Configurazione di un tunnel VPN da sito a sito tra i router della serie RV e le appliance ASA 5500 Adaptive Security

Obiettivo

La sicurezza è essenziale per proteggere la proprietà intellettuale di un'azienda, garantendo al tempo stesso la business continuity e fornendo la possibilità di estendere l'ambiente di lavoro aziendale ai dipendenti che necessitano di accesso alle risorse aziendali in qualsiasi momento e da qualsiasi luogo.

Le soluzioni di sicurezza VPN stanno diventando sempre più importanti per le piccole e medie imprese. Una VPN è una rete privata costruita all'interno di un'infrastruttura di rete pubblica, come Internet globale. Una VPN estende una rete privata tra uffici geograficamente separati. Consente a un computer host di inviare e ricevere dati attraverso reti pubbliche in quanto parte integrante della rete privata con tutte le funzionalità. Le VPN aumentano la sicurezza per un'organizzazione distribuita, rendendo più semplice per il personale lavorare da siti diversi senza compromettere la rete. Le motivazioni per utilizzare la VPN sono i requisiti per "virtualizzare" una parte delle comunicazioni di un'organizzazione e l'economia delle comunicazioni.

Ci sono diverse topologie VPN: Hub and Spoke, Point-to-point e Full mesh. Questo suggerimento riguarda la VPN da sito a sito (point-to-point), che fornisce un'infrastruttura basata su Internet per estendere le risorse di rete agli uffici remoti, agli uffici privati e ai siti dei partner aziendali. Tutto il traffico tra i siti viene crittografato utilizzando il protocollo IP Security (IPsec) e vengono integrate funzionalità di rete quali routing, qualità del servizio (QoS) e supporto multicast.

I router Cisco serie RV offrono soluzioni VPN robuste e di facile gestione per piccole aziende attente ai costi. Le appliance Cisco ASA serie 5500 Adaptive Security aiutano le organizzazioni a bilanciare la sicurezza con la produttività. Combina il firewall per l'ispezione stateful più implementato del settore con servizi completi di sicurezza di rete di nuova generazione, tra cui: visibilità e controllo granulare di applicazioni e microapplicazioni, sicurezza Web, sistemi di prevenzione delle intrusioni (IPS), accesso remoto altamente sicuro e altro ancora.
In questa breve guida viene descritto un esempio di progettazione per la creazione di una VPN IPsec da sito a sito tra i router della serie RV e un'appliance ASA 5500 Series Adaptive Security.

Dispositivi interessati

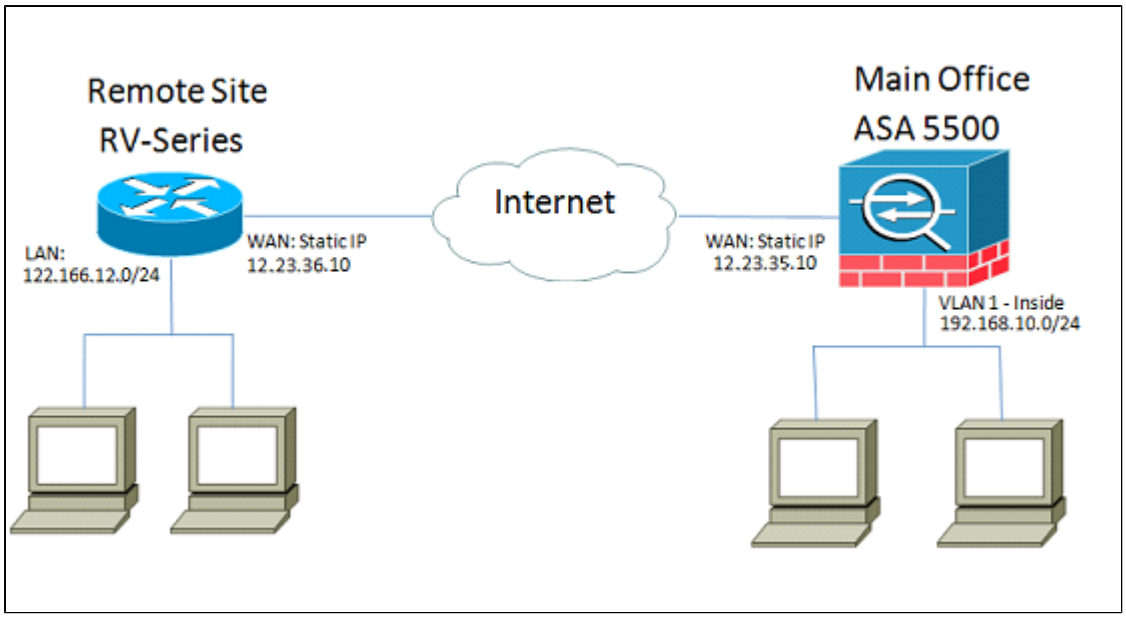
· Cisco serie RV0xx VPN Router
â€¢ Cisco ASA serie 5500 Adaptive Security Appliance

Versione del software

· 4.2.2.08 [Cisco serie RV0xx VPN Router]

Preconfigurazione

L'immagine seguente mostra un'implementazione di esempio di un tunnel VPN da sito a sito con un router serie RV (sito remoto) e un'appliance ASA 5500 (ufficio principale).



Con questa configurazione, un host nella rete del sito remoto con indirizzo 122.166.12.x e un host nella VLAN 1 presso l'ufficio principale possono comunicare tra loro in modo sicuro.

Caratteristiche principali

IKE (Internet Key Exchange)

IKE (Internet Key Exchange) è il protocollo utilizzato per configurare un'associazione di sicurezza (SA, Security Association) nella suite di protocolli IPSec. IKE si basa sul protocollo Oakley e su ISAKMP (Internet Security Association and Key Management Protocol) e utilizza uno scambio di chiavi Diffie-Hellman per impostare un segreto di sessione condiviso da cui derivano le chiavi crittografiche. È necessario mantenere manualmente una policy sicura per ogni peer.

