System i

Segurança
Funcionamento em Rede Privada Virtual

Versão 6 Edição 1

System i

Segurança
Funcionamento em Rede Privada Virtual

Versão 6 Edição 1

Nota

Antes de utilizar estas informações e e o produto que suportam, não deixe de ler as informações na secção "Avisos", na página 87.

Esta edição aplica-se à versão 6, edição 1, modificação 0 do i5/OS da IBM (número de produto 5761-SS1) e para todas as edições e modificações subsequentes até indicação em contrário em novas edições. Esta versão não é executada em todos os modelos RISC (reduced instruction set computer), nem nos modelos CISC.

Índice

Funcionamento em Rede Privada Virtual

Uma rede privada virtual (VPN - virtual private network) 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 é um componente de instalação opcional do System i Navigator, a interface gráfica de utilizador (GUI) do i5/OS. A VPN permite criar um caminho seguro terminal a terminal entre qualquer combinação de sistema central e porta de ligação. A VPN utiliza métodos de autenticação, algoritmos de codificação e outras protecções para assegurar que os dados enviados entre os dois terminais de uma ligação permanecem seguros.

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 IPSec (IP Security Architecture). A 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 Layer 2 Tunnel Protocol (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 a 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. Reveja estes tópicos para confirmar que sabe como funcionam as VPNs e como poderá utilizá-las:

Novidades da V6R1

Não deixe de ker as informações novas e significativamente alteradas sobre o conjunto de tópicos Funcionamento em Rede Privada Virtual.

Nova Função: IP versão 6

Agora poderá utilizar IP versão 6 para criar uma VPN com os seguintes tipos de ligação: sistema a sistema, sistema a porta de ligação, e porta de ligação a porta de ligação. As ligações VPN suportam IP versão 6 para endereços, intervalos, sub-redes e nomes de sistema central. Todos os assistentes VPN foram actualizados para aceitarem os novos tipos de ID de IP versão 6.

- Internet Protocol versão 6

Como ver o que há de novo ou alterado

Para o ajudar a ver onde foram efectuadas alterações técnicas, estas informações utilizam:

- A » imagem para marcar onde começam as informações novas ou alteradas.
- A « imagem para marcar onde terminam as informações novas ou alteradas.

Para encontrar outras informações sobre o que há de novo ou foi alterado nesta edição, consulte o Memo to Users.

Ficheiro PDF para rede privada virtual

Pode ver e imprimir um ficheiro PDF com estas informações.

Para ver ou descarregar a versão em PDF deste documento, seleccione Rede Privada Virtual (VPN) (cerca de 1100 KB).

Guardar ficheiros PDF

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

1. Clique com o botão direito do rato na hiperligação para o PDF no browser.
2. Faça clique em **Guardar Destino Como** se estiver a utilizar o Internet Explorer. Faça clique em **Guardar Ligação Como** se estiver a utilizar o Netscape Communicator.
3. Navegue para o directório no qual pretende guardar o PDF.
4. Faça clique em **Guardar**.

Descarregar o Adobe Acrobat Reader

Necessita do Adobe Acrobat Reader para ver ou imprimir estes PDFs. Poderá descarregar uma cópia no sítio na Web da Adobe (www.adobe.com/products/acrobat/readstep.html) .

Conceitos da VPN

É importante que tenha, pelo menos, conhecimentos básicos sobre as tecnologias VPN padrão antes de implementar uma ligação VPN.

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

Protocolos de Segurança de IP

O protocolo IP Security (IPSec) faculta uma base estável e duradoura para segurança de nível de rede.

O IPSec suporta todos os algoritmos criptográficos usados actualmente e pode 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 alegado 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.

Nota: Algumas configurações de VPN poderão ter alguma vulnerabilidade a nível da segurança, dependendo da forma como o IPSec está configurado. A vulnerabilidade afecta as configurações nas quais o IPsec está configurado para usar Encapsulating Security Payload (ESP) em modo túnel com confidencialidade (codificação), mas sem protecção de integridade (autenticação) nem Authentication Header (AH). Sempre que o ESP é seleccionado, a configuração predefinida inclui um algoritmo de autenticação que faculta protecção de integridade. Assim sendo, a não ser que o algoritmo de autenticação na transformação de ESP seja removido, a configuração de VPN ficará protegida desta vulnerabilidade. A configuração da VPN da IBM Universal Connection não é afectada por esta vulnerabilidade.

Para verificar se o sistema se encontra afectado por esta vulnerabilidade de segurança, siga estes passos:

1. No System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP** → **Rede Privada Virtual** → **Políticas de Segurança de IP**.
2. Faça clique com o botão direito do rato na política de dados que pretende verificar e seleccione **Propriedades**.
3. Faça clique no separador **Propostas**.
4. Seleccione qualquer uma das propostas de protecção de dados que usam o protocolo ESP e faça clique em **Editar**.
5. Faça clique no separador **Transformações**.
6. Seleccione qualquer uma das transformações da lista que usem o protocolo ESP e faça clique em **Editar**.
7. Verifique se o algoritmo de Autenticação tem qualquer outro valor que não seja **Nenhum**.

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 sítio na Web: http://www.rfc-editor.org.

Os protocolos IPSec principais são listados a seguir:

Conceitos relacionados

"Gestão de chaves" na página 6
Uma VPN dinâmica proporciona segurança adicional às comunicações, com o protocolo Internet Key Exchange (IKE) para a gestão de chaves. O IKE permite aos servidores VPN em cada extremo da ligação negociar novas chaves em intervalos específicos.

Informações relacionadas

http://www.rfc-editor.org

Cabeçalho de Autenticação (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 garantir a autenticação da origem dos dados, o AH inclui uma chave partilhada secreta no algoritmo que utiliza para a autenticação. Para garantir 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 designadas unicamente por autenticação. De forma simplista, o AH assegura que nada interfere com os dados em trânsito para o terminal.

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 destinatário. 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 sítio na 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 túnel. 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 túnel, mas não proporciona tanta segurança.

O modo de túnel 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 de resposta pode detectar se o datagrama foi alterado em trânsito.

Quando ambos os extremos de uma associação de segurança forem portas de ligação, utilize o modo de túnel. No modo de túnel, 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 funcionar com um túnel 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 túnel é que este protege totalmente o datagrama IP encapsulado. Além disso, o modo de túnel 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 restringida nalgumas regiões, enquanto o AH não é regulado e pode ser utilizado livremente em todo o mundo.

Usar ESN com AH

Se usar o protocolo AH, é provável que pretenda activar o Extended Sequence Number (ESN). O ESN permite a transmissão de grandes volumes de dados a uma elevada velocidade sem ter de voltar a inserir as informações. A ligação VPN usa uma sequência de números de 64 bits em vez de números de 32 bits através de IPSec. A utilização da sequência de números de 64 bits confere mais tempo antes de ter de voltar a inserir, o que evita a exaustão de sequências de números e minimiza o uso de recursos do sistema.

Quais os algoritmos utilizados pelo AH para proteger a minha informação?

O AH utiliza algoritmos conhecidos por **códigos de autenticação de mensagens atribuídos aleatoriamente (hashed message authentication codes - HMAC)**. Mais especificamente, a VPN utiliza os HMAC-MD5 ou HMAC-SHA. Tanto os MD5 como os SHA recebem dados de entrada de comprimento variável e uma chave secreta para produzir dados de saída 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 na respectiva saída de dados, mas os SHA são considerados mais seguros, uma vez que produzem atribuições aleatórias mais abrangentes.

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 sítio na Web: http://www.rfc-editor.org.

Conceitos relacionados

"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.

Informações relacionadas

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 em comunicação utilizam uma chave partilhada para codificação e descodificação dos dados que trocam.

Se decidir utilizar codificação e autenticação, o sistema de resposta 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 ESP

É possível aplicar o ESP de duas formas: modo de transporte ou modo de túnel. 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 túnel, mas não proporciona tanta segurança. Na maioria dos casos, os sistemas centrais utilizam o ESP em modo de transporte.

O modo de túnel 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 têm de utilizar o ESP em modo de túnel.

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 remetente e o destinatário têm de acordar numa chave, antes de efectuarem comunicações seguras entre si. A VPN utiliza Data Encryption Standard (DES), triple-DES (3DES), RC5, RC4 ou Advanced Encryption Standard (AES) para codificação.

Se optar pelo algoritmo de AES para codificação, é provável que pretenda activar o Extended Sequence Number (ESN). O ESN permite a transmissão de grandes volumes de dados a uma elevada velocidade. A ligação de VPN usa uma sequência de números de 64 bits em vez de números de 32 bits através de IPSec. A utilização da sequência de números de 64 bits confere mais tempo antes de ter de voltar a inserir, o que evita a exaustão de sequências de números e minimiza o uso de recursos do sistema.

A Internet Engineering Task Force (IETF) define formalmente DES no 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 e outros RFCs na Internet, no seguinte endereço na 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 entrada de comprimento variável e uma chave secreta para produzir dados de saída 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 na respectiva saída de dados, mas os SHA são considerados mais seguros, uma vez que produzem atribuições aleatórias mais abrangentes.

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

Conceitos relacionados

"Cabeçalho de Autenticação (Authentication Header)" na página 3
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.

Informações relacionadas

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, o tempo sistema de processamento envolvido pode ultrapassar os benefícios.

Gestão de chaves

Uma VPN dinâmica proporciona segurança adicional às comunicações, com o protocolo Internet Key Exchange (IKE) para a gestão de chaves. O IKE permite aos servidores VPN em cada extremo da ligação negociar novas chaves em intervalos específicos.

A cada negociação bem sucedida, os servidores VPN voltam a criar as chaves que protegem uma ligação, tornando assim mais difícil que um elemento estranho capture informações da ligação. Além disso, se utilizar sigilo de reencaminhamento perfeito (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 a utilização dos 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 terminal 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 têm de acordar uma 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 fora de banda, por exemplo por telefone ou por correio registado, antes das negociações de IKE. Trate 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 com o Digital Certificate Manager. Além disso, algumas soluções da VPN necessitam da Assinatura RSA para interoperacionalidade. Por exemplo, a VPN do Windows 2000 utiliza Assinatura RSA como o método de autenticação predefinido. Por fim, a Assinatura RSA fornece mais escalabilidade que as chaves pré-partilhadas. Os certificados utilizados têm de 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 troca de dados de aplicação. Atenção, até este ponto, não foram realmente enviados nenhuns dados de aplicação. 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 chaves, 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 utilizando o System i Navigator, tem de definir uma política de IKE para activar as negociações de fase 1 e uma política de dados para governar 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

Caso pretenda ler mais sobre o protocolo Internet Key Exchange (IKE) e a gestão de chaves, reveja os seguintes Internet Engineering Task Force (IETF) Request for Comments (RFC):

- 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 sítio na Web: http://www.rfc-editor.org.

Conceitos relacionados

"Cenário: VPN com Firewall de Fácil Utilização" na página 31
Neste cenário, uma grande seguradora pretende estabelecer uma VPN entre uma porta de ligação em Lisboa e um sistema central no Porto, sendo que ambas as redes estão protegidas por uma firewall.

"Protocolos de Segurança de IP" na página 2
O protocolo IP Security (IPSec) faculta uma base estável e duradoura para segurança de nível de rede.

