Panoramica e best practice della VPN per router Cisco RV

Obiettivo

L'obiettivo di questo documento è fornire una panoramica delle best practice delle VPN (Virtual Private Network) a tutti i nuovi router Cisco serie RV.

Sommario

Introduzione

Sembra che tanto tempo fa l'unico posto dove si poteva lavorare era in ufficio. Forse ricorderete che a quei tempi dovevamo andare in ufficio il fine settimana per risolvere una questione lavorativa. Non c'era altro modo per ottenere i dati dalle risorse aziendali se non si era fisicamente in ufficio. Quei giorni sono finiti. Nei tempi di oggi, è possibile essere in viaggio; condurre affari da casa, da un altro ufficio, da una caffetteria, o anche da un altro paese. Il lato negativo è che gli hacker sono sempre alla ricerca di prendere i vostri dati sensibili. Il semplice utilizzo di Internet non è sicuro. Cosa si può fare per ottenere flessibilità e sicurezza? Configura una VPN!

Una connessione VPN 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 una connessione sicura a un'infrastruttura di rete sottostante per proteggere la rete privata e le relative risorse.

Un tunnel VPN stabilisce una rete privata in grado di inviare i dati in modo sicuro utilizzando la crittografia per codificare i dati e l'autenticazione per garantire l'identità del client. Le filiali utilizzano spesso una connessione VPN, in quanto è utile e necessario per consentire ai dipendenti di accedere alla rete privata anche quando si trovano all'esterno dell'ufficio.

Normalmente, le VPN da sito a sito connettono intere reti l'una all'altra. Estendono una rete e consentono di rendere disponibili risorse di computer da una posizione in altre posizioni. Tramite l'utilizzo di un router che supporta la VPN, un'azienda può connettere più siti fissi su una rete pubblica, ad esempio Internet.

La configurazione da client a sito di una VPN consente a un host remoto o a un client di agire come se si trovassero sulla stessa rete locale. È possibile configurare una connessione VPN tra il router e un endpoint dopo che il router è stato configurato per la connessione Internet. Il client VPN dipende dalle impostazioni del router VPN, oltre ai requisiti delle impostazioni corrispondenti, per stabilire una connessione. Inoltre, alcune applicazioni client VPN sono specifiche della piattaforma e dipendono anche dalla versione del sistema operativo. Le impostazioni devono essere identiche o non possono comunicare.

Una VPN può essere configurata con uno dei seguenti elementi:

- SSL (Secure Sockets Layer)
- IPSec (Internet Protocol Security)
- Protocollo PPTP (Point to Point Tunneling Protocol) - non sicuro come SSL o IPSec
- GRE (Generic Routing Encapsulation)
- L2TP (Layer 2 Tunneling Protocol)

Se non hai mai configurato una VPN prima, riceverai molte nuove informazioni in questo articolo. Questa non è una guida dettagliata, ma una panoramica di riferimento. Pertanto, sarebbe utile leggere questo articolo nella sua interezza prima di procedere e tentare di configurare una VPN sulla rete. In questo articolo vengono forniti collegamenti a passaggi specifici.

I prodotti di terze parti non Cisco, tra cui TheGreenBow, OpenVPN, Shrew Soft e EZ VPN non sono supportati da Cisco. Sono inclusi esclusivamente a scopo orientativo. Se oltre all'articolo avete bisogno di supporto, contattate il supporto di terze parti.

Vantaggi dell'utilizzo di una connessione VPN

- L'utilizzo di una connessione VPN consente di proteggere i dati e le risorse di rete riservati.
- Offre convenienza e accessibilità per i dipendenti remoti o aziendali, che potranno accedere facilmente alle risorse principali dell'ufficio senza dover essere fisicamente presenti e mantenere la sicurezza della rete privata e delle sue risorse.
- La comunicazione tramite una connessione VPN offre un livello di protezione più elevato rispetto ad altri metodi di comunicazione remota. Questo è possibile grazie a un algoritmo di crittografia avanzato che protegge la rete privata da accessi non autorizzati.
- Le posizioni geografiche effettive degli utenti sono protette e non esposte al pubblico o a reti condivise come Internet.
- Una VPN consente di aggiungere nuovi utenti o un gruppo di utenti senza la necessità di componenti aggiuntivi o una configurazione complessa.

