo tunnel.



Passaggio 1. Scegliere il gruppo DH Fase 1 appropriato dall'elenco a discesa Gruppo DH Fase 1. La fase 1 viene utilizzata per stabilire l'associazione di sicurezza logica simplex tra le due estremità del tunnel e supportare la comunicazione di autenticazione protetta. DH è un protocollo di scambio chiave crittografica utilizzato durante la connessione di fase 1 per condividere la chiave segreta per autenticare la comunicazione.

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

·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 basso e il gruppo di autenticazione più non sicuro. Richiede meno tempo per calcolare i tasti IKE. È preferibile se la velocità della rete è bassa.

Passaggio 2. Scegliere la crittografia appropriata per la fase 1 per cifrare la chiave dall'elenco a discesa Crittografia fase 1. si consiglia AES-128, AES-192 o AES-256. Il tunnel VPN deve utilizzare lo stesso metodo di crittografia per entrambe le estremità.

·DES: DES è un vecchio metodo di crittografia a 56 bit che non è molto sicuro al giorno d'oggi.

·3DES: 3DES è un semplice metodo di crittografia a 168 bit che consente di aumentare le dimensioni della chiave tramite la crittografia dei dati per tre volte, garantendo una maggiore protezione rispetto a DES.

·AES-128 — AES è un metodo di crittografia a 128 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 10 cicli.

·AES-192 — Metodo di crittografia a 192 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni a 12 cicli.

·AES-256 — È un metodo di crittografia a 256 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 14 cicli.

Passaggio 3. Scegliere il metodo di autenticazione appropriato dall'elenco a discesa Fase 1 Autenticazione. Il tunnel VPN deve utilizzare lo stesso metodo di autenticazione per entrambe le estremità. Si consiglia SHA1.

·MD5 — MD5 rappresenta una funzione hash esadecimale a 32 cifre che fornisce protezione ai dati da attacchi dannosi tramite il calcolo del checksum.

·SHA1: una funzione hash a 160 bit più sicura di MD5.

Passaggio 4. Immettere il periodo di tempo in secondi durante il quale il tunnel VPN rimane attivo nel campo Durata ASA fase 1.

Passaggio 5. Selezionare la casella di controllo Perfect Forward Secrecy per proteggere ulteriormente le chiavi. Questa opzione consente di generare una nuova chiave in caso di violazione di una chiave. I dati crittografati vengono compromessi solo tramite la chiave compromessa. In questo modo la comunicazione risulta più sicura e autenticata, poiché protegge le altre chiavi quando viene compromessa un'altra chiave. Si tratta di un'azione consigliata in quanto offre maggiore protezione.

Passaggio 6. Scegliere il gruppo DH Fase 2 appropriato dall'elenco a discesa Gruppo DH Fase 2. La fase 1 viene utilizzata per stabilire l'associazione di sicurezza logica simplex tra le due estremità del tunnel e supportare la comunicazione di autenticazione protetta. DH è un protocollo di scambio chiave crittografica utilizzato durante la connessione di fase 1 per condividere la chiave segreta per autenticare la comunicazione.

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

·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 basso e il gruppo di autenticazione più non sicuro. Richiede meno tempo per calcolare i tasti IKE. È preferibile se la velocità della rete è bassa.

Nota: Poiché non viene generata alcuna nuova chiave, non è necessario configurare il gruppo DH per la fase 2 se nel passaggio 5 è stata deselezionata l'opzione Segretezza inoltro perfetta.

Passaggio 7. Scegliere la crittografia appropriata per la fase 2 per crittografare la chiave dall'elenco a discesa Crittografia fase 2. si consiglia AES-128, AES-192 o AES-256. Il tunnel VPN deve utilizzare lo stesso metodo di crittografia per entrambe le estremità.

·DES: DES è un vecchio metodo di crittografia a 56 bit che non è molto sicuro al giorno d'oggi.

·3DES: 3DES è un semplice metodo di crittografia a 168 bit che consente di aumentare le dimensioni della chiave tramite la crittografia dei dati per tre volte, garantendo una maggiore protezione rispetto a DES.

·AES-128 — AES è un metodo di crittografia a 128 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 10 cicli.

·AES-192 — Metodo di crittografia a 192 bit che trasforma il testo normale in testo cifrato

attraverso ripetizioni a 12 cicli.

·AES-256 — È un metodo di crittografia a 256 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 14 cicli.

Passaggio 8. Scegliere il metodo di autenticazione appropriato dall'elenco a discesa Autenticazione fase 2. Il tunnel VPN deve utilizzare lo stesso metodo di autenticazione per entrambe le estremità.

·MD5 — MD5 rappresenta una funzione hash esadecimale a 32 cifre che fornisce protezione ai dati da attacchi dannosi tramite il calcolo del checksum.