Tarefas relacionadas

"Configurar uma política Internet Key Exchange" na página 51
A política IKE define qual o nível de autenticação e de protecção de codificação é utilizado pelo IKE durante negociações de fase 1.

"Configurar uma política de dados" na página 52
Uma política de dados define qual o nível de autenticação ou de codificação que protege os dados que circulam na VPN.

Informações relacionadas

http://www.rfc-editor.org

Layer 2 Tunnel Protocol

As ligações Layer 2 Tunneling Protocol (L2TP), também chamadas linhas virtuais, proporcionam um acesso pouco dispendioso a utilizadores remotos, ao permitir ao sistema de rede de uma empresa gerir os endereços de IP atribuídos aos respectivos utilizadores remotos. 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 túnel: túnel voluntário e túnel obrigatório. A maior diferença entre estes dois tipos de túnel é o terminal. No túnel voluntário, o túnel termina no cliente remoto, enquanto que no túnel obrigatório termina no ISP (Internet Service Provider - fornecedor de serviços de internet).

Com um **túnel obrigatório** de L2TP, um sistema central remoto inicia uma ligação ao respectivo 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 túnel obrigatório, o ISP tem de suportar o LT2P.

Com um **túnel voluntário** de L2TP, a ligação é criada pelo utilizador remoto, de modo geral através de um cliente de túnel L2TP. Por conseguinte, o utilizador remoto envia pacotes L2TP ao respectivo ISP, que

os remete para a rede da empresa. Com um túnel voluntário, o ISP não necessita de suportar L2TP. O cenário Proteger um túnel voluntário de L2TP com IPSec, fornece um exemplo de configuração de um sistema para uma sucursal a fim de estabelecer ligação com a rede através de um sistema de porta de ligação com um túnel de L2TP protegido pela VPN.

Pode ver uma apresentação visual sobre o conceito de túneis voluntários de L2TP protegidos por IPSec. É necessário o plug-in de Flash. Em alternativa, pode utilizar a versão HTML desta apresentação.

Na realidade, o L2TP é uma variante de um protocolo de encapsulamento de IP. O túnel de L2TP é criado pelo encapsulamento de uma estrutura L2TP dentro de um pacote do Protocolo User Datagram (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 túnel de L2TP. Em seguida, pode aplicar os protocolos Authentication Header (AH), Encapsulated Security Payload (ESP) e Internet Key Exchange (IKE) de uma forma simples.

Conceitos relacionados

"Cenário: Proteger um túnel voluntário de L2TP com IPSec" na página 24
Neste cenário, irá aprender como configurar 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.

Conversão de endereços de rede para a VPN

A VPN fornece uma forma de executar a conversão de endereços da rede, denominada NAT de VPN. A NAT de 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.

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 optar por comunicar com outra rede e ambas as redes utilizarem endereços 10.*.*.*, levando a que os endereços colidam e larguem todos os pacotes. A aplicação da NAT aos endereços de partida pode ser a resposta para este problema. Contudo, se o tráfego de dados estiver protegido por uma VPN, a NAT convencional não terá resultados, 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 NAT de 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: A NAT de VPN não é suportada em protocolo FTP, de momento.

Como devo utilizar a NAT de VPN?

Existem dois tipos diferentes de NAT de VPN que é necessário ter em conta antes de começar. São eles:

NAT de VPN para impedir conflitos entre endereços de IP

Este tipo de NAT de VPN permite evitar possíveis conflitos entre endereços de IP quando configurar uma ligação VPN entre redes ou sistemas com esquemas de endereçamento semelhantes. Um cenário típico é aquele em que ambas as empresas criam ligações VPN, através de um dos intervalos de endereços de IP privados designados. Por exemplo, 10.*.*.*. A forma como configura este tipo de NAT de VPN depende do facto de o sistema ser o iniciador ou o programa de resposta da ligação VPN. Quando o sistema for o iniciador da ligação, pode converter os endereços locais em endereços compatíveis com o

endereço da ligação VPN parceira. Quando o sistema for o programa de resposta da ligação, pode converter os endereços remotos da ligação VPN parceira em endereços compatíveis com o esquema de endereçamento local. Configure este tipo de conversão de endereços apenas para as ligações dinâmicas.

NAT de VPN para ocultar endereços locais

Este tipo de NAT de VPN é utilizado principalmente para ocultar o endereço de IP real do sistema local, mediante conversão deste endereço noutro que possa ser disponibilizado publicamente. Quando configurar a NAT de 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 ainda equilibrar o fluxo de tráfego de um endereço individual através de vários endereços. A NAT de VPN para endereços locais requer que o sistema seja o programa de resposta das respectivas ligações.

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

1. Dispõe de um ou mais sistemas aos quais pretende que as pessoas tenham acesso através de uma VPN?
2. Necessita de ser flexível em relação aos verdadeiros endereços de IP dos sistemas?
3. Dispõe de um ou mais endereços de IP globalmente encaminháveis?

O cenário Utilizar conversão da rede para a VPN dá um exemplo de configuração de NAT de VPN para ocultar endereços locais no modelo System i.

Para instruções passo a passo sobre a configuração da NAT de VPN no sistema, utilize a ajuda online disponível na interface da VPN no System i Navigator.

Conceitos relacionados

"Cenário: Utilizar conversão de endereços de rede para a VPN" na página 43
Neste cenário, a sua empresa pretende trocar dados sensíveis com um dos parceiros empresariais, por meio da VPN. Para proteger ainda mais a privacidade da estrutura de rede da sua empresa, também irá utilizar a NAT de VPN para ocultar o endereço de IP do sistema utilizado para hospedar as aplicações a que o parceiro de negócios tem acesso.

"Folha de trabalho de planeamento para ligações manuais" na página 48
Preencha esta folha de trabalho antes de configurar uma ligação manual.

IPSec compatível com NAT com protocolo 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.

O problema: A NAT convencional interrompe a VPN

A conversão de endereços da rede (NAT, Network address translation) permite ocultar os endereços de IP privados não registados atrás de um conjunto de endereços de IP registados. Tal ajuda a proteger a rede interna das redes externas. A NAT ajuda também a aliviar o problema de esgotamento 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 tal acontece, a parte destinatária da ligação VPN rejeita o pacote e a negociação da ligação VPN falha.

A 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, a parte destinatária decompõe o cabeçalho adicional, deixando o pacote IPSec original, que irá passar agora por todas as restantes validações.

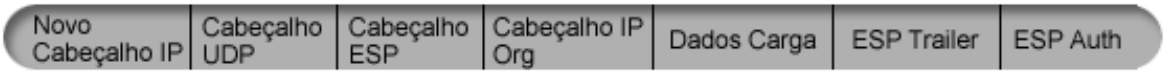
Apenas pode aplicar encapsulamento UDP a VPNs que vão utilizar ESP IPSec em modo de túnel ou modo de transporte. Além disso, o sistema só pode agir como cliente para encapsulamento UDP. Isto é, apenas pode *iniciar* tráfego encapsulado UDP.

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

Datagrama IPv4 original:

Após aplicar IPSec ESP em modo túnel:

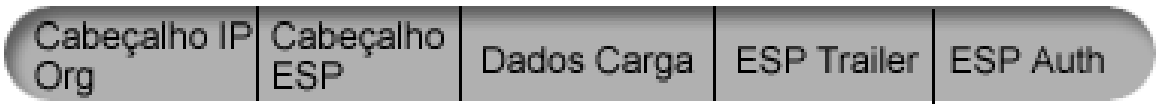
Após aplicar o Encapsulamento UDP:



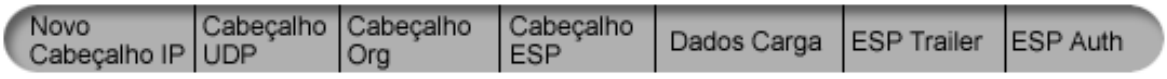
Os gráficos abaixo ilustram o formato de um pacote ESP com encapsulamento UDP no modo de transporte:

Datagrama IPv4 original:

Após aplicar IPSec ESP em modo de transporte:



Após aplicar o Encapsulamento UDP:



Depois de o pacote estar encapsulado, o sistema envia o pacote para o respectivo parceiro da VPN através da porta 4500 UDP. Normalmente, os parceiros da VPN executam negociações IKE através da porta 500 UDP. No entanto, quando IKE detecta NAT durante a negociação de chaves, os pacotes de IKE subsequentes são enviados através da porta 4500, porta de destino 4500. Isto também significa que a porta 4500 não pode ter restrições a nenhumas regras de filtro aplicáveis. A parte destinatária da ligação pode determinar se o pacote é o pacote IKE ou um pacote encapsulado UDP porque os primeiros 4 bytes

da carga útil UDP foram definidos como zero num pacote IKE. Para que funcione devidamente, ambas os extremos da ligação têm de suportar encapsulamento UDP.

Conceitos relacionados

"Cenário: VPN com Firewall de Fácil Utilização" na página 31
Neste cenário, uma grande seguradora pretende estabelecer uma VPN entre uma porta de ligação em Lisboa e um sistema central no Porto, sendo que ambas as redes estão protegidas por uma firewall.

Compressão de IP

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 segurança alguma e tem de ser utilizado juntamente com uma transformação de AH ou ESP quando é feita uma comunicação através de uma ligação 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 sítio na Web: http://www.rfc-editor.org.

Informações relacionadas

http://www.rfc-editor.org

Filtragem da VPN e IP

A filtragem IP e a VPN estão estreitamente relacionadas. De facto, a maioria das ligações da VPN requerem regras de filtro para funcionarem correctamente. Este tópico, fornece informações sobre quais os filtros requeridos pela VPN, bem como outros conceitos de filtragem relacionados com a VPN.

A maioria das ligações da VPN exige regras de filtro para funcionar correctamente. As regras de filtro 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 um filtro de políticas. O filtro de políticas define quais os endereços, protocolos e portas que podem utilizar a VPN. Além disso, as ligações que suportam o protocolo Internet Key Exchange (IKE) contêm regras escritas explicitamente para permitir o processamento de IKE na ligação. A VPN pode gerar estas regras automaticamente. Sempre que for possível, deve permitir que seja a VPN a criar os filtros de políticas. Isto vai ajudar a eliminar os erros, mas também elimina a necessidade de configurar as regras como um passo à parte utilizando o editor de Regras de Pacotes no System i Navigator.

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

Conceitos relacionados

"Configurar regras de pacotes da VPN" na página 55
Se estiver a criar uma ligação pela primeira vez, deve permitir que a VPN crie automaticamente as regras de pacotes da VPN. Pode fazê-lo com o assistente Nova Ligação ou nas páginas de propriedades da VPN para configurar a ligação.

Ligações da VPN sem filtros de políticas

Se os terminais da VPN forem endereços de IP únicos e específicos e quiser iniciar a VPN sem ter de escrever ou activar regras de filtro no sistema, pode configurar um filtro de políticas dinâmico.

Uma regra de filtro 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 optar por configurar uma ligação que não necessite de uma regra de filtro de políticas. Por exemplo, pode ter carregadas

regras de pacotes alheias a VPNs na interface a utilizar pela ligação da VPN e assim, em vez de desactivar as regras activas nessa interface, configurar a VPN de forma a que o sistema faça a gestão dinâmica de todos os filtros para essa ligação. O filtro de políticas para este tipo de ligação chama-se **filtro de políticas dinâmico**. Antes de poder utilizar um filtro de políticas dinâmico na ligação da VPN, tem de garantir o seguinte:

- A ligação só pode ser iniciada pelo sistema local.
- Os terminais de dados da ligação têm de ser sistemas únicos. Isto é, não podem ser sub-redes nem intervalos de endereços.
- Não pode ser carregada nenhuma regra de filtro de política para a ligação.

