Configurazione della connettività di AnyConnect Virtual Private Network (VPN) sul router serie RV34x

Obiettivo

Scopo di questo documento è mostrare come configurare la connettività di AnyConnect VPN sul router serie RV34x.

Vantaggi dell'uso di AnyConnect Secure Mobility Client:

1. Connettività sicura e persistente
2. Sicurezza costante e applicazione delle policy
3. Installabile da Adaptive Security Appliance (ASA) o da sistemi di distribuzione software aziendali
4. Personalizzabile e traducibile
5. Facile configurazione
6. Supporto di IPSec (Internet Protocol Security) e SSL (Secure Sockets Layer)
7. Supporto del protocollo Internet Key Exchange versione 2.0 (IKEv2.0)

Introduzione

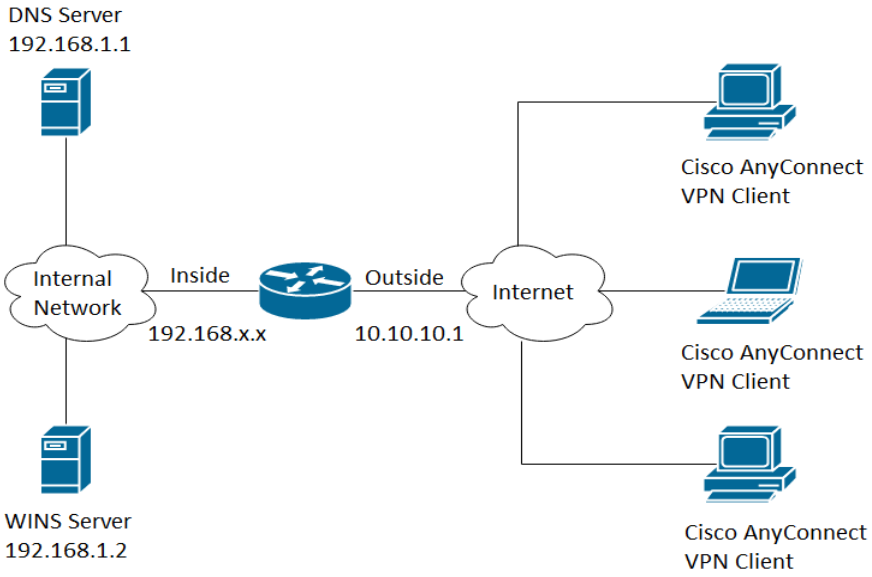
Una connessione VPN (Virtual Private Network) consente agli utenti di accedere, inviare e ricevere dati da e verso una rete privata tramite una rete pubblica o condivisa, ad esempio Internet, ma garantisce comunque connessioni sicure a un'infrastruttura di rete sottostante per proteggere la rete privata e le relative risorse.

Un client VPN è un software installato ed eseguito su un computer che desidera connettersi alla rete remota. Questo software client deve essere configurato con la stessa configurazione del server VPN, ad esempio l'indirizzo IP e le informazioni di autenticazione. Queste informazioni di autenticazione includono il nome utente e la chiave già condivisa che verrà utilizzata per crittografare i dati. A seconda della posizione fisica delle reti da connettere, un client VPN può anche essere un dispositivo hardware. Ciò si verifica in genere se la connessione VPN viene utilizzata per connettere due reti che si trovano in percorsi diversi.

Cisco AnyConnect Secure Mobility Client è un'applicazione software per la connessione a una VPN che funziona su diversi sistemi operativi e configurazioni hardware. Questa applicazione software consente di rendere accessibili le risorse remote di un'altra rete come se l'utente fosse connesso direttamente alla rete, ma in modo sicuro. Cisco AnyConnect Secure Mobility Client offre un nuovo modo innovativo di proteggere gli utenti di dispositivi mobili su piattaforme basate su computer o smart phone, offrendo agli utenti finali un'esperienza più fluida e sempre protetta, oltre a un'applicazione completa delle policy per gli amministratori IT.

Sul router RV34x, a partire dalla versione 1.0.3.15 del firmware e in futuro, non è necessario acquistare una licenza AnyConnect. Le licenze client sono a pagamento.

