Visão geral e melhores práticas de VPN de roteadores Cisco RV

Objetivo

O objetivo deste documento é fornecer uma visão geral das melhores práticas de VPN (Virtual Private Network) para qualquer pessoa nova nos roteadores da série Cisco RV.

Table Of Contents

Introduction

Parece que faz tanto tempo que o único lugar onde você podia trabalhar era no escritório. Você deve se lembrar de ter que ir ao escritório no fim de semana para resolver um problema de trabalho. Não havia outra maneira de obter dados dos recursos da empresa, a menos que você estivesse fisicamente em seu escritório. Esses dias acabaram. Nos dias de hoje, você pode estar em movimento; conduzindo negócios em casa, em outro escritório, em um café ou mesmo em outro país. A desvantagem é que os hackers estão sempre procurando capturar seus dados confidenciais. Usar apenas a Internet pública não é seguro. O que você pode fazer para obter flexibilidade e segurança? Configure uma VPN!

Uma conexão VPN permite que os usuários acessem, enviem e recebam dados de uma rede privada, passando por uma rede pública ou compartilhada, como a Internet, mas ainda garantindo uma conexão segura a uma infraestrutura de rede subjacente para proteger a rede privada e seus recursos.

Um túnel VPN estabelece uma rede privada que pode enviar dados com segurança usando criptografia para codificar os dados e autenticação para garantir a identidade do cliente. Os escritórios corporativos geralmente usam uma conexão VPN, pois é útil e necessário permitir que seus funcionários tenham acesso à rede privada mesmo que estejam fora do escritório.

Normalmente, as VPNs site a site conectam redes inteiras entre si. Eles estendem uma rede e permitem que os recursos de computador de um local estejam disponíveis em outros locais. Com o uso de um roteador com capacidade para VPN, uma empresa pode conectar vários sites fixos em uma rede pública, como a

Internet.

A configuração de cliente para site para uma VPN permite que um host remoto, ou cliente, atue como se estivesse localizado na mesma rede local. Uma conexão VPN pode ser configurada entre o roteador e um endpoint depois que o roteador tiver sido configurado para conexão com a Internet. O cliente VPN depende das configurações do roteador VPN, além do requisito de configurações correspondentes para estabelecer uma conexão. Além disso, alguns dos aplicativos de cliente VPN são específicos da plataforma, eles também dependem da versão do sistema operacional (SO). As configurações devem ser exatamente as mesmas ou não podem se comunicar.

Uma VPN pode ser configurada com qualquer um dos seguintes:

- Secure Socket Layer (SSL)
- Segurança de Protocolo Internet (IPSec - Internet Protocol Security)
- Point to Point Tunneling Protocol (PPTP)- não tão seguro quanto SSL ou IPSec
- Encapsulamento de roteamento genérico (GRE)
- Protocolo de Tunelamento de Camada 2 (L2TP - Layer 2 Tunneling Protocol)

Se você nunca configurou uma VPN antes, receberá muitas informações novas em todo este artigo. Este não é um guia passo a passo, mas uma visão geral para referência. Portanto, seria útil ler este artigo na íntegra antes de prosseguir e tentar configurar uma VPN em sua rede. Links para etapas específicas são fornecidos neste artigo.

Produtos de terceiros que não são da Cisco, incluindo TheGreenBow, OpenVPN, Shrew Soft e EZ VPN não são suportados pela Cisco. Eles são incluídos estritamente para fins de orientação. Se você precisar de suporte além do artigo, entre em contato com o terceiro para obter suporte.

Benefícios do uso de uma conexão VPN

- Usar uma conexão VPN ajuda a proteger dados e recursos confidenciais da rede.
- Ele oferece conveniência e acessibilidade para funcionários remotos ou corporativos, já que eles poderão acessar facilmente os principais recursos do escritório sem ter que estar fisicamente presentes e, ainda assim, manter a segurança da rede privada e de seus recursos.
- A comunicação usando uma conexão VPN fornece um nível mais alto de segurança em comparação com outros métodos de comunicação remota. Um avançado algoritmo de criptografia torna isso possível, protegendo a rede privada contra acesso não autorizado.
- As localizações geográficas reais dos usuários são protegidas e não estão expostas às redes públicas ou compartilhadas, como a Internet.
- Uma VPN permite que novos usuários ou um grupo de usuários sejam adicionados sem a necessidade de componentes adicionais ou uma configuração complicada.

