Como as redes virtuais privadas trabalham

Índice

Introdução

Este capas de documento os fundamentos dos VPN, tais como componentes VPN, Tecnologias, o Tunelamento, e a Segurança básicos VPN.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este original não é restringido à versão de software e hardware específica.

Convenções

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

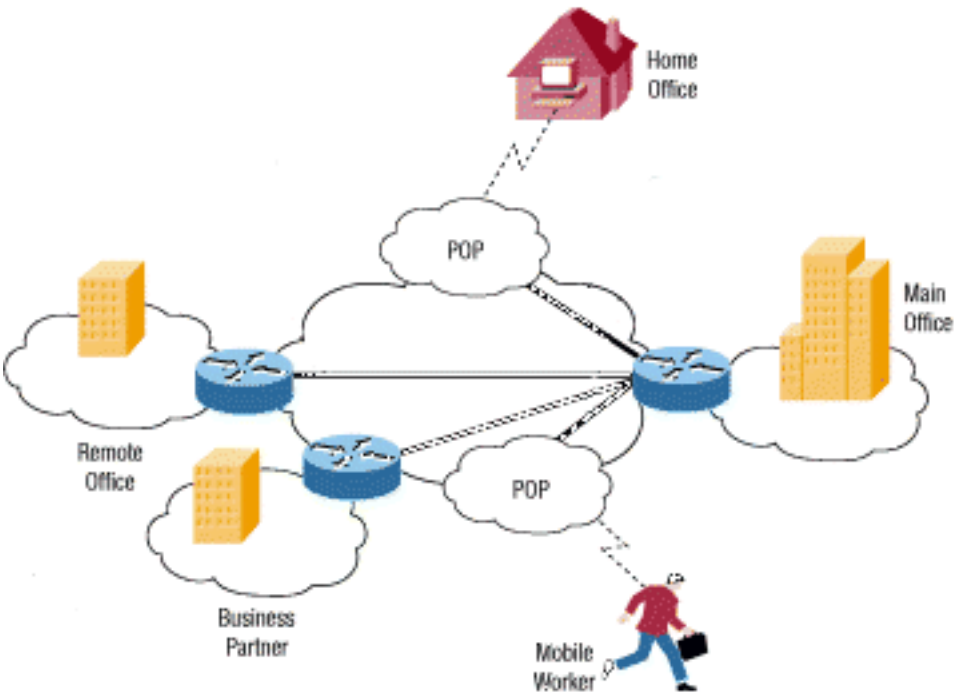
Informações de fundo

O mundo mudou muito nos últimos pares de décadas. Em vez simplesmente de tratar as preocupações locais ou regionais, muitos negócios agora têm que pensar sobre mercados globais e logística. Muitas empresas mandam facilidades espalhar para fora em todo o país, ou mesmo em todo o mundo. Mas há uma coisa que todas as empresas precisam: uma maneira de manter

rapidamente, seguro, e comunicações confiável onde quer que seus escritórios são situados.

Até recentemente, uma comunicação confiável significou o uso das linhas alugadas manter um Wide Area Network (WAN). As linhas alugadas, variando do Integrated Services Digital Network (ISDN, que é executado em 144 kbps) (o OC3, que é executado no 155 Mbps) à fibra Carrier-3 Ótica, fornecem uma empresa uma maneira de expandir sua rede privada além de sua área geográfica imediata. WAN tem vantagens óbvias sobre uma rede pública como o Internet quando se trata da confiança, do desempenho, e da Segurança; mas manter WAN, particularmente ao usar linhas alugadas, pode tornar-se bastante cara (ele frequentemente elevações no custo como a distância entre os aumentos dos escritórios). Adicionalmente, as linhas alugadas não são uma solução viável para as organizações onde parte da força de trabalho é altamente móvel (como é o caso com o grupo de marketing) e pôde frequentemente precisar de conectar remotamente à rede corporativa e de alcançar dados sensíveis.

Enquanto a popularidade do Internet cresceu, os negócios giraram-lhe para como meio de estender suas próprias redes. Vieram primeiramente os intranet, que são locais projetados para o uso somente por empregados da empresa. Agora, muitas empresas criam seu próprio Virtual Private Networks (VPNs) para acomodar as necessidades de funcionários remotos e de escritórios distantes.



