

# Configurazione di un tunnel VPN da sito a sito tra Cisco RV320 Gigabit Dual WAN VPN Router e Cisco serie 500 Integrated Services Adapter

## Obiettivo

Una rete privata virtuale (VPN) è una tecnologia ampiamente utilizzata per connettere reti remote a una rete privata principale, simulando un collegamento privato sotto forma di canale crittografato su linee pubbliche. Una rete remota può connettersi a una rete principale privata come se facesse parte della rete principale privata senza problemi di sicurezza a causa di una negoziazione in due fasi che crittografa il traffico VPN in modo che solo gli endpoint VPN sappiano come decrittografarlo.

In questa breve guida viene fornito un esempio di progettazione per la creazione di un tunnel VPN IPsec da sito a sito tra un Cisco serie 500 Integrated Services Adapter e un router Cisco serie RV.

## Dispositivi interessati

- Cisco serie RV RV320 Router
- Cisco serie 500 Integrated Services Adapter (ISA570)

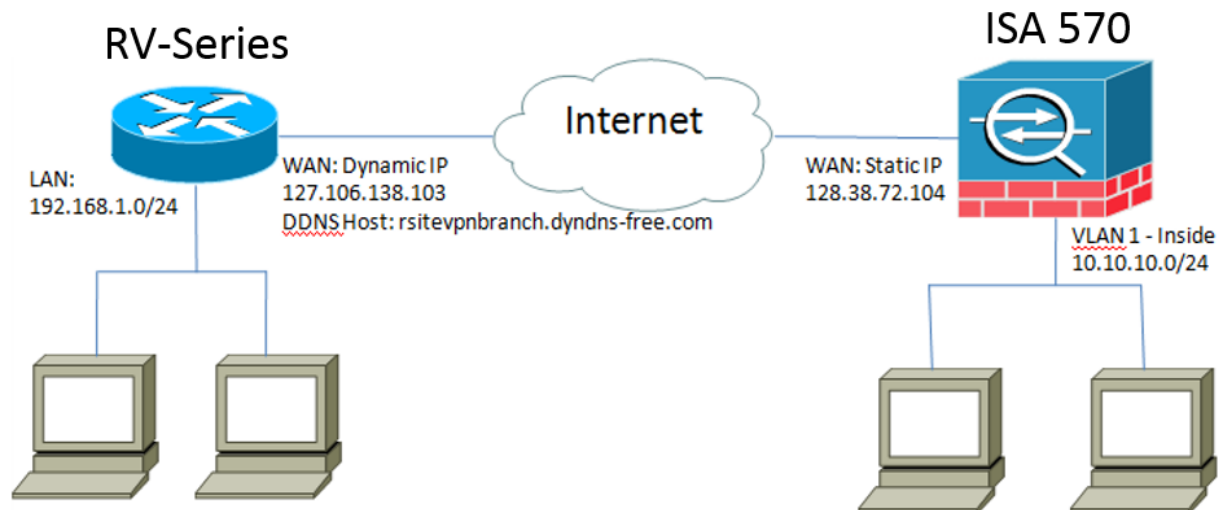
## Versione del software

- 4.2.2.08 [Cisco serie RV0xx VPN Router]

## Preconfigurazione

Esempio di rete

Di seguito viene illustrata una topologia VPN da sito a sito.



Viene configurato e stabilito un tunnel VPN IPsec da sito a sito tra il router Cisco serie RV presso l'ufficio remoto e il Cisco serie 500 ISA presso l'ufficio principale. Con questa configurazione, un host nella LAN 192.168.1.0/24 presso l'ufficio remoto e un host nella LAN 10.10.10.0/24 presso l'ufficio principale possono comunicare tra loro in modo sicuro tramite VPN.

## Concetti fondamentali

### 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, Internet Security Association e il protocollo ISAKMP (Key Management Protocol) e utilizza uno scambio di chiavi Diffie-Hellman per impostare un segreto di sessione condiviso da cui derivano le chiavi crittografiche.

### Protocollo ISAKMP (Internet Security Association and Key Management Protocol)

Il protocollo ISAKMP (Internet Security Association and Key Management Protocol) viene utilizzato per negoziare il tunnel VPN tra due endpoint VPN. 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.