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



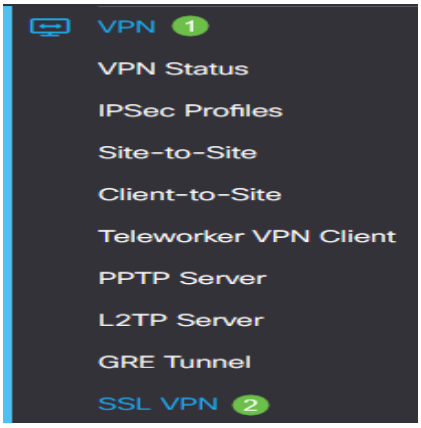
Dispositivi interessati | Versione firmware

- Cisco AnyConnect Secure Mobility Client | 4.4 (scarica la versione più recente)
- Serie RV34x | 1.0.03.15 (scarica la versione più recente)

Configurazione della connettività VPN AnyConnect su RV34x

Configurazione di SSL VPN su RV34x

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. Selezionare Interfaccia 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, è selezionato 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.

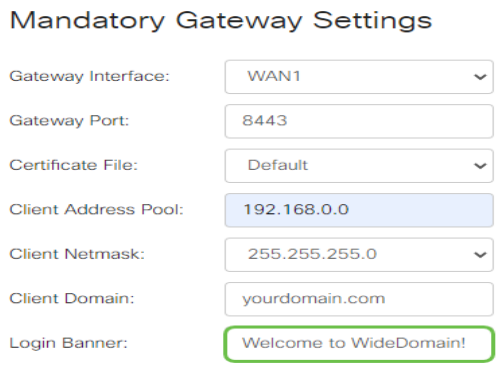
Passaggio 7. Selezionare la maschera di rete client dall'elenco a discesa.

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 di dominio del client è WideDomain.com.

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.

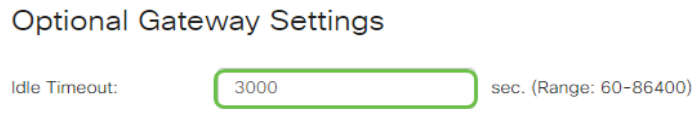


Nota: nell'esempio riportato di seguito, il banner di accesso è Welcome to Widedomain!.

Impostazioni gateway opzionali

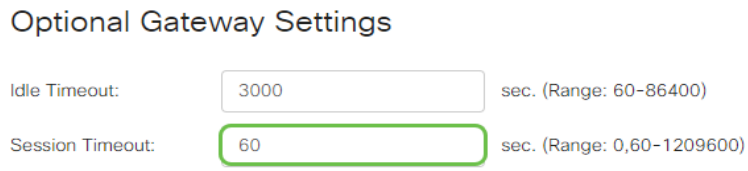
Le seguenti impostazioni di configurazione sono facoltative:

Passaggio 1. Immettere un valore in secondi per il timeout di inattività compreso tra 60 e 86400. Indica per quanto tempo la sessione VPN SSL può rimanere inattiva.



Nota: nell'esempio viene utilizzato 3000.

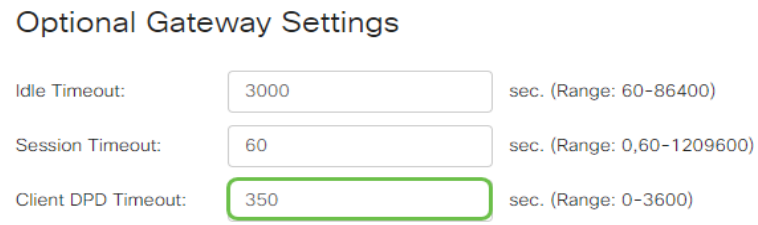
Passaggio 2. Immettere un valore in secondi nel campo *Timeout sessione*. Tempo necessario per il timeout della sessione TCP (Transmission Control Protocol) o UDP (User Datagram Protocol) dopo il tempo di inattività specificato. L'intervallo è compreso tra 60 e 1209600.



Nota: nell'esempio viene utilizzato 60.

