Funzionamento delle reti private virtuali

Sommario

Introduzione

Questo documento descrive i fondamenti delle VPN, come i componenti VPN di base, le tecnologie, il tunneling e la sicurezza VPN.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

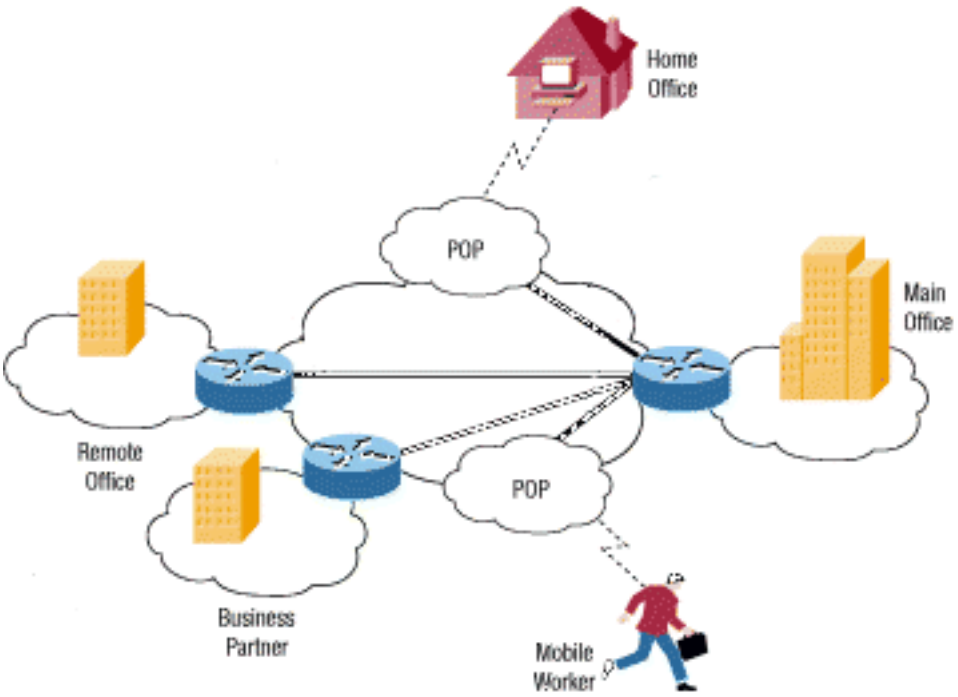
Premesse

Il mondo è cambiato molto negli ultimi due decenni. Anziché limitarsi ad affrontare le preoccupazioni locali o regionali, molte imprese devono ora pensare ai mercati globali e alla logistica. Molte aziende hanno sedi sparse in tutto il paese, o anche in tutto il mondo. Ma c'è una cosa di cui tutte le aziende hanno bisogno: un modo per mantenere comunicazioni veloci, sicure e

affidabili ovunque si trovino gli uffici.

Fino a poco tempo fa, comunicare in modo affidabile significava usare linee affittate per mantenere una rete WAN (Wide Area Network). Le linee affittate, che spaziano da ISDN (Integrated Services Digital Network) con velocità di trasmissione di 144 Kbps a OC3 (Optical Carrier-3) con velocità di trasmissione di 155 Mbps, offrono a un'azienda un modo per espandere la propria rete privata al di là della propria area geografica. Una rete WAN presenta vantaggi evidenti rispetto a una rete pubblica come Internet in termini di affidabilità, prestazioni e sicurezza; ma mantenere una WAN, in particolare quando si utilizzano linee affittate, può diventare piuttosto costoso (spesso aumenta in termini di costi con l'aumentare della distanza tra gli uffici). Inoltre, le linee affittate non rappresentano una soluzione praticabile per le organizzazioni in cui una parte della forza lavoro è altamente mobile (come nel caso dello staff di marketing) e spesso deve connettersi alla rete aziendale in remoto e accedere ai dati riservati.

Con l'aumento della popolarità di Internet, le aziende vi hanno fatto ricorso come mezzo per estendere le proprie reti. Le intranet sono state create inizialmente per essere utilizzate esclusivamente dai dipendenti dell'azienda. Molte aziende creano ora reti VPN (Virtual Private Network) per soddisfare le esigenze di dipendenti e uffici remoti.



