Novità di Cisco Business: Glossario delle apparecchiature e della rete di base

Obiettivo

L'obiettivo di questo documento è far conoscere ai principianti le apparecchiature Cisco Business (Small Business) e alcuni termini generali che è necessario conoscere. Gli argomenti includono Hardware Available, Cisco Business Terms, General Networking Terms, Cisco Tools, The Basics of Exchange Data, The Basics of an Internet Connection e Networks and How They Fit Together.

Introduzione

Stai iniziando a configurare la rete con le apparecchiature Cisco? Può essere travolgente entrare nel nuovo mondo della creazione e della manutenzione di una rete. In questo articolo vengono illustrate alcune nozioni di base. Più lo sapete, meno intimidatorio sarà!

Hardware disponibile da Cisco Business

Router

I router connettono più reti e indirizzano i dati dove è necessario. Connettono inoltre i computer di tali reti a Internet. I router consentono a tutti i computer della rete di condividere una singola connessione Internet, con un conseguente risparmio di costi.

Un router svolge la funzione di dispatcher. Analizza i dati inviati attraverso la rete, sceglie il miglior percorso per i dati da trasferire e li invia.

I router consentono di collegare l'azienda al mondo, proteggere le informazioni dalle minacce alla sicurezza e persino decidere quali computer hanno la priorità sugli altri.

Oltre a queste funzioni di rete di base, i router dispongono di funzionalità aggiuntive per rendere la rete più semplice o sicura. A seconda delle esigenze, ad esempio, è possibile scegliere un router con un firewall, una rete privata virtuale (VPN) o un sistema di comunicazione IP (Internet Protocol).

I router aziendali Cisco più recenti includono la serie RV160, RV260, RV340 e RV345.

Switch

Gli switch sono alla base della maggior parte delle reti aziendali. Uno switch funge da controller e connette computer, stampanti e server a una rete in un edificio o in un campus.

Gli switch consentono ai dispositivi della rete di comunicare tra loro e con altre reti, creando una rete di risorse condivise. Grazie alla condivisione delle informazioni e all'allocazione delle risorse, gli switch consentono di risparmiare denaro e aumentare la produttività.

Sono disponibili due tipi di switch di base tra cui scegliere: gestiti e non gestiti.

> Uno switch non gestito funziona immediatamente ma non può essere configurato. Le apparecchiature per reti domestiche in genere offrono switch non gestiti.
> Èpossibile configurare uno switch gestito. È possibile monitorare e regolare uno switch gestito in locale o in remoto, offrendo un maggiore controllo sul traffico di rete e sull'accesso.

Per ulteriori informazioni sugli switch, consultare il Glossario dei termini Switch.

Gli switch sviluppati più di recente includono Cisco Business Switch serie CBS110, CBS220, CBS250 e CBS350.

Per conoscere le differenze tra gli switch CBS, selezionare

Access Point Wireless

Un punto di accesso wireless consente ai dispositivi di connettersi alla rete senza cavi. Una rete wireless semplifica la connessione di nuovi dispositivi e offre un supporto flessibile ai lavoratori mobili.

Un punto di accesso funge da amplificatore per la rete. Mentre un router fornisce la larghezza di banda, un punto di accesso estende tale larghezza di banda in modo che la rete possa supportare molti dispositivi e che tali dispositivi possano accedere alla rete da un punto più lontano.

Ma un access point non si limita a estendere il Wi-Fi. Può inoltre fornire dati utili sui dispositivi della rete, fornire una sicurezza proattiva e servire a molti altri scopi pratici.

I punti di accesso wireless più recenti, Cisco Business Wireless, includono AC140,

AC145 e AC240, che consentono l'uso di una rete mesh wireless. Se non si ha familiarità con le reti wireless mesh, è possibile leggere ulteriori informazioni in Benvenuti in Cisco Business Wireless Mesh Networking o Domande frequenti (FAQ) per una rete wireless aziendale Cisco.

Per conoscere alcuni termini comuni ai punti di accesso wireless, consultate il glossario dei termini WAP.

Telefono multipiattaforma

I telefoni MPP forniscono comunicazioni Voice over IP (VoIP) utilizzando il protocollo SIP (Session Initiation Protocol). In questo modo si elimina la necessità di linee telefoniche tradizionali, rendendo i telefoni più portatili all'interno dell'azienda. Con il VoIP, un telefono utilizza un'infrastruttura di rete e una connessione Internet esistenti invece di costose linee T1. In questo modo è possibile gestire un numero maggiore di chiamate con un numero inferiore di "righe". Altre opzioni vantaggiose includono la messa in attesa delle chiamate, il parcheggio delle chiamate, il trasferimento delle chiamate e altro ancora. Alcuni modelli permettono la comunicazione video oltre al VoIP.

I telefoni MPP sono costruiti per assomigliare a normali telefoni e vengono utilizzati solo per questo scopo, ma essenzialmente sono un computer e fanno parte della rete. I telefoni MPP richiedono il servizio di un provider di servizi di telefonia Internet (ITSP) o di un server di controllo delle chiamate IP Private Branch Exchange (PBX). WebEx Calling, Ring Central e Verizon sono esempi di ITSP. Alcuni esempi di servizi IP PBX che funzionano con i telefoni MPP Cisco includono le piattaforme Asterisco, Centile e Metaswitch. Molte funzionalità di questi telefoni sono programmate specificamente tramite fornitori di terze parti (come FreePBX), quindi i processi (parcheggio, accesso alla segreteria telefonica, ecc.) possono variare.

I telefoni MPP Cisco Business più recenti includono la serie 6800, 7800 e 8800.

A cui si fa riferimento comunemente negli ambienti aziendali Cisco

Guida all'amministrazione e Guida introduttiva

Sono disponibili due diverse risorse in cui eseguire una ricerca per ottenere informazioni dettagliate sul prodotto e le relative caratteristiche. Quando si esegue una ricerca sul sito o sul Web con il numero di modello, è possibile aggiungere una delle due guide per visualizzare le guide più lunghe.

Impostazioni predefinite

I dispositivi vengono forniti con impostazioni predefinite preselezionate. Si tratta spesso delle impostazioni più comuni scelte da un amministratore. È possibile modificare le impostazioni in base alle proprie esigenze.