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

Para instruções sobre a configuração de uma ligação de forma a não exigir um filtro de políticas, utilize a ajuda online da VPN.

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 filtro especificamente escritas para permitir o tráfego IKE, o tráfego IKE estará implicitamente garantido no sistema.

Para estabelecer uma ligação, a maioria das VPNs exigem que as negociações do Internet Key Exchange (IKE) ocorram para que o processamento IPSec possa ser executado. O IKE utiliza a porta 500, de modo que para funcionar correctamente, terá de permitir datagramas UDP pela porta 500 para este tipo de tráfego IP. Caso não existam regras de filtro especificamente escritas para permitir o tráfego IKE, o tráfego IKE estará 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 filtro activas.

Cenários: VPN

Consulte estes cenários para se familiarizar com os aspectos técnicos e de configuração que cada um destes tipos de ligação básica envolve.

Conceitos relacionados

Cenário de QoS: Resultados seguros e previsíveis (VPN e QoS)

Informações relacionadas

OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM e(logo)server iSeries Server with Windows 2000 VPN Clients, REDP0153

AS/400 Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00

AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00

Cenário: Ligação de uma sucursal

Neste cenário, a empresa pretende estabelecer uma VPN entre as sub-redes de dois departamentos remotos através de dois modelos System i, que desempenharão as funções de porta de ligação VPN.

Situação

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 VPN, o que pode ser a rede privada da empresa ou a Internet pública.

Importante: Este cenário mostra as portas de ligação de segurança do modelo System i 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.

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 sistemas 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 de IP a cada cliente.

Objectivos

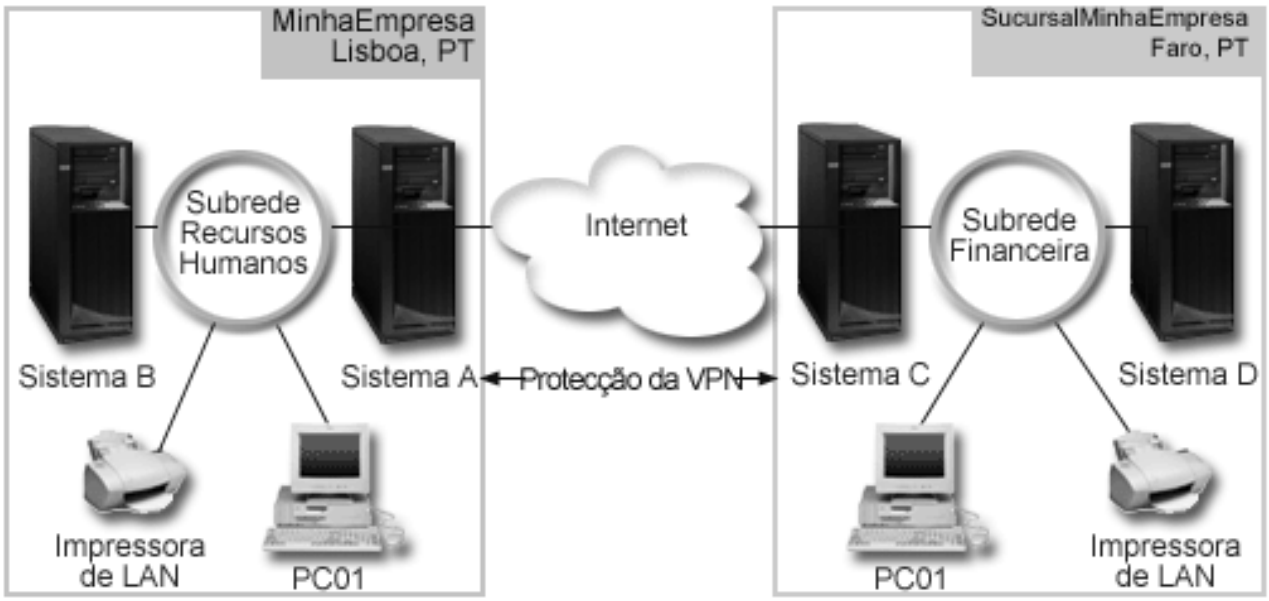
Neste cenário, a MinhaEmp, Lda. pretende estabelecer uma VPN entre as sub-redes dos departamentos de Recursos Humanos e Financeiro através de um par de modelos System i. Ambos os sistemas servirão de portas de ligação VPN. Em termos das configurações da VPN, uma porta de ligação executa a gestão de chaves e aplica a IPSec aos dados que circulam através de encaminhamento. As portas de ligação não são terminais de dados da ligação.

Os objectivos deste cenário são os seguintes:

- A VPN tem de 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 sistemas de porta 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 Sistema A é executado no i5/OS Versão 5 Edição 3 (V5R3) ou posterior e serve de porta de ligação 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 terminal de dados de encaminhamento da VPN do lado de MinhaEmp Lisboa.
- O Sistema A estabelece ligação à Internet através do endereço de IP 204.146.18.227. Isto é o terminal da ligação. Ou seja, o Sistema A executa a gestão de chaves e aplica a IPSec a datagramas de IP de chegada e de partida.
- O Sistema A estabelece ligação à respectiva sub-rede com o endereço de IP 10.6.11.1.
- O Sistema B é um sistema de produção na sub-rede dos Recursos Humanos que executa aplicações TCP/IP padrão.

Departamento Financeiro

- O Sistema C é executado no i5/OS Versão 5 Edição 3 (V5R3) ou posterior e serve de porta de ligação VPN do Departamento Financeiro.
- A sub-rede é 10.196.8.0 com a máscara 255.255.255.0. Esta sub-rede representa o terminal de dados de encaminhamento da VPN do lado de MinhaEmp Aveiro.
- O Sistema C estabelece ligação à Internet através do endereço de IP 208.222.150.250. Isto é o terminal da ligação. Ou seja, o Sistema C executa a gestão de chaves e aplica a IPSec a datagramas de IP de chegada e de partida.
- O Sistema C estabelece ligação à respectiva sub-rede com o endereço de IP 10.196.8.5.

Tarefas de configuração

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

Nota: Antes de dar início a estas tarefas, verifique o encaminhamento de TCP/IP para se certificar de que dois sistemas de porta de ligação podem comunicar um com o outro pela Internet. Isto garante

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.

Conceitos relacionados

Equilíbrio de volumes de trabalho e encaminhamento de TCP/IP

Informações relacionadas

AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00

Preencher as folhas de trabalho de planeamento

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

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

Tabela 1. Requisitos do sistema

Lista de verificação de pré-requisitos	**Respostas**
O sistema executa i5/OS V5R3 ou posterior?	Sim
A opção Gestor de Certificados Digitais está instalada?	Sim
O System i Access for Windows está instalado?	Sim
O System i Navigator está instalado?	Sim
O subcomponente de Rede do System i Navigator está instalado?	Sim
O IBM TCP/IP Connectivity Utilities for i5/OS 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 sistema (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 terminais necessários?	Sim
Aplicou as mais recentes correcções temporárias de programas (PTFs)?	Sim
Se o túnel de VPN passa por firewalls ou encaminhadores que implementem filtragem de pacotes de IP, as regras de filtro da firewall ou dos encaminhadores suportam protocolos de 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

Tabela 2. Configuração da VPN

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(a)
Está a utilizar certificados para autenticar a ligação? Em caso negativo, qual é a chave pré-partilhada?	Nada ultra-secreto
Qual é o identificador do servidor de chaves locais?	Endereço de IP: 204.146.18.227

Tabela 2. Configuração da VPN (continuação)

Necessita destas informações para configurar a VPN	Respostas
Qual é o identificador do terminal de dados local?	Sub-rede: 10.6.0.0 Máscara: 255.255.0.0
Qual é o identificador do servidor de chaves remotas?	Endereço de IP: 208.222.150.250
Qual é o identificador do terminal 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 na ligação?	Qualquer uma
De que tipo de segurança e de rendimento de sistema necessita para proteger os seus dados?	equilibrado(a)
A que interfaces é aplicada a ligação?	TRLINE

Configurar a VPN no Sistema A

Siga esta tarefa para configurar o Sistema A

Utilize os seguintes passos e as informações das folhas de trabalho para configurar a VPN no Sistema A do seguinte modo:

1. Em System i Navigator, expanda **Sistema A** → **Rede** → **Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Rede Privada Virtual** e seleccione **Nova Ligação** para iniciar o assistente de Nova Ligação.
3. Reveja a página **Bem-vindo(a)** para mais informações sobre quais os objectos que o assistente cria.
4. Faça clique em **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 em **Seguinte** para ir para a página **Cenário da Ligação**.
8. Seleccione **Ligar a porta de ligação a outra ligação**.
9. Faça clique em **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 em **Seguinte** para ir para a página **Certificado para terminal da Ligação Local**.
12. Seleccione **Não** para indicar que não utilizará certificados para autenticar a ligação.
13. Faça clique em **Seguinte** para ir para a página **Servidor de Chaves Locais**.
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 em **Seguinte** para ir para a página **Servidor de Chaves Remotas**.
17. Seleccione **Endereço de IP versão 4** no campo **Tipo de identificador**.
18. Introduza `208.222.150.250` no campo **Identificador**.
19. Insira `ultra-secreto` no campo **Chave pré-partilhada**
20. Faça clique em **Seguinte** para ir para a página **Terminal 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 em **Seguinte** para ir para a página **Destino Final dos 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 em **Seguinte** para ir para a página **Serviços de Dados**.
29. Aceite os valores predefinidos e, em seguida, faça clique em **Seguinte** para ir para a página **Política de Dados**.
30. Seleccione **Criar uma nova política** e, em seguida, seleccione **Segurança e rendimento equilibrados**.
31. Seleccione **Utilizar o algoritmo de codificação RC4**.
32. Faça clique em **Seguinte** para ir para a página **Interfaces Aplicáveis**.
33. Seleccione **TRLINE** na tabela de **Linhas**.
34. Faça clique em **Seguinte** para ir para a página **Resumo**. Reveja os objectos que o assistente irá criar para se certificar de que estão correctos.
35. Faça clique em **Terminar** para concluir a configuração.
36. Quando surgir a caixa de diálogo **Activar Filtros de Políticas**, seleccione **Sim, activar os filtros de políticas gerados** para de seguida seleccionar **Permitir todo o tráfego restante**.
37. Faça clique em **OK** para concluir a configuração. Quando lhe for pedido, especifique que pretende activar as regras para todas as interfaces.

Tarefas relacionadas

"Configurar a VPN no Sistema C"
Siga os mesmos passos utilizados para configurar a VPN no Sistema A, alterando os endereços de IP conforme necessário. Utilize as folhas de trabalho de planeamento como guia.

Configurar a VPN no Sistema C

Siga os mesmos passos utilizados para configurar a VPN no Sistema A, alterando os endereços de IP conforme necessário. Utilize as folhas de trabalho de planeamento como guia.