Una VPN tipica può avere una LAN (Local-Area Network) principale presso la sede centrale di un'azienda, altre LAN presso uffici o strutture remote e singoli utenti che si connettono da fuori sul campo.

Una VPN è una rete privata che utilizza una rete pubblica, in genere Internet, per connettere utenti o siti remoti. Anziché utilizzare una connessione dedicata e reale, come una linea in leasing, una VPN utilizza connessioni "virtuali" instradate attraverso Internet dalla rete privata della società al sito o dipendente remoto.

Cosa rende una VPN?

Sono disponibili due tipi di VPN comuni.

- **Accesso remoto**: chiamata anche VPDN (Virtual Private Dial-up Network), è una connessione utente-LAN utilizzata da un'azienda con dipendenti che devono connettersi alla rete privata da varie postazioni remote. In genere, un'azienda che desidera configurare una VPN ad accesso remoto di grandi dimensioni fornisce una forma di account di accesso remoto ai propri utenti tramite un provider di servizi Internet (ISP). I telelavoratori possono quindi comporre un numero da 1 a 800 per raggiungere Internet e utilizzare il software client VPN per accedere alla rete aziendale. Un buon esempio di azienda che necessita di una VPN ad accesso remoto potrebbe essere una grande azienda con centinaia di addetti alle vendite sul campo. Le VPN ad accesso remoto consentono connessioni protette e crittografate tra la rete privata di un'azienda e gli utenti remoti tramite un provider di servizi di terze parti.
- **Da sito a sito**: utilizzando apparecchiature dedicate e la crittografia su larga scala, un'azienda può connettere più siti fissi tramite una rete pubblica, ad esempio Internet. Ogni sito ha bisogno solo di una connessione locale alla stessa rete pubblica, così risparmiando denaro su lunghe linee affittate private. Le VPN da sito a sito possono essere ulteriormente suddivise in Intranet o Extranet. Una VPN da sito a sito creata tra gli uffici della stessa azienda viene definita VPN Intranet, mentre una VPN creata per connettere l'azienda al partner o al cliente viene definita VPN Extranet.

Una VPN ben progettata può offrire grandi vantaggi a un'azienda. Può ad esempio:

- Estensione della connettività geografica
- Riduzione dei costi operativi rispetto alle tradizionali WAN
- Riduzione dei tempi di transito e dei costi di trasferimento per gli utenti remoti
- Migliorare la produttività
- Semplificazione della topologia di rete
- Opportunità di networking globali
- Supporto per i telelavoratori
- Rapido ritorno sugli investimenti (ROI) rispetto alla WAN tradizionale

Quali funzionalità sono necessarie in una VPN ben progettata? Dovrebbe includere i seguenti elementi:

- Sicurezza
- Affidabilità
- Scalabilità
- Gestione della rete
- Gestione delle policy

Analogia: Ogni LAN è una IsLANd

Immaginate di vivere su un'isola in un enorme oceano. Ci sono migliaia di altre isole intorno a voi, alcune molto vicine ed altre più lontane. Il modo normale di viaggiare è prendere un traghetto dalla vostra isola a qualsiasi isola si desidera visitare. Viaggiare su un traghetto significa che non avete quasi nessuna privacy. Qualunque cosa tu faccia può essere vista da qualcun altro.

Supponiamo che ogni isola rappresenti una LAN privata e che l'oceano sia Internet. Quando si viaggia in traghetto, è simile alla connessione a un server Web o a un altro dispositivo tramite Internet. Non avete alcun controllo sui cavi e sui router che compongono Internet, proprio come non avete alcun controllo sulle altre persone sul traghetto. In questo modo è possibile che si verifichino problemi di protezione se si tenta di connettersi tra due reti private utilizzando una

risorsa pubblica.

La vostra isola decide di costruire un ponte verso un'altra isola in modo che ci sia un modo più facile, sicuro e diretto per le persone di viaggiare tra le due. È costoso costruire e mantenere il ponte, anche se l'isola con cui si sta collegando è molto vicina. Ma la necessità di un percorso sicuro e affidabile è così grande che lo si fa comunque. La vostra isola vorrebbe collegarsi ad una seconda isola che è molto più lontana, ma si decide che è troppo costosa.