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

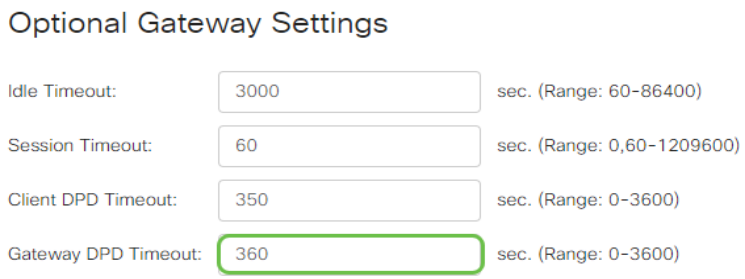
Nota: questa funzionalità deve essere abilitata su entrambe le estremità del tunnel VPN.



Nota: nell'esempio, viene usato 350.

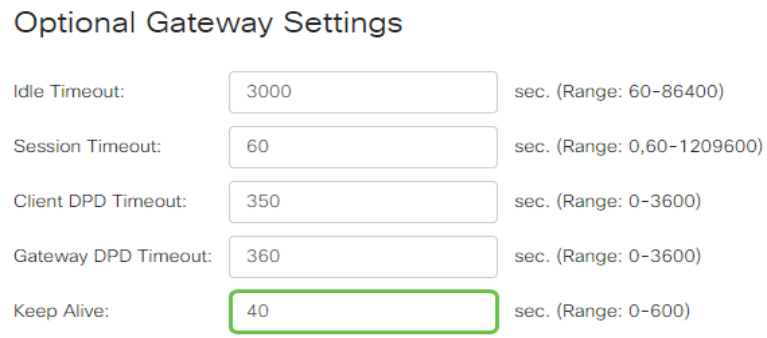
Passaggio 4. Immettere un valore in secondi nel campo *GatewayDPD Timeout* (Timeout DPD) compreso tra 0 e 3600. Questo valore specifica l'invio periodico di messaggi HELLO/ACK per controllare lo stato del tunnel VPN.

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



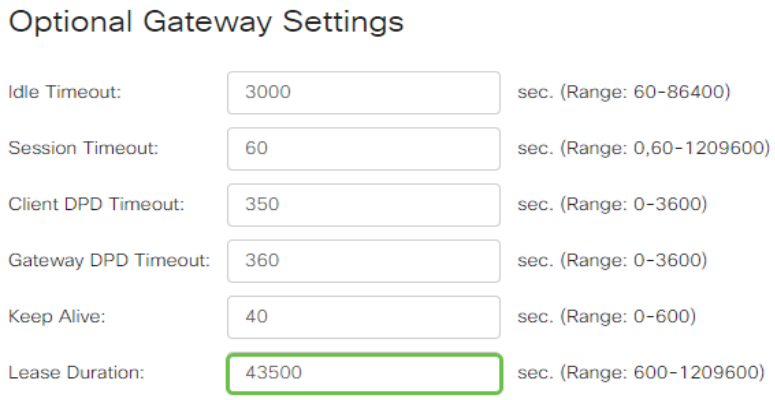
Nota: nell'esempio, viene usato 360.

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



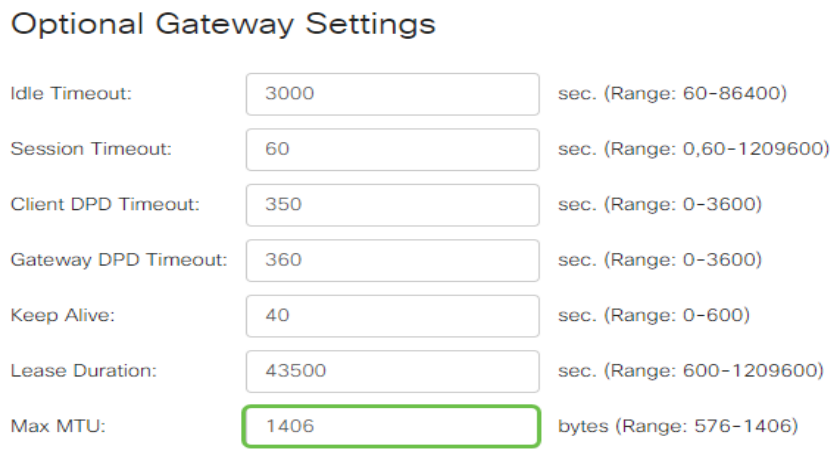
Nota: nell'esempio viene utilizzato 40.