Rischi dell'utilizzo di una connessione VPN

- Potrebbero esistere rischi per la sicurezza dovuti a una configurazione errata. Poiché la progettazione e l'implementazione di una VPN può essere complicata, è necessario affidare il compito di configurare la connessione a un professionista esperto e competente in modo da garantire che la sicurezza della rete privata non venga compromessa.
- Può essere meno affidabile. Poiché una connessione VPN richiede una connessione a Internet, è importante disporre di un provider con una reputazione collaudata e testata per fornire un servizio Internet eccellente e garantire tempi di inattività minimi o nulli.
- Se si verifica una situazione in cui è necessario aggiungere una nuova infrastruttura o una nuova serie di configurazioni, possono verificarsi problemi tecnici dovuti all'incompatibilità, in particolare se si

tratta di prodotti o fornitori diversi da quelli già in uso.
- Si possono verificare velocità di connessione lente. Se si utilizza una connessione ISP che fornisce un servizio VPN gratuito, è probabile che anche la connessione risulti lenta poiché questi provider non assegnano la priorità alle velocità di connessione. È importante notare che il throughput VPN dipende dalle funzionalità hardware del router.

Per ulteriori informazioni sul funzionamento delle VPN, fare clic qui.

Suggerimenti per la configurazione di una VPN

1. Usare una subnet LAN IP diversa su entrambe le estremità durante la configurazione della VPN tra siti diversi. Ad esempio, se il sito a cui ci si connette utilizza uno schema di indirizzamento 192.168.x.x, è possibile utilizzare una subnet 10.x.x.x o 172.16.x.x - 172.31.x.x. In alternativa, è possibile avere subnet mask diverse. Quando si modifica l'indirizzo IP del router, i dispositivi DHCP (Dynamic Host Configuration Protocol) selezionano automaticamente un indirizzo IP in tale subnet.
2. Usare l'IP pubblico statico sull'interfaccia WAN del router per una connettività VPN stabile.
3. Accertarsi che il livello di crittografia e autenticazione selezionato sia lo stesso del router a cui si desidera stabilire un tunnel VPN per la VPN.
4. Accertarsi che la chiave PSK e la durata della chiave immesse siano le stesse del router remoto. Un PSK può essere ciò che si desidera, deve semplicemente corrispondere sul sito e con il client quando si configurano come client sul loro computer. A seconda del dispositivo, è possibile che alcuni simboli non consentiti non siano utilizzabili. Durata chiave indica la frequenza con cui il sistema modifica la chiave. È preferibile un certificato poiché è considerato più sicuro.
5. Per la maggior parte delle VPN, i client non hanno bisogno di un certificato per utilizzare una VPN, ma solo per la verifica tramite il router. Ad esempio, OpenVPN richiede sia certificati client che certificati del sito.
6. Impostare la durata dell'ASA nella fase I su un valore più lungo rispetto alla durata dell'ASA nella fase II. Se si rende la Fase I più breve della Fase II, sarà necessario rinegoziare il tunnel frequentemente in senso inverso rispetto al tunnel di dati. Un tunnel di dati necessita di maggiore sicurezza, pertanto è preferibile che la durata nella Fase II sia inferiore a quella della Fase I.
7. Cambiare tutte le password in qualcosa di più complesso.

Tipi di VPN

SSL (Secure Sockets Layer)

Cisco serie RV34x supporta una VPN SSL con AnyConnect. Gli RV160 e RV260 possono usare OpenVPN, un'altra VPN SSL. Il server VPN SSL 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.

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

Per impostare l'accesso in SSL, è possibile procedere in due modi:

1. Certificato autofirmato: un certificato firmato dal proprio creatore. Questa opzione non è consigliata e deve essere utilizzata solo in un ambiente di test.
2. Certificato firmato CA: molto più sicuro e consigliato. A pagamento, una terza parte verifica che la rete sia legittima e crea un certificato CA che viene quindi allegato al sito. Per ulteriori informazioni sui certificati CA, vedere la sezione Certificati di questo articolo.