IPSec (Internet Protocol Security)

IPsec utilizza servizi di sicurezza crittografica per proteggere le comunicazioni sulle reti IP (Internet Protocol). IPsec supporta l'autenticazione peer a livello di rete, l'autenticazione dell'origine dati, l'integrità, la riservatezza (crittografia) e la protezione della riproduzione dei dati. IPSec include molte tecnologie e metodi di crittografia dei componenti. Il funzionamento di IPSec può essere suddiviso in cinque fasi principali:
Passaggio 1. Il "traffico interessante" avvia il processo IPSec. Il traffico viene considerato interessante quando il criterio di sicurezza IPSec configurato nei peer IPSec avvia il processo IKE.
Passaggio 2. Fase IKE 1 - Durante questa fase, IKE autentica i peer IPSec e negozia le associazioni di protezione IKE, configurando un canale sicuro per la negoziazione delle associazioni di protezione IPSec nella fase 2.
Passaggio 3. Fase 2 di IKE: IKE negozia i parametri dell'associazione di protezione IPSec e imposta le associazioni di protezione IPSec corrispondenti nei peer.
Passaggio 4. Trasferimento dati: i dati vengono trasferiti tra peer IPSec in base ai parametri IPSec e alle chiavi archiviate nel database ASA.
Passaggio 5. Terminazione tunnel IPSec - Le associazioni di protezione IPSec terminano con l'eliminazione o con il timeout.

ISAKMP

Per negoziare il tunnel tra i due endpoint, vengono utilizzati l'ISAKMP (Internet Security Association)

e il protocollo ISAKMP (Key Management Protocol). Definisce le procedure per l'autenticazione, la comunicazione e la generazione di chiavi e viene utilizzato dal protocollo IKE per scambiare le chiavi di crittografia e stabilire la connessione protetta.

Suggerimenti per la progettazione

Topologia VPN: con una VPN da sito a sito, viene configurato un tunnel IPsec protetto tra tutti i siti e tra tutti gli altri. Una topologia multisito viene in genere implementata come mesh completa di tunnel VPN da sito a sito, ovvero ogni sito ha stabilito tunnel per ogni altro sito. Se non è necessaria alcuna comunicazione tra gli uffici remoti, viene utilizzata una topologia VPN hub-spoke per ridurre il numero di tunnel VPN, ovvero ogni sito stabilisce un tunnel VPN solo per l'ufficio principale.
WAN IP addressing e DNS: il tunnel VPN deve essere stabilito tra due indirizzi IP pubblici. Se i router WAN ricevono indirizzi IP statici dal provider di servizi Internet (ISP), il tunnel VPN può essere implementato direttamente utilizzando indirizzi IP pubblici statici. Tuttavia, la maggior parte delle piccole imprese utilizza servizi Internet a banda larga a costi contenuti, come DSL o modem via cavo, e riceve indirizzi IP dinamici dai propri ISP. In questi casi, il DNS può essere utilizzato per mappare l'indirizzo IP dinamico a un nome di dominio completo (FQDN).
Indirizzamento IP LAN: l'indirizzo di rete IP della LAN privata di ciascun sito non deve avere sovrapposizioni. L'indirizzo di rete IP predefinito della LAN in ciascun sito remoto deve essere sempre modificato.
Autenticazione VPN: il protocollo IKE viene utilizzato per autenticare i peer VPN quando si stabilisce un tunnel VPN. Esistono diversi metodi di autenticazione IKE e la chiave già condivisa è il metodo più pratico. Cisco consiglia di applicare una chiave già condivisa efficace.
Crittografia VPN: per garantire la riservatezza dei dati trasportati sulla VPN, vengono utilizzati algoritmi di crittografia per crittografare il payload dei pacchetti IP. DES, 3DES e AES sono tre standard di crittografia comuni. AES è considerato il sistema più sicuro rispetto a DES e 3DES. Cisco consiglia di utilizzare la crittografia AES-128 bit o superiore (ad esempio, AES-192 e AES-256). Tuttavia, maggiore è il livello dell'algoritmo di crittografia, maggiori saranno le risorse di elaborazione necessarie.

Suggerimenti per la configurazione

Elenco di controllo pre-configurazione
Passaggio 1. Verificare che l'ASA e il router RV siano entrambi collegati al gateway Internet (il router o il modem ISP).
Passaggio 2. Accendere il router Cisco RV e connettere i PC, i server e gli altri dispositivi IP interni allo switch LAN o alle porte dello switch sul router RV.
Passaggio 3. Fare lo stesso per la rete dietro l'appliance ASA. Passaggio 4. Verificare che gli indirizzi di rete IP LAN siano configurati in ogni sito e siano subnet diverse. Nell'esempio, la LAN dell'ufficio principale utilizza 192.168.10.0/24,and la LAN del sito remoto utilizza 122.166.12.0/24.
Passaggio 4. Verificare che i PC e i server locali siano in grado di comunicare tra loro e con il router.

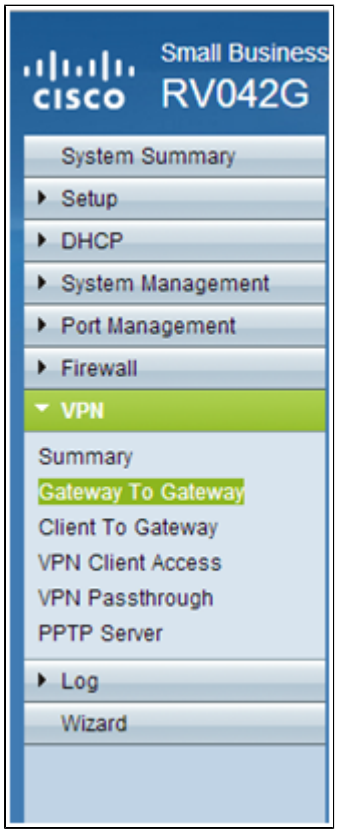
Identificazione della connessione WAN

È necessario sapere se l'ISP distribuisce un indirizzo IP dinamico o se è stato ricevuto un indirizzo IP statico. Di solito l'ISP fornisce un IP dinamico, ma è necessario confermarlo per completare la configurazione.