Riscos do uso de uma conexão VPN

- Pode haver riscos de segurança devido a erros de configuração. Como o projeto e a implementação de uma VPN pode ser complicado, é necessário confiar a tarefa de configuração da conexão a um profissional experiente e com conhecimento para garantir que a segurança da rede privada não seja comprometida.
- Pode ser menos confiável. Como uma conexão VPN requer uma conexão com a Internet, é importante ter um provedor com reputação comprovada e testada para fornecer um excelente serviço de Internet e

garantir um tempo de inatividade mínimo ou nulo.
- Se ocorrer uma situação em que haja necessidade de adicionar uma nova infraestrutura ou um novo conjunto de configurações, poderão surgir problemas técnicos devido à incompatibilidade, especialmente se ela envolver produtos ou fornecedores diferentes daqueles que você já está usando.
- Podem ocorrer velocidades de conexão lentas. Se você estiver usando uma conexão ISP que fornece serviço VPN gratuito, pode ser esperado que sua conexão também seja lenta, já que esses provedores não priorizam as velocidades de conexão. É importante observar que o throughput da VPN depende dos recursos de hardware do roteador.

Para obter mais informações sobre como as VPNs funcionam, clique aqui.

Dicas para usar ao configurar uma VPN

1. Use uma sub-rede IP de LAN diferente em ambas as extremidades ao configurar a VPN entre sites diferentes. Por exemplo, se o site ao qual você se conecta usa um esquema de endereçamento 192.168.x.x, você desejaria usar uma sub-rede 10.x.x.x ou 172.16.x.x - 172.31.x.x. Outra opção seria ter diferentes máscaras de sub-rede. Quando você altera o endereço IP do roteador, os dispositivos no protocolo DHCP selecionam automaticamente um endereço IP nessa sub-rede.
2. Use o IP público estático na interface WAN do roteador para conectividade VPN estável.
3. Certifique-se de que o nível de criptografia e autenticação selecionado seja o mesmo do roteador para o qual você deseja estabelecer um túnel VPN para a VPN.
4. Certifique-se de que a PSK e o Key Lifetime inseridos sejam iguais aos do roteador remoto. Uma PSK pode ser o que você quiser, ela só precisa corresponder no local e com o cliente quando ele é configurado como um cliente em seu computador. Dependendo do dispositivo, pode haver símbolos proibidos que não podem ser usados. Vida útil da chave é a frequência com que o sistema altera a chave. Um Certificado é preferível, pois é considerado mais seguro.
5. Para a maioria das VPNs, os clientes não precisam de um Certificado para usar uma VPN, é apenas para verificação através do roteador. Por exemplo, o OpenVPN requer certificados de cliente e de site.
6. Defina o tempo de vida da SA na Fase I por mais tempo do que o tempo de vida da SA da Fase II. Se você tornar sua Fase I mais curta que a Fase II, terá que renegociar o túnel para frente e para trás com frequência, ao contrário do túnel de dados. Um túnel de dados precisa de mais segurança, portanto, é melhor ter um tempo de vida na Fase II menor do que na Fase I.
7. Altere todas as senhas para algo mais complexo.

Tipos de VPN

SSL (Secure Sockets Layer - Camada de Soquetes Segura)

Os roteadores Cisco série RV34x suportam uma VPN SSL, usando o AnyConnect. O RV160 e o RV260 têm a opção de usar o OpenVPN, que é outra VPN SSL. O servidor VPN SSL permite que os usuários remotos estabeleçam um túnel VPN seguro usando um navegador da Web. Esse recurso permite acesso fácil a uma ampla variedade de recursos da Web e aplicativos habilitados para Web usando o suporte de navegador HTTP (Hypertext Transfer Protocol) over SSL HTTPS (Hypertext Transfer Protocol Secure).

