Como funcionam as redes virtuais privadas

Índice

Introdução

Este documento aborda os princípios de VPNs, como componentes básicos de VPN, tecnologias, túnel e segurança de VPN.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

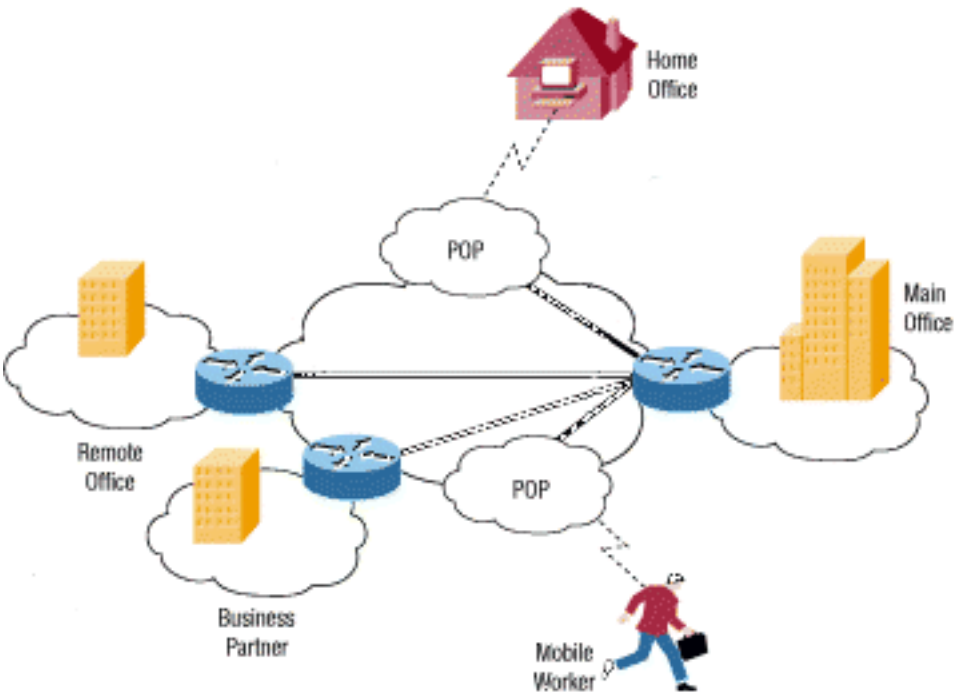
Informações de Apoio

O mundo passou por muitas mudanças nas duas últimas décadas. Em vez de simplesmente lidar com preocupações locais ou regionais, muitas empresas agora têm de pensar em mercados globais e logística. Muitas empresas possuem instalações dentro do país ou até mesmo espalhadas pelo mundo. Porém, todas as empresas precisam de algo em comum: uma forma de

manter a comunicação rápida, segura e confiável onde quer que estejam seus escritórios.

Até recentemente, uma comunicação confiável significava o uso de linhas alugadas para manter uma rede de longa distância (WAN). As linhas alugadas, que variam de Integrated Services Digital Network (ISDN, que funciona a 144 Kbps) até a fibra Optical Carrier-3 (OC3, que opera a 155 Mbps), fornecem a empresas uma maneira de expandir a rede privada além de sua área geográfica imediata. Uma WAN tem vantagens óbvias em uma rede pública, como a Internet, quando se trata de confiabilidade, desempenho e segurança; mas a manutenção de uma WAN, particularmente ao usar linhas alugadas, pode se tornar muito cara (muitas vezes aumenta o custo à medida que aumenta a distância entre os escritórios). Além disso, as linhas alugadas não são uma solução viável para empresas em que parte da força de trabalho é altamente móvel (como é o caso da equipe de marketing) e talvez precisem se conectar remotamente à rede corporativa e acessar dados confidenciais.

Àmedida que a popularidade da Internet cresceu, as empresas recorreram a ela como meio de ampliar suas próprias redes. Primeiro vieram as intranets, que são sites projetados para serem usados somente pelos funcionários da empresa. Agora, muitas empresas criam suas próprias redes VPNs (Virtual Private Networks) para atender às necessidades de funcionários remotos e escritórios distantes.