Nome utente e password predefiniti

Nelle precedenti apparecchiature Cisco Business, il valore predefinito era *admin* per nome utente e password. Ora, la maggior parte di essi ha un valore predefinito di *cisco* sia per il nome utente che per la password. Sui telefoni VoIP (Voice over IP), è necessario eseguire il login come *amministratore* per modificare molte configurazioni. Si consiglia di modificare la password per renderla più complessa ai fini della sicurezza.

Indirizzi IP predefiniti

La maggior parte delle apparecchiature Cisco è fornita con indirizzi IP predefiniti per router, switch e punti di accesso wireless. Se non si ricorda l'indirizzo IP e non si dispone di una configurazione speciale, è possibile utilizzare una graffetta aperta per premere il pulsante di ripristino sul dispositivo per almeno 10 secondi. Verranno ripristinate le impostazioni predefinite. Se lo switch o il protocollo WAP non è connesso a un router con DHCP abilitato e si è connessi direttamente allo switch o al protocollo WAP con il computer, questi sono gli indirizzi IP predefiniti.

L'indirizzo IP predefinito di un router aziendale Cisco è 192.168.1.1.
L'indirizzo IP predefinito di uno switch Cisco Business è 192.168.1.254.
L'indirizzo IP predefinito per un punto di accesso wireless (AP) per piccole imprese è 192.168.1.245. Non è disponibile alcun indirizzo IP predefinito per i nuovi punti di accesso wireless mesh.

Ripristina valori predefiniti

Èpossibile che in un determinato momento si desideri ripristinare le impostazioni predefinite di Cisco Business, dello switch o del punto di accesso wireless e iniziare da zero. Ciò si rivela utile quando si spostano le apparecchiature da una rete all'altra o come ultima risorsa quando non è possibile risolvere un problema di configurazione. Quando si ripristinano le impostazioni predefinite di fabbrica, tutte le configurazioni vengono perse.

Èpossibile eseguire il backup delle configurazioni in modo da ripristinarle dopo un ripristino di fabbrica. Per ulteriori informazioni, fare clic sui seguenti collegamenti:

- Riavviare o ripristinare le impostazioni predefinite del router serie RV34x con l'utility basata sul Web
- Backup e ripristino o sostituzione del firmware su uno switch
- Scaricare, eseguire il backup, copiare ed eliminare i file di configurazione su un punto di accesso wireless
- Gestire i file di configurazione sul punto di accesso WAP125 o WAP581

Se non si esegue il backup della configurazione, sarà necessario configurare nuovamente il dispositivo da zero in modo da avere i dettagli della connessione. La maggior parte dei modelli dispone di un articolo che descrive in dettaglio i passaggi da seguire per un ripristino, ma il modo più semplice per farlo è utilizzare una graffetta aperta e premere il pulsante di ripristino sul dispositivo per almeno 10 secondi. Questo

non si applica ai telefoni MPP, quindi per ulteriori informazioni consulta Ripristino di un telefono IP Cisco.

Interfaccia utente Web

Ogni apparecchiatura Cisco Business è dotata di un'interfaccia Web, ad eccezione degli switch non gestiti serie 100.

Questo tipo di interfaccia, quello che viene visualizzato sullo schermo, mostra le opzioni per la selezione. Non è necessario conoscere alcun comando per spostarsi attraverso queste schermate. L'interfaccia utente Web viene anche definita GUI (Graphical User Interface), interfaccia basata sul Web, guida basata sul Web, utilità basata sul Web o utilità di configurazione Web.

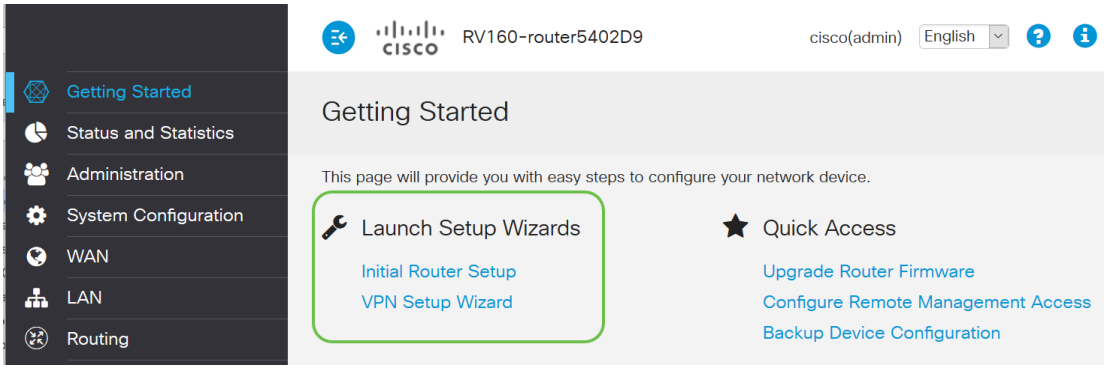
Uno dei modi più semplici per modificare la configurazione di un dispositivo è tramite l'interfaccia utente Web. L'interfaccia utente Web fornisce all'amministratore uno strumento che contiene tutte le possibili funzionalità che possono essere modificate per modificare le prestazioni di un dispositivo.

Dopo aver effettuato l'accesso a un dispositivo Cisco, verrà visualizzata una schermata dell'interfaccia utente Web che include un riquadro di navigazione in basso a sinistra. Contiene un elenco delle funzionalità di primo livello del dispositivo. Il riquadro di spostamento viene talvolta definito anche albero di spostamento, barra di spostamento o mappa di spostamento.

I colori di questa pagina possono variare, così come le funzioni di livello superiore, a seconda dell'apparecchiatura e della versione del firmware.

Installazione guidata

Questa schermata interattiva viene visualizzata quando si accede a un dispositivo Cisco Small Business per la prima volta, ed eventualmente successivamente. Può essere un ottimo modo per essere operativi sulla rete. È possibile modificare diverse impostazioni predefinite preselezionate. Alcuni dispositivi vengono forniti con più di una procedura guidata. In questo esempio vengono illustrate due procedure guidate di configurazione, *Configurazione iniziale router* e *Configurazione guidata VPN*.



