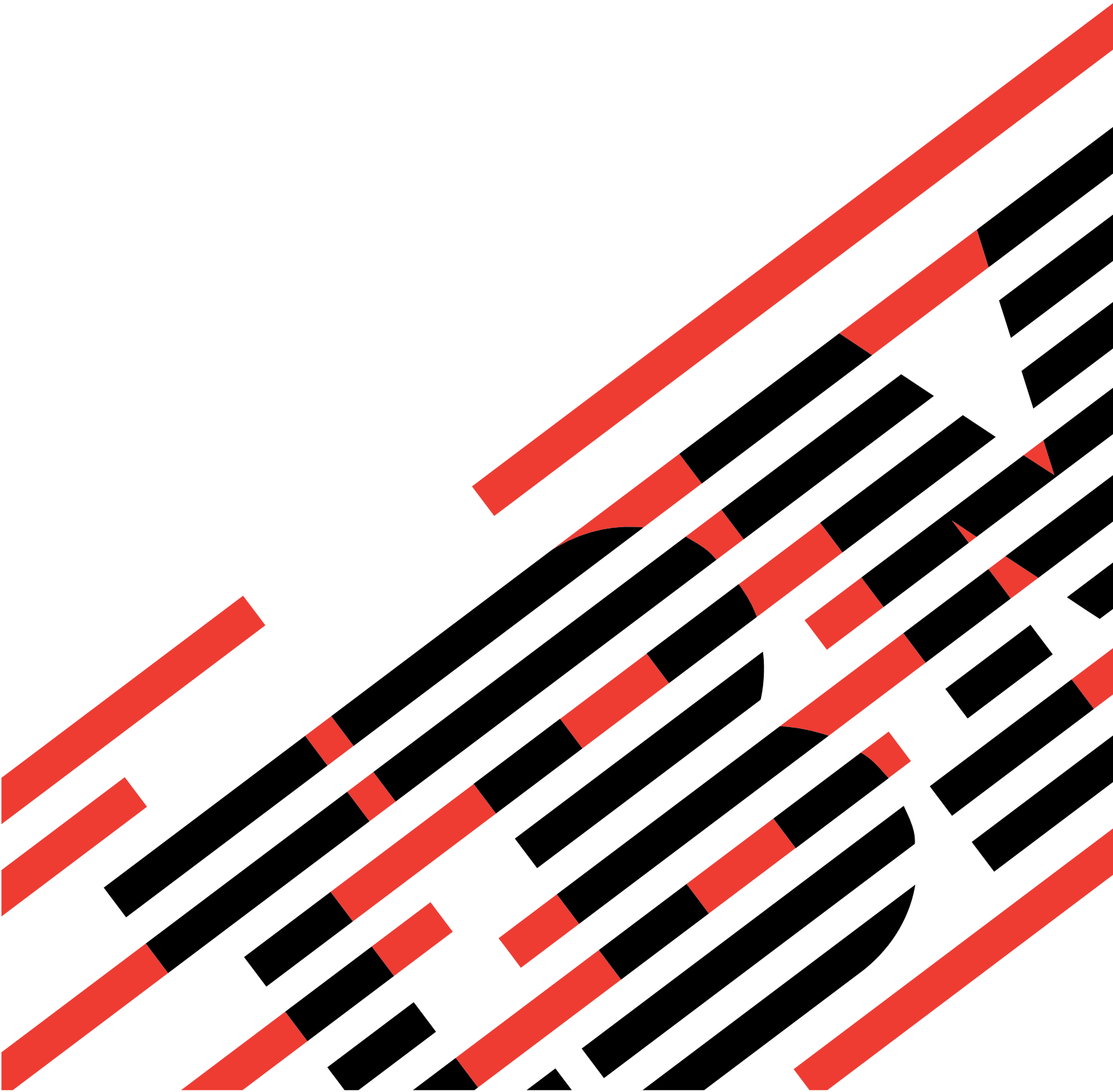
IBM

eserver

iSeries

Virtual private networking



IBM

@server

iSeries

Virtual private networking

Índice

Virtual private networking

Uma rede privada virtual (VPN) permite que uma empresa expanda a respectiva intranet privada de forma segura, através da estrutura existente de uma rede pública, como a Internet. Com a VPN, uma empresa pode controlar o tráfego da rede, enquanto proporciona importantes funções de segurança, tais como a autenticação e a privacidade dos dados.

A VPN do OS/400 é um componente de instalação opcional do iSeries Navigator, a interface gráfica do utilizador (GUI) para o OS/400. A VPN permite-lhe criar um caminho seguro extremo a extremo entre qualquer combinação de sistema central e porta de ligação. A VPN do OS/400 utiliza métodos de autenticação, algoritmos de codificação e outras protecções para assegurar que os dados enviados entre os dois extremos de uma ligação permanecem a salvo.

A VPN é executada na camada de rede do modelo de pilha de comunicações em camadas de TCP/IP. Mais especificamente, a VPN utiliza a estrutura aberta Arquitectura do IP Security (IPSec). O IPSec fornece funções de segurança de base para a Internet, bem como blocos de construção flexíveis a partir dos quais pode criar redes privadas virtuais sólidas e seguras.

A VPN suporta ainda as soluções para VPN do Protocolo Layer 2 Tunnel (L2TP). As ligações do L2TP, também denominadas linhas virtuais, proporcionam um acesso pouco dispendioso a utilizadores remotos, ao permitir a um servidor de rede de uma empresa gerir os endereços de IP atribuídos aos respectivos utilizadores remotos. Além disso, as ligações do L2TP proporcionam um acesso seguro ao sistema ou à rede, quando são protegidos com o IPSec.

É importante compreender o impacto que uma VPN terá em toda a rede. Um planeamento e uma implementação adequados são fundamentais para o sucesso. Deve rever estes tópicos para certificar-se de que sabe como funcionam as VPNs e como poderá utilizá-las:

O que há de novo na V5R2?
Este tópico descreve quais são as informações novas ou que foram significativamente alteradas nesta edição.

Imprimir este tópico
Se preferir uma versão destas informações em suporte físico, consulte este capítulo para imprimir o ficheiro em PDF.

Cenários da VPN
Reveja este cenários para se familiarizar com os tipos básicos de VPN e com os passos que terão de ser executados na configuração dos mesmos.

Conceitos da VPN
É importante que tenha, pelo menos, conhecimentos básicos sobre as tecnologias VPN standard. Este tópico proporciona-lhe informações de concepção sobre os protocolos que a VPN utiliza na sua implementação.

Planear a VPN
O primeiro passo para utilizar com sucesso a VPN, é o planeamento. Este tópico fornece mais informações sobre a migração de edições anteriores, requisitos de configuração e ligações para um consultor de planeamento que irá gerar uma folha de trabalho personalizada de acordo com as suas especificações.

Configurar a VPN
Depois do planeamento da VPN, pode começar a configurá-la. Este tópico fornece uma descrição geral do que pode fazer com a VPN e como fazê-lo.

Administrar a VPN
Este tópico descreve as várias tarefas que pode executar para gerir as ligações VPN activas, incluindo a forma de alterá-las, supervisioná-las ou eliminá-las.

Resolução de problemas da VPN
Consulte este tópico quando tiver problemas com as ligações VPN.

Informações relacionadas com a VPN
Consulte esta referência para obter outras fontes de informação sobre a VPN, assim como outros tópicos relacionados.

O que há de novo na V5R2

Os melhoramentos da função da virtual private networking (VPN) da Versão 5 Edição 2 (V5R2), incluem:

- A NAT compatível com IPSec, também conhecida como encapsulamento UDP, para indicar as diversas incompatibilidades entre o IPSec a as tecnologias de conversão de endereços da rede (NAT). O encapsulamento UDP permite que o iSeries esteja atrás de uma firewall que utilize NAT. Ao contrário de edições anteriores da VPN do OS/400, já não é necessário colocar o iSeries no perímetro da rede, utilizar um endereço público ou utilizar um IP virtual para criar ligações de VPN.
- Filtragem de políticas dinâmica. Pode criar uma VPN que não contenha uma regra de filtragem de políticas associada. O sistema irá gerir todos os filtros de forma dinâmica para a ligação, o que quer dizer que, não tem de configurar regras de pacotes para ter uma ligação da VPN.
- Assistente Migrar Filtragem de Políticas. Se actualizou o sistema da V4R4 ou da V4R5 e pretende utilizar as regras anteriormente carregada no sistema antes da actualização, deve utilizar o assistente Migrar Regras de Políticas para remover a filtragem de políticas dos ficheiros de regras de pacotes criados. O assistente irá introduzir filtragem de políticas equivalentes no conjunto de filtragem de políticas gerado pela VPN. Isto irá ajudar a garantir que as filtragens de políticas antigas e as novas irão funcionar em conjunto da forma pretendida.
- Algoritmo Advanced Encryption Standard (AES). A VPN do OS/400 suporta agora AES para protecção de dados.

As alterações do tópico da VPN da V5R2 incluem:

- Cenários adicionais para melhor compreender o funcionamento da VPN numa definição corporativa:
- Actualizações no consultor de planeamento da VPN, o qual ajuda a determinar o tipo de VPN que deve ser criado para corresponder a determinadas necessidades empresariais. O consultor sugere ainda os passos a executar para configurar a VPN.

Para encontrar mais informações sobre o que há de novo ou alterado nesta edição, consulte o

Memorando para Utilizadores  .

Cenários da VPN

Reveja as seguintes opções para ficar familiarizado com os aspectos técnicos e de configuração que cada um destes tipos de ligação básica envolve:

- **Cenário da VPN: Ligação simples de uma sucursal**
  Neste cenário, a sua empresa pretende estabelecer uma VPN entre as sub-redes de dois departamentos remotos, através de dois computadores iSeries que actuam como portas de ligação da VPN.
- **Cenário da VPN: Ligação base entre empresas**
  Neste cenário, a sua empresa pretende estabelecer uma VPN entre uma estação de trabalho cliente da sua divisão de produção e uma estação de trabalho cliente do departamento de fornecimento do seu parceiro comercial.

- **Cenário da VPN: Proteger um direccionamento voluntário de L2TP com IPSec**
  Este cenário mostra uma ligação entre um sistema central da sucursal e uma sede que utilize o L2TP protegido pelo IPSec. A sucursal possui um endereço de IP atribuído dinamicamente, enquanto que a sede possui um endereço de IP estático e globalmente encaminhável.
- **Cenário da VPN: Utilizar conversão de endereços da rede para a VPN**
  Neste cenário, a sua empresa pretende trocar dados sensíveis com um dos parceiros através da VPN do OS/400. Para proteger a privacidade da estrutura de rede da sua empresa, irá utilizar a NAT da VPN para ocultar os endereços de IP do iSeries utilizado para hospedar as aplicações a que o parceiro de negócios tem acesso.

Mais cenários da VPN
Para obter mais cenários da configuração da VPN, consulte as outras fontes de informação da VPN que se seguem:

- **Cenário da QoS: Resultados seguros e previsíveis (VPN e QoS)**
  Pode criar políticas de qualidade do serviço (QoS) com a VPN. Este exemplo mostra as duas em utilização conjunta.
- **OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM e(logo)server iSeries Server with Windows 2000 VPN Clients, REDP0153**
  Este Redpaper da IBM fornece um processo passo a passo para a configuração do direccionamento da VPN utilizando a VPN da V5R1 e o L2TP nativo do Windows 2000 e o suporte IPSec.
- **AS/400 Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00**
  Este redbook explora os conceitos da VPN e descreve a implementação dos mesmos através do Protocolo IP Security (IPSec) e do Protocolo Layer 2 Tunneling (L2TP) no OS/400.
- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00**
  Este redbook explora todas as funcionalidades de segurança da rede nativa no sistema AS/400, tais como filtros de IP, NAT, VPN, servidor proxy de HTTP, SSL, DNS, reencaminhamento de correio, auditorias e registos em diário. Descreve a utilização das mesma através de exemplos práticos.

Cenário da VPN: Ligação simples de uma sucursal

Suponha que a sua empresa pretende minimizar os custos suportados com as comunicações para e entre as respectivas sucursais. Actualmente, a sua empresa utiliza retransmissão de estruturas ou linhas dedicadas, mas pretende explorar outras opções para transmitir dados confidenciais internos que sejam menos dispendiosas, mais seguras e globalmente acessíveis. Ao explorar a Internet, pode facilmente estabelecer uma Rede privada virtual (VPN) que corresponda às necessidades da empresa.

A empresa e as respectivas sucursais necessitam todas de protecção da VPN através da Internet, mas não dentro das respectivas intranets. Como considera as redes internas fiáveis, a melhor solução é criar uma VPN de porta de ligação a porta de ligação. Neste caso, ambas as portas de ligação estão ligadas directamente à rede interveniente. Por outras palavras, são sistemas de *limite* ou *margem*, que não são protegidos por firewalls. Este exemplo serve como introdução útil aos passos que abrangem uma configuração de VPN básica. Quando este cenário se refere ao termo *Internet* refere-se à rede interveniente entre as duas portas de ligação da VPN, o que pode significar a rede privada da empresa ou a Internet pública.

> **Nota importante:**
> Este cenário mostra as portas de ligação de segurança do iSeries ligadas directamente à Internet. A ausência de uma firewall é propositada, de modo a simplificar o cenário. No entanto, isto não quer dizer que não seja necessária a utilização de uma firewall. De facto, deve ter em conta os riscos de segurança envolvidos cada vez que estabelece ligação à Internet. Reveja o redbook, AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00 , para obter uma descrição detalhada dos vários métodos de redução deste tipo de risco.

Vantagens

Este cenário apresenta as seguintes vantagens:

- A utilização da Internet ou de uma rede interna existente reduz os custos das linhas privadas entre sub-redes remotas.
- A utilização da Internet ou de uma rede interna existente reduz a complexidade da instalação e manutenção de linhas privadas e equipamento associado.
- A utilização da Internet permite às ligações remotas ligarem a quase todas as partes do mundo.
- A utilização da VPN proporciona aos utilizadores acesso a todos os servidores e recursos de ambos os lados da ligação, como se estivessem ligados através de uma linha dedicada ou de uma ligação de rede alargada (WAN).
- A utilização dos métodos de autenticação e codificação standard da indústria informática garante a segurança das informações sensíveis passadas de uma localização para outra.
- A alteração dinâmica e regular das chaves de codificação simplifica a configuração e minimiza o risco de elas serem descodificadas e da segurança ter falhas.
- A utilização de endereços de IP privados em cada sub-rede remota torna desnecessária a atribuição de endereços da Internet a cada cliente.

Objectivos

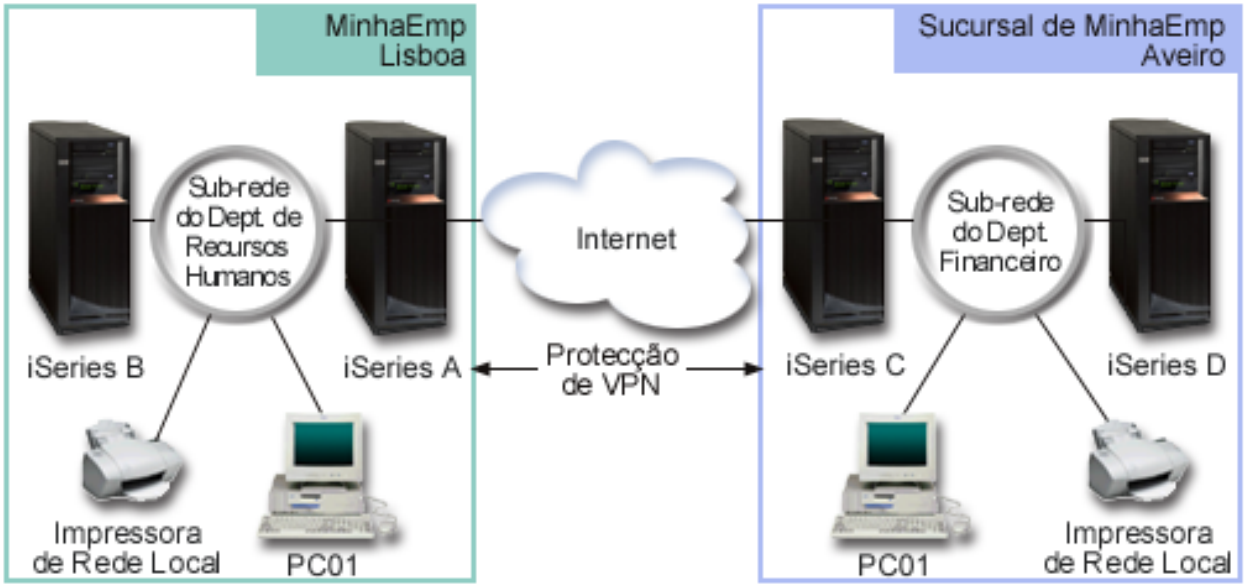
Neste cenário, a MinhaEmp, Inc. pretende estabelecer uma VPN entre as sub-redes dos departamentos de Recursos Humanos e Financeiro através de um par de servidores iSeries. Ambos os servidores actuarão como portas de ligação da VPN. Em termos das configurações da VPN, uma porta de ligação executa a gestão de chaves e aplica o IPSec aos dados que circulam através de encaminhamento. As portas de ligação não são pontos de terminação de dados da ligação.

Os objectivos deste cenário são os seguintes:

- A VPN deve proteger todo o tráfego de dados entre as sub-redes do departamento de Recursos Humanos e do Financeiro.
- O tráfego de dados não necessita da protecção da VPN a partir do momento em que alcança qualquer uma das sub-redes.
- Todos os clientes e sistemas centrais de cada rede têm acesso total à rede uns dos outros, incluindo a todas as aplicações.
- Os servidores de portas de ligação podem comunicar uns com os outros e ter acesso às aplicações uns dos outros.

Detalhes

A figura seguinte ilustra as características da rede de MinhaEmp.



Departamento de Recursos Humanos

- O iSeries-A runs é executado na Versão 5 Edição 2 do OS/400 (V5R2) e actua como porta de ligação da VPN do Departamento de Recursos Humanos.
- A sub-rede é 10.6.0.0 com a máscara 255.255.0.0. Esta sub-rede representa o ponto de terminação de dados de encaminhamento da VPN do lado de MinhaEmp Lisboa.
- O iSeries-A estabelece ligação à Internet através do endereço de IP 204.146.18.227. Isto é o ponto de terminação da ligação. Ou seja, o iSeries-A executa a gestão de chaves e aplica o IPSec a datagramas de IP de recepção e de envio.
- O iSeries-A estabelece ligação à respectiva sub-rede através do endereço de IP 10.6.11.1.
- O iSeries-B é um servidor de produção na sub-rede dos Recursos Humanos que executa aplicações TCP/IP standard.

Departamento Financeiro

- O iSeries-C é executado na Versão 5 Edição 2 do OS/400 (V5R2) e actua como porta de ligação da VPN do Departamento Financeiro.
- A sub-rede é 10.196.8.0 com a máscara 255.255.255.0. Esta sub-rede representa o ponto de terminação de dados de encaminhamento da VPN do lado de MinhaEmp Aveiro.
- O iSeries-C estabelece ligação à Internet através do endereço de IP 208.222.150.250. Isto é o ponto de terminação da ligação. Ou seja, o iSeries-C executa a gestão de chaves e aplica o IPSec a datagramas de IP de recepção e de envio.
- O iSeries-C estabelece ligação à respectiva sub-rede através do endereço de IP 10.196.8.5.

Tarefas de configuração

Deve concluir cada uma destas tarefas para configurar a ligação da sucursal descrita neste cenário:

1. Verificar o encaminhamento de TCP/IP para se certificar de que dois servidores de portas de ligação podem comunicar um com o outro através da Internet. Isto permite assegurar que os sistemas centrais em cada sub-rede efectuam o encaminhamento de forma correcta para a respectiva porta de ligação para terem acesso à sub-rede remota.
   Nota: O encaminhamento não será abordado neste tópico. Caso tenha questões, consulte Encaminhamento e equilíbrio do volume de trabalho do TCP/IP no Information Center.

2. Preencher (Consulte 6) as folhas de trabalho de planeamento e as listas de selecção para ambos os sistemas.
3. Configurar (Consulte 7) a VPN na porta de ligação da VPN de Recursos Humanos (iSeries-A).
4. Configurar (Consulte 8) a VPN na porta de ligação da VPN do Departamento Financeiro (iSeries-C).
5. Verifique se os servidores VPN foram iniciados (Consulte 8).
6. Testar (Consulte 8) as comunicações entre as duas sub-redes remotas.

Detalhes da configuração

Após a conclusão do primeiro passo, a verificação do correcto funcionamento do encaminhamento de TCP/IP e de que os servidores de portas de ligação podem comunicar, é possível iniciar a configuração da VPN.

Passo 2: Preencher as folhas de trabalho de planeamento

As seguintes listas de selecção de planeamento ilustram o tipo de informações de que necessita antes de começar a configuração da VPN. Todas as respostas à lista de selecção de pré-requisitos devem ser SIM, antes de prosseguir com a configuração da VPN.

Nota: Estas folhas de trabalho aplicam-se ao iSeries-A. Repita o processo para o iSeries-C, invertendo os endereços de IP conforme a necessidade.

Lista de selecção de pré-requisitos	Respostas
O OS/400 está na V5R2 (5722-SS1) ou posterior?	Sim
A opção Digital Certificate Manager (5722-SS1 Opção 34) está instalada?	Sim
O Cryptographic Access Provider (5722-AC2 ou AC3) está instalado?	Sim
O iSeries Access para Windows (5722-XE1) está instalado?	Sim
O iSeries Navigator está instalado?	Sim
O subcomponente de Rede do iSeries Navigator está instalado?	Sim
O TCP/IP Connectivity Utilities for OS/400 (5722-TC1) está instalado?	Sim
Definiu o valor do sistema de retenção de dados de segurança do servidor (QRETSVRSEC *SEC), para 1?	Sim
O TCP/IP está configurado no iSeries (incluindo interfaces de IP, encaminhamentos, nome do sistema central local e nome do domínio local)?	Sim
Foi estabelecida uma comunicação de TCP/IP normal entre os pontos de terminação necessários?	Sim
Aplicou as mais recentes correcções temporárias de programas (PTFs)?	Sim
Se o direccionamento de VPN atravessa firewalls ou encaminhadores que implementam filtragem de pacotes de IP, as regras de filtragem da firewall ou do encaminhador suportam protocolos AH e ESP?	Sim
As firewalls ou os encaminhadores estão configurados para permitir os protocolos IKE (UDP porta 500), AH e ESP?	Sim
As firewalls estão configuradas para permitir o reencaminhamento de IP?	Sim

Necessita destas informações para configurar a VPN	Respostas
Que tipo de ligação está a criar?	porta de ligação-a-porta de ligação
Que nome irá dar ao grupo de chaves dinâmicas?	HRgw2FINgw
De que tipo de segurança e de rendimento de sistema necessita para proteger as suas chaves?	equilibrado

Necessita destas informações para configurar a VPN	Respostas
Está a utilizar certificados para autenticar a ligação? Em caso negativo, qual é a chave pré-partilhada?	Não materialsensível
Qual é o identificador do servidor de chaves local?	Endereço de IP: 204.146.18.227
Qual é o identificador do ponto de terminação de dados local?	Sub-rede: 10.6.0.0 Máscara: 255.255.0.0
Qual é o identificador do servidor de chaves remoto?	Endereço de IP: 208.222.150.250
Qual é o identificador do ponto de terminação de dados remoto?	Sub-rede: 10.196.8.0 Máscara: 255.255.255.0
Quais as portas e os protocolos que pretende que tenham permissão para circular através da ligação?	Quaisquer
De que tipo de segurança e de rendimento de sistema necessita para proteger os seus dados?	equilibrado
A que interfaces é aplicada a ligação?	TRLINE

Passo 3: Configurar VPN no iSeries-A

Utilize as informações das folhas de trabalho para configurar a VPN no iSeries-A do seguinte modo:

1. No iSeries Navigator, expanda iSeries-A **—>Rede —>Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Virtual Private Networking** e seleccione **Nova Ligação** para iniciar o assistente de Nova Ligação.
3. Reveja a página **Boas-vindas** para mais informações sobre qual o objecto que o assistente cria.
4. Faça clique sobre **Seguinte** para ir para a página **Nome da Ligação**.
5. No campo **Nome**, introduza `HRgw2FINgw`.
6. (opcional) Especifique uma descrição para este grupo de ligações.
7. Faça clique sobre **Seguinte** para ir para a página **Cenário da Ligação**.
8. Seleccione **Ligar a porta de ligação a outra ligação**.
9. Faça clique sobre **Seguinte** para ir para a página **Política do Internet Key Exchange**.
10. Seleccione **Criar uma nova política** e, em seguida, seleccione **Segurança e rendimento equilibrados**.
11. Faça clique sobre **Seguinte** para ir para a página **Certificado para Ponto de Terminação da Ligação Local**.
12. Seleccione **Não** para indicar que não utilizará certificados para autenticar a ligação.
13. Faça clique sobre **Seguinte** para ir para a página **Servidor de Chaves Local**.
14. Seleccione **Endereço de IP versão 4** no campo **Tipo de identificador**.
15. Seleccione `204.146.18.227` no campo **Endereço de IP**.
16. Faça clique sobre **Seguinte** para ir para a página **Servidor de Chaves Remoto**.
17. Seleccione **Endereço de IP versão 4** no campo **Tipo de identificador**.
18. Introduza `208.222.150.250` no campo **Identificador**.
19. Introduza `materialsensível` no campo **Chave pré-partilhada**.
20. Faça clique sobre **Seguinte** para ir para a página **Ponto de Terminação de Dados Local**.
21. Seleccione **Sub-rede de IP versão 4** no campo **Tipo de identificador**.
22. Introduza `10.6.0.0` no campo **Identificador**.
23. Introduza `255.255.0.0` no campo **Máscara da sub-rede**.

24. Faça clique sobre **Seguinte** para ir para a página **Ponto de Terminação de Dados Remoto**.
25. Seleccione **Sub-rede de IP versão 4** no campo **Tipo de identificador**.
26. Introduza `10.196.8.0` no campo **Identificador**.
27. Introduza `255.255.255.0` no campo **Máscara da sub-rede**.
28. Faça clique sobre **Seguinte** para ir para a página **Serviços de Dados**.
29. Aceite os valores assumidos e, em seguida, faça clique sobre **Seguinte** para ir para a página **Política de Dados**.
30. Seleccione **Criar uma nova política** e, em seguida, seleccione **Segurança e rendimento equilibrados**. Seleccione **Utilizar o algoritmo de codificação RC4**.
31. Faça clique sobre **Seguinte** para ir para a página **Interfaces Aplicáveis**.
32. Seleccione **TRLINE** na tabela de **Linhas**.
33. Faça clique sobre **Seguinte** para ir para a página **Resumo**. Reveja os objectos que o assistente irá criar para se certificar de que estão correctos.
34. Faça clique sobre **Terminar** para concluir a configuração.
35. Quando a caixa de diálogo **Activar Filtragens de Políticas** for apresentada, seleccione **Sim, activar os filtros de políticas gerados** e, em seguida, seleccione **Permitir todo o tráfego**. Faça clique sobre **OK** para concluir a configuração. Quando lhe for pedido, especifique que pretende activar as regras para todas as interfaces.

Terminou a configuração da VPN no iSeries-A. O passo seguinte consiste em configurar a VPN na porta de ligação da VPN do Departamento Financeiro (iSeries-C).

Passo 4: Configurar a VPN no iSeries-C

Siga os mesmos passos utilizados para configurar o iSeries-A, invertendo os endereços de IP conforme a necessidade. Utilize as folhas de trabalho de planeamento como guia. Após concluir a configuração da porta de ligação da VPN do Departamento Financeiro, as suas ligações estarão num estado *on-demand* assim, a ligação é iniciada quando os datagramas de IP que esta ligação da VPN deve proteger são enviados. O passo seguinte é iniciar os servidores da VPN, caso ainda não tenham sido iniciados.

Passo 6: Iniciar os servidores da VPN

Siga estes passos para iniciar os servidores da VPN:

1. No iSeries Navigator, expanda **o servidor —>Rede —>Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Virtual Private Networking** e seleccione **Iniciar**.

