Configurare la VPN SSL (Secure Sockets Layer Virtual Private Network) sul router RV340 o RV345

Avviso speciale: Struttura delle licenze: firmware versioni 1.0.3.15 e successive. Inoltre, AnyConnect sarà a pagamento solo per le licenze client.

Per ulteriori informazioni sulle licenze AnyConnect sui router serie RV340, consultare l'articolo Licenze AnyConnect per i router serie RV340.

Obiettivo

Il gateway VPN (Virtual Private Network) Secure Sockets Layer consente agli utenti remoti di stabilire un tunnel VPN sicuro utilizzando un browser Web. Questa funzionalità consente di accedere facilmente a un'ampia gamma di risorse Web e applicazioni abilitate per il Web utilizzando il protocollo HTTP (Hypertext Transfer Protocol) nativo sul supporto del browser HTTPS (Hypertext Transfer Protocol Secure) SSL.

SSL VPN consente agli utenti di accedere in remoto alle reti con restrizioni, utilizzando un percorso sicuro e autenticato tramite la crittografia del traffico di rete.

I router RV340 e RV345 supportano il client VPN Cisco AnyConnect o noto anche come Anyconnect Secure Mobility Client. Per impostazione predefinita, questi router supportano due tunnel VPN SSL e l'utente può registrare una licenza per supportare fino a 50 tunnel. Una volta installata e attivata, la VPN SSL stabilisce un tunnel VPN sicuro e ad accesso remoto.

Lo scopo di questo articolo è quello di mostrare come configurare una VPN SSL sull'RV340 o sul router RV345.

Dispositivi interessati

- RV340
- RV345
- Cisco Secure Mobility Client

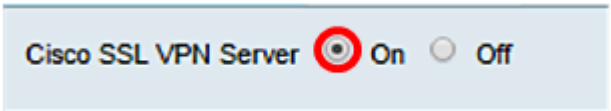
Versione del software

- 1.0.03.15 — RV340, RV345
- 4.4.01054 — AnyConnect Secure Mobility Client

Configura VPN SSL

Passaggio 1. Accedere all'utility basata sul Web del router e scegliere VPN > SSL VPN.

Passaggio 2. Fare clic sul pulsante di opzione On per abilitare Cisco SSL VPN Server.



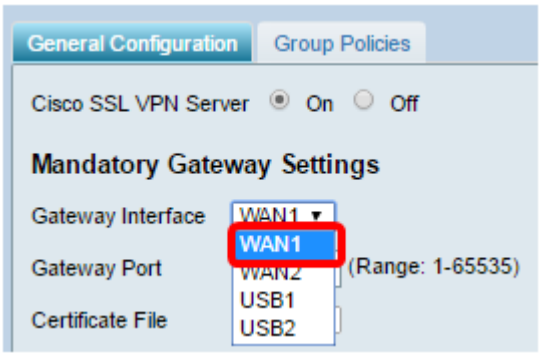
Impostazioni gateway obbligatorie

Le seguenti impostazioni di configurazione sono obbligatorie:

Passaggio 3. Scegliere l'interfaccia del gateway dall'elenco a discesa. Questa sarà la porta che verrà utilizzata per passare il traffico attraverso i tunnel VPN SSL. Le opzioni sono:

- WAN1
- WAN2

- USB1
- USB2

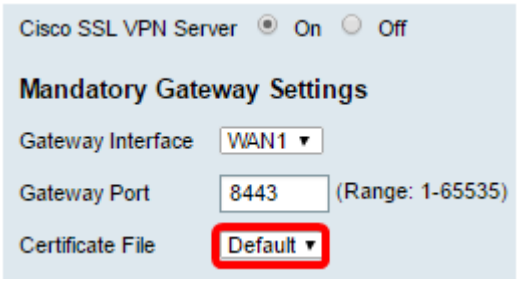


Nota: Nell'esempio, viene scelta WAN1.

Passaggio 4. Immettere il numero di porta utilizzato per il gateway VPN SSL nel campo Porta gateway compreso tra 1 e 65535.

Nota: nell'esempio, il numero di porta è 8443.

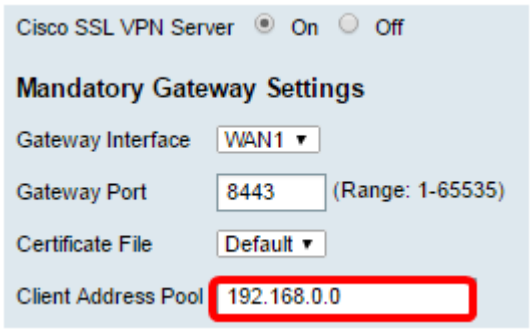
Passaggio 5. Scegliere il file di certificato dall'elenco a discesa. Questo certificato autentica gli utenti che tentano di accedere alla risorsa di rete tramite i tunnel VPN SSL. L'elenco a discesa contiene un certificato predefinito e i certificati importati.