Um VPN típico pôde ter uma rede de área local (LAN) principal na sede corporativa de uma empresa, outros LAN em escritórios remotos ou em facilidades, e usuários individuais que conectam para fora dentro do campo.

Um VPN é uma rede privada que use uma rede pública (geralmente o Internet) para conectar junto locais remotos ou usuários. Em vez de usar um dedicado, a conexão do mundo real, tal como a linha alugada, um VPN usa as conexões “virtuais” distribuídas através do Internet da rede privada da empresa ao local remoto ou ao empregado.

Que faz um VPN?

Há dois tipos comuns de VPN.

- **Acesso remoto** — Igualmente chamou um Virtual Private Dial-up Network (VPDN), isto é uma conexão usuário a LAN usada por uma empresa que tivesse os empregados que precisam de conectar à rede privada das várias posições remotas. Tipicamente, um corporaçõ que deseje estabelecer um grande acesso remoto VPN fornece algum formulário da conta do tratamento por imagens do Internet a seus usuários que usam um provedor de serviço do Internet (ISP). Os trabalhadores à distância podem então discar um número 1-800 para alcançar o Internet e para usar seu software do cliente VPN para alcançar a rede corporativa. Um bom exemplo de uma empresa que precisasse um acesso remoto VPN seria uma grande empresa com centenas de povos das vendas no campo. Os acessos remoto VPN permitem seguro, conexões criptografada entre a rede privada de uma empresa e usuários remotos através de um fornecedor de serviço de terceira parte.
- **Local-à-local** — Com o uso do equipamento dedicado e da criptografia em larga escala, uma empresa pode conectar sites fixo múltiplo sobre uma rede pública tal como o Internet. Cada local precisa somente uma conexão local à mesma rede pública, salvar desse modo o dinheiro em linhas alugadas privadas longas. Os VPN de Site-para-Site podem mais ser categorizados em intranet ou em extranet. Um VPN de Site-para-Site construído entre escritórios da mesma empresa seriam um intranet VPN, quando um VPN construído para conectar a empresa a seu sócio ou cliente for referido como um extranet VPN.

Um VPN bem-desenvolvida pode extremamente beneficiar uma empresa. Por exemplo, pode:

- Estenda a conectividade geográfica
- Reduza custos operacionais contra WAN tradicionais
- Reduza o tempo de trânsito e os custos de viagem para usuários remotos
- Melhore a produtividade
- Simplifique a topologia de rede
- Forneça oportunidades globais dos trabalhos em rede
- Forneça o apoio do telecommuter
- Forneça um returno de investimento mais rápido (ROI) do que o WAN tradicional

Que características são precisadas em um VPN bem-desenvolvida? Deve incorporar estes artigos:

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

Analogia: Cada LAN é uma ilha

Imagine que você vive em uma ilha em um oceano enorme. Há uns milhares de outras ilhas toda em torno de você, de algum muito perto e de outro mais distante afastado. O modo normal viajar é tomar uma balsa de sua ilha a qualquer ilha você deseja visitar. Viajar em uma balsa significa que você não tem quase nenhuma privacidade. Qualquer coisa que você faz pode ser considerado por alguma outra pessoa.

Supõe que cada ilha representa uma LAN privada e o oceano é o Internet. Quando você viaja pela balsa, é similar a quando você conecta a um servidor de Web ou a um outro dispositivo através do Internet. Você não tem nenhum controle sobre os fios e o Roteadores que compõe o

Internet, apenas como você não tem nenhum controle sobre os outros povos na balsa. Isto deixa-o susceptível às questões de segurança se você tenta conectar entre duas redes privadas usando uns recursos públicos.

Sua ilha decide construir uma ponte a uma outra ilha de modo que haja um mais fácil, mais seguro e a maneira direta para que os povos viajem entre os dois. É caro construir e manter a ponte, mesmo que a ilha que você está conectando com seja muito próxima. Mas a necessidade para um seguro, caminho seguro é tão grande que você o faz de qualquer maneira. Sua ilha gostaria de conectar a uma segunda ilha que estivesse muito mais distante ausente, mas você decide que é demasiado cara.