Proprietario Cisco

Sviluppato e di proprietà di Cisco. Ad esempio, il protocollo CDP (Cisco Discovery

Protocol) è di proprietà di Cisco. In genere, i protocolli proprietari Cisco possono essere utilizzati solo su dispositivi Cisco.

Models in a Series

Cisco offre ai titolari di piccole imprese molti modelli diversi per soddisfare le esigenze della loro azienda. Spesso, un modello viene offerto con diverse funzioni, numero di porte, Power over Ethernet o anche wireless. Se una serie contiene più modelli, Cisco sostituirà con una x il numero o la lettera che varia a seconda del modello, ma le informazioni si applicano a tutti i modelli della serie. Ad esempio, i router RV340 e RV345 sono compatibili con la serie RV34x. Se un dispositivo ha una P all'estremità, offre Power over Ethernet. Se il nome di un dispositivo termina in W, offre funzionalità wireless. In generale, più alto è il numero del modello, maggiori saranno le funzionalità del dispositivo. Per visualizzare i dettagli, leggere i seguenti articoli:

- Anello decoder prodotto - Router
- Decoder Product ID - Switch
- Anello decoder prodotto - WAP
- Cisco Business Wireless Model Decoder (Mesh Wireless)

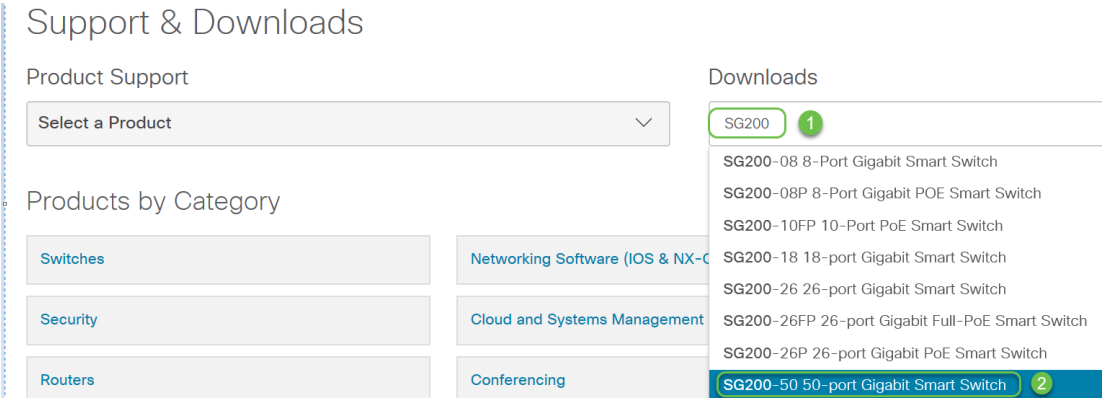
Firmware

Noto anche come immagine. Programma che controlla il funzionamento e la funzionalità del dispositivo.

Aggiorna firmware

L'aggiornamento del firmware è essenziale per ottimizzare le prestazioni di ogni dispositivo. È molto importante installare gli aggiornamenti quando vengono rilasciati. Quando Cisco rilascia un aggiornamento del firmware, spesso contiene miglioramenti come nuove funzionalità o corregge un bug che può causare una vulnerabilità della sicurezza o un problema di prestazioni.

Andare al supporto Cisco e immettere il nome del dispositivo che deve essere aggiornato in *Download*. Viene visualizzato un menu a discesa. Scorrere verso il basso e scegliere il modello specifico che si possiede.



Suggerimento: se si esaminano diverse versioni del firmware Cisco, ognuna segue un formato x.x.x.x. che sono considerati quattro ottetti. In caso di aggiornamento

secondario, il quarto ottetto viene modificato. Il terzo ottetto cambia quando è un cambiamento più grande. Il secondo ottetto rappresenta un cambiamento importante. Il primo ottetto cambia se si tratta di una revisione completa.

Per ulteriori informazioni, fare clic su questo collegamento per scaricare e aggiornare il firmware su qualsiasi dispositivo.

In questo articolo vengono fornite alcune idee per la risoluzione dei problemi in caso di problemi con l'aggiornamento dello switch: aggiornare il firmware su uno switch serie 200/300.

Condizioni generali di rete

Una volta installata l'apparecchiatura, è necessario acquisire familiarità con alcuni termini comuni relativi alle reti.

Interfaccia

Un'interfaccia è in genere rappresentata dallo spazio tra un sistema e l'altro. Qualsiasi cosa possa comunicare con il computer, incluse le porte. A un'interfaccia di rete in genere viene assegnato un indirizzo IP locale. Un'interfaccia utente consente all'utente di interagire con il sistema operativo.

Nodo

Termine generico che descrive qualsiasi dispositivo che stabilisce una connessione o un'interazione all'interno di una rete o che è in grado di inviare, ricevere e archiviare informazioni, comunicare con Internet e disporre di un indirizzo IP.

Host

Un host è un dispositivo che rappresenta un endpoint per le comunicazioni in una rete, l'host può fornire dati o un servizio (come DNS) ad altri nodi. A seconda della topologia, uno switch o un router può essere un host. Tutti gli host sono anche nodi. Gli esempi includono un computer, un server o una stampante.

Programma

Un programma contiene istruzioni che possono essere eseguite su un computer.

Applicazione

Il software applicativo è un programma che consente di eseguire attività. Spesso vengono indicati in modo intercambiabile in quanto sono simili, ma non tutti i programmi sono applicazioni.

Procedure ottimali

Metodo consigliato per l'installazione e l'esecuzione della rete.

Topologia

Modalità fisica di connessione delle apparecchiature. Mappa della rete.

Configurazione

Si riferisce alla configurazione. È possibile lasciare invariate le impostazioni predefinite, quelle che vengono preconfigurate al momento dell'acquisto delle apparecchiature, oppure configurare in base alle proprie esigenze. Le impostazioni predefinite sono le configurazioni di base, spesso consigliate. Quando si accede al dispositivo, è possibile che sia disponibile una procedura guidata che consente di eseguire in modo semplificato le operazioni necessarie.

Indirizzo MAC

Identificatore univoco per ogni dispositivo. Si trova sul dispositivo fisico e può essere rilevato con Bonjour, LLDP o CDP. Uno switch tiene traccia degli indirizzi MAC sui dispositivi man mano che interagisce con essi e crea una tabella di indirizzi MAC. In questo modo lo switch può sapere a chi indirizzare i pacchetti di informazioni.