Questo documento contiene link ad articoli su AnyConnect. Per una panoramica di AnyConnect, fare clic qui.

Profilo IPsec

Easy VPN (EZVPN), TheGreenBow e Shrew Soft sono VPN per la sicurezza del protocollo Internet (IPSec). Le VPN IPSec forniscono tunnel protetti tra due peer o da un client a un sito. I pacchetti considerati sensibili devono essere inviati tramite questi tunnel protetti. I parametri che includono l'algoritmo hash, l'algoritmo di crittografia, la durata della chiave e la modalità da utilizzare per proteggere i pacchetti sensibili devono essere definiti specificando le caratteristiche di questi tunnel. Quindi, quando il peer IPsec rileva un pacchetto sensibile di questo tipo, configura il tunnel sicuro appropriato e invia il pacchetto attraverso questo tunnel al peer remoto.

Quando il protocollo IPsec viene implementato in un firewall o in un router, offre una protezione avanzata che può essere applicata a tutto il traffico che attraversa il perimetro. Il traffico all'interno di un'azienda o di un gruppo di lavoro non comporta il sovraccarico delle attività di elaborazione relative alla sicurezza.

Affinché le due estremità di un tunnel VPN possano essere crittografate e stabilite correttamente, entrambe devono concordare i metodi di crittografia, decrittografia e autenticazione. Il profilo IPsec è la configurazione centrale di IPsec che definisce algoritmi quali la crittografia, l'autenticazione e il gruppo Diffie-Hellman (DH) per la negoziazione nelle fasi I e II in modalità automatica e in modalità di generazione manuale delle chiavi.

Componenti importanti di IPSec sono IKE (Internet Key Exchange) fase 1 e fase 2.

Lo scopo principale della fase uno di IKE è autenticare i peer IPSec e configurare un canale sicuro tra i peer per consentire gli scambi IKE. La fase uno di IKE esegue le seguenti funzioni:

- Autentica e protegge le identità dei peer IPSec
- Negozia un criterio di associazione di sicurezza IKE corrispondente tra peer per proteggere lo scambio IKE
- Esegue uno scambio Diffie-Hellman autenticato con il risultato finale di avere chiavi segrete condivise corrispondenti
- Imposta un tunnel sicuro per negoziare i parametri della fase due di IKE
- Si verifica in due modalità, modalità principale e aggressiva

Lo scopo della seconda fase di IKE è negoziare le associazioni di protezione IPSec per configurare il tunnel IPSec. La fase due di IKE esegue le seguenti funzioni:

- Negozia i parametri SA IPSec protetti da un'associazione di protezione IKE esistente
- Stabilisce le associazioni di protezione IPSec
- Rinegozia periodicamente le associazioni di protezione IPSec per garantire la sicurezza
- Esegue facoltativamente uno scambio Diffie-Hellman aggiuntivo
- Viene utilizzata una sola modalità, modalità rapida

Se nei criteri IPSec è specificata l'opzione PFS (Perfect Forward Secrecy), verrà eseguito un nuovo scambio DH con ogni modalità rapida, fornendo materiale per le chiavi con maggiore entropia (durata del materiale della chiave) e quindi maggiore resistenza agli attacchi crittografici. Ogni scambio di DH richiede elevate esponenzialità, con conseguente aumento dell'utilizzo della CPU e riduzione dei costi delle prestazioni.