Questa situazione è molto simile ad avere una linea affittata. I ponti (linee affittate) sono separati dall'oceano (Internet), ma sono anche in grado di collegare le isole (LAN). Molte aziende hanno scelto questo percorso a causa dell'esigenza di sicurezza e affidabilità nella connessione degli uffici remoti. Tuttavia, se gli uffici sono molto distanti, il costo può essere proibitivo - proprio come cercare di costruire un ponte che si estende su una grande distanza.

Come si inserisce VPN in questa analogia? Potremmo dare ad ogni abitante delle nostre isole il proprio piccolo sottomarino con queste proprietà.

- Èveloce.
- Èfacile portare con sé ovunque si vada.
- Èin grado di nascondervi completamente da qualsiasi altra barca o sottomarino.
- Èaffidabile.
- Non costa molto aggiungere altri sottomarini alla flotta una volta acquistato il primo.

Anche se viaggiano nell'oceano insieme ad altri traffici, gli abitanti delle nostre due isole potrebbero viaggiare avanti e indietro ogni volta che lo desiderano, con privacy e sicurezza. È essenzialmente così che funziona una VPN. Ogni membro remoto della rete può comunicare in modo sicuro e affidabile utilizzando Internet come supporto per la connessione alla LAN privata. Una VPN può crescere per ospitare più utenti e diverse posizioni molto più facilmente di una linea in leasing. Infatti, la scalabilità è un vantaggio importante che le VPN hanno rispetto alle tipiche linee in leasing. A differenza delle linee affittate, dove il costo aumenta in proporzione alle distanze coinvolte, la posizione geografica di ogni ufficio conta poco nella creazione di una VPN.

Tecnologie VPN

Una VPN ben progettata utilizza diversi metodi per mantenere la connessione e la sicurezza dei dati.

- **Riservatezza dei dati**: questo è forse il servizio più importante fornito da qualsiasi implementazione VPN. Poiché i dati privati viaggiano su una rete pubblica, la riservatezza dei dati è fondamentale e può essere raggiunta crittografando i dati. Si tratta del processo che consente di prendere tutti i dati inviati da un computer a un altro e di codificarli in un formato che solo l'altro computer sarà in grado di decodificare.La maggior parte delle VPN utilizza uno di questi protocolli per fornire la crittografia.**IPsec**: il protocollo IPsec (Internet Protocol Security Protocol) offre funzionalità di protezione avanzate, ad esempio algoritmi di crittografia più affidabili e autenticazione più completa. IPsec dispone di due modalità di crittografia: tunnel e trasporto. La modalità tunnel crittografa l'intestazione e il payload di ciascun pacchetto, la modalità trasporto crittografa solo il payload. Solo i sistemi conformi a IPsec possono trarre vantaggio da questo protocollo. Inoltre, tutti i dispositivi devono utilizzare una chiave o un certificato comune e devono avere criteri di protezione molto simili impostati.Per gli utenti VPN ad accesso remoto, una forma di pacchetto software di terze parti fornisce la connessione e la crittografia sul PC degli utenti. IPsec supporta la crittografia a 56 bit (DES

singolo) o a 168 bit (DES triplo).**PPTP/MPPE** - PPTP è stato creato dal PPTP Forum, un consorzio che include US Robotics, Microsoft, 3COM, Ascend e ECI Telematics. PPTP supporta VPN multiprotocollo, con crittografia a 40 bit e a 128 bit, tramite un protocollo denominato MPPE (Microsoft Point-to-Point Encryption). È importante notare che PPTP di per sé non fornisce la crittografia dei dati.**L2TP/IPsec** - Denominato comunemente L2TP su IPsec, fornisce la sicurezza del protocollo IPsec sul tunneling del protocollo L2TP (Layer 2 Tunneling Protocol). L2TP è il prodotto di una partnership tra i membri del forum PPTP, Cisco, e la Internet Engineering Task Force (IETF). Utilizzata principalmente per VPN ad accesso remoto con sistemi operativi Windows 2000, poiché Windows 2000 fornisce un client IPsec e L2TP nativo. I provider di servizi Internet possono inoltre fornire connessioni L2TP per gli utenti della connessione remota e quindi crittografare il traffico con IPsec tra il punto di accesso e il server di rete della sede remota.