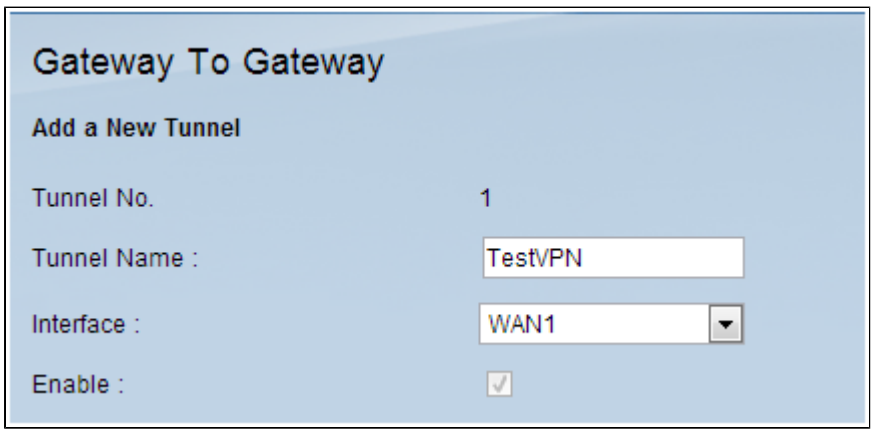
Configurazione di RV042G presso l'ufficio remoto

Passaggio 1. Accedere all'interfaccia utente Web e andare alla sezione **VPN > Gateway to Gateway**. Poiché si sta aggiungendo una connessione LAN a LAN, gli endpoint saranno il gateway di ciascuna

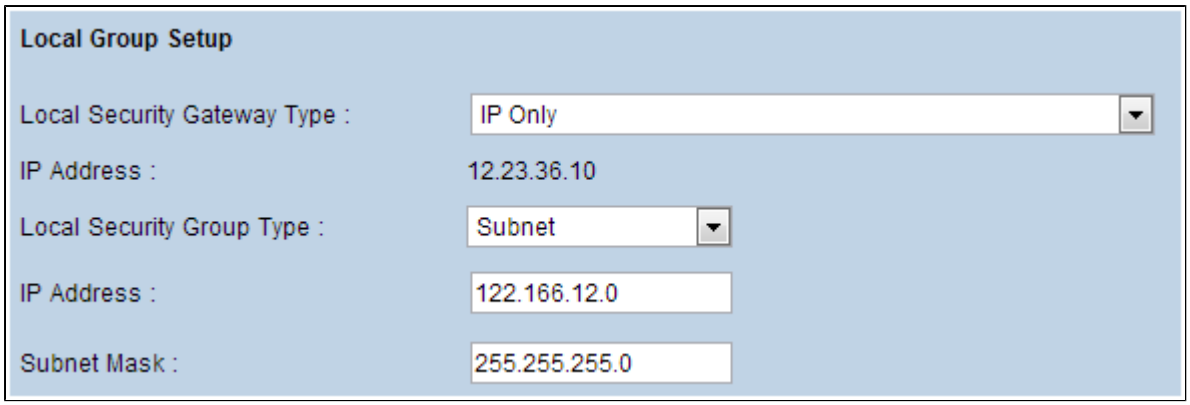
rete.



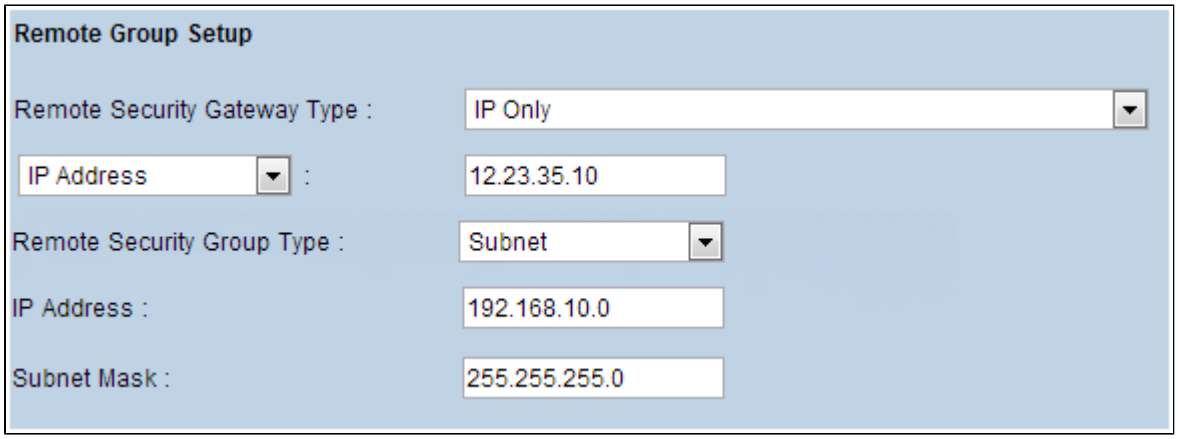
Passaggio 2. Configurare gli endpoint locale e remoto sul router
a) Configurare il Nome tunnel per identificarlo da qualsiasi altro tunnel che si sia già configurato.



b) Local Group Setup configura gli host locali da consentire sul tunnel VPN. Verificare di disporre della subnet e della maschera corrette per la rete a cui si desidera concedere l'accesso attraverso il tunnel.