A VPN SSL permite que os usuários acessem remotamente redes restritas, usando um caminho seguro e autenticado, criptografando o tráfego de rede.

Há duas opções para configurar o acesso em SSL:

1. Certificado autoassinado: um certificado que é assinado por seu próprio criador. Isso não é recomendado e deve ser usado somente em um ambiente de teste.
2. Certificado assinado pela CA: muito mais seguro e altamente recomendado. Por uma taxa, um terceiro valida que a rede é legítima e cria um Certificado CA que é anexado ao site. Para obter mais

informações sobre certificados CA, consulte a seção Certificados deste artigo.

Há links para artigos no AnyConnect neste documento. Para obter uma visão geral do AnyConnect, clique aqui.

Perfil IPsec

Easy VPN (EZVPN), TheGreenBow e Shrew Soft são VPNs de Internet Protocol Security (IPSec). As VPNs IPSec fornecem túneis seguros entre dois pares ou de um cliente para um local. Os pacotes que são considerados confidenciais devem ser enviados através desses túneis seguros. Os parâmetros que incluem algoritmo de hash, algoritmo de criptografia, tempo de vida da chave e modo devem ser usados para proteger esses pacotes confidenciais devem ser definidos especificando as características desses túneis. Em seguida, quando o peer de IPsec vê um pacote tão sensível, ele configura o túnel seguro apropriado e envia o pacote por meio desse túnel para o peer remoto.

Quando o IPsec é implementado em um firewall ou roteador, ele fornece uma segurança forte que pode ser aplicada a todo o tráfego que atravessa o perímetro. O tráfego dentro de uma empresa ou grupo de trabalho não incorre na sobrecarga do processamento relacionado à segurança.

Para que as duas extremidades de um túnel VPN sejam criptografadas e estabelecidas com êxito, ambas precisam concordar com os métodos de criptografia, descriptografia e autenticação. O perfil IPsec é a configuração central no IPsec que define os algoritmos como criptografia, autenticação e grupo Diffie-Hellman (DH) para a negociação das Fases I e II no modo automático, bem como no modo de chaveamento manual.

Componentes importantes do IPsec incluem a Fase 1 e a Fase 2 do Internet Key Exchange (IKE).

A finalidade básica da fase um do IKE é autenticar os peers IPSec e configurar um canal seguro entre os peers para permitir trocas de IKE. A fase um do IKE executa as seguintes funções:

- Autentica e protege as identidades dos pares IPSec
- Negocia uma política de Associações de Segurança (SA) IKE correspondente entre pares para proteger a troca IKE
- Executa uma troca Diffie-Hellman autenticada com o resultado final de ter chaves secretas compartilhadas correspondentes
- Configura um túnel seguro para negociar parâmetros da fase dois do IKE
- Ocorre em dois modos, principal e agressivo

A finalidade da fase dois do IKE é negociar SAs de IPSec para configurar o túnel de IPSec. A fase dois do IKE executa as seguintes funções:

- Negocia parâmetros IPSec SA protegidos por uma SA IKE existente
- Estabelece associações de segurança IPSec
- Renegociar periodicamente SAs de IPSec para garantir a segurança
- Executa opcionalmente uma troca adicional Diffie-Hellman
- Apenas um modo usado, modo rápido

Se o PFS (Perfect Forward Secrecy) for especificado na política IPSec, uma nova troca DH é realizada com cada modo rápido, fornecendo material de chaveamento que tem maior entropia (vida do material-chave) e, portanto, maior resistência a ataques criptográficos. Cada troca de DH requer grandes exponenciações, aumentando assim o uso da CPU e exigindo um custo de desempenho.