- Configurazione del profilo IPSec (Internet Protocol Security) su un router serie RV34x
- Configurazione dei profili IPSec (modalità di impostazione automatica della trasparenza) sugli switch RV160 e RV260
- Configurazione della modalità di codifica manuale del profilo IPsec sui router RV160 e RV260

Protocollo PPTP (Point-to-Point Tunneling Protocol)

PPTP è un protocollo di rete utilizzato per creare tunnel VPN tra reti pubbliche. I server PPTP sono anche noti come server VPDN (Virtual Private Dialup Network). Il protocollo PPTP viene talvolta utilizzato rispetto ad altri protocolli perché è più veloce e può essere utilizzato sui dispositivi mobili. Tuttavia, è importante notare che non è sicuro come altri tipi di VPN. Sono disponibili diversi metodi per la connessione con account di tipo PPTP. Per ulteriori informazioni, fare clic sui collegamenti:

- Configurazione di un server PPTP (Point-to-Point Tunneling Protocol) sul router serie Rv34x
- Configurazione del server PPTP (Point to Point Tunneling Protocol) su router VPN serie RV320 e RV325 su Windows

Generic Routing Encapsulation

GRE (Generic Routing Encapsulation) è un protocollo di tunneling che fornisce un approccio semplice e generico al trasporto di pacchetti di un protocollo su un altro protocollo tramite l'incapsulamento.

GRE incapsula un payload, ossia un pacchetto interno che deve essere recapitato a una rete di destinazione all'interno di un pacchetto IP esterno. Il tunnel GRE si comporta come un collegamento point-to-point virtuale che ha due endpoint identificati dall'origine del tunnel e dall'indirizzo di destinazione del tunnel.

Gli endpoint del tunnel inviano i payload attraverso i tunnel GRE indirizzando i pacchetti incapsulati attraverso le reti IP intermedie. Gli altri router IP non analizzano il payload (il pacchetto interno), ma si limitano ad analizzare il pacchetto IP esterno quando lo inoltrano verso l'endpoint del tunnel GRE. Dopo aver raggiunto l'endpoint del tunnel, l'incapsulamento GRE viene rimosso e il payload viene inoltrato alla destinazione finale del pacchetto.

L'incapsulamento dei datagrammi in una rete viene eseguito per diversi motivi, ad esempio quando un server di origine desidera influenzare il percorso di un pacchetto verso l'host di destinazione. Il server di origine è anche noto come server di incapsulamento.

L'incapsulamento IP-in-IP implica l'inserimento di un'intestazione IP esterna sull'intestazione IP esistente. Gli indirizzi di origine e destinazione nell'intestazione IP esterna puntano agli endpoint del tunnel IP-in-IP. Lo stack di intestazioni IP viene usato per indirizzare il pacchetto su un percorso predeterminato verso la destinazione, a condizione che l'amministratore di rete conosca gli indirizzi di loopback dei router che trasportano il pacchetto.

Questo meccanismo di tunneling può essere utilizzato per determinare la disponibilità e la latenza per la maggior parte delle architetture di rete. Si noti che l'intero percorso dall'origine alla destinazione non deve essere incluso nelle intestazioni, ma è possibile scegliere un segmento della rete per indirizzare i pacchetti.

Protocollo di tunneling di livello 2

L2TP non fornisce meccanismi di crittografia per il traffico che instrada. Per crittografare i dati, si basa invece su altri protocolli di protezione, ad esempio IPSec.

Viene stabilito un tunnel L2TP tra il L2TP Access Concentrator (LAC) e il L2TP Network Server (LNS). Viene inoltre stabilito un tunnel IPSec tra questi dispositivi e tutto il traffico del tunnel L2TP viene crittografato utilizzando IPSec.

Alcuni termini chiave con L2TP:

- **CHAP -** Challenge Handshake Authentication Protocol. Protocollo PPP (Point to Point Authentication Protocol).

- **L2TP Access Concentrator (LAC) -** Un LAC può essere un server di accesso alla rete Cisco connesso alla rete PSTN (Public Switched Telephone Network). I LAC devono implementare solo supporti per il funzionamento su L2TP. Un LAC può connettersi al sistema LNS utilizzando una rete locale o una rete WAN, ad esempio un Frame Relay pubblico o privato. Il LAC è l'iniziatore delle chiamate in arrivo e il destinatario delle chiamate in uscita.
- **Server di rete L2TP (LNS):** quasi tutti i router Cisco connessi a una rete locale o WAN, ad esempio un Frame Relay pubblico o privato, possono fungere da LAN. Si tratta del lato server del protocollo L2TP e deve funzionare su qualsiasi piattaforma che termina le sessioni PPP. L'LNS è l'iniziatore delle chiamate in uscita e il destinatario delle chiamate in arrivo. La figura 1 illustra la routine di chiamata tra il LAC e il LNS.
- **VPDN (Virtual Private Dial Network) -** Tipo di VPN di accesso che utilizza il protocollo PPP per fornire il servizio.