Quando terminar a configuração da porta de ligação VPN do Departamento Financeiro, as suas ligações estarão num estado *a pedido*, pelo que a ligação é iniciada quando forem enviados os datagramas de IP que esta ligação VPN tem de proteger. O passo seguinte é iniciar os servidores da VPN, caso ainda não tenham sido iniciados.

Tarefas relacionadas

"Configurar a VPN no Sistema A" na página 17
Siga esta tarefa para configurar o Sistema A

Iniciar a VPN

Depois de configurar a ligação VPN nos Sistemas A e C, terá de a iniciar.

Siga estes passos para iniciar a VPN:

1. Em System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP**.
2. Faça clique com o botão direito do rato em **Rede Privada Virtual** e seleccione **Iniciar**.

Testar uma ligação

Depois de concluir a configuração de ambos os sistemas e de iniciar os servidores VPN, deve testar a conectividade para se assegurar de que as sub-redes remotas conseguem comunicar entre elas.

Para testar a ligação, siga estes passos:

1. Em System i Navigator, expanda **Sistema A** → **Rede**.
2. Faça clique com o botão direito do rato em **Configuração de TCP/IP**, seleccione **Utilitários** e depois **Ping**.
3. Na caixa de diálogo **Ping a partir de**, insira `Sistema C` no campo **Ping**.
4. Faça clique em **Efectuar Ping Agora** para verificar a conectividade do Sistema A ao Sistema C.
5. Faça clique em **OK** quando tiver terminado.

Cenário: Ligação básica 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.

Situação

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 sítio na 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 empresas.

Objectivos

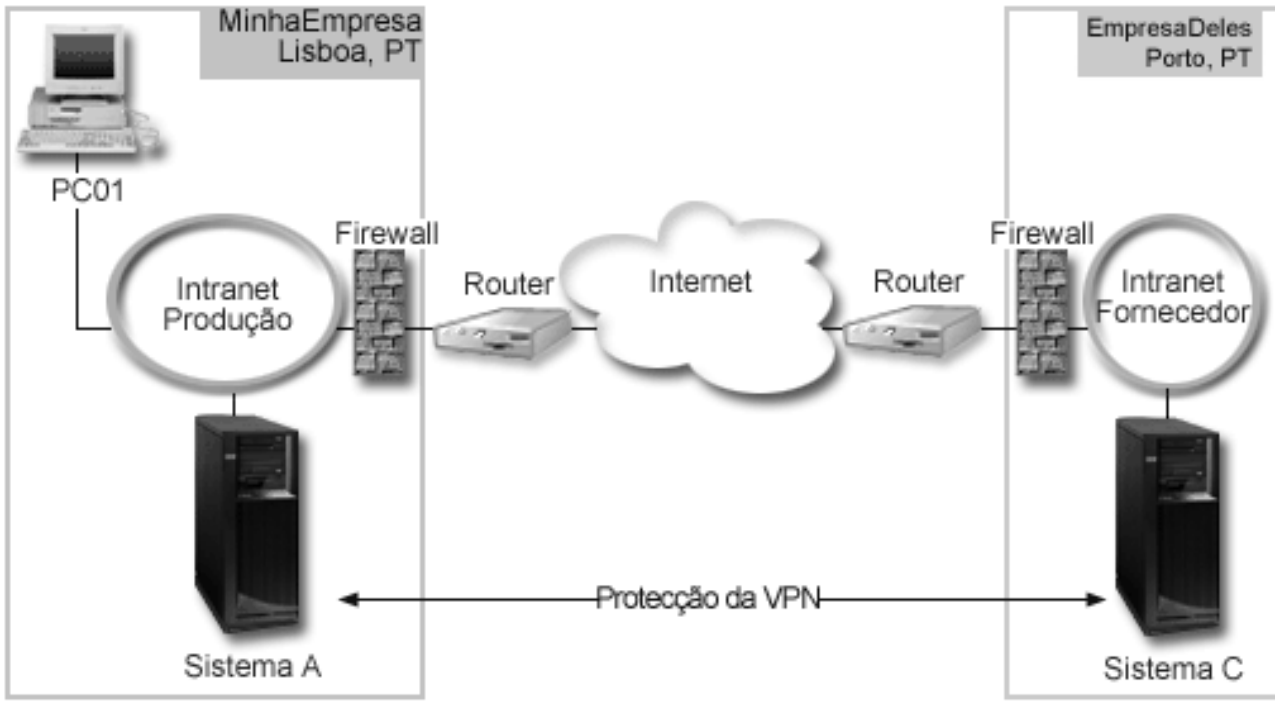
Neste cenário, MinhaEmp pretende estabelecer uma VPN entre um sistema central na respectiva divisão de peças e um sistema central no departamento de produção de um dos parceiros comerciais, a OutraEmp.

Uma vez que as informações partilhadas por estas duas empresas são extremamente confidenciais, têm de ser protegidas à medida que são trocadas pela Internet. Além disso, os dados não podem 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 terminal a terminal, integridade e codificação.

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 OutraEmp.



Rede de Fornecimento da MinhaEmp

- O Sistema A é executado em i5/OS Versão 5 Edição 3 (V5R3), ou posterior.
- O Sistema A tem o endereço IP 10.6.1.1. Este é o terminal da ligação, assim como o terminal de dados. Ou seja, o Sistema A executa negociações IKE, aplica a IPSec a datagramas de IP de chegada e de partida e é a origem e o terminal que circulam na VPN.
- O Sistema A está na sub-rede 10.6.0.0, com a máscara 255.255.0.0
- Só o Sistema A pode iniciar a ligação com o Sistema C.

Rede de Produção da OutraEmp

- O Sistema C é executado em i5/OS Versão 5 Edição 3 (V5R3), ou posterior.
- O Sistema C tem o endereço IP 10.196.8.6. Este é o terminal da ligação, assim como o terminal de dados. Ou seja, o Sistema A executa negociações IKE, aplica a IPSec a datagramas de IP de chegada e de partida e é a origem e o terminal de dados que circulam na VPN.
- O Sistema C está na sub-rede 10.196.8.0 com a máscara 255.255.255.0

Tarefas de configuração

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

Nota: Antes de dar início a estas tarefas, verifique o encaminhamento de TCP/IP para se certificar de que dois sistemas de porta de ligação podem comunicar um com o outro pela Internet. Assim se garante 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.

Conceitos relacionados

Equilíbrio de volumes de trabalho e encaminhamento de TCP/IP

Preencher as folhas de trabalho de planeamento

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

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

Tabela 3. Requisitos do sistema

Lista de verificação de pré-requisitos	**Respostas**
O sistema executa i5/OS V5R3 ou posterior?	Sim
A opção Gestor de Certificados Digitais está instalada?	Sim
O System i Access for Windows está instalado?	Sim
O System i Navigator está instalado?	Sim
O subcomponente de Rede do System i Navigator está instalado?	Sim
O IBM TCP/IP Connectivity Utilities for i5/OS 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 sistema (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 terminais necessários?	Sim
Aplicou as mais recentes correcções temporárias de programas (PTFs)?	Sim
Se o túnel de VPN passa por firewalls ou encaminhadores que implementem filtragem de pacotes de IP, as regras de filtro da firewall ou dos encaminhadores suportam protocolos de 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

Tabela 4. Configuração da VPN

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(a)
Está a utilizar certificados para autenticar a ligação? Em caso negativo, qual é a chave pré-partilhada?	Nada ultra-secreto
Qual é o identificador do servidor de chaves locais?	Endereço de IP: 204.146.18.227
Qual é o identificador do terminal de dados local?	Sub-rede: 10.6.0.0 Máscara: 255.255.0.0
Qual é o identificador do servidor de chaves remotas?	Endereço de IP: 208.222.150.250
Qual é o identificador do terminal 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 na ligação?	Qualquer uma

Tabela 4. Configuração da VPN (continuação)

Necessita destas informações para configurar a VPN	Respostas
De que tipo de segurança e de rendimento de sistema necessita para proteger os seus dados?	equilibrado(a)
A que interfaces é aplicada a ligação?	TRLINE

Configurar a VPN no Sistema A

Siga estes passos para configurar uma ligação VPN no Sistema A.

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

1. No System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Rede Privada Virtual** e, em seguida, seleccione **Nova Ligação** para iniciar o Assistente de ligação.
3. Reveja a página **Bem-vindo(a)** para mais informações sobre quais os objectos que o assistente cria.
4. Faça clique em **Seguinte** para ir para a página **Nome da Ligação**.
5. No campo **Nome**, introduza `MinhaEmpParaOutraEmp`.
6. Opcional: Especifique uma descrição para este grupo de ligações.
7. Faça clique em **Seguinte** para ir para a página **Cenário da Ligação**.
8. Seleccione **Ligar o sistema central a outro sistema central**.
9. Faça clique em **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 em **Seguinte** para ir para a página **Certificado para terminal da Ligação Local**.
12. Seleccione **Sim** para indicar que utilizará certificados para autenticar a ligação. Em seguida, seleccione o certificado que representa o Sistema A.

    Nota: Caso pretenda utilizar um certificado para autenticar o terminal da ligação local, tem de primeiro criar o certificado no Digital Certificate Manager (DCM).
13. Faça clique em **Seguinte** para ir para a página **Identificador do Terminal da Ligação Local**.
14. Seleccione **Endereço IP versão 4** como tipo de identificador. O endereço de IP associado tem de ser 10.6.1.1. Mais uma vez, estas informações são definidas no certificado que criar no DCM.
15. Faça clique em **Seguinte** para ir para a página **Servidor de Chaves Remotas**.
16. Seleccione **Endereço de IP versão 4** no campo **Tipo de identificador**.
17. Introduza `10.196.8.6` no campo **Identificador**.
18. Faça clique em **Seguinte** para ir para a página **Serviços de Dados**.
19. Aceite os valores predefinidos e, em seguida, faça clique em **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 em **Seguinte** para ir para a página **Interfaces Aplicáveis**.
22. Seleccione **TRLINE**.
23. Faça clique em **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 em **Terminar** para concluir a configuração.
25. Quando surgir a caixa de diálogo **Activar Filtro de Políticas**, seleccione **Não, regras de pacotes serão activadas mais tarde** e em seguida clique em **OK**.

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

1. Faça clique em **Por Grupo**, na área de janela da esquerda da interface da VPN; o novo grupo de chaves dinâmicas, MinhaEmpParaOutraEmp, é apresentado na área de janela da da direita. Faça clique com o botão direito do rato na mesma e seleccione **Propriedades**.
2. Siga para a página **Política** e seleccione a opção **Sistema local inicia a ligação**.
3. Faça clique em **OK** para guardar as alterações.

Configurar a VPN no Sistema C

Siga os mesmos passos utilizados para configurar a VPN no Sistema A, alterando os endereços de IP conforme necessário. Utilize as folhas de trabalho de planeamento como guia.

Quando terminar a configuração da porta de ligação VPN do Departamento Financeiro, as suas ligações estarão num estado *a pedido*, pelo que a ligação é iniciada quando forem enviados os datagramas de IP que esta ligação VPN tem de proteger. O passo seguinte é iniciar os servidores da VPN, caso ainda não tenham sido iniciados.

Activar regras de pacotes

O assistente VPN cria automaticamente as regras de pacotes necessárias para que a ligação funcione correctamente. Contudo, tem de activá-las em ambos os sistemas antes de iniciar a configuração da VPN.