Passo 7: Testar ligação

Após a conclusão da configuração de ambos os servidores e o início bem sucedido dos servidores da VPN, deve testar a conectividade para se certificar de que as sub-redes remotas conseguem comunicar entre elas. Para fazê-lo, execute os seguintes passos:

1. No iSeries Navigator, expanda **iSeries-A —>Rede**.
2. Faça clique com o botão direito do rato sobre **Configuração de TCP/IP** e seleccione **Utilitários** e, em seguida, seleccione **Ping**.
3. Na caixa de diálogo **Efectuar Ping a partir de**, introduza `iSeries-C` no campo **Ping**.
4. Faça clique sobre **Efectuar Ping Agora** para verificar a conectividade do iSeries-A para o iSeries-C.
5. Faça clique sobre **OK** quando tiver terminado.

Cenário da VPN: Ligação base entre empresas

Muitas empresas utilizam retransmissão de estruturas ou linhas dedicadas para fornecer comunicações seguras com os parceiros comerciais, subsidiárias e fornecedores. Infelizmente, estas soluções são, com frequência, dispendiosas e limitadas geograficamente. A VPN oferece uma alternativa às empresas que desejam comunicações privadas e de baixo custo.

Suponha que é um grande fornecedor de partes de um fabricante. Uma vez que é crítico dispor de determinadas partes e quantidades no preciso momento em que o fabricante precisa delas, é necessário estar sempre a par do estado do stock do fabricante e dos planos de produção. Pode acontecer tratar desta interacção manualmente hoje, mas achar que, além de demorada, é dispendiosa e mesmo incorrecta por vezes. É necessário encontrar uma forma mais eficaz, mais fácil e menos dispendiosa de comunicar com o fabricante. Contudo, dada a natureza confidencial e urgente das informações trocadas, o fabricante não quer publicá-las no site da Web da empresa ou distribuí-las mensalmente num relatório externo. Ao explorar a Internet pública, pode facilmente estabelecer uma rede privada virtual (VPN) que corresponda às necessidades de ambas as empresa.

Objectivos

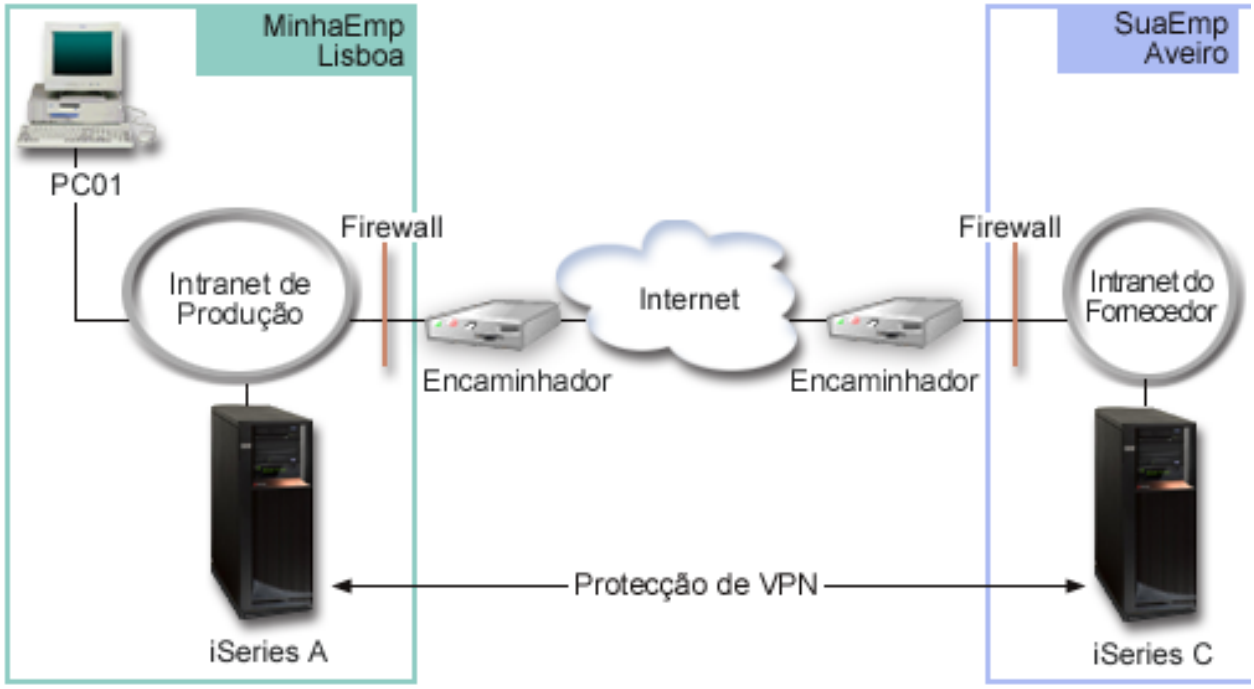
Neste cenário, MinhaEmp pretende estabelecer uma VPN entre um sistema central na respectiva divisão de peças e um sistema central no departamento de produção de um dos parceiros comerciais, a SuaEmp.

Uma vez que as informações partilhadas por estas duas empresas são extremamente confidenciais, devem ser protegidas à medida que são trocadas pela Internet. Além disso, os dados não devem circular livremente dentro das redes das próprias empresas, porque cada rede não considera a outra fidedigna. Por outras palavras, ambas as empresas necessitam de autenticação extremidade a extremidade, integridade e codificação.

Nota importante:
O objectivo deste cenário é apresentar, por meio de um exemplo, uma simples configuração da VPN entre sistemas centrais. Num ambiente de rede típico, será também necessário ter em conta a configuração de uma firewall, os requisitos de endereçamento de IP, encaminhamento, etc.

Detalhes

A figura seguinte ilustra as características da rede de MinhaEmp e SuaEmp.



Rede de Fornecimento da MinhaEmp

- O iSeries-A é executado na Versão 5 Edição 2 do OS/400 (V5R2).
- O iSeries-A tem um endereço de IP 10.6.1.1. Este é o ponto de terminação da ligação, assim como o ponto de terminação de dados. Ou seja, o iSeries-A executa as negociações e aplica o IPSec a datagramas de IP de recepção e de envio e, além disso, é a fonte e o destino dos dados que circulam na VPN.
- O iSeries-A está na sub-rede 10.6.0.0, com a máscara 255.255.0.0
- Apenas o iSeries-A pode iniciar a ligação com o iSeries-C.

Rede de Produção da SuaEmp

- O iSeries-C é executado na Versão 5 Edição 2 do OS/400 (V5R2).
- O iSeries-C tem um endereço de IP 10.196.8.6. Este é o ponto de terminação da ligação, assim como o ponto de terminação de dados. Ou seja, o iSeries-A executa as negociações e aplica o IPSec a datagramas de IP de recepção e de envio e, além disso, é a fonte e o destino dos dados que circulam na VPN.
- O iSeries-C está na sub-rede 10.196.8.0 com máscara 255.255.255.0

Tarefas de configuração

Deve concluir cada uma destas tarefas para configurar a ligação entre empresas descrita neste cenário:

1. Verificar o encaminhamento de TCP/IP para se certificar de que o iSeries-A e o iSeries-C podem comunicar um com o outro através da Internet. Isto assegura que os sistemas centrais em cada sub-rede efectuam o encaminhamento de forma correcta para a respectiva porta de ligação para terem acesso à sub-rede remota. Deve ter em atenção que, para este cenário, é necessário ter em conta o encaminhamento de endereços privados que não existiam antes.

   Nota:O encaminhamento não será abordado neste tópico. Caso tenha questões, consulte o tópico Encaminhamento e equilíbrio do volume de trabalho do TCP/IP no Information Center.

2. Preencher (Consulte 11) as folhas de trabalho de planeamento e as listas de selecção para ambos os sistemas.
3. Configurar a (Consulte 12) VPN no iSeries-A na rede de Fornecimento da MinhaEmp.
4. Configurar a (Consulte 13) VPN no iSeries-C na rede de Produção da SuaEmp.
5. Activar (Consulte 13) as regras de filtragem em ambos os servidores.
6. Iniciar (Consulte 13) a ligação a partir do iSeries-A.
7. Testar (Consulte 14) as comunicações entre as duas sub-redes remotas.

Detalhes da configuração

Após a conclusão do primeiro passo, a verificação do correcto funcionamento do encaminhamento de TCP/IP e de que os servidores podem comunicar, é possível iniciar a configuração da VPN.

Passo 2: Preencher as folhas de trabalho de planeamento

As seguintes listas de selecção de planeamento ilustram o tipo de informações de que necessita antes de começar a configuração da VPN. Todas as respostas à lista de selecção de pré-requisitos devem ser SIM, antes de prosseguir com a configuração da VPN.

Nota: Estas folhas de trabalho aplicam-se ao iSeries-A. Repita o processo para o iSeries-C, invertendo os endereços de IP conforme a necessidade.

Lista de selecção de pré-requisitos	Respostas
O OS/400 está na versão V5R2 (5722-SS1) ou posterior?	Sim
A opção Digital Certificate Manager (5722-SS1 Opção 34) está instalada?	Sim
O Cryptographic Access Provider (5722-AC2 ou AC3) está instalado?	Sim
O iSeries Access para Windows (5722-XE1) está instalado?	Sim
O iSeries Navigator está instalado?	Sim
O subcomponente de Rede do iSeries Navigator está instalado?	Sim
O TCP/IP Connectivity Utilities for OS/400 (5722-TC1) está instalado?	Sim
Definiu o valor do sistema de retenção de dados de segurança do servidor (QRETSVRSEC *SEC), para 1?	Sim
O TCP/IP está configurado no iSeries (incluindo interfaces de IP, encaminhamentos, nome do sistema central local e nome do domínio local)?	Sim
Foi estabelecida uma comunicação de TCP/IP normal entre os pontos de terminação necessários?	Sim
Aplicou as mais recentes correcções temporárias de programas (PTFs)?	Sim
Se o direccionamento de VPN atravessa firewalls ou encaminhadores que implementam filtragem de pacotes de IP, as regras de filtragem da firewall ou do encaminhador suportam protocolos AH e ESP?	Sim
As firewalls ou os encaminhadores estão configurados para permitir os protocolos IKE (UDP porta 500), AH e ESP?	Sim
As firewalls estão configuradas para permitir o reencaminhamento de IP?	Sim

Necessita destas informações para configurar a VPN	Respostas
Que tipo de ligação está a criar?	sistema central-a-sistema central
Que nome irá dar ao grupo de chaves dinâmicas?	MinhaEmp2SuaEmp
De que tipo de segurança e de rendimento de sistema necessita para proteger as suas chaves?	mais elevada

Está a utilizar certificados para autenticar a ligação? Em caso negativo, qual é a chave pré-partilhada?	Sim
Qual é o identificador do servidor de chaves local?	Endereço de IP: 10.6.1.1
Qual é o identificador do ponto de terminação de dados local?	Endereço de IP: 10.6.1.1
Qual é o identificador do servidor de chaves remoto?	Endereço de IP: 10.196.8.6
Qual é o identificador do ponto de terminação de dados remoto?	Endereço de IP: 10.196.8.6
Quais as portas e os protocolos que pretende que tenham permissão para circular através da ligação?	Quaisquer
De que tipo de segurança e de rendimento de sistema necessita para proteger os seus dados?	mais elevada
A que interfaces é aplicada a ligação?	TRLINE

Passo 3: Configurar VPN no iSeries-A

Utilize as informações das folhas de trabalho para configurar a VPN no iSeries-A do seguinte modo:

1. No iSeries Navigator, expanda o servidor **—>Rede —>Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Virtual Private Networking** e, em seguida, seleccione **Nova Ligação** iniciar o assistente de Ligação.
3. Reveja a página **Boas-vindas** para mais informações sobre qual o objecto que o assistente cria.
4. Faça clique sobre **Seguinte** para ir para a página **Nome da Ligação**.
5. No campo **Nome**, introduza `MinhaEmp2SuaEmp`.
6. (opcional) Especifique uma descrição para este grupo de ligações.
7. Faça clique sobre **Seguinte** para ir para a página **Cenário da Ligação**.
8. Seleccione **Ligar o sistema central a outro sistema central**.
9. Faça clique sobre **Seguinte** para ir para a página **Política do Internet Key Exchange**.
10. Seleccione **Criar uma nova política** e, em seguida, seleccione **Segurança mais elevada, rendimento inferior**.
11. Faça clique sobre **Seguinte** para ir para a página **Certificado para Ponto de Terminação da Ligação Local**.
12. Seleccione **Sim** para indicar que utilizará certificados para autenticar a ligação. Em seguida, seleccione o certificado que representa o iSeries-A.
    Nota: Caso pretenda utilizar um certificado para autenticar o ponto de terminação de ligações local, deve primeiro criar o certificado no Digital Certificate Manger (DCM).
13. Faça clique sobre **Seguinte** para ir para a página **Identificador do Ponto de Terminação de Ligações Local**.
14. Seleccione **Endereço IP versão 4** como o tipo de identificador. O endereço de IP associado deve ser 10.6.1.1. Mais uma vez, estas informações são definidas no certificado que criar no DCM.
15. Faça clique sobre **Seguinte** para ir para a página **Servidor de Chaves Remoto**.
16. Seleccione **Endereço de IP versão 4** no campo **Tipo de identificador**.
17. Introduza `10.196.8.6` no campo **Identificador**.
18. Faça clique sobre **Seguinte** para ir para a página **Serviços de Dados**.
19. Aceite os valores assumidos e, em seguida, faça clique sobre **Seguinte** para ir para a página **Política de Dados**.
20. Seleccione **Criar uma nova política** e, em seguida, seleccione **Segurança mais elevada, rendimento inferior**. Seleccione **Utilizar o algoritmo de codificação RC4**.
21. Faça clique sobre **Seguinte** para ir para a página **Interfaces Aplicáveis**.
22. Seleccione **TRLINE**.

23. Faça clique sobre **Seguinte** para ir para a página **Resumo**. Reveja os objectos que o assistente irá criar para se certificar de que estão correctos.
24. Faça clique sobre **Terminar** para concluir a configuração.
25. Quando a caixa de diálogo **Activar Filtragens de Políticas** é apresentada, seleccione **Não, as regras de pacotes serão activadas mais tarde** e em seguida faça clique sobre **OK**.

O passo seguinte é especificar que apenas o iSeries-A pode iniciar esta ligação. Pode fazê-lo através da personalização das propriedades do grupo de chaves dinâmicas MinhaEmp2SuaEmp criado pelo assistente:

1. Faça clique sobre **Por Grupo**, no painel da esquerda da interface da VPN; o novo grupo de chaves dinâmicas, MinhaEmp2SuaEmp, é apresentado no painel da direita. Faça clique com o botão direito do rato sobre o mesmo e seleccione **Propriedades**.
2. Vá para a página **Política** e seleccione a opção **Sistema local inicia a ligação**.
3. Faça clique sobre **OK** para guardar as alterações.

Terminou a configuração da VPN no iSeries-A. O passo seguinte consiste em configurar a VPN no iSeries-C da rede de Produção da SuaEmp.

Passo 4: Configurar a VPN no iSeries-C

Siga os mesmos passos utilizados para configurar o iSeries-A, invertendo os endereços de IP conforme a necessidade. Utilize as folhas de trabalho de planeamento como guia. Quando terminar a configuração da porta do iSeries-C, deve activar as regras de filtragem criados pelo assistente de Ligação em cada servidor.

Passo 5: Activar regras de pacotes

O sistema cria automaticamente as regras de pacotes necessárias para que a ligação funcione correctamente . Contudo, deve activá-las em ambos os sistemas antes de iniciar a configuração da VPN. Para fazê-lo no iSeries-A, execute os seguintes passos:

1. No iSeries Navigator, expanda **iSeries-A —>Rede —>Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Regras de Pacotes** e seleccione **Activar**. Isto abre a caixa de diálogo Activar Regras de Pacotes.
3. Seleccione se pretende seleccionar apenas as regras geradas da VPN, apenas um ficheiro seleccionado ou ambos. Pode escolher a última opção, por exemplo, se tiver diversas regras PERMIT e DENY que pretende forçar na interface para além das regras geradas da VPN.
4. Seleccione a interface em que pretende activar as regras. Neste caso, seleccione **Todas as interfaces**.
5. Faça clique sobre **OK** na caixa de diálogo, para confirmar que pretende verificar e activar as regras na interface ou nas interfaces especificadas. Após fazer clique em OK, o sistema verifica os erros de sintaxe e de semântica e comunica os resultados numa janela de mensagens na parte inferior do editor. Para mensagens de erro associadas a um ficheiro e número de linha específico, pode fazer clique com o botão direito do rato sobre o erro e seleccionar **Ir Para a Linha** para destacar o erro no ficheiro.
6. Repita estes passos para activar as regras de pacotes no iSeries-C.

Passo 6: Iniciar ligação

Siga estes passos para iniciar a ligação da MinhaEmp2SuaEmp a partir do iSeries-A:

1. No iSeries Navigator, expanda **iSeries-A —>Rede —>Políticas de IP**.

2. Se o servidor da VPN não tiver iniciado, faça clique com o botão direito do rato sobre **Virtual Private Networking** e seleccione **Iniciar**. Isto inicia o servidor da VPN.
3. Expanda **Virtual Private Networking —>Ligações Seguras**.
4. Faça clique sobre **Todas as Ligações** para visualizar uma lista de ligações no painel da direita.
5. Faça clique com o botão direito do rato sobre **MinhaEmp2SuaEmp** e seleccione **Iniciar**.
6. No menu **Ver**, seleccione **Actualizar**. Se a ligação for iniciada com êxito, o estado deve mudar de *Inactivo* para *Activado*. A ligação pode levar alguns minutos a iniciar, pelo que deve efectuar actualizações periódicas até o estado mudar para *Activado*.

Passo 7: Testar ligação

Após a conclusão da configuração de ambos os servidores e o início bem sucedido da ligação, deve testar a conectividade, para se certificar de que os sistemas centrais remotos conseguem comunicar um com o outro. Para fazê-lo, execute os seguintes passos:

1. No iSeries Navigator, expanda **iSeries-A —>Rede**.
2. Faça clique com o botão direito do rato sobre **Configuração de TCP/IP** e seleccione **Utilitários**e, em seguida, seleccione **Ping**.
3. Na caixa de diálogo **Efectuar Ping a partir de**, introduza `iSeries-C` no campo **Ping**.
4. Faça clique sobre **Efectuar Ping Agora** para verificar a conectividade do iSeries-A para o iSeries-C.
5. Faça clique sobre **OK** quando tiver terminado.

Cenário da VPN: Proteger um direccionamento voluntário de L2TP com o IPSec

Suponha que a sua empresa possui uma pequena sucursal noutro país. No decorrer de um dia útil normal, a sucursal poderá requerer acesso a informações confidenciais num iSeries da intranet da empresa. A sua empresa utiliza actualmente uma dispendiosa linha dedicada para fornecer à sucursal o acesso à rede da empresa. Apesar de a sua empresa pretender continuar a fornecer acesso seguro à respectiva intranet, pretende sobretudo reduzir as despesas associadas à linha dedicada. Tal é possível através da criação de um direccionamento voluntário do Protocolo Layer 2 Tunnel (L2TP) que expande a rede da empresa de tal forma que a sucursal parece fazer parte da sub-rede da empresa. A VPN protege o tráfego de dados no direccionamento de L2TP.

Com um direccionamento voluntário de L2TP, a sucursal remota estabelece um direccionamento directamente ao servidor de rede L2TP (LNS) da rede da empresa. A funcionalidade do concentrador de acesso de L2TP (LAC) reside no cliente. O direccionamento é visível ao Fornecedor de Serviços da Internet (ISP) do cliente remoto, pelo que não é necessário que o ISP suporte L2TP. Se pretender saber mais informações sobre conceitos L2TP, consulte Protocolo Layer 2 Tunnel (L2TP).

> **Nota importante:**
> Este cenário mostra as portas de ligação de segurança do iSeries ligadas directamente à Internet. A ausência de uma firewall é propositada, de modo a simplificar o cenário. No entanto, isto não quer dizer que não seja necessária a utilização de uma firewall. De facto, deve ter em conta os riscos de segurança envolvidos cada vez que estabelece ligação à Internet. Reveja este redbook, AS/400
>
> Internet Security Scenarios: A Practical Approach, SG24-5954-00  , para obter uma descrição detalhada dos diversos métodos utilizados para redução destes riscos.

Objectivos

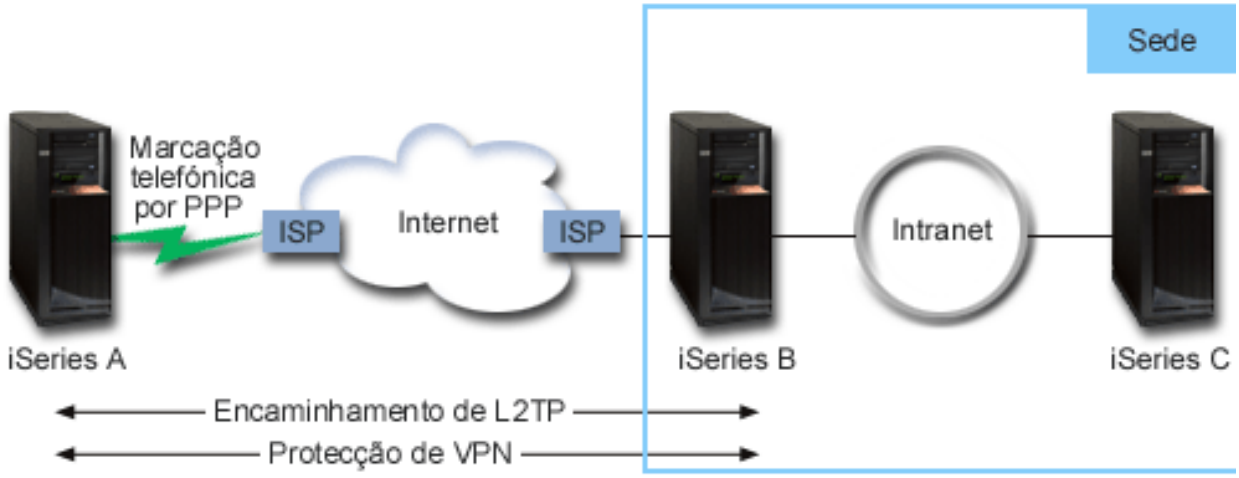
Neste cenário, um sistema iSeries de uma sucursal estabelece ligação à rede da sede através de um iSeries de porta de ligação com um direccionamento de L2TP protegido pela VPN.

Os objectivos principais deste cenário são:

- O sistema da sucursal inicia sempre a ligação à sede.
- O sistema da sucursal é o único sistema na rede da sucursal que necessita de ter acesso à rede da sede. Por outras palavras, a função que esta desempenha é a de um sistema central, e não de uma porta de ligação, na rede da sucursal.
- O sistema da sede é um computador anfitrião na rede da sede.

Detalhes

A figura seguinte ilustra as características da rede para este cenário:



iSeries-A

- Deve ter acesso a aplicações TCP/IP em todos os sistemas da rede da empresa.
- Recebe endereços de IP atribuídos dinamicamente do ISP.
- Deve ser configurado para fornecer suporte de L2TP.

iSeries-B

- Deve ter acesso a aplicações TCP/IP no iSeries-A.
- A sub-rede é 10.6.0.0 com a máscara 255.255.0.0. Esta sub-rede representa o ponto de terminação de dados do encaminhamento de VPN do lado da empresa.
- Estabelece ligação à Internet através do endereço de IP 205.13.237.6. Isto é o ponto de terminação da ligação. Ou seja, o iSeries-B executa a gestão de chaves e aplica o IPSec a datagramas de IP de recepção e de envio. O iSeries-B estabelece ligação à respectiva sub-rede através do endereço de IP 10.6.11.1.

Em termos do L2TP, o *iSeries-A* actua como o iniciador de L2TP, enquanto que o *iSeries-B* actua como o terminador de L2TP.

Tarefas de configuração

Partindo do princípio que a configuração TCP/IP já existe e funciona, deve concluir as seguintes tarefas:

1. Configurar a VPN (Consulte 16) no iSeries-A.
2. Configurar um perfil de ligação PPP (Consulte 18) e uma linha virtual para o iSeries-A.
3. Aplicar (Consulte 19)o grupo de chaves dinâmicas ao perfil PPP.
4. Configurar a VPN (Consulte 19) no iSeries-B.

5. Configurar um perfil de ligação PPP (Consulte 19) e uma linha virtual para o iSeries-B.
6. Activar (Consulte 20) regras de pacotes no iSeries-A e no iSeries-B.
7. Iniciar (Consulte 21) a ligação a partir do iSeries-A.

Detalhes da configuração

Após a verificação de que o TCP/IP está a funcionar correctamente e que os servidores iSeries conseguem comunicar, está pronto para iniciar a configuração da ligação descrita neste cenário.

Passo 1: Configurar a VPN no iSeries-A

Siga estes passos configurar a VPN no iSeries-A:

1. **Configure a política do Internet Key Exchange**
   a. No iSeries Navigator, expanda iSeries-A **—> Rede—> Políticas de IP—> Virtual Private Networking—> Políticas de Segurança de IP**.
   b. Faça clique com o botão direito do rato sobre **Políticas do Internet Key Exchange** e seleccione **Nova Política do Internet Key Exchange**
   c. Na página **Servidor Remoto**, seleccione **Endereço de IP versão 4** como o tipo de identificador e, em seguida, introduza `205.13.237.6` no campo **Endereço de IP**.
   d. Na página **Associações**, seleccione **Chave Pré-partilhada** para indicar que esta ligação utiliza uma chave pré-partilhada para autenticar esta política.
   e. Introduza a chave pré-partilhada no campo **Chave**. Trate a chave pré-partilhada como se tratasse de uma palavra-passe.
   f. Seleccione **Identificador de chaves** para o tipo de identificador do servidor de chaves local e, em seguida, introduza o identificador de chaves no campo **Identificador**. Por exemplo, `thisisthekeyid`. Lembre-se que o servidor de chaves local tem um endereço de IP atribuído dinamicamente, o qual não é possível conhecer logo. O iSeries-B utiliza este identificador para identificar o iSeries-A quando este inicia uma ligação.
   g. Na página **Conversões**, faça clique sobre **Adicionar** para adicionar as conversões propostas pelo iSeries-A ao iSeries-B para protecção de chaves e para especificar se a política do IKE utiliza a protecção de identidades ao iniciar negociações de fase 1.
   h. Na página **Conversão de Políticas do IKE**, seleccione **Chave Pré-partilhada** para o método de autenticação, **SHA** para o algoritmo hash e **3DES-CBC** para o algoritmo de codificação. Aceite mais tarde os valores assumidos para o grupo Diffie-Hellman Expirar Chaves do IKE.
   i. Faça clique sobre **OK** para regressar à página **Conversões**.
   j. Seleccione **Negociação de modo agressivo do IKE (sem protecção de identidade)**
   k. Faça clique sobre **OK** para guardar as configurações.
2. **Configurar a política de dados**
   a. Na interface da VPN, faça clique com o botão direito do rato sobre **Políticas de dados** e seleccione **Nova Política de Dados**.
   b. Na página **Geral**, especifique o nome da política de dados. Por exemplo, `l2tpremoteuser`.
   c. Vá para a página **Propostas**. Uma proposta é um conjunto de protocolos que os servidores de chave iniciadores e receptores utilizam para estabelecer uma ligação dinâmica entre dois pontos de terminação. É possível utilizar uma única política de dados em vários objectos da ligação. No entanto, nem todos os servidores de chave da VPN remotos possuem, necessariamente, as mesmas propriedades de política de dados. Por isso, é possível adicionar várias propostas a uma política de dados. Ao estabelecer uma ligação da VPN a um servidor de chaves remoto, deve existir, pelo menos, uma proposta correspondente na política de dados do iniciador e do receptor.
   d. Faça clique sobre **Adicionar** para adicionar uma conversão da política de dados.
   e. Seleccione **Transporte** para o modo de encapsulamento.
   f. Especifique um valor de expiração da chaves.

g. Faça clique sobre **OK** para regressar à página **Conversões**.

h. Faça clique sobre **OK** para guardar a nova política de dados.