Uma VPN típica pode ter uma rede local (LAN) principal na sede corporativa de uma empresa, outras LANs em instalações ou escritórios remotos e usuários individuais que se conectam de fora no campo.

Uma VPN é uma rede privada que usa uma rede pública (geralmente a Internet) para conectar locais ou usuários remotos. Em vez de usar uma conexão dedicada do mundo real, como uma linha alugada, uma VPN usa conexões "virtuais" roteadas por meio da Internet, da rede privada da empresa até o local ou funcionário remoto.

Quais são as características de uma VPN?

Há dois tipos comuns de VPNs.

- **Acesso remoto** — Também conhecida como rede virtual privada de dial-up (VPDN), essa é uma conexão de usuário para LAN usada por uma empresa que tem funcionários que precisam se conectar à rede privada de vários locais remotos. Normalmente, uma empresa que deseja configurar uma grande VPN de acesso remoto fornece uma forma de conta dial-up da Internet a seus usuários usando um provedor de serviços de Internet (ISP). Os funcionários remotos podem então discar um número de discagem gratuita para acessar a Internet e usar o software cliente VPN para acessar a rede corporativa. Um bom exemplo de uma empresa que precisa de uma VPN de acesso remoto seria uma grande empresa com centenas de vendedores no campo. As VPNs de acesso remoto permitem conexões seguras e criptografadas entre a rede privada de uma empresa e usuários remotos por meio de um provedor de serviços terceirizado.
- **De site para site** — Por meio do uso de equipamentos dedicados e criptografia em larga escala, uma empresa pode conectar vários sites fixos em uma rede pública, como a Internet. Cada site precisa apenas de uma conexão local com a mesma rede pública, economizando, assim, dinheiro em longas linhas privadas alugadas. As VPNs de site para site podem ser categorizadas em intranets ou extranets. Uma VPN de site para site criada entre escritórios da mesma empresa é considerada uma VPN de intranet, enquanto uma VPN criada para conectar a empresa ao seu parceiro ou cliente é chamada de VPN de extranet.

Uma VPN bem projetada pode beneficiar muito uma empresa. Por exemplo, ela pode:

- Estender a conectividade geográfica
- Reduzir custos operacionais em relação às WANs tradicionais
- Reduzir tempos de trânsito e custos de viagem para usuários remotos
- Melhorar a produtividade
- Simplificar topologias de rede
- Fornecer oportunidades de rede global
- Fornecer suporte a funcionários remotos
- Fornecer retorno sobre o investimento (ROI) mais rápido do que a WAN tradicional

Quais recursos são necessários em uma VPN bem projetada? Ela deve incorporar estes itens:

- Security
- Confiabilidade
- Escalabilidade
- Gerenciamento de redes
- Gerenciamento de políticas

Analogia: Cada LAN é uma IsLANd (ilha)

Imagine que você mora em uma ilha em um enorme oceano. Há milhares de outras ilhas ao seu redor, algumas muito próximas e outras mais distantes. A maneira normal de viajar é pegar um barco de sua ilha para qualquer ilha que você queira visitar. Viajar em um barco significa que você não tem nenhuma privacidade. Tudo o que você faz pode ser visto por outra pessoa.

Suponha que cada ilha representa uma LAN privada e o oceano é a Internet. Quando você viaja de barco, é semelhante a quando você se conecta a um servidor da Web ou a outro dispositivo por meio da Internet. Você não tem controle sobre os fios e roteadores que compõem a Internet, assim como não tem controle sobre as outras pessoas no barco. Isso deixa você suscetível a problemas de segurança se tentar se conectar entre duas redes privadas usando um recurso

público.

Sua ilha decide construir uma ponte para outra ilha para que haja uma maneira mais fácil, segura e direta de as pessoas viajarem entre as duas. É caro construir e manter a ponte, mesmo que a ilha à qual você está se conectando esteja muito próxima. Mas a necessidade de um caminho seguro e confiável é tão grande que você faz isso de qualquer maneira. Sua ilha gostaria de se conectar a uma segunda ilha que é muito mais distante, mas você decide que isso é muito caro.