Nota: In questo esempio, viene scelto Predefinito.

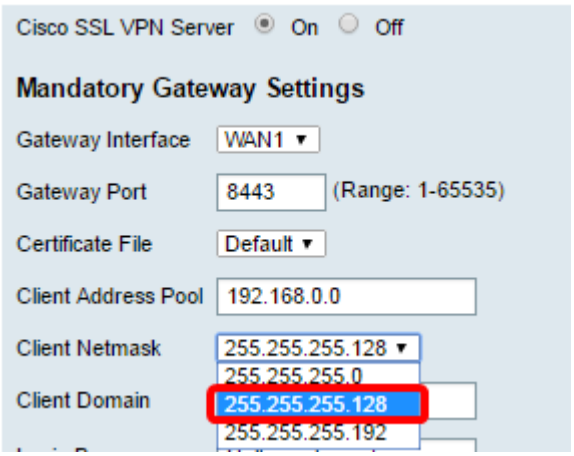
Passaggio 6. Immettere l'indirizzo IP del pool di indirizzi client nel campo Pool di indirizzi client. Questo pool sarà l'intervallo di indirizzi IP che verranno allocati ai client VPN remoti.

Nota: Verificare che l'intervallo di indirizzi IP non si sovrapponga ad alcun indirizzo IP della rete locale.



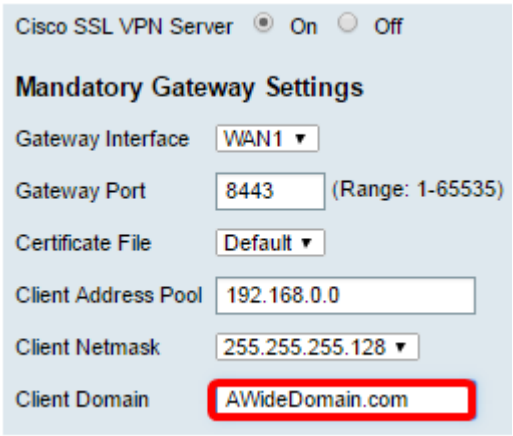
Nota: nell'esempio viene usato 192.168.0.0.

Passaggio 7. Scegliere la maschera di rete client dall'elenco a discesa.



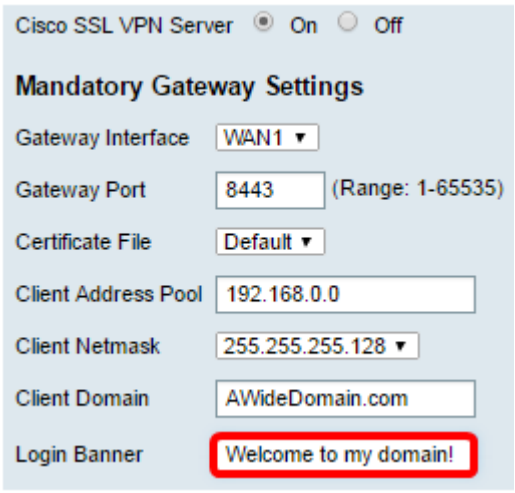
Nota: nell'esempio, viene scelto 255.255.255.128.

Passaggio 8. Immettere il nome del dominio del client nel campo Dominio client. Questo sarà il nome di dominio da inviare ai client VPN SSL.



Nota: Nell'esempio, il nome del dominio del client è AWideDomain.

Passaggio 9. Immettere il testo che verrà visualizzato come banner di accesso nel campo Banner di accesso. Questo sarà il banner che verrà visualizzato ogni volta che un client esegue l'accesso.



Nota: In questo esempio, Benvenuto nel mio dominio! viene utilizzato come banner di accesso.

Impostazioni gateway opzionali

Le seguenti impostazioni di configurazione sono facoltative:

Passaggio 1. Immettere un valore in secondi per il timeout di inattività compreso tra 60 e 86400. Questo valore indica il periodo di tempo durante il quale la sessione VPN SSL può rimanere inattiva.

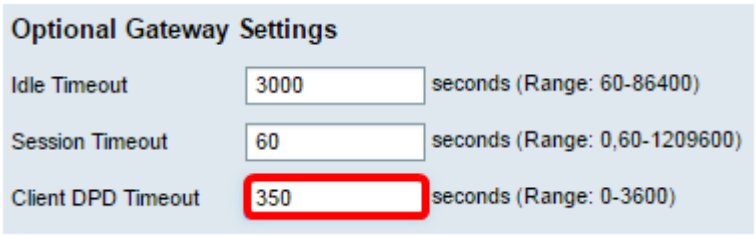
Nota: Nell'esempio viene utilizzato 3000.