### IPsec (Internet Protocol Security)

IP Security Protocol (IPsec) è una suite di protocolli per la protezione delle comunicazioni IP tramite autenticazione e crittografia di ogni pacchetto IP di un flusso di dati. IPsec include anche protocolli per stabilire l'autenticazione reciproca tra gli agenti all'inizio della sessione e la negoziazione delle chiavi crittografiche da utilizzare durante la sessione. IPsec può essere utilizzato per proteggere i flussi di dati tra una coppia di host, gateway o reti.

## Suggerimenti per la progettazione

**Topologia VPN:** per topologia VPN point-to-point si intende un tunnel IPsec protetto configurato tra il sito principale e il sito remoto.

Le aziende spesso richiedono più siti remoti in una topologia multisito e implementano una topologia VPN hub e spoke o una topologia VPN a rete completa. Una topologia VPN hub e spoke indica che i siti remoti non richiedono la comunicazione con altri siti remoti e che ogni sito remoto stabilisce solo un tunnel IPsec protetto con il sito principale. Una topologia VPN a rete completa implica che i siti remoti devono comunicare con altri siti remoti e che ogni sito remoto stabilisce un tunnel IPsec protetto con il sito principale e tutti gli altri siti remoti.

**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, algoritmi di crittografia più avanzati richiedono più risorse di elaborazione da un router.

**Indirizzamento IP dinamico della WAN e servizio DNS (Dynamic Domain Name Service):** è necessario stabilire il tunnel VPN 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 cavo, e riceve indirizzi IP dinamici dai propri ISP. In questi casi, è possibile utilizzare il servizio DNS (Dynamic Domain Name Service) 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.

## Suggerimenti per la configurazione

### Elenco di controllo pre-configurazione

Passaggio 1. Collegare un cavo Ethernet tra l'RV320 e il relativo modem DSL o via cavo e collegare un cavo Ethernet tra l'ISA570 e il relativo modem DSL o via cavo.

Passaggio 2. Accendere l'RV320 e collegare i PC, i server e gli altri dispositivi IP interni alle porte LAN dell'RV320.

Passaggio 3. Accendere ISA570, quindi collegare i PC interni, i server e gli altri dispositivi IP alle porte LAN di ISA570.

Passaggio 4. Verificare di configurare gli indirizzi IP di rete in ogni sito in subnet diverse.

Nell'esempio, la LAN dell'ufficio remoto utilizza 192.168.1.0 e la LAN dell'ufficio principale 10.10.10.0.

Passaggio 5. Verificare che i PC locali siano in grado di connettersi ai rispettivi router e ad altri PC sulla stessa LAN.

## Identificazione della connessione WAN

È necessario sapere se l'ISP fornisce un indirizzo IP dinamico o statico. L'ISP in genere fornisce un indirizzo IP dinamico, ma è necessario confermarlo prima di completare la configurazione del tunnel VPN da sito a sito.

# Configurazione del tunnel VPN IPsec da sito a sito per RV320 nella sede remota

Passaggio 1. Accedere a **VPN > Gateway-to-Gateway** (vedere immagine)

a) Immettere un nome di tunnel, ad esempio UfficioRemoto.

b.) Impostare Interface su WAN1.

c.) Impostare la modalità di impostazione chiavi su IKE con chiave già condivisa.

d.) Immettere l'indirizzo IP locale e l'indirizzo IP remoto.

L'immagine seguente mostra la pagina RV320 Gigabit Dual WAN VPN Router Gateway to Gateway:

The screenshot displays the configuration interface for a Cisco RV320 Gigabit Dual WAN VPN Router. The left sidebar shows the navigation menu with 'VPN' expanded and 'Gateway to Gateway' selected. The main content area is titled 'Gateway to Gateway' and contains the following configuration sections:

- Add a New Tunnel:**
  - Tunnel No.: 2
  - Tunnel Name: [Empty field]
  - Interface: WAN1 (dropdown)
  - Keying Mode: IKE with Preshared key (dropdown)
  - Enable:
- Local Group Setup:**
  - Local Security Gateway Type: IP Only (dropdown)
  - IP Address: 0.0.0.0
  - Local Security Group Type: Subnet (dropdown)
  - IP Address: 192.168.1.0
  - Subnet Mask: 255.255.255.0
- Remote Group Setup:**
  - Remote Security Gateway Type: IP Only (dropdown)
  - IP Address: [Empty field]
  - Remote Security Group Type: Subnet (dropdown)
  - IP Address: [Empty field]

© 2013 Cisco Systems, Inc. All Rights Reserved.