3. **Configurar o grupo de chaves dinâmicas**

4.

a. Na interface da VPN, expanda **Ligações Seguras**.

b. Faça clique com o botão direito do rato sobre **Por Grupo** e seleccione **Novo Grupo de Chaves Dinâmicas**.

c. Na página **Geral**, especifique um nome para o grupo. Por exemplo, `l2tptocorp`.

d. Seleccione **Protege um direccionamento de L2TP iniciado localmente**.

e. Para a função do sistema, seleccione **Ambos os sistemas são sistemas centrais**.

f. Vá para a página **Política**. Seleccione a política de dados criada no passo dois, `l2tpremoteuser`, na lista pendente **Política de dados**.

g. Seleccione **Sistema local inicia ligação** para indicar que apenas o iSeries-A pode iniciar ligações com o iSeries-B.

h. Vá para a página **Ligações**. Seleccione **Gerar a seguinte regra de filtragem de políticas para este grupo**. Faça clique sobre **Editar** para definir os parâmetros da filtragem de políticas.

i. Na página **Filtragem de Políticas- Endereços Locais**, seleccione **Identificador de Chaves** para o tipo de identificador.

j. Para o identificador, seleccione o identificador de chaves, `thisisthekeyid`, definido na política do IKE.

k. Vá para a página **Filtragem de Políticas - Endereços Remotos**. Seleccione **Endereço de IP versão 4** na lista pendente **Tipo de identificador**.

l. Introduza `205.13.237.6` no campo **Identificador**.

m. Vá para a página **Filtragem de Políticas - Serviços**. Introduza `1701` nos campos **Porta Local** e **Porta Remota**. A porta 1701 é a bem conhecida porta para L2TP.

n. Seleccione **UDP** na lista pendente **Protocolo**.

o. Faça clique sobre **OK** para regressar à página **Ligações**.

p. Vá para a página **Interfaces**. Seleccione uma linha qualquer ou o perfil PPP ao qual este grupo será aplicado. Ainda não foi criado o perfil PPP para este grupo. Após a criação do mesmo, é necessário editar as propriedades deste grupo, de modo a que se aplique ao perfil PPP criado no passo seguinte.

q. Faça clique sobre **OK** para criar o grupo de chaves dinâmicas l2tptocorp.

É agora necessário adicionar uma ligação ao grupo que acabou de ser criado.

5. **Configurar a ligação de chaves dinâmicas**

a. Na interface da VPN, expanda **Por Grupo**. Esta acção apresenta uma lista de todos os grupos de chaves dinâmicas que foram configurados no iSeries-A.

b. Faça clique com o botão direito do rato sobre **12tptocorp** e seleccione **Nova Ligação de Chaves Dinâmicas**.

c. Na página **Geral**, especifique uma descrição opcional para a ligação.

d. Para o servidor de chaves remotas, seleccione **Endereço de IP Versão 4** para o tipo de identificador.

e. Seleccione `205.13.237.6` na lista pendente **Endereço de IP**.

f. Anule a selecção de **Iniciar por pedido**.

g. Vá para a página **Endereços Locais**. Seleccione **Identificador da Chave** para o tipo de identificador e, em seguida, seleccione `thisisthekeyid`, na lista pendente **Identificador**.

h. Vá para a página **Endereços Remotos**. Seleccione **Endereço de IP versão 4** para o tipo de identificador.

i. Introduza `205.13.237.6` no campo **Identificador**.

j. Vá para a página **Serviços**. Introduza 1701 nos campos **Porta Local** e **Porta Remota**. A porta 1701 é a bem conhecida porta para L2TP.
k. Seleccione **UDP** na lista pendente **Protocolo**.
l. Faça clique sobre **OK** para criar a ligação de chaves dinâmicas.

Terminou a configuração da VPN no iSeries-A. O passo seguinte é configurar um perfil PPP para o iSeries-A.

Passo 2: Configurar um perfil de ligação PPP e uma linha virtual no iSeries-A

Esta secção descreve os passos que devem ser executados para criar o perfil PPP para o iSeries-A. O perfil PPP não possui qualquer linha física associada: em vez disso, utiliza uma linha virtual. Isto acontece porque o tráfego PPP é direccionado através do direccionamento de L2TP, enquanto a VPN protege o direccionamento de L2TP.

Execute os seguintes passos para criar um perfil de ligação PPP para o iSeries-A:

1. No iSeries Navigator, expanda iSeries-A **—>Rede—>Serviços de Acesso Remoto**.
2. Faça clique com o botão direito do rato sobre **Perfis de Ligação do Originador** e seleccione **Novo Perfil**.
3. Na página **Configuração**, seleccione **PPP** para o tipo de protocolo.
4. Para selecções do Modo, seleccione **L2TP (linha virtual)**.
5. Seleccione **Iniciador por pedido (encaminhamento voluntário)** na lista pendente **Modo operativo**.
6. Faça clique sobre **OK** para ir para as páginas de propriedades de perfis PPP.
7. Na página **Geral**, introduza um nome que identifique o tipo e o destino da ligação. Neste caso, introduza toCORP. O nome especificado deve ter 10 caracteres ou menos.
8. (opcional) Especifique uma descrição para o perfil.
9. Vá para a página **Ligação**.
10. No campo **Nome da linha virtual**, seleccione **tocorp** na lista pendente. Lembre-se que esta linha não tem qualquer interface física associada. A linha virtual descreve várias características deste perfil PPP; por exemplo, o tamanho máximo da estrutura, as informações de autenticação, o nome do sistema central local e outras. É aberta a caixa de diálogo **Propriedades da Linha L2TP**.
11. Na página **Geral**, introduza uma descrição da linha virtual.
12. Vá para a página **Autenticação**.
13. No campo **Nome do sistema central local**, introduza o nome do sistema central do servidor de chaves local, iSeriesA.
14. Faça clique sobre **OK** para guardar a descrição da nova linha virtual e regresse à página **Ligação**.
15. Introduza o endereço do ponto de terminação do direccionamento remoto, 205.13.237.6, no campo **Endereço do ponto de terminação do direccionamento remoto**.
16. Seleccione **Requer Protecção IPSec** e seleccione o grupo de chaves dinâmicas criado no passo um, l2tptocorp, na lista pendente **Nome do grupo de ligações**.
17. Vá para a página **Definições TCP/IP**.
18. Na secção **Endereço de IP local**, seleccione **Atribuído por sistema remoto**.
19. Na secção **Endereço de IP remoto**, seleccione **Utilizar endereço de IP fixo**. Introduza 10.6.11.1, que é o endereço de IP do sistema remoto na respectiva sub-rede.
20. Na secção de encaminhamento, seleccione **Definir encaminhamentos estáticos adicionais** e faça clique sobre **Encaminhamentos**. Se não houver informações de encaminhamento para o perfil PPP, o iSeries-A é apenas capaz de atingir o ponto de terminação do direccionamento remoto, não conseguindo atingir qualquer outro sistema da sub-rede 10.6.0.0.*.
21. Faça clique sobre **Adicionar** para adicionar uma entrada de encaminhamento estático.

22. Introduza a sub-rede, `10.6.0.0`, e a máscara de sub-rede, `255.255.0.0` para encaminhar todo o tráfego 10.6.*.*.* através do direccionamento de L2TP.
23. Faça clique sobre **OK** para adicionar o percurso estático.
24. Faça clique sobre **OK** para fechar a caixa de diálogo Encaminhamento.
25. Vá para a página **Autenticação** para definir o nome do utilizador e a palavra-passe deste perfil PPP.
26. Na secção de identificação do sistema local, seleccione **Permitir que o sistema remoto verifique a identidade deste sistema**.
27. Em **Protocolo de autenticação a utilizar** seleccione **Requerer palavra-passe codificada (CHAP-MD5)**
28. Introduza o nome do utilizador, `iSeriesA` e uma palavra-passe.
29. Faça clique sobre **OK** para guardar o perfil PPP.

Passo 3: Aplicar o grupo de chaves dinâmicas `l2tptocorp` ao perfil PPP `toCorp`

Após a configuração do perfil de ligação PPP, é necessário voltar ao grupo de chaves dinâmicas `l2tptocorp` criado e associá-lo ao perfil PPP. Para fazê-lo, execute os seguintes passos:

1. Navegue para a interface da VPN, em seguida expanda **Ligações Seguras—>Por Grupo**.
2. Faça clique com o botão direito do rato sobre o grupo de chaves dinâmicas `l2tptocorp` e seleccione **Propriedades**.
3. Vá para a página **Interfaces** e seleccione **Aplicar este grupo** para o perfil PPP criado no passo dois `toCorp`.
4. Faça clique sobre **OK** para aplicar `l2tptocorp` ao perfil PPP `toCorp`.

Passo 4: Configurar a VPN no iSeries-B

Siga os mesmos passos utilizados para configurar o iSeries-A, invertendo os endereços de IP e identificadores conforme a necessidade. Considere os seguintes aspectos antes de começar:

- A identidade do servidor de chaves remoto, no identificador de chaves, especificado para o servidor de chaves local no iSeries-A. Por exemplo, `thisisthekeyid`.
- Utilize *exactamente* a mesma chave pré-partilhada.
- Certifique-se de que as conversões correspondem às configuradas no iSeries-A ou as ligações não terão êxito.
- Não especifique **Protege um encaminhamento L2TP iniciado localmente** na página **Geral** do grupo de chaves dinâmicas.
- O sistema remoto inicia a ligação.
- Especifique que a ligação deve ser iniciada por pedido.

Passo 5: Configurar um perfil de ligação PPP e uma linha virtual no iSeries-B

Siga os seguintes passos para criar um perfil de ligação PPP para o iSeries-B:

1. No iSeries Navigator, expanda iSeries-B **—>Rede—> Serviços de Acesso Remoto**.
2. Faça clique com o botão direito do rato sobre **Perfis de Ligação do Receptor** e seleccione **Novo Perfil**.
3. Na página **Configuração**, seleccione **PPP** para o tipo de protocolo.
4. Para selecções do Modo, seleccione **L2TP (linha virtual)**.
5. Seleccione **Terminador (servidor da rede)** na lista pendente **Modo operativo**.
6. Faça clique sobre **OK** para aceder às páginas de propriedades dos perfis PPP.

7. Na página **Geral**, introduza um nome que identifique o tipo e o destino da ligação. Neste caso, introduza `tobranch`. O nome especificado deve ter 10 caracteres ou menos.
8. (opcional) Especifique uma descrição para o perfil.
9. Vá para a página **Ligação**.
10. Seleccione o endereço de IP do ponto de terminação de encaminhamento local 205.13.237.6.
11. No campo **Nome da linha virtual**, seleccione **tobranch** na lista pendente. Lembre-se que esta linha não tem qualquer interface física associada. A linha virtual descreve várias características deste perfil PPP; por exemplo, o tamanho máximo da estrutura, as informações de autenticação, o nome do sistema central local e outras. É aberta a caixa de diálogo **Propriedades da Linha L2TP**.
12. Na página **Geral**, introduza uma descrição da linha virtual.
13. Vá para a página **Autenticação**.
14. No campo **Nome do sistema central local**, introduza o nome do sistema central do servidor de chaves local, `iSeriesB`.
15. Faça clique sobre **OK** para guardar a descrição da nova linha virtual e regresse à página **Ligação**.
16. Vá para a página **Definições TCP/IP**.
17. Na secção **Endereço de IP local**, seleccione o endereço de IP fixo do sistema local 10.6.11.1.
18. Na secção **Endereço de IP remoto**, seleccione **Conjunto de endereços** como o método de atribuição. Introduza um endereço de início e, em seguida, especifique o número de endereços que podem ser atribuídos ao sistema remoto.
19. Seleccione **Permitir que o sistema remoto tenha acesso a outras redes (reencaminhamento de IP)**.
20. Vá para a página **Autenticação** para definir o nome do utilizador e a palavra-passe deste perfil PPP.
21. Na secção de identificação do sistema local, seleccione **Permitir que o sistema remoto verifique a identidade deste sistema**. Isto abre a caixa de diálogo **Identificação do Sistema Local**.
22. Em **Protocolo de autenticação a utilizar** seleccione **Requerer palavra-passe codificada (CHAP-MD5)**
23. Introduza o nome do utilizador `iSeriesB` e uma palavra-passe.
24. Faça clique sobre **OK** para guardar o perfil PPP.

Passo 6: Activar regras de pacotes

A VPN cria automaticamente as regras de pacotes necessárias para que a ligação funcione correctamente. Contudo, deve activá-las em ambos os sistemas antes de iniciar a configuração da VPN. Para fazê-lo no iSeries-A, execute os seguintes passos:

1. No iSeries Navigator, expanda **iSeries-A —>Rede —>Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Regras de Pacotes** e seleccione **Activar**. Isto abre a caixa de diálogo Activar Regras de Pacotes.
3. Seleccione se pretende seleccionar apenas as regras geradas da VPN, apenas um ficheiro seleccionado ou ambos. Pode escolher a última opção, por exemplo, se tiver diversas regras PERMIT e DENY que pretende forçar na interface para além das regras geradas da VPN.
4. Seleccione a interface em que pretende activar as regras. Neste caso, seleccione **Todas as interfaces**.
5. Faça clique sobre **OK** na caixa de diálogo, para confirmar que pretende verificar e activar as regras na interface ou nas interfaces especificadas. Após fazer clique em OK, o sistema verifica os erros de sintaxe e de semântica e comunica os resultados numa janela de mensagens na parte inferior do editor. Para mensagens de erro associadas a um ficheiro e número de linha específico, pode fazer clique com o botão direito do rato sobre o erro e seleccionar **Ir Para a Linha** para destacar o erro no ficheiro.
6. Repita estes passos para activar as regras de pacotes no iSeries-B.

Passo 7: Iniciar ligação

O passo final é iniciar a ligação. Antes de poder iniciar uma ligação L2TP, deve activar o terminador L2TP para responder aos pedidos do iniciador. Depois de garantir que todos os serviços exigidos foram iniciados, inicie a ligação PPP no lado do terminador. Os passos seguintes descrevem a forma como iniciar a ligação PPP no iSeries-B:

1. No iSeries Navigator, expanda iSeries-B **—> Rede—> Serviços de Acesso Remoto**.
2. Faça clique sobre **Perfis de Ligação de Receptor** para visualizar uma lista de perfis de receptor no painel da direita.
3. Faça clique com o botão direito do rato sobre `tobranch` e seleccione **Iniciar**. Depois de o perfil de ligação iniciar, a janela é actualizada e apresenta a ligação como `A aguardar pedidos de ligação`. Agora, o iSeries-A já pode responder a pedidos da ligação L2TP do iSeries-B.

Siga estes passos para iniciar a ligação L2TP no iSeries-A:

1. No iSeries Navigator, expanda iSeries-A **—> Rede—> Serviços de Acesso Remoto**.
2. Faça clique sobre **Perfis de Ligação do Originador** para visualizar uma lista de perfis de receptor no painel da direita.
3. Faça clique com o botão direito do rato sobre **toCORP** e seleccione **Iniciar**. Depois de o perfil de ligação iniciar, a janela é actualizada e apresenta a ligação como `A estabelecer direccionamento L2TP`.
4. Prima F5 para actualizar o ecrã. Se o início do direccionamento L2TP for bem sucedido, o estado da ligação irá apresentar `Ligações activas`.

Cenário da VPN: Utilizar a conversão de endereços de rede para a VPN

Suponha que é o administrador da rede de uma pequena fábrica em Minneapolis. Um dos seus parceiros de negócios, um fornecedor de peças em Chicago, gostava de passar a negociar mais com a sua empresa através da Internet. Torna-se fundamental que a sua empresa tenha as peças e as quantidades necessárias no momento exacto, como tal, o fornecedor necessita de estar a par do estado do inventário e dos planos de produção. Actualmente esta operação é realizada manualmente, o que pode resultar numa tarefa demorada, dispendiosa e por vezes incorrecta, tornando-se assim necessário que investigue outras opções.

Tendo em conta a confidencialidade e a importância da altura em que as informações são trocadas, decide então criar uma VPN entre a rede do fornecedor e a rede da sua empresa. A fim de proteger futuramente a privacidade da estrutura de rede da sua empresa, decide que irá necessitar de ocultar os endereços de IP privados do iSeries utilizado para hospedar as aplicações a que o parceiro de negócios tem acesso. A questão é: Como fazer com que isto funcione?

Resposta: VPN do OS/400. Utilize-a não apenas para criar as definições da ligação na porta de ligação da VPN na rede da sua empresa mas também para fornecer a conversão de endereços necessários para ocultar os endereços privados locais. Ao contrário da conversão de endereços de rede (NAT, network address translation), que modifica os endereços de IP nas associações seguras (SAs, security associations) requeridas pela VPN para funcionar, a NAT da VPN executa a conversão de endereços antes da validação SA através da atribuição de um endereço quando a ligação é iniciada.

Objectivos

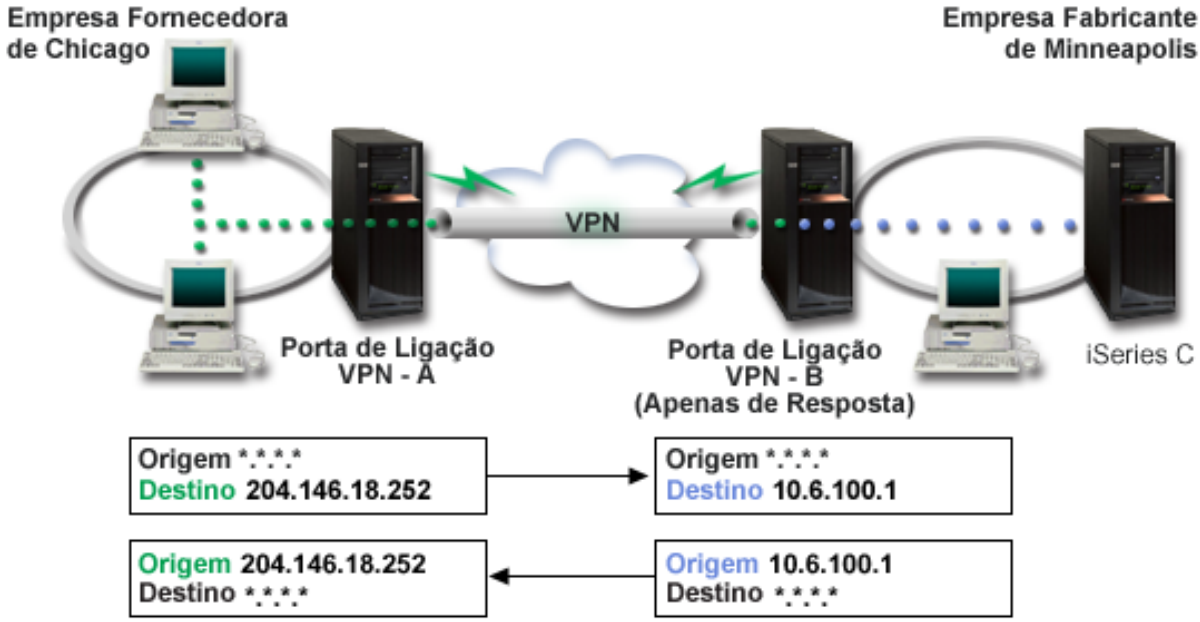
Os objectivos deste cenário são:

- permitir a todos os clientes na rede do fornecedor o acesso a um único sistema central iSeries na rede do fabricante sobre uma ligação da VPN parta de ligação-a-porta de ligação.

- ocultar os endereços de IP do sistema central iSeries na rede do fabricante, convertendo-os em endereços de IP públicos através da conversão de endereços de rede para a VPN (NAT para a VPN).

Detalhes

O diagrama seguinte ilustra as características da rede do fornecedor e da rede do fabricante:



- A porta de ligação A da VPN é configurada de forma a iniciar sempre as ligações para a porta de ligação B da VPN.
- A porta de ligação A da VPN define o ponto de terminação de destino para a ligação como 204.146.18.252 (o endereço público atribuído ao iSeries C).
- O iSeries C tem o endereço de IP privado 10.6.100.1 na rede do fabricante.
- Foi definido um endereço publico de 204.146.18.252 no conjunto de serviços local na porta de ligação B da VPN para o endereço privado 10.6.100.1 do iSeries C.
- A porta de ligação B da VPN converte o endereço público do iSeries C no respectivo endereço privado, 10.6.100.1, para a recepção de datagramas. A porta de ligação B da VPN converte datagramas devolvidos e de envio do endereço 10.6.100.1 para o endereço público 204.146.18.252 do iSeries C. Em relação aos clientes na rede do fornecedor, o iSeries C tem o endereço de IP 204.146.18.252. Nunca irão ficar a saber que ocorreu esta conversão de endereços.

Tarefas de Configuração

Deve concluir cada uma das tarefas seguintes para configurar a ligação descrita neste cenário:

1. Configurar uma porta de ligação-a-porta de ligação simples da VPN, entre a **porta de ligação A da VPN** e **a porta de ligação B da VPN**.
2. Definir um conjunto de serviços local na **porta de ligação B da VPN** para ocultar os endereços privados do **iSeries C** com o identificador público 204.146.18.252.
3. Configurar a **porta de ligação B da VPN** para converter os endereços locais utilizando os endereços do conjunto de serviços local.

Conceitos da VPN

A Virtual private networking (VPN) utiliza diversos protocolos TCP/IP importantes para proteger o tráfego de dados. Para melhor compreender o funcionamento de qualquer VPN, deve estar familiarizado com estes protocolos e conceitos e com a forma como a VPN do OS/400 os utiliza:

- **Protocolos IP Security (IPSec)**
  Os IPSec facultam uma base estável e duradoura para proporcionar segurança a nível da camada de rede.
- **Gestão de chaves**
  Uma VPN dinâmica proporciona segurança adicional às comunicações, através da utilização do protocolo Internet Key Exchange (IKE) para a gestão de chaves. O IKE permite aos servidores da VPN em cada extremo da ligação negociar novas chaves em intervalos específicos.
- **Protocolo Layer 2 Tunneling (L2TP)**
  Caso tencione utilizar uma ligação da VPN para maior segurança das comunicações entre a sua rede e os clientes remotos, deve também estar familiarizado com o (L2TP).
- **Conversão de endereços de rede para a VPN (NAT da VPN)**
  A VPN do OS/400 fornece uma forma de executar a conversão de endereços da rede, denominada NAT da VPN. A NAT da VPN é diferente da NAT tradicional no sentido em que converte endereços antes de aplicar os protocolos IKE e IPSec. Consulte este tópico para obter mais informações.
- **Encapsulamento UDP**
  O encapsulamento UDP permite o tráfego IPSec através de um dispositivo NAT convencional. Reveja este tópico para obter mais informações sobre o que é e qual a razão para a sua utilização nas ligações VPN.
- **Compressão IP (IPComp, IP compression)**
  O IPComp reduz o tamanho dos datagramas de IP através da compressão dos mesmos, de modo a aumentar o rendimento nas comunicações entre dois parceiros na VPN.
- **VPN e filtragem IP**
  A filtragem IP e a VPN estão estreitamente relacionadas. De facto, a maioria das ligações da VPN requerem regras de filtragem para funcionarem correctamente. Este tópico, fornece-lhe informações sobre quais os filtros requeridos pela VPN, bem como, outros conceitos de filtragem relacionados com a VPN.

Protocolos IP Security (IPSec)

Os IPSec facultam uma base estável e duradoura para proporcionar segurança a nível da camada de rede. Estes protocolos suportam todos os algoritmos criptográficos usados actualmente e podem também acolher algoritmos novos e mais desenvolvidos, à medida que estes vão surgindo. Os protocolos IPSec abrangem os seguintes pontos de segurança mais importantes:

Autenticação da origem de dados
Verifica se cada datagrama teve origem no suposto remetente.

Integridade dos dados
Verifica se o conteúdo de um datagrama foi alterado durante a circulação, quer seja deliberadamente, quer devido a erros aleatórios.

Confidencialidade de dados
Oculta o conteúdo de uma mensagem, normalmente através de codificação.

Protecção de repetição
Assegura que o elemento estranho não consegue interceptar um datagrama e repeti-lo mais tarde.

Gestão automática de chaves criptográficas e associações de segurança
Assegura que a sua política de VPN pode ser implementada em toda a rede com pouca ou nenhuma configuração manual.

A VPN utiliza dois protocolos IPSec para proteger os dados à medida que estes circulam pela VPN: Authentication Header (AH) e Encapsulating Security Payload (ESP). A outra parte da implementação dos

IPSec é o protocolo Internet Key Exchange (IKE) ou gestão por chave. Enquanto os IPSec codificam os dados, o IKE suporta a negociação automática das associações de segurança (SAs) e a geração e actualização automática das chaves criptográficas.

Os protocolos IPSec principais são listados a seguir:

- **Protocolo Authentication Header (AH)**
- **Protocolo Encapsulating Security Payload (ESP)**
- **Protocolos AH e ESP combinados**
- **Protocolos Internet Key Exchange (IKE)**

A Internet Engineering Task Force (IETF) define formalmente os IPSec no Request for Comment (RFC) 2401, *Security Architecture for the Internet Protocol*. Pode visualizar este RFC na Internet, no seguinte site da Web: http://www.rfc-editor.org .

Authentication Header

O protocolo Authentication Header (AH) proporciona a autenticação da origem dos dados, a integridade dos dados e a protecção de repetição. No entanto, o AH não proporciona a confidencialidade dos dados, o que significa que todos os dados são enviados sem protecção.

O AH assegura a integridade dos dados pela soma de verificação gerada pelo código de autenticação de uma mensagem, como, por exemplo, o MD5. Para assegurar a autenticação da origem dos dados, o AH inclui uma chave partilhada secreta no algoritmo que utiliza para a autenticação. Para assegurar a protecção de repetição, o AH utiliza um campo de número de sequência dentro do cabeçalho do AH. Como nota informativa, refira-se que estas três funções distintas são frequentemente englobadas e referidas unicamente por **autenticação**. De forma simplista, o AH assegura que nada interfere com os dados em trânsito para o destino final.

Apesar de o AH autenticar o maior número possível de datagramas IP, os valores de determinados campos no cabeçalho IP não podem ser previstos pelo receptor. O AH não protege estes campos, que são conhecidos como campos **variáveis**. No entanto, o AH protege sempre a carga útil do pacote IP.

A Internet Engineering Task Force (IETF) define formalmente o AH no Request for Comment (RFC) 2402, *IP Authentication Header*. Pode visualizar este RFC na Internet, no seguinte site da Web: http://www.rfc-editor.org .

Formas de utilização do AH

É possível aplicar o AH de duas formas: modo de transporte ou modo de direccionamento. No modo de transporte, o cabeçalho IP do datagrama é o cabeçalho IP mais afastado, seguido pelo cabeçalho do AH e, por fim, pela carga útil do datagrama. O AH autentica todo o datagrama, excepto os campos variáveis. No entanto, as informações contidas no datagrama são transportadas sem protecção e são, por isso, susceptíveis de serem corrompidas. O modo de transporte exige menos tempo de processamento do sistema do que o modo de direccionamento, mas não proporciona tanta segurança.

O modo de direccionamento cria um novo cabeçalho IP e utiliza-o como o cabeçalho IP mais afastado do datagrama. O cabeçalho do AH segue-se ao novo cabeçalho IP. O datagrama original (tanto o cabeçalho IP, como a carga útil original) vem por último. O AH autentica todo o datagrama, o que significa que o sistema receptor pode detectar se o datagrama foi alterado quando em trânsito.

Quando ambos os extremos de uma associação de segurança forem portas de ligação, utilize o modo de direccionamento. No modo de direccionamento, os endereços de origem e de destino do cabeçalho IP mais afastado não precisam de ser iguais aos do cabeçalho IP original. Por exemplo, duas portas de ligação de segurança podem operar um direccionamento AH para autenticar todo o tráfego entre as redes que ligam. De facto, esta é uma configuração muito habitual.

A principal vantagem da utilização do modo de direccionamento é que o modo de direccionamento protege totalmente o datagrama IP encapsulado. Além disso, o modo de direccionamento torna possível a utilização de endereços privados.