Per maggiori informazioni su L2TP, fare clic sui seguenti link:

- Configurazione delle impostazioni WAN L2TP sul router RV34x
- Guida alla configurazione di Wide-Area Networking: servizi di layer 2, Cisco IOS XE release 3S

VPN compatibili con i router VPN della serie Cisco RV

	RV34X	RV32X	RV160X/RV260X
IPSec (IKEv1)			
ShrewSoft	Sì	Sì	Sì
Arcobaleno	Sì	Sì	Sì
Client incorporato Mac	Sì	Sì	No
iPhone/iPad	Sì	Sì	No
Android	Sì	Sì	Sì
L2TP/IPSec	Sì (PAP)	No	No
PPTP	Sì (PAP)	Sì*	Sì (PAP)
Other (Altro)			
AnyConnect	Sì	No	No
Openvpn	No	Sì	Sì
IKEv2			
Windows	Sì*	No	Sì*
Mac	Sì	No	Sì
iPhone	Sì	No	Sì
Android	Sì	No	Sì

Tecnologia VPN	Dispositivi supportati	Client supportati*	Dettagli e avvertenze
IPSec (IKEv1)	RV34X, RV32X, RV160X/RV260X	Nativo: Mac, iPhone, iPad, Android	Procedure semplificate di installazione, risoluzione dei problemi e supporto. È disponibile su tutti i router, è semplice da configurare (per la maggior parte), ha la migliore registrazione per risolvere i problemi. E include il maggior numero di dispositivi.

		Altro: EasyVPN (Cisco VPN Client), ShrewSoft, Greenbow	Questo è il motivo per cui in genere consigliamo ShrewSoft (libero e funziona) e Greenbow (non libero, ma funziona). Per Windows, sono disponibili come opzioni i client ShrewSoft e Greenbow, in quanto Windows non dispone di un client VPN nativo IPSec puro. Per ShrewSoft e Greenbow, è un po' più coinvolto, ma non difficile. Una volta configurati per la prima volta, i profili client possono essere esportati e quindi importati su altri client. Per i router RV160X/RV260X, poiché non è disponibile l'opzione Easy VPN, è necessario utilizzare l'opzione Client di terze parti, che non funziona con Mac, iPhone o iPad. Tuttavia, è possibile configurare i client ShrewSoft, Greeenbow e Android per la connessione. Per i client Mac, iPhone e iPad, consiglio IKEv2 (vedere di seguito).
AnyConnect	RV34X	Windows, Mac, iPhone, iPad, Android	Alcuni clienti richiedono una soluzione Cisco completa ed è questa. È semplice da configurare, dispone di funzioni di log, ma può essere difficile comprendere i log. Richiede la necessità di acquistare licenze client a costi elevati. È una soluzione Cisco completa e viene aggiornata. La risoluzione dei problemi non è semplice come IPSec, ma è migliore delle altre opzioni VPN.
L2TP/IPSec	RV34X	Nativo: Windows	Questo è quello che consiglierò ai clienti che devono utilizzare il client VPN integrato in Windows. Di seguito sono riportati due avvertimenti: 1. L'autenticazione PAP è supportata solo quando si utilizza l'autenticazione locale. Dobbiamo accedere a ciascun client e selezionare la crittografia opzionale o non, disabilitare le opzioni MS-CHAP e abilitare PAP. Il nome utente e la password vengono quindi inviati in chiaro. Non si tratta di un problema grave, in quanto tutto è crittografato con IPSec e deve essere configurato su ogni client. Su Windows, questo è configurabile, ma non su Mac, iPhone, iPad, o dispositivi Android, quindi può essere utilizzato solo dai client Windows a meno che non abbiano un server di autenticazione esterno come Radius o LDAP. 2. Se il router è dietro un dispositivo NAT, la connessione avrà esito negativo sui computer Windows. Per ovviare al problema, è necessario creare una chiave del Registro di sistema in ciascun client per consentire il protocollo NAT sia sul client