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



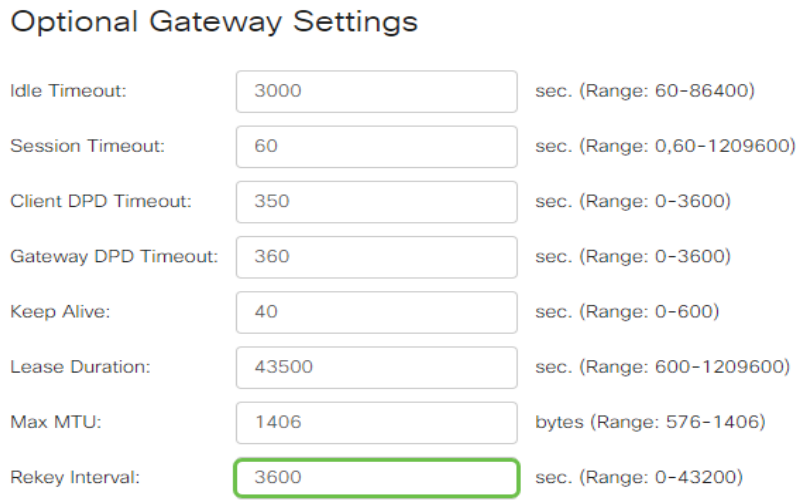
Nota: nell'esempio viene utilizzato 43500.

Passaggio 7. Immettere le dimensioni in byte del pacchetto che può essere inviato sulla rete. L'intervallo è compreso tra 576 e 1406.



Nota: nell'esempio viene usato il valore 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 è compreso tra 0 e 43200.

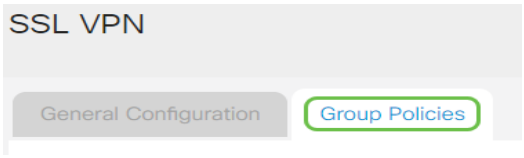


Nota: nell'esempio viene utilizzato 3600.

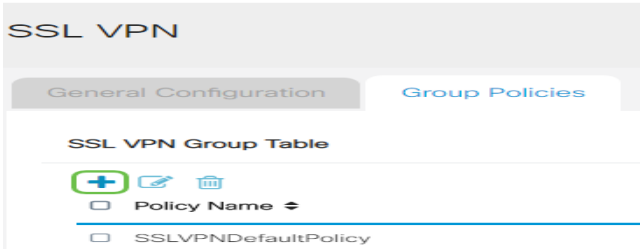
Passaggio 9. Fare clic su **Apply** (Applica).

Configura Criteri di gruppo

Passaggio 1. Fare clic sulla scheda **Criteri di gruppo**.



Passaggio 2. Per aggiungere un criterio di gruppo, fare clic sul pulsante **Aggiungi** nella tabella Gruppo VPN SSL.

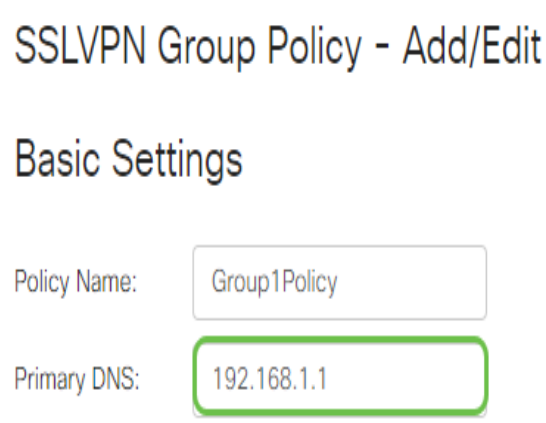


Nota: nella tabella Gruppo VPN SSL viene visualizzato l'elenco dei criteri di gruppo nel dispositivo. È inoltre possibile modificare il primo criterio di gruppo dell'elenco, denominato SSLVPNDefaultPolicy. Si tratta del criterio predefinito fornito dal dispositivo.