Porquê o AH?
Em muitos casos, os seus dados exigem apenas autenticação. Apesar de o protocolo Encapsulating Security Payload (ESP) poder executar autenticação, o AH não afecta o rendimento do sistema tanto quanto o ESP. Outra vantagem da utilização do AH é que este autentica todo o datagrama. O ESP, por sua vez, não autentica o cabeçalho IP principal ou outras informações que venham antes do cabeçalho do ESP.

Além disso, o ESP exige sólidos algoritmos criptográficos para ser implementado. A criptografia sólida é restrita em alguns países, enquanto o AH não é regulado e pode ser utilizado livremente em todo o mundo.

Quais os algoritmos utilizados pelo AH para proteger a minha informação?
O AH utiliza algoritmos conhecidos por **códigos de autenticação de mensagens atribuídos aleatoriamente (HMAC)**. Mais especificamente, a VPN utiliza os HMAC-MD5 ou HMAC-SHA. Tanto os MD5 como os SHA recebem dados de input de comprimento variável e uma chave secreta para produzir dados de output de comprimento fixo (chamados valores de atribuição aleatória). Se a atribuição aleatória de duas mensagens corresponder, é bem provável que seja a mesma. Tanto os MD5 como os SHA codificam o comprimento da mensagem no seu output, mas os SHA são considerados mais seguros, uma vez que produzem atribuições aleatórias de maior dimensão.

A Internet Engineering Task Force (IETF) define formalmente o HMAC-MD5 no Request for Comments (RFC) 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. A Internet Engineering Task Force (IETF) define formalmente os HMAC-SHA em Request for Comments (RFC) 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*. Pode visualizar estes RFCs na Internet, no seguinte site da Web:

http://www.rfc-editor.org  .

Encapsulating Security Payload

O protocolo Encapsulating Security Payload (ESP) proporciona confidencialidade de dados e, como opção, autenticação da origem dos dados, verificação da integridade dos dados e protecção de repetição. A diferença entre o ESP e o protocolo Authentication Header (AH) é que o ESP proporciona ainda a codificação, para além de ambos proporcionarem autenticação, verificação da integridade e protecção de repetição.Com o ESP, ambos os sistemas de comunicação utilizam uma chave partilhada para codificação e descodificação dos dados que trocam.

Se decidir utilizar a codificação e a autenticação, o sistema receptor autenticará primeiro o pacote e, depois, se o primeiro passo for bem sucedido, prosseguirá com a descodificação. Este tipo de configuração reduz o tempo de processamento do sistema, bem como a sua vulnerabilidade a intrusões por negação de serviço.

Duas formas de utilizar o ESP
É possível aplicar o ESP de duas formas: modo de transporte ou modo de direccionamento. No modo de transporte, o cabeçalho do ESP segue-se ao cabeçalho IP do datagrama IP original. Se o datagrama já possuir um cabeçalho IPSec, o cabeçalho do ESP virá antes deste. O final do ESP e os dados de autenticação opcionais seguem-se à carga útil.

O modo de transporte não autentica ou codifica o cabeçalho IP, o que poderia expor informações sobre o seu endereço a potenciais elementos estranhos, quando o datagrama estivesse em trânsito. O modo de transporte exige menos tempo de processamento do sistema do que o modo de direccionamento, mas não proporciona tanta segurança. Na maioria dos casos, os sistemas centrais utilizam o ESP em modo de transporte.

O modo de direccionamento cria um novo cabeçalho IP e utiliza-o como o cabeçalho IP mais afastado do datagrama, seguido pelo cabeçalho do ESP e, depois, pelo datagrama original (tanto o cabeçalho IP, como a carga útil original). O final do ESP e os dados de autenticação opcionais estão anexados à carga útil. Quando utilizar a codificação e a autenticação, o ESP protege completamente o datagrama original, uma vez que representa agora os dados da carga útil do novo pacote ESP. O ESP, no entanto, não protege o novo cabeçalho IP. As portas de ligação devem utilizar o ESP em modo de direccionamento.

Que algoritmos utiliza o ESP para proteger as minhas informações?
O ESP utiliza uma chave simétrica que ambas as partes comunicantes utilizam para codificar e descodificar os dados que trocam. O emissor e o receptor devem acordar uma chave, antes de efectuarem comunicações seguras entre si. A VPN do OS/400 utiliza Data Encryption Standard (DES), triple-DES (3DES), RC5, RC4 ou Advanced Encryption Standard (AES) para codificação.

A Internet Engineering Task Force (IETF) define formalmente DES em Request for Comment (RFC) 1829, *The ESP DES-CBC Transform*. A Internet Engineering Task Force (IETF) define formalmente 3DES em RFC 1851, *The ESP Triple DES Transform*. Pode visualizar estes RFCs na Internet, no seguinte endereço da Web: http://www.rfc-editor.org .

O ESP utiliza algoritmos HMAC-MD5 e HMAC-SHA para proporcionar funções de autenticação. Tanto os MD5 como os SHA recebem dados de input de comprimento variável e uma chave secreta para produzir dados de output de comprimento fixo (chamados valores de atribuição aleatória). Se a atribuição aleatória de duas mensagens corresponder, é bem provável que seja a mesma. Tanto os MD5 como os SHA codificam o comprimento da mensagem no seu output, mas os SHA são considerados mais seguros, uma vez que produzem atribuições aleatórias maiores.

A Internet Engineering Task Force (IETF) define formalmente HMAC-MD5 em Request for Comments (RFC) 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. A Internet Engineering Task Force (IETF) define formalmente os HMAC-SHA em Request for Comments (RFC) 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*. Pode visualizar estes RFCs na Internet, no seguinte endereço da Web: http://www.rfc-editor.org .

AH e ESP combinados
A VPN permite combinar AH e ESP para ligações sistema central-a-sistema central em modo de transporte. A combinação destes protocolos protege todo o datagrama de IP. Apesar de a combinação entre os dois protocolos oferecer maior segurança, as despesas gerais de processamento envolvidas pode ultrapassar os benefícios.

Gestão de chaves
A cada negociação bem sucedida, os servidores da VPN regeneram as chaves que protegem uma ligação, tornando assim mais difícil que um elemento estranho capture informações da ligação. Além disso, se utilizar ″perfect forward secrecy″, os elementos estranhos não poderão adivinhar chaves futuras com base em informações sobre chaves passadas.

O gestor de chaves da VPN é a implementação da IBM do protocolo Internet Key Exchange (IKE). O gestor de chaves suporta a negociação automática das associações de segurança (SAs), bem como a geração e actualização automática das chaves criptográficas.

Uma **associação de segurança (SA)** contém informações necessárias para utilizar os protocolos IPSec. Por exemplo, uma SA identifica tipos de algoritmos, comprimentos e durações de chaves, partes participantes e modos de encapsulamento.

As chaves criptográficas, como o nome deixa entender, bloqueiam, ou protegem, as informações, até que estas atinjam o destino final em segurança.

Nota:A geração segura das chaves é o factor mais importante no estabelecimento de uma ligação segura e privada. Se as chaves forem postas em risco, os seus esforços de autenticação e codificação, por muito intensos que sejam, tornam-se inúteis.

Fases da gestão de chaves
O gestor de chaves da VPN utiliza duas fases distintas na implementação das mesmas.

Fase 1
A fase 1 estabelece um segredo mestre a partir do qual as chaves criptográficas subjacentes derivam, de modo a proteger o tráfego dos dados do utilizador. Esta situação acontece mesmo se ainda não existir protecção de segurança entre os dois extremos. A VPN utiliza o modo de assinatura RSA ou as chaves pré-partilhadas para autenticar as negociações de fase 1, bem como para estabelecer as chaves que protegem as mensagens IKE que circulam durante as negociações de fase 2 subsequentes.

Uma *chave pré-partilhada* é uma cadeia não trivial com até 128 caracteres de comprimento. Ambos os extremos de uma ligação devem acordar a chave pré-partilhada. A vantagem da utilização de chaves pré-partilhadas reside na simplicidade das mesmas, e a desvantagem prende-se com o facto de a palavra-passe partilhada ter de ser distribuída de forma exterior à banda, por exemplo por telefone ou por correio registado, antes das negociações de IKE. Deve assim tratar a chave pré-partilhada como se tratasse de uma palavra-passe.

A autenticação *Assinatura RSA* fornece mais segurança que as chaves pré-partilhadas, uma vez que este modo utiliza certificados digitais para fornecer autenticação. Deve configurar os certificados digitais através da utilização do Digital Certificate Manager (5722-SS1 opção 34). Além disso, algumas soluções da VPN necessitam da Assinatura RSA para interoperabilidade. Por exemplo, a VPN do Windows 2000 utiliza Assinatura RSA como o método assumido de autenticação. Por fim, a Assinatura RSA fornece mais escalabilidade que as chaves pré-partilhadas. Os certificados utilizados devem ter origem em autoridades de certificação da confiança de ambos os servidores de chaves.

Fase 2
A fase 2, por outro lado, negoceia as associações de segurança e as chaves que protegem a verdadeira permuta de dados de aplicação. Atenção, até este ponto, nenhuns dados de aplicação foram realmente enviados. A fase 1 protege as mensagens do IKE da fase 2.

Assim que as negociações da fase 2 estiverem concluídas, a VPN estabelece uma ligação segura e dinâmica na rede e entre os extremos que definiu para a ligação. Todos os dados enviados pela VPN são entregues com o grau de segurança e eficiência acordado pelos servidores de chave, durante os processos de negociação da fase 1 e da fase 2.

De modo geral, as negociações de fase 1 são efectuadas uma vez por dia, enquanto que as da fase 2 são actualizadas a cada 60 minutos ou a cada cinco minutos. Velocidades de actualização mais rápidas aumentam a segurança dos dados, mas diminuem o rendimento do sistema. Utilize durações de chave curtas para proteger os dados mais sensíveis.

Quando cria uma VPN dinâmica através da utilização do iSeries Navigator, deve definir uma política do IKE para permitir negociações de fase 1 e uma política de dados para reger as negociações de fase 2. Opcionalmente,pode utilizar o assistente de Nova Ligação. O assistente cria automaticamente cada um dos objectos de configuração que a VPN necessita para funcionar correctamente, incluindo uma política de IKE e política de dados.

Leituras sugeridas
Se quer obter mais informações sobre o protocolo Internet Key Exchange (IKE) e a gestão de chaves, deve rever os seguintes Request for Comments (RFC) da Internet Engineering Task Force (IETF):

- RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP*

- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409, *The Internet Key Exchange (IKE)*

Pode visualizar estes RFCs na Internet, no seguinte site da Web: http://www.rfc-editor.org .

Protocolo Layer 2 Tunnel (L2TP)

As ligações do Protocolo Layer 2 Tunneling (L2TP), também chamadas linhas virtuais, proporcionam um acesso pouco dispendioso a utilizadores remotos, ao permitir a um servidor de rede de uma empresa gerir os endereços de IP atribuídos aos respectivos utilizadores remotos. Para além disso, as ligações do L2TP fornecem acesso protegido ao sistema ou à rede quando as utiliza em conjunto com o IP Security (IPSec).

O L2TP suporta dois modos de direccionamento: o direccionamento voluntário e o direccionamento obrigatório. A maior diferença entre estes dois tipos de direccionamento é o ponto de terminação. No direccionamento voluntário, o direccionamento termina no cliente remoto, enquanto que o direccionamento obrigatório termina no ISP.

Com um **direccionamento obrigatório** de L2TP, um sistema central remoto inicia uma ligação ao respectivo Fornecedor de Serviços da Internet (ISP). O ISP estabelece então uma ligação L2TP entre o utilizador remoto e a rede da empresa. Apesar de o ISP estabelecer a ligação, é o utilizador quem decide a forma de proteger o tráfego através da VPN. Com um direccionamento obrigatório, o ISP deve suportar o LT2P.

Com um **direccionamento voluntário** de L2TP, a ligação é criada pelo utilizador remoto, de modo geral através de um cliente de direccionamento de L2TP. Como resultado, o utilizador remoto envia pacotes L2TP ao respectivo ISP, que os remete para a rede da empresa. Com um direccionamento voluntário, o ISP não necessita de suportar o L2TP. O cenário, *Proteger um direccionamento voluntário de L2TP com IPSec* fornece um exemplo de como configurar um iSeries de uma sucursal para estabelecer uma ligação com a rede da sede através de um iSeries de porta de ligação com um direccionamento de L2TP protegido pela VPN.

Na realidade, o L2TP é uma variante de um protocolo de encapsulamento de IP. O direccionamento de L2TP é criado pelo encapsulamento de uma estrutura L2TP dentro de um pacote do Protocolo de Datagramas do Utilizador (UDP), que, por sua vez, é encapsulado dentro de um pacote IP. Os endereços de origem e destino deste pacote IP definem os extremos da ligação. Uma vez que o protocolo de encapsulamento externo é o IP, pode aplicar os protocolos IPSec ao pacote de IP composto. Este procedimento protege os dados que fluem no direccionamento de L2TP. Então, pode aplicar os protocolos Authentication Header (AH), Encapsulated Security Payload (ESP) e Internet Key Exchange (IKE) de uma forma simples.

Conversão de endereços de rede para a VPN

A conversão de endereços de rede (NAT) pega nos endereços de IP privados e converte-os em endereços de IP públicos. Isto ajuda a conservar endereços públicos importantes, enquanto que, ao mesmo tempo, permite que os sistemas centrais na rede tenham acesso aos serviços e aos sistemas centrais remotos pela Internet (ou outra rede pública).

Além disso, se utilizar endereços de IP privados, estes podem entrar em conflito com endereços de IP semelhantes que sejam recebidos. Por exemplo, poderá pretender comunicar com outra rede e ambas as redes utilizarem endereços 10.*.*.*, levando a que os endereços colidam e larguem os pacotes. A aplicação da NAT aos endereços de envio parece a resposta a este problema. Contudo, se o tráfego de dados estiver protegido por uma VPN, a NAT convencional não terá resultado, uma vez que altera os endereços de IP nas associações de segurança (SAs) necessárias para o funcionamento da VPN. Para evitar este problema, a VPN fornece uma versão de conversão de endereços de rede denominada por

NAT da VPN. Esta executa conversão de endereços antes da validação da SA através da atribuição de um endereço à ligação quando esta é iniciada. O endereço continua associado à ligação até que seja eliminada.

Nota: Nesta situação, o FTP não suporta a NAT da VPN.

Como devo utilizar a NAT da VPN?
Existem dois tipos diferentes de NAT da VPN que é necessário ter em conta antes de começar. Eles são:

NAT da VPN para impedir conflitos entre endereços de IP
Este tipo de NAT da VPN permite-lhe evitar possíveis conflitos entre endereços de IP quando configurar uma ligação da VPN entre redes ou sistemas com esquemas de endereçamento semelhantes. Um cenário típico é aquele em que ambas as empresas criam ligações da VPN, através de um dos intervalos de endereços de IP privados pré-determinados. Por exemplo, 10.*.*.*. A forma como configura este tipo de NAT da VPN depende do facto de o servidor ser o iniciador ou o receptor da ligação da VPN. Quando o servidor for o iniciador da ligação, pode converter os endereços locais em endereços compatíveis com o endereço da ligação da VPN parceira. Quando o servidor for o receptor da ligação, pode converter os endereços remotos da ligação da VPN parceira em endereços compatíveis com o esquema de endereçamento local. Configure este tipo de conversão de endereços apenas para as ligações dinâmicas.

NAT da VPN para ocultar endereços locais
Este tipo de NAT da VPN é utilizado principalmente para ocultar o endereço de IP real do sistema local através da conversão deste endereço noutro que possa ser tornado disponível publicamente. Quando configura a NAT da VPN, é possível especificar que cada endereço de IP conhecido publicamente possa ser convertido num endereço que faça parte de um conjunto de endereços ocultos. Esta especificação permite-lhe ainda equilibrar o fluxo de tráfego de um endereço individual através de endereços múltiplos. A NAT da VPN para endereços locais requer que o servidor seja o receptor das respectivas ligações.

Utilize a NAT da VPN para ocultar endereços locais, se responder afirmativamente às perguntas seguintes:

1. Possui um ou mais servidores aos quais pretende que as pessoas tenham acesso através de uma VPN?
2. Necessita de ser flexível em relação aos verdadeiros endereços de IP do seu sistema?
3. Possui um ou mais endereços de IP globalmente encaminháveis?

O cenário, *Utilizar conversão de endereços da rede para a VPN* fornece-lhe um exemplo de como configurar a NAT da VPN para ocultar endereços locais no iSeries.

Para obter instruções passo-a-passo sobre como configurar a NAT da VPN no iSeries, utilize a ajuda online disponível na interface da VPN iSeries Navigator.

NAT compatível com IPSec

Problema: A NAT convencional quebra a VPN
A conversão de endereços da rede (NAT, Network address translation) permite ocultar os endereços de IP provados não registados atrás de um conjunto de endereços de IP registados. Isto ajuda-o a proteger a rede interna das redes externas. A NAT ajuda também a aliviar o problema de descongestionamento dos endereços de IP, tendo em conta que muitos endereços privados podem ser representados por um conjunto pequeno de endereços registados.

Infelizmente, a NAT convencional não funciona com os pacotes IPSec porque quando um pacote passa através de um dispositivo NAT, o endereço original no pacote é alterado, invalidando assim o pacote. Quando isto acontece, o terminal de recepção da ligação da VPN rejeita o pacote e a negociação da ligação da VPN falha.

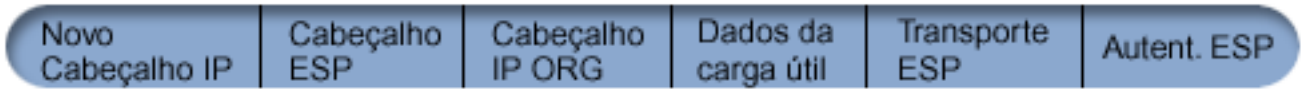
Solução: Encapsulamento UDP
Em resumo, o encapsulamento UDP reinicia um pacote IPSec num novo cabeçalho duplicado de IP/UDP. O endereço no novo cabeçalho de IP é convertido quando passa pelo dispositivo NAT. Em seguida, quando o pacote chega ao destino, o terminal de recepção decompõe o cabeçalho adicional, deixando o pacote IPSec original, que irá passar agora por todas as restantes validações.

Apenas pode aplicar o encapsulamento UDP a VPNs que vão utilizar IPSec ESP no modo de direccionamento ou modo de transporte. Adicionalmente, na V5R2, o iSeries apenas pode agir como cliente para o encapsulamento UDP. Isto é, apenas pode *iniciar* tráfego encapsulado UDP.

Os gráficos abaixo ilustram o formato de um pacote ESP com encapsulamento UDP no modo de direccionamento:

Datagrama IPv4 original:

Após aplicar IPSec ESP no modo de direccionamento:

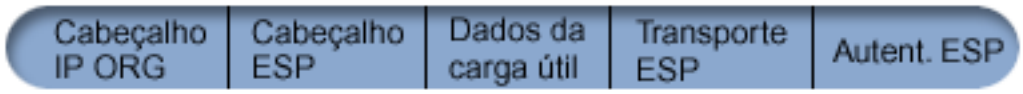


Após o aplicar Encapsulamento UDP:

Os gráficos abaixo ilustram o formato de um pacote ESP com encapsulamento UDP no modo de transporte:

Datagrama IPv4 original:

Após aplicar IPSec ESP no modo de transporte:



Após aplicar o Encapsulamento UDP:

Logo que o pacote esteja encapsulado, o iSeries envia o pacote para o parceiro da VPN através da porta 500 da UDP. Lembre-se de que os parceiros da VPN, já executam negociações IKE através da porta 500 da UDP. Ao enviar o tráfego encapsulado da UDP através da mesma porta, os dois parceiros da VPN não vão ter necessidade de abrir portas adicionais nas firewalls ou escrever novas regras de pacotes para permitir o tráfego através da ligação. O terminal de recepção da ligação pode determinar se o pacote é o pacote IKE ou um pacote encapsulado UDP porque os primeiros 8 bytes da carga útil da UDP foram definidos como zero para um pacote encapsulado UDP. Ambos os terminais da ligação devem suportar encapsulamento UDP para que funcione correctamente. «

Compressão de IP (IPComp)

O protocolo IP Payload Compression (IPComp) reduz o tamanho dos datagramas de IP através da compressão dos mesmos, de modo a aumentar o rendimento nas comunicações entre dois parceiros. O objectivo é aumentar o rendimento geral das comunicações quando estas são efectuadas através de ligações lentas ou congestionadas. O IPComp não fornece qualquer segurança e deve ser utilizado juntamente com uma conversão de AH ou ESP quando é feita uma comunicação através de uma ligação da VPN.

A Internet Engineering Task Force (IETF) define formalmente o IPComp em Request for Comments (RFC) 2393, *IP Payload compression Protocol (IPComp)*. Pode visualizar este RFC na Internet, no seguinte site da Web: http://www.rfc-editor.org .

Filtragem da VPN e IP

A maioria das ligações da VPN requerem regras de filtragem para funcionar correctamente. As regras de filtragem necessárias dependem do tipo de ligação da VPN que está a configurar bem como, do tipo de tráfego que pretende controlar. Normalmente, cada ligação irá ter uma filtragem de políticas. A filtragem de políticas define quais os endereços, protocolos e portas que podem utilizar a VPN. Adicionalmente, as ligações que suportam o protocolo Internet Key Exchange (IKE) contém regras escritas explicitamente para permitir o processamento de IKE na ligação.

Após a V5R1 do sistema operativo, a VPN pode criar estas regras automaticamente. Sempre que for possível, deve permitir que seja a VPN a criar a filtragem de políticas. Isto irá ajudar a eliminar erros e também elimina a necessidade de ter de configurar as regras como um passo separado utilizando o editor de Regras de Pacotes do iSeries Navigator.

É obvio que existem sempre excepções. Reveja estes tópicos para obter mais informações sobre outros conceitos de filtragem e VPN, menos comuns e técnicas que possam ser aplicadas em determinada situação específica:

- **Migrar filtragem de políticas para a edição actual**
  Na V4R1 e V4R5 do sistema operativo, era necessário configurar as regras de pacotes da VPN, como um passo diferente. Não eram geradas automaticamente como parte das configurações da VPN. Neste tópico são apresentadas considerações especiais para a migração das filtragens de políticas da V4R4 e da V4R5 para a edição actual e indicações de como proceder.
- **Ligação da VPN sem filtragem de políticas**
  Se os pontos de terminação da VPN são endereços de IP únicos e específicos e pretende iniciar a VPN sem ter de escrever ou activar regras de filtragem no sistema, pode configurar uma filtragem de políticas dinâmica. Este tópico explica as razões pelas quais pode vir a ter em consideração esta opção e como deve proceder.
- **IKE implícito**
  Para que as negociações de IKE existam na VPN, tem de permitir datagramas UDP pela porta 500 para este tipo de tráfego IP. No entanto, caso não existam regras de filtragem especificamente escritas para permitir o tráfego IKE, então o tráfego IKE está implicitamente garantido no sistema. Leia este tópico para obter mais informações sobre como é que isto funciona no iSeries.

Migrar filtragem de políticas para a edição actual

Nas versões V4R4 e V4R5 do sistema operativo, era necessário configurar as regras de pacotes da VPN como um passo separado na interface Regras de pacotes do iSeries Navigator. Não eram geradas automaticamente como parte das configurações da VPN. Após a V5R1 do sistema operativo, a GUI da VPN pode criar estas regras de pacotes automaticamente.

Existem vários itens que é necessário ter em conta caso tenha criado regras de filtragem de políticas (regras onde action=IPSEC) na V4R4 ou na V4R5 e pretenda utilizar essas mesmas regras na edição actual. Ou uma vez que a VPN *vai* gerar as regras de filtragem de políticas necessita de adicionar regras

adicionais que permitam outro tipo de tráfego IP, por exemplo telnet, na ligação. Siga estas recomendações para ajudá-lo a evitar potenciais erros de configuração.

Para clarificar: Quando este tópico se refere ao ficheiro de regras do *cliente*, está a referir-se a qualquer ficheiro de regras que tenha criado através da utilização do editor Regras de Pacotes no iSeries Navigator. Em contraste com isto está o ficheiro de regras *VPNPOLICYFILTERS.I3P*, que é o ficheiro de regras gerado automaticamente pela VPN como parte das configurações da VPN.

- Se tiver ligações da VPN da V4R4 ou da V4R5 e não tenciona configurar outras ligações da VPN na edição actual, pode activar as regras de filtragem e iniciar as ligações, como habitualmente.
- » Se tiver ligações da VPN da V4R4 ou da V4R5 e planeia configurar novas ligações da VPN na edição actual, deve utilizar o assistente **Migrar Filtragem de Políticas**. O assistente remove a filtragem de políticas dos ficheiros de regras de pacotes criados e insere filtragem de políticas equivalentes no VPNPOLICYFILTERS.I3P, gerado pela VPN. Para ter acesso ao assistente, siga estes passos:
  1. No iSeries Navigator, expanda o servidor **—>Rede —>Políticas de IP**.
  2. Faça clique com o botão direito do rato sobre **Virtual Private Networking** e seleccione **Migrar Filtragem de Políticas**.
  3. Quando concluir o assistente, faça clique sobre **Terminar**.
  4. Faça clique sobre **Ajuda** caso tenha questões sobre o preenchimento de uma página ou de qualquer um dos respectivos campos.«
- Se a VPN gerou as regras de filtragem de políticas, mas é necessário adicionar algumas regras de filtragem não VPN, deve configurar estas regras utilizando o Editor de Regras de Pacotes no iSeries Navigator. Caso alguma destas regras de filtragem não VPN tenham de ser introduzidas antes dos filtros da VPN, os nomes dos conjuntos das mesmas devem começar por `PREIPSEC`. Por exemplo, `PREIPSECMIRULES`. Isto irá ajudar o sistema a determinar a ordem pela qual deverão ser feitas as regras de filtragem. Os nomes de conjunto de todas as outras regras não VPN não devem ter o prefixo `PREIPSEC`. Por exemplo, `MAISREGRAS`.
- Deve sempre permitir que a VPN crie as regras de filtragem de políticas. No entanto, as regras de filtragem não VPN devem permanecer no ficheiro de regras do cliente. Lembre-se que, se for necessário introduzir qualquer um destes filtros não VPN antes dos filtros de políticas no ficheiro de regras VPNPOLICYFILTERS, terá de adicionar `PREIPSEC` como prefixo ao nome do conjunto. Assim assegura-se de que as regras do cliente e as regras da VPN funcionam em conjunto como o pretendido. Por exemplo, a VPN gerou as regras de filtragem de políticas (conjuntos da VPN),mas foram adicionadas regras adicionais (as seus conjuntos) de forma a permitir outro tráfego IP através da ligação. Quando carrega as regras no sistema, elas são ordenadas da seguinte forma:
  1. Conjuntos cujos nomes começam por PREIPSEC
  2. Conjuntos da VPN cujos nomes começam por PREIPSEC
  3. Conjuntos da VPN com ACTION=IPSEC (filtragem de políticas)
  4. Conjuntos com ACTION=IPSEC (filtragem de políticas)
  5. Os restantes conjuntos.
  6. Os restantes conjuntos da VPN.

  Verifique o ficheiro EXPANDED.OUT para visualizar a ordem do ficheiro de saída de dados intercalado. EXPANDED.OUT é escrito no directório onde o ficheiro de regras de clientes está localizado.
- » Ao utilizar o iSeries Navigator, pode escolher para activação:
  – apenas o ficheiro de regras gerado pela VPN, VPNPOLICYFILTERS.I3P
  – apenas o ficheiro de regras cliente
  – o ficheiro de regras gerado pela VPN e o ficheiro de regras cliente «
- Active as regras de filtragem em todas as interfaces em vez de numa interface individual. Isto ajuda a garantir que os filtros serão activados e que definirão a ordem correcta dos filtros de políticas.

- Deve sempre verificar as regras de filtragem antes de tentar activá-las. Se a verificação for feita sem erros, deve em seguida verificar o EXPANDED.OUT para se certificar de que as regras estão ordenadas como o pretendido. Após a conclusão deste passo, pode activar as regras.