Esta situação é muita como ter uma linha alugada. As pontes (linhas alugadas) são separadas do oceano (Internet), contudo das elas podem conectar as ilhas (LAN). Muitas empresas escolheram esta rota devido à necessidade para a Segurança e à confiança em conectar seus escritórios remotos. Contudo, se os escritórios são muito afastadas, o custo pode ser proibitivamente alto - apenas como a tentativa construir uma ponte que meça uma grande distância.

Assim como o VPN cabe dentro a esta analogia? Nós poderíamos dar a cada habitante de nossas ilhas seu próprio submarino pequeno com estas propriedades.

- Érápido.
- Éfácil tomar com você onde quer que você vai.
- Pode escondê-lo completamente de todos os outros barcos ou submarinos.
- Éseguro.
- Custa pouco para adicionar submarinos adicionais a sua frota uma vez que os primeiros são comprados.

Embora viajassem no oceano junto com o outro tráfego, os habitantes de nossas duas ilhas poderiam viajar para a frente e para trás sempre que quiseram com à privacidade e à Segurança. Isso é essencialmente como um VPN trabalha. Cada membro remoto de sua rede pode comunicar-se em um seguro e em uma maneira confiável usando o Internet como o media para conectar à LAN privada. Um VPN pode crescer para acomodar mais usuários e lugar diferentes muito mais fáceis do que uma linha alugada. De fato, a escalabilidade é uma vantagem principal que os VPN tenham sobre linhas alugadas típicas. Ao contrário das linhas alugadas onde o custo aumenta em proporção às distâncias envolvidas, as localizações geográficas de cada matéria do escritório pouco na criação de um VPN.

Tecnologias de VPN

Um VPN bem-desenvolvida usa diversos métodos a fim manter seus conexão e dados seguros.

- **Confidencialidade de dados** — Este é talvez o serviço o mais importante proporcionado por toda a implementação de VPN. Desde que seus dados privados viajam sobre uma rede pública, a confidencialidade de dados é vital e pode ser alcançada cifrando os dados. Este é o processo de tomar todos os dados que um computador está enviando ao outro e está codificando os em um formulário que somente o outro computador poderá descodificar.A maioria de VPN usam um destes protocolos para fornecer a criptografia.**IPsec** — O protocolo de segurança de protocolo do Internet (IPsec) fornece recursos de segurança avançada tais como uns algoritmos de criptografia mais fortes e uma mais autenticação abrangente. IPsec tem dois modos de criptografia: túnel e transporte. O modo de túnel cifra o encabeçamento e o payload de cada pacote quando o modo de transporte cifrar somente o payload. Somente

os sistemas que são IPsec-complacentes podem aproveitar-se deste protocolo. Também, todos os dispositivos devem usar uma chave comum ou certificate e devem mandar políticas de segurança muito similares estabelecer-se.Para usuários do acesso remoto VPN, algum formulário do pacote de software de terceira parte fornece a conexão e a criptografia no PC dos usuários. Suportes de IPSec 56-bit (único DES) ou criptografia do 168-bit (DES triplo).**PPTP/MPPE** — O PPTP foi criado pelo fórum PPTP, um consórcio que incluísse US Robotics, Microsoft, 3COM, ascensão, e telemática ECI. O PPTP apoia o multi-protocol VPN, com criptografia 40-bit e de 128-bit usando um protocolo chamado criptografia Point-to-Point microsoft (MPPE). É importante notar que o PPTP por si só não fornece a criptografia de dados.**L2TP/IPsec** — O L2TP geralmente chamado sobre IPsec, isto fornece a Segurança do protocolo IPSec sobre o Tunelamento do protocolo Layer 2 Tunneling Protocol (L2TP). O L2TP é o produto de uma parceria entre os membros do fórum PPTP, Cisco, e o Internet Engineering Task Force (IETF). Usado primeiramente para acessos remoto VPN com sistemas operacionais do Windows 2000, desde que o Windows 2000 fornece um IPSEC nativo e cliente L2TP. Os provedores de serviço da Internet podem igualmente fornecer conexões L2TP para usuários de discagem de entrada, e cifram então esse tráfego com o IPsec entre seu acesso-ponto e o servidor de rede do escritório remoto.