- Configuração do Perfil de Segurança de Protocolo Internet (IPSec - Internet Protocol Security) em um RV34x Series Router
- Configuração de perfis IPSec (modo de digitação automática) no RV160 e RV260

- Configurando o modo de chave manual de perfil IPsec em roteadores RV160 e RV260

Point-to-Point Tunneling Protocol (PPTP)

O PPTP é um protocolo de rede usado para criar túneis VPN entre redes públicas. Os servidores PPTP também são conhecidos como servidores VPDN (Virtual Private Dialup Network). O PPTP às vezes é usado em outros protocolos porque é mais rápido e tem a capacidade de trabalhar em dispositivos móveis. No entanto, é importante observar que ele não é tão seguro quanto outros tipos de VPNs. Há vários métodos para conexão com contas do tipo PPTP. Clique nos links para saber mais:

- Configurar um servidor PPTP (Point-to-Point Tunneling Protocol) no roteador série Rv34x
- Configurar o Servidor de Protocolo de Encapsulamento Ponto a Ponto (PPTP - Point to Point Tunneling Protocol) nas séries de roteadores VPN RV320 e RV325 no Windows

Encapsulamento de roteamento genérico

O Generic Routing Encapsulation (GRE) é um protocolo de tunelamento que fornece uma abordagem genérica simples para transportar pacotes de um protocolo sobre outro por meio de encapsulamento.

O GRE encapsula uma carga útil, isto é, um pacote interno que precisa ser entregue a uma rede de destino dentro de um pacote IP externo. O túnel GRE se comporta como um link ponto-a-ponto virtual que tem dois pontos finais identificados pelo endereço origem e destino do túnel.

Os pontos de extremidade do túnel enviam payloads através de túneis GRE, roteando pacotes encapsulados através de redes IP de intervenção. Outros roteadores IP ao longo do caminho não analisam o payload (o pacote interno); eles apenas analisam o pacote IP externo à medida que o encaminham em direção ao ponto final do túnel GRE. Ao alcançar o ponto final do túnel, o encapsulamento de GRE é removido e o payload é encaminhado ao destino final do pacote.

O encapsulamento de datagramas em uma rede é feito por várias razões, como quando um servidor de origem deseja influenciar a rota que um pacote toma para alcançar o host de destino. O servidor de origem também é conhecido como servidor de encapsulamento.

O encapsulamento IP-em-IP envolve a inserção de um cabeçalho IP externo sobre o cabeçalho IP existente. O endereço origem e destino no cabeçalho IP externo apontam para os pontos finais do túnel IP-em-IP. A pilha de cabeçalhos IP é usada para direcionar o pacote por um caminho predeterminado até o destino, desde que o administrador de rede conheça os endereços de loopback dos roteadores que transportam o pacote.

Esse mecanismo de tunelamento pode ser usado para determinar a disponibilidade e a latência para a maioria das arquiteturas de rede. Deve-se observar que todo o caminho da origem até o destino não precisa ser incluído nos cabeçalhos, mas um segmento da rede pode ser escolhido para direcionar os pacotes.

Protocolo de túnel camada 2

O L2TP não fornece mecanismos de criptografia para o tráfego que ele encaminha. Em vez disso, ele depende de outros protocolos de segurança, como o IPSec, para criptografar os dados.

Um túnel L2TP é estabelecido entre o Concentrador de Acesso L2TP (LAC) e o Servidor de Rede L2TP (LNS). Um túnel IPSec também é estabelecido entre esses dispositivos e todo o tráfego do túnel L2TP é criptografado usando IPSec.

Alguns termos-chave com L2TP:

- **CHAP -** Challenge Handshake Authentication Protocol (Protocolo de autenticação de handshake de

desafio). Um protocolo de autenticação ponto a ponto (PPP).

- **Concentrador de Acesso L2TP (LAC) -** Um LAC pode ser um servidor de acesso à rede Cisco conectado à rede telefônica pública comutada (PSTN). O LAC precisa apenas implementar mídia para operação sobre L2TP. Um LAC pode se conectar ao LNS usando uma rede local ou uma rede de longa distância, como Frame Relay público ou privado. O LAC é o iniciador de chamadas de entrada e o receptor de chamadas de saída.
- **Servidor de rede L2TP (LNS - L2TP Network Server) -** Quase todos os roteadores Cisco conectados a uma rede local ou a uma rede de longa distância, como Frame Relay público ou privado, podem atuar como um LNS. É o lado do servidor do protocolo L2TP e deve operar em qualquer plataforma que encerre sessões PPP. O LNS é o iniciador de chamadas de saída e o receptor de chamadas de entrada. A Figura 1 descreve a rotina de chamada entre o LAC e o LNS.
- **Rede de Discagem Privada Virtual (VPDN - Virtual Private Dial Network) -** Um tipo de VPN de acesso que usa o PPP para fornecer o serviço.