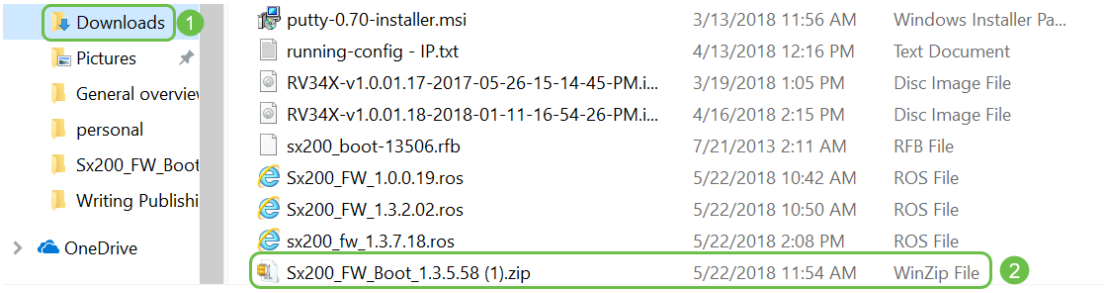
Apri origine

Programma disponibile gratuitamente per il pubblico.

File Zip

Gruppo di file compressi in un file zip. Viene utilizzato quando si desidera trasferire più file in un unico passaggio. Il ricevitore può aprire il file zip e accedere a ciascuno separatamente. Un file zip termina con *.zip*.

Se viene visualizzato un file in un formato che termina con *.zip*, è necessario decomprimerlo. Se non si dispone di un programma di decompressione, è necessario scaricarne uno. Ci sono diverse opzioni gratuite online. Dopo aver scaricato un programma di decompressione, fare clic su **Download** e individuare il file *.zip* da decomprimere.



Fare clic con il pulsante destro del mouse sul nome del file zip; verrà visualizzata una schermata simile a questa. Posizionare il puntatore del mouse sul software di decompressione e scegliere **Estrai qui**. Nell'esempio, viene usato 7-Zip.

CLI (Command Line Interface)

CLI (Command Line Interface): A volte indicato come terminale. Questa opzione viene utilizzata come ulteriore opzione per la scelta delle configurazioni su dispositivi quali router e switch. Se siete esperti, questo può essere un modo molto più semplice per ottenere le impostazioni, dal momento che non dovreste navigare attraverso varie schermate di interfaccia Web. Il problema è che è necessario conoscere i comandi e immetterli perfettamente. Dal momento che stai leggendo un articolo per principianti, CLI probabilmente non dovrebbe essere la tua prima scelta.

Macchina virtuale

La maggior parte dei computer dispone di funzionalità superiori a quelle necessarie. È possibile effettuare il provisioning di un computer per contenere tutto il necessario per eseguire più computer. Il problema è che se una parte va in tilt o ha bisogno di un riavvio, lo seguono tutti.

Se si installa VMware o Hyper-V, è possibile caricare software, server Web, server di posta elettronica, FindIT e altro su un unico computer. Una macchina virtuale può persino utilizzare un sistema operativo diverso. Sono logicamente indipendenti l'uno dall'altro. Ognuno esegue le funzioni di un dispositivo separato senza esserne effettivamente uno. Sebbene l'hardware sia condiviso, ogni macchina virtuale alloca una parte del ricorso fisico per ogni sistema operativo. Ciò consente di risparmiare denaro, energia e spazio.

Strumenti Cisco che potresti usare

Cisco Business Dashboard (CBD)

Questo è uno strumento Cisco usato per monitorare e mantenere le reti. Il CBD consente di identificare i dispositivi Cisco della rete e altre utili funzionalità di gestione.

Si tratta di uno strumento utile se si eseguono le attività da casa o se si supervisiona più di una rete. CBD può essere eseguito su una macchina virtuale. Per ulteriori informazioni su CBD, visitare il sito del supporto per Cisco Business Dashboard o la panoramica di Cisco Business Dashboard.

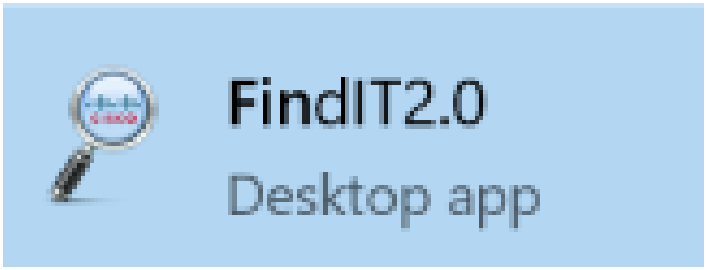
FindIT Network Discovery Utility

Questo semplice strumento è molto semplice, ma può aiutarti a trovare rapidamente le apparecchiature Cisco sulla tua rete. Cisco FindIT individua automaticamente tutti i dispositivi Cisco per piccole imprese supportati nello stesso segmento di rete locale del PC.