Essa situação é muito semelhante a ter uma linha alugada. As pontes (linhas alugadas) estão separadas do oceano (Internet), mas são capazes de conectar as ilhas (LANs). Muitas empresas escolheram essa rota devido à necessidade de segurança e confiabilidade na conexão de seus escritórios remotos. No entanto, se os escritórios estiverem muito distantes um do outro, o custo pode ser inviável, assim como tentar construir uma ponte que se estenda por uma grande distância.

Então, como a VPN se encaixa nessa analogia? Podemos dar a cada habitante de nossas ilhas um pequeno submarino com essas propriedades.

- Ele é rápido.
- Éfácil levá-lo aonde quer que você vá.
- Écapaz de escondê-lo completamente de quaisquer outros barcos ou submarinos.
- Éconfiável.
- Custa pouco para adicionar submarinos adicionais à sua frota, uma vez que o primeiro é comprado.

Embora eles estejam viajando no oceano junto com outro tráfego, os habitantes de nossas duas ilhas poderiam viajar entre elas sempre que quisessem com privacidade e segurança. Em resumo, assim é o funcionamento de uma VPN. Cada membro remoto da rede pode se comunicar de maneira segura e confiável usando a Internet como meio de conexão com a LAN privada. Uma VPN pode crescer para acomodar mais usuários e locais diferentes, de modo muito mais fácil do que uma linha dedicada. Na verdade, a escalabilidade é uma grande vantagem que as VPNs têm sobre linhas alugadas típicas. Diferentemente das linhas alugadas, em que o custo aumenta proporcionalmente às distâncias envolvidas, as localizações geográficas de cada escritório não são muito importantes na criação de uma VPN.

Tecnologias de VPN

Uma VPN bem projetada usa vários métodos para manter a conexão e os dados seguros.

- **Confidencialidade de dados** — Este seja talvez o serviço mais importante fornecido por qualquer implementação de VPN. Como os dados privados trafegam por uma rede pública, a confidencialidade dos dados é vital e pode ser obtida com a criptografia dos dados. Este é o processo de coletar todos os dados que um computador está enviando para outro e codificá-los em um formato que somente o outro computador poderá decodificar.A maioria das VPNs usa um desses protocolos para fornecer criptografia.**IPsec** — O Internet Protocol Security Protocol (IPsec) fornece recursos de segurança aprimorados, como algoritmos de criptografia mais fortes e autenticação mais abrangente. O IPsec tem dois modos de criptografia: túnel e transporte. O modo de túnel criptografa o cabeçalho e o payload de cada pacote, enquanto o modo de transporte criptografa apenas o payload. Somente os sistemas compatíveis com o IPsec podem utilizar esse protocolo. Além disso, todos os dispositivos devem usar uma chave ou um certificado comum e devem ter políticas de segurança muito semelhantes

configuradas.Para usuários de VPN de acesso remoto, uma forma de pacote de software de terceiros fornece a conexão e a criptografia no PC do usuário. O IPsec é compatível com criptografia de 56 bits (DES único) ou de 168 bits (DES triplo).**PPTP/MPPE** — O PPTP foi criado pelo PPTP Forum, um consórcio que inclui US Robotics, Microsoft, 3COM, Ascend e ECI Telematics. O PPTP suporta VPNs multiprotocolo, com criptografia de 40 bits e 128 bits usando um protocolo chamado Microsoft Point-to-Point Encryption (MPPE). É importante observar que o PPTP por si só não fornece criptografia de dados.**L2TP/IPsec** — Normalmente chamado de L2TP por IPsec, isso fornece a segurança do protocolo IPsec no túnel do Layer 2 TunnelingProtocol (L2TP). L2TP é o produto de uma parceria entre os membros do fórum PPTP, da Cisco e de Internet Engineering Task Force (IETF). Usado principalmente para VPNs de acesso remoto com sistemas operacionais Windows 2000, já que o Windows 2000 fornece um cliente IPsec e L2TP nativo. Os provedores de serviços de Internet também podem fornecer conexões L2TP para usuários de discagem e, em seguida, criptografar esse tráfego com o IPsec entre seu access point e o servidor de rede do escritório remoto.