- **Integridade de dados** — Quando for importante que seus dados estão cifrados sobre uma rede pública, são apenas como importantes verificar que não estiverem mudados quando no trânsito. Por exemplo, IPsec tem um mecanismo para assegurar-se de que a porção criptografada do pacote, ou o encabeçamento e a porção de dados inteiros do pacote, não estejam alterados. Se alterar é detectada, o pacote está deixado cair. A integridade de dados pode igualmente envolver autenticar o peer remoto.
- **Autenticação de origem de dados** — É extremamente importante verificar a identidade da fonte dos dados que são enviados. Isto é necessário para guardar contra um número de ataques que dependem da falsificação a identidade do remetente.
- **Anti repetição** — Esta é a capacidade para detectar e para rejeitar pacotes replayed e ajudas impeça a falsificação.
- **Tunelamento de dados/confidencialidade de fluxo de tráfego** — O Tunelamento é o processo de encapsular um pacote inteiro dentro de um outro pacote e de enviá-lo sobre uma rede. O tunelamento de dados é útil nos casos onde é desejável esconder a identidade do dispositivo que origina o tráfego. Por exemplo, um dispositivo único que use IPsec encapsula o tráfego que pertence a um número de anfitriões atrás dele e adiciona seu próprio encabeçamento sobre os pacotes existentes. Cifrando o pacote original e o encabeçamento (e distribuindo o pacote baseou no encabeçamento adicional da camada 3 adicionado na parte superior), o dispositivo do Tunelamento esconde eficazmente o origem real do pacote. Somente o par confiado pode determinar o origem verdadeira, depois que descasca afastado o encabeçamento adicional e decifra o cabeçalho original. Como referido no RFC 2401 , "… a divulgação das características externos de uma comunicação igualmente pode ser um interesse em algumas circunstâncias. A confidencialidade de fluxo de tráfego é o serviço que endereça este último interesse escondendo endereços de rementente e destinatário, tamanho da mensagem, ou frequência de uma comunicação. No contexto de IPsec, usar o ESP no modo de túnel, especialmente em um gateway de segurança, pode fornecer algum nível da confidencialidade de fluxo de tráfego."Todos os protocolos de codificação alistados aqui igualmente usam o Tunelamento como meios transferir os dados criptografados através da rede pública. É importante realizar que escavar um túnel, por si só, não fornece a segurança de dados. O pacote original é encapsulado meramente dentro de um outro protocolo e pôde ainda ser visível com um dispositivo de captura de pacote se não cifrado.

Menciona-se aqui, contudo, desde que é uma parte integral de como os VPN funcionam.O Tunelamento exige três protocolos diferentes.**Protocolo de passageiro** — Os dados originais (IPX, NetBeui, IP) que são levados.**Encapsulando o protocolo** — O protocolo (GRE, IPsec, L2F, PPTP, L2TP) que é envolvido em torno dos dados originais.**Protocolo do portador** — O protocolo usado pela rede sobre que a informação está viajando.O pacote original (protocolo de passageiro) é interior encapsulado o protocolo encapsulando, que é posto então dentro do encabeçamento de protocolo do portador (geralmente IP) para a transmissão sobre a rede pública. Note que o protocolo encapsulando igualmente realiza bastante frequentemente a criptografia dos dados. Protocolos tais como o IPX e o NetBeui, que não seriam transferidos normalmente através do Internet, pode com segurança e firmemente ser transmitido.Para VPN de Site-para-Site, o protocolo encapsulando é geralmente IPsec ou Generic Routing Encapsulation (GRE). O GRE inclui a informação em que tipo de pacote você está encapsulando e informação sobre a conexão entre o cliente e servidor.Para acessos remoto VPN, escavar um túnel ocorre normalmente usando o Point-to-Point Protocol (PPP). Parte da pilha TCP/IP, PPP é o portador para outros protocolos IP ao comunicar-se sobre a rede entre o computador host e um sistema remoto. O tunelamento PPP usará uma do PPTP, do L2TP ou da transmissão da camada 2 de Cisco (L2F).