Passaggio 2. Configurare le impostazioni del tunnel IPsec (vedere immagine)

a) Impostare *Encryption* su 3DES.

b.) Impostare *Authentication* su SHA1.

c.) Controlla *Perfect Forward Secrecy*.

d.) Configurare la *chiave già condivisa* (deve essere la stessa su entrambi i router).

Di seguito viene illustrata la configurazione di IPsec (Fasi 1 e 2):

**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption :

Phase 1 Authentication:

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:


Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Preshared Key Strength Meter: 

**Nota:** Tenere presente che le impostazioni del tunnel IPsec su entrambi i lati del tunnel VPN IPsec da sito a sito devono corrispondere. In caso di discrepanze tra le impostazioni del tunnel IPsec della RV320 e della ISA570, entrambi i dispositivi non riusciranno a negoziare la chiave di crittografia e a connettersi.

Passaggio 3. Fare clic su **Save** per completare la configurazione.

## Configurazione del tunnel VPN IPsec da sito a sito per ISA570 nella sede principale

Passaggio 1. Vai a **VPN > Criteri IKE** (vedi immagine)

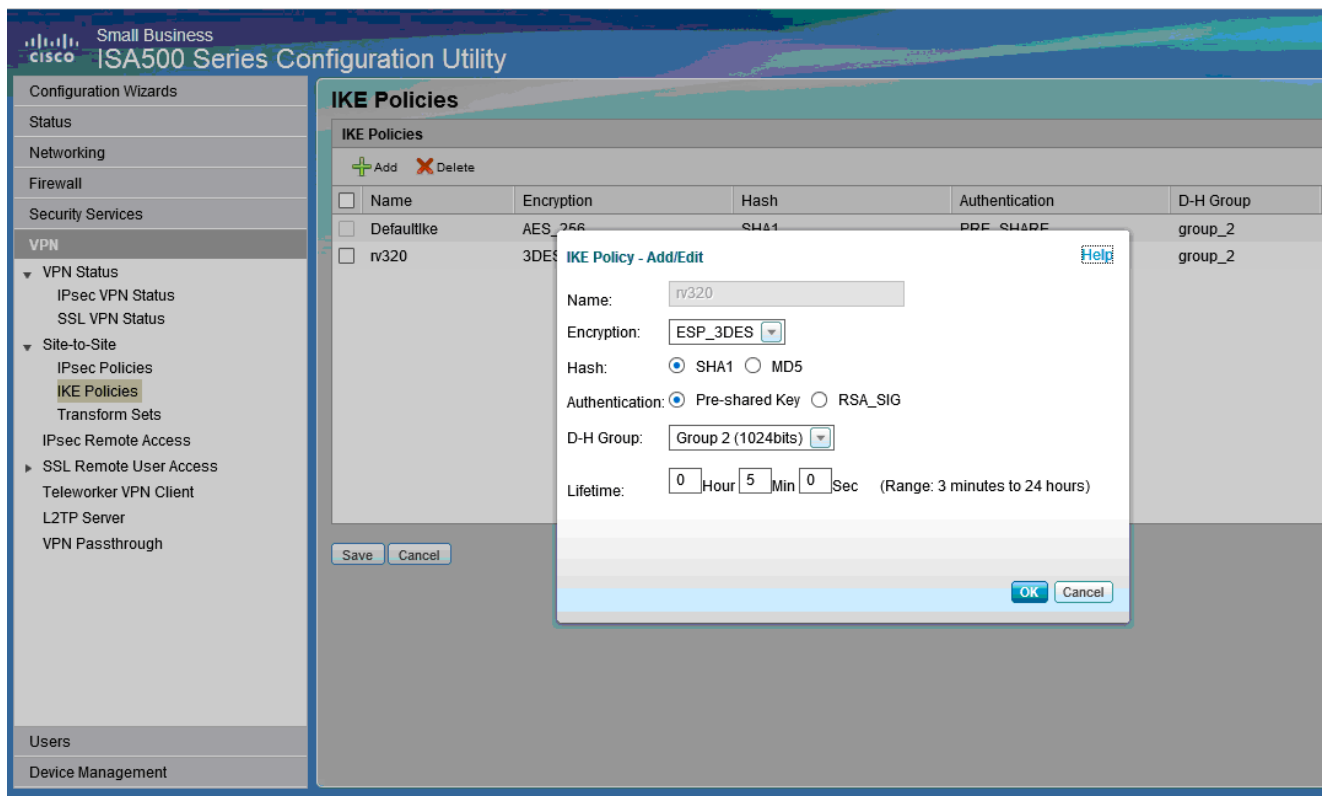
a) Impostare *Encryption* su ESP\_3DES.