Para activar regras de pacotes no Sistema A, siga estes passos:

1. Em System i Navigator, expanda **Sistema A** → **Rede** → **Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Regras de Pacotes** e seleccione **Activar**. Abre-se a caixa de diálogo **Activar Regras de Pacotes**.
3. Seleccione se pretende activar somente 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 aplicar 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 em **OK** na caixa de diálogo para confirmar que pretende verificar e activar as regras na interface ou 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 específicos, 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 Sistema C.

Iniciar uma ligação

Depois de configurar a ligação VPN terá de a iniciar.

Siga estes passos para iniciar a ligação MinhaEmpParaOutraEmp a partir do Sistema A:

1. Em System i Navigator, expanda **Sistema A** → **Rede** → **Políticas de IP**.
2. Se o servidor VPN não se tiver iniciado, faça clique com o botão direito do rato em **Rede Privada Virtual** e seleccione **Iniciar**. Isto inicia o servidor VPN.
3. Expanda **Rede Privada Virtual** → **Ligações Seguras**.
4. Faça clique em **Todas as Ligações** para ver uma lista de ligações na área de janela da direita.
5. Faça clique com o botão direito do rato em **MinhaEmpParaOutraEmp** e seleccione **Iniciar**.
6. No menu **Ver**, seleccione **Actualizar**. Se a ligação for iniciada com êxito, o estado deve mudar de *Inactivo* para *Activo*. A ligação pode levar alguns minutos a iniciar, pelo que deve efectuar actualizações periódicas até o estado mudar para *Activado*.

Testar uma ligação

Depois de concluir a configuração de ambos os sistemas e de iniciar os servidores VPN, deve testar a conectividade para se assegurar de que as sub-redes remotas conseguem comunicar entre elas.

Para testar a ligação, siga estes passos:

1. Em System i Navigator, expanda **Sistema A** → **Rede**.
2. Faça clique com o botão direito do rato em **Configuração de TCP/IP**, seleccione **Utilitários** e depois **Ping**.
3. Na caixa de diálogo **Ping a partir de**, insira `Sistema C` no campo **Ping**.
4. Faça clique em **Efectuar Ping Agora** para verificar a conectividade do Sistema A ao Sistema C.
5. Faça clique em **OK** quando tiver terminado.

Cenário: Proteger um túnel voluntário de L2TP com IPSec

Neste cenário, irá aprender como configurar 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.

Situação

Suponha que a sua empresa possui uma pequena sucursal noutro país. No decorrer de um dia útil normal, a sucursal poderá necessitar de acesso a informações confidenciais num modelo System i dentro 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 túnel voluntário do Layer 2 Tunnel Protocol (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 túnel de L2TP.

Com um túnel voluntário de L2TP, a sucursal remota estabelece um túnel directamente ao servidor de rede L2TP (LNS) da rede da empresa. A funcionalidade do concentrador de acesso de L2TP (LAC) reside no cliente. O túnel 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 sobre conceitos de L2TP, consulte o tópico Layer 2 Tunnel Protocol (L2TP).

Importante: Este cenário mostra as portas de ligação de segurança, 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. Considere os riscos de segurança envolvidos sempre que ligar à Internet.

Objectivos

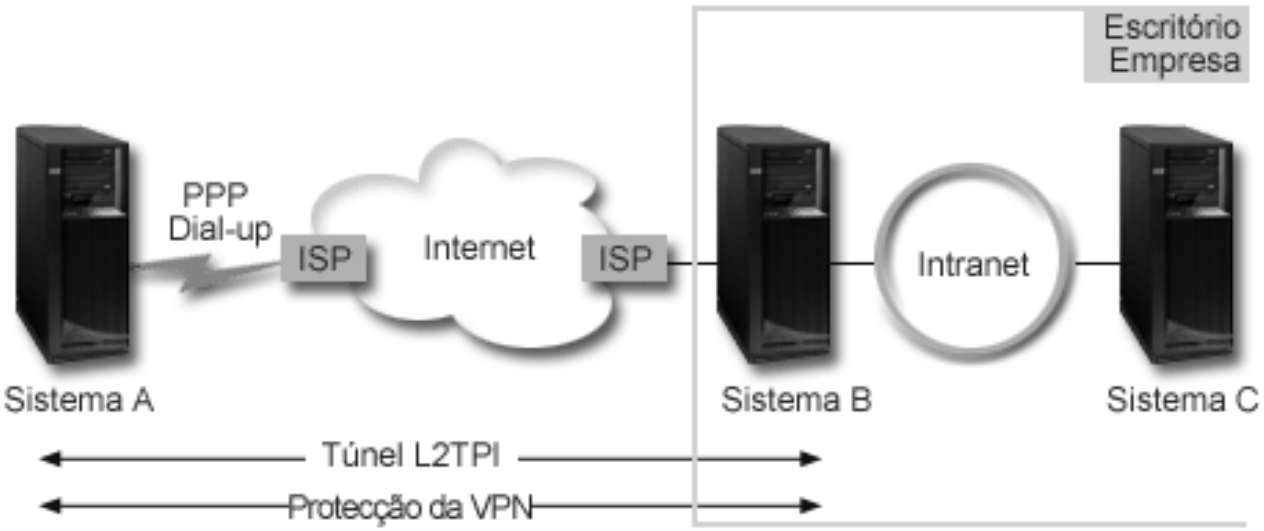
Neste cenário, um sistema da sucursal estabelece ligação à rede da sede através de um sistema de porta de ligação com um túnel de L2TP protegido pela VPN.

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 de sistema central na rede da sede.

Detalhes

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



Sistema A

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

Sistema B

- Deve ter acesso a aplicações TCP/IP no Sistema A.
- A sub-rede é 10.6.0.0 com a máscara 255.255.0.0. Esta sub-rede representa o terminal de dados do túnel de VPN do lado da empresa.
- Estabelece ligação à Internet através do endereço de IP 205.13.237.6. Este é o terminal da ligação. Ou seja, o Sistema C executa a gestão de chaves e aplica o IPSec a datagramas de IP de chegada e de partida. O Sistema B estabelece ligação à respectiva sub-rede com o endereço de IP 10.6.11.1.

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

Tarefas de configuração

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

Conceitos relacionados

"Layer 2 Tunnel Protocol" na página 8
As ligações Layer 2 Tunneling Protocol (L2TP), também chamadas linhas virtuais, proporcionam um acesso pouco dispendioso a utilizadores remotos, ao permitir ao sistema de rede de uma empresa gerir os endereços de IP atribuídos aos respectivos utilizadores remotos. Além disso, as ligações do L2TP fornecem acesso protegido ao sistema ou à rede quando as utiliza em conjunto com o IP Security (IPSec).

Informações relacionadas

AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00

Configurar a VPN no Sistema A

Siga estes passos para configurar uma ligação VPN no Sistema A.

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

1. **Configure a política do Internet Key Exchange**
   a. No System i Navigator, expanda Sistema A → **Rede** → **Políticas de IP** → **Rede Privada Virtual** → **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 locais e, em seguida, introduza o identificador de chaves no campo **Identificador**. Por exemplo, `iddachave`. Lembre-se que o servidor de chaves locais tem um endereço de IP atribuído dinamicamente, o qual não é possível conhecer antecipadamente. O Sistema B utiliza este identificador para identificar o Sistema A quando este inicia uma ligação.
   g. Na página **Transformações**, faça clique em **Adicionar** para adicionar as transformações propostas pelo Sistema A ao Sistema 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 **Transformação 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 predefinidos para o grupo Diffie-Hellman Expirar Chaves do IKE.
   i. Faça clique em **OK** para regressar à página **Transformações**.
   j. Seleccione **negociação em modo agressivo IKE (sem protecção de identidade).**

      Nota: Se utilizar as chaves pré-partilhadas e um modo de negociação agressivo junto com a sua configuração, seleccione palavras-passe obscuras que sejam difíceis de decifrar em ataques que fazem pesquisas no dicionário. Também se recomenda que mude periodicamente as suas palavras-passe.
   k. Faça clique em **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, `l2tputilizadorremoto`
   c. Siga para a página **Propostas**. Uma proposta é um conjunto de protocolos que os servidores de chaves iniciadores e de resposta utilizam para estabelecer uma ligação dinâmica entre dois terminais. É possível utilizar uma única política de dados em vários objectos da ligação. No entanto, nem todos os servidores de chaves da VPN remotos têm, necessariamente, as mesmas propriedades de política de dados. Por isso, é possível adicionar várias propostas a uma política de dados. Ao estabelecer uma ligação VPN a um servidor de chaves remotas, tem de existir, pelo menos, uma proposta correspondente na política de dados do iniciador e do programa de resposta.
   d. Faça clique em **Adicionar** para adicionar uma transformação da política de dados.
   e. Seleccione **Transporte** para o modo de encapsulamento.
   f. Faça clique em **OK** para regressar à página **Transformações**.
   g. Especifique um valor de expiração da chaves.
   h. Faça clique em **OK** para guardar a nova política de dados.

3. **Configurar o grupo de chaves dinâmicas**
   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, `l2tpparaempresa`.
   d. Seleccione **Protege um túnel de L2TP iniciado localmente**.
   e. Para a função do sistema, seleccione **Ambos os sistemas são sistemas centrais**.
   f. Siga para a página **Política**. Seleccione a política de dados criada no passo **Configurar a política de dados**, `l2tputilizadorremoto`, na lista pendente **Política de dados**.
   g. Seleccione **Sistema local inicia ligação** para indicar que só o Sistema A pode iniciar ligações com o Sistema B.
   h. Siga para a página **Ligações**. Seleccione **Gerar a seguinte regra de filtro de políticas para este grupo**. Faça clique em **Editar** para definir os parâmetros do filtro de políticas.
   i. Na página **Filtro de Políticas - Endereços Locais**, seleccione **Identificador de Chaves** para o tipo de identificador.
   j. Para o identificador, seleccione o identificador de chaves, `iddachave`, definido na política do IKE.
   k. Avance para a página **Filtro 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. Siga para a página **Filtro de Políticas - Serviços**. Introduza `1701` nos campos **Porta Local** e **Porta Remota**. A porta 1701 é a porta para L2TP conhecida.
   n. Seleccione **UDP** na lista pendente **Protocolo**.
   o. Faça clique em **OK** para regressar à página **Ligações**.
   p. Siga 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 em **OK** para criar o grupo de chaves dinâmicas l2tpparaempresa.
4. **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 Sistema A.
   b. Faça clique com o botão direito do rato sobre **l2tpparaempresa** 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. Desmarque **Iniciar a pedido**.
   g. Siga para a página **Endereços Locais**. Seleccione **Identificador da Chave** para o tipo de identificador e, em seguida, seleccione `iddachave`, na lista pendente **Identificador**.
   h. Siga 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. Siga para a página **Serviços**. Introduza `1701` nos campos **Porta Local** e **Porta Remota**. A porta 1701 é a porta para L2TP conhecida.
   k. Seleccione **UDP** na lista pendente **Protocolo**.
   l. Faça clique em **OK** para criar a ligação de chaves dinâmicas.

Tarefas relacionadas

"Configurar a VPN no Sistema B" na página 29
Para configurar a VPN no Sistema B, siga os mesmos passos utilizados para configurar no Sistema A, alterando endereços de IP e identificadores conforme a necessidade.