			che sul router.
IPSec (IKEv2)	RV34X, RV160X/RV260X	Nativo: Windows, Mac, iPhone, iPad, Android	Il client nativo Windows per IKEv2 richiede l'autenticazione del certificato, che richiede un'infrastruttura PKI in quanto sia il router che tutti i client devono disporre di certificati provenienti dalla stessa CA (o da un'altra CA attendibile). Per coloro che vogliono utilizzare IKEv2, lo configuriamo per i loro dispositivi Mac, iPhone, iPad e Android e di solito lo configuriamo per i loro computer Windows (ShrewSoft, Greenbow, o L2TP/IPSec).
Apri VPN	RV32X, RV160X/RV260X	Open VPN è il client	Maggiore difficoltà di configurazione, risoluzione dei problemi e supporto. Supportato su RV160X/RV260X e RV320. La configurazione è più complessa di IPSec o AnyConnect, in particolare se utilizzano certificati, operazione che la maggior parte richiede. La risoluzione dei problemi è più difficile perché non abbiamo log utili sul router e ci affidiamo ai log del client. Inoltre, gli aggiornamenti della versione del client OpenVPN hanno modificato senza preavviso i certificati accettati. Inoltre, abbiamo riscontrato che questo non funziona con i Chromebook e abbiamo dovuto adottare una soluzione IPSec.

* Verifichiamo quante più combinazioni possibili. Se esiste una combinazione hardware/software specifica, contattare. In caso contrario, consultare la guida alla configurazione per dispositivo per la versione più recente sottoposta a test.

Certificati

Avete mai visitato un sito Web e vi è stato segnalato che non è sicuro? Non ti convince che le tue informazioni private siano al sicuro, e non lo sono! Se un sito è protetto, prima del nome del sito verrà visualizzata un'icona di blocco chiusa. Questo è un simbolo che il sito è stato verificato come sicuro. Si desidera essere certi che l'icona del lucchetto sia chiusa. Lo stesso vale per la tua VPN.

Quando si configura una VPN, è necessario ottenere un certificato da un'Autorità di certificazione (CA). I certificati vengono acquistati da siti di terze parti e utilizzati per l'autenticazione. È un modo ufficiale per dimostrare che il tuo sito è sicuro. Essenzialmente, la CA è una fonte attendibile che verifica che l'azienda sia legittima e che possa essere considerata attendibile. Per una VPN è sufficiente un certificato di livello inferiore a un costo minimo. L'utente viene estratto dall'autorità di certificazione e, una volta verificate le informazioni, l'autorità di certificazione rilascerà il certificato all'utente. Il certificato può essere scaricato come file nel computer. È quindi possibile accedere al router (o al server VPN) e caricarlo in tale posizione.

L'autorità di certificazione utilizza l'infrastruttura a chiave pubblica (PKI, Public Key Infrastructure) per l'emissione di certificati digitali che utilizzano la crittografia a chiave pubblica o privata per garantire la protezione. Le CA sono responsabili della gestione delle richieste di certificati e dell'emissione di certificati

digitali. Alcune CA di terze parti includono IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust e Verisign.

È importante che tutti i gateway in una VPN utilizzino lo stesso algoritmo, in caso contrario non saranno in grado di comunicare. Per semplificare le procedure, si consiglia di acquistare tutti i certificati dalla stessa terza parte attendibile. In questo modo è possibile gestire più certificati in modo più semplice in quanto devono essere rinnovati manualmente.

Nota: i client di solito non hanno bisogno di un certificato per usare una VPN; è solo per la verifica tramite il router. Un'eccezione è OpenVPN, che richiede un certificato client.

Per semplicità, alcune piccole aziende scelgono di utilizzare una password o una chiave già condivisa al posto di un certificato. Si tratta di una soluzione meno sicura che può essere installata gratuitamente.