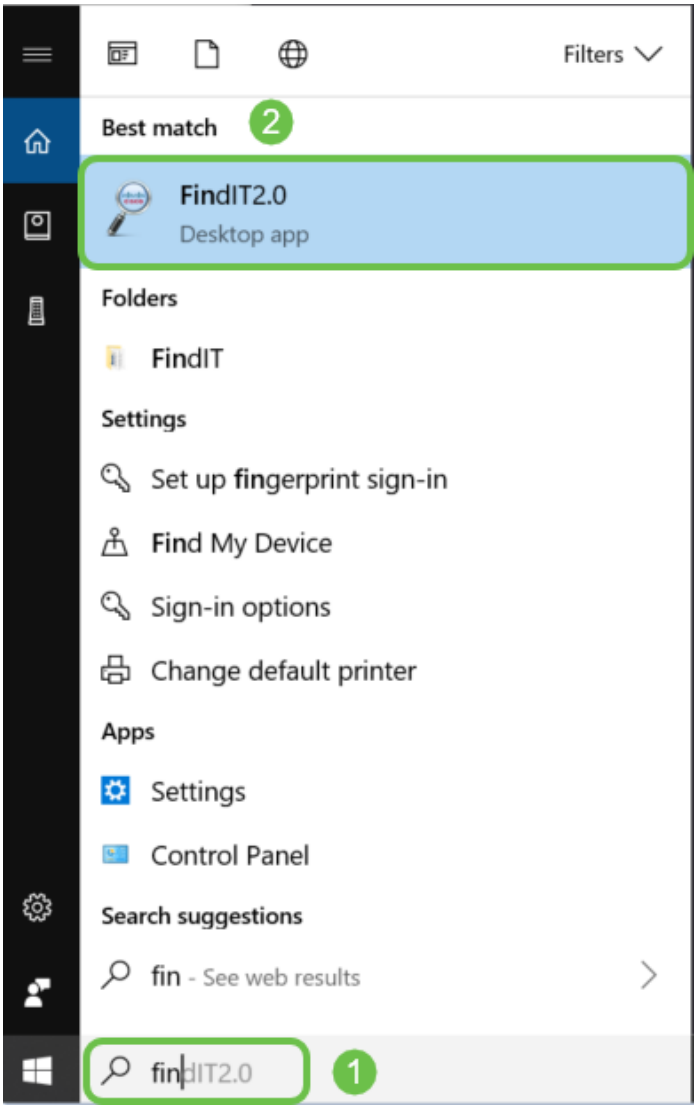
Fare clic per ulteriori informazioni e per scaricare Cisco Small Business FindIT Network Discovery Utility.

Fare clic su questo collegamento per leggere un articolo su Come installare e configurare Cisco FindIT Network Discovery Utility.

L'aspetto dell'applicazione è analogo a quello di Windows 10.



Una volta scaricato, è possibile trovarlo qui in Windows 10.



AnyConnect (serie RV34x router/VPN)

Questa VPN è utilizzata specificamente con i router serie RV34x (e con apparecchiature di grandi aziende/aziende). Cisco AnyConnect Secure Mobility Client offre agli utenti remoti una connessione VPN sicura. Offre agli utenti finali remoti i vantaggi di un client VPN Cisco Secure Sockets Layer (SSL) e supporta anche applicazioni e funzioni non disponibili su una connessione VPN SSL basata su browser. Comunemente utilizzata da utenti remoti, AnyConnect consente di connettersi all'infrastruttura informatica aziendale come se si trovassero fisicamente in ufficio, anche se non lo sono. Ciò aumenta la flessibilità, la mobilità e la produttività dei lavoratori. Per usare AnyConnect, sono necessarie licenze client. Cisco AnyConnect è compatibile con i seguenti sistemi operativi: Windows 7, 8, 8.1 e 10, Mac OS X 10.8 e versioni successive e Linux Intel (x64).

Per ulteriori informazioni, fare riferimento ai seguenti articoli:

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

Nozioni di base sullo scambio di dati

Pacchetto

Nelle reti, le informazioni vengono inviate in blocchi, detti pacchetti. In caso di problemi di connessione, i pacchetti possono andare persi.

Latenza

Ritardi nel trasferimento dei pacchetti.

Ridondanza

In una rete, la ridondanza è configurata in modo che se una parte della rete presenta problemi, l'intera rete non viene interrotta. Consideralo un piano di backup se succede qualcosa alla configurazione principale.

Protocolli

Due dispositivi devono avere alcune delle stesse impostazioni per comunicare. Pensatela come una lingua. Se una persona parla solo il tedesco e l'altra solo lo spagnolo, non sarà in grado di comunicare. Protocolli diversi interagiscono tra loro e possono esistere più protocolli trasmessi l'uno all'altro. I protocolli hanno scopi diversi; di seguito sono elencati e descritti brevemente alcuni esempi.

Protocolli di indirizzamento

- **Session Initiation Protocol (SIP):** è il protocollo principale per i telefoni VoIP (Voice over IP) che comunicano tramite Internet. Entrambi i lati della rete devono essere configurati utilizzando lo stesso protocollo per comunicare in modo che entrambi abbiano bisogno del SIP per avviare la comunicazione su VoIP.
- **Il protocollo DHCP (Dynamic Host Configuration Protocol)** gestisce un pool di indirizzi IP disponibili, assegnandoli agli host quando si uniscono alla rete.
- **Protocollo** ARP (**Address Resolution Protocol**): esegue il mapping di un indirizzo IP dinamico a un indirizzo MAC fisico permanente in una LAN.
- **IPv4:** questa è la versione più comune di IP usata attualmente. Un indirizzo IP viene scritto come 4 set di numeri (detti anche ottetti) separati da un punto tra ogni set. Ogni set può essere un numero compreso tra 0 e 255. Un esempio di indirizzo IPv4 è 8.8.8.8, che è il server DNS pubblico di Google. Poiché il numero di dispositivi disponibili è superiore a quello degli indirizzi IP univoci, l'acquisto di un indirizzo IP pubblico permanente può comportare costi elevati.
- **IPv6:** nell'ultima versione vengono utilizzati 8 set di numeri separati da due punti. Poiché utilizza un sistema numerico esadecimale, è possibile che l'indirizzo IP contenga lettere. Un'azienda può avere indirizzi IPv4 e IPv6 in esecuzione contemporaneamente.

Poiché si parla di IPv6, di seguito sono riportati alcuni dettagli importanti da conoscere per questo protocollo di indirizzamento:

Abbreviazioni IPv6: se tutti i numeri in più set sono zero, due punti in una riga possono

rappresentare tali set, questa abbreviazione può essere utilizzata solo una volta. Ad esempio, uno degli indirizzi IPv6 di Google è 2001:4860:4860::8888. Alcuni dispositivi utilizzano campi separati per tutte le otto parti degli indirizzi IPv6 e non possono accettare l'abbreviazione IPv6. In questo caso, è necessario digitare 2001:4860:4860:0:0:0:8888.

Esadecimale: un sistema numerico che usa una base 16 invece della base 10, che è ciò che usiamo nella matematica di tutti i giorni. I numeri da 0 a 9 sono rappresentati nello stesso modo. 10-15 sono rappresentate dalle lettere A-F.