Ligações da VPN sem filtragem de políticas

» Uma regra de filtragem de políticas define quais os endereços, protocolos e portas que podem utilizar uma VPN e direcciona o tráfego apropriado através da ligação. Em alguns casos, pode querer configurar uma ligação que não necessita de uma regra de filtragem de políticas. Por exemplo, pode ter carregadas regras de pacotes não VPN na interface a utilizar pela ligação da VPN assim, em vez de desactivar as regras activas nessa interface, decide configurar a VPN de forma a que o sistema faça a gestão dinâmica de todos os filtros para essa ligação. A filtragem de política para este tipo de ligação é referida como **filtragem de políticas dinâmica**. Antes de poder utilizar uma filtragem de políticas dinâmica na ligação da VPN, deve garantir o seguinte:

- A ligação só pode ser iniciada pelo servidor local.
- Os pontos de terminação de dados da ligação têm de ser sistemas únicos. Isto é, não podem ser sub-redes ou uma intervalo de endereços.
- Não pode ser carregada qualquer regra de filtragem de política para a ligação.

Caso se verifiquem todos estes critérios, pode configurar a ligação para que não seja necessária uma filtragem de políticas. Quando a ligação é iniciada, o tráfego entre os pontes de terminação de dados irá ocorrer independentemente das regras de pacotes que estejam activas no sistema.

Para obter instruções passo-a-passo sobre como configurar uma ligação para que não seja necessário uma filtragem de política, utilize a ajuda para a VPN. «

IKE implícito

» Para estabelecer uma comunicação, a maioria das VPNs necessitam que as negociações do Internet Key Exchange (IKE)ocorram para que o processamento IPSec possa ser executado. O IKE utiliza a bem conhecida porta 500, assim para que o IKE funcione correctamente, necessita de permitir datagramas UDP pela porta 500 para este tipo de tráfego IP. Caso não existam regras de filtragem especificamente escritas para permitir o tráfego IKE, então o tráfego IKE está implicitamente garantido. No entanto, as regras escritas especificamente para o tráfego UDP pela porta 500 são geridas com base no que está definido nas regras de filtragem activas. «

Planear a VPN

O planeamento é uma parte essencial de uma solução VPN global. Há que tomar muitas decisões complexas para garantir que a ligação funcione adequadamente. Utilize estes recursos para recolher todas as informações necessárias para garantir o sucesso da VPN:

- **Requisitos de configuração da VPN**
  Antes de começar, certifique-se de que dispõe dos requisitos mínimos para criar uma VPN.
- **Determinar que tipo de VPN deve criar**
  Determinar a forma como utilizar a VPN é um dos primeiros passos para um planeamento bem sucedido. Este tópico descreve os vários tipos de ligação que podem ser configurados.
- **Utilize o consultor de planeamento da VPN**
  O consultor de planeamento coloca questões sobre a rede e, com base nas respostas, fornece sugestões para criar a VPN.
  Nota: Utilize apenas o consultor de planeamento da VPN para ligações que suportem o protocolo Internet Key Exchange (IKE). Utilize a folha de trabalho de planeamento para ligações manuais para os tipos de ligações manuais.
- **Preencher as folhas de trabalho de planeamento da VPN**
  Caso prefira, pode imprimir e preencher as folhas de trabalho de planeamento para recolher informações detalhadas sobre os planos de utilização da VPN.

Depois de planear a VPN, pode começar a configurá-la.

Requisitos de configuração da VPN

Para funcionar correctamente no iSeries e com clientes de rede, certifique-se de que o iSeries e o PC cliente cumprem os seguintes requisitos:

Requisitos do iSeries na V5R2

- OS/400, Versão 5 Edição 2 (5722-SS1) ou posterior
- Digital Certificate Manager (5722-SS1 Opção 34)
- Cryptographic Access Provider (5722-AC2 ou AC3)
- iSeries Access for Windows(5722-XE1) e iSeries Navigator
  - Componente de rede do iSeries Navigator
- Definir o valor do sistema de retenção de dados de segurança do servidor (QRETSVRSEC *SEC), para 1
- O TCP/IP deve ser configurado, incluindo as interfaces de IP, os encaminhamentos, o nome do sistema central local e o nome do domínio local

Requisitos do cliente

- Uma estação de trabalho com um sistema operativo de 32 bits do Windows correctamente ligado ao iSeries e configurado para TCP/IP
- Uma unidade de processamento de 233 Mhz
- 32 MB RAM para clientes Windows 95/98
- 64 MB RAM para clientes Windows NT e 2000
- iSeries Access for Windows e o iSeries Navigator instalados no PC cliente
- Software que suporte o protocolo IP Security (IPSec)
- Software que suporte o L2TP, se os utilizadores remotos utilizarem o L2TP para estabelecer uma ligação com o seu sistema.

Determinar que tipo de VPN deve criar

Determinar a forma como utilizar a VPN é um dos primeiros passos para um planeamento bem sucedido. Para tal, deve compreender o papel que tanto o servidor de chaves local, como o servidor de chaves remoto desempenham na ligação. Por exemplo, os pontos de terminação da *ligação* são diferentes dos pontos de terminação dos *dados*? São iguais ou alguma combinação de ambos? Os pontos de terminação da ligação autenticam e codificam (ou descodificam) o tráfego de dados da ligação e, como opção, proporcionam a gestão das chaves através do protocolo Internet Key Exchange (IKE). Os pontos de terminação de dados, por outro lado, definem a ligação entre dois sistemas face ao tráfego IP que flui pela VPN; por exemplo, todo o tráfego TCP/IP entre 123.4.5.6 e 123.7.8.9. De modo geral, quando os pontos de terminação de dados e da ligação são diferentes, o servidor da VPN é uma porta de ligação. Quando são iguais, o servidor da VPN é um sistema central.

Os vários tipos de implementações da VPN com capacidade para corresponder às necessidades das empresas são:

Porta de ligação a porta de ligação
Os pontos de terminação da ligação de ambos os sistemas são diferentes dos pontos de terminação de dados. O protocolo IP Security (IPSec) protege o tráfego à medida que este circula entre as portas de ligação. No entanto, o IPSec não protege o tráfego de dados em ambos os lados das portas de ligação, dentro das redes internas. Esta é uma configuração normal das ligações entre sucursais, pois o tráfego encaminhado para além das portas de ligação das sucursais, para dentro das redes internas, é frequentemente considerado como fiável.

Porta de ligação a sistema central
O IPSec protege o tráfego de dados à medida que este circula entre a porta de ligação e um sistema central numa rede remota. A VPN não protege o tráfego de dados dentro da rede local, pois é considerado fiável.

Sistema central a porta de ligação
A VPN protege o tráfego de dados à medida que este circula entre um sistema central de uma rede local e uma porta de ligação remota. A VPN não protege o tráfego de dados dentro da rede remota.

Sistema central a sistema central
Os pontos de terminação da ligação são iguais aos pontos de terminação de dados, tanto no sistema local como no remoto. A VPN protege o tráfego de dados à medida que este circula entre um sistema central numa rede local e um sistema central numa rede remota. Este tipo de VPN proporciona uma protecção IPSec extremo a extremo.

Preencher as folhas de trabalho de planeamento da VPN

Utilize as folhas de trabalho de planeamento da VPN para recolher informações detalhadas sobre os planos de utilização da VPN. Estas informações são necessárias para planear adequadamente a estratégia da VPN. Pode também utilizar estas informações para configurar a VPN. Escolha a folha de trabalho para o tipo de ligação que pretende criar.

- **Folha de trabalho de planeamento para ligações dinâmicas**
  Conclua esta folha de cálculo antes de configurar uma ligação dinâmica.
- **Folha de trabalho de planeamento para ligações manuais**
  Conclua esta folha de cálculo antes de configurar uma ligação manual.
- **Consultor de planeamento da VPN**
  Pode ainda, se preferir, utilizar o consultor para planeamento interactivo e instruções de configuração. O consultor de planeamento coloca questões sobre a rede e, com base nas respostas, fornece sugestões para criar a VPN.

  Nota: Utilize apenas o consultor de planeamento da VPN para as ligações dinâmicas. Utilize a folha de trabalho de planeamento para ligações manuais para os tipos de ligações manuais.

Se criar várias ligações com propriedades semelhantes, poderá querer definir os valores assumidos da VPN. Os valores assumidos configurados permanecem nas folhas de propriedade da VPN. Isto significa que não é necessário configurar as mesmas propriedades várias vezes. Para definir os valores assumidos da VPN, seleccione **Editar** no menu principal da VPN e, depois, seleccione **Valores assumidos**.

Folha de trabalho de planeamento para ligações dinâmicas

Antes de criar ligações da VPN dinâmicas, preencha esta folha de trabalho. A folha de trabalho pressupõe que irá utilizar o Assistente de Nova Ligação. O assistente permite-lhe configurar uma VPN com base nos seus requisitos de segurança básicos. Em alguns casos, poderá necessitar de especificar as propriedades que o assistente configura para a ligação. Por exemplo, poderá decidir que pretende o registo em diário ou que o servidor da VPN inicie sempre que o TCP/IP iniciar. Se for este o caso, faça clique com o botão direito do rato sobre o grupo de chaves dinâmicas ou sobre a ligação criada pelo assistente e seleccione **Propriedades**.

Deve responder a cada questão antes de continuar com a configuração da VPN.

Lista de selecção de pré-requisitos	Respostas
O OS/400 está na V5R2 (5722-SS1) ou posterior?	
A opção Digital Certificate Manager (5722-SS1 Opção 34) está instalada?	

O Cryptographic Access Provider (5722-AC2 ou AC3) está instalado?	
O iSeries Access (5722-XE1) está instalado?	
O iSeries Navigator está instalado?	
O subcomponente de Rede do iSeries Navigator está instalado?	
O TCP/IP Connectivity Utilities for OS/400 (5722-TC1) está instalado?	
Definiu o valor do sistema de retenção de dados de segurança do servidor (QRETSVRSEC *SEC), para 1?	
O TCP/IP está configurado no iSeries (incluindo interfaces de IP, encaminhamentos, nome do sistema central local e nome do domínio local)?	
Foi estabelecida uma comunicação de TCP/IP normal entre os pontos de terminação necessários?	
Aplicou as mais recentes correcções temporárias de programas (PTFs)?	
Se o direccionamento de VPN atravessa firewalls ou encaminhadores que implementam filtragem de pacotes de IP, as regras de filtragem da firewall ou do encaminhador suportam protocolos AH e ESP?	
As firewalls ou os encaminhadores estão configurados para permitir os protocolos IKE (UDP porta 500), AH e ESP?	
As firewalls estão configuradas para permitir o reencaminhamento de IP?	

Necessita destas informações para configurar uma ligação dinâmica da VPN	**Respostas**
Que tipo de ligação está a criar? • Porta de ligação a porta de ligação • Sistema central a porta de ligação • Porta de ligação a sistema central • Sistema central a sistema central	
Que nome irá dar ao grupo de chaves dinâmicas?	
De que tipo de segurança e de rendimento de sistema necessita para proteger as suas chaves? • Segurança máxima, rendimento mínimo • Segurança e rendimento equilibrados • Segurança mínima e rendimento máximo	
Está a utilizar certificados para autenticar a ligação? Em caso negativo, qual é a chave pré-partilhada?	
Qual é o identificador do servidor de chaves local?	
Qual é o identificador do ponto de terminação de dados local?	
Qual é o identificador do servidor de chaves remoto?	
Qual é o identificador do ponto de terminação de dados remoto?	
De que tipo de segurança e de rendimento de sistema necessita para proteger os seus dados? • Segurança máxima, rendimento mínimo • Segurança e rendimento equilibrados • Segurança mínima e rendimento máximo	

Folha de trabalho de planeamento para ligações manuais

Preencha esta folha de trabalho para ajudá-lo a criar as ligações da Rede privada virtual (VPN) que não utilizam IKE para a gestão de chaves.

Deve responder a cada uma destas questões antes de continuar com a configuração da VPN:

Lista de selecção de pré-requisitos	Respostas
O OS/400 está na versão V5R2 (5722-SS1) ou posterior?	
A opção Digital Certificate Manager (5722-SS1 Opção 34) está instalada?	
O Cryptographic Access Provider (5722-AC2 ou AC3) está instalado?	
O iSeries Access (5722-XE1) está instalado?	
O iSeries Navigator está instalado?	
O subcomponente de Rede do iSeries Navigator está instalado?	
O TCP/IP Connectivity Utilities for OS/400 (5722-TC1) está instalado?	
Definiu o valor do sistema de retenção de dados de segurança do servidor (QRETSVRSEC *SEC), para 1?	
O TCP/IP está configurado no iSeries (incluindo interfaces de IP, encaminhamentos, nome do sistema central local e nome do domínio local)?	
Foi estabelecida uma comunicação de TCP/IP normal entre os pontos de terminação necessários?	
Aplicou as mais recentes correcções temporárias de programas (PTFs)?	
Se o direccionamento de VPN atravessa firewalls ou encaminhadores que implementam filtragem de pacotes de IP, as regras de filtragem da firewall ou do encaminhador suportam protocolos AH e ESP?	
As firewalls ou os encaminhadores estão configurados para permitir os protocolos AH e ESP?	
As firewalls estão configuradas para permitir o reencaminhamento de IP?	

Necessita destas informações para configurar uma VPN manual	Respostas
Que tipo de ligação está a criar? • Sistema central a sistema central • Sistema central a porta de ligação • Porta de ligação a sistema central • Porta de ligação a porta de ligação	
Que nome irá dar à ligações?	
Qual é o identificador do ponto de terminação da ligação local?	
Qual é o identificador do ponto de terminação da ligação remota?	
Qual é o identificador do ponto de terminação de dados local?	
Qual é o identificador do ponto de terminação de dados remoto?	
Que tipo de tráfego irá permitir para esta ligação (porta local, porta remota e protocolo)?	
Pretende conversão de endereços para esta ligação? Consulte Conversão de endereços de rede para VPN para mais informações.	
Irá utilizar o modo de direccionamento ou modo de transporte?	
Que protocolo IPSec irá a ligação utilizar (AH, ESP ou AH com ESP)? Consulte IP Security (IPSec) para mais informações.	
Que algoritmo de autenticação irá a ligação utilizar (HMAC-MD5 ou HMAC-SHA)?	
Que algoritmo de codificação irá a ligação utilizar (DES-CBC ou 3DES-CBC)? **Nota:** Especifique apenas um algoritmo de codificação, se seleccionou ESP como protocolo IPSec.	

Necessita destas informações para configurar uma VPN manual	Respostas
Qual é a chave de recepção do AH? Se utilizar MD5, a chave é uma cadeia hexadecimal de 16 bytes. Se utilizar SHA, a chave é uma cadeia hexadecimal de 20 bytes. A sua chave de recepção deve corresponder exactamente à chave de envio do servidor remoto.	
Qual é a chave de envio do AH? Se utilizar MD5, a chave é uma cadeia hexadecimal de 16 bytes. Se utilizar SHA, a chave é uma cadeia hexadecimal de 20 bytes. A sua chave de envio deve corresponder exactamente à chave de recepção do servidor remoto.	
Qual é a chave de recepção do ESP? Se utilizar DES, a chave é uma cadeia hexadecimal de 8 bytes. Se utilizar 3DES, a chave é uma cadeia hexadecimal de 24 bytes. A sua chave de recepção deve corresponder exactamente à chave de envio do servidor remoto.	
Qual é a chave de envio do ESP? Se utilizar DES, a chave é uma cadeia hexadecimal de 8 bytes. Se utilizar 3DES, a chave é uma cadeia hexadecimal de 24 bytes. A sua chave de envio deve corresponder exactamente à chave de recepção do servidor remoto.	
Qual é o Índice de Políticas de Segurança (SPI) de recepção? O SPI de recepção é uma cadeia hexadecimal de 4 bytes, em que o primeiro byte está definido para 00. O seu SPI de recepção deve corresponder exactamente ao SPI de envio do servidor remoto.	
Qual é o SPI de envio? O SPI de envio é uma cadeia hexadecimal de 4 bytes. O seu SPI de envio deve corresponder exactamente ao SPI de recepção do servidor remoto.	

Configurar a VPN

A VPN proporciona-lhe várias formas diferentes para configurar as ligações da VPN. Continue a leitura para que possa, mais facilmente, decidir qual o tipo de ligação a configurar e como fazê-lo.

Qual o tipo de ligação que devo configurar?
Uma ligação **dinâmica** é uma ligação que gere e negoceia dinamicamente as chaves que a protegem, enquanto está activa, através da utilização do protocolo Internet Key Exchange (IKE). As ligações dinâmicas fornecem um nível de segurança extra para os dados que nelas circulam, pois as chaves são alteradas automaticamente, em intervalos regulares. Desta forma, é menos provável que um elemento estranho capture uma chave, tenha tempo para quebrá-la e utilize-a para desviar ou capturar o tráfego que a chave protege.

Uma ligação **manual (Consulte 40)**, por outro lado, não fornece suporte para negociações IKE e consequentemente, administração de chaves automática. Além disso, ambos os extremos da ligação exigem que configure vários atributos que devem corresponder de forma exacta. As ligações manuais utilizam chaves estáticas que não são actualizadas ou alteradas enquanto a ligação estiver activa. Deve parar uma ligação manual para alterar a respectiva chave associada. Se considerar este facto um risco para a segurança, crie uma ligação dinâmica.

Como configurar uma ligação da VPN dinâmica?
Uma VPN é, na verdade, um grupo de objectos da configuração que definem as características de uma

ligação. Uma ligação da VPN dinâmica necessita que cada um deste objectos funcione correctamente. Siga as ligações abaixo para obter informações específicas sobre como configurar cada um dos objectos da configuração da VPN:

Sugestão:
Configurar ligações com o assistente de Nova Ligação
De modo geral, deve utilizar o assistente de Ligação para criar todas as ligações dinâmicas. O assistente cria automaticamente cada um dos objectos de configuração que a VPN necessita para funcionar correctamente, incluindo as regras de pacotes. Se especificar que pretende que o assistente active as regras de pacotes da VPN, pode ignorar os passos até ao passo seis, abaixo: *Iniciar a ligação*. Caso contrário, depois de o assistente terminar a configuração da VPN, o utilizador deve activar as regras de pacotes e, em seguida, poderá iniciar a ligação.

Caso opte por não utilizar o assistente para configurar as ligações da VPN dinâmicas, siga estes passos para concluir a configuração:

1. **Configurar políticas de segurança da VPN**
   Deve definir as políticas de segurança da VPN para todas as ligações dinâmicas. A política do Internet Key Exchange e política de dados determinam a forma como o IKE protege as respectivas negociações de fase 1 e fase 2. As configurações que executar a seguir dependem do tipo de ligação que utilizar.
2. **Configurar ligações seguras**
   Uma vez definidas as políticas de segurança para uma ligação, deve em seguida configurar a ligação segura. Para as ligações dinâmicas, o objecto da ligação segura inclui um grupo e uma ligação de chaves dinâmicas. O **grupo de chaves dinâmicas** define as características comuns de uma ou mais ligações da VPN, enquanto que a **ligação de chaves dinâmicas** define as características de ligações de dados individuais entre pares de pontos de terminação. A ligação de chaves dinâmicas existe dentro do grupo de chaves dinâmicas.

   Nota: Só é necessário concluir os dois passos seguintes, *Configurar regras de pacotes* e *Definir uma interface para as regras*, se seleccionar a opção **A regra de filtragem de políticas será definida nas Regras de Pacotes**, na página **Grupo de Chaves Dinâmicas - Ligações** da interface da VPN. Caso contrário, estas regras são criadas como parte das configurações da VPN e são aplicadas à interface especificada.

   É recomendado que permita sempre que a interface da VPN crie as regras de filtragem de políticas. Pode fazê-lo se seleccionar a opção **Gerar a seguinte filtragem de políticas para este grupo**, na página **Grupo de Chaves Dinâmicas - Ligações**.
3. **Configurar regras de pacotes**
   Depois de concluir as configurações da VPN, deve criar e aplicar regras de filtragem que permitam ao tráfego de dados circular pela ligação. As regras **pré-IPSec** da VPN permitem todo o tráfego do IKE nas interfaces especificadas, de modo a que o IKE possa negociar ligações. A regra de **filtragem de políticas** define quais os endereços, os protocolos e as portas que podem utilizar o novo grupo de chaves dinâmicas associado.

   Se está a fazer a migração a partir da V4R4 ou da V4R5 e tem a filtragem de políticas e de ligações da VPN e pretende continuar a edição actual, deve rever o tópico *Migrar filtragem de políticas para a edição actual* para garantir que a filtragem de políticas anterior e a actual irão funcionar em conjunto como pretende.
4. **Definir uma interface para as regras**
   Depois de configurar as regras de pacotes e quaisquer outras regras de que necessite para activar a ligação da VPN, deve definir uma interface à qual aplicá-las.
5. **Activar regras de pacotes**
   Depois de definir uma interface para as regras de pacotes, deve activá-las antes de poder iniciar a ligação.
6. **Iniciar a ligação**
   Conclua esta tarefa para iniciar as ligações.

Como configurar uma ligação da VPN manual?
Tal como o nome sugere, uma ligação manual é uma ligação em que deve configurar todas as propriedades da VPN de forma manual, incluindo chaves de recepção e de envio. Siga as ligações abaixo para obter informações específicas sobre como configurar uma ligação manual:

1. **Configurar ligações manuais**
   As ligações manuais definem as características de uma ligação, incluindo os protocolos de segurança e os pontos de terminação da ligação e de dados.

   Nota: Só é necessário concluir os dois passos seguintes, *Configurar regra de filtragem de políticas* e *Definir uma interface para as regras*, se seleccionar a opção **A regra de filtragem de políticas será definida nas Regras de Pacotes**, na página **Ligação Manual - Ligação** da interface da VPN. Caso contrário, estas regras são criadas como parte das configurações da VPN.

   É recomendado que permita sempre que a interface da VPN crie as regras de filtragem de políticas. Pode fazê-lo através da selecção da opção **Gerar um filtro que corresponda aos pontos de terminação de dados**, na página **Ligação Manual - Ligação**.
2. **Configure uma regra de filtragem de políticas**
   Após a configuração dos atributos da ligação manual, deve criar e aplicar uma regra de filtragem de políticas que permita ao tráfego de dados circular pela ligação. A regra de **filtragem de políticas** define quais os endereços, os protocolos e as portas podem utilizar a ligação associada.
3. **Definir uma interface para as regras**
   Depois de configurar as regras de pacotes e quaisquer outras regras de que necessite para activar a ligação da VPN, deve definir uma interface à qual aplicá-las.
4. **Activar regras de pacotes**
   Depois de definir uma interface para as regras de pacotes, deve activá-las antes de poder iniciar a ligação.
5. **Iniciar a ligação**
   Conclua esta tarefa para iniciar ligações iniciadas localmente.

Configurar ligações da VPN com o assistente de Nova Ligação

O assistente de Nova Ligação permite-lhe criar uma rede privada virtual (VPN, virtual private network) entre qualquer combinação de sistemas centrais e portas de ligação. Por exemplo, sistema central a sistema central, porta de ligação a sistema central, sistema central a porta de ligação ou porta de ligação a porta de ligação.

O assistente cria automaticamente cada um dos objectos de configuração que a VPN necessita para funcionar correctamente, incluindo as regras de pacotes. No entanto, se necessitar de adicionar uma função à VPN como, por exemplo, registo em diário ou conversão de endereços para a VPN (VPN NAT), poderá querer especificar a VPN através das folhas de propriedades da ligação ou do grupo de chaves dinâmicas apropriadas. Para fazê-lo, deve primeiro parar a ligação, se esta estiver activa. Depois, faça clique com o botão direito do rato sobre a ligação ou grupo de chaves dinâmicas e seleccione **Propriedades**.

Conclua o consultor de planeamento da VPN antes de começar. O consultor fornece-lhe um meio para obter informações importantes necessárias para a criação da VPN.

Para criar uma VPN com o assistente de Ligação, siga estes passos:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Virtual Private Networking** e seleccione **Nova Ligação** para iniciar o assistente.
3. Conclua o assistente para criar uma ligação básica da VPN. Faça clique sobre **Ajuda** caso necessite de assistência.

Configurar políticas de segurança da VPN

Depois de determinar a forma como irá utilizar a VPN, deve definir as políticas de segurança da VPN. Especificamente, é necessário:

- **Configurar uma política do Internet Key Exchange (IKE)**
  A política do IKE define qual o nível de autenticação e de protecção de codificação é utilizado pelo IKE durante as negociações da fase 1. A fase 1 do IKE estabelece as chaves que protegem as mensagens que circulam nas negociações da fase 2 subsequentes. Não necessita de definir uma política do IKE ao criar uma ligação manual. Além disso, se criar a VPN com o assistente de Nova Ligação, este pode criar igualmente uma política do IKE.
- **Configurar uma política de dados**
  Uma política de dados define qual o nível de autenticação ou de codificação que protege os dados que circulam na VPN. Os sistemas comunicantes acordam estes atributos durante as negociações da fase 2 do protocolo Internet Key Exchange (IKE). Não necessita de definir uma política de dados ao criar uma ligação manual. Além disso, se criar a VPN com o assistente de Nova Ligação, este pode criar igualmente a política de dados.

Após a configuração das políticas de segurança da VPN, deve, em seguida, configurar as ligações seguras.

Configurar uma política do Internet Key Exchange (IKE)

Uma política de IKE define qual o nível de autenticação ou de codificação é utilizado pelo IKE de protecção durante as negociações da fase 1. A fase 1 do IKE estabelece as chaves que protegem as mensagens que circulam nas negociações da fase 2 subsequentes. A VPN utiliza o modo de assinatura RSA ou as chaves pré-partilhadas para autenticar negociações de fase 1. Se tenciona utilizar certificados digitais para autenticar os servidores de chaves, deve configurá-los previamente através do Digital Certificate Manager (5722-SS1 Opção 34). A política de IKE também identifica qual o servidor de chaves remoto que irá utilizar esta política.

Para definir uma política de IKE ou efectuar alterações numa já existente, siga estes passos:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP—> Virtual Private Networking—> Políticas de Segurança de IP**.
2. Para criar uma nova política, faça clique com o botão direito do rato sobre **Políticas do Internet Key Exchange** e seleccione **Nova Política do Internet Key Exchange**. Para efectuar alterações numa política existente, faça clique sobre **Políticas do Internet Key Exchange** no painel da esquerda, em seguida faça clique com o botão direito do rato sobre a política que pretende alterar no painel da direita e seleccione **Propriedades**.
3. Preencha cada uma das folhas de propriedades. Faça clique sobre **Ajuda** caso tenha questões acerca do preenchimento de uma página ou de qualquer um dos respectivos campos.
4. Faça clique sobre **OK** para guardar as alterações.

Configurar uma política de dados

Uma política de dados define qual o nível de autenticação ou de codificação que protege os dados que circulam na VPN. Os sistemas comunicantes acordam estes atributos durante as negociações da fase 2 do protocolo Internet Key Exchange (IKE).

Para definir uma política de dados ou efectuar alterações numa já existente, siga estes passos:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP—> Virtual Private Networking—> Políticas de Segurança de IP**.
2. Para criar uma nova política de dados, faça clique com o botão direito do rato sobre **Políticas de Dados** e seleccione **Nova Política de Dados**. Para efectuar alterações numa política de dados existente, faça clique sobre **Políticas de Dados** (no painel da esquerda), em seguida faça clique com o botão direito do rato sobre a política de dados que pretende alterar (no painel da direita) e seleccione **Propriedades**.

3. Preencha cada uma das folhas de propriedades. Faça clique sobre **Ajuda** caso tenha questões acerca do preenchimento de uma página ou de qualquer um dos respectivos campos.
4. Faça clique sobre **OK** para guardar as alterações.

Configurar a ligação segura da VPN

Após a configuração das políticas de segurança para a ligação, deve em seguida configurar a ligação segura. Para as ligações dinâmicas, o objecto da ligação segura inclui um grupo e uma ligação de chaves dinâmicas.