Configurar um perfil de ligação PPP e uma linha virtual no Sistema A

Agora que a ligação VPN está configurada no Sistema A, terá de criar o perfil PPP para o Sistema A. O perfil PPP não dispõe de nenhuma linha física associada; em contrapartida, utiliza uma linha virtual. Tal acontece porque o tráfego PPP é direccionado através do túnel L2TP, enquanto a VPN protege o túnel L2TP.

Siga estes passos para criar um perfil de ligação PPP para o Sistema A:

1. No System i Navigator, expanda Sistema 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 a pedido (túnel voluntário)** na lista pendente **Modo de operação**.
6. Faça clique em **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 `paraEmpresa`. O nome especificado tem de ter 10 caracteres ou menos.
8. Opcional: Especifique uma descrição para o perfil.
9. Avance para a página **Ligação**.
10. No campo **Nome da linha virtual**, seleccione **paraEmpresa** na lista pendente. Lembre-se que esta linha não tem nenhuma 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. Surge a caixa de diálogo **Propriedades da Linha L2TP**.
11. Na página **Geral**, introduza uma descrição da linha virtual.
12. Siga para a página **Autenticação**.
13. No campo **Nome do sistema central local**, introduza o nome do sistema central do servidor de chaves locais, `SistemaA`.
14. Faça clique em **OK** para guardar a descrição da nova linha virtual e regresse à página **Ligação**.
15. Introduza o endereço do terminal do túnel remoto, `205.13.237.6`, no campo **Endereço do terminal do túnel remoto**.
16. Seleccione **Requer Protecção IPSec** e seleccione o grupo de chaves dinâmicas criado no passo anterior ("Configurar a VPN no Sistema A" na página 26), `l2tpparaempresa` na lista pendente **Nome do grupo de ligações**.
17. Avance para a página **Definições de TCP/IP**.
18. Na secção **Endereço de IP local**, seleccione **Atribuído pelo 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 em **Encaminhamentos**. Se não houver informações de encaminhamento para o perfil PPP, o Sistema A só é capaz de atingir o terminal do túnel remoto, mas nenhum outro sistema da sub-rede 10.6.0.0.
21. Faça clique em **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 túnel de L2TP.
23. Faça clique em **OK** para adicionar o percurso estático.
24. Faça clique em **OK** para fechar a caixa de diálogo Encaminhamento.

25. Siga 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)**. Na secção de identificação do sistema local, seleccione **Permitir que o sistema remoto verifique a identidade deste sistema**.
28. Introduza o nome do utilizador, `SistemaA` e uma palavra-passe.
29. Faça clique em **OK** para guardar o perfil PPP.

Aplicar o grupo de chaves dinâmicas l2tpparaempresa ao perfil PPP paraEmpresa

Após a configuração do perfil de ligação PPP, é necessário voltar ao grupo de chaves dinâmicas `l2tpparaempresa` criado e associá-lo ao perfil PPP.

Para associar o grupo de chaves dinâmicas ao perfil PPP, siga estes passos:

1. Em System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP** → **Rede Privada Virtual** → **Ligações Seguras** → **Por Grupo**.
2. Faça clique com o botão direito do rato sobre o grupo de chaves dinâmicas `l2tpparaempresa` e seleccione **Propriedades**.
3. Avance para a página **Interfaces** e seleccione **Aplicar este grupo** para o perfil PPP criado na secção "Configurar um perfil de ligação PPP e uma linha virtual no Sistema A" na página 28, `paraEmpresa`.
4. Faça clique em **OK** para aplicar `v` ao perfil PPP `paraEmpresa`.

Configurar a VPN no Sistema B

Para configurar a VPN no Sistema B, siga os mesmos passos utilizados para configurar no Sistema A, alterando endereços de IP e identificadores conforme a necessidade.

Considere os seguintes aspectos antes de começar:

- Identifique o servidor de chaves remotas pelo identificador de chaves especificado para o servidor de chaves locais no Sistema A. Por exemplo, `iddachave`.
- Utilize *exactamente* a mesma chave pré-partilhada.
- Assegure-se de que as transformações correspondem às configuradas no Sistema A ou não terá ligações satisfatórias.
- 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 a pedido.

Tarefas relacionadas

"Configurar a VPN no Sistema A" na página 26
Siga estes passos para configurar uma ligação VPN no Sistema A.

Configurar um perfil de ligação PPP e uma linha virtual no Sistema B

Agora que a ligação VPN está configurada no Sistema B, terá de criar o perfil PPP para o Sistema B. O perfil PPP não dispõe de nenhuma linha física associada; em contrapartida, utiliza uma linha virtual. Tal acontece porque o tráfego PPP é direccionado através do túnel L2TP, enquanto a VPN protege o túnel L2TP.

Siga estes passos para criar um perfil de ligação PPP para o Sistema B:

1. No System i Navigator, expanda Sistema B → **Rede** → **Serviços de Acesso Remoto**.
2. Faça clique com o botão direito do rato sobre **Perfis de Ligação do Programa de Resposta** 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 em **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 tem de ter 10 caracteres ou menos.
8. Opcional: Especifique uma descrição para o perfil
9. Avance para a página **Ligação**.
10. Seleccione o endereço de IP do terminal do túnel local 205.13.237.6.
11. No campo **Nome da linha virtual**, seleccione **tobranch** na lista pendente. Lembre-se que esta linha não tem nenhuma 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. Surge a caixa de diálogo **Propriedades da Linha L2TP**.
12. Na página **Geral**, introduza uma descrição da linha virtual.
13. Avance para a página **Autenticação**
14. No campo **Nome do sistema central local**, introduza o nome do sistema central do servidor de chaves locais, `SistemaB`.
15. Faça clique em **OK** para guardar a descrição da nova linha virtual e regresse à página **Ligação**.
16. Avance para a página **Definições de 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. Siga 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 `SistemaB` e uma palavra-passe.
24. Faça clique em **OK** para guardar o perfil PPP.

Activar regras de pacotes

O assistente 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 activar regras de pacotes no Sistema A, siga estes passos:

1. Em System i Navigator, expanda **Sistema A → Rede → Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Regras de Pacotes** e seleccione **Activar**. Abre-se a caixa de diálogo **Activar Regras de Pacotes**.
3. Escolha se pretende activar somente 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 aplicar 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 em **OK** na caixa de diálogo para confirmar que pretende verificar e activar as regras na interface ou 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 específicos, 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 Sistema B.

Cenário: VPN com Firewall de Fácil Utilização

Neste cenário, uma grande seguradora pretende estabelecer uma VPN entre uma porta de ligação em Lisboa e um sistema central no Porto, sendo que ambas as redes estão protegidas por uma firewall.

Situação

Suponha que é uma grande seguradora sediada no Porto e que acabou de abrir uma nova sucursal em Lisboa. A sucursal de Lisboa tem de aceder à base de dados dos clientes na sede no Porto. Quer garantir que as informações que são transferidas estão protegidas uma vez que a base de dados contém informações confidenciais sobre os seus clientes, tais como nomes, endereços e números de telefone. Decide ligar ambos os escritórios através da Internet usando uma Rede Privada virtual (VPN). Ambos os escritórios encontram-se protegidos por uma firewall e usam a Conversão de Endereços de Rede (network address translation - NAT) para ocultar os endereços de IP privados não registados atrás de um conjunto de endereços de IP registados. No entanto, as ligações de VPN têm algumas incompatibilidades bem conhecidas com a NAT. Uma ligação VPN rejeita pacotes enviados por um dispositivo NAT, pois a NAT altera o endereço de IP no pacote, invalidando, desse modo, o pacote. No entanto, pode usar uma ligação VPN com NAT, caso implemente encapsulamento de UDP.

Neste cenário, o endereço de IP privado da rede de Lisboa é colocado num novo cabeçalho de IP e é convertido quando atravessa a Firewall C (observe a imagem seguinte). Seguidamente, quando o pacote atinge a Firewall D, converte o endereço de IP de destino no endereço de IP do Sistema E e, assim sendo, o pacote será remetido para o Sistema E. Finalmente, quando o pacote chega ao Sistema E, decompõe o cabeçalho de UDP, deixando o pacote IPSec original, que irá passar agora por todas as validações e permitir uma ligação VPN segura.

Objectivos

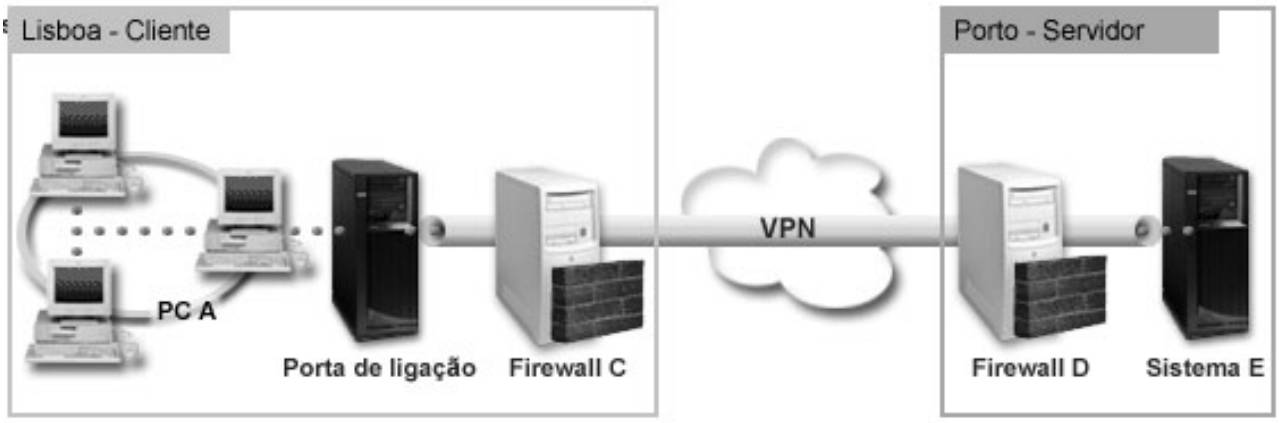
Neste cenário, uma grande seguradora pretende estabelecer uma VPN entre uma porta de ligação em Lisboa (Cliente) e um sistema central no Porto (Servidor), sendo que ambas as redes estão protegidas por uma firewall.

Os objectivos deste cenário são os seguintes:

- A sucursal de Lisboa inicia sempre a ligação ao sistema central do Porto.
- A VPN tem de proteger todo o tráfego de dados entre a porta de ligação de Lisboa e o sistema central do Porto.
- Permitir que todos os utilizadores da porta de ligação de Lisboa acedam a uma base de dados System i localizada na rede do Porto, através de uma ligação de VPN.

Detalhes

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



Rede de Lisboa - Cliente

- A Porta de Ligação B é executada em i5/OS Versão 5 Edição 4 (V5R4), ou posterior.
- A Porta de Ligação B estabelece ligação à Internet pelo endereço de IP 214.72.189.35 e é o terminal de ligação do túnel da VPN. A Porta de Ligação B executa negociações de IKE e aplica o encapsulamento UDP a datagramas de IP de partida.
- A Porta de Ligação B e o PC A encontram-se na sub-rede 10.8.11.0 com a máscara 255.255.255.0
- O PC A é a origem e o destino para dados que circulam pela ligação de VPN, sendo, por isso, o terminal de dados do túnel da VPN.
- Só a Porta de Ligação B pode iniciar a ligação com o Sistema E.
- A firewall C tem uma regra NAT Masq com o endereço de IP público 129.42.105.17, que oculta o endereço de IP da Porta de Ligação B

Rede do Porto - Servidor

- O Sistema E é executado em i5/OS Versão 5 Edição 4 (V5R4), ou posterior.
- O Sistema E tem o endereço de IP 56.172.1.1.
- O Sistema E é o programa de resposta para este cenário.
- A Firewall D tem o endereço de IP 146.210.18.51.
- A Firewall D tem uma regra NAT Estática que correlaciona o IP público (146.210.18.15) com o o IP privado do Sistema E (56.172.1.1). Assim sendo, da perspectiva dos clientes, o endereço de IP do Sistema E é o endereço de IP público (146.210.18.51) da Firewall D.

