

Configurazione VPN avanzata su RV215W

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. Questo articolo spiega come configurare la configurazione VPN avanzata su RV215W.

Dispositivi interessati

RV215W

Versione del software

•1.1.0.5

Configurazione VPN avanzata

Impostazioni iniziali

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

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

Advanced VPN Setup

NAT Traversal: Enable
NETBIOS: Enable

IKE Policy Table

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

VPN Policy Table

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

Passaggio 2. (Facoltativo) Selezionare la casella di controllo **Abilita** nel campo 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. (Facoltativo) Selezionare la casella di controllo **Abilita** nel campo NETBIOS se si desidera 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.

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. Nella tabella dei criteri IKE fare clic su **Aggiungi riga** per creare un nuovo criterio IKE. Per modificare un criterio IKE, selezionare la relativa casella di controllo e fare clic su **Modifica**. La pagina *Impostazione VPN avanzata* cambia:

The screenshot shows the 'Advanced VPN Setup' configuration page. The main section is titled 'Add / Edit IKE Policy Configuration'. It contains several fields and options for configuring an IKE policy:

- Policy Name:** IKE1
- Exchange Mode:** Main
- IKE SA Parameters:**
 - Encryption Algorithm:** 3DES
 - Authentication Algorithm:** SHA2-256
 - Pre-Shared Key:** presharedkey
 - Diffie-Hellman (DH) Group:** Group5 (1536 bit)
 - SA-Lifetime:** 3000 Seconds (Range: 30 - 86400, Default: 3600)
 - Dead Peer Detection:** Enable
 - DPD Delay:** 15 (Range: 10 - 999, Default: 10)
 - DPD Timeout:** 45 (Range: 30 - 1000, Default: 30)
- Extended Authentication:**
 - XAUTH Type:** Enable
 - Username:** User1
 - Password:** password

At the bottom of the form are three buttons: 'Save', 'Cancel', and 'Back'.

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

Passaggio 3. Dall'elenco a discesa Modalità scambio, scegliere un'opzione.

·Principale: questa opzione 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: questa opzione consente alla policy 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.

IKE SA Parameters	
Encryption Algorithm:	3DES
Authentication Algorithm:	SHA2-256
Pre-Shared Key:	presharedkey
Diffie-Hellman (DH) Group:	Group5 (1536 bit)
SA-Lifetime:	3000 Seconds (Range: 30 - 86400, Default: 3600)
Dead Peer Detection:	<input checked="" type="checkbox"/> Enable
DPD Delay:	15 (Range: 10 - 999, Default: 10)
DPD Timeout:	45 (Range: 30 - 1000, Default: 30)

Passaggio 4. Dall'elenco a discesa Algoritmo di crittografia, scegliere un'opzione.

·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 esegue la crittografia dei dati 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 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.

Passaggio 5. Dall'elenco a discesa Algoritmo di autenticazione, scegliere un'opzione.

·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 6. Nel campo Chiave già condivisa immettere una chiave già condivisa utilizzata dal criterio IKE.

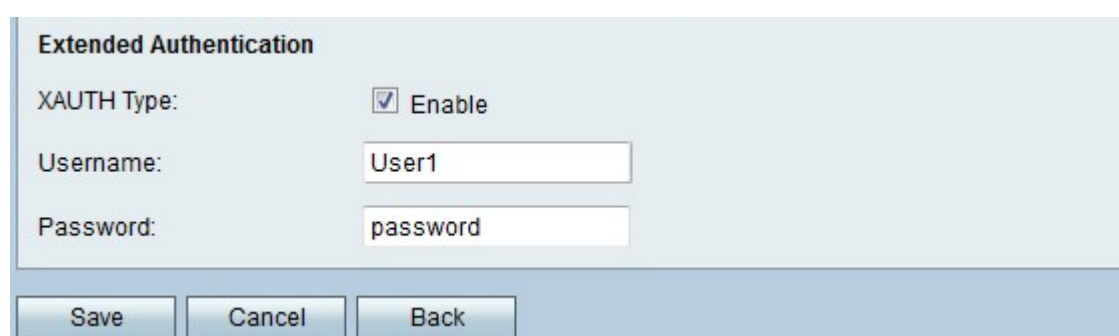
Passaggio 7. Dall'elenco a discesa Gruppo Diffie-Hellman (DH), scegliere il gruppo DH utilizzato da IKE. Gli host di un gruppo DH possono scambiarsi le chiavi senza essere a conoscenza gli uni degli altri. Più alto è il numero di bit del gruppo, più sicuro è il gruppo.