Para obter mais informações sobre L2TP, clique nos seguintes links:

- Definir as configurações L2TP WAN no roteador RV34x
- Guia de configuração de rede de longa distância: serviços de camada 2, Cisco IOS XE versão 3S

VPNs compatíveis com os roteadores VPN Cisco RV Series

	RV34X	RV32X	RV160X/RV260X
IPSec (IKEv1)			
ShrewSoftName	Yes	Yes	Yes
Arco-verde	Yes	Yes	Yes
cliente interno Mac	Yes	Yes	No
iPhone/iPad	Yes	Yes	No
Android	Yes	Yes	Yes
L2TP/IPSec	Sim (PAP)	No	No
PPTP	Sim (PAP)	Sim*	Sim (PAP)
Outro			
AnyConnect	Yes	No	No
Openvpn	No	Yes	Yes
IKEv2			
Windows	Sim*	No	Sim*
Mac	Yes	No	Yes
iPhone	Yes	No	Yes
Android	Yes	No	Yes

Tecnologia VPN	Dispositivos suportados	Clientes suportados*	Detalhes e avisos
IPSec (IKEv1)	RV34X, RV32X, RV160X/RV260X	Nativo: Mac, iPhone, iPad, Android	Mais fácil de configurar, solucionar problemas e oferecer suporte. Ele está disponível em todos os roteadores, é simples de configurar (em sua maioria), tem o melhor registro para solucionar problemas. E inclui a maioria dos dispositivos. É por isso que

		Outros: EasyVPN (Cisco VPN Client), ShrewSoft, Greenbow	geralmente recomendamos ShrewSoft (livre e funciona) e Greenbow (não livre, mas funciona). Para o Windows, temos clientes ShrewSoft e Greenbow como opções, já que o Windows não tem um cliente VPN nativo IPSec puro. Para a ShrewSoft e a Greenbow, é um pouco mais envolvido, mas não é difícil. Uma vez configurado pela primeira vez, os perfis de cliente podem ser exportados e importados em outros clientes. Para roteadores RV160X/RV260X, como não temos a opção Easy VPN, precisamos usar a opção 3rd Party Client, que não funciona com Mac, iPhone ou iPad. No entanto, podemos configurar clientes ShrewSoft, Greenbow e Android para se conectar. Para clientes Mac, iPhone e iPad, eu recomendo IKEv2 (veja abaixo).
AnyConnect	RV34X	Windows, Mac, iPhone, iPad, Android	Alguns clientes solicitam uma solução completa da Cisco e é isso. É simples de configurar, tem registro, mas pode ser um desafio entender os registros. Requer custo incorrido do requisito de licenciamento do cliente. É uma solução completa da Cisco e é atualizada. A solução de problemas não é tão fácil quanto o IPSec, mas melhor do que as outras opções de VPN.
L2TP/IPSec	RV34X	Nativo: Windows	Isso é o que recomendarei para clientes que precisam usar o cliente VPN integrado no Windows. Duas ressalvas são: 1. Oferecemos suporte apenas à autenticação PAP ao usar a Autenticação Local. Temos que entrar em cada cliente e selecionar criptografia opcional ou não, desabilitar opções MS-CHAP e habilitar o PAP. Isso significa que o nome de usuário/senha são enviados sem formatação. Não é um grande negócio, já que tudo é criptografado com IPSec e precisa ser configurado em cada cliente. No Windows, isso é configurável, mas não em dispositivos Mac, iPhone, iPad ou Android, portanto, realmente só pode ser usado por clientes Windows, a menos que eles tenham um servidor de autenticação externo como Radius ou LDAP. 2. Se o roteador estiver por trás de um dispositivo NAT, a conexão falhará em máquinas Windows. A solução é criar uma chave de registro em cada cliente para permitir o NAT no cliente e no roteador.

IPSec (IKEv2)	RV34X, RV160X/RV260X	Nativo: Windows, Mac, iPhone, iPad, Android	O cliente nativo do Windows para IKEv2 requer autenticação de certificado, que requer uma infraestrutura de PKI, pois o roteador e todos os clientes precisam ter certificados da mesma CA (ou de outra CA confiável). Para aqueles que desejam usar IKEv2, configuramos isso para seus dispositivos Mac, iPhone, iPad e Android e geralmente configuramos IKEv1 para suas máquinas Windows (ShrewSoft, Greenbow ou L2TP/IPSec).
VPN aberta	RV32X, RV160X/RV260X	O Open VPN é o cliente	Mais difícil de configurar, de solucionar problemas e de oferecer suporte. Suportado em RV160X/RV260X e RV320. A configuração é mais complexa do que o IPSec ou o AnyConnect, especialmente se eles usarem certificados, o que a maioria faz. A solução de problemas é mais difícil, já que não temos nenhum log útil no roteador e dependemos dos logs do cliente. Além disso, as atualizações da versão do cliente OpenVPN alteraram sem aviso quais certificados eles aceitaram. Além disso, descobrimos que isso não funciona nos Chromebooks e tivemos que ir para uma solução IPSec.

* Nós testamos quantas combinações pudermos, se houver uma combinação específica de hardware/software, entre em contato aqui. Caso contrário, consulte o guia de configuração relacionado por dispositivo para obter a versão testada mais recente.

Certificados

Você já visitou um site e recebeu um aviso de que ele não é seguro? Isso não deixa você confiante de que suas informações privadas estão seguras, e não está! Se um site for seguro, você verá um ícone de cadeado fechado antes do nome do site. Este é um símbolo de que o site foi verificado como seguro. Certifique-se de ver o ícone de cadeado fechado. O mesmo vale para a sua VPN.

Ao configurar uma VPN, você deve obter um certificado de uma CA (Certificate Authority, autoridade de certificação). Os certificados são comprados de sites de terceiros e usados para autenticação. É uma maneira oficial de provar que seu site é seguro. Essencialmente, a CA é uma fonte confiável que verifica se você é uma empresa legítima e se é confiável. Para uma VPN, você só precisa de um certificado de nível inferior com um custo mínimo. Você é submetido a check-out pela CA e, depois que a CA verificar suas informações, ela emitirá o Certificado para você. Este certificado pode ser baixado como um arquivo no seu computador. Em seguida, você pode ir para o roteador (ou servidor VPN) e carregá-lo lá.

A CA usa Public Key Infrastructure (PKI) ao emitir certificados digitais, que usa criptografia de chave pública ou chave privada para garantir a segurança. As autoridades de certificação são responsáveis por gerenciar solicitações de certificado e emitir certificados digitais. Algumas CAs de terceiros incluem IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust e Verisign.

É importante que todos os gateways em uma VPN usem o mesmo algoritmo, caso contrário eles não poderão se comunicar. Para simplificar, recomenda-se que todos os certificados sejam adquiridos do mesmo

terceiro confiável. Isso torna vários certificados mais fáceis de gerenciar, pois eles precisam ser renovados manualmente.

Observação: os clientes geralmente não precisam de um certificado para usar uma VPN; é apenas para verificação através do roteador. Uma exceção a isso é o OpenVPN, que requer um certificado de cliente.

Algumas pequenas empresas optam por usar uma senha ou uma chave pré-compartilhada em vez de um Certificado para simplificar. Isso é menos seguro, mas pode ser configurado sem custo.

Mais informações sobre certificados podem ser encontradas nos links abaixo:

- Certificado (Importar/Exportar/Gerar CSR) no RV160 e RV260 Series Router
- Substitua o certificado autoassinado padrão por um certificado SSL de terceiros no RV34x Series Router

VPN site a site em um roteador

Para o roteador local e remoto, é importante verificar se a chave pré-compartilhada (PSK)/senha/certificado usados para a conexão VPN e se todas as configurações de segurança correspondem. Se um ou mais roteadores usarem o Network Address Translation (NAT), que a maioria dos roteadores da série Cisco RV usa, você precisará fazer isenções de firewall para a conexão VPN nos roteadores local e remoto.

Confira estes artigos site a site para obter mais informações:

- Configuração da VPN Site a Site no RV34x
- Configurar uma VPN site a site em um roteador RV340 ou RV345
- Cisco Tech Talk: Configurando VPN Site a Site em RV340 Series Routers (vídeo)
- Configuração de VPN Site a Site em um roteador RV160 e RV260 (Configurações Básicas)
- VPN site a site no roteador RV160 e RV260 (configurações avançadas e failover)

VPN Cliente a Site em um Roteador

Para que uma VPN possa ser configurada no lado do cliente, um administrador precisa configurá-la no roteador.

Clique para visualizar estes artigos de configuração do roteador:

- Configurando o assistente de configuração de VPN nos roteadores RV160 e RV260
- Configuração do cliente Soft VPN Shrew com o RV160 e o RV260
- Cisco Tech Talk: Configuração de Shrew Soft VPN em RV160 e RV260 (vídeo)
- Configurar e usar o cliente VPN IPsec GreenBow para conectar com roteadores RV160 e RV260

Criar um perfil de cliente para site

Em uma conexão VPN Cliente a Site, os clientes da Internet podem se conectar ao servidor para acessar a rede corporativa ou LAN atrás do servidor, mas ainda manter a segurança da rede e seus recursos. Esse recurso é muito útil, pois cria um novo túnel VPN que permite que funcionários remotos e pessoas em viagem de negócios acessem sua rede usando um software cliente VPN sem comprometer a privacidade e a segurança. Os artigos a seguir são específicos para os RV34x Series Routers:

- Configure a conexão VPN (Virtual Private Network) de cliente para site no RV34x Series Router
- Configurar a conectividade da rede virtual privada (VPN) do AnyConnect no roteador da série RV34x

A VPN de cliente para site não funcionará se o encaminhamento de portas estiver definido para *todo o*

tráfego de origem e destino *todo o tráfego*.

Grupos de usuários

Os grupos de usuários são criados no roteador para uma coleção de usuários que compartilham o mesmo conjunto de serviços. Esses grupos de usuários incluem opções para o grupo, como uma lista de permissões sobre como eles podem acessar a VPN. Dependendo do dispositivo, o PPTP, a VPN IPSec de site a site e a VPN IPSec de cliente a site podem ser permitidos. Por exemplo, o RV260 tem opções que incluem o OpenVPN, mas L2TP não é suportado. A série RV340 é equipada com AnyConnect para VPN SSL, bem como Captive Portal ou EZ VPN.

Essas configurações permitem que os administradores controlem e filtrem para que somente usuários autorizados possam acessar a rede. Shrew Soft e TheGreenBow são dois dos clientes VPN mais comuns disponíveis para download. Eles precisam ser configurados com base nas configurações de VPN do roteador para que possam estabelecer com êxito um túnel VPN. O artigo a seguir aborda especificamente a criação de um grupo de usuários:

- Crie um grupo de usuários para configuração da VPN no roteador RV34x

Ao configurar grupos de usuários para uma VPN, certifique-se de deixar a conta admin padrão no grupo admin e criar uma nova conta de usuário e grupo de usuários para VPN. Se você mover sua conta de administrador para um grupo diferente, impedirá que você faça login no roteador. Como resultado, você teria que fazer uma redefinição de fábrica e configurar para esse roteador novamente, deixando a conta admin padrão no grupo admin sozinho.