- **Integridade de dados** — Embora seja importante a criptografia de dados em uma rede pública, também é essencial verificar se eles não foram alterados em trânsito. Por exemplo, o IPsec tem um mecanismo para garantir que a parte criptografada do pacote, ou o cabeçalho inteiro e a parte de dados do pacote, não tenha sido adulterada. Se a violação for detectada, o pacote será descartado. A integridade de dados também pode envolver a autenticação do par remoto.
- **Autenticação da origem de dados** — É extremamente importante verificar a identidade da origem dos dados enviados. Isso é necessário para proteger contra vários ataques que dependem da falsificação da identidade do remetente.
- **Anti-replay** — Esta é a capacidade de detectar e rejeitar pacotes repetidos e ajuda a evitar falsificações.
- **Confidencialidade de túnel de dados/fluxo de dados** — Túnel é o processo de encapsulamento de um pacote inteiro em outro pacote e seu envio por meio de uma rede. O túnel de dados é útil nos casos em que é desejável ocultar a identidade do dispositivo que origina o tráfego. Por exemplo, um único dispositivo que usa IPsec encapsula o tráfego que pertence a um número de hosts por trás dele e adiciona seu próprio cabeçalho sobre os pacotes atuais. Ao criptografar o pacote e o cabeçalho originais (e rotear o pacote com base no cabeçalho adicional da camada 3 adicionado no topo), o dispositivo de túnel efetivamente oculta a origem real do pacote. Somente o par confiável é capaz de determinar a origem verdadeira, depois de eliminar o cabeçalho adicional e descriptografar o cabeçalho original. Conforme mencionado em RFC 2401 , "...a divulgação das características externas da comunicação também pode ser uma preocupação em algumas circunstâncias. A confidencialidade do fluxo de tráfego é o serviço que trata dessa última preocupação, ocultando os endereços de origem e de destino, a duração da mensagem ou a frequência da comunicação. No contexto IPsec, o uso do ESP no modo de túnel, especialmente em um gateway de segurança, pode fornecer um nível de confidencialidade do fluxo de tráfego."Todos os protocolos de criptografia listados aqui também usam o túnel como um meio de transferir os dados criptografados pela rede pública. É importante perceber que o túnel, sozinho, não oferece segurança de dados. O pacote original é simplesmente encapsulado dentro de outro protocolo e pode ainda estar visível com um dispositivo de captura de pacotes caso não seja criptografado. É mencionado aqui, no entanto, já que é parte integrante de como as VPNs funcionam.O túnel requer três protocolos diferentes.**Protocolo Passenger** — Os dados originais (IPX, NetBeui, IP) que são

transportados.**Protocolo Encapsulating** — O protocolo (GRE, IPsec, L2F, PPTP, L2TP) que é envolvido em torno dos dados originais.**Protocolo Carrier** — O protocolo usado pela rede sobre a qual a informação está viajando.O pacote original (protocolo Passenger) é encapsulado dentro do protocolo Encapsulating, que é então colocado no cabeçalho do protocolo Carrier (geralmente IP) para transmissão pela rede pública. Observe que o protocolo Encapsulating também realiza com bastante frequência a criptografia dos dados. Protocolos como IPX e NetBeui, que normalmente não seriam transferidos pela Internet, podem ser transmitidos com segurança.Para VPNs de site para site, o protocolo Encapsulating geralmente é IPsec ou Generic Routing Encapsulation (GRE). O GRE inclui informações sobre o tipo de pacote que você está encapsulando e informações sobre a conexão entre o cliente e o servidor.Para VPNs de acesso remoto, o túnel normalmente ocorre usando o Point-to-Point Protocol (PPP). Parte da pilha TCP/IP, o PPP é o compartimento para outros protocolos IP ao se comunicar pela rede entre o computador host e um sistema remoto. O túnel PPP utilizará um dos PPTP, L2TP ou o Layer 2 Forwarding (L2F) da Cisco.