Passaggio 3. Immettere il nome del criterio desiderato nel campo *Nome criterio*.

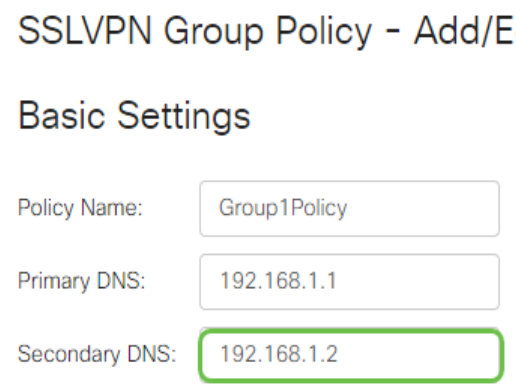
Nota: in questo esempio viene utilizzato Criteri di gruppo 1.

Passaggio 4. Immettere l'indirizzo IP del DNS primario nel campo fornito. Per impostazione predefinita, questo indirizzo IP è già specificato.



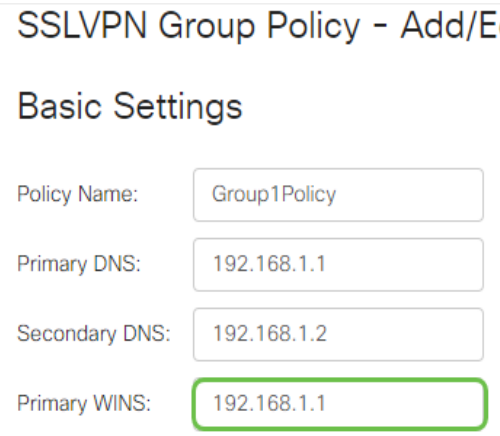
Nota: nell'esempio viene usato 192.168.1.1.

Passaggio 5. (Facoltativo) Immettere l'indirizzo IP del DNS secondario nell'apposito campo. Questo fungerà da backup in caso di errore del DNS primario.



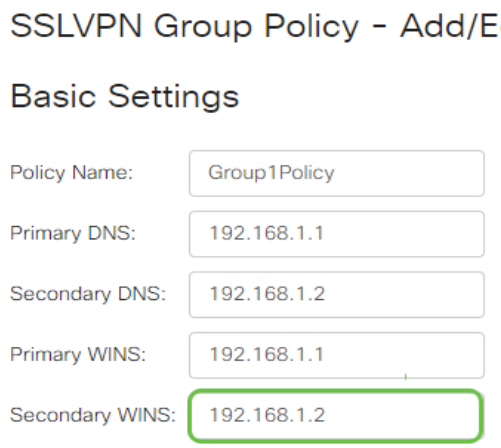
Nota: nell'esempio viene usato 192.168.1.2.

Passaggio 6. (Facoltativo) Immettere l'indirizzo IP del server WINS primario nell'apposito campo.



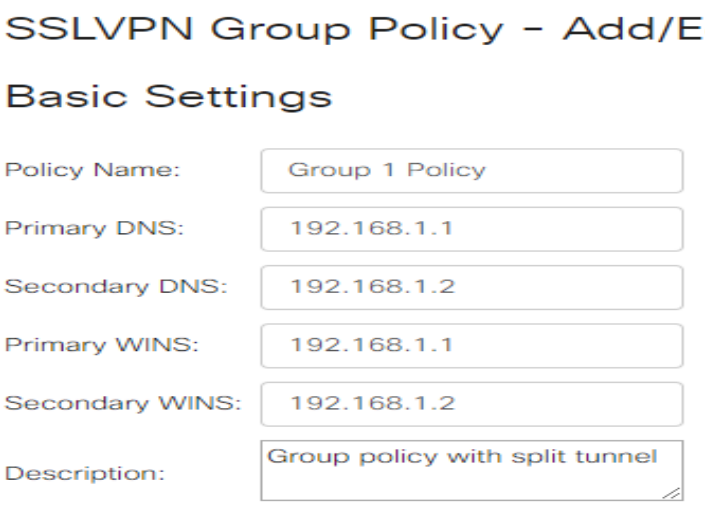
Nota: nell'esempio viene usato 192.168.1.1.