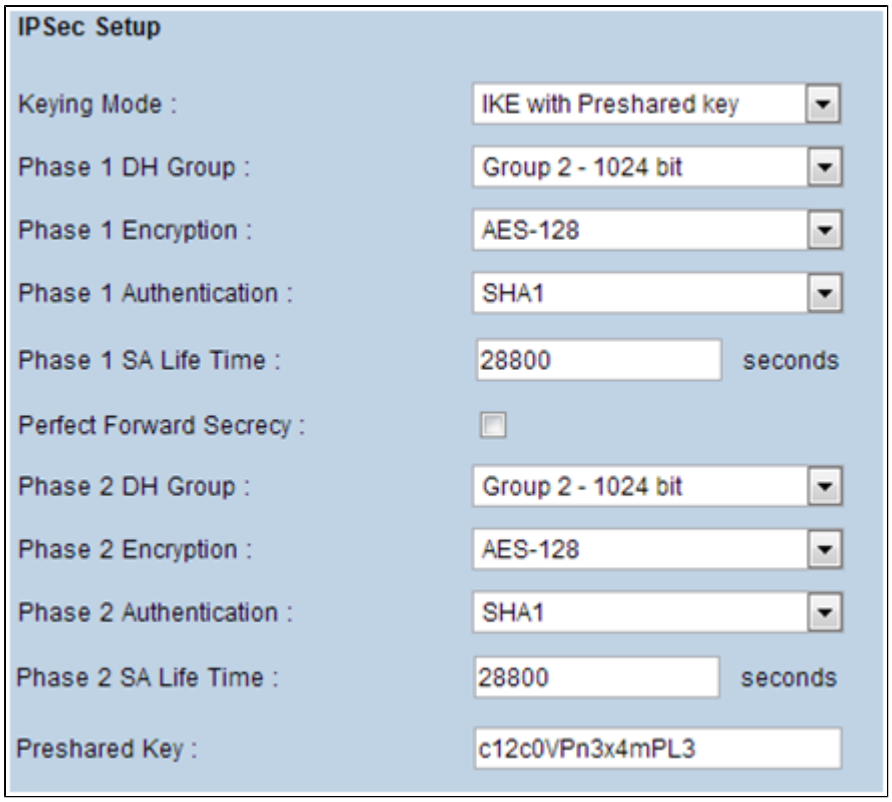


C) Installazione gruppo remoto configura l'endpoint remoto e il traffico di rete per il router da cercare. Immettere l'indirizzo IP statico del gateway remoto per stabilire la connessione nel campo Indirizzo IP gateway. Immettere quindi la subnet consentita sulla VPN dal sito remoto (la LAN dell'ufficio principale).



Passaggio 3. Configurare le impostazioni del tunnel.
a) Per ottenere risultati ottimali, si desidera configurare una chiave già condivisa.
La fase 1 e la fase 2 sono fasi diverse dell'autenticazione, la fase 1 crea il tunnel iniziale e inizia la negoziazione, la fase 2 finalizza la negoziazione della chiave di crittografia e protegge la trasmissione dei dati una volta stabilito il tunnel.
b) Il gruppo DH corrisponderà al gruppo di policy crypto isakmp sull'appliance ASA, che verrà visualizzato nella sezione successiva. Sull'appliance ASA, il valore predefinito è Group 2, mentre le versioni più recenti del codice ASA richiedono almeno DH Group 2. Il vantaggio è che il bit è più alto e quindi il tempo di CPU è maggiore.
c) La cifratura della fase 1 definisce l'algoritmo di cifratura utilizzato. Il valore predefinito nella serie RV è DES, ma il valore predefinito sull'appliance ASA è 3DES. Tuttavia, si tratta di standard precedenti e non sono efficienti nell'implementazione corrente. La crittografia AES è più veloce e sicura; Cisco consiglia di utilizzare almeno AES-128 (o semplicemente AES) per ottenere i migliori risultati.
d) La fase 1 dell'autenticazione verifica l'integrità del pacchetto. Le opzioni sono SHA-1 e MD5 e dovrebbero funzionare in quanto producono risultati simili.
La configurazione della fase 2 segue le stesse regole della fase 1. Quando si configurano le impostazioni IPSec, tenere presente che le impostazioni sull'appliance ASA devono corrispondere a quelle sull'RV042G. In caso di discrepanze, i dispositivi non saranno in grado di negoziare la chiave di crittografia e la connessione non riuscirà.

Nota: salvare le impostazioni prima di uscire da questa pagina.



Configurazione di ASA 5500 presso l'ufficio principale (CLI)

Nota: assicurarsi di utilizzare spesso il comando "write mem" per evitare di perdere le configurazioni. In primo luogo, queste sono le interfacce che abbiamo configurato sull'appliance ASA. Poiché le configurazioni possono differire, assicurarsi di modificarle di conseguenza.

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan10
 nameif outside
 security-level 0
 ip address 12.23.35.10 255.255.255.0
```

Passaggio 1. Configurazione della gestione della crittografia (ISAKMP)
Il primo passo sarà configurare la policy ISAKMP, che viene usata per negoziare la crittografia del tunnel. Questa configurazione deve essere IDENTICA su entrambi gli endpoint. In questa sezione vengono configurate le impostazioni di crittografia in modo che corrispondano alla Fase 1 della configurazione RV.

```
ASA5505(config)# crypto isakmp policy 1
ASA5505(config-isakmp-policy)# authentication pre-share
ASA5505(config-isakmp-policy)# encryption aes
ASA5505(config-isakmp-policy)# hash sha
ASA5505(config-isakmp-policy)# group 2
ASA5505(config-isakmp-policy)# lifetime 28800
ASA5505(config-isakmp-policy)# exit
ASA5505(config)#
```

Passaggio 2. Selezione traffico
Queste funzionalità sono uguali a quelle del gruppo di sicurezza locale e remota sull'RV042G. Sull'ASA, gli elenchi degli accessi vengono utilizzati per definire il traffico che la rete considera "interessante" da consentire sulla VPN.
Configurare innanzitutto gli oggetti di rete per il sito remoto e il sito locale:

```
object network insidenet
 subnet 192.168.10.0 255.255.255.0
object network rsite
 subnet 122.166.12.0 255.255.255.0
```

Configurare quindi l'elenco degli accessi in modo che utilizzi questi oggetti:

```
access-list vpn extended permit ip object insidenet object rsite
```

In alternativa, è possibile utilizzare le subnet stesse, ma in implementazioni più grandi è più semplice utilizzare oggetti e gruppi di oggetti.
Passaggio 3. Configurazione tunnel IPSec (fase 2 autenticazione)
Qui configureremo il "Set di trasformazioni" e il gruppo di tunnel, che imposterà l'autenticazione della Fase 2. Se si imposta Fase 2 in modo che sia diversa da Fase 1, si avrà un set di trasformazioni diverso. Qui esp-aes definisce la crittografia ed esp-sha-hmac definisce l'hash.
Il comando tunnel-group configura le informazioni del tunnel specifiche della connessione, come la chiave già condivisa. Utilizzare l'IP pubblico del peer remoto come nome del gruppo di tunnel.

```
ASA5505(config)# crypto ipsec transform-set asarv esp-aes esp-sha-hmac
ASA5505(config)# tunnel-group 12.23.36.10 type ipsec-l2l
ASA5505(config)# tunnel-group 12.23.36.10 ipsec-attributes
ASA5505(config-tunnel-ipsec)# pre-shared-key c12c0VPn3x4mPL3
ASA5505(config-tunnel-ipsec)# exit
ASA5505(config)#
```

Passaggio 4. Configurazione mappa crittografica
Ora dobbiamo applicare la configurazione delle fasi 1 e 2 a una "mappa crittografica" che permetta all'ASA di stabilire la VPN e inviare il traffico corretto. Pensa a questo come unire i pezzi della VPN.