O **grupo de chaves dinâmicas** define as características comuns de uma ou mais ligações da VPN. Configurar um grupo de chaves dinâmicas permite-lhe utilizar as mesmas políticas, mas diferentes pontos de terminação de dados para cada ligação dentro do grupo. Os grupos de chaves dinâmicas permitem-lhe ainda negociar de forma bem sucedida com os iniciadores remotos, quando os pontos de terminação de dados propostos pelo sistema remoto não são especificamente conhecidos com antecedência. Os grupos procedem a esta negociação associando as informações sobre políticas no grupo de chaves dinâmicas a uma regra de filtragem de políticas com um tipo de acção IPSEC. Se os pontos de terminação de dados específicos facultados pelo iniciador remoto estiverem dentro do intervalo especificado na regra de filtragem IPSEC, podem ficar sujeitos à política definida no grupo de chaves dinâmicas.

A **ligação de chaves dinâmicas** define as características de ligações de dados individuais entre pares de pontos de terminação. A ligação de chaves dinâmicas existe dentro do grupo de chaves dinâmicas. Após a configuração de um grupo de chaves dinâmicas para descrever que políticas as ligações no grupo devem utilizar, é necessário criar ligações de chaves dinâmicas individuais para ligações iniciadas localmente.

Para configurar o objecto da ligação segura, conclua estas tarefas:

Parte 1: Configurar um grupo de chaves dinâmicas:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP—> Virtual Private Networking—> Ligações Seguras**.
2. Faça clique com o botão direito do rato sobre **Por Grupo** e seleccione **Novo Grupo de Chaves Dinâmicas**.
3. Faça clique sobre **Ajuda** caso tenha questões acerca do preenchimento de uma página ou de qualquer um dos respectivos campos.
4. Faça clique sobre **OK** para guardar as alterações.

Parte 2: Configurar uma ligação de chaves dinâmicas:

1. No iSeries Navigator, expanda o servidor **—> Rede —> Políticas de IP—> Virtual Private Networking—> Ligações Seguras—> Por Grupo**.
2. No painel da esquerda da janela iSeries Navigator, faça clique com o botão direito do rato sobre o grupo de chaves dinâmicas criado na parte um e seleccione **Nova Ligação de Chaves Dinâmicas**.
3. Faça clique sobre **Ajuda** caso tenha questões acerca do preenchimento de uma página ou de qualquer um dos respectivos campos.
4. Faça clique sobre **OK** para guardar as alterações.

Após a conclusão destes passos, é necessário activar as regras de pacotes que a ligação necessita para funcionar correctamente.

Nota: Na maior parte dos casos, deve permitir que a interface da VPN gere automaticamente as regras de pacotes da VPN, através da selecção da opção **Gerar a seguinte filtragem de políticas para este grupo**, na página **Grupo de Chaves Dinâmicas - Ligações**. Contudo, se seleccionar a opção **A filtragem de políticas será definida nas Regras de Pacotes**, deve configurar regras de pacotes da VPN utilizando o editor de Regras de Pacotes e, em seguida, activá-las.

Configurar uma ligação manual

Tal como o nome sugere, uma ligação manual é uma ligação em que deve configurar todas as propriedades da VPN de forma manual. Além disso, ambos os extremos da ligação exigem que configure vários elementos que devem corresponder de forma *exacta*. Por exemplo, as chaves de recepção devem corresponder às chaves de envio do sistema remoto ou a ligação falhará.

As ligações manuais utilizam chaves estáticas que não são actualizadas ou alteradas enquanto a ligação estiver activa. Deve parar uma ligação manual para alterar a respectiva chave associada. Se considerar este facto um risco para a segurança e que ambas os extremos da ligação suportam o Internet Key Exchange (IKE), deve considerar a configuração de uma ligação dinâmica.

Para definir as propriedades da sua ligação manual, siga estes passos:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP—> Virtual Private Networking—> Ligações Seguras**.
2. Faça clique com o botão direito do rato sobre **Todas as Ligações** e seleccione **Nova Ligação Manual**.
3. Preencha cada uma das folhas de propriedades. Faça clique sobre **Ajuda** caso tenha questões acerca do preenchimento de uma página ou de qualquer um dos respectivos campos.
4. Faça clique sobre **OK** para guardar as alterações.

Nota: Na maior parte dos casos, deve permitir que a interface da VPN gere automaticamente as regras de pacotes da VPN, seleccionando a opção **Gerar uma filtragem de políticas que corresponda aos pontos de terminação de dados**, na página **Ligação Manual - Ligação**. Contudo, se seleccionar a opção **A filtragem de políticas será definida nas Regras de Pacotes**, deve configurar uma regra de filtragem de políticas manualmente e, em seguida, activá-las.

Configurar regras de pacotes da VPN

Se estiver a criar uma ligação pela primeira vez, deve permitir que a VPN gere automaticamente as regras de pacotes da VPN. Pode fazê-lo através da utilização do assistente de Nova Ligação ou das páginas de propriedades da VPN para configurar a ligação.

Caso decida criar as suas próprias regras de pacotes da VPN utilizando o editor de Regras de Pacotes no iSeries Navigator, deverá também criar quaisquer regras adicionais da mesma forma. De modo oposto, se for a VPN a criar as regras de filtragem de políticas, deve criar todas as regras de filtragem de políticas adicionais desta forma.

Normalmente as VPNs requerem dois tipos de regras de filtragem: Regras de filtragem de Pre-IPSec e regras de filtragem de políticas. Reveja os tópicos abaixo para saber como deve configurar estas regras utilizando o editor de Regras de Pacotes no iSeries Navigator. Se quiser ler mais sobre outras VPNs e opções de filtragem, consulte a secção *VPN e filtragem de IP* do tópico conceitos da VPN.

- **Regras Pré-IPSec**
  As regras pré-IPSec são quaisquer regras no sistema anteriores às regras com um tipo de acção IPSEC. Este tópico só discute as regras pré-IPSec necessárias para o funcionamento correcto da VPN. Neste caso, as regras pré-IPSec são um par de regras que permitem o processamento do IKE na ligação. O IKE permite a ocorrência da geração de chaves dinâmicas e de negociações na ligação. Poderá ser necessário adicionar outras regras pré-IPSec, dependendo do ambiente de rede e da política de segurança.

  Nota: Apenas necessita de configurar este tipo de regra pré-IPSec se já tiver outras regras que permitam IKE para sistemas específicos. Caso não existam regras de filtragem especificamente escritas para permitir o tráfego IKE, então o tráfego IKE está implicitamente garantido.
- **Regra de filtragem de políticas**
  A regra de filtragem de políticas define o tráfego que pode utilizar a VPN e qual a política de protecção de dados a aplicar a esse tráfego.

Considerações a ter antes de começar
Quando adiciona regras de filtragem a uma interface, o sistema adiciona automaticamente uma regra DENY de valor assumido a essa interface. Isto significa que qualquer tráfego que não seja expressamente permitido é recusado. Não é possível visualizar ou alterar esta regra. Desta forma, pode acontecer que tráfego que funcionava anteriormente falhe misteriosamente, após a activação das regras de filtragem da VPN. Se pretender permitir outro tráfego na interface para além do da VPN, deve adicionar regras PERMIT explícitas para fazê-lo.

Depois de configurar as regras de filtragem adequadas, deve definir a interface às quais são aplicadas e, depois, activá-las.

É fundamental que configure as regras de filtragem de forma correcta. Caso contrário, as regras de filtragem podem bloquear todo o tráfego IP que entra e sai do iSeries. Isto inclui a ligação ao iSeries Navigator, utilizada para configurar as regras de filtragem.

Se as regras de filtragem não permitirem o tráfego no iSeries Navigator, este não pode comunicar com o iSeries. Se porventura ficar nesta situação, terá de iniciar a sessão do iSeries através de uma interface que ainda tenha conectividade, como a consola de operações. Utilize o comando RMVTCPTBL para remover todos os filtros deste sistema. Este comando termina também os servidores *VPN e, depois, reinicia-os. Em seguida, configure os filtros e volte a activá-los.

Configurar a regra de filtragem pré-IPSec
Atenção: Só deve concluir esta tarefa se tiver especificado que não pretende que a VPN gere a regra de filtragem de políticas automaticamente.

Dois servidores de Internet Key Exchange (IKE) negoceiam e actualizam dinamicamente as chaves. O IKE utiliza a bem conhecida porta 500. Para que o IKE funcione correctamente, necessita de permitir datagramas UDP pela porta 500 para este tráfego IP. Para fazê-lo, crie um par de regras de filtragem: uma para o tráfego de recepção e outra para o de envio, de modo a que a ligação possa negociar chaves automaticamente para proteger a ligação:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Regras de Pacotes** e seleccione **Editor de Regras**. Isto abre o editor Regras de Pacotes, que lhe permite criar ou editar regras NAT e de filtragem para o iSeries.
3. No diálogo de Boas-vindas, seleccione **Criar um novo ficheiro de regras de pacote** e clique em **OK**.
4. No editor Regras de Pacotes seleccione **Inserir —> Filtro**.
5. Na página **Geral**, especifique um nome do conjunto para as regras de filtragem da VPN.É recomendada a criação de pelo menos três conjuntos diferentes: o primeiro para as regras de filtragem pré-IPSec, o segundo para as regras de filtragem de políticas e o último para regras de filtragem PERMIT e DENY. O conjunto que contém as regras de filtragem pré-IPSec deve ter o prefixo *preipsec*. Por exemplo, preipsecfiltros.
6. No campo **Acção**, seleccione **PERMIT** na lista pendente.
7. No campo **Direcção**, seleccione **OUTBOUND** na lista pendente.
8. No campo **Nome do endereço de origem**, seleccione **=** na primeira lista na primeira lista pendente e, em seguida, introduza o endereço de IP do servidor de chaves local no segundo campo. Especificou o endereço de IP do servidor de chaves local na política do IKE.
9. No campo **Nome do endereço de destino**, seleccione **=** na primeira lista na primeira lista pendente e, em seguida, introduza o endereço de IP do servidor de chaves remoto no segundo campo. Especificou também o endereço de IP do servidor de chaves remoto na política do IKE.
10. Na página **Serviços**, seleccione **Serviço**. Isto activa os campos **Protocolo**, **Porta de origem** e **Porta de destino**.
11. No campo **Protocolo**, seleccione **UDP** na lista pendente.

12. Para **Porta de origem**, seleccione **=** no primeiro campo e, depois, introduza `500` no segundo campo.
13. Repita o passo anterior para **Porta de destino**.
14. Faça clique sobre **OK**.
15. Repita estes passos para configurar o filtro INBOUND. Utilize o mesmo nome do conjunto e os mesmo endereços inversos, conforme a necessidade.

Nota: Uma opção menos segura, mas mais fácil, para permitir o tráfego do IKE através da ligação consiste na configuração de apenas um filtro pré-IPSec e na utilização de valores globais (*) nos campos **Direcção**, **Nome do endereço de origem** e **Nome do endereço de destino**.

O próximo passo é configurar uma regra de filtragem de políticas para definir qual o tráfego IP protegido pela ligação da VPN.

Configurar uma regra de filtragem de políticas

Atenção: Só deve concluir esta tarefa se tiver especificado que não pretende que a VPN gere a regra de filtragem de políticas automaticamente.

A regra de filtragem de políticas (uma regra onde acção=IPSEC) define quais os endereços, protocolos e portas que podem utilizar a VPN. Também identifica a política que será aplicada ao tráfego na ligação da VPN. Para configurar uma regra de filtragem de políticas, siga estes passos:

Nota: Se acabou de configurar a regra pré-IPSec (apenas para ligações dinâmicas) o editor Regras de Pacotes ainda deve estar aberto; vá para o passo quatro.

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Regras de Pacotes** e seleccione **Editor de Regras**. Isto abre o editor Regras de Pacotes, que lhe permite criar ou editar regras NAT e de filtragem para o iSeries.
3. No diálogo de Boas-vindas, seleccione **Criar um novo ficheiro de regras de pacote** e clique em **OK**.
4. No editor Regras de Pacotes seleccione **Inserir —> Filtro**.
5. Na página **Geral**, especifique um nome do conjunto para as regras de filtragem da VPN.É recomendada a criação de pelo menos três conjuntos diferentes: o primeiro para as regras de filtragem pré-IPSec, o segundo para as regras de filtragem de políticas e o último para regras de filtragem PERMIT e DENY. Por exemplo, `filtrospolíticas`
6. No campo **Acção**, seleccione **IPSEC** na lista pendente. O campo **Direcção** tem como valor assumido DE ENVIO e não pode alterá-lo. Apesar de este campo ter como valor assumido DE ENVIO, é, na verdade, bidireccional. DE ENVIO é apresentado para clarificar a semântica dos valores de input. Por exemplo, os valores de origem são valores locais e os valores de destino são valores remotos.
7. Para **Nome do endereço de origem**, seleccione **=** no primeiro campo e, em seguida, introduza o endereço de IP do ponto de terminação de dados local no segundo campo. Pode também especificar um intervalo de endereços de IP ou um endereço de IP mais uma máscara de sub-rede, depois de defini-los através da utilização da função **Definir Endereços**.
8. Para **Nome do endereço de destino**, seleccione **=** no primeiro campo e, em seguida, introduza o endereço de IP do ponto de terminação de dados remoto no segundo campo. Pode também especificar um intervalo de endereços de IP ou um endereço de IP mais uma máscara de sub-rede, depois de defini-los através da utilização da função **Definir Endereços**.
9. No campo **Registo em diário**, especifique que nível de registo em diário pretende.
10. No campo **Nome da ligação**, seleccione a definição de ligação à qual estas regras de filtragem se aplicam.
11. (opcional) Introduza uma descrição.

12. Na página **Serviços**, seleccione **Serviço**. Isto activa os campos **Protocolo**, **Porta de origem** e **Porta de destino**.
13. Nos campos **Protocolo**, **Porta de origem** e **Porta de destino**, seleccione o valor adequado para o tráfego. Ou pode ainda seleccionar o asterisco (*) na lista pendente. Isto permite a qualquer protocolo que esteja a utilizar qualquer porta que utilize a VPN.
14. Faça clique sobre **OK**.

O passo seguinte é definir a interface à qual estas regras de filtragem se aplicam.

Nota: Quando adiciona regras de filtragem para uma interface, o sistema adiciona automaticamente uma regra DENY assumida para essa interface. Isto significa que qualquer tráfego que não seja expressamente permitido é recusado. Não é possível visualizar ou alterar esta regra. Desta forma, pode acontecer que ligações que funcionavam anteriormente tenham falhas misteriosas, depois de activar as regras de pacotes da VPN. Se pretender permitir outro tráfego na interface para além do da VPN, deve adicionar regras PERMIT explícitas para fazê-lo.

Definir uma interface para as regras de filtragem da VPN

Depois de configurar as regras de pacotes da VPN e quaisquer outras regras de que necessite para activar a ligação da VPN, deve definir a interface à qual se aplicam.

Para definir uma interface à qual aplicar as regras de filtragem da VPN, siga estes passos:

Nota: Se acabou de configurar as regras de pacotes da VPN, a interface Regras de Pacotes ainda deve estar aberta; vá para o passo quatro.

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Regras de Pacotes** e seleccione **Editor de Regras**. Isto abre o editor Regras de Pacotes, que lhe permite criar ou editar regras NAT e de filtragem para o iSeries.
3. No diálogo de Boas-vindas, seleccione **Criar um novo ficheiro de regras de pacote** e clique em **OK**.
4. No editor Regras de Pacotes seleccione **Inserir —> Interface de Filtragem**.
5. Na página **Geral**, seleccione **Nome da linha** e, em seguida, seleccione, na lista pendente, a descrição da linha à qual se aplicam as regras de pacotes da VPN.
6. (opcional) Introduza uma descrição.
7. Na página **Conjuntos de Filtros**, faça clique sobre **Adicionar**, para adicionar cada nome do conjunto para o filtros configurados.
8. Faça clique sobre **OK**.
9. Guarde o ficheiro de regras. O ficheiro é guardado no sistema de ficheiros integrado do iSeries com uma extensão .i3p.
   Nota:Não guarde o ficheiro no seguinte directório:
   `/QIBM/UserData/OS400/TCPIP/RULEGEN`

   Este directório é apenas para utilização do sistema. Se alguma vez tiver de utilizar o comando RMVTCPTBL *ALL para desactivar as regras de pacotes, o comando irá eliminar todos os ficheiros contidos neste directório.

Depois de definir uma interface para as regras de filtragem, deve activá-las antes de poder iniciar a VPN.

Activar as regras de pacotes da VPN

Deve activar as regras de pacotes da VPN antes de poder iniciar as ligações da VPN. Não pode activar (ou desactivar) as regras de pacotes quando as ligações da VPN estão a ser executadas no sistema. Por isso, antes de activar as regras de filtragem da VPN, certifique-se de que não existem ligações activas associadas.

Se criou as ligações da VPN com o assistente de Nova Ligação, pode escolher ter as regras associadas automaticamente activadas. Tenha em atenção que, caso existam outras regras de pacotes activas em qualquer uma das interfaces que especificar, serão substituídas pelas regras de filtragem de políticas da VPN.

» Caso decida activar as regras criadas pela VPN utilizando o Editor Regras de Pacotes, siga os passos seguintes:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Regras de Pacotes** e seleccione **Activar**. Isto abre a caixa de diálogo Activar Regras de Pacotes.
3. Seleccione se pretende seleccionar apenas as regras geradas da VPN, apenas um ficheiro seleccionado ou ambos. Pode escolher a última opção, por exemplo, se tiver diversas regras PERMIT e DENY que pretende forçar na interface para além das regras geradas da VPN.
4. Seleccione a interface em que pretende activar as regras. Pode escolher a activação numa interface específica, num identificador ponto-a-ponto ou em todas interface e todos os identificadores ponto-a-ponto.
5. Faça clique sobre **OK** na caixa de diálogo, para confirmar que pretende verificar e activar as regras na interface ou nas interfaces especificadas. Após fazer clique em OK, o sistema verifica os erros de sintaxe e de semântica e comunica os resultados numa janela de mensagens na parte inferior do editor. Para mensagens de erro associadas a um ficheiro e número de linha específico, pode fazer clique com o botão direito do rato sobre o erro e seleccionar **Ir Para a Linha** para destacar o erro no ficheiro. «

Depois de activar as regras de filtragem, pode iniciar a ligação da VPN.

Iniciar uma ligação da VPN

Estas instruções partem do princípio que configurou correctamente a ligação da VPN. Siga estes passos para iniciar a ligação da VPN:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP**.
2. Se o servidor da VPN não tiver iniciado, faça clique com o botão direito do rato sobre **Virtual Private Networking** e seleccione **Iniciar**. Isto inicia o servidor da VPN.
3. Certifique-se de que as regras de pacotes estão activadas.
4. Expanda **Virtual Private Networking—> Ligações Seguras**.
5. Faça clique sobre **Todas as Ligações** para visualizar uma lista de ligações no painel da direita.
6. Faça clique com o botão direito do rato sobre a ligação que pretende iniciar e seleccione **Iniciar**. Para iniciar várias ligações, seleccione cada ligação que pretende iniciar, faça clique com o botão direito do rato sobre e seleccione **Iniciar**.

Gerir a VPN

Utilize a interface da VPN no iSeries Navigator para processar todas as tarefas de gestão, incluindo:

- **Iniciar uma ligação da VPN**
  Conclua esta tarefa para iniciar ligações iniciadas localmente.
- **Definir atributos assumidos para as ligações**
  Os valores assumidos gerem os painéis utilizados para criar novas políticas e ligações. Pode definir valores assumidos para níveis de segurança, gestão de sessões chave, validades das chaves e das ligações.
- **Repor ligações em estado de erro**
  Repor ligações com erro devolve-as ao estado de inactividade.
- **Visualizar informações dos erros**
  Conclua esta tarefa para ajudá-lo a determinar a razão do erro na ligação.

- **Visualizar os atributos de ligações activas**
  Conclua esta tarefa para verificar o estado e outros atributos das ligações activas.
- **Utilizar o rastreio do servidor da VPN**
  O rastreio do servidor da VPN permite configurar, iniciar, parar e visualizar os rastreios dos servidores do Gestor de Ligações e de Chaves da VPN. Isto é semelhante à utilização do comando TRCTCPAPP *VPN no ecrã verde excepto que pode visualizar o rastreio enquanto a ligação está activa.
- **Visualizar registos de trabalho do servidor da VPN**
  Siga estas instruções para visualizar os registos de trabalhos para o Gestor de Chaves e o de Ligações da VPN.
- **Parar ligações**
  Conclua esta tarefa para parar ligações activas.
- **Visualizar os atributos de Associações de Segurança (SA, Security Associations)**
  Conclua esta tarefa para visualizar os atributos das Associações de Segurança (SAs) associados a uma ligação activada.
- **Eliminar objectos da configuração da VPN**
  Antes de eliminar um objecto da configuração da VPN da base de dados de políticas da VPN, certifique-se de que compreende de que forma afecta outras ligações e grupos de ligações da VPN.

Definir atributos assumidos para as ligações

Os valores de segurança assumidos geram vários campos quando inicialmente cria novos objectos da VPN.

Para definir valores de segurança assumidos para as ligações da VPN, siga estes passos:

1. No iSeries Navigator, expanda o servidor **—>Rede —>Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Virtual Private Networking** e, depois, seleccione **Valores Assumidos**.
3. Faça clique sobre **Ajuda** caso tenha questões acerca do preenchimento de uma página ou de qualquer um dos respectivos campos.
4. Faça clique sobre **OK** após o preenchimento de cada uma das folhas de propriedades.

Repor ligações em estado de erro

Para actualizar uma ligação tenha o estado de erro, siga estes passos:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP—> Virtual Private Networking—> Ligações Seguras**
2. Faça clique sobre **Todas as Ligações** para visualizar uma lista de ligações no painel da direita.
3. Faça clique com o botão direito do rato sobre a ligação que pretende repor e seleccione **Repor**. Isto repõe a ligação no estado de inactividade. Para repor várias ligações com o estado de erro, seleccione cada ligação que pretenda repor, faça clique com o botão direito do rato e seleccione **Repor**.

Visualizar informações dos erros

Para visualizar informações sobre ligações com erro, siga estes passos:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP—> Virtual Private Networking—> Ligações Seguras**
2. Faça clique sobre **Todas as Ligações** para visualizar uma lista de ligações no painel da direita.
3. Faça clique com o botão direito do rato sobre a ligação com erro que pretende visualizar e seleccione **Informações dos Erros**.

Visualizar os atributos de ligações activas

Para visualizar os atributos de uma ligação activa ou por pedido, siga estes passos:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP—> Virtual Private Networking—> Ligações Seguras**
2. Faça clique sobre **Todas as Ligações** para visualizar uma lista de ligações no painel da direita.
3. Faça clique com o botão direito do rato sobre a ligação activa ou por pedido que pretende visualizar e seleccione **Propriedades.**
4. Vá para a página **Atributos Actuais** para visualizar os atributos da ligação.

Pode também visualizar os atributos de todas as ligações a partir da janela iSeries Navigator. Por valor assumido, os únicos atributos apresentados são Estado, Descrição e Tipo de Ligação. Pode alterar os dados que serão apresentados seguindo estes passos:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP—> Virtual Private Networking—> Ligações Seguras**
2. Faça clique sobre **Todas as Ligações** para visualizar uma lista de ligações no painel da direita.
3. No menu **Objectos**, seleccione **Colunas**. Esta acção abre uma caixa de diálogo que permite seleccionar os atributos que pretende visualizar na janela iSeries Navigator.

Tenha em atenção que quando altera as colunas para visualização, as alterações não são específicas a uma determinado utilizador ou PC, mas são feitas no sistema inteiro.

Utilizar o rastreio do servidor da VPN

Para visualizar o rastreio do servidor da VPN, siga estes passos:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Virtual Private Networking**, seleccione **Ferramentas de Diagnóstico** e, em seguida, **Rastreio do Servidor**.

Para especificar qual o tipo de rastreio que pretende que o Gestor de Chaves e o Gestor de Ligações da VPN gerem, siga estes passos:

1. Na janela **Rastreio Virtual Private Networking**, faça clique sobre  (Opções).
2. Na página **Gestor de Ligações**, especifique qual o tipo de rastreio que pretende que o servidor do Gestor de Ligações execute.
3. Na **página Gestor de Chaves**, especifique qual o tipo de rastreio que pretende que o servidor do Gestor de Chaves execute.
4. Faça clique sobre **Ajuda** caso tenha questões acerca do preenchimento de uma página ou de qualquer um dos respectivos campos.
5. Faça clique sobre **OK** para guardar as alterações.
6. Faça clique sobre  (Iniciar) para iniciar o rastreio. Faça clique sobre  (Actualizar) periodicamente para visualizar as informações de rastreio mais recentes.

Visualizar registos de trabalhos do servidor da VPN

Para visualizar os registos de trabalhos actuais do Gestor de Chaves ou do Gestor de Ligações da VPN, siga estes passos:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP.**
2. Faça clique com o botão direito do rato sobre **Virtual Private Networking** e seleccione **Ferramentas de Diagnóstico** e, em seguida, seleccione o registo de trabalhos que pretende visualizar.

Visualizar os atributos de Associações de Segurança (SA, Security Associations)

Para visualizar os atributos das associações de segurança (SAs) associados a uma ligação activada. Para fazê-lo, siga estes passos:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP—> Virtual Private Networking—> Ligações Seguras**
2. Faça clique sobre **Todas as Ligações** para visualizar uma lista de ligações no painel da direita.
3. Faça clique com o botão direito do rato sobre a ligação activa adequada e seleccione **Associações de Segurança.**A janela apresentada permite visualizar as propriedades de cada uma das SAs associadas a uma determinada ligação.

Parar uma ligação da VPN

Para parar uma ligação activa ou por pedido, siga estes passos:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP—> Virtual Private Networking—> Ligações Seguras**
2. Faça clique sobre **Todas as Ligações** para visualizar uma lista de ligações no painel da direita.
3. Faça clique com o botão direito do rato sobre a ligação que pretende parar e seleccione **Parar**. Para parar várias ligações, seleccione cada ligação que pretende parar, faça clique com o botão direito do rato sobre e seleccione **Parar**.

Eliminar objectos da configuração da VPN

Se estiver certo de que necessita de eliminar uma ligação da VPN da base de dados de políticas da VPN, siga estes passos:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP—> Virtual Private Networking—> Ligações Seguras**
2. Faça clique sobre **Todas as Ligações** para visualizar uma lista de ligações no painel da direita.
3. Faça clique com o botão direito do rato sobre a ligação que pretende eliminar e seleccione **Eliminar**.

Resolução de problemas da VPN

A VPN é uma tecnologia complexa e em rápida mudança que obriga a pelo menos um conhecimento básico de tecnologias IPSec standard. Deve também estar familiarizado com as regras de pacotes de IP, uma vez que a VPN necessita de várias regras de filtragem para funcionar correctamente. Devido a esta complexidade, pode, periodicamente, ter problemas com as ligações da VPN. A resolução de problemas da VPN nem sempre é uma tarefa fácil. É preciso compreender os ambientes do sistema e da rede, assim como os componentes utilizados para geri-los. Os tópicos que se seguem fornecem-lhe sugestões para a resolução dos vários problemas que pode encontrar durante a utilização da VPN:

- **Como começar com a resolução de problemas da VPN**
  É aqui que começa a encontrar e a corrigir os problemas da ligação da VPN.
- **Erros de configuração comuns da VPN e correcção dos mesmos**
  Este tópico identifica os erros mais comuns dos utilizadores e fornece resoluções possíveis.
- **Resolução de problemas da VPN com o diário QIPFILTER**
  Este tópico fornece informações acerca das regras de filtragem da VPN.
- **Resolução de problemas da VPN com o diário QVPN**
  Este tópico fornece informações acerca do tráfego IP e das ligações.
- **Resolução de problemas da VPN com os registos de trabalhos da VPN**
  Este tópico descreve os vários registos de trabalhos utilizados pela VPN.
- R**esolução de problemas da VPN com o rastreio de Comunicações do OS/400**
  Este tópico descreve como rastrear dados numa linha de comunicação.