- **AAA** — Autenticação, autorização e contabilização (Authentication, Authorization, and Accounting) são usadas para acesso mais seguro em um ambiente VPN de acesso remoto. Sem a autenticação do usuário, qualquer pessoa que usa um laptop/PC com software cliente VPN pré-configurado pode estabelecer uma conexão segura na rede remota. Com a autenticação do usuário, no entanto, um nome de usuário e uma senha válidos também devem ser inseridos antes que a conexão seja concluída. Nomes de usuário e senhas podem ser armazenados no próprio dispositivo de terminação VPN ou em um servidor AAA externo, que pode fornecer autenticação para vários outros bancos de dados, como Windows NT, Novell, LDAP e assim por diante.Quando uma solicitação para estabelecer um túnel é recebida de um cliente dial-up, o dispositivo VPN solicita um nome de usuário e uma senha. Isso pode ser autenticado localmente ou enviado para o servidor AAA externo, que verifica:Quem você é (autenticação)O que você tem permissão para fazer (autorização)O que você realmente faz (contabilização)As informações de contabilização são especialmente úteis para rastrear o uso do cliente para fins de auditoria de segurança, cobrança ou relatórios.
- **Não-repúdio** — Em certas transferências de dados, especialmente aquelas relacionadas a transações financeiras, o não-repúdio é uma característica altamente desejável. Isso é útil para evitar situações em que um lado nega ter participado de uma transação. Assim como um banco exige a assinatura antes de honrar um cheque, o trabalho de não-repúdio anexa uma assinatura digital à mensagem enviada, evitando assim a possibilidade de o remetente negar participação na transação.

Existem vários protocolos que podem ser usados para criar uma solução VPN. Todos esses protocolos fornecem um subconjunto dos serviços listados neste documento. A escolha de um protocolo depende do conjunto de serviços desejados. Por exemplo, uma empresa pode estar confortável com os dados sendo transferidos em texto simples, mas extremamente preocupada com a manutenção de sua integridade, enquanto outra empresa pode achar absolutamente essencial manter a confidencialidade dos dados. A escolha de protocolos pode ser diferente. Para obter mais informações sobre os protocolos disponíveis e seus pontos fortes relativos, consulte Qual solução VPN é ideal para você?

Produtos VPN

Com base no tipo de VPN (acesso remoto ou de site para site), você precisa colocar em prática determinados componentes para criar a VPN. São eles:

- Cliente de software de desktop para cada usuário remoto
- Hardware dedicado, como um Cisco VPN Concentrator ou um Cisco Secure PIX Firewall
- Servidor VPN dedicado para serviços dial-up
- Network Access Server (NAS) usado pelo provedor de serviços para acesso VPN de usuário remoto
- Rede privada e centro de gerenciamento de políticas

Como não existe um padrão amplamente aceito para a implementação de uma VPN, muitas empresas desenvolveram, por conta própria, soluções prontas para uso. Por exemplo, a Cisco oferece várias soluções VPN que incluem:

- VPN Concentrator — Incorporando as mais avançadas técnicas de criptografia e autenticação disponíveis, os Cisco VPN Concentrators são criados especificamente para criar uma VPN de acesso remoto ou de site para site e, de preferência, são implantados onde o requisito é que um único dispositivo manipule um grande número de túneis VPN. O VPN Concentrator foi desenvolvido especificamente para lidar com a necessidade de um dispositivo VPN de acesso remoto e criado sob medida. Os concentradores fornecem alta disponibilidade, alto desempenho e escalabilidade e incluem componentes, chamados módulos Scalable Encryption Processing (SEP), que permitem aos usuários aumentar facilmente a capacidade e a taxa de transferência. Os concentradores são oferecidos em modelos adequados para pequenas empresas com 100 ou menos usuários de acesso remoto e grandes empresas com até 10.000 usuários remotos simultâneos. 
- Roteador com VPN ativado/Roteador otimizado para VPN — Todos os roteadores Cisco que executam o software Cisco IOS® suportam VPNs IPsec. O único requisito é que o roteador execute uma imagem do Cisco IOS com o conjunto de recursos apropriados. A solução VPN do Cisco IOS suporta totalmente os requisitos VPN de acesso remoto, intranet e extranet. Isso significa que os roteadores Cisco podem funcionar igualmente bem quando conectados a um host remoto que executa o software VPN Client ou quando conectados a outro dispositivo VPN, como um roteador, PIX Firewall ou VPN Concentrator. Os roteadores com VPN ativada são apropriados para VPNs com requisitos moderados de criptografia e túnel e fornecem serviços VPN totalmente por meio dos recursos do software Cisco IOS. Exemplos de roteadores com VPN ativada incluem as séries Cisco 1000, Cisco 1600, Cisco 2500, Cisco 4000, Cisco 4500 e Cisco 4700.Os roteadores otimizados para VPN da Cisco fornecem escalabilidade, roteamento, segurança e qualidade de serviço (QoS). Os roteadores são baseados no software Cisco IOS e há um dispositivo adequado para todas as situações, desde o acesso de pequenas empresas/home-office (SOHO), passando pela agregação de VPN do site central, até as necessidades corporativas de grande escala. Os roteadores otimizados para VPN são projetados para atender aos altos requisitos de criptografia e túnel e geralmente usam hardware adicional, como cartões de criptografia, para obter alto desempenho. Exemplos de roteadores otimizados para VPN incluem as séries Cisco 800,