```
ASA5505(config)# crypto map asarv 1 match address vpn
ASA5505(config)# crypto map asarv 1 set peer 12.23.36.10
ASA5505(config)# crypto map asarv 1 set transform-set asarv
ASA5505(config)# crypto map asarv interface outside
ASA5505(config)#
```

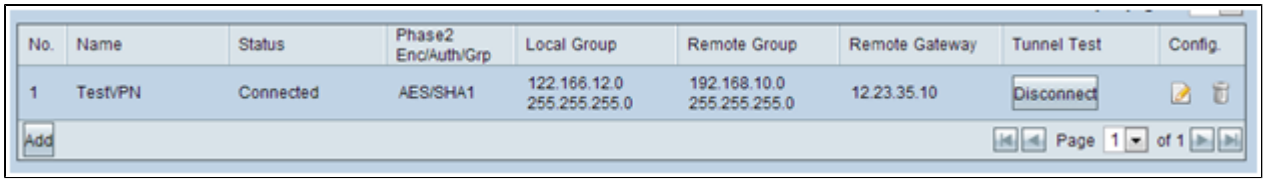
Passaggio 5. Verifica lo stato della VPN
Infine, controllare gli endpoint per verificare che la connessione VPN sia attiva e funzionante. La connessione non viene stabilita da sola. È necessario passare il traffico in modo che l'ASA possa rilevarla e tentare di stabilire la connessione. Sull'appliance ASA, usare il comando "show crypto isakmpsa" per visualizzare lo stato.