Protocolli di trasferimento dati

- **Transmission Control Protocol (TCP) e User Datagram Protocol (UDP):** sono due modalità di trasporto dei dati. Il protocollo TCP richiede una connessione, chiamata handshake a tre vie, prima dell'invio dei dati, pertanto a volte si verifica un ritardo. In caso di perdita di dati (pacchetti), questi verranno nuovamente inviati. UDP è meno affidabile, ma più veloce. Spesso, voce e video utilizzano UDP.
- **FTP (File Transfer Protocol):** questo protocollo viene utilizzato per trasferire file da un client a un server.
- **HTTP (Hypertext Transfer Protocol) e HTTPS (Hypertext Transfer Protocol Secure):** base generale per la comunicazione dei dati su Internet. Queste informazioni sono disponibili all'inizio dei siti Web, scritti come *http://* e *https://*. I siti che iniziano con *https://* sono più sicuri da utilizzare.
- **RIP (Routing Information Protocol):** questo protocollo è in uso da molto tempo. Sono disponibili tre versioni, ognuna delle quali aggiunge maggiore sicurezza e funzionalità. I router condividono i percorsi. L'obiettivo è quello di prevenire i loop impostando un numero massimo di "hop" da un router all'altro. Altri protocolli più efficienti per il routing includono **Enhanced Interior Gateway Routing Protocol (EIGRP)**, **Open Shortest Path First (OSPF)** e **Intermediate System to Intermediate System (IS-IS)**. Queste ultime tre scalano meglio di RIP ma possono essere più complicate da impostare.
- **Secure Shell (SSH):** canale sicuro che fornisce una route sicura per il traffico della riga di comando. Protocollo crittografato utilizzato per comunicare con un server remoto. Molte tecnologie aggiuntive sono basate sul protocollo SSH.

Protocolli di rilevamento

- **Cisco Discovery Protocol (CDP):** rileva le informazioni su altre apparecchiature Cisco direttamente connesse e le salva. **Bonjour** e **Link Layer Discovery Protocol (LLDP)** eseguono le stesse funzioni e possono ottenere informazioni anche su dispositivi non Cisco. La maggior parte dei dispositivi per piccole imprese utilizza LLDP.
- **LLDP (Layer Link Discovery Protocol):** Consente a un dispositivo di annunciare la propria identificazione, configurazione e funzionalità ai dispositivi adiacenti che archiviano i dati in un MIB (Management Information Base). Le informazioni condivise tra i vicini consentono di ridurre il tempo necessario per aggiungere un nuovo dispositivo alla LAN (Local Area Network) e forniscono inoltre i dettagli necessari per risolvere molti problemi di configurazione. LLDP può essere utilizzato in scenari in cui è necessario lavorare tra dispositivi che non sono proprietari Cisco e dispositivi che sono proprietari Cisco. Lo switch fornisce tutte le informazioni sullo stato LLDP corrente delle porte e può

essere utilizzato per risolvere i problemi di connettività all'interno della rete. Questo è uno dei protocolli utilizzati dalle applicazioni di individuazione della rete, ad esempio FindIT Network Management, per individuare i dispositivi nella rete.

Identificazione dei protocolli

- **DNS (Domain Name System):** una volta assegnato un nome di dominio completo (FQDN) a un indirizzo IP, questo viene inserito in un database. Ad esempio, quando si esegue una ricerca in *www.google.com*, è possibile immettere il nome del sito Web e il database eseguirà la ricerca e sarà possibile ottenere il nome tramite il relativo indirizzo IP. Il **provider di servizi Internet (ISP)** utilizza il server DNS predefinito ed è già stato configurato. È tuttavia possibile modificare manualmente questa impostazione se si riscontrano velocità ridotte durante l'utilizzo di Internet.
- **DNS dinamico:** denominato anche DNS, aggiorna automaticamente un server nel DNS con la configurazione attiva dei relativi nomi host, indirizzi o altre informazioni pertinenti. In altre parole, il DNS assegna un nome di dominio fisso a un indirizzo IP WAN dinamico. Questo permette di risparmiare sui costi di acquisto di un indirizzo IP permanente.
- **Protocollo Internet (IP):** gli indirizzi IP sono identificatori univoci che consentono l'invio e la ricezione di dati tra host su Internet. Ciò avviene tramite indirizzi Internet pubblici, che richiedono l'acquisto da un ISP.
- **Media Access Control (indirizzo MAC):** a ciascun dispositivo è collegato un identificatore univoco. La situazione non cambia. È consigliabile conoscere l'indirizzo MAC durante la configurazione della rete e la risoluzione dei problemi. In genere si trova sul dispositivo e contiene lettere e numeri. Gli switch tengono traccia degli indirizzi MAC dei dispositivi e creano una tabella di indirizzi MAC.

Protocolli di risoluzione dei problemi

- **Ping:** il ping è un metodo comune per la risoluzione dei problemi. Un ping invia messaggi echo ICMP a un indirizzo IP. Viene ricevuto un messaggio in risposta. Una risposta corretta indica una connettività fisica bidirezionale. È un modo per verificare se un pacchetto dati di rete può essere distribuito a un indirizzo senza problemi.
- **Protocollo ICMP (Internet Control Message Protocol):** messaggi relativi a errori e informazioni operative. Quando si esegue un test PING, viene inviato un messaggio echo ICMP alla destinazione. Una connessione riuscita ottiene una risposta dal dispositivo.

Server

Computer o programma in un computer che fornisce servizi ad altri computer. Un server può essere virtuale o anche un'applicazione. Su un dispositivo possono essere presenti più server. I server possono condividere tra loro. Possono essere utilizzati con Windows, Mac o Linux.

Server Web - formattazione e presentazione di pagine Web per browser Web
File server: condividere file e cartelle con gli utenti di una rete
Server di posta elettronica - invio, ricezione e archiviazione di messaggi di posta

elettronica
Server DNS: per convertire nomi descrittivi come www.cisco.com nell'indirizzo IP 173.37.145.84, ad esempio
Server di messaggistica istantanea - controlla il flusso e gestisce i messaggi istantanei (Jabber, Skype)

QoS (Quality of Service)

Queste impostazioni sono configurate in modo da assicurare che venga data priorità al traffico in rete, generalmente voce o video, in quanto è spesso la più evidente in caso di ritardo dei pacchetti (dati).