·SHA1 — SHA1 è una funzione hash a 160 bit più sicura di MD5.

·Null — Non viene utilizzato alcun metodo di autenticazione.

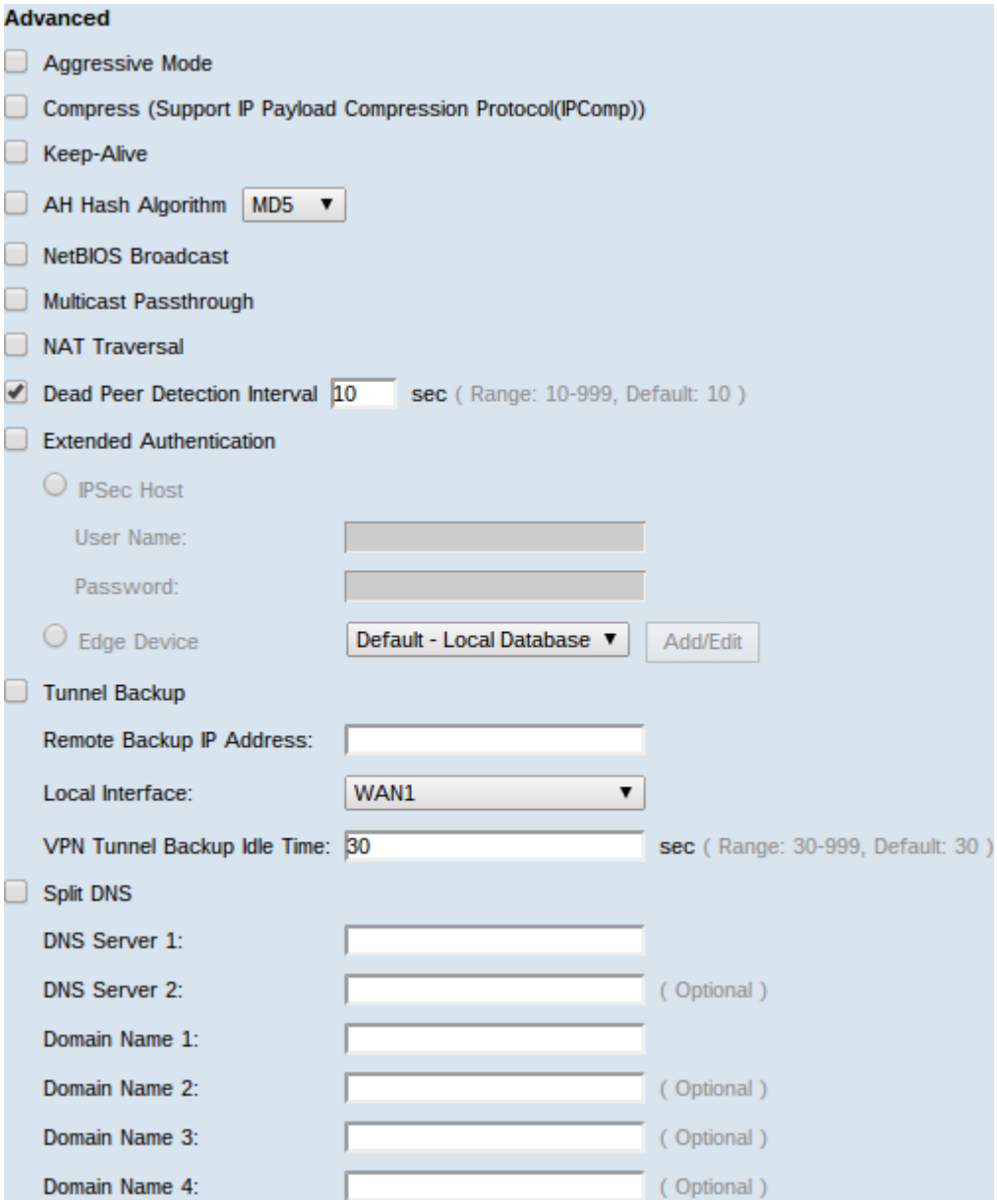
Passaggio 9. Immettere il periodo di tempo in secondi durante il quale il tunnel VPN rimane attivo nel campo Durata SA fase 2.

Passaggio 10. Fare clic su **Save** per salvare le impostazioni.

(Facoltativo) Configurazione avanzata IPSec per IKE con certificato e IKE con chiave già condivisa

Le opzioni avanzate sono disponibili se è stato selezionato IKE con certificato o IKE con chiave condivisa dall'elenco a discesa Modalità di impostazione chiavi nel passaggio 3 di Aggiungi nuovo tunnel. Le stesse impostazioni sono disponibili per entrambi i tipi di modalità di trasparenza.

Passaggio 1. Fare clic sul pulsante **Advanced+** per visualizzare le opzioni IPSec avanzate.