```
ASA5505(config)# show crypto isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 12.23.36.10
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE
ASA5505(config)#
```

Sulla RV42G andare alla pagina **VPN** > Riepilogo e controllare lo Stato.

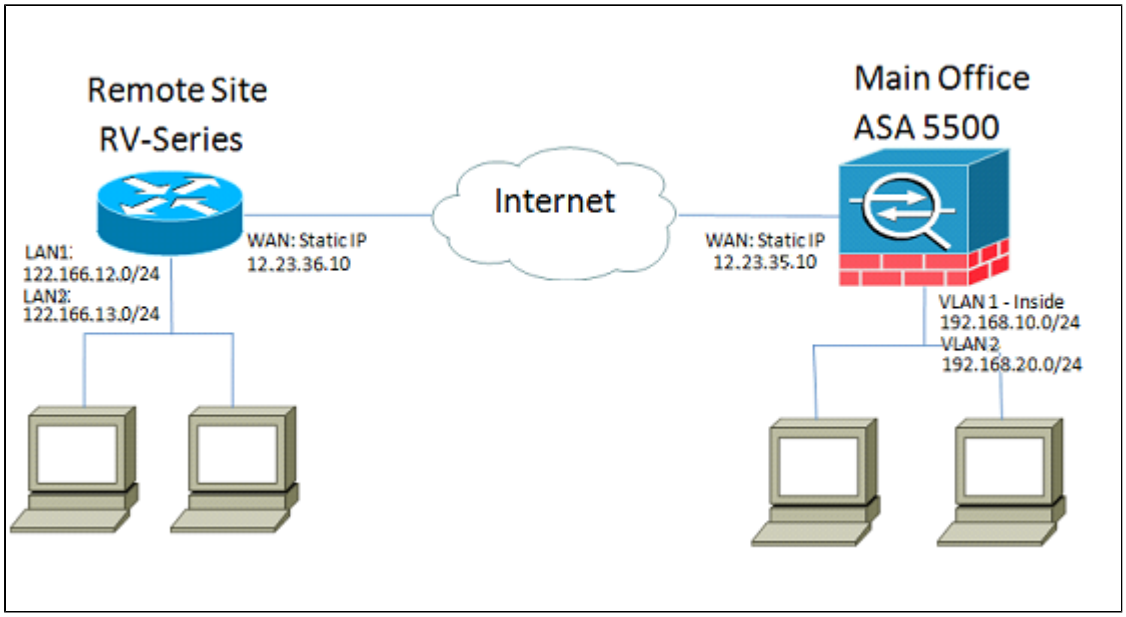


No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	TestVPN	Connected	AES/SHA1	122.166.12.0 255.255.255.0	192.168.10.0 255.255.255.0	12.23.35.10	Disconnect	

Add — Page 1 of 1

Scenario alternativo: più subnet nella rete

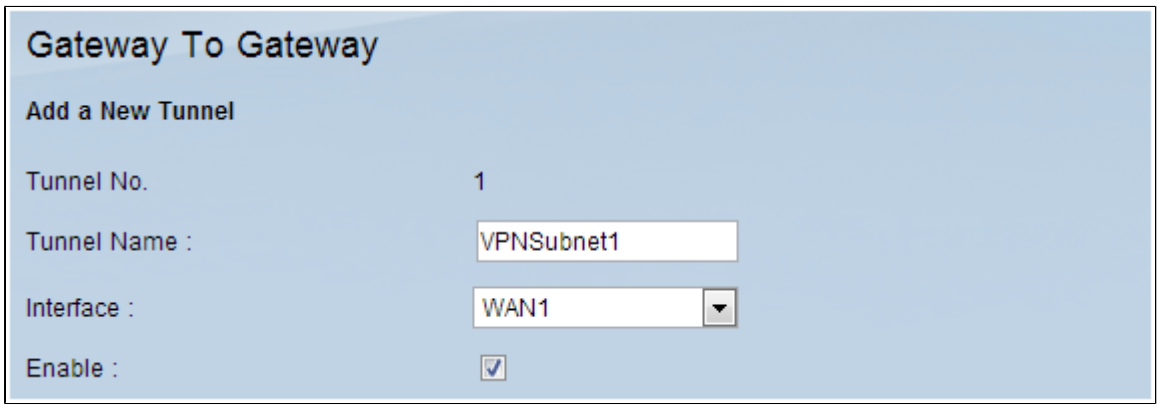
Non farti prendere dal panico. Questa procedura può sembrare eccessivamente complicata quando si configura la rete, ma la parte più complessa è già stata eseguita in precedenza. La configurazione della VPN per più subnet richiede una configurazione aggiuntiva ma una complessità aggiuntiva molto ridotta (a meno che lo schema della subnet non sia esteso). L'esempio che abbiamo utilizzato in questa sezione utilizza 2 subnet in ogni sito. La topologia di rete aggiornata è molto simile:



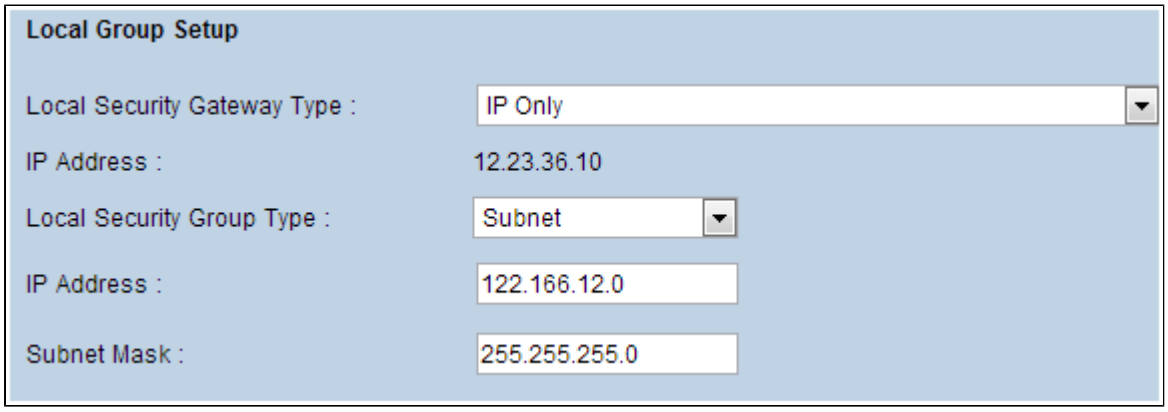
Configurazione di RV042G

Come prima, configureremo prima l'RV042G. RV042G non è in grado di configurare più subnet su un singolo tunnel. Sarà quindi necessario aggiungere una voce per la nuova subnet. In questa sezione verrà illustrata solo la configurazione VPN per più subnet, non eventuali configurazioni di configurazione aggiuntive per tali subnet.
Passaggio 1. Configurazione del primo tunnel
Per ogni tunnel verrà utilizzata la stessa configurazione dell'esempio relativo alla subnet singola.

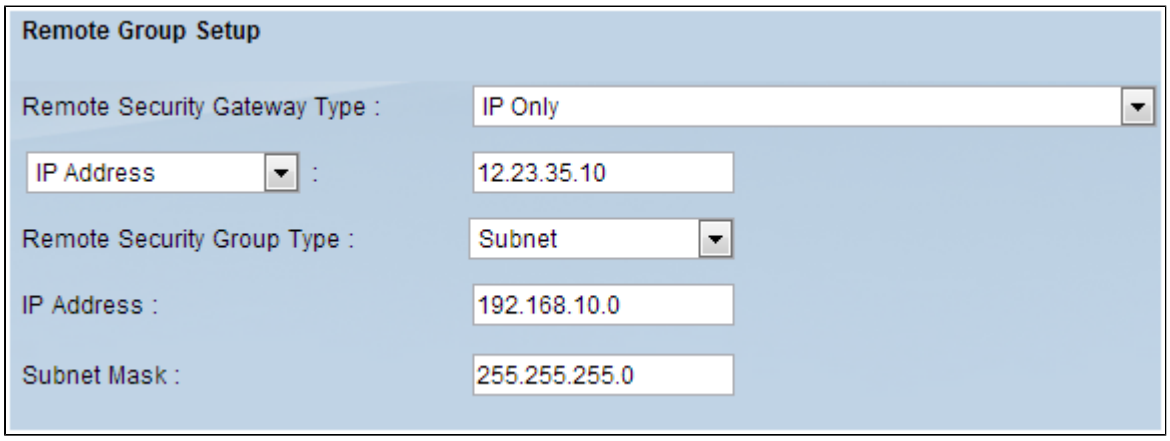
Come in precedenza, per configurare questa impostazione, andare su **VPN > Da gateway a gateway** e aggiungere un nuovo tunnel oppure, se si sta utilizzando un tunnel esistente, andare alla pagina **VPN > Riepilogo** e modificare quello esistente.
a) Configurare il nome del tunnel, ma modificare in quanto più di una modifica verrà apportata per renderla più descrittiva.



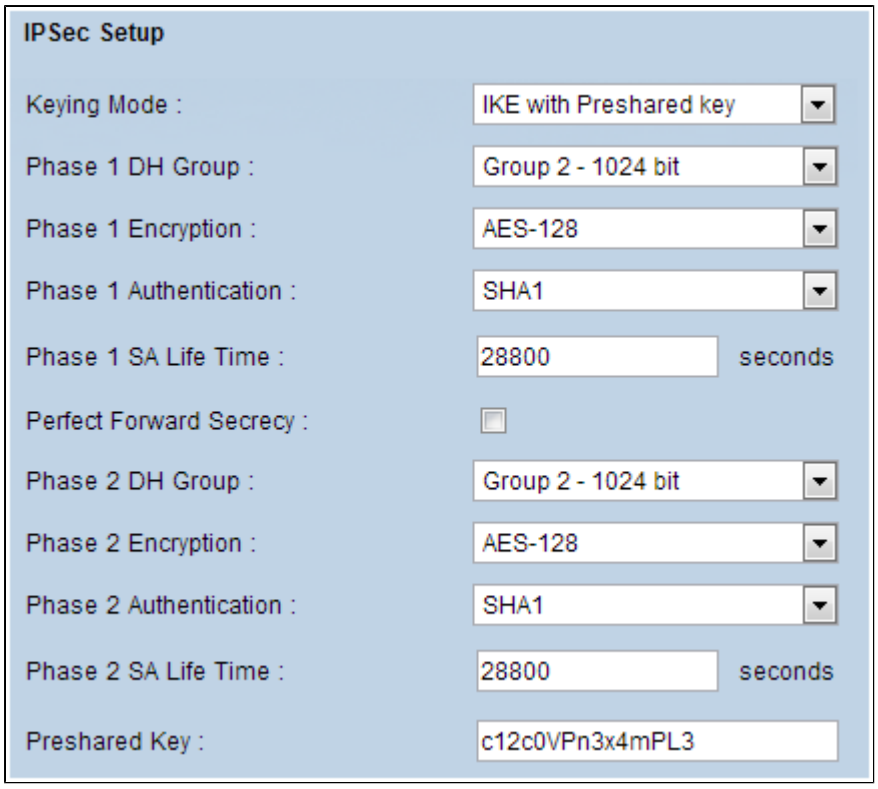
b) Successivamente configureremo il gruppo locale, come prima. Configurare questa opzione solo per UNA delle subnet a cui è necessario accedere. Avremo una voce tunnel per 122.166.12.x e un'altra per la subnet 122.166.13.x.