Passaggio 7. (Facoltativo) Immettere l'indirizzo IP del server WINS secondario nell'apposito campo.



Nota: nell'esempio viene usato 192.168.1.2.

Passaggio 8. (Facoltativo) Inserire una descrizione del criterio nel campo *Descrizione*.



Nota: in questo esempio vengono utilizzati Criteri di gruppo con tunnel suddiviso.

Passaggio 9. (Facoltativo) Fare clic su un pulsante di opzione per scegliere i criteri proxy di Internet Explorer per abilitare le impostazioni proxy di Microsoft Internet Explorer (MSIE) per stabilire il tunnel VPN. Le opzioni sono:

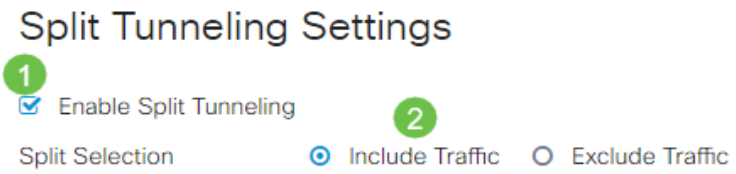
- None - Consente al browser di non utilizzare le impostazioni proxy.
- Auto - Consente al browser di rilevare automaticamente le impostazioni del proxy.
- Bypass-local: consente al browser di ignorare le impostazioni proxy configurate sull'utente remoto.
- Disabled - Disattiva le impostazioni del proxy MSIE.

Nota: in questo esempio, è selezionato Disabilitato. Si tratta dell'impostazione predefinita.

Passaggio 10. (Facoltativo) Nell'area Impostazioni tunneling ripartito, selezionare la casella di controllo **Abilita tunneling ripartito** per consentire l'invio del traffico Internet non crittografato direttamente a Internet. Il tunneling completo invia tutto il traffico al dispositivo terminale, dove viene instradato alle risorse di destinazione, eliminando la rete aziendale dal percorso per

l'accesso al Web.

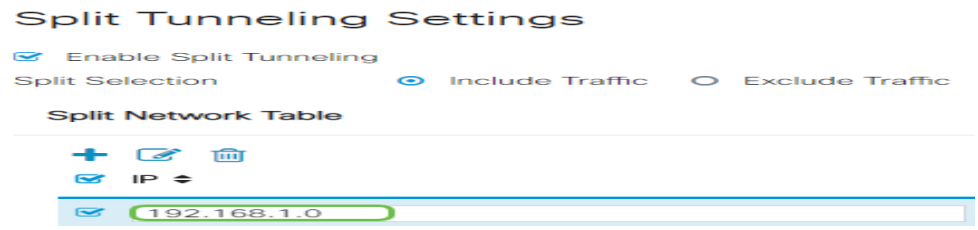
Passaggio 11. (Facoltativo) Fare clic su un pulsante di opzione per scegliere se includere o escludere il traffico quando si applica il tunneling suddiviso.



Nota: nell'esempio riportato di seguito è stato scelto Includi traffico.

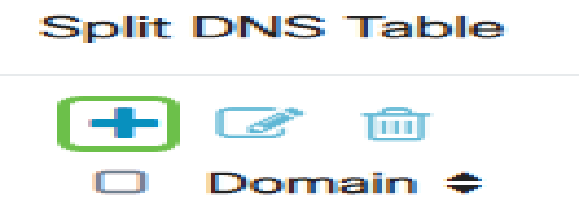
Passaggio 12. Nella tabella Dividi rete fare clic sul pulsante **Aggiungi** per aggiungere l'eccezione Dividi rete.

Passaggio 13. Immettere l'indirizzo IP della rete nell'apposito campo.



Nota: nell'esempio viene usato 192.168.1.0.