Como começar com a resolução de problemas da VPN

Existem várias formas de começar a analisar os problemas da VPN:

1. Certifique-se sempre de que aplicou as mais recentes Correcções Temporárias de Ficheiros (PTFs).
2. Certifique-se de que respeita os requisitos de configuração mínimos da VPN.

3. Reveja quaisquer mensagens de erro que se encontrem na Informações dos Erros ou nos registos de trabalhos do servidor da VPN para os sistemas local e remoto. De facto, quando está a resolver problemas na ligação da VPN, é muitas vezes necessário olhar para ambos os extremos da ligação. Além disso, é necessário ter em conta que existem quatro endereços que deve verificar: Os pontos de terminação de ligações local e remoto, que são os endereços onde o IPSec é aplicado aos pacotes de IP e os pontos de terminação de dados local e remoto, que são os endereços de origem e de destino dos pacotes de IP.
4. Se as mensagens de erro que encontrar não fornecerem informações suficientes para resolver o problema, verifique o diário Filtro de IP.
5. O rastreio de comunicações do sistema iSeries proporciona-lhe outra hipótese de encontrar informações de carácter geral sobre se o sistema local recebe ou envia pedidos de ligação.
6. O comando Rastrear Aplicação de TCP (TRCTCPAPP) proporciona-lhe ainda outra forma de isolar os problemas. De modo geral, a Assistência IBM utiliza o TRCTCPAPP para obter output de rastreio, por forma a analisar os problemas da ligação.

Outras aspectos a verificar

Se ocorrer um erro depois de configurar uma ligação e não tiver a certeza em que local da rede ele ocorreu, procure reduzir a complexidade do ambiente. Por exemplo, em vez de investigar todas as partes da ligação da VPN em simultâneo, comece com a própria ligação IP. A lista seguinte faculta-lhe algumas directrizes básicas acerca da forma como começar a análise dos problemas da VPN, desde a ligação IP mais simples até à ligação da VPN mais complexa:

1. Comece com uma configuração IP entre os sistemas centrais local e remoto. Remova quaisquer filtros de IP na interface utilizada pelos sistemas local e remoto para comunicar. Consegue efectuar o PING do sistema central local para o remoto?

   Nota: Lembre-se de pedir informações no comando PING; introduza o endereço do sistema remoto e utilize PF10 para parâmetros adicionais, em seguida introduza o endereço da Internet local. Isto é particularmente importante quando tiver várias interfaces físicas ou lógicas. Isto assegura que os endereços correctos são colocados nos pacotes PING.

   Se a resposta for **sim**, prossiga para o passo 2. Se a resposta for **não**, verifique a configuração IP, o estado da interface e as entradas de encaminhamento. Se a configuração estiver correcta, efectue um rastreio de comunicação para verificar, por exemplo, se um pedido PING sai do sistema. Se enviar um pedido PING, mas não receber uma resposta, o problema está na rede ou no sistema remoto.

   Nota: Podem existir encaminhadores ou firewalls intermediárias que efectuam a filtragem de pacotes de pacotes e podem estar a filtrar os pacotes PING. O PING baseia-se normalmente no protocolo ICMP. Se o PING tiver êxito, isso quer dizer que existe conectividade. Se o PING não tiver êxito, só é possível saber que o PING falhou. Pode querer tentar outros protocolos IP entre os dois sistemas, tal como Telnet ou FTP para verificar a conectividade.
2. Verifique as regras de filtragem para a VPN e certifique-se de que estão activadas. A filtragem é iniciada de forma correcta? Se a resposta for **sim**, prossiga para o passo 3. Se a resposta for **não**, verifique se existem mensagens de erro na janela Regras de Pacotes no iSeries Navigator. Certifique-se de que as regras de filtragem não especificam Conversão de Endereços de Rede (NAT) para qualquer tráfego na VPN.
3. Inicie a ligação da VPN. A ligação é iniciada de forma correcta? Se a resposta for **sim**, prossiga para o passo 4. Se a resposta for **não**, verifique se existem erros no registo de trabalhos QTOVMAN, no registo de trabalhos QTOKVPNIKE.
   Quando utiliza a VPN, o seu Fornecedor de Serviços de Internet (ISP) e todas as portas de ligação de segurança da sua rede devem suportar os protocolos Authentication Header (AH) e Encapsulated Security Payload (ESP). A escolha de utilizar o AH ou o ESP depende dos objectivos que definir para a ligação da VPN.

4. Consegue activar uma sessão de utilizadores na ligação da VPN? Se a resposta for **sim**, é porque a ligação da VPN funciona como desejado. Se a resposta for **não**, verifique nas regras de pacotes e nos grupos de chaves dinâmicas da VPN se existem definições de filtragem que não permitam o tráfego de utilizadores desejado.

Erros de configuração comuns da VPN e correcção dos mesmos

Esta secção descreve alguns dos problemas mais comuns que ocorrem na VPN e fornece ligações a sugestões para os resolver.

Nota: Quando configura a VPN, está a criar vários objectos de configuração diferentes, sendo cada um necessário para que a VPN active uma ligação. Em relação à GUI da VPN, estes objectos são: as Políticas do IP Security e as Ligações Seguras. Assim, quando estas informações se referem a um objecto, referem-se a uma ou mais destas partes da VPN.

Mensagens de erro comuns que é possível encontrar

Mensagem	Sintoma
TCP5B28	Quando tenta activar regras de filtragem numa interface, recebe esta mensagem: violação da ordem TCP5B28 CONNECTION_DEFINITION
Item não encontrado	Quando faz clique com o botão direito do rato sobre um objecto da VPN e selecciona **Propriedades** ou **Eliminar**, recebe uma mensagem que diz **Item não encontrado**.
O PARÂMETRO PINBUF NÃO É VÁLIDO	Quando tenta iniciar uma ligação, recebe uma mensagem que diz **O PARÂMETRO PINBUF NÃO É VÁLIDO...**
Item não encontrado, Servidor de chaves remoto...	Quando selecciona **Propriedades** para uma ligação de chaves dinâmicas, recebe um erro que diz que o servidor não consegue encontrar o servidor de chaves especificado.
Não é possível actualizar o objecto	Quando selecciona **OK** na folha de propriedades para um grupo de chaves dinâmicas ou para uma ligação manual, recebe uma mensagem em como o sistema não consegue actualizar o objecto.
Não é possível codificar chave...	Recebe uma mensagem em como o sistema não consegue consegue codificar as chaves, porque o valor QRETSVRSEC deve estar definido para 1.
CPF9821	Quando tenta expandir ou abrir as Políticas de IP no iSeries Navigator, surge a mensagem CPF9821- Não autorizado a programar QTFRPRS na biblioteca QSYS.

Outros problemas que podem surgir

Erro	Sintoma
Todas as chaves estão em branco	Quando visualiza as propriedades de uma ligação manual, todas as chaves pré-partilhadas e as chaves de algoritmos para a ligação estão em branco.
Surge o início de sessão num sistema diferente	A primeira que utiliza a interface Regras de Pacotes no iSeries Navigator, é apresentado um ecrã de início de sessão num sistema diferente do actual.
Nenhum estado da ligação	Uma ligação não tem um valor na coluna **Estado** na janela iSeries Navigator.

Ligações paradas ainda activas	Depois de parar uma ligação, a janela iSeries Navigator indica que a ligação ainda está activa.
3DES não é uma escolha para codificação	Não é possível escolher uma codificação de algoritmo 3DES quando trabalha com uma conversão de políticas de IKE, uma conversão de políticas de dados ou uma ligação manual.
Apresentação de colunas inesperadas	Configurou as colunas que pretende visualizar na janela iSeries Navigator para as ligações da VPN; quando mais tarde a visualizou, foram apresentadas colunas diferentes.
As regras de filtragem activas não foram desactivadas	Quando tenta desactivar o conjunto de regras de filtragem actual, é apresentada a mensagem `As regras activas não foram desactivadas` na janela de resultados.
O grupo de chaves dinâmicas para uma ligação é alterado	Quando cria uma ligação de chave dinâmica, especifica um grupo de chaves dinâmicas e um identificador para o servidor de chaves remoto. Mais tarde, quando visualiza as propriedades do objecto da ligação associado, a página Geral da folha de propriedades apresenta o mesmo identificador do servidor de chaves remoto, mas um grupo de chaves dinâmicas diferentes.

Mensagem de erro da VPN: TCP5B28

Sintoma:

Quando tenta activar as regras de filtragem numa determinada interface, recebe esta mensagem de erro:

```
TCP5B28: violação de ordem CONNECTION_DEFINITION
```

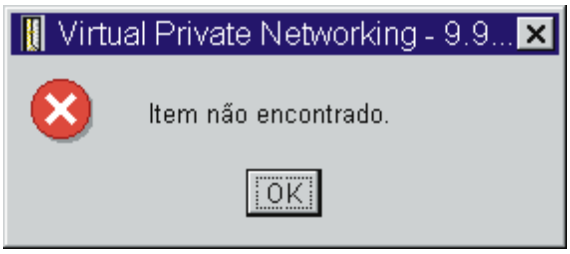
Possível resolução:

As regras de filtragem que estava a tentar activar continham definições da ligação que estavam ordenadas de forma diferente do que acontecia num conjunto de regras activado previamente. A forma mais fácil de resolver este erro é activar o ficheiro de regras em **todas as interfaces** em vez de numa determinada interface.

Mensagem de erro da VPN: Item não encontrado

Sintoma:

Quando faz clique com o botão direito do rato sobre um objecto da janela Virtual Private Networking e selecciona **Propriedades** ou **Eliminar**, é apresentada a mensagem seguinte:



Possível resolução:

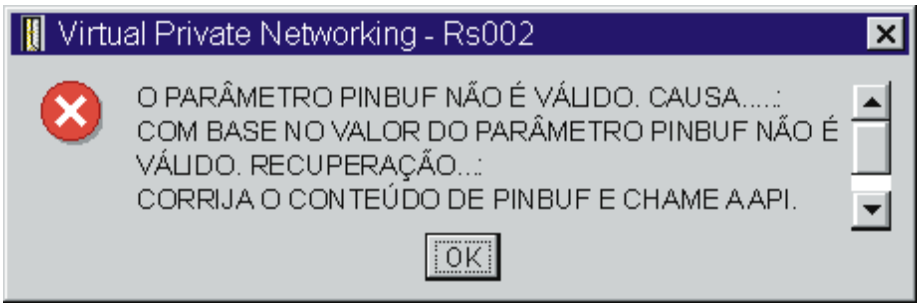
- Pode ter eliminado o objecto ou mudado o nome do mesmo e ainda não actualizou a janela. Desta forma, o objecto ainda é apresentado na janela Virtual Private Networking. Para verificar se é este o caso, no menu **Ver**, seleccione **Actualizar**. Se o objecto ainda surgir na janela Virtual Private Networking, prossiga para o próximo item da lista.

- Quando configurou as propriedades do objecto, pode ter ocorrido um erro de comunicação entre o servidor da VPN e o iSeries. Muitos dos objectos que são apresentados na janela Virtual Private Networking estão relacionados com mais do que um objecto da base de dados de política da VPN. Isto significa que os erros de comunicação podem fazer com que alguns dos objectos da base de dados continuem a estar relacionados com um objecto da VPN. Sempre que criar ou actualizar um objecto, deve ocorrer um erro quando a perda de sincronização realmente acontecer. A única forma de corrigir o problema é seleccionar **OK** na janela do erro. Isto inicia a folha de propriedades do objecto que está a dar erro. Apenas o campo do nome na folha de propriedades possui um valor. Tudo o resto está em branco (ou contém valores assumidos). Introduza os atributos correctos do objecto e seleccione **OK** para guardar as alterações.
- Ocorreu um erro semelhante quando tentou eliminar o objecto. Para corrigir este problema, preencha a folha de propriedades em branco que abre quando faz clique sobre **OK** na mensagem de erro. Isto actualiza todas as ligações à base de dados de política da VPN que foram perdidas. Pode então eliminar o objecto.

Mensagem de erro da VPN: O PARÂMETRO PINBUF NÃO É VÁLIDO

Sintoma:

Quando tenta iniciar uma ligação, é apresentada uma mensagem semelhante à seguinte:



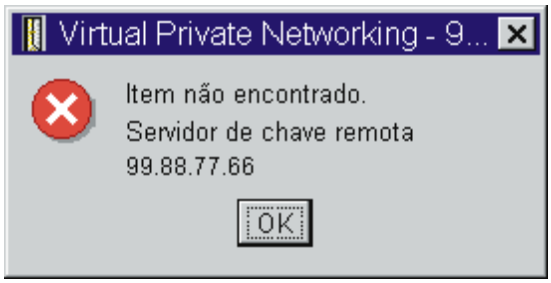
Possível resolução:

Isto acontece quando o sistema está definido para utilizar determinados locales para os quais as letras minúsculas não fazem uma correspondência correcta. Para corrigir este erro, deve certificar-se de que todos os objectos utilizam apenas maiúsculas ou alterar o locale do sistema.

Mensagem de erro da VPN: Item não encontrado, Servidor de chave remoto...

Sintoma:

Quando selecciona **Propriedades** para uma ligação de chaves dinâmicas, surge uma mensagem semelhante à seguinte:



Possível resolução:

Isto acontece quando cria uma ligação a um determinado identificador de servidor de chave remoto e, depois, o servidor de chave remoto é removido do respectivo grupo de chaves dinâmicas. Para corrigir este erro, faça clique sobre **OK** na mensagem de erro. Isto abre a folha de propriedades da ligação de chaves dinâmicas com erro. A partir daqui, pode voltar adicionar o servidor de chaves remoto ao grupo de

chaves dinâmicas ou seleccionar outro identificador de servidor de chaves remoto. Faça clique sobre **OK** na folha de propriedades, para guardar as alterações.

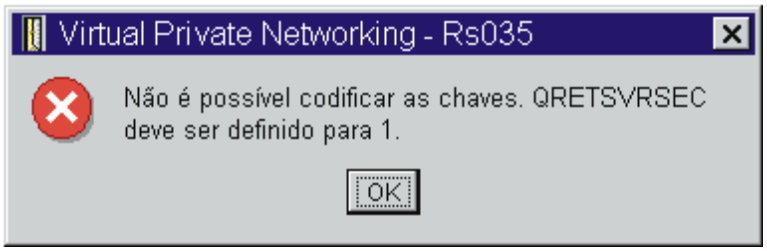
Mensagem de erro da VPN: Não é possível actualizar o objecto

Sintoma:
Quando selecciona **OK** na folha de propriedades para um grupo de chaves dinâmicas ou para uma ligação manual, surge a seguinte mensagem:

Possível resolução:
Este erro acontece quando uma ligação activa está a utilizar o objecto que o utilizador procura alterar. Não é possível fazer alterações a um objecto dentro de uma ligação activa. Para efectuar alterações num objecto, identifique a ligação activa adequada e, em seguida, faça clique com o botão direito do rato sobre **Parar** no menu de contexto que surge.

Mensagem de erro da VPN: Não é possível codificar chave...

Sintoma:
É apresentada a seguinte mensagem de erro



Possível resolução:
O QRETSVRSEC é um valor do sistema que indica se o sistema pode armazenar chaves codificadas. Se este valor for definido para 0, as chaves pré-partilhadas e as chaves para os algoritmos de uma ligação manual não podem ser armazenadas na base de dados de política da VPN. Para corrigir este problema, utilize uma sessão de emulação 5250 no sistema. Escreva `wrksysval` na linha de comando e prima **Enter**. Procure QRETSVRSEC na lista e escreva `2` (alterar) ao lado. No painel seguinte, escreva `1` e prima **Enter**.

Mensagem de erro da VPN: CPF9821

Sintoma:
Quando tenta expandir as Políticas de IP no iSeries Navigator, surge a mensagem `CPF9821- Não autorizado a programar QTFRPRS na biblioteca QSYS`.

Possível resolução:
Poderá não dispor da autoridade necessária para obter o estado actual das Regras de Pacotes ou do gestor de ligações da VPN. Certifique-se de que dispõe de autoridade *IOSYSCFG. Agora, deve ter acesso às funções das Regras de Pacotes no iSeries Navigator.

Erro da VPN: Todas as chaves estão em branco

Sintoma:
Todas as chaves pré-partilhadas e as chaves de algoritmo para ligações manuais estão em branco.

Possível resolução:
Isto acontece sempre que o valor de sistema QRETSVRSEC é reposto para 0. Definir o valor de sistema para 0 apaga todas as chaves da base de dados da política da VPN. Para corrigir este problema, deve definir o valor de sistema para 1 e, depois, voltar a escrever todas as chaves. Consulte a Mensagem de erro: Não é possível codificar chaves, para obter mais informações sobre a forma como proceder.

Erro da VPN: Surge o início de sessão num sistema diferente ao utilizar Regras de Pacotes

Sintoma:
A primeira vez que utiliza as Regras de Pacotes é apresentado um ecrã de início de sessão de um sistema diferente do actual.

Possível resolução:
As Regras de Pacotes utilizam o código universal para armazenar as regras de segurança de pacotes no sistema de ficheiros integrado. O início de sessão adicional permite ao Client Access Express obter a tabela de conversão adequada para o código universal. Isto deve apenas acontecer uma vez.

Erro da VPN: Estado da ligação em branco na janela iSeries Navigator

Sintoma:
Uma ligação não tem um valor na coluna **Estado** na janela iSeries Navigator.

Possível resolução:
O valor de estado em branco indica que a ligação está a meio de iniciar. Por outras palavras, ainda não está a ser executada, mas também ainda não teve qualquer erro. Quando actualizar a janela, a ligação deve apresentar um estado `Com Erro`, `Activada`, `Por Pedido` ou `Inactiva`.

Erro da VPN: Ligação com estado de activada após ter sido parada

Sintoma:
Depois de parar uma ligação, a janela iSeries Navigator indica que a ligação ainda está activa.

Possível resolução:
Isto acontece normalmente por ainda não ter actualizado a janela iSeries Navigator. Por isso, a janela contém informações desactualizadas. Para corrigir isto, no menu **Ver**, seleccione **Actualizar**.

Erro da VPN: 3DES não é uma escolha para codificação

Sintoma:
Não é possível escolher uma codificação de algoritmo 3DES quando trabalhar com uma conversão de políticas de IKE, uma conversão de políticas de dados ou uma ligação manual.

Possível resolução:
O mais provável é que tenha apenas o Cryptographic Access Provider AC2 (5722-AC2) instalado no sistema e não o Cryptographic Access Provider AC3 (5722-AC3). O AC2 apenas permite o algoritmo de codificação Data Encryption Standard (DES), devido a restrições impostas ao comprimento das chaves.

Erro da VPN: Colunas inesperadas são apresentadas na janela iSeries Navigator

Sintoma:
Configurou as colunas que pretende visualizar na janela iSeries Navigator para as ligações da VPN; quando mais tarde a visualizou, foram apresentadas colunas diferentes.

Possível resolução:
Quando altera as colunas para visualização, as alterações não são específicas a uma determinado utilizador ou PC, mas são feitas no sistema inteiro. Por isso, quando outra pessoa altera as colunas na janela, as alterações afectam todos os que visualizam ligações nesse sistema.

Erro da VPN: As regras de filtragem activas não foram desactivadas

Sintoma:

Quando tenta desactivar o conjunto de regras de filtragem actual, é apresentada a mensagem `As regras activas não foram desactivadas` na janela de resultados.

Possível resolução:

De modo geral, esta mensagem de erro significa que existe, pelo menos uma ligação da VPN activa. Tem de parar cada uma das ligações com o estado de `activada`. Para fazê-lo, faça clique com o botão direito do rato sobre cada ligação activa e seleccione **Parar**. Agora deverá ser capaz de desactivar as regras de filtragem.

Erro da VPN: O grupo de ligações de chave para uma ligação foi alterado

Sintoma:

Quando cria uma ligação de chave dinâmica, especifica um grupo de chaves dinâmicas e um identificador para o servidor de chaves remoto. Mais tarde, quando selecciona **Propriedades** no objecto de ligação associado, a página **Geral** da folha de propriedades apresenta o mesmo identificador de servidor de chaves remoto, mas um grupo de chaves dinâmicas diferente.

Possível resolução:

O identificador é a única informação armazenada na base de dados de política da VPN que faz referência ao servidor de chaves remoto da ligação de chave dinâmica. Quando a VPN procura uma política para um servidor de chaves remoto, procura o primeiro grupo de chaves dinâmicas que possuir esse identificador de servidor de chaves remoto. Por isso, quando visualiza as propriedades de uma destas ligações, esta utiliza o mesmo grupo de chaves dinâmicas que a VPN encontrou. Se não pretender associar o grupo de chaves dinâmicas àquele servidor de chaves remoto, pode proceder de uma das seguintes formas:

1. Remova o servidor de chaves remoto do grupo de chaves dinâmicas.
2. Expanda **Por Grupos** no painel esquerdo da interface da VPN e seleccione e arraste o grupo de chaves dinâmicas pretendido para a parte superior da tabela no painel direito. Isto garante que a VPN verifica primeiro este grupo de chaves dinâmicas para o servidor de chaves remoto.

Resolução de problemas da VPN com o diário QIPFILTER

O diário QIPFILTER está localizado na biblioteca QUSRSYS e contém informações sobre conjuntos de regras de filtragem, bem como informações sobre se um datagrama IP foi permitido ou recusado. O registo em diário é executado com base na opção de registo em diário especificada nas regras de filtragem.

Como activar o diário Filtro de Pacotes IP

Utilize o editor Regras de Pacotes no iSeries Navigator para activar o diário QIPFILTER. Tem de activar a função de registo para cada regra de filtragem individual. Não existe uma função que permita o registo em todos os datagramas IP que entrem ou saiam do sistema.

Nota: Para activar o diário QIPFILTER os filtros devem estar desactivados.

Os passos seguintes descrevem a forma como activar o registo em diário numa determinada regra de filtragem:

1. No iSeries Navigator, expanda o servidor **—> Rede—> Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Regras de Pacotes IP** e seleccione **Configuração**. Isto apresenta a interface Regras de Pacotes.
3. Abra um ficheiro de regras de filtragem existentes.
4. Faça duplo clique sobre a regra de filtragem que pretende registar em diário.
5. Na página **Geral**, seleccione **FULL** no campo **Registo em diário** conforme a caixa de diálogo mostrada em cima. Esta acção activa o registo desta regra de filtragem específica.
6. Faça clique sobre **OK**.

7. Guarde e active o ficheiro de regras de filtragem alterado.

Se um datagrama IP corresponder às definições da regra de filtragem, será criada uma entrada no diário QIPFILTER.

Com utilizar o diário QIPFILTER
O OS/400 cria automaticamente o diário, na primeira vez que a filtragem de pacotes de IP for activada. Para visualizar os detalhes específicos de uma entrada do diário, pode visualizar as entradas do diário no ecrã ou utilizar um ficheiro de output.

Ao copiar as entradas do diário para um ficheiro de output, pode facilmente visualizar as entradas através de utilitários de consulta, como o Query/400 ou SQL. Pode também gravar os seus próprios programas HLL para processar as entradas nos ficheiros de output.

O que se segue é um exemplo de um comando Ver Diário (DSPJRN):

```
DSPJRN JRN(QIPFILTER) JRNCDE((M)) ENTTYP((TF)) OUTPUT(*OUTFILE)
    OUTFILFMT(*TYPE4) OUTFILE(minhabib/meufich) ENTDTALEN(*VARLEN *CALC)
```

Utilize os passos seguintes para copiar as entradas do diário QIPFILTER para o ficheiro de output:

1. Crie uma cópia do ficheiro de output QSYS/QATOFIPF criado pelo sistema para uma biblioteca do utilizador, através do comando Criar Objecto Duplicado (CRTDUPOBJ). O que se segue é um exemplo do comando CRTDUPOBJ:

   ```
   CRTDUPOBJ OBJ(QATOFIPF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(minhabib)
        NEWOBJ(meufich)
   ```

2. Utilize o comando Ver Diário (DSPJRN) para copiar as entradas do diário QUSRSYS/QIPFILTER para o ficheiro de output que criou no passo anterior.

Se copiou o DSPJRN para um ficheiro de output que não existe, o sistema cria um ficheiro, mas este não contém as descrições dos campos apropriadas.

Nota: O diário QIPFILTER contém apenas entradas de permissão e recusa das regras de filtragem em que a opção de registo em diário está definida como FULL. Por exemplo, se apenas configurou regras de filtragem PERMIT, os datagramas IP que não forem explicitamente autorizados são recusados. Para os datagramas recusados, não é adicionada qualquer entrada no diário. Para a análise de problemas, poderá adicionar uma regra de filtragem que recuse explicitamente qualquer outro tráfego e execute um registo em diário FULL. Então, obterá entradas DENY no registo em diário para todos os datagramas IP recusados. Por motivos relacionados com o rendimento, não é recomendável que permita o registo em diário a todas as regras de filtragem. Assim que os conjuntos de filtragem sejam testados, reduza o registo em diário para um subconjunto de entradas útil.

Consulte Campos do diário QIPFILTER para ver uma tabela que descreve o ficheiro de output do QIPFILTER.

Campos do diário QIPFILTER
A tabela seguinte descreve os campos do ficheiro de output do QIPFILTER:

Nome do Campo	Comprimento do Campo	Numérico	Descrição	Comentários
TFENTL	5	S	Comprimento da Entrada	
TFSEQN	10	S	Número de sequência	
TFCODE	1	N	Código de diário	Sempre M
TFENTT	2	N	Tipo de entrada	Sempre TF

TFTIME	26	N	Marca de hora de SAA	
TFJOB	10	N	Nome do trabalho	
TFUSER	10	N	Perfil do utilizador	
TFNBR	6	S	Número do trabalho	
TFPGM	10	N	Nome do programa	
TFRES1	51	N	Reservado	
TFUSPF	10	N	Utilizador	
TFSYMN	8	N	Nome do sistema	
TFRES2	20	N	Reservado	
TFRESA	50	N	Reservado	
TFLINE	10	N	Descrição de linha	*ALL se TFREVT for U* , Espaço em branco se TFREVT for L*, Nome de linha se TFREVT for L
TFREVT	2	N	Acontecimento de regra	L* ou L quando as regras estão carregadas. U* quando as regras não estão carregadas, A quando é acção de filtragem
TFPDIR	1	N	Direcção de Pacotes IP	O é de envio, I é de recepção
TFRNUM	5	N	Número de regra	Aplica-se ao número de regra no ficheiro de regras activas
TFACT	6	N	Acção de filtragem efectuada	PERMIT, DENY ou IPSEC
TFPROT	4	N	Protocolo de transporte	1 é ICMP 6 é TCP 17 é UDP 50 é ESP 51 é AH
TFSRCA	15	N	Endereço de IP de origem	
TFSRCP	5	N	Porta origem	Não utilizado se TFPROT= 1 (ICMP)
TFDSTA	15	N	Endereço de IP de destino	
TFDSTP	5	N	Porta de destino	Não utilizado se TFPROT= 1 (ICMP)
TFTEXT	76	N	Texto adicional	Contém descrição se TFREVT= L* ou U*

Resolução de problemas da VPN com o diário QVPN

A VPN utiliza um diário separado para registar informações sobre o tráfego IP e sobre as ligações, denominado diário QVPN. O QVPN é armazenado na biblioteca QUSRSYS. O código do diário é M e o tipo de diário é TS. Raramente irá utilizar entradas de diário todos os dias. No entanto, poderá considerá-las úteis para a resolução de problemas e para verificar se o sistema, as chaves e as ligações estão a funcionar da forma que especificou. Por exemplo, as entradas de diário ajudam-no a compreender o que acontece aos pacotes de dados. Mantêm-no igualmente informado relativamente ao estado de VPN actual.

Como activar o diário da VPN

Utilize a interface Virtual private networking no iSeries Navigator para activar o diário da VPN. Não existe uma função que permita o registo em todas as ligações da VPN. Assim, tem de activar a função de registo em diário para cada grupo de chaves dinâmicas ou ligação manual individual.