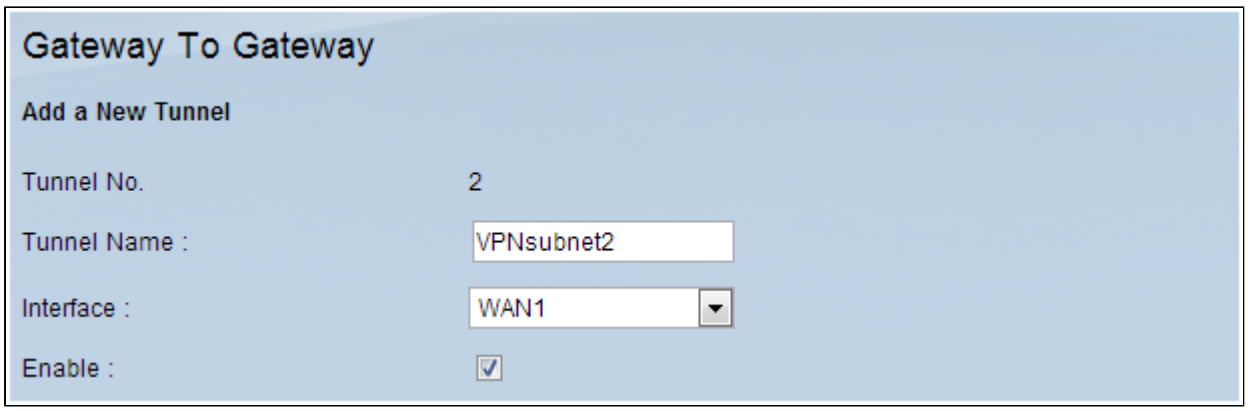
c) Configurare ora il sito remoto, utilizzando nuovamente la stessa procedura descritta sopra.



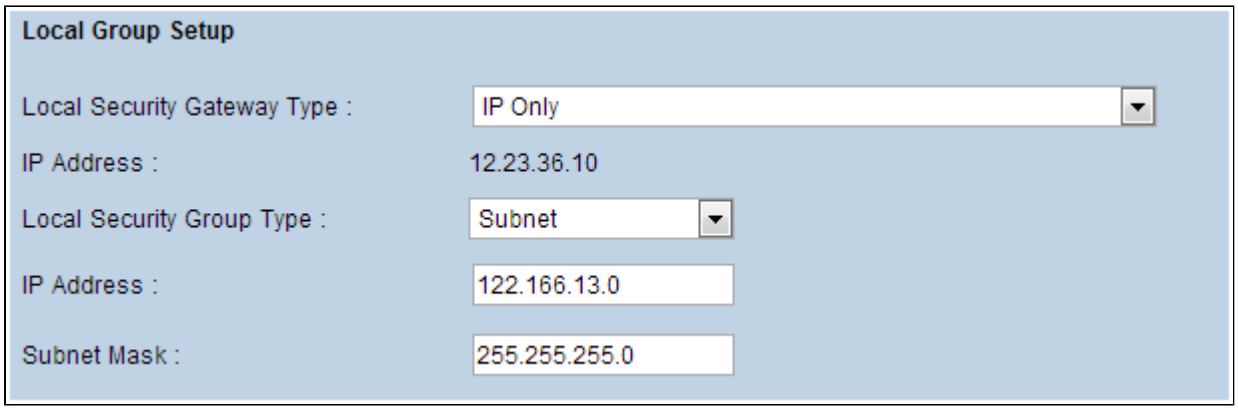
d) Infine, configurare le impostazioni di crittografia. Tenere presenti queste impostazioni, in quanto si desidera che siano le stesse su entrambi i tunnel che si stanno configurando.



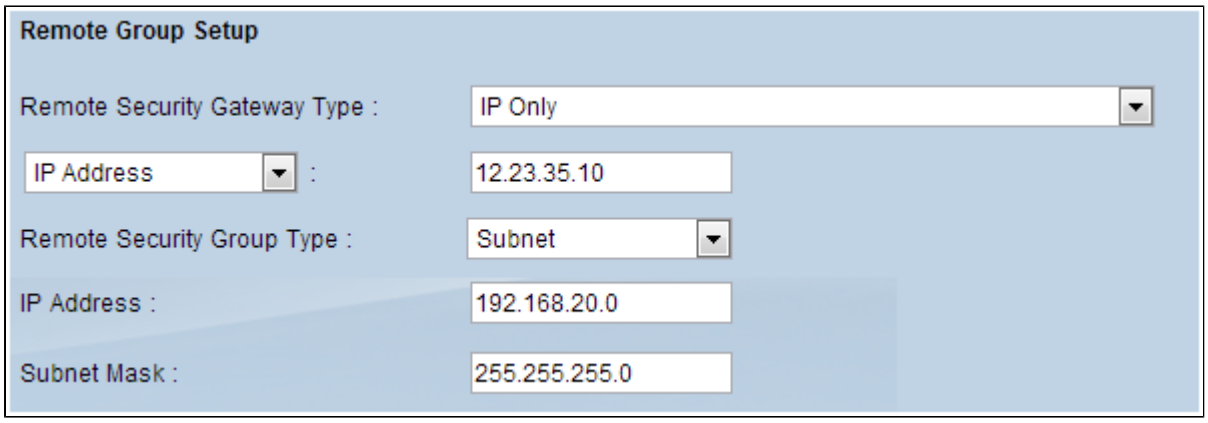
Passaggio 2. Configurazione del secondo tunnel
Ora che la subnet 1 è configurata per il tunnel VPN, è necessario andare a **VPN > Gateway to Gateway** e aggiungere un secondo tunnel. Questa seconda voce verrà configurata in modo analogo alla prima, ma con le subnet secondarie di ogni sito.
a) Assicuratevi di nominarlo qualcosa che lo distingua, in modo da sapere quale collegamento è.



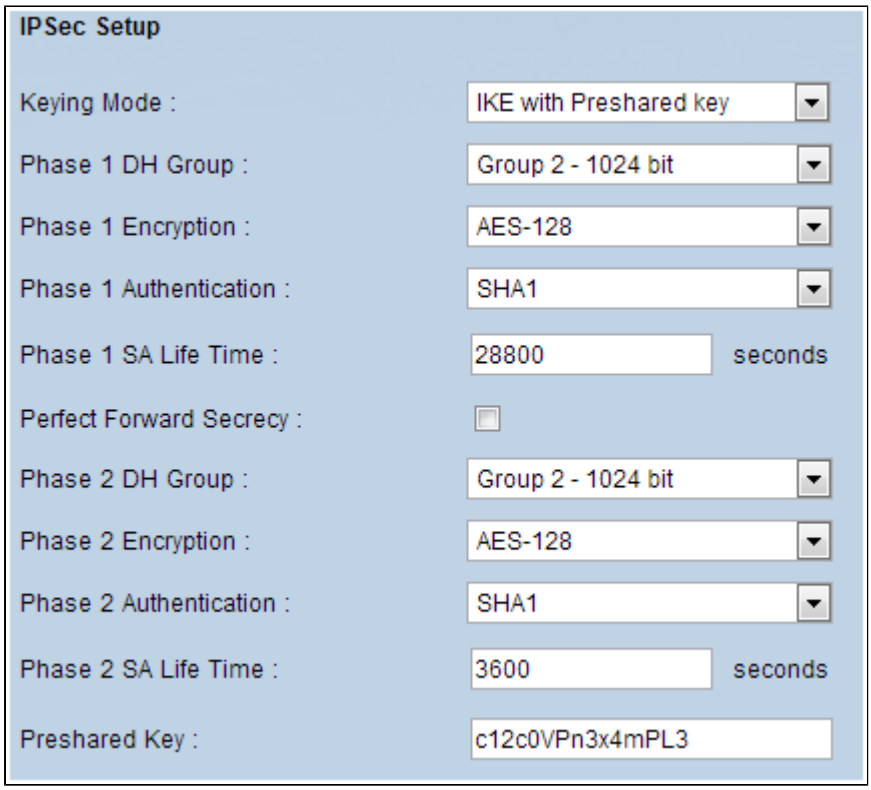
b) Utilizzare la seconda subnet come gruppo "Sicurezza locale".



C) E utilizzare la seconda subnet remota come gruppo "Sicurezza remota".



d) Configurare la crittografia per le Fasi 1 e 2 come per il primo tunnel.



Configurazione dell'ASA

A questo punto, la configurazione dell'appliance ASA viene modificata. Questa configurazione è incredibilmente semplice. È possibile utilizzare la stessa configurazione di cui sopra, in quanto utilizza tutte le stesse impostazioni di crittografia, con una modifica solo di lieve entità. Dobbiamo etichettare il traffico aggiuntivo come "interessante" affinché il firewall lo invii sulla VPN. Poiché per identificare il traffico interessato viene utilizzato un elenco degli accessi, è sufficiente modificare tale elenco.
Passaggio 1. Per iniziare, eliminare il vecchio elenco degli accessi in modo da poter modificare gli oggetti nell'appliance ASA. Usare la forma "no" del comando per rimuovere le configurazioni dalla CLI.
Passaggio 2. Dopo aver rimosso l'ACL, si desidera creare nuovi oggetti per le nuove subnet interessate (supponendo che non sia già stato fatto durante l'impostazione di tali subnet). Vogliamo

anche renderli più descrittivi.
In base alla configurazione VLAN indicata di seguito:

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan2
 nameif engineering
 security-level 100
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan10
 nameif outside
 security-level 0
 ip address 12.23.35.10 255.255.255.0
```