Passaggio 8. Nel campo Durata associazione di protezione immettere la durata in secondi di un'associazione di protezione per la VPN prima del rinnovo dell'associazione di protezione.

Passaggio 9. (Facoltativo) Selezionare la casella di controllo **Abilita** nel campo Dead Peer Detection (DPD) per abilitare Dead Peer Detection (DPD). Il DPD controlla i peer IKE per verificare se un peer ha smesso di funzionare. La DPD impedisce lo spreco di risorse di rete su peer inattivi.

Passaggio 10. (Facoltativo) Se DPD è stato abilitato nel passaggio 9, immettere la frequenza (in secondi) con cui il peer viene controllato per verificare l'attività nel campo Ritardo DPD.

Passaggio 11. (Facoltativo) Se nel passaggio 9 è stato abilitato DPD, immettere il numero di secondi di attesa prima che un peer inattivo venga eliminato nel campo Timeout DPD.



The screenshot shows a configuration window titled "Extended Authentication". It contains the following elements:

- XAUTH Type:** A checkbox labeled "Enable" is checked.
- Username:** A text input field containing the text "User1".
- Password:** A text input field containing the text "password".
- Buttons:** At the bottom, there are three buttons: "Save", "Cancel", and "Back".

Passaggio 12. (Facoltativo) Selezionare la casella di controllo **Abilita** nel campo Tipo XAUTH per abilitare l'autenticazione estesa (XAUTH). XAUTH consente a più utenti di utilizzare un singolo criterio VPN anziché un criterio VPN per ogni utente.

Passaggio 13. (Facoltativo) Se XAUTH è stato abilitato nel passaggio 12, immettere il nome utente da utilizzare per il criterio nel campo Nome utente.

Passaggio 14. (Facoltativo) Se XAUTH è stato abilitato nel Passaggio 12, immettere la password da utilizzare per il criterio nel campo Password.

Passaggio 15. Fare clic su **Salva**. Viene visualizzata nuovamente la pagina originale *Advanced VPN Setup*.

Impostazioni criteri VPN

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

Passaggio 1. Nella tabella Criteri VPN, fare clic su **Aggiungi riga** per creare un nuovo criterio VPN. Per modificare un criterio VPN, selezionare la casella di controllo corrispondente al criterio e fare clic su **Modifica**. La pagina *Impostazione VPN avanzata* cambia:

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

Local Traffic Selection

Local IP:

IP Address:

(Hint: 1.2.3.4)

Subnet Mask:

(Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP:

IP Address:

(Hint: 1.2.3.4)

Subnet Mask:

(Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Auto Policy Parameters

SA-Lifetime:

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

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group:

 Enable

Select IKE Policy:

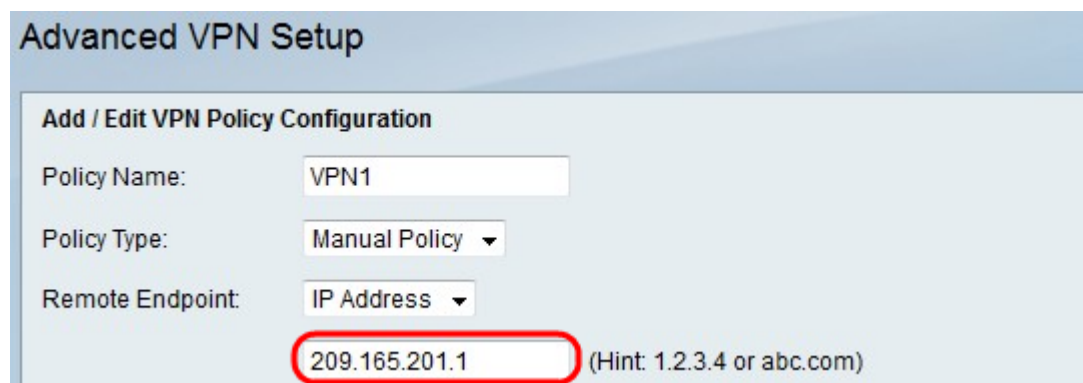
Passaggio 2. Nel campo Nome criterio, immettere un nome per il criterio VPN.

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

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

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

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



Advanced VPN Setup

Add / Edit VPN Policy Configuration

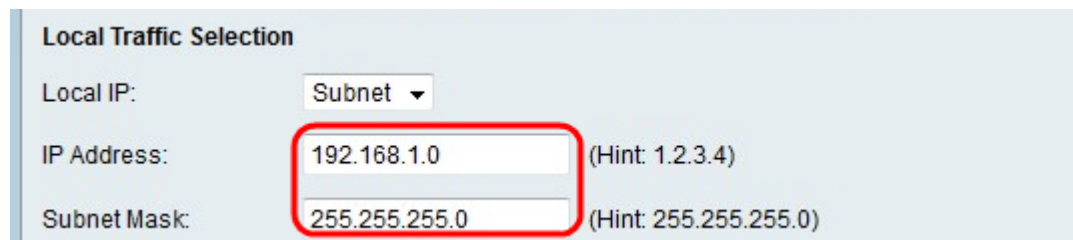
Policy Name:

Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

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



Local Traffic Selection

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Passaggio 6. Dall'elenco a discesa IP locale, scegliere un'opzione.

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

Passaggio 7. Nel campo Indirizzo IP, immettere l'indirizzo IP dell'host o della subnet locale.

Passaggio 8. (Facoltativo) Se si sceglie Subnet nel passaggio 6, immettere la subnet mask per la subnet locale nel campo Subnet mask.

Passaggio 9. Dall'elenco a discesa Remote IP (IP remoto), scegliere un'opzione.

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

Remote Traffic Selection

Remote IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Passaggio 10. Nel campo Indirizzo IP, immettere l'indirizzo IP dell'host o della subnet remota.

Passaggio 11. (Facoltativo) Se si sceglie Subnet nel passaggio 9, immettere la subnet mask per la subnet remota nel campo Subnet mask.

Nota: Se nel passo 3 è stata scelta l'opzione Criteri manuali, eseguire i passi da 12 a 19; in caso contrario, saltare il passaggio 20.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Passaggio 12. 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.

Passaggio 13. Nel campo SPI-Outgoing, immettere da tre a otto caratteri esadecimali per il tag SPI per il traffico in uscita sulla connessione VPN.

Passaggio 14. Dall'elenco a discesa Algoritmo di crittografia, scegliere un'opzione.

- 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 esegue la crittografia dei dati 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 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.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Passaggio 15. Nel campo Chiave in ingresso, immettere una chiave per il criterio in ingresso. La lunghezza della chiave dipende dall' algoritmo scelto nel passaggio 14.

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

Passaggio 16. Nel campo Esclusione, immettere una chiave per il criterio in uscita. La lunghezza della chiave dipende dall' algoritmo scelto nel passaggio 14. La lunghezza della chiave è la stessa del passaggio 15.

Passaggio 17. Dall'elenco a discesa Algoritmo di integrità, scegliere un'opzione.

- MD5 — Message-Digest Algorithm 5 (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: la funzione Secure Hash 1 (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 — Secure Hash Algorithm 2 con un valore hash a 256 bit (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.

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Passaggio 18. Nel campo Chiave in ingresso, immettere una chiave per il criterio in ingresso. La lunghezza della chiave dipende dall' algoritmo scelto nel passaggio 17.

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

Passaggio 19. Nel campo Esclusione, immettere una chiave per il criterio in uscita. La lunghezza della chiave dipende dall' algoritmo scelto nel passaggio 17. La lunghezza della chiave è la stessa del passaggio 18.

Nota: Se nel passo 3 è stata scelta l'opzione Criteri automatici, eseguire i passi da 20 a 25; in caso contrario, andare al passo 26.

Auto Policy Parameters

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

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

Select IKE Policy:

Passaggio 20. Nel campo Durata SA immettere il numero di secondi che devono trascorrere prima del rinnovo dell'associazione di protezione.

Passaggio 21. Dall'elenco a discesa Algoritmo di crittografia, scegliere un'opzione.

- 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 esegue la crittografia dei dati 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 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.

Passaggio 22. Dall'elenco a discesa Algoritmo di integrità, scegliere un'opzione.

·MD5 — Message-Digest Algorithm 5 (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: la funzione Secure Hash 1 (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 — Secure Hash Algorithm 2 con un valore hash a 256 bit (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.

Passaggio 23. 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 24. (Facoltativo) Se si è scelto di abilitare PFS nel passaggio 23, scegliere un gruppo Diffie-Hellman (DH) a cui unirsi per l'elenco a discesa seguente. Maggiore è il numero di gruppo, più il gruppo è sicuro.

Passaggio 25. Dall'elenco a discesa Seleziona criterio IKE scegliere il criterio IKE da utilizzare per il criterio VPN.

Nota: Se si fa clic su **Visualizza**, viene visualizzata la sezione Configurazione IKE della pagina *Configurazione VPN avanzata*.

Passaggio 26. Fare clic su **Salva**. Viene visualizzata nuovamente la pagina originale *Advanced VPN Setup*.

Passaggio 27. Fare clic su **Salva**.