Passaggio 14. Nella tabella DNS suddiviso fare clic sul pulsante **Aggiungi** per aggiungere l'eccezione DNS suddiviso.

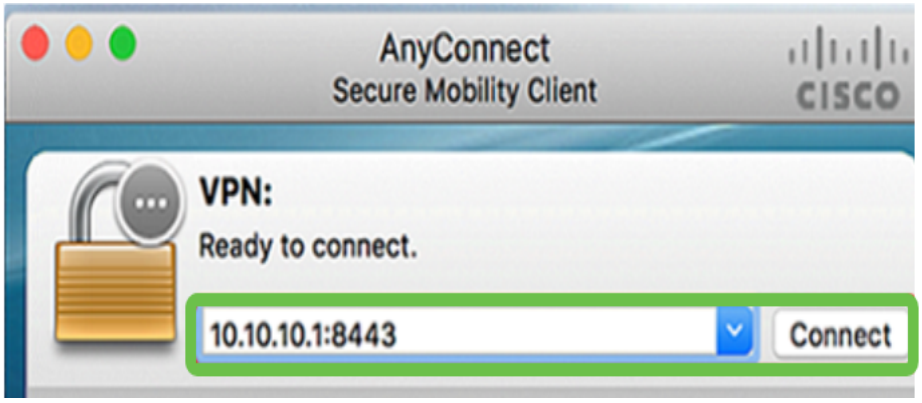


Passaggio 15. Immettere il nome del dominio nell'apposito campo e fare clic su **Applica**.

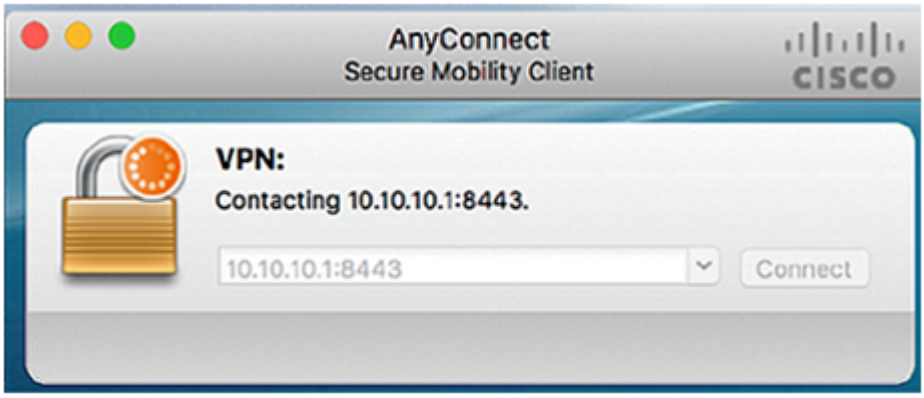
Verifica della connettività VPN di AnyConnect

Passaggio 1. Fare clic sull'icona **AnyConnect Secure Mobility Client**.

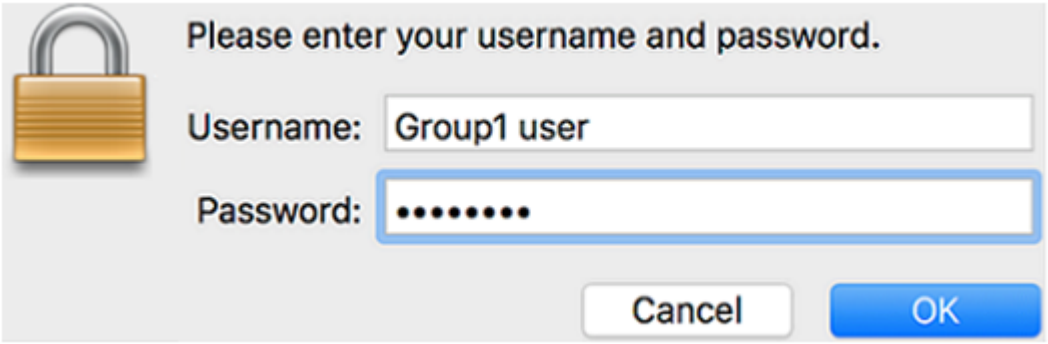
Passaggio 2. Nella finestra AnyConnect Secure Mobility Client, immettere l'indirizzo IP del gateway e il numero di porta del gateway separati da due punti (:), quindi fare clic su **Connect**.