Ulteriori informazioni sui certificati sono disponibili nei seguenti link:

- Certificato (importazione/esportazione/generazione di CSR) sui router serie RV160 e RV260
- Sostituire il certificato autofirmato predefinito con un certificato SSL di terze parti sul router serie RV34x

VPN da sito a sito su un router

Per il router locale e remoto, è importante verificare che la chiave pre-condivisa (PSK)/la password/il certificato utilizzati per la connessione VPN e le impostazioni di sicurezza corrispondano. Se uno o più router utilizzano Network Address Translation (NAT), utilizzato dalla maggior parte dei router Cisco serie RV, sono necessarie delle esenzioni dal firewall per la connessione VPN sul router locale e remoto.

Per ulteriori informazioni, consultare i seguenti articoli da sito a sito:

- Configurazione della VPN da sito a sito sulla RV34x
- Configurazione di una VPN da sito a sito su un router RV340 o RV345
- Cisco Tech Talk: Configurazione di VPN da sito a sito sui router serie RV340 (video)
- Configurazione della VPN da sito a sito su un router RV160 e RV260 (impostazioni di base)
- VPN da sito a sito sui router RV160 e RV260 (impostazioni avanzate e failover)

VPN da client a sito su un router

Prima di poter configurare una VPN sul lato client, è necessario che un amministratore la configuri sul router.

Fare clic per visualizzare gli articoli di configurazione del router seguenti:

- Configurazione guidata VPN Setup sui router RV160 e RV260
- Configurazione di Show Soft VPN Client con RV160 e RV260
- Cisco Tech Talk: Configurazione di Shrew Soft VPN su RV160 e RV260 (video)
- Configurazione e utilizzo del client VPN IPsec GreenBow per la connessione con i router RV160 e RV260

Creazione di un profilo da client a sito

In una connessione VPN da client a sito, i client di Internet possono connettersi al server per accedere alla rete aziendale o alla LAN dietro il server, mantenendo tuttavia la sicurezza della rete e delle relative risorse. Questa funzione è molto utile perché crea un nuovo tunnel VPN che consente ai telelavoratori e agli utenti

business di accedere alla rete utilizzando un software client VPN senza compromettere la privacy e la sicurezza. I seguenti articoli sono specifici dei router della serie RV34x:

- Configurazione della connessione VPN (Virtual Private Network) da client a sito sul router serie RV34x
- Configurazione della connettività di AnyConnect Virtual Private Network (VPN) sul router serie RV34x

La VPN da client a sito non funzionerà se Port Forwarding è impostato per *All Traffic di* origine e *All Traffic di* destinazione.

Gruppi di utenti

I gruppi di utenti vengono creati sul router per un insieme di utenti che condividono lo stesso insieme di servizi. Questi gruppi di utenti includono opzioni per il gruppo, come un elenco di autorizzazioni su come possono accedere alla VPN. A seconda del dispositivo, è possibile utilizzare PPTP, VPN IPSec da sito a sito e VPN IPSec da client a sito. Ad esempio, l'RV260 offre opzioni che includono OpenVPN, ma L2TP non è supportato. La serie RV340 è dotata di AnyConnect per una VPN SSL, nonché di Captive Portal o EZ VPN.

Queste impostazioni consentono agli amministratori di controllare e filtrare in modo che solo gli utenti autorizzati possano accedere alla rete. Shrew Soft e TheGreenBow sono due dei client VPN più comuni disponibili per il download. Per stabilire correttamente un tunnel VPN, è necessario configurarli in base alle impostazioni VPN del router. L'articolo seguente riguarda in modo specifico la creazione di un gruppo di utenti:

- Creare un gruppo di utenti per la configurazione della VPN sul router RV34x

Quando si impostano i gruppi di utenti per una VPN, assicurarsi di lasciare l'account amministratore predefinito nel gruppo amministrativo e creare un nuovo account utente e gruppo di utenti per la VPN. Se si sposta l'account admin in un gruppo diverso, non sarà possibile accedere al router. Di conseguenza, è necessario eseguire di nuovo il reset di fabbrica e la configurazione per quel router, lasciando l'account di amministratore predefinito nel solo gruppo di amministratori.