- **Integrità dei dati**: sebbene sia importante che i dati siano crittografati su una rete pubblica, è altrettanto importante verificare che non siano stati modificati durante la trasmissione. Ad esempio, IPsec ha un meccanismo che assicura che la parte crittografata del pacchetto, o l'intera intestazione e la parte dati del pacchetto, non sia stata manomessa. Se viene rilevata una manomissione, il pacchetto viene scartato. L'integrità dei dati può inoltre comportare l'autenticazione del peer remoto.
- **Autenticazione origine dati**: è estremamente importante verificare l'identità dell'origine dei dati inviati. Ciò è necessario per prevenire una serie di attacchi che dipendono dallo spoofing dell'identità del mittente.
- **Anti Replay**: consente di rilevare e rifiutare i pacchetti riprodotti e di prevenire lo spoofing.
- **Tunneling dei dati/Riservatezza del flusso di traffico**: il tunneling è il processo di incapsulamento di un intero pacchetto in un altro pacchetto e di invio in rete. Il tunneling dei dati è utile nei casi in cui è consigliabile nascondere l'identità del dispositivo da cui proviene il traffico. Ad esempio, un singolo dispositivo che usa IPsec incapsula il traffico che appartiene a un certo numero di host dietro di esso e aggiunge la propria intestazione sui pacchetti esistenti. Crittografando il pacchetto e l'intestazione originali (e instradando il pacchetto in base all'intestazione di layer 3 aggiuntiva aggiunta in cima), il dispositivo di tunneling nasconde effettivamente l'origine effettiva del pacchetto. Solo il peer attendibile è in grado di determinare la vera origine, dopo aver eliminato l'intestazione aggiuntiva e decrittografato l'intestazione originale. Come indicato nella RFC 2401 , "...la divulgazione delle caratteristiche esterne della comunicazione può anche essere un problema in alcune circostanze. La riservatezza del flusso di traffico è il servizio che risolve quest'ultimo problema nascondendo gli indirizzi di origine e di destinazione, la lunghezza del messaggio o la frequenza delle comunicazioni. Nel contesto IPsec, l'uso di ESP in modalità tunnel, soprattutto a un gateway di sicurezza, può fornire un certo livello di riservatezza del flusso di traffico."Tutti i protocolli di crittografia elencati utilizzano il tunneling per trasferire i dati crittografati sulla rete pubblica. È importante rendersi conto che il tunneling, da solo, non fornisce sicurezza dei dati. Il pacchetto originale viene semplicemente incapsulato in un altro protocollo e, se non criptato, potrebbe essere ancora visibile con un dispositivo di acquisizione dei pacchetti. Viene tuttavia menzionato in questo documento poiché è parte integrante del funzionamento delle VPN.Il tunneling richiede tre protocolli diversi.**Protocollo passeggeri**: i dati originali (IPX, NetBeui, IP) trasportati.**Protocollo di incapsulamento**: il protocollo (GRE, IPsec, L2F, PPTP, L2TP) racchiuso tra i dati originali.**Protocollo vettore**: il protocollo utilizzato dalla rete su cui viaggiano le informazioni.Il pacchetto originale (protocollo passeggeri) viene incapsulato nel protocollo di incapsulamento, che viene quindi inserito nell'intestazione del protocollo vettore (generalmente IP) per la trasmissione sulla rete pubblica. Notare che il protocollo di

incapsulamento esegue spesso anche la crittografia dei dati. Protocolli quali IPX e NetBeui, che normalmente non vengono trasferiti tramite Internet, possono essere trasmessi in modo sicuro.Per le VPN da sito a sito, il protocollo di incapsulamento è in genere IPsec o GRE (Generic Routing Encapsulation). Il GRE include informazioni sul tipo di pacchetto da incapsulare e sulla connessione tra il client e il server.Per le VPN ad accesso remoto, il tunneling in genere viene eseguito utilizzando il protocollo PPP (Point-to-Point Protocol). Parte dello stack TCP/IP, il protocollo PPP è il protocollo portante per altri protocolli IP quando comunica in rete tra il computer host e un sistema remoto. Il tunneling PPP utilizzerà uno dei protocolli PPTP, L2TP o L2F (Layer 2 Forwarding) di Cisco.