- **AAA** — O autenticação, autorização e relatório é usado para mais acesso seguro em um ambiente do acesso remoto VPN. Sem autenticação de usuário, qualquer um que se senta em um laptop/PC com software PRE-configurado do cliente VPN pode estabelecer uma conexão segura na rede remota. Com autenticação de usuário contudo, um nome de usuário válido e uma senha igualmente têm que ser incorporados antes que a conexão esteja terminada. Os nomes de usuário e senha podem ser armazenados no dispositivo de terminação próprio VPN, ou em um servidor AAA externo, que possa fornecer a autenticação a numeroso outros bases de dados tais como o Windows NT, Novell, LDAP, e assim por diante.Quando um pedido estabelecer um túnel vem dentro de um cliente dial-up, o dispositivo VPN alerta para um nome de usuário e senha. Isto pode então ser autenticado localmente ou enviado ao servidor AAA externo, que verifica:Quem você é (autenticação)O que é permitido você fazer (autorização)O que você faz realmente (contabilidade)A informação de contabilidade é especialmente útil para seguir o uso do cliente para finalidades do exame de segurança, do faturamento ou do relatório.
- **Não repudiação** — Em determinadas transferências de dados, especialmente aqueles relacionaram-se às transações financeiras, não repudiação são uma característica altamente desejável. Isto é útil em impedir as situações onde uma extremidade nega ter participado em uma transação. Bem como um banco exige sua assinatura antes de honrar sua verificação, trabalhos da não repudiação anexando uma assinatura digital à mensagem enviada, assim impossibilitando a possibilidade de remetente que nega a participação na transação.

Um número de protocolos existem que podem ser usados para construir uma solução de VPN. Todos estes protocolos proporcionam algum subconjunto dos serviços alistados neste original. A escolha de um protocolo depende do conjunto de serviço desejado. Por exemplo, uma organização pôde ser confortável com os dados que estão sendo transferidos no texto claro mas extremamente - referido sobre a manutenção de sua integridade, quando uma outra organização pôde encontrar a confidencialidade de dados de manutenção absolutamente essencial. Sua escolha dos protocolos pôde assim ser diferente. Para obter mais informações sobre dos protocolos disponíveis e de suas forças relativas, refira que solução de VPN é direita para você?

Produtos VPN

Baseado no tipo de VPN (acesso remoto ou local-à-local), você precisa de pôr determinados componentes no lugar para construir seu VPN. Estes puderam incluir:

- Cliente de software de área de trabalho para cada usuário remoto
- Hardware dedicado tal como um Cisco VPN concentrator ou um firewall PIX segura Cisco
- Servidor de VPN dedicado para serviços dial-up
- Servidor do acesso de rede (NAS) usado pelo provedor de serviços para o acesso do usuário remoto VPN
- Centro da rede privada e do Gerenciamento de políticas

Porque não há nenhum padrão extensamente aceitado para executar um VPN, muitas empresas desenvolveram soluções turn-key no seus próprios. Por exemplo, Cisco oferece diversas soluções de VPN que incluem:

- **Concentrador VPN** — Incorporando a maioria de técnicas da criptografia avançada e da autenticação disponíveis, os Cisco VPN concentratores são construídos especificamente criando um acesso remoto ou um VPN de Site-para-Site e idealmente distribuídos onde a exigência é para que um dispositivo único segure muito um número grande de túneis VPN. O concentrador VPN foi desenvolvido especificamente para endereçar a exigência para finalidade-construída, dispositivo do acesso remoto VPN. Os concentradores fornecem a Alta disponibilidade, o alto desempenho e a escalabilidade e incluem os componentes, chamados os módulos do Scalable Encryption Processing (SEP), que permitem usuários de aumentar facilmente a capacidade e a taxa de transferência. Os concentradores são oferecidos nos modelos apropriados para empresas de pequeno porte com 100 ou menos usuários de acesso remotos às grandes organizações de empreendimento com os até 10,000 usuários remotos simultâneos. 
- **Roteador VPN-permitido Router/VPN-Optimized** — Todo o Roteadores de Cisco que executa o suporte de software IPsec VPN de Cisco IOS®. A única exigência é que o roteador deve executar uma imagem IOS Cisco com o conjunto de recursos apropriado. A solução de VPN do Cisco IOS apoia inteiramente exigências do Acesso remoto, do intranet e do extranet VPN. Isto significa que o Roteadores de Cisco pode trabalhar igualmente bem quando conectado a um software running do cliente VPN do host remoto ou quando conectado a um outro dispositivo VPN tal como um roteador, o Firewall PIX ou o concentrador VPN. o Roteadores VPN-permitido é apropriado para VPN com exigências da criptografia moderada e do Tunelamento e proporciona serviços VPN inteiramente através das Funcionalidades do software Cisco IOS. Os exemplos do Roteadores VPN-permitido incluem o Cisco 1000, o Cisco 1600, o Cisco2500, Cisco 4000, o Cisco4500, e o Cisco 4700 Series.Os roteadores otimizado de VPN de Cisco fornecem a escalabilidade, o roteamento, a Segurança, e o Qualidade de Serviço (QoS). O Roteadores é baseado no software do Cisco IOS, e há um dispositivo apropriado para cada situação, do acesso do small office/home office (SOHO) com a agregação da instalação central VPN às necessidades do empreendimento de larga