Cisco 1700, Cisco 2600, Cisco 3600, Cisco 7200 e Cisco

7500.

- **Cisco Secure PIX Firewall** — O firewall Private Internet eXchange (PIX) combina a conversão dinâmica de endereços de rede, servidor proxy, filtragem de pacotes, firewall e recursos de VPN em uma única peça de hardware. Em vez de usar o software Cisco IOS, esse dispositivo tem um sistema operacional altamente otimizado que negocia a capacidade de lidar com uma variedade de protocolos para extrema robustez e desempenho, concentrando-se em IP. Como nos roteadores Cisco, todos os modelos PIX Firewall suportam IPsec VPN. Os requisitos de licenciamento para ativar o recurso de VPN devem ser

atendidos.

- **Cisco VPN Clients** — A Cisco oferece os clientes VPN de hardware e software. O Cisco VPN Client (software) está disponível com o Cisco VPN 3000 Series Concentrator sem custo adicional. Esse cliente de software pode ser instalado na máquina host e usado para se conectar com segurança ao concentrador de site central (ou a qualquer outro dispositivo VPN, como um roteador ou firewall). O VPN 3002 Hardware Client é uma alternativa para implantar o software VPN Client em cada máquina e fornece conectividade VPN para vários dispositivos.

A escolha dos dispositivos que você usaria para criar a solução VPN é, em última análise, um problema de design que depende de vários fatores, incluindo a taxa de transferência desejada e o número de usuários. Por exemplo, em um site remoto com um grupo de usuários por trás de um PIX 501, você poderia configurar o PIX atual como o endpoint IPsec VPN, desde que aceite a taxa de transferência 3DES de 501 de aproximadamente 3 Mbps e o limite máximo de 5 pares de VPN. Por outro lado, em um site central atuando como um endpoint VPN para um grande número de túneis VPN, a escolha de um roteador otimizado para VPN ou um concentrador VPN provavelmente seria uma boa ideia. A escolha agora dependeria do tipo (LAN para LAN ou acesso remoto) e do número de túneis VPN sendo configurados. A ampla variedade de dispositivos da Cisco que suportam a VPN fornece aos designers de rede uma alta flexibilidade e uma solução robusta para atender a todas as necessidades de projeto.

Informações Relacionadas

- Entendendo o VPDN
- VPNs (Virtual private networks, redes virtuais privadas)

- Página de suporte de Cisco VPN 3000 Series Concentrators
- Página de suporte do Cisco VPN 3000 Client
- Página do suporte de protocolo do IPsec Negotiation/IKE
- Página de suporte de PIX 500 Series Firewalls
- RFC 1661: O Point-to-Point Protocol (PPP)
- RFC 2661: Layer Two Tunneling Protocol "L2TP"
- Como funciona: Como funcionam as redes virtuais privadas
- Resumo de VPNs
- Página VPN de Tom Dunigan
- Consórcio de rede virtual privada
- Request for comments (RFC)
- Suporte Técnico - Cisco Systems