- AAA: autenticazione, autorizzazione e accounting vengono utilizzati per un accesso più sicuro in un ambiente VPN ad accesso remoto. Senza l'autenticazione dell'utente, chiunque lavori su un laptop/PC con software client VPN preconfigurato può stabilire una connessione sicura alla rete remota. Con l'autenticazione utente, tuttavia, è necessario immettere un nome utente e una password validi prima di completare la connessione. I nomi utente e le password possono essere archiviati sul dispositivo di terminazione VPN stesso o su un server AAA esterno, che può fornire l'autenticazione a numerosi altri database come Windows NT, Novell, LDAP e così via.Quando un client remoto invia una richiesta per stabilire un tunnel, il dispositivo VPN richiede un nome utente e una password. L'autenticazione può essere eseguita localmente o inviata al server AAA esterno, che controlla:Chi sei (Autenticazione)Operazioni consentite (autorizzazione)Effetti (contabilità)Le informazioni di accounting sono particolarmente utili per tenere traccia dell'utilizzo dei client a scopo di verifica della sicurezza, fatturazione o creazione di report.
- Non ripudio: in alcuni trasferimenti di dati, in particolare quelli relativi alle transazioni finanziarie, il non ripudio è una caratteristica altamente desiderabile. Ciò è utile per prevenire situazioni in cui un fine nega di aver preso parte a una transazione. Come in una banca che richiede la firma prima di onorare l'assegno, il non ripudio funziona allegando una firma digitale al messaggio inviato, impedendo così la possibilità di negare la partecipazione del mittente alla transazione.

Esistono diversi protocolli che possono essere utilizzati per creare una soluzione VPN. Tutti i protocolli forniscono un sottoinsieme dei servizi elencati nel presente documento. La scelta del protocollo dipende dall'insieme di servizi desiderati. Ad esempio, un'organizzazione potrebbe essere a proprio agio con il trasferimento dei dati in testo chiaro ma estremamente preoccupata per il mantenimento della propria integrità, mentre un'altra organizzazione potrebbe trovare assolutamente essenziale mantenere la riservatezza dei dati. La scelta dei protocolli potrebbe quindi essere diversa. Per ulteriori informazioni sui protocolli disponibili e sui relativi punti di forza, fare riferimento alla sezione Qual è la soluzione VPN giusta per te?

Prodotti VPN

In base al tipo di VPN (accesso remoto o da sito a sito), è necessario implementare alcuni componenti per creare la VPN. Tra queste vi sono:

- Client software desktop per ogni utente remoto
- Hardware dedicato come Cisco VPN Concentrator o Cisco Secure PIX Firewall
- Server VPN dedicato per servizi di connessione remota
- Server di accesso alla rete (NAS) utilizzato dal provider di servizi per l'accesso VPN degli utenti remoti
- Centro gestione criteri e rete privata

Poiché non esiste uno standard ampiamente accettato per l'implementazione di una VPN, molte aziende hanno sviluppato soluzioni chiavi in mano da sole. Ad esempio, Cisco offre diverse soluzioni VPN, tra cui:

- **VPN Concentrator**: incorporando le tecniche di crittografia e autenticazione più avanzate disponibili, Cisco VPN Concentrator è progettato appositamente per la creazione di VPN ad accesso remoto o da sito a sito e, idealmente, viene implementato laddove è necessario che un singolo dispositivo gestisca un numero elevato di tunnel VPN. VPN Concentrator è stato appositamente sviluppato per soddisfare i requisiti di un dispositivo VPN ad accesso remoto appositamente progettato. I concentratori forniscono elevata disponibilità, elevate prestazioni e scalabilità e includono componenti, denominati moduli SEP (Scalable Encryption Processing), che consentono agli utenti di aumentare facilmente capacità e throughput. I concentratori sono disponibili in modelli adatti per le piccole aziende con un massimo di 100 utenti con accesso remoto per le grandi aziende con un massimo di 10.000 utenti remoti simultanei. 
- **Router abilitato per VPN/Router ottimizzato per VPN**: tutti i router Cisco con software Cisco IOS® supportano le VPN IPsec. L'unico requisito è che il router debba eseguire un'immagine Cisco IOS con le funzionalità appropriate. La soluzione VPN per Cisco IOS supporta completamente i requisiti di accesso remoto, Intranet ed Extranet VPN. Ciò significa che i router Cisco possono funzionare correttamente anche quando sono connessi a un host remoto che esegue il software VPN Client o a un altro dispositivo VPN, ad esempio un router, un firewall PIX o un concentratore VPN. I router abilitati per le VPN sono appropriati per le VPN con requisiti moderati di crittografia e tunneling e offrono servizi VPN interamente tramite le funzionalità software di Cisco IOS. Esempi di router abilitati per la VPN includono Cisco serie 1000, Cisco 1600, Cisco 2500, Cisco 4000, Cisco 4500 e Cisco 4700.I router ottimizzati per le VPN di Cisco forniscono scalabilità, routing, sicurezza e qualità del servizio (QoS). I router sono basati sul software Cisco IOS e vi è un dispositivo adatto a tutte le situazioni, dall'accesso per piccoli uffici/uffici domestici (SOHO) all'aggregazione VPN del sito centrale fino alle esigenze dell'azienda su larga scala. I router ottimizzati per la VPN sono progettati per soddisfare gli elevati requisiti di crittografia e tunneling e spesso utilizzano hardware aggiuntivo, ad esempio schede di crittografia, per ottenere prestazioni elevate. Esempi di router ottimizzati per la VPN includono Cisco 800, Cisco 1700, Cisco 2600, Cisco 3600, Cisco