Os passos seguintes descrevem a forma como activar a função de registo em diário para um determinado grupo de chaves dinâmicas ou uma determinada ligação manual:

1. No iSeries Navigator, expanda o servidor **—> rede—> Políticas de IP—> Virtual Private Networking—> Ligações Seguras.**
2. Para grupos de chaves dinâmicas, expanda **Por Grupo** e, em seguida, faça clique com o botão direito do rato sobre o grupo de chaves dinâmicas para o qual pretende activar o registo em diário e seleccione **Propriedades.**
3. Para ligações manuais, expanda **Todas as Ligações** e, em seguida, faça clique com o botão direito do rato sobre a ligação manual para a qual pretende activar o registo em diário.
4. Na página **Geral**, seleccione o nível de registo em diário necessário. Pode escolher entre quatro opções. São elas:
   Nenhum
   Não há qualquer registo em diário neste grupo de ligações.
   Todos
   É feito o registo em diário de todas as actividades relacionadas com as ligações, tais como iniciar ou parar uma ligação, a actualização de chaves, bem como informações sobre tráfego IP.
   Actividade das Ligações
   É feito o registo em diário de actividades relacionadas com as ligações, como iniciar ou parar uma ligação.
   Tráfego IP
   É feito o registo em diário de todo o tráfego da VPN associado a esta ligação. É feita uma entrada de registo sempre que é invocada uma regra de filtragem. O sistema grava as informações de tráfego IP no diário QIPFILTER, que se encontra na biblioteca QUSRSYS.
5. Faça clique sobre **OK**.
6. Inicie a ligação para activar o registo em diário.

Nota: Antes de parar o registo em diário, certifique-se de que a ligação está inactiva. Para alterar o estado de registo em diário de um grupo de ligações, certifique-se de que não estão associadas ligações activas a esse grupo específico.

Como utilizar o diário da VPN

Para visualizar os detalhes específicos de uma entrada do diário da VPN, pode visualizar as entradas no ecrã ou utilizar o ficheiro de output.

Ao copiar as entradas do diário para o ficheiro de output, pode facilmente visualizar as entradas através de utilitários de consulta, como o Query/400 ou SQL. Pode também gravar os seus próprios programas HLL para processar as entradas nos ficheiros de output. O que se segue é um exemplo de um comando Ver Diário (DSPJRN):

```
DSPJRN JRN(QVPN) JRNCDE((M)) ENTTYP((TS)) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4)
    OUTFILE(minhabib/meufich) ENTDTALEN(*VARLEN *CALC)
```

Utilize os passos seguintes para copiar as entradas do diário da VPN para o ficheiro de output:

1. Crie uma cópia do ficheiro de output QSYS/QATOVSOF criado pelo sistema na biblioteca do utilizador. Pode fazê-lo através do comando Criar Objecto Duplicado (CRTDUPOBJ). O que se segue é um exemplo do comando CRTDUPOBJ:

   ```
   CRTDUPOBJ OBJ(QATOVSOF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(minhabib)
        NEWOBJ(meufich)
   ```

2. Utilize o comando Ver Diário (DSPJRN) para copiar as entradas do diário QUSRSYS/QVPN para o ficheiro de output que criou no passo anterior. Se tentar copiar o comando DSPJRN para um ficheiro de output que não existe, o sistema cria um ficheiro para si, mas este não contém as descrições do campo apropriadas.

Consulte Campos do diário QVPN para ver uma tabela que descreve os campos do ficheiro de output QVPN.

Campos do diário QVPN

A tabela seguinte descreve os campos do ficheiro de output do diário QVPN:

Nome do Campo	Comprimento do Campo	Numérico	Descrição	Comentários
TSENTL	5	S	Comprimento da Entrada	
TSSEQN	10	S	Número de sequência	
TSCODE	1	N	Código de diário	Sempre M
TSENTT	2	N	Tipo de entrada	Sempre TS
TSTIME	26	N	Marca de tempo da entrada SAA	
TSJOB	10	N	Nome do trabalho	
TSUSER	10	N	Utilizador do trabalho	
TSNBR	6	S	Número do trabalho	
TSPGM	10	N	Nome do programa	
TSRES1	51	N	Não utilizado	
TSUSPF	10	N	Nome do perfil do utilizador	
TSSYNM	8	N	Nome do sistema	
TSRES2	20	N	Não utilizado	
TSRESA	50	N	Não utilizado	
TSESDL	4	S	Comprimento de dados específicos	
TSCMPN	10	N	Componente VPN	
TSCONM	40	N	Nome da ligação	
TSCOTY	10	N	Tipo de Ligação	
TSCOS	10	N	Estado da Ligação	
TSCOSD	8	N	Data de início	
TSCOST	6	N	Hora de início	
TSCOED	8	N	Data final	
TSCOET	6	N	Hora final	
TSTRPR	10	N	Protocolo de transporte	
TSLCAD	43	N	Endereço do cliente local	
TSLCPR	11	N	Portas Locais	
TSRCAD	43	N	Endereço do cliente remoto	

TSCPR	11	N	Portas remotas	
TSLEP	43	N	Ponto de terminação local	
TSREP	43	N	Ponto de terminação remoto	
TSCORF	6	N	Número de vezes actualizado	
TSRFDA	8	N	Data da próxima actualização	
TSRFTI	6	N	Hora da próxima actualização	
TSRFLS	8	N	Actualizar tempo de vida	
TSSAPH	1	N	Fase SA	
TSAUTH	10	N	Tipo de Autenticação	
TSENCR	10	N	Tipo de codificação	
TSDHGR	2	N	Grupo Diffie-Hellman	
TSERRC	8	N	Código de erro	

Resolução de problemas da VPN com os registos de trabalhos da VPN

Quando se deparar com problemas nas ligações da VPN, é sempre aconselhável analisar os registos de trabalhos. De facto, existem vários registos de trabalhos que contêm mensagens de erro e outras informações relacionadas com o ambiente de uma VPN.

É importante analisar os registos de trabalhos de ambos os extremos da ligação, se estes forem servidores iSeries. Quando uma ligação dinâmica não iniciar, será útil perceber o que está a acontecer no sistema remoto.

Os registos de trabalhos da VPN, QTOVMAN e QTOKVPNIKE, são executados no subsistema QSYSWRK. Pode visualizar os respectivos registos de trabalhos a partir do OS/400 Operations Navigator.

Esta secção apresenta os trabalhos mais importantes para um ambiente VPN. A lista seguinte apresenta os nomes dos trabalhos com uma breve explicação da sua utilização:

QTCPIP
Este é o trabalho de base que inicia todas as interfaces TCP/IP. Se tem problemas graves com o TCP/IP em geral, analise o registo de trabalho QTCPIP.

QTOKVPNIKE
O trabalho QTOKVPNIKE é o trabalho de gestão chave da VPN. O gestor de chave da VPN aguarda na porta 500 UDP para executar o processamento do protocolo Internet Key Exchange (IKE).

QTOVMAN
Este trabalho é o gestor de ligações para ligações da VPN. O registo de trabalhos associado contém mensagens de qualquer tentativa de ligação que falhe.

QTPPANSxxx
Este trabalho é utilizado para ligações por marcação PPP. Responde a tentativas de marcação em que *ANS está definido num perfil PPP.

QTPPPCTL
Este é um trabalho PPP para ligações por marcação.

QTPPPL2TP
Este é o trabalho de gestão do Protocolo de Túnel de Camada Dois (L2TP). Se tiver problemas em configurar um direccionamento de L2TP, verifique a existência de mensagens neste registo de trabalhos.

Mensagens de erro comuns do Gestor de Ligações da VPN

Esta secção descreve alguns dos erros mais comuns do Gestor de Ligações da VPN que podem ocorrer.

No geral, o Gestor de Ligações da VPN regista duas mensagens no registo de trabalhos QTOVMAN quando ocorre um erro numa ligação da VPN. A primeira mensagem fornece detalhes relacionados com o erro. Pode visualizar as informações referentes a estes erros no iSeries Navigator fazendo clique com o botão direito do rato sobre o erro e seleccionando **Informações do Erro**.

A segunda mensagem descreve a acção que estava a tentar executar na ligação quando o erro ocorreu. Por exemplo, a iniciar ou a pará-la. A mensagens TCP8601, TCP8602 e TCP860A, descritas abaixo, são exemplos típicos deste segundo tipo de mensagem.

Mensagens de erro do Gestor de Ligações da VPN

Mensagem	Causa	Recuperação
TCP8601 Não foi possível iniciar a ligação da VPN [*nome da ligação*]	Não foi possível iniciar esta ligação da VPN devido a um destes códigos de razão: *0* - Uma mensagem anterior no registo de trabalhos com o mesmo nome de ligação da VPN tem informações mais detalhadas. *1* - Configuração da política da VPN. *2* - Falha na rede de comunicações. *3* - O Gestor de Chaves da VPN não conseguiu negociar uma nova associação de segurança. *4* - O ponto de terminação remoto para esta ligação não está configurado correctamente. *5* - O Gestor de Chaves da VPN não conseguiu responder ao Gestor de Ligações da VPN. *6* - Falha no carregamento da ligação da VPN no Componente IP Security. *7* - Falha no Componente PPP.	1. Verifique se existem mensagens adicionais nos registos de trabalhos. 2. Corrija os erros e repita o pedido. 3. Utilize o iSeries Navigator para visualizar o estado da ligação. As ligações que não conseguiram iniciar serão as que apresentam o estado com erro.
TCP8602 Ocorrência de erro ao parar a ligação da VPN [*nome da ligação*]	Foi feito um pedido para que a ligação da VPN especificada fosse parada; não foi parada ou parou com erro, com o Código de Razão: *0* - Uma mensagem anterior no registo de trabalhos com o mesmo nome de ligação da VPN tem informações mais detalhadas. *1* - A ligação da VPN não existe. *2* - Falha interna nas comunicações com o Gestor de Chaves da VPN. *3* - Falha interna nas comunicações com o componente IPSec. *4* - Falha na comunicação com o ponto de terminação remoto da ligação da VPN.	1. Verifique se existem mensagens adicionais nos registos de trabalhos. 2. Corrija os erros e repita o pedido. 3. Utilize o iSeries Navigator para visualizar o estado da ligação. As ligações que não conseguiram iniciar serão as que apresentam o estado com erro.

TCP8604 Falha no início da ligação da VPN [*nome da ligação*]	Falha no início desta ligação da VPN com um destes códigos de razão: *1* - Não foi possível converter o nome do sistema central remoto para um endereço de IP. *2* - Não foi possível converter o nome do sistema central local para um endereço de IP. *3* - A regra de filtragem de políticas da VPN associada a esta ligação da VPN não está carregada. *4* - Um valor de chave especificada pelo utilizador não é válido para o respectivo algoritmo associado. *5* - O valor de iniciação para a ligação da VPN não permite a acção especificada. *6* - Uma função do sistema para a ligação da VPN é inconsistente com informações do grupo de ligações. *7* - Reservado. *8* - Os pontos de terminação de dados (endereços e serviços locais e remotos) desta ligação da VPN são inconsistentes com informações do grupo de ligações. *9* - Tipo de identificador não válido.	1. Verifique se existem mensagens adicionais nos registos de trabalhos. 2. Corrija os erros e repita o pedido. 3. Utilize o iSeries Navigator para verificar ou corrigir a configuração da política da VPN. Certifique-se de que o grupo de chaves dinâmicas associado a esta ligação tem valores aceitáveis configurados.
TCP8605 O Gestor de Ligações da VPN não conseguiu comunicar com o Gestor de Chaves da VPN	O Gestor de Ligações da Ligação da VPN requer os serviços do Gestor de Chaves da VPN para estabelecer associações de segurança para ligações dinâmicas da VPN. O Gestor de Ligações da VPN não conseguiu comunicar com o Gestor de Chaves da VPN.	1. Verifique se existem mensagens adicionais nos registos de trabalhos. 2. Verifique se a interface *LOOPBACK está activa através da utilização do comando NETSTAT OPTION(*IFC). 3. Termine o servidor da VPN através da utilização do comando ENDTCPSVR SERVER(*VPN). Em seguida, reinicie o servidor da VPN através da utilização do comando STRTCPSRV SERVER(*VPN). **Nota:** Isto faz com que todas as ligações da VPN sejam terminadas.

TCP8606 O Gestor de Chaves da VPN não conseguiu estabelecer a associação de segurança pedida para a ligação [*nome da ligação*]	O Gestor de Chaves da VPN não conseguiu estabelecer a associação de segurança pedida devido a um destes códigos de razão: *24* - Falha na autenticação da ligação de chaves do Gestor de Chaves da VPN. *8300* - Ocorrência de falha durante as negociações de ligações de chaves do Gestor de Chaves da VPN. *8306* - Não foi encontrada qualquer chave pré-partilhada local. *8307* - Não foi encontrada qualquer política de fase 1 do IKE remoto. *8308* - Não foi encontrada qualquer chave pré-partilhada remota. *8327* - O tempo de espera das negociações da ligação de chaves do Gestor de Chaves da VPN foi excedido. *8400* - Ocorrência de falha durante as negociações de ligações da VPN do Gestor de Chaves da VPN. *8407* - Não foi encontrada qualquer política de fase 2 do IKE remoto. *8408* - O tempo de espera das negociações da ligação da VPN do Gestor de Chaves da VPN foi excedido. *8500 ou 8509* - Ocorrência de erro na rede do Gestor de Chaves da VPN.	1. Verifique se existem mensagens adicionais nos registos de trabalhos. 2. Corrija os erros e repita o pedido. 3. Utilize o iSeries Navigator para verificar ou corrigir a configuração da política da VPN. Certifique-se de que o grupo de chaves dinâmicas associado a esta ligação tem valores aceitáveis configurados.
TCP8608 A ligação da VPN [*nome da ligação*] não conseguiu obter um endereço de NAT	Este grupo de chaves dinâmicas ou esta ligação de dados especificou que a conversão de endereços de rede (NAT) fosse efectuada num ou mais endereços e essa operação falhou provavelmente devido a um destes códigos de razão: *1* - O endereço ao qual deve ser aplicada a NAT não é um endereço de IP único. *2* - Todos os endereços disponíveis foram utilizados.	1. Verifique se existem mensagens adicionais nos registos de trabalhos. 2. Corrija os erros e repita o pedido. 3. Utilize o iSeries Navigator para verificar ou corrigir a política da VPN. Certifique-se de que o grupo de chaves dinâmicas associado a esta ligação tem valores aceitáveis para endereços configurados.
TCP8620 O ponto de terminação da ligação local não está disponível	Não foi possível activar esta ligação da VPN, uma vez que o ponto de terminação da ligação local não estava disponível.	1. Verifique se existem mensagens adicionais nos registos de trabalhos referentes a esta ligação. 2. Certifique-se de que o ponto de terminação da ligação local está definido e que foi iniciado através da utilização do comando NETSTAT OPTION(*IFC). 3. Corrija quaisquer erros e repita o pedido.

TCP8621 O ponto de terminação de dados local não está disponível	Não foi possível activar esta ligação da VPN, uma vez que o ponto de terminação de dados local não estava disponível.	1. Verifique se existem mensagens adicionais nos registos de trabalhos referentes a esta ligação. 2. Certifique-se de que o ponto de terminação da ligação local está definido e que foi iniciado através da utilização do comando NETSTAT OPTION(*IFC). 3. Corrija quaisquer erros e repita o pedido.
TCP8622 A encapsulação de transportes não é permitida com uma porta de ligação	Não foi possível activar esta ligação da VPN, uma vez que a política negociada especificou o modo de encapsulamento do transporte e esta ligação está definida como uma porta de ligação de segurança.	1. Verifique se existem mensagens adicionais nos registos de trabalhos referentes a esta ligação. 2. Utilize o iSeries Navigator para alterar a política da VPN associada a esta ligação da VPN. 3. Corrija quaisquer erros e repita o pedido.
TCP8623 A ligação da VPN sobrepõe-se a uma existente	Não foi possível activar esta ligação da VPN, uma vez que uma ligação da VPN existente já está activada. Esta ligação tem um do ponto de terminação de dados local de [*valor do ponto de terminação de dados local*] e um de dados remoto de [*valor do ponto de terminação de dados remoto*].	1. Verifique se existem mensagens adicionais nos registos de trabalhos referentes a esta ligação. 2. Utilize o iSeries Navigator para visualizar todas as ligações activadas com pontos de terminação de dados local e remoto que sobreponham a ligação. Altere a política da ligação existente se ambas as ligações forem necessárias. 3. Corrija quaisquer erros e repita o pedido.
TCP8624 Ligação da VPN que não se encontre dentro do âmbito da regra de filtragem de políticas associada	Não foi possível activar esta ligação da VPN, uma vez que os pontos de terminação de dados não se encontram dentro da regra de filtragem de políticas definida.	1. Verifique se existem mensagens adicionais nos registos de trabalhos referentes a esta ligação. 2. Utilize o iSeries Navigator para visualizar as restrições do ponto de terminação de dados para esta ligação ou para este grupo de chaves dinâmicas. Se a opção **Subconjunto de filtragens de políticas** ou **Personalizar para corresponder à filtragem de políticas** estiver seleccionada, verifique os pontos de terminação de dados da ligação. Estes devem caber na regra de filtragem activa com uma acção IPSEC e um nome de ligação da VPN associado a esta ligação. Altere a política da ligação existente ou a regra de filtragem para activar esta ligação. 3. Corrija quaisquer erros e repita o pedido.

TCP8625 A ligação da VPN não conseguiu verificar um algoritmo ESP	Não foi possível activar esta ligação da VPN, uma vez que a chave secreta associada à ligação foi insuficiente.	1. Verifique se existem mensagens adicionais nos registos de trabalhos referentes a esta ligação. 2. Utilize o iSeries Navigator para visualizar a política associada a esta ligação e introduza uma chave secreta diferente. 3. Corrija quaisquer erros e repita o pedido.
TCP8626 O ponto de terminação da ligação da VPN não é igual ao ponto de terminação de dados	Não foi possível activar esta ligação da VPN, uma vez que a política especifica que é um sistema central e o ponto de terminação da ligação da VPN não é igual ao ponto de terminação de dados.	1. Verifique se existem mensagens adicionais nos registos de trabalhos referentes a esta ligação. 2. Utilize o iSeries Navigator para visualizar as restrições do ponto de terminação de dados para esta ligação ou para este grupo de chaves dinâmicas. Se a opção **Subconjunto de filtragens de políticas** ou **Personalizar para corresponder à filtragem de políticas** estiver seleccionada, verifique os pontos de terminação de dados da ligação. Estes devem caber na regra de filtragem activa com uma acção IPSEC e um nome de ligação da VPN associado a esta ligação. Altere a política da ligação existente ou a regra de filtragem para activar esta ligação. 3. Corrija quaisquer erros e repita o pedido.
TCP8628 A regra de filtragem de políticas não foi carregada	A regra de filtragem de políticas para esta ligação não está activa.	1. Verifique se existem mensagens adicionais nos registos de trabalhos referentes a esta ligação. 2. Utilize o iSeries Navigator para visualizar a filtragem de políticas activas. Verifique a regra de filtragem de políticas para esta ligação. 3. Corrija quaisquer erros e repita o pedido.
TCP8629 O pacote IP foi abandonado para a ligação da VPN	Esta ligação da VPN tem uma NAT da VPN configurada e o conjunto de endereços de NAT necessário excedeu os endereços de NAT disponíveis.	1. Verifique se existem mensagens adicionais nos registos de trabalhos referentes a esta ligação. 2. Utilize o iSeries Navigator para aumentar o número de endereços de NAT atribuídos a esta ligação da VPN. 3. Corrija quaisquer erros e repita o pedido.

TCP862A Falha no início da ligação PPP	Esta ligação da VPN foi associada a um perfil PPP. Quando esta foi iniciada, foi feita uma tentativa to iniciar o perfil PPP, mas ocorreu uma falha.	1. Verifique se existem mensagens adicionais nos registos de trabalhos referentes a esta ligação. 2. Verifique o registo de trabalhos associado com a ligação PPP. 3. Corrija quaisquer erros e repita o pedido.

Resolução de problemas da VPN com o rastreio de comunicações do OS/400

O iSeries fornece a capacidade de rastrear dados numa linha de comunicações, tal como uma interface de rede local (LAN) ou rede alargada (WAN). O utilizador médio poderá não compreender todo o conteúdo dos dados de rastreio. Contudo, é possível utilizar as entradas do rastreio para determinar se ocorreu uma troca de dados entre os sistemas local e remoto.

Iniciar o rastreio de comunicações

Utilize o comando Iniciar Rastreio de Comunicações (STRCMNTRC) para iniciar o rastreio de comunicações no sistema. O que se segue é um exemplo do comando STRCMNTRC:

```
STRCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) MAXSTG(2048) TEXT('Problemas da VPN')
```

Os parâmetros do comando são explicados na lista seguinte:

CFGOBJ (Objecto da configuração)
O nome do objecto de configuração ao qual será feito o rastreio. O objecto pode ser a descrição de uma linha, a descrição de uma interface de rede ou a descrição de um servidor de rede.

CFGTYPE (Tipo de configuração)
Está a ser feito o rastreio a uma linha (*LIN), a uma interface de rede (*NWI) ou a um servidor de rede (*NWS).

MAXSTG (Tamanho da memória tampão)
O tamanho da memória tampão para o rastreio. O valor assumido é 128 KB. O intervalo vai de 128 KB a 64 MB. O tamanho máximo real da memória tampão ao nível do sistema é definido nas Ferramentas de Serviço do Sistema (SST). Por isso, poderá receber uma mensagem de erro quando utilizar um tamanho de memória tampão maior no comando STRCMNTRC do que o definido nas SST. Tenha em atenção que a soma dos tamanhos de memória tampão especificados em todos os rastreios de comunicações já iniciados não pode exceder o tamanho de memória tampão máximo definido nas SST.

DTADIR (Direcção dos dados)
A direcção do tráfego de dados ao qual será feito o rastreio. A direcção pode ser apenas tráfego de envio (*SND), apenas tráfego de recepção (*RCV) ou ambas as direcções (*BOTH).

TRCFULL (Rastreio cheio)
O que ocorre quando a memória tampão de rastreio está cheia. Este parâmetro tem dois valores possíveis. O valor assumido é *WRAP, o que significa que, quando a memória tampão está cheia, o rastreio é reiniciado. Os registos de rastreio mais antigos são substituídos por novos, à medida que estes são recolhidos.

O segundo valor, *STOPTRC, pára o rastreio quando a memória tampão de rastreio especificada no parâmetro MAXSTG está cheia de registos de rastreio. Como regra geral, defina sempre o tamanho da memória tampão suficientemente grande para armazenar todos os registos de rastreio. Se o rastreio reiniciar ciclicamente, poderá perder importantes informações de rastreio. Se tiver um

problema que surja com muita frequência, defina a memória tampão com um tamanho suficientemente grande para que um reinício da memória tampão não elimine quaisquer informações importantes.

USRDTA (Número de bytes do utilizador a rastrear)
Define o número de dados ao qual será efectuado o rastreio, na parte de dados do utilizador das estruturas de dados. Por valor assumido, apenas os primeiros 100 bytes dos dados do utilizador são capturados para interfaces LAN. Para todas as outras interfaces, são capturados todos os dados do utilizador. Certifique-se de que especificou *MAX, se suspeitar de problemas nos dados do utilizador de uma estrutura.

TEXT (Descrição do rastreio)
Fornece uma descrição explicativa do rastreio.

Parar o rastreio de comunicações
Por norma, se não existirem indicações em contrário, o rastreio pára logo que a condição que estiver a ser rastreada ocorrer. Utilize o comando Terminar Rastreio de Comunicações (ENDCMNTRC) para parar o rastreio. O comando seguinte é um exemplo do comando ENDCMNTRC:

```
ENDCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN)
```

O comando possui dois parâmetros:

CFGOBJ (Objecto da configuração)
O nome do objecto de configuração ao qual está a ser feito o rastreio. O objecto pode ser a descrição de uma linha, a descrição de uma interface de rede ou a descrição de um servidor de rede.

CFGTYPE (Tipo de configuração)
Está a ser feito o rastreio a uma linha (*LIN), a uma interface de rede (*NWI) ou a um servidor de rede (*NWS).

Imprimir os dados de rastreio
Depois de parar o rastreio de comunicações, necessita de imprimir os dados de rastreio. Utilize o comando Imprimir Rastreio de Comunicações (PRTCMNTRC) para executar esta tarefa. Como todo o tráfego da linha é capturado durante o período de rastreio, possui diversas opções de filtragem para a geração de output. Procure que o ficheiro colocado em spool se mantenha tão pequeno quanto o possível. Isto torna a análise mais rápida e eficiente. No caso de um problema com a VPN, apenas deve filtrar o tráfego IP e, se possível, num endereço de IP específico. Tem ainda a opção de filtrar um número de porta IP específico. O que se segue é um exemplo do comando PRTCMNTRC:

```
PRTCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) FMTTCP(*YES) TCPIPADR('10.50.21.1)
    SLTPORT(500) FMTBCD(*NO)
```

Neste exemplo, o rastreio é formatado para o tráfego IP e contém apenas dados para o endereço de IP, em que o endereço de origem e de destino é 10.50.21.1 e o número da porta IP de origem ou de destino é 500.

Apenas os parâmetros do comando mais importantes para a análise dos problemas da VPN são explicados a seguir:

CFGOBJ (Objecto da configuração)
O nome do objecto de configuração ao qual está a ser feito o rastreio. O objecto pode ser a descrição de uma linha, a descrição de uma interface de rede ou a descrição de um servidor de rede.

CFGTYPE (Tipo de configuração)
Está a ser feito o rastreio a uma linha (*LIN), a uma interface de rede (*NWI) ou a um servidor de rede (*NWS).

FMTTCP (Formatar dados TCP/IP)
Formata ou não o rastreio para dados TCP/IP ou UDP/IP. Especifique *YES para formatar o rastreio de dados IP.

TCPIPADR (Formatar dados TCP/IP por endereço)
Este parâmetro é constituído por dois elementos. Se especificar endereços de IP em ambos os elementos, apenas será impresso o tráfego IP entre os referidos endereços.

SLTPORT (Número da porta IP)
O número de porta IP a filtrar.

FMTBCD (Formatar dados de difusão)
Para saber se todas as estruturas de difusão são ou não impressas. O valor assumido é sim. Se não quiser, por exemplo, pedidos Address Resolution Protocol (ARP), especifique *NO; caso contrário, pode ficar sobrecarregado com mensagens de difusão.

Informações relacionadas com a VPN

Para obter mais cenários e descrições da configuração da VPN, consulte outras fontes de informação:

- **OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM e(logo)server iSeries Server with Windows 2000 VPN Clients, REDP0153** 
  Este Redpaper da IBM fornece um processo passo a passo para a configuração do direccionamento da VPN utilizando a VPN da V5R1 e o L2TP nativo do Windows 2000 e o suporte IPSec.

- **AS/400 Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00** 
  Este redbook explora os conceitos da VPN e descreve a implementação dos mesmos através do Protocolo IP Security (IPSec) e do Protocolo Layer 2 Tunneling (L2TP) no OS/400.

- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00** 
  Este redbook explora todas as funcionalidades de segurança da rede nativa no sistema AS/400, tais como filtros de IP, NAT, VPN, servidor proxy de HTTP, SSL, DNS, reencaminhamento de correio, auditorias e registos em diário. Descreve a utilização das mesma através de exemplos práticos.

- **Virtual Private Networking: Securing Connections** 
  Esta página da Web apresenta as novidades de última hora referentes à VPN, lista os PTFs mais recentes e estabelece ligação a outros sites de interesse.
- **Outros manuais e redbooks relacionados com a segurança**
  Consulte esta página para obter uma lista com outras informações relacionadas com segurança que se encontram disponíveis online.

Para guardar um PDF na estação de trabalho para ser visualizado ou impresso:

1. Faça clique com o botão direito do rato sobre o PDF no browser (faça clique com o botão direito do rato sobre a ligação acima).
2. Faça clique sobre **Guardar Destino Como...**
3. Navegue para o directório no qual pretende guardar o PDF.
4. Faça clique sobre **Guardar**.

Se necessitar do Adobe Acrobat Reader para ver ou imprimir estes PDFs, poderá descarregar uma cópia do site da Web da Adobe (www.adobe.com/prodindex/acrobat/readstep.html)  .