Tarefas de configuração

Conceitos relacionados

"Gestão de chaves" na página 6
Uma VPN dinâmica proporciona segurança adicional às comunicações, com o protocolo Internet Key Exchange (IKE) para a gestão de chaves. O IKE permite aos servidores VPN em cada extremo da ligação negociar novas chaves em intervalos específicos.

"IPSec compatível com NAT com protocolo UDP" na página 10
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.

Preencher as folhas de trabalho de planeamento

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

Nota: Existem folhas de trabalho em separado para a Porta de Ligação B e o Sistema E.

Tabela 5. Requisitos do sistema

Lista de verificação de pré-requisitos	**Respostas**
O sistema operativo está na i5/OS V5R4 ou posterior?	Sim
A opção Gestor de Certificados Digitais está instalada?	Sim
O System i Access for Windows está instalado?	Sim
O System i Navigator está instalado?	Sim
O subcomponente de Rede do System i Navigator está instalado?	Sim
O IBM TCP/IP Connectivity Utilities for i5/OS 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 sistema (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 terminais necessários?	Sim
Aplicou as mais recentes correcções temporárias de programas (PTFs)?	Sim
Se o túnel de VPN passa por firewalls ou encaminhadores que implementem filtragem de pacotes de IP, as regras de filtro da firewall ou dos encaminhadores suportam protocolos de AH e ESP?	Sim
As firewalls ou os encaminhadores estão configurados para permitir o tráfego através da porta 4500 para negociações de chaves. Normalmente, os parceiros da VPN executam negociações IKE através da porta 500 UDP, quando a IKE detecta que são enviados pacotes NAT através da porta 4500.	Sim
As firewalls estão configuradas para permitir o reencaminhamento de IP?	Sim

Tabela 6. Configuração da Porta de Ligação B

Necessita destas informações para configurar a VPN para a Porta de Ligação B	**Respostas**
Que tipo de ligação está a criar?	porta-de-ligação-para-outro sistema central
Que nome irá dar ao grupo de chaves dinâmicas?	CHIgw2MINhost
De que tipo de segurança e de rendimento de sistema necessita para proteger as suas chaves?	equilibrado
Está a utilizar certificados para autenticar a ligação? Em caso negativo, qual é a chave pré-partilhada?	Não: ultra-secreto
Qual é o identificador do servidor de chaves locais?	Endereço de IP: 214.72.189.35
Qual é o identificador do terminal de dados local?	Sub-rede: 10.8.11.0 Máscara: 255.255.255.0
Qual é o identificador do servidor de chaves remotas?	Endereço de IP: 146.210.18.51
Qual é o identificador do terminal de dados remoto?	Endereço de IP: 146.210.18.51
Quais as portas e os protocolos que pretende que tenham permissão para circular na ligação?	Quaisquer

Tabela 6. Configuração da Porta de Ligação B (continuação)

Necessita destas informações para configurar a VPN para a Porta de Ligação B	**Respostas**
De que tipo de segurança e de rendimento de sistema necessita para proteger os seus dados?	equilibrado(a)
A que interfaces é aplicada a ligação?	TRLINE

Tabela 7. Configuração do Sistema E

Necessita destas informações para configurar a VPN para o Sistema E	**Respostas**
Que tipo de ligação está a criar?	sistema central a outra porta de ligação
Que nome irá dar ao grupo de chaves dinâmicas?	CHIgw2MINhost
De que tipo de segurança e de rendimento de sistema necessita para proteger as suas chaves?	mais elevado(a)
Está a utilizar certificados para autenticar a ligação? Em caso negativo, qual é a chave pré-partilhada?	Não : ultra-secreto
Qual é o identificador do servidor de chaves locais?	Endereço de IP: 56.172.1.1
Qual é o identificador do servidor de chaves remotas? **Nota:** Se o endereço de IP da Firewall C for desconhecido, pode usar *ANYIP como identificador para o servidor de chaves remotas.	Endereço de IP: 129.42.105.17
Qual é o identificador do terminal de dados remoto?	Sub-rede: 10.8.11.0 Máscara: 255.255.255.0
Quais as portas e os protocolos que pretende que tenham permissão para circular na ligação?	Quaisquer
De que tipo de segurança e de rendimento de sistema necessita para proteger os seus dados?	mais elevado(a)
A que interfaces é aplicada a ligação?	TRLINE

Referências relacionadas

Consultor de planeamento da VPN

Configurar a VPN na Porta de Ligação B

Siga estes passos para configurar uma ligação VPN na Porta de Ligação B.

Utilize as informações das folhas de trabalho de planeamento para configurar a VPN na Porta de Ligação B do seguinte modo:

1. No System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Rede Privada Virtual** e, em seguida, seleccione **Nova Ligação** iniciar o assistente de Ligação.
3. Reveja a página **Bem-vindo(a)** para mais informações sobre quais os objectos que o assistente cria.
4. Faça clique em **Seguinte** para ir para a página **Nome da Ligação**.
5. No campo **Nome**, insira `CHIgw2MINhost`.
6. Opcional: Especifique uma descrição para este grupo de ligações.
7. Faça clique em **Seguinte** para ir para a página **Cenário da Ligação**.
8. Seleccione **Ligar a porta de ligação a outro sistema central** .
9. Faça clique em **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**.

Nota: Se surgir uma mensagem de erro com a indicação: ″Não foi possível processar o pedido de certificado″, pode ignorá-la pois não se encontra a usar certificados para a troca de chaves.

11. Opcional: Se tiver certificados instalados irá ver a página **Certificado para Terminal da Ligação Local**. Seleccione Não para indicar que irá utilizar certificados para autenticar a ligação.
12. Faça clique em **Seguinte** para ir para a página **Servidor de Chaves Locais**.
13. Seleccione **IP versão 4** como o campo **Tipo de Identificador**.
14. Seleccione `214.72.189.35` no campo **Endereço de IP**.
15. Faça clique em **Seguinte** para ir para a página **Servidor de Chaves Remotas**.
16. Seleccione **Endereço de IP versão 4** no campo de **Tipo de Identificador**.
17. Insira `146.210.18.51` no campo **Identificador**.

    Nota: A Porta de Ligação B está a iniciar uma ligação a uma NAT Estática (Static NAT); tem de especificar troca de chaves em modo principal para inserir um único IP para a chave remota. A troca de chaves em modo principal é seleccionada por predefinição ao criar uma ligação com o Assistente de Ligações VPN. Se for usado o modo agressivo nesta situação, tem de ser inserido um tipo que não seja IPV4 de identificador remoto para a chave remota.
18. Insira `ultra-secreto` no campo **Chave pré-partilhada**
19. Faça clique em **Seguinte** para ir para a página **Terminal de Dados Local**.
20. Seleccione **Sub-rede de IP versão 4** no campo **Tipo de identificador**.
21. Insira `10.8.0.0` no campo **Identificador**.
22. Introduza `255.255.255.0` no campo **Máscara da sub-rede**.
23. Faça clique em **Seguinte** para ir para a página **Serviços de Dados**.
24. Aceite os valores predefinidos e, em seguida, faça clique em **Seguinte** para seguir para a página de Política de Dados.
25. Seleccione **Criar uma nova política** e, em seguida, seleccione **Segurança e rendimento equilibrados**.
26. Faça clique em **Seguinte** para ir para a página **Interfaces Aplicáveis**.
27. Seleccione **TRLINE** na tabela de Linhas.
28. Faça clique em **Seguinte** para ir para a página **Resumo**.
29. Reveja os objectos que o assistente irá criar para se certificar de que estão correctos.
30. Faça clique em **Terminar** para concluir a configuração.
31. Quando surgir a caixa de diálogo **Activar Filtros de Políticas**, seleccione **Sim**, activar os filtros de políticas gerados e, seguidamente, seleccione **Permitir todo o tráfego restante**.
32. Faça clique em **OK** para concluir a configuração.

Configurar a VPN no Sistema E

Siga estes passos para configurar uma ligação VPN no Sistema E.

Utilize as informações das folhas de trabalho de planeamento para configurar a VPN no Sistema E do seguinte modo:

1. No System i Navigator, expanda **sistema → Rede → Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Rede Privada Virtual** e, em seguida, seleccione **Nova Ligação** iniciar o assistente de Ligação.
3. Reveja a página **Bem-vindo(a)** para mais informações sobre quais os objectos que o assistente cria.
4. Faça clique em **Seguinte** para ir para a página **Nome da Ligação**.
5. No campo **Nome**, insira `CHIgw2MINhost`.
6. Opcional: Especifique uma descrição para este grupo de ligações.
7. Faça clique em **Seguinte** para ir para a página **Cenário da Ligação**.
8. Seleccione **Ligar o sistema central a outra porta de ligação** .

9. Faça clique em **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**.

    Nota: Se surgir uma mensagem de erro com a indicação: ″Não foi possível processar o pedido de certificado″, pode ignorá-la pois não se encontra a usar certificados para a troca de chaves.
11. Opcional: Se tiver certificados instalados irá ver a página **Certificado para Terminal da Ligação Local**. Seleccione Não para indicar que irá utilizar certificados para autenticar a ligação.
12. Faça clique em **Seguinte** para seguir para a página **Servidor de Chaves Locais**.
13. Seleccione **Endereço de IP versão 4** como o campo de **Tipo de Identificador**.
14. Seleccione `56.172.1.1` no campo **Endereço de IP**.
15. Faça clique em **Seguinte** para ir para a página **Servidor de Chaves Remotas**.
16. Seleccione **Endereço de IP versão 4** no campo de **Tipo de Identificador**.
17. Introduza `129.42.105.17` no campo **Identificador**.

    Nota: Se o endereço de IP da Firewall C for desconhecido, pode usar *ANYIP como identificador para o servidor de chaves remotas.
18. Insira `ultra-secreto` no campo **Chave pré-partilhada**
19. Faça clique em **Seguinte** para ir para a página **Terminal de Dados Remoto**.
20. Seleccione **Sub-rede de IP versão 4** no campo **Tipo de identificador**.
21. Insira `10.8.11.0` no campo **Identificador**.
22. Introduza `255.255.255.0` no campo **Máscara da sub-rede**.
23. Faça clique em **Seguinte** para ir para a página **Serviços de Dados**.
24. Aceite os valores predefinidos e, em seguida, faça clique em **Seguinte** para seguir para a página de Política de Dados.
25. Seleccione **Criar uma nova política** e, em seguida, seleccione **Segurança e rendimento equilibrados**.
26. Faça clique em **Seguinte** para ir para a página **Interfaces Aplicáveis**.
27. Seleccione **TRLINE** na tabela de Linhas.
28. Faça clique em **Seguinte** para ir para a página **Resumo**.
29. Reveja os objectos que o assistente irá criar para se certificar de que estão correctos.
30. Faça clique em **Terminar** para concluir a configuração.
31. Quando surgir a caixa de diálogo **Activar Filtros de Políticas**, seleccione **Sim**, activar os filtros de políticas gerados e, seguidamente, seleccione **Permitir todo o tráfego restante**.
32. Faça clique em **OK** para concluir a configuração.