b.) Impostare *Hash* su SHA1.

c.) Impostare *Authentication (Autenticazione)* su Pre-shared Key (Chiave già condivisa).

d.) Impostare *Gruppo D-H* sul Gruppo 2 (1024 bit).

L'immagine seguente mostra i criteri IKE:

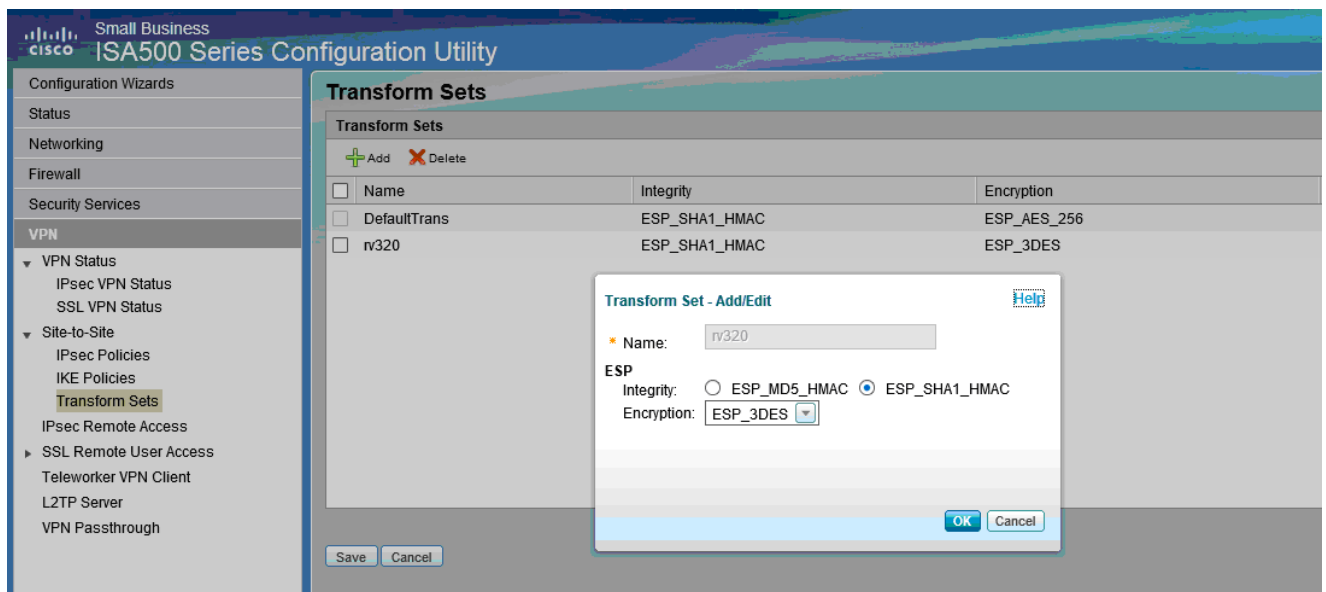


Passaggio 2. Andare su **VPN > Set trasformazioni IKE** (vedere immagine)

a) Impostare *Integrity* su ESP\_SHA1\_HMAC.

b.) Impostare *Encryption* su ESP\_DES.

Di seguito vengono illustrati i set di trasformazioni IKE:



Passaggio 3. Andare su **VPN > Criteri IPsec > Aggiungi > Impostazioni di base** (vedere l'immagine)

a) Immettere una *descrizione*, ad esempio RV320.

b.) Impostare *Abilita criteri IPsec* su On.

c.) Impostare *Remote Type* su *Static IP*.

d.) Immettere l' *indirizzo remoto*.