Passaggio 2. Selezionare la casella di controllo Modalità aggressiva se la velocità della rete è bassa. Scambia gli ID dei punti finali del tunnel in testo non crittografato durante la connessione SA, operazione che richiede meno tempo per lo scambio ma meno protezione.

Passaggio 3. Selezionare la casella di controllo Comprimi (Support IP Payload Compression Protocol (IPComp)) per comprimere le dimensioni del datagramma IP. IPComp è un protocollo di compressione IP che viene utilizzato per comprimere le dimensioni del datagramma IP se la velocità della rete è bassa e l'utente desidera trasmettere rapidamente i dati senza alcuna perdita attraverso la rete lenta.

Passaggio 4. Selezionare la casella di controllo Keep-Alive se si desidera che la connessione del tunnel VPN rimanga sempre attiva. Aiuta a ristabilire le connessioni immediatamente se una connessione diventa inattiva.

Passaggio 5. Selezionare la casella di controllo AH Hash Algorithm se si desidera autenticare l'intestazione AH (Authenticate Header). AH fornisce l'autenticazione all'origine dei dati, l'integrità dei dati tramite checksum e la protezione viene estesa nell'intestazione IP. Il tunnel deve avere lo stesso algoritmo per entrambi i lati.

·MD5 — MD5 rappresenta una funzione hash esadecimale a 128 cifre che fornisce protezione ai dati da attacchi dannosi tramite il calcolo del checksum.

·SHA1 — SHA1 è una funzione hash a 160 bit più sicura di MD5.

Passaggio 6. Selezionare Trasmissione NetBIOS se si desidera consentire il traffico non instradabile attraverso il tunnel VPN. L'opzione di default è deselezionata. NetBIOS viene utilizzato per rilevare risorse di rete come stampanti, computer e così via nella rete tramite alcune applicazioni software e funzionalità di Windows come Risorse di rete.

Passaggio 7. Se il router VPN è dietro un gateway NAT, selezionare la casella per abilitare l'attraversamento NAT. Network Address Translation (NAT) consente agli utenti con indirizzi LAN privati di accedere alle risorse Internet utilizzando un indirizzo IP instradabile pubblicamente come indirizzo di origine. Tuttavia, per il traffico in entrata, il gateway NAT non dispone di un metodo automatico per convertire l'indirizzo IP pubblico in una particolare destinazione sulla LAN privata. Questo problema impedisce il corretto scambio di IPSec. NAT traversal imposta questa traduzione in ingresso. La stessa impostazione deve essere utilizzata su entrambe le estremità del tunnel.

Passaggio 8. Selezionare Dead Peer Detection Interval per verificare periodicamente la vivacità del tunnel VPN tramite hello o ACK. Se si seleziona questa casella di controllo, immettere la durata o l'intervallo in secondi dei messaggi di benvenuto desiderati.

Passaggio 9. Selezionare Autenticazione estesa per utilizzare un nome utente e una password host IPSec per autenticare i client VPN o per utilizzare il database disponibile in Gestione utenti. Affinché funzioni, è necessario che sia attivata in entrambi i dispositivi. Fare clic sul pulsante di scelta **Host IPSec** per utilizzare l'host e il nome utente IPSec e immettere il nome utente e la password nei campi Nome utente e Password. In alternativa, fare clic sul pulsante di scelta **Periferica perimetrale** per utilizzare un database. Selezionare il database desiderato dall'elenco a discesa Periferica perimetrale.

Passaggio 10. Selezionare la casella di controllo Tunnel Backup per abilitare il backup del tunnel. Questa funzione è disponibile quando è stato selezionato Intervallo rilevamento peer inattivo. Questa funzione consente al dispositivo di ristabilire il tunnel VPN tramite un'interfaccia WAN o un indirizzo IP alternativo.

·Indirizzo IP di backup remoto: un indirizzo IP alternativo per il peer remoto. Immettere in questo campo l'indirizzo IP WAN già impostato per il gateway remoto.

·Interfaccia locale: l'interfaccia WAN utilizzata per ristabilire la connessione. Selezionare l'interfaccia desiderata dall'elenco a discesa.

·Tempo di inattività del backup del tunnel VPN: il tempo scelto per l'utilizzo del tunnel di backup se il tunnel primario non è connesso. Immettilo in secondi.

Passaggio 11. Selezionare la casella di controllo Dividi DNS per abilitare la divisione del DNS. Questa funzionalità consente di inviare richieste DNS a un server DNS definito in base ai nomi di dominio specificati. Immettere i nomi dei server DNS nei campi Server DNS 1 e Server DNS 2 e immettere i nomi di dominio nei campi Nome dominio #.

Passaggio 12. Fare clic su **Save** per completare la configurazione del dispositivo.