escala. Os roteadores otimizado de VPN são projetados cumprir requisitos de tunelamento e criptografia superior e utilizar frequentemente o hardware adicional tal como placas de criptografia para conseguir o alto desempenho. Os exemplos dos roteadores otimizado de VPN incluem o Cisco 800, o Cisco 1700, o Cisco 2600, o Cisco 3600, o Cisco7200, e o

Cisco7500 Series.

- **Firewall PIX segura Cisco** — O Firewall do intercâmbio de Internet privada (PIX) combina a tradução de endereço de rede dinâmica, o servidor proxy, o filtragem de pacote, o Firewall, e os recursos de VPN em uma única parte de hardware. Em vez de usar o software do Cisco IOS, este dispositivo tem um sistema operacional altamente aerodinâmico que troque a capacidade para segurar uma variedade de protocolos para o vigor e o desempenho extremos focalizando no IP. Como com Roteadores de Cisco, todos os modelos de firewall de PIX apoiam o IPSec VPN. Tudo que é exigido é que os requisitos de licenciamento para

permitir a característica VPN devem ser cumpridos.

- **Cisco VPN Client** — Cisco oferece ambos os clientes VPN do hardware e software. O Cisco VPN Client (software) vem empacotado com o concentrador da Cisco VPN 3000 Series sem qualquer custo adicional. Este cliente de software pode ser instalado na máquina host e ser usado para conectar firmemente ao concentrador da instalação central (ou a algum outro dispositivo VPN tal roteador ou Firewall). O cliente da ferragem VPN 3002 é uma alternativa a distribuir o software do cliente VPN em cada máquina e fornece a conectividade de VPN a um número de dispositivos.

A escolha dos dispositivos que você se usaria para construir sua solução de VPN é finalmente um problema de desenho que dependa de um número de fatores, incluindo a taxa de transferência desejada e o número de usuários. Por exemplo, em um local remoto com um número limitado de usuários atrás de um PIX 501, você poderia considerar configurar o PIX existente como o valor-limite do IPSec VPN, contanto que você aceita a taxa de transferência 501's 3DES aproximadamente de 3 Mbps e o limite de um máximo de pares 5 VPN. Por outro lado, em uma instalação central atuar como um ponto final de VPN para um grande número túneis VPN, indo dentro para um roteador otimizado de VPN ou um concentrador VPN seria provavelmente uma boa ideia. A escolha agora dependeria do tipo (LAN-à-LAN ou Acesso remoto) e do número de túneis VPN que estão sendo estabelecido-se s. O amplo intervalo dos dispositivos Cisco que apoiam o VPN fornece os projetistas de rede uma quantidade elevada de flexibilidade e de uma solução robusta encontrar cada necessidade do projeto.

Informações Relacionadas

- Entendendo o VPDN
- Virtual Private Networks (VPNs)
- Página de suporte do Concentradores Cisco VPN série 3000
- Página de suporte do Cisco VPN 3000 Client
- Página do suporte de protocolo do IPsec Negotiation/IKE
- Página de suporte dos Firewall da série PIX 500
- RFC 1661: O Point-to-Point Protocol (PPP)
- RFC 2661: Protocolo layer two tunneling "L2TP"
- Como o material trabalha: Como as redes virtuais privadas trabalham
- Vista geral dos VPN
- Página VPN de Tom Dunigan
- Consórcio de Virtual Private Network
- Request for comments (RFC)
- Suporte técnico - Cisco Systems