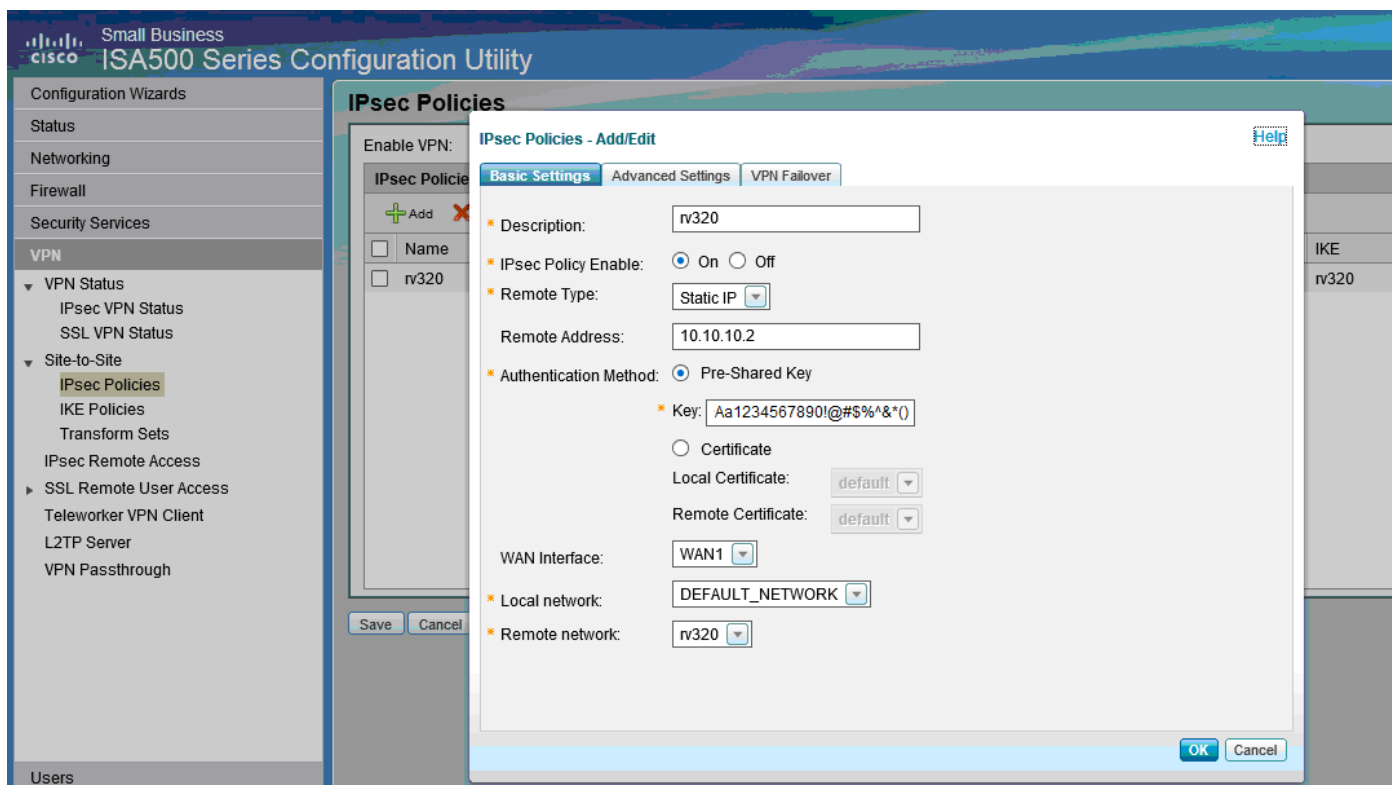
e.) Impostare *Authentication Method (Metodo di autenticazione)* su Pre-Shared Key (Chiave già condivisa).

f.) Impostare *WAN Interface* su WAN1.

g.) Impostare *Local Network* su DEFAULT\_NETWORK.

h.) Impostare *Remote Network* su RV320.