7200 e Cisco serie 7500.

- **Cisco Secure PIX Firewall**: il firewall PIX (Private Internet eXchange) combina le funzionalità di traduzione dinamica degli indirizzi di rete, server proxy, filtraggio dei pacchetti, firewall e VPN in un unico componente hardware. Anziché utilizzare il software Cisco IOS, questo dispositivo ha un sistema operativo altamente semplificato che scambia la capacità di gestire una varietà di protocolli per un'estrema robustezza e prestazioni concentrandosi sull'IP. Come per i router Cisco, tutti i modelli PIX Firewall supportano la VPN IPsec. È sufficiente soddisfare

i requisiti delle licenze per abilitare la funzionalità VPN.
- **Client VPN Cisco**: Cisco offre client VPN hardware e software. Cisco VPN Client (software) viene fornito con Cisco VPN serie 3000 Concentrator senza costi aggiuntivi. Questo client software può essere installato sul computer host e utilizzato per connettersi in modo sicuro al concentratore del sito centrale (o a qualsiasi altro dispositivo VPN come un router o un firewall). Il client hardware VPN 3002 è un'alternativa all'installazione del software client VPN su ogni computer e fornisce connettività VPN a numerosi dispositivi.

La scelta dei dispositivi da utilizzare per creare la soluzione VPN è in ultima analisi un problema di progettazione che dipende da una serie di fattori, tra cui il throughput desiderato e il numero di utenti. Ad esempio, su un sito remoto con un gruppo di utenti dietro un PIX 501, si potrebbe prendere in considerazione la configurazione del PIX esistente come endpoint VPN IPsec, a condizione che si accetti il throughput 3DES del 501 di circa 3 Mbps e il limite di un massimo di 5 peer VPN. D'altra parte, su un sito centrale che agisce come endpoint VPN per un elevato numero di tunnel VPN, accedere a un router ottimizzato per VPN o a un concentratore VPN sarebbe probabilmente una buona idea. La scelta dipende dal tipo (da LAN a LAN o accesso remoto) e dal numero di tunnel VPN configurati. L'ampia gamma di dispositivi Cisco che supportano VPN offre ai progettisti di rete un'elevata flessibilità e una soluzione solida per soddisfare tutte le esigenze di progettazione.

Informazioni correlate

- Informazioni sulla VPDN
- VPN (Virtual Private Network)
- Pagina di supporto per Cisco VPN serie 3000 concentrator
- Pagina di supporto per i client Cisco VPN 3000
- Negoziazione IPsec/pagina di supporto del protocollo IKE

- Pagina di supporto per i firewall PIX serie 500
- RFC 1661: Protocollo PPP (Point-to-Point Protocol)
- RFC 2661: Protocollo L2TP (Layer Two Tunneling Protocol)
- Funzionamento: Funzionamento delle reti private virtuali
- Panoramica delle VPN
- Pagina VPN di Tom Dunigan
- Consorzio Virtual Private Network
- RFC (Requests for Comments)
- Supporto tecnico – Cisco Systems