Account utente

Gli account utente vengono creati sul router per consentire l'autenticazione degli utenti locali che utilizzano il database locale per diversi servizi, ad esempio PPTP, VPN Client, accesso GUI (Graphical User Interface) Web e SSLVPN (Secure Sockets Layer Virtual Private Network). In questo modo gli amministratori possono controllare e filtrare solo gli utenti autorizzati ad accedere alla rete. L'articolo seguente riguarda in modo specifico la creazione di un account utente:

- Creare un account utente per la configurazione del client VPN sul router RV34x

Da client a sito presso la sede del client

In una connessione VPN da client a sito, i client di Internet possono connettersi al server per accedere alla rete aziendale o alla LAN dietro il server, mantenendo tuttavia la sicurezza della rete e delle relative risorse. Questa funzione è molto utile perché crea un nuovo tunnel VPN che consente ai telelavoratori e agli utenti business di accedere alla rete utilizzando un software client VPN senza compromettere la privacy e la sicurezza. La VPN è configurata per crittografare e decrittografare i dati durante l'invio e la ricezione.

L'applicazione AnyConnect funziona con VPN SSL e viene utilizzata in modo specifico con i router RV34x. Non è disponibile con altre serie di router RV. A partire dalla versione 1.0.3.15, la licenza del router non è

più necessaria, ma è necessario acquistare le licenze per il lato client della VPN. Per ulteriori informazioni su Cisco AnyConnect Secure Mobility Client, fare clic qui. Per le istruzioni sull'installazione, selezionare uno dei seguenti articoli:

- Installare Cisco AnyConnect Secure Mobility Client su un computer Mac
- Installare Cisco AnyConnect Secure Mobility Client su un computer Windows

Alcune applicazioni di terze parti possono essere utilizzate per la VPN da client a sito con tutti i router della serie RV. Come accennato in precedenza, Cisco non supporta queste applicazioni; queste informazioni vengono fornite a scopo informativo.

Il client VPN GreenBow è un'applicazione client VPN di terze parti che consente a un dispositivo host di configurare una connessione protetta per il tunnel IPsec client-sito o SSL. Si tratta di un'applicazione a pagamento che include supporto.

- Configurazione e utilizzo del client VPN IPsec GreenBow per la connessione con i router RV160 e RV260

OpenVPN è un'applicazione open source gratuita che può essere configurata e utilizzata per una VPN SSL. Utilizza una connessione client-server per garantire comunicazioni protette tra un server e una posizione remota del client tramite Internet.

- OpenVPN su router RV160 e RV260

Shrew Soft è un'applicazione open source gratuita che può essere configurata e utilizzata anche per una VPN IPsec. Utilizza una connessione client-server per garantire comunicazioni protette tra un server e una posizione remota del client tramite Internet.

- Configurazione di Show Soft VPN Client con RV160 e RV260

Easy VPN è stato comunemente utilizzato sui router RV32x. Ecco alcune informazioni di riferimento:

- Configurazione di Easy Client per gateway VPN (Virtual Private Network) su RV320 e RV325 VPN Router
- Cisco Easy VPN - Domande e risposte
- Easy VPN su router basati su software Cisco IOS

Installazione guidata

I router Cisco serie RV più recenti sono dotati di una procedura guidata per la configurazione della VPN che guida l'utente attraverso i passaggi di configurazione. La Configurazione guidata VPN consente di configurare connessioni VPN di base da LAN a LAN e ad accesso remoto e di assegnare chiavi già condivise o certificati digitali per l'autenticazione. Per ulteriori informazioni, consultare i seguenti articoli:

- Configurazione guidata VPN Setup su RV160 e RV260
- Configurazione della connessione VPN (Virtual Private Network) sul router serie RV34x con la Configurazione guidata

Conclusioni

Questo articolo ti ha portato a una migliore comprensione delle VPN insieme a suggerimenti per farti arrivare. A questo punto è possibile procedere alla configurazione personalizzata. Prendetevi un po' di tempo per visualizzare i collegamenti e decidere il modo migliore per configurare una VPN sul vostro router Cisco serie RV.

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).