Nota: nell'esempio viene utilizzato 10.10.10.1:8443. Il software mostrerà ora che sta contattando la rete remota.

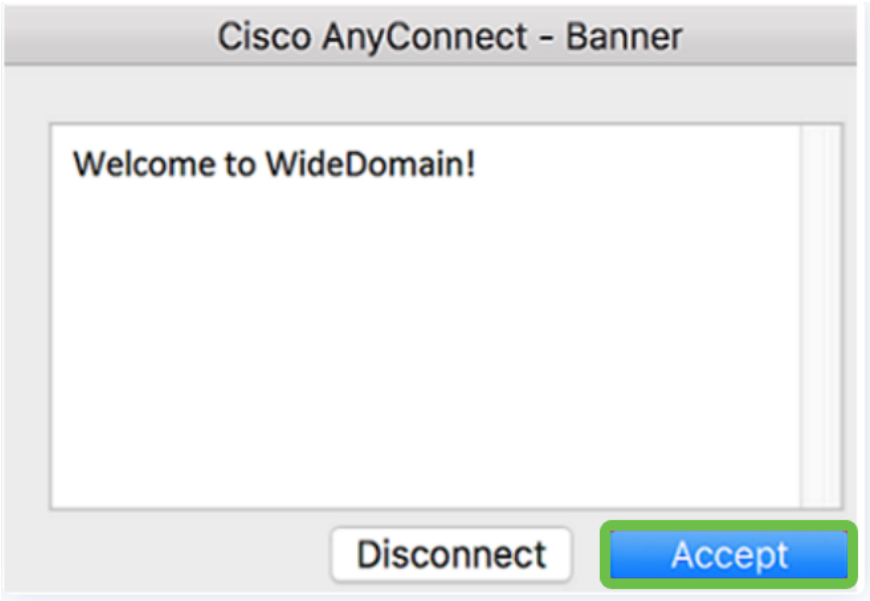


Passaggio 3. Immettere il nome utente e la password del server nei campi corrispondenti e quindi fare clic su **OK**.

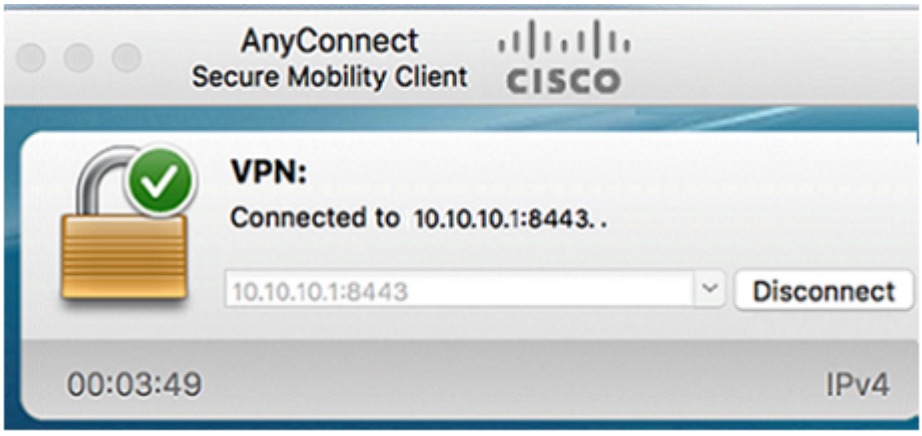


Nota: nell'esempio, il nome utente è Group1 user.

Passaggio 4. Non appena la connessione è stabilita, il banner di accesso viene visualizzato. Fare clic su **Accetta**.



A questo punto, la finestra AnyConnect dovrebbe indicare la connessione VPN alla rete riuscita.



Passaggio 5. (Facoltativo) Per disconnettersi dalla rete, fare clic su **Disconnetti**.

A questo punto, la connettività VPN AnyConnect con router serie RV34x deve essere configurata correttamente.

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).