Passaggio 2. Immettere un valore in secondi nel campo Timeout sessione. Tempo necessario per il timeout della sessione TCP (Transmission Control Protocol) o UDP (User Datagram Protocol) dopo il tempo di inattività specificato. L'intervallo ammesso è compreso tra 60 e 1209600.

Nota: Nell'esempio viene utilizzato 60.

Passaggio 3. Immettere un valore in secondi nel campo Timeout DPD client compreso tra 0 e 3600. Questo valore specifica l'invio periodico di messaggi HELLO/ACK per controllare lo stato del tunnel VPN.

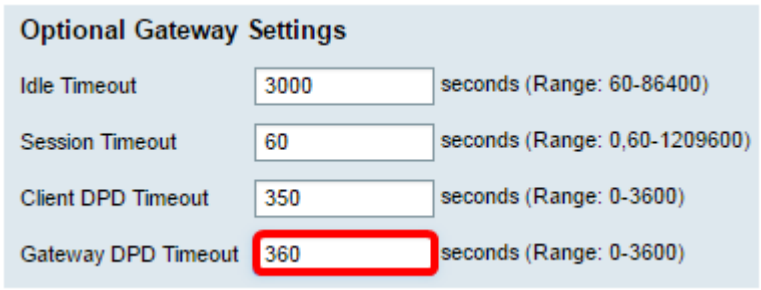
Nota: Questa funzionalità deve essere abilitata su entrambe le estremità del tunnel VPN.



Nota: Nell'esempio viene utilizzato 350.

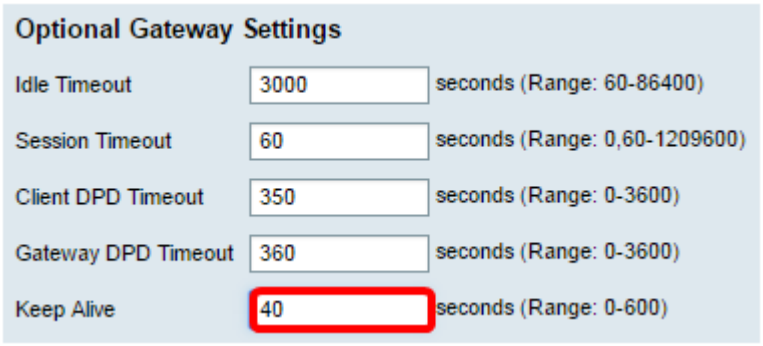
Passaggio 4. Immettere un valore in secondi nel campo GatewayDPD Timeout compreso tra 0 e 3600. Questo valore specifica l'invio periodico di messaggi HELLO/ACK per controllare lo stato del tunnel VPN.

Nota: Questa funzionalità deve essere abilitata su entrambe le estremità del tunnel VPN.



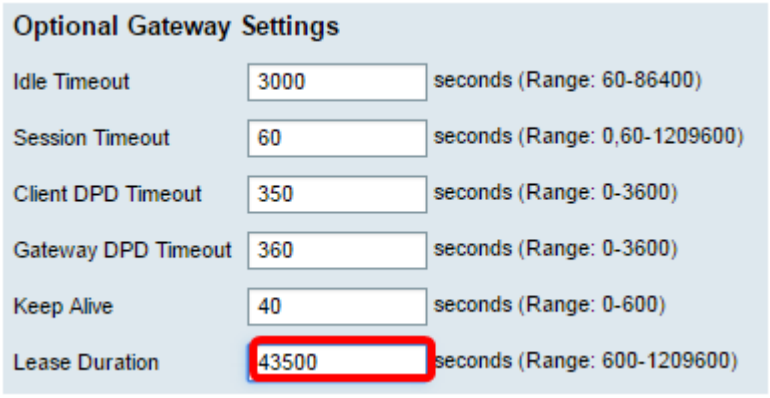
Nota: Nell'esempio viene utilizzato 360.

Passaggio 5. Immettere un valore in secondi nel campo Keep Alive compreso tra 0 e 600. Questa funzione assicura che il router sia sempre connesso a Internet. Tenterà di ristabilire la connessione VPN se viene interrotta.