L'immagine seguente mostra le impostazioni di base dei criteri IPsec:



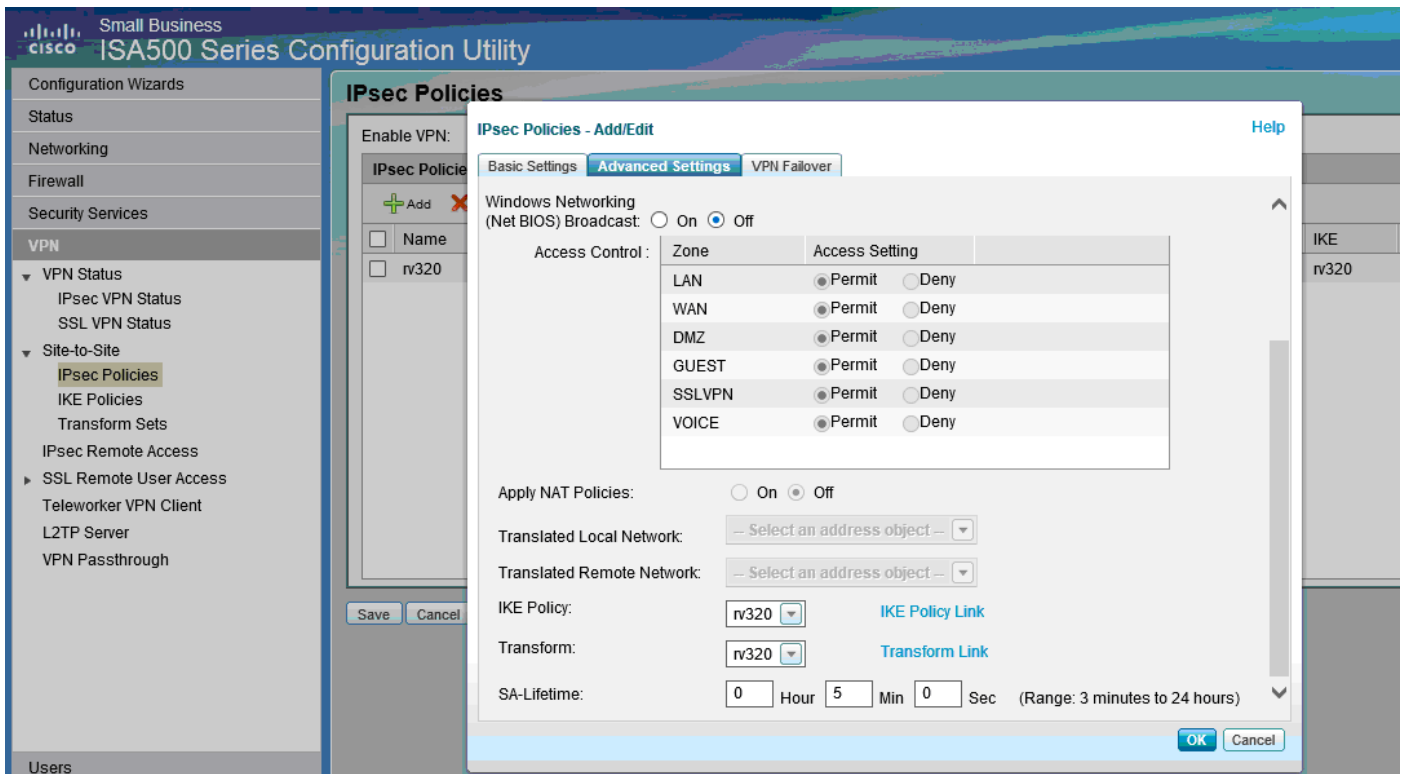
Passaggio 4. Andare su **VPN > Criteri IPsec > Aggiungi > Impostazioni avanzate** (vedere la figura)

a) Impostare *Criteri IKE* e *Set di trasformazioni IKE* rispettivamente su quelli creati nei passaggi 1 e 2.

b.) Impostare *SA-Lifetime* su 0 Hour 5 Min 0 Sec.

c.) Fare clic su **OK**.

Di seguito vengono illustrate le impostazioni avanzate dei criteri IPsec:



Passaggio 5. Connettere il tunnel VPN IPsec da sito a sito (vedere immagine)

a.) Impostare *Abilita VPN* su On.

b.) Fare clic sul pulsante **Connetti**.

L'immagine seguente mostra il pulsante Connetti:

