Cisco VPN 3000 Concentrator FAQ

Índice

Introdução

Este documento responde perguntas frequentes (FAQ) sobre o Cisco VPN 3000 Series Concentrator.

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

Geral

Q. O que significa a mensagem de erro "Lost Service"?

A. Se não houver tráfego enviado entre o VPN Concentrator e o VPN Client por um período de tempo, um pacote do Dead Peer Detection (DPD) será enviado do VPN Concentrator para o VPN Client para garantir que seu peer ainda esteja lá. Se houver um problema de conectividade entre os dois peers onde o VPN Client não responde ao VPN Concentrator, o VPN Concentrator continuará a enviar pacotes DPD durante algum tempo. Isso encerrará o túnel e gerará o erro se não receber uma resposta durante esse tempo. Consulte o bug da Cisco ID CSCdz45586 (somente clientes registrados).

O erro deve ser semelhante a este:

```
SEV=4 AUTH/28 RPT=381 XXX.XXX.XXX.XX User [SomeUser] disconnected:
Duration: HH:MM:SS Bytes xmt: 19560 Bytes rcv: 17704 Reason:
Lost Service YYYY/MM/DD HH:MM:SS XXX.XXX.XXX.XXX
syslog notice
45549 MM/DD/YYYY HH:MM:SS SEV=4 IKE/123 RPT=XXX.XXX.XXX.XXX
Group [SomeDefault] User [SomeUser]
IKE lost contact with remote peer, deleting connection (keepalive type: DPD)
```

Causa: O peer IKE remoto não respondeu aos keepalives dentro da janela de tempo esperada. Portanto, a conexão com o peer IKE foi eliminada. A mensagem inclui o mecanismo de keepalive usado. Este problema é reproduzido somente quando a interface pública é desconectada durante uma sessão do túnel ativo. O cliente necessita monitorar sua conectividade de rede à medida que estes eventos são gerados para identificar a causa raiz de seu problema de conectividade de rede potencial.

Desabilite o keepalive de IKE ao ir para **%System Root%\Program Files\Cisco Systems\VPN Client\Profiles** no PC cliente que está experimentando o problema e edite o arquivo **PCF** (onde aplicável) para a conexão.

Altere **'ForceKeepAlives=0'** (padrão) para **'ForceKeepAlives=1'**.

Se o problema persistir, abra uma solicitação de serviço junto ao Suporte Técnico da Cisco e forneça o "Log Viewer" do cliente e os log do VPN Concentrator quando o problema ocorre.

Q. Qual é o significado da mensagem de erro "q_send failures detected for EMQ1 queue"?

A. Esta mensagem de erro ocorre quando há um excesso de eventos/informações de depuração no buffer. Não há nenhum impacto negativo, a não ser a possível perda de algumas mensagens de evento. Tente reduzir os eventos ao número mínimo necessário para prevenir a mensagem.

Q. Meu grupo eliminado ainda aparece na configuração do VPN Concentrator. Como posso eliminá-lo?

A. Copie a configuração em um editor de texto (tal como o bloco de notas) e manualmente edite ou suprima da informação afetada do grupo denotada perto **[ipaddrgrouppool #.0]**. Salve a configuração e transfira-a para o VPN Concentrator. Um exemplo é mostrado aqui.

```
!--- Change to 14.1 or any other number that is not in use !--- any number other than 0).
[ipaddrgrouppool 14.0] rowstatus=1 rangename= startaddr=172.18.124.1 endaddr=172.18.124.2
```

Q. É possível ter servidores SDI principais múltiplos?

A. Os VPN 3000 Concentrators podem baixar somente um arquivo de segredo de nó de cada vez. Na versão do SDI anterior à 5.0, você pode adicionar vários servidores SDI, mas todos eles devem compartilhar o mesmo arquivo de segredo de nó (pense neles como os servidores principais e de backup). Na versão do SDI 5.0, você pode entrar somente um servidor SDI principal (os servidores de backup são listados no arquivo de segredo de nó) e servidores de réplica.

Q. Estou recebendo a mensagem de erro "SSL certificate will expire in 28 days" do emissor. O que devo fazer?

A. Essa mensagem indica que o seu certificado SSL (Secure Socket Layer) vencerá dentro de 28 dias. Esse certificado é usado para navegar no gerenciamento da Web via HTTPS. Você pode deixar o certificado com as configurações padrão, ou você pode configurar opções diferentes antes de gerar o certificado novo. Selecione **Configuration > System > Management Protocols > SSL** para fazer isso. Selecione **Administration > Certificate Management** e clique em **Generate** para renovar o certificado.

Se você estiver preocupado com a segurança no Concentrador VPN e quiser impedir o acesso não autorizado, desabilite o HTTP e/ou HTTPS na interface pública indo para Configuration > Policy Management > Traffic Management > Filters. Se precisar acessar seu VPN Concentrator pela Internet, via HTTP ou HTTPS, especifique o acesso com base no endereço de origem indo para Administration > Access Rights > Access Control List (Administração > Direitos de Acesso > Lista de Controle de Acesso). Você pode usar o menu de ajuda no canto superior direito da janela

para obter mais informações.

Q. Como posso eu ver as informações de usuário no banco de dados de usuários interno? Elas não são visíveis quando eu olho no arquivo de configuração.

A. Selecione a **administração > direitos de acesso > ajustes do acesso**, escolha o **arquivo de configuração Encryption=None**, e salvar a configuração para ver usuários e senhas. Você deveria poder procurar o usuário específico.

Q. Quantos usuários podem o depósito de base de dados interno?

A. O número de usuários depende da versão, especificado na seção **Configuration > User Management** do Guia do Usuário do VPN 3000 Concentrator. Um total de 100 usuários ou grupos (a soma dos usuários e dos grupos deve igualar 100 ou menos) é possível nos VPN 3000 Releases 2.2 a 2.5.2. Nos VPN 3000 Releases 3.0 ou posteriores, o número para os 3005 e 3015 Concentrators permanece 100. Para o VPN 3030 e 3020 Concentrator, o número é 500. Para os VPN 3060 ou 3080 Concentrators, o número é 1000. Além disso, usar um servidor de autenticação externa melhora a dimensionabilidade e a capacidade de gerenciamento.

Q. Qual é a diferença entre o gateway padrão do túnel e o gateway padrão?

A. O VPN 3000 Concentrator usa o gateway padrão do túnel para rotear os usuários do túnel na rede privada (normalmente o roteador interno). O VPN Concentrator usa o gateway padrão para rotear pacotes para a Internet (geralmente o roteador externo).

Q. Se eu colocar meu VPN 3000 Concentrator atrás de um firewall ou roteador que esteja executando listas de controle de acesso, preciso permitir o acesso de quais portas e protocolos?

A. Este gráfico lista as portas e os protocolos.

Serviço	Número de Protocolo	Porta de origem	Porta de Destino
Conexão de Controle de PPTP	6 (TCP)	1023	1723
Encapsulamento de Túnel PPTP	47 (GRE)	N/A	N/A
Gerenciamento Chave de ISAKMP/IPSec	17 (UDP)	500	500
Encapsulamento do Túnel de IPsec	50 (ESP)	N/A	N/A
Transparência de NAT de IPSec	17 (UDP)	10000 (padrão)	10000 (padrão)

Nota: A porta de transparência da tradução de endereço de rede (NAT) é configurável para qualquer valor no intervalo de 4001 a 49151. Nas versões 3.5 ou mais recentes, você pode configurar o IPsec sobre TCP ao ir para **Configuration > System > Tunneling Protocols > IPSec > IPSec over TCP**. É possível digitar até 10 portas TCP separadas por vírgulas (1 a 65535). Se a opção estiver configurada, certifique-se de que essas portas sejam permitidas no firewall ou

roteador que estiver executando as listas de controle de acesso.

Q. Como posso restaurar o VPN Concentrator para os padrões de fábrica?

A. Na tela File Management, elimine o arquivo "config" e reinicialize. Se este arquivo for excluído acidentalmente, uma cópia de backup "config.bak" será mantida.

Q. Posso usar o TACACS+ para a autenticação administrativa? O que devo ter em mente ao fazer isso?

A. Sim, a partir do VPN 3000 Concentrator versão 3.0, é possível utilizar o TACACS+ para fins de autenticação administrativa. Depois de configurar o TACACS+, certifique-se de testar autenticação antes de fazer logout. A configuração imprópria do TACACS+ poderá impedir seu acesso. Isso exigirá um início de sessão via porta de console para desabilitar o TACACS+ e corrigir o problema.

Q. O que eu faço quando esqueço a senha administrativa?

A. Nas versões 2.5.1 e mais recentes, conecte um PC à porta de console do VPN Concentrator usando um cabo serial RS-232 direto com o PC ajustado para:

- 9600 bits por segundo
- 8 bits de dados
- sem paridade
- 1 bit de parada
- controle de fluxo de hardware ativado
- Emulação de VT100

Reinicialize o VPN Concentrator. Depois que a verificação de diagnóstico estiver concluída, uma linha de três pontos (...) será mostrada no console. Pressione **CTRL-C** em até três segundos após o aparecimento dos pontos. Aparece um menu que permite restaurar as senhas do sistema para os valores padrão.

Q. Qual é a finalidade do nome do grupo e da senha do grupo?

A. O nome do grupo e a senha do grupo são usados para criar uma combinação que é, em seguida, usada para criar uma associação de segurança.

Q. Faz o proxy ARP do concentrador VPN em nome dos usuários em túnel?

A. Sim.

Q. Onde coloco o VPN 3000 Concentrator em relação ao meu firewall de rede?

A. O VPN 3000 Concentrator pode ser colocado nas seguintes posições em relação a um firewall: na frente, atrás, em paralelo ou na zona desmilitarizada (DMZ). Não é aconselhável ter as interfaces públicas e privadas na mesma LAN virtual (VLAN).

Q. Há alguma maneira de desabilitar o proxy ARP no Cisco VPN 3000

Concentrator?

A. O protocolo proxy address resolution (ARP) não pode ser desabilitado no Cisco VPN 3000 Concentrator.

Q. Onde posso encontrar os bugs registrados para o VPN 3000 Concentrator?

A. Os usuários podem usar o Bug Toolkit (clientes registrados somente) para encontrar a informação detalhada sobre erros.

Q. Onde posso encontrar exemplos de configuração do VPN 3000 Concentrator?

A. Além do que a documentação do VPN 3000 concentrator, mais exemplos de configuração podem ser encontrados na página de suporte do concentrador da Cisco VPN 3000 Series.

Q. Como posso aumentar o log para obter depurações melhores para eventos específicos?

A. Você pode ir para **Configuration > System > Events > Classes** e configurar eventos específicos (como IPsec ou PPTP) para obter depurações melhores. A depuração deve ser ativada somente durante o troubleshooting porque pode causar a degradação do desempenho. Para a depuração de IPsec, ative o IKE, IKEDBG, IPSEC, IPSECDBG, AUTH e AUTHDBG. Se estiver usando certificados, adicione a classe CERT à lista.

Q. Como posso monitorar o tráfego para o VPN 3000 Concentrator?

A. A interface HTML que vem com o VPN 3000 concentrator permite que você tenha a funcionalidade de monitoramento básica ao olhar sob **Monitoring > Sessions**. O VPN 3000 Concentrator também pode ser monitorado com o Simple Network Management Protocol (SNMP) usando um gerenciador de SNMP à sua escolha. Alternativamente, você pode comprar o Cisco VPN/Security Management Solution (VMS). O Cisco VMS fornece a funcionalidade básica para auxiliá-lo se você implantar o VPN 3000 Concentrator Series e necessitar de monitoração detalhada do acesso remoto e de VPNs site a site e é baseado no IPsec, L2TP e PPTP. Consulte VPN Security Management Solution para obter mais detalhes sobre o VMS.

Q. A Cisco VPN 3000 Concentrator Series tem um firewall integrada? Se sim, quais recursos são suportados?

A. Enquanto a série possui recursos de filtragem/porta stateless e NAT, a Cisco sugere que você use um dispositivo como o Cisco Secure PIX Firewall para o firewall corporativo.

Q. Que opções de roteamento e protocolos de VPN são suportados pelo Cisco VPN 3000 Concentrator Series?

A. A série oferece suporte a estas opções de roteamento:

- Routing Information Protocol (RIP)
- RIP2
- Open Shortest Path First (OSPF)

- rotas estáticas
- Virtual Router Redundancy Protocol (VRRP)

Os protocolos de VPN com suporte incluem o Point-to-Point Tunneling Protocol (PPTP), L2TP, L2TP / IPsec e IPsec com ou sem um dispositivo NAT entre o VPN 3000 e o cliente final. O IPsec via NAT é conhecido como transparência de NAT.

Q. Quais mecanismos/sistemas de autenticação são suportados por equipamentos Cisco VPN 3000 Concentrator para PCs clientes?

A. O domínio, o RAIO ou o proxy RADIUS, o RSA Security SecurID (SDI), os Certificados digitais, e a autenticação interna de NT são apoiados.

Q. Posso fazer a Tradução de Endereço de Rede estática (NAT) para usuários que saem através do VPN 3000 Concentrator?

A. Você só pode executar a Tradução de Endereço de Porta (PAT) para os usuários que estão saindo. Você não pode fazer o NAT estático no VPN 3000 Concentrator.

Q. Como posso atribuir um endereço IP estático a um usuário de Point-to-Point Tunneling Protocol (PPTP) ou IPsec específico através do VPN 3000 Concentrator?

A. Esta lista explica como atribuir endereços IP estáticos:

- **Usuários de PPTP**Na seção IP Address Management, além de escolher suas opções de pool ou Dynamic Host Configuration Protocol (DHCP), marque a opção **Use Client Address**. Em seguida, defina o usuário e o endereço IP no VPN 3000 Concentrator. Este usuário obtém sempre o endereço IP configurado no VPN Concentrator ao se conectar.
- **Usuários de IPsec**Na seção IP Address Management, além de escolher suas opções de pool ou DHCP, marque a opção **Use Address from Authentication Server**. Em seguida, defina o usuário e o endereço IP no VPN 3000 Concentrator. Este usuário obtém sempre o endereço IP configurado no VPN Concentrator ao se conectar. Todos os outros que pertencem ao o mesmo grupo ou a outros grupos obtêm um endereço IP do pool global ou do DHCP.Com o software Cisco VPN 3000 Concentrator versão 3.0 e posterior, há a opção de configurar um conjunto de endereços em uma base de grupo. Esse recurso também pode ajudá-lo a atribuir um endereço IP estático a um usuário específico. Se você configurar um pool para um grupo, o usuário com IP estático receberá o endereço IP atribuído a ele, e outros membros do mesmo grupo receberão endereços IP do pool do grupo. Isso se aplica somente quando você usa o VPN Concentrator como um servidor de autenticação.

Nota: Se você usa um servidor de autenticação externo, será necessário usar o servidor externo para atribuir corretamente os endereços.

Q. Quais são os problemas de compatibilidade conhecidos apresentados pelos produtos PPTP da Microsoft e pelo VPN 3000 Concentrator?

A. Essa informação é baseada no VPN 3000 Series Concentrator Software Release 3.5 ou posterior; VPN 3000 Series Concentrators, modelos 3005, 3015, 3020, 3030, 3060, 3080; e sistemas operacionais Microsoft Windows 95 e posteriores.

- **Rede de comunicação dial-up do Windows 95 (DUN) 1.2**Não há suporte à Microsoft Point-to-Point Encryption (MPPE) no DUN 1.2. Para conectar usando o MPPE, instale o Windows 95 DUN 1.3. Você pode fazer o download da atualização do Microsoft DUN 1.3 no site da Microsoft.
- **Windows NT 4.0**O Windows NT tem suporte total para conexões Point-to-Point Tunneling Protocol (PPTP) para o VPN Concentrator. É necessário o Service Pack 3 (SP3) ou posterior. Se você estiver executando o SP3, deverá instalar os patches de desempenho e segurança de PPTP. Consulte o site da Microsoft para obter informações sobre o desempenho do Microsoft PPTP e sobre o upgrade de segurança para Winnt 4.0.Observe que o Service Pack 5 de 128 bits não lida corretamente com as chaves MPPE, e o PPTP poderá falhar ao transmitir dados. Quando isso ocorre, o log de eventos mostra esta mensagem:`103 12/09/1999 09:08:01.550 SEV=6 PPP/4 RPT=3 80.50.0.4 User [ testuser ] disconnected. Experiencing excessive packet decrypt failure.`Para resolver este problema, transfira a elevação para que como obtenha o Windows NT Service Pack o mais atrasado 6a e o pacote de serviços 6a do Windows NT 4.0 disponível. Consulte o artigo da Microsoft Chaves MPPE Não Manipuladas Corretamente para uma Solicitação de MS-CHAP de 128 bitspara obter mais informações.

Q. Qual é o número máximo de filtros permitidos em um VPN 3000 Concentrator?

A. O número máximo de filtros que você pode adicionar em uma unidade VPN 30xx (mesmo uma 3030 ou 3060) é fixado em 100. Os usuários podem encontrar informações adicionais sobre este problema no bug da Cisco ID CSCdw86558 (somente clientes registrados).

Q. Qual é o número máximo de rotas na linha 30xx de VPN Concentrators?

A. O número máximo de rotas é:

- O VPN 3005 Concentrator anteriormente mantinha um máximo de 200 rotas. Esse número aumentou agora para 350 rotas. Consulte o bug da Cisco ID CSCeb35779 (somente clientes registrados) para obter detalhes.
- O VPN 3030 Concentrator foi testado com até 10.000 rotas.
- O limite da tabela de roteamento nos VPN 3030, 3060 e 3080 Concentrators é proporcional aos recursos disponíveis/memória em cada dispositivo.
- O VPN 3015 Concentrator não possui nenhum limite máximo predefinido. Isso é aplicável para o protocolo Routing Information Protocol (RIP) e Open Shortest Path First (OSPF).
- O VPN 3020 Concentrator - Devido a uma limitação da Microsoft, PCs Windows XP não são capazes de receber um grande número rotas estáticas Classless (CSR). O VPN 3000 Concentrator limita o número de CSRs que são introduzidas em uma resposta de mensagem DHCP INFORM quando configurado para agir assim. O VPN 3000 Concentrator limita o número de rotas a 28-42, dependendo da classe.

Q. Como posso limpar completamente as estatísticas de interface no VPN 3000 Concentrator?

A. Selecione a **monitoração > as estatísticas > o MIB-II > os Ethernet** e restaure as estatísticas para cancelar estatísticas para a sessão atual. Lembre-se de que isso não limpa totalmente as

estatísticas. Você precisa reinicializar para limpar de fato as estatísticas (em vez de reiniciar para fins de monitoração).

Q. Que portas devo permitir no VPN Concentrator para a comunicação do Network Time Protocol (NTP)?

A. Permita a porta 123 TCP e UDP.

Q. Quais são as funções das portas UDP 625xx?

A. As portas são usadas para a comunicação do VPN Client entre o shim real/Deterministic NDIS Extender (DNE) e a pilha TCP/IP do PC, e são somente para uso no desenvolvimento interno. Por exemplo, a porta 62515 é usada pelo VPN Client para enviar informações para o log do VPN Client. Outras funções de porta são mostradas aqui.

- 62514 - Cisco Systems, Inc. VPN Serviço ao driver IPSec do Cisco Systems
- 62515 - Cisco Systems IPsec Driver para Cisco Systems, Inc. VPN Service
- 62516 – Cisco Systems, Inc. Serviço VPN para XAUTH
- 62517 - XAUTH to Cisco Systems, Inc. VPN Service
- 62518 - Cisco Systems, Inc. VPN Service para CLI
- 62519 - CLI to Cisco Systems, Inc VPN Service
- 62520 - Cisco Systems, Inc. Serviço VPN para UI
- 62521 - UI para Serviço VPN da Cisco Systems, Inc.
- 62522 - Mensagens de registro de eventos
- 62523 Gerenciador de conexão para serviço VPN da Cisco Systems, Inc.
- 62524 - PPPTool para Serviço VPN da Cisco Systems, Inc.

Q. Posso remover a barra de flutuação WebVPN?

A. Você não pode remover a barra de ferramentas flutuante nem evitar de carregar a barra de ferramentas flutuante enquanto estabelece uma sessão de WebVPN. Isso ocorre porque quando você fecha essa janela, a sessão é terminada imediatamente e quando, você tenta iniciar sessão outra vez, a janela é carregada novamente. Esta é a maneira como as sessões de WebVPN foram originalmente projetadas. Você pode fechar a janela principal mas não é possível fechar a janela flutuante.

Software

Q. O WebVPN apoia o acesso à Web da probabilidade (OWA) 2003?

A. O apoio OWA 2003 para o WebVPN no VPN 3000 concentrator está agora disponível com transferências da versão 4.1.7 (clientes registrados somente).

Q. Onde posso obter as revisões de software mais recentes para o VPN 3000 Concentrator?

A. Todos os Cisco VPN 3000 Concentrators são enviados com o código mais atual, mas os usuários podem verificar os downloads (somente clientes registrados) para ver software mais

atual está disponível.

Consulte a página Documentação do Cisco VPN 3000 Series Concentrator para obter a documentação mais recente sobre o VPN 3000 Concentrator.

Q. Eu preciso de um servidor TFTP para fazer o upgrade do VPN 3000 Concentrator? Há uma maneira alternativa de atualizar o equipamento?

A. Além de usar o TFTP, você pode fazer o upgrade do VPN Concentrator ao baixar o software mais recente em seu disco rígido. Então, usando um navegador no sistema em que o software está, vá para **Administração > Software Upgrade** e procure o software baixado em seu disco rígido (da mesma forma como você abre um arquivo). Ao encontrá-lo, selecione a guia Upload.

Q. O que significa "k9" nos nomes de códigos mais recentes (por exemplo, "vpn3000-3.0.4.Rel-k9.bin")?

A. A designação de k9 para o nome da imagem substituiu a designação originalmente utilizada 3DES (por exemplo, vpn3000-2.5.2.F-3des.bin). Portanto, "k9" agora significa que está é uma imagem 3DES.

Q. Devo usar a opção de compactação de dados sob o grupo IPSec para todos os meus usuários?

A. A Compressão de dados aumenta o requisito de memória e a utilização CPU para cada sessão do usuário e diminui consequentemente o throughput geral do concentrador VPN. Por este motivo, a Cisco recomenda que você habilite a compactação de dados somente se cada membro do grupo for um usuário remoto que se conecte via modem. Se qualquer membro do grupo se conectar via banda larga, não habilite a compactação de dados para o grupo. Em vez disso, divida o grupo em dois grupos, um para usuários de modem e o outro para usuários de banda larga. Habilite a compactação de dados apenas para o grupo de usuários do modem.

Outros recursos avançados

Q. O Balanceamento de carga trabalha com conexões de LAN para LAN?

A. O balanceamento de carga é eficaz somente nas sessões remotas iniciadas com o Cisco VPN Software Client (Releases 3.0 e posteriores). Todos os demais clientes (PPTP, L2TP) e conexões de LAN para LAN podem se conectar a um VPN Concentrator em que o balanceamento de carga está habilitado, mas não podem participar do balanceamento de carga.

Q. Como eu descriptografo as senhas do arquivo de configuração?

A. Vá ao **Configuration > System > aos protocolos de gestão > ao XML** e então à **administração | File management e selecione o formato XML**. Use o mesmo nome, ou um nome diferente, e abra o arquivo a fim de ver as senhas.

Q. Eu posso usar o VRRP (Protocolo de Redundância do Roteador Virtual) e o balanceamento de carga juntos?

A. Você não pode utilizar o balanceamento de carga com VRRP. Em uma configuração VRRP, o dispositivo de backup permanecerá ocioso até o VPN Concentrator ativo falhar. Em uma configuração de balanceamento de carga, não há dispositivos ociosos.

Q. Todo o tráfego de VPN de cliente de acesso remoto tem que atravessar um túnel criptografado ao concentrador VPN na empresa ou no provedor de serviços? Por exemplo, pode o acesso à Web plano para outros sites ser aberto diretamente pela conexão com a Internet do ISP?

A. Sim. Esse conceito é conhecido como "divisão de tunelamento". O tunelamento dividido possibilita o acesso seguro aos recursos corporativos através de um túnel criptografado ao mesmo tempo que permite o acesso à Internet diretamente através dos recursos do ISP (isso elimina a rede corporativa do caminho do acesso à Web). O Cisco VPN 3000 Concentrator Series para o Cisco VPN Client e o VPN 3002 Hardware Client pode oferecer suporte a tunelamento por divisão. Para segurança adicional, este recurso pode ser controlado pelo administrador do VPN Concentrator, e não pelo usuário.

Q. É seguro usar tunelamento dividido?

A. O Split Tunneling permite que você tenha a conveniência de consultar o Internet quando conectado através do túnel VPN. Contudo, ele poderá representar um risco se o usuário da VPN conectado à rede corporativa estiver vulnerável a ataques. Recomendamos que, nesse caso, os usuários usem um firewall pessoal. As Release Notes de qualquer versão do VPN Cliente discutem a interoperabilidade com firewall pessoais.

Q. Como o balanceamento de carga funciona no Cisco VPN 3000 Concentrator?

A. A carga é calculada como uma porcentagem derivada das conexões ativa divididas pelas conexões máxima configuradas. O mestre tenta sempre ter a menor carga porque ele é responsável pela carga adicional (inerente) de manter todas as sessões de LAN a LAN administrativas, por calcular toda carga restante do membro do cluster e por todos os redirecionamentos de clientes.

Para um cluster funcional recém-configurado, o mestre tem uma carga de aproximadamente 1 por cento antes que todas as conexões sejam estabelecidas. Consequentemente, o mestre reorienta as conexões para o concentrador de backup até que o porcentagem de carga no backup seja mais alta que a porcentagem de carga no mestre. Por exemplo, em dois VPN 3030 Concentrators em estados "ociosos", o mestre tem uma carga de 1 por cento. O secundário recebe 30 conexões (carga de 2 por cento) antes que o mestre aceite conexões.

Para verificar se o mestre aceita conexões, vá para **Configuration > System > General > Sessions** e reduza o número máximo de conexão para um número artificialmente baixo para aumentar rapidamente a carga colocada no VPN Concentrator de backup.

Q. Quantos dispositivos de fim de cabeçalho pode o monitor VPN seguir?

A. O VPN Monitor pode rastrear 20 dispositivos headend. Em um cenário hub-and-spoke, as conexões de locais remotos são monitoradas no headend. Não há nenhuma necessidade de monitorar todos os locais e usuários remotos, já que essa informação pode ser rastreada no roteador de hub. Esses dispositivos headend podem oferece suporte a até 20.000 usuários

remotos ou 2.500 locais remotos. Um dispositivo VPN dual-homed que vá para os sites spoke conta como dois do máximo de 20 dispositivos que podem ser monitorados.

Informações Relacionadas

- Página de suporte do Cisco VPN 3000 Concentrator
- Página de suporte ao Cisco VPN 3000 Client
- Suporte Técnico e Documentação - Cisco Systems