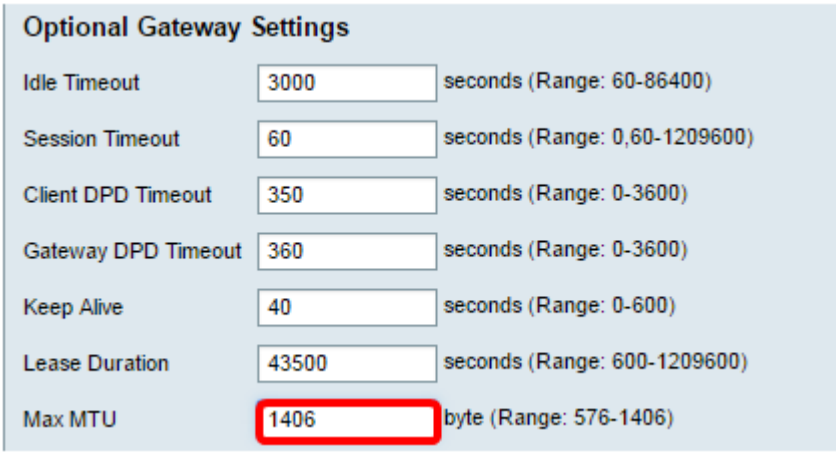
Nota: Nell'esempio viene utilizzato 40.

Passaggio 6. Immettere un valore in secondi per la durata del tunnel da connettere nel campo Durata lease. L'intervallo ammesso è compreso tra 600 e 1209600.



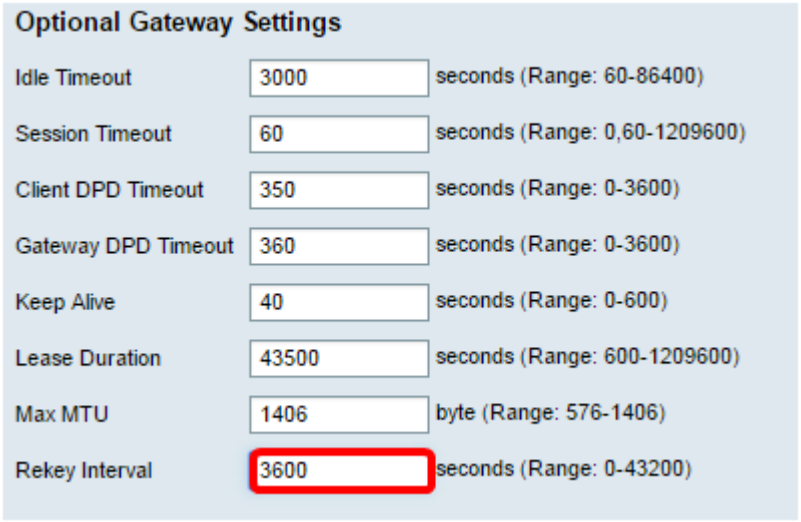
Nota: Nell'esempio viene utilizzato 43500.

Passaggio 7. Immettere le dimensioni del pacchetto in byte che possono essere inviate tramite la rete. L'intervallo è compreso tra 576 e 1406.



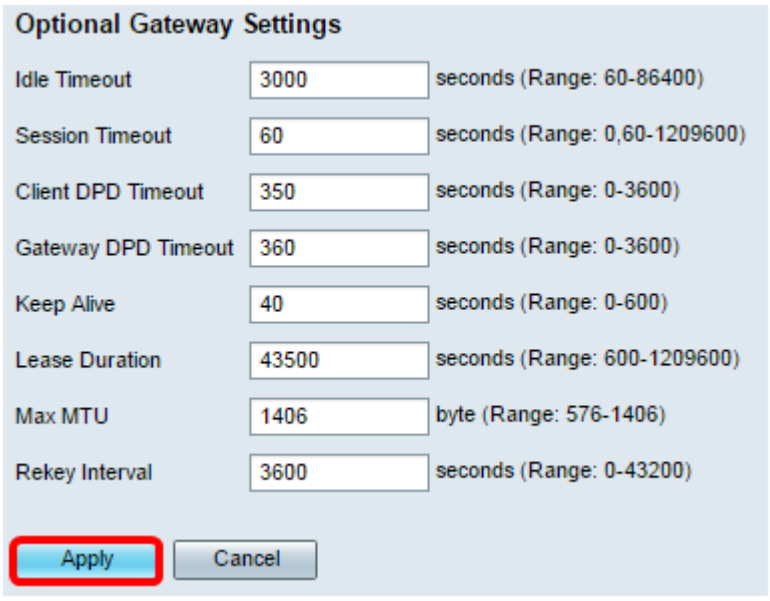
Nota: Nell'esempio viene utilizzato 1406.

Passaggio 8. Immettere il tempo dell'intervallo di inoltro nel campo Intervallo di reimpostazione chiavi. La funzione Rekey consente alle chiavi SSL di rinegoziare dopo la creazione della sessione. L'intervallo ammesso è compreso tra 0 e 43200.



Nota: Nell'esempio viene utilizzato 3600.

Passaggio 9. Fare clic su Applica.



Passaggio 10. (Facoltativo) Per salvare in modo permanente la configurazione, fare clic sull' 

icona lampeggiante.

A questo punto, è necessario configurare correttamente la VPN SSL sul router RV34x.

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).