Nozioni di base sulla connessione Internet

ISP (Internet Service Provider)

Per accedere a Internet sulla rete è necessario disporre di un ISP. Sono disponibili numerose opzioni tra cui scegliere per le velocità di connessione e una varietà di prezzi per soddisfare le esigenze della vostra azienda. Oltre all'accesso a Internet, un ISP offre servizi di hosting di e-mail, pagine Web e altro ancora.

Browser Web

Applicazione inclusa nel dispositivo. Puoi scaricarne altri. Una volta scaricato, è possibile aprire e immettere l'indirizzo IP o il sito Web a cui si desidera accedere tramite Internet. Alcuni esempi di browser Web sono:

Microsoft Edge

 ,

Cromatura

 ,

Firefox

 ,

e Safari.

Se non si riesce ad aprire qualcosa o si verificano altri problemi di navigazione, provare ad aprire un browser Web diverso e riprovare.

URL (Uniform Resource Locator)

In un browser, in genere si digita il nome del sito Web a cui si desidera accedere, ovvero l'URL e l'indirizzo Web. Ogni URL deve essere univoco. Un esempio di URL è https://www.cisco.com.

Gateway predefinito

Questo è il router usato dal traffico della rete locale (LAN) per comunicare con il provider di servizi Internet (ISP) e Internet. In altre parole, il router si connette ad altri dispositivi esterni all'edificio e tramite Internet.

Firewall

Un firewall è un dispositivo di sicurezza di rete che controlla il traffico di rete in entrata e in uscita e decide se consentire o bloccare il traffico specifico in base a un insieme definito di regole di sicurezza, denominate Access Control Lists (ACL).

I firewall sono stati la prima linea di difesa nella sicurezza della rete per decenni. Esse creano una barriera tra reti interne protette e controllate che possono essere considerate attendibili e non attendibili all'esterno delle reti, ad esempio Internet.

Un firewall può essere costituito da hardware, software o entrambi.

Per ulteriori informazioni, consultare il documento sulla configurazione delle impostazioni base del firewall sui router serie RV34x.

Access Control Lists (ACLs)

Elenchi che bloccano o consentono l'invio di traffico da e verso determinati utenti. È possibile configurare le regole di accesso in modo che siano sempre attive o basate su una pianificazione definita. Una regola di accesso viene configurata in base a diversi criteri per consentire o negare l'accesso alla rete. La regola di accesso viene pianificata in base all'ora in cui le regole di accesso devono essere applicate al router. Tali impostazioni vengono configurate nelle impostazioni di protezione o del firewall. Ad esempio, un'azienda potrebbe voler impedire ai dipendenti di trasmettere eventi sportivi live o di connettersi a Facebook durante l'orario di lavoro.

Larghezza di banda

Quantità di dati che è possibile inviare da un punto all'altro in un determinato periodo di tempo. Se si dispone di una connessione Internet con una larghezza di banda maggiore, la rete può spostare i dati molto più velocemente rispetto a una connessione Internet con una larghezza di banda inferiore. Lo streaming video richiede molta più larghezza di banda rispetto all'invio di file. Se si riscontra un ritardo nell'accesso a una pagina Web o nel flusso di video, potrebbe essere necessario aumentare la larghezza di banda della rete.

Cavo Ethernet

La maggior parte dei dispositivi di una rete dispone di porte Ethernet. I cavi Ethernet sono la spina che li collega per una connessione cablata. Entrambe le estremità del cavo RJ45 sono identiche e hanno l'aspetto delle vecchie prese telefoniche. Possono essere utilizzati per collegare dispositivi e per connettersi a Internet. I cavi collegano le periferiche per l'accesso a Internet e la condivisione dei file. Alcuni computer richiedono una scheda Ethernet, in quanto potrebbero non fornire una porta Ethernet.

Reti e loro integrazione

LAN (Local Area Network)

Una rete che può essere grande come diversi edifici o piccola come una casa. Tutti gli utenti connessi alla LAN si trovano nella stessa posizione fisica e sono connessi allo stesso router.

In una rete locale, a ciascun dispositivo viene assegnato un indirizzo IP interno univoco. Seguono un modello 10.x.x.x, 172.16.x.x - 172.31.x.x o 192.168.x.x. Questi indirizzi sono visibili solo all'interno di una rete, tra dispositivi e sono considerati privati. Milioni di località possono avere lo stesso pool di indirizzi IP interni dell'azienda. Non importa, sono usate solo all'interno della loro rete privata, quindi non ci sono conflitti. Affinché i dispositivi della rete possano comunicare tra loro, devono tutti seguire lo stesso schema degli altri dispositivi, trovarsi nella stessa subnet ed essere univoci. Questi indirizzi non devono mai essere visualizzati in questo schema come indirizzi IP pubblici, in quanto sono riservati solo agli indirizzi LAN privati.

Tutti questi dispositivi inviano dati tramite un gateway predefinito (un router) per accedere a Internet. Quando il gateway predefinito riceve le informazioni, deve eseguire Network Address Translation (NAT) e modificare l'indirizzo IP, in quanto qualsiasi elemento che circola su Internet richiede un indirizzo IP univoco.

WAN (Wide Area Network)

Una rete WAN (Wide Area Network) è una rete distribuita, a volte globalmente. Molte LAN possono connettersi a una singola WAN.

Solo gli indirizzi WAN possono comunicare tra loro attraverso Internet. Ogni indirizzo WAN deve essere univoco. Affinché i dispositivi all'interno di una rete siano in grado di inviare e ricevere informazioni su Internet, è necessario disporre di un router al

margine della rete (un gateway predefinito) in grado di eseguire NAT.

Fare clic per leggere Configurare le regole di accesso su un router serie RV34x.

NAT (Network Address Translation)

Un router riceve un indirizzo WAN tramite un provider di servizi Internet (ISP). Il router è dotato di funzionalità NAT che trasferisce il traffico in uscita dalla rete, converte l'indirizzo privato nell'indirizzo WAN pubblico e lo invia tramite Internet. Fa l'inverso quando riceve il traffico. Questa opzione è stata configurata perché non vi sono sufficienti indirizzi IPv4 permanenti disponibili per tutti i dispositivi nel mondo.

Il vantaggio di NAT è che fornisce una sicurezza aggiuntiva nascondendo l'intera rete interna dietro quell'unico indirizzo IP pubblico. Gli indirizzi IP interni spesso rimangono invariati, ma se vengono scollegati per un certo periodo di tempo, configurati in un certo modo o ripristinati i valori predefiniti, potrebbero non esserlo.