Contas do usuário

As Contas de Usuário são criadas no roteador para permitir a autenticação de usuários locais usando o banco de dados local para vários serviços como PPTP, VPN Client, logon de Interface Gráfica de Usuário (GUI - Graphical User Interface) da Web e Rede Virtual Privada (SSLVPN - Virtual Private Network) de Camada de Soquetes Segura. Isso permite que os administradores controlem e filtrem usuários autorizados apenas para acessar a rede. O artigo a seguir aborda especificamente a criação de uma conta de usuário:

- Crie uma conta de usuário para a configuração do cliente VPN no roteador RV34x

Cliente a site no local do cliente

Em uma conexão VPN Cliente a Site, os clientes da Internet podem se conectar ao servidor para acessar a rede corporativa ou LAN atrás do servidor, mas ainda mantêm a segurança da rede e seus recursos. Esse recurso é muito útil, pois cria um novo túnel VPN que permite que funcionários remotos e pessoas que viajam a negócios acessem sua rede usando um software cliente VPN sem comprometer a privacidade e a segurança. A VPN é configurada para criptografar e descriptografar dados à medida que são enviados e recebidos.

O aplicativo AnyConnect funciona com VPN SSL e é usado especificamente com os roteadores RV34x. Não está disponível com outras séries RV de roteadores. Começando com a versão 1.0.3.15, uma licença de roteador não é mais necessária, mas as licenças precisam ser adquiridas para o lado do cliente da VPN. Para obter mais informações sobre o Cisco AnyConnect Secure Mobility Client, clique aqui. Para obter instruções sobre a instalação, selecione um dos seguintes artigos:

- Instalar o Cisco AnyConnect Secure Mobility Client em um computador Mac
- Instalar o Cisco AnyConnect Secure Mobility Client em um computador com Windows

Há alguns aplicativos de terceiros que podem ser utilizados para VPN cliente a site com todos os roteadores

da série RV. Como dito anteriormente, a Cisco não oferece suporte a esses aplicativos; essas informações estão sendo fornecidas para fins de orientação.

O GreenBow VPN Client é um aplicativo cliente VPN de terceiros que possibilita que um dispositivo de host configure uma conexão segura para o túnel IPsec de cliente para site ou SSL. Este é um aplicativo pago que inclui suporte.

- Configurar e usar o cliente VPN IPsec GreenBow para conectar com roteadores RV160 e RV260

O OpenVPN é um aplicativo gratuito de código aberto que pode ser configurado e usado para uma VPN SSL. Ele usa uma conexão cliente-servidor para fornecer comunicações seguras entre um servidor e um local de cliente remoto pela Internet.

- OpenVPN em roteadores RV160 e RV260

Shrew Soft é um aplicativo gratuito de código aberto que pode ser configurado e usado para uma VPN IPsec também. Ele usa uma conexão cliente-servidor para fornecer comunicações seguras entre um servidor e um local de cliente remoto pela Internet.

- Configuração do cliente Soft VPN Shrew com o RV160 e o RV260

O Easy VPN era comumente usado em roteadores RV32x. Aqui estão algumas informações para referência:

- Configurar Easy Client para Rede Virtual Privada (VPN - Virtual Private Network) de Gateway em RV320 e RV325 VPN Router Series
- Perguntas e respostas sobre o Cisco Easy VPN
- Easy VPN em roteadores baseados no software Cisco IOS

Assistente de configuração

Os roteadores Cisco série RV mais recentes vêm com um Assistente de configuração de VPN que o orienta através das etapas de configuração. O Assistente para configuração de VPN permite configurar conexões VPN básicas de LAN para LAN e de acesso remoto e atribuir chaves pré-compartilhadas ou certificados digitais para autenticação. Confira estes artigos para obter mais informações:

- Configurando o assistente de configuração de VPN no RV160 e RV260
- Configurar a Conexão VPN (Rede Virtual Privada) usando o Assistente para Configuração no RV34x Series Router

Conclusão

Este artigo o levou a uma melhor compreensão das VPNs, além de dicas para colocá-lo no caminho. Agora você deve estar pronto para configurar o seu próprio! Reserve um tempo para visualizar os links e decidir a melhor maneira de configurar uma VPN em seu roteador Cisco série RV.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.