È necessario un gruppo di oggetti per la rete interna principale (192.168.10.x) e la rete di progettazione (192.168.20.x). Configurare gli oggetti di rete nel modo seguente:

```
ASA5505(config)# show run object
object network ASAvlan1
 subnet 192.168.10.0 255.255.255.0
object network ASAvlan2
 subnet 192.168.20.0 255.255.255.0
object network RVvlan1
 subnet 122.166.12.0 255.255.255.0
object network RVvlan2
 subnet 122.166.13.0 255.255.255.0
```

Passaggio 3. Una volta configurati gli oggetti di rete rilevanti, è possibile configurare l'elenco degli accessi in modo che venga contrassegnato il traffico appropriato. Si desidera verificare di disporre di una voce dell'elenco degli accessi per entrambe le reti dietro l'appliance ASA su entrambe le subnet remote. Il risultato finale dovrebbe essere simile a questo.

```
ASA5505(config)# show run access-list
access-list vpn extended permit ip object ASAvlan1 object RVvlan1
access-list vpn extended permit ip object ASAvlan1 object RVvlan2
access-list vpn extended permit ip object ASAvlan2 object RVvlan1
access-list vpn extended permit ip object ASAvlan2 object RVvlan2
```

Passaggio 4. Ora, poiché il vecchio elenco degli accessi è stato eliminato, è necessario riapplicarlo alla mappa crittografica utilizzando lo stesso comando di prima:

```
ASA5505(config)# crypto map asarv 1 match address vpn
```

Verificare la connessione

Ed è tutto! Il tunnel dovrebbe essere operativo. Avviare la connessione e controllare lo stato utilizzando il comando "show crypto isakmpsa" sull'appliance ASA.

```
ASA5505(config)# show crypto isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 12.23.36.10
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE
ASA5505(config)#
```

Nella serie RV lo stato viene visualizzato nella pagina VPN > Summary (Riepilogo).

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	VPNSubnet1	Connected	AES/SHA1	122.166.12.0 255.255.255.0	192.168.10.0 255.255.255.0	12.23.35.10	Disconnect	
2	VPNsubnet2	Connected	AES/SHA1	122.166.13.0 255.255.255.0	192.168.20.0 255.255.255.0	12.23.35.10	Disconnect	

Add Page 1 of 1

Qui è disponibile un video relativo a questo articolo...

Fare clic qui per visualizzare altre Tech Talks di Cisco

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).