NAT statico

Èpossibile configurare l'indirizzo IP interno in modo che rimanga invariato configurando il protocollo DHCP (Dynamic Host Configuration Protocol) statico sul router. Non è garantito che gli indirizzi IP pubblici rimangano gli stessi, a meno che non si paghi per avere un indirizzo IP pubblico statico tramite l'ISP. Molte aziende pagano per questo servizio in modo che i dipendenti e i clienti abbiano una connessione più affidabile ai loro server (Web, posta, VPN, ecc.), ma può essere costoso.

Il protocollo NAT statico esegue il mapping di una conversione uno-a-uno degli indirizzi IP privati agli indirizzi IP pubblici. Crea una traduzione fissa degli indirizzi privati negli indirizzi pubblici. Ciò significa che sarà necessario un numero di indirizzi pubblici uguale a quello degli indirizzi privati. Ciò è utile quando un dispositivo deve essere accessibile dall'esterno della rete.

Fare clic per leggere Configurazione di NAT e NAT statico su RV160 e RV260.

CGNAT

Il protocollo NAT di livello carrier è simile e consente a più client di utilizzare lo stesso indirizzo IP.

VLAN

Una LAN virtuale o VLAN (Virtual Local Area Network) consente di segmentare logicamente una LAN (Local Area Network) in più domini di broadcast. Quando sulla rete vengono trasmessi anche dati sensibili, la creazione di VLAN offre una maggiore sicurezza e il traffico viene quindi indirizzato a VLAN specifiche. Solo gli utenti che appartengono alla VLAN possono accedere e modificare i dati trasmessi su tale rete. L'uso delle VLAN inoltre può migliorare le prestazioni in quanto riduce la necessità di inviare pacchetti broadcast e multicast a destinazioni non necessarie.

Una VLAN viene usata principalmente per formare gruppi tra gli host, indipendentemente dalla loro posizione fisica. Pertanto, una VLAN migliora la sicurezza con l'aiuto della formazione del gruppo tra gli host. La creazione di una VLAN non ha alcun effetto finché la VLAN non è collegata manualmente o dinamicamente ad almeno una porta. Una delle ragioni più comuni per configurare una VLAN è quella di configurare una VLAN separata per la voce e una VLAN separata per i dati. In questo modo, i pacchetti vengono indirizzati per entrambi i tipi di dati nonostante si utilizzi la stessa rete.

Per ulteriori informazioni, consultare il documento sulle best practice e i suggerimenti sulla sicurezza delle VLAN per i router aziendali Cisco.

Sottorete

Le subnet sono spesso reti indipendenti all'interno di una rete IP.

SSID

SSID (Service Set Identifier) è un identificatore univoco che i client wireless possono connettere o condividere tra tutti i dispositivi di una rete wireless. Fa distinzione tra maiuscole e minuscole e non deve superare i 32 caratteri alfanumerici. Questo nome è anche denominato Nome rete wireless.

VPN (Virtual Private Network)

La tecnologia si è evoluta e le attività aziendali vengono spesso condotte all'esterno dell'ufficio. I dispositivi sono più mobili e i dipendenti spesso lavorano da casa o in viaggio. Ciò può causare alcune vulnerabilità della sicurezza. Una rete VPN (Virtual Private Network) è un ottimo modo per connettere in modo sicuro i dipendenti remoti di una rete. Una VPN consente a un host remoto di agire come se si trovasse sulla stessa rete locale.

Una VPN è configurata per fornire una trasmissione dati sicura. Ci sono diverse opzioni per configurare una VPN e il modo in cui i dati vengono crittografati. Le VPN utilizzano SSL (Secure Sockets Layer), PPTP (Point to Point Tunneling Protocol) e protocollo di tunneling di livello due.

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 e l'autenticazione. Le filiali utilizzano principalmente 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.

Èpossibile configurare una connessione VPN tra il router e un endpoint dopo che il

router è stato configurato per una connessione Internet. Il client VPN dipende interamente dalle impostazioni del router VPN per poter stabilire una connessione.

Una VPN supporta la VPN da sito a sito per un tunnel da gateway a gateway. Ad esempio, un utente può configurare un tunnel VPN in una succursale per connettersi al router di una sede aziendale, in modo che la succursale possa accedere in modo sicuro alla rete aziendale. In una connessione VPN da sito a sito chiunque può avviare la comunicazione. Questa configurazione ha una connessione crittografata costante.

La VPN IPsec supporta anche la VPN da client a server per un tunnel da host a gateway. La VPN da client a server è utile per la connessione da notebook/PC a una rete aziendale tramite il server VPN. In questo caso, solo il client può avviare la connessione.

Fare clic per leggere la panoramica di Cisco Business VPN e le best practice.

Certificati

Un passaggio sicuro nella configurazione di una VPN consiste nel ottenere un certificato da un'Autorità di certificazione (CA). Utilizzato per l'autenticazione. I certificati possono essere acquistati da diversi siti di terze parti. 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, il certificato verrà rilasciato 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.

I client in genere non necessitano di un certificato per utilizzare una VPN; la verifica viene effettuata solo tramite il router. Un'eccezione è OpenVPN, che richiede un certificato client.

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

Alcuni articoli su questo argomento che potrebbero interessarti:

- 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
- Gestione dei certificati sui router serie RV34x

Chiave già condivisa (PSK)

Si tratta di una password condivisa, decisa e condivisa prima della configurazione di una VPN e può essere utilizzata come alternativa per l'utilizzo di un certificato. Un PSK

può essere qualsiasi cosa si voglia che sia, deve semplicemente corrispondere al 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

Frequenza con cui il sistema modifica la chiave. Questa impostazione deve essere uguale a quella del router remoto.

Conclusioni

Ecco, ora avete molte delle basi per farvi arrivare.

Se desideri continuare ad apprendere di più, controlla questi collegamenti.

Procedure consigliate per l'impostazione di indirizzi IP statici Panoramica e best practice di Cisco Business VPN Best practice per VLAN e suggerimenti per la sicurezza sui router Cisco Business Backup su Internet - Windows Backup su Internet - Mac Come accedere a uno switch