Iniciar Ligação

Depois de configurar a ligação VPN no Sistemas E terá de a iniciar.

Siga estes passos para confirmar se a ligação CHIgw2MINhost no Sistema E está activa:

1. Em System i Navigator, expanda **Sistema E → Rede → Ligações Seguras → Todas as Ligações**.
2. Consulte **CHIgw2MINhost** e verifique se o campo **Estado** está *Inactivo* ou *A Pedido*.

Siga estes passos para iniciar a ligação de CHIgw2MINhost a partir da Porta de Ligação B:

1. Em System i Navigator, expanda **Porta de Ligação B → Rede → Políticas de IP**.
2. Se o servidor VPN não se tiver iniciado, faça clique com o botão direito do rato em **Rede Privada Virtual** e seleccione **Iniciar**.
3. Expanda **Rede Privada Virtual → Ligações Seguras**.
4. Faça clique em **Todas as Ligações** para visualizar uma lista de ligações na área de janela da direita.
5. Faça clique com o botão direito do rato sobre **CHIgw2MINhost** e seleccione **Iniciar**.

6. No menu **Ver**, seleccione **Actualizar**. Se a ligação for iniciada com êxito, o campo **Estado** deve mudar de *A iniciar* ou de *A Pedido* para *Activado*. A ligação pode levar alguns minutos a iniciar, pelo que deve efectuar actualizações periódicas até o estado mudar para *Activado*.

Testar a ligação

Depois de concluir a configuração da Porta de Ligação B e do Sistema E, e de iniciar os servidores VPN, deve testar a conectividade para se assegurar de que ambos os sistemas conseguem comunicar entre si.

Para testar as ligações, siga estes passos:

1. Localize um sistema na rede PC A e abra uma sessão de Telnet.
2. Especifique o endereço de IP público para o Sistema E, o qual é 146.210.18.51.
3. Especifique as informações de início de sessão que sejam necessárias. Se conseguir ver o ecrã de início de sessão, a ligação está a funcionar.

Cenário: ligação VPN a utilizadores remotos

O administrador terá de configurar uma ligação VPN a utilizadores remotos para activar ligações remotas.

As tarefas seguintes mostram como o administrador configura uma ligação VPN a utilizadores remotos.

Preencher folhas de trabalho de planeamento para ligação VPN da sucursal às vendas remotas

O administrador da sucursal utiliza o consultor de planeamento VPN para criar folhas de trabalho de planeamento dinâmicas e ajudar a configurar a VPN nos sistemas e estações de trabalho remotas.

O consultor de planeamento VPN é uma ferramenta interactiva que faz perguntas específicas sobre as necessidades de VPN em questão. Com base nas respostas dadas, o consultor gera uma folha de trabalho de planeamento personalizada ao ambiente e que se pode usar quando se configurar a ligação VPN. Esta folha de trabalho pode depois ser utilizada para configurar uma VPN no sistema. Cada qual das folhas de trabalho seguintes é gerada com o consultor de planeamento VPN e utilizada para configurar uma VPN, com o assistente Nova Ligação VPN em System i Navigator.

Tabela 8. Folha de trabalho de planeamento para ligação VPN entre a sucursal e as vendas remotas

O que pergunta o assistente VPN	**O que recomenda o consultor VPN**
Que nome pretende dar a este grupo de ligações?	SalestoRemote
Que tipo de grupo de ligações pretende criar?	Seleccione **Ligar o sistema central a outro sistema central**
Que política Internet Key Exchange pretende utilizar para proteger a chave?	Seleccione **Criar nova política** e depois **Segurança mais elevada, rendimento inferior**.
Está a utilizar certificados?	Seleccione **Não**

Tabela 8. Folha de trabalho de planeamento para ligação VPN entre a sucursal e as vendas remotas (continuação)

O que pergunta o assistente VPN	O que recomenda o consultor VPN
Introduza o identificador para representar o servidor de chaves locais para esta ligação.	Tipo de identificador: **Endereço IP versão 4**, endereço IP:**192.168.1.2**. Para endereço IPv6, tipo de identificador: **Endereço IP versão 6**, endereço IP:**2001:DB8::2** **Nota:** Os endereços IP utilizados neste cenário são meramente exemplificativos. Não reflectem nenhum esquema de endereços IP e não devem ser usados em nenhuma configuração verdadeira. Deverá utilizar os seus endereços de IP quando realizar tais tarefas.
Qual é o identificador do servidor de chaves a que pretende ligar?	Tipo de identificador: **Qualquer endereço de IP**, **Chave pré-partilhada**: chaveempresa. **Nota:** A chave pré-partilhada é uma cadeia de texto com 32 caracteres que a i5/OS VPN utiliza para autenticar a ligação e estabelecer as chaves que protegem os dados. Regra geral, deverá tratar uma chave pré-partilhada da mesma forma que uma palavra-passe.
Quais são as portas e os protocolos dos dados que esta ligação irá proteger?	**Porta Local**: 1701, **Porta Remota**: Qualquer porta, **Protocolo**: UDP
Que política de dados pretende utilizar para proteger os dados?	Seleccione **Criar nova política** e depois **Segurança mais elevada, rendimento inferior**.
Verifique as interfaces no sistema local a que esta ligação se irá aplicar.	ETHLINE (sucursal)

Configurar o perfil terminador L2TP para Sistema A

Se quiser configurar as ligações remotas a estações de trabalho remotas, terá de configurar o Sistema A para aceitar chegada de ligações desses clientes.

Para configurar um perfil terminador L2TP (Layer Two Tunneling Protocol) para o Sistema A, siga estes passos:

1. Em System i Navigator, expanda ***Sistema A*** → **Rede** → **Serviços de Acesso Remoto**.
2. Clique com o botão direito do rato em **Perfis de Ligação Destinatários** para definir o Sistema A como servidor que permite chegada de ligações oriundas de utilizadores remotos, e seleccione **Novo Perfil**.
3. Seleccione as seguintes opções na página Configuração:
   - **Tipo de protocolo:** PPP
   - **Tipo de ligação:** L2TP (linha virtual)

Nota: O campo **Modo operativo** deve apresentar automaticamente **Terminador (servidor de rede)**.

- **Tipo de serviço de linha:** Linha única

4. Faça clique em **OK**. Irá iniciar a página Propriedades do Novo Perfil Ponto a Ponto.
5. No separador **Geral**, preencha os seguintes campos:
   - **Nome**: EMPRESAL2TP
   - Seleccione **Iniciar perfil com TCP** se quiser que o perfil se inicie automaticamente com TCP.
6. No separador **Ligação**, seleccione **192.168.1.2** (**2001:DB8::2** em IPv6) para o **Endereço IP terminal do túnel local**.

   Importante: Os endereços IP utilizados neste cenário são meramente exemplificativos. Não reflectem nenhum esquema de endereços IP e não devem ser usados em nenhuma configuração verdadeira. Utilize os seus endereços de IP quando realizar tais tarefas.
7. Seleccione **EMPRESAL2TP** como **Nome da linha virtual**. Irá iniciar a página Propriedades do Novo L2TP.
8. Na página Autenticação, introduza `sistemaa` como nome de sistema central. Faça clique em **OK**. Voltará à página Ligação.
9. Na página Ligação, seleccione as seguintes opções e introduza `25` como **Número máximo de ligações**.
   a. Clique no separador **Autenticação** e seleccione **Pedir a este sistema que verifique a identidade do sistema remoto**.
   b. Seleccione **Autenticar localmente com lista de validação**.
   c. Introduza `QL2TP` no campo **Nome da lista de validação** e clique em **Novo**.
10. Na página Lista de Validação, seleccione **Adicionar**.
11. Adicionar nomes de utilizador e palavra-passe para cada funcionário remoto. Faça clique em **OK**.
12. Na página Confirmação da Palavra-passe, reintroduza a palavra-passe para cada funcionário remoto. Faça clique em **OK**.
13. Na página Definição de TCP/IP, seleccione 10.1.1.1 (2001:DA8::1 em IPv6) para **Endereço IP Local**.
14. No campo **Método de atribuição de endereço IP**, seleccione **Conjunto de Endereços**.
15. No campo **Endereço IP de Início**, introduza `10.1.1.100` e `49` para **Número de Endereços**. Para endereço de IPv6, no campo **Endereço IP de Início**, introduza `2001:DA8::1:1` e `65535` para **Número de Endereços**.
16. Seleccione **Permitir que o sistema remoto tenha acesso a outras redes (reencaminhamento de IP)**. Faça clique em **OK**.

Iniciar perfil de ligação destinatário

Depois de configurar o perfil de ligação destinatário do protocolo L2TP (Layer Two Tunneling Protocol) para o Sistema A, o administrador terá de iniciar esta ligação para aguardar chegada de pedidos oriundos de clientes remotos.

Nota: Poderá receber uma mensagem de erro em como o subsistema QUSRWRK não foi iniciado. Esta mensagem ocorre quando se tenta iniciar o perfil de ligação destinatário. Para iniciar o subsistema QUSRWRK, siga estes passos:

1. Numa interface baseada em caracteres, introduza `strsbs`.
2. No ecrã Iniciar Subsistema, introduza `QUSRWRK` no campo **Descrição do subsistema**.

Para iniciar o perfil de ligação destinatário para clientes remotos, siga estas tarefas:

1. Em System i Navigator, seleccione **Actualizar** no menu **Ver**. Irá actualizar a instância do System i Navigator.
2. Em System i Navigator, expanda *Sistema A* → **Rede** → **Serviços de Acesso Remoto**.

3. Clique duas vezes em **Perfis de Ligação Destinatários**, clique com o botão direito do rato em **EMPRESAL2TP** e seleccione **Iniciar**.
4. Aparece o campo **Estado**, onde se lê **A aguardar pedidos de ligação**.

Configurar uma ligação VPN no Sistema A para clientes remotos

Depois de configurar o perfil de ligação destinatário do protocolo L2TP (Layer Two Tunneling Protocol) para o Sistema A, o administrador terá de configurar uma VPN para proteger a ligação entre clientes remotos e a rede da sucursal.

Para configurar uma VPN para clientes remotos, siga estas tarefas:

Importante: Os endereços IP utilizados neste cenário são meramente exemplificativos. Não reflectem nenhum esquema de endereços IP e não devem ser usados em nenhuma configuração verdadeira. Utilize os seus endereços de IP quando realizar tais tarefas.

1. Em System i Navigator, expanda ***Sistema A*** → **Rede** → **Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Rede Privada Virtual** e seleccione **Nova Ligação** para iniciar o assistente de Nova Ligação VPN. Reveja a página Bem-vindo(a) para mais informações sobre os objectos que o assistente cria.
3. Clique em **Seguinte** para ir à página Nome da Ligação.
4. No campo **Nome**, introduza `SalestoRemote`.
5. Opcional: Especifique uma descrição para este grupo de ligações. Clique em **Seguinte**.
6. Na página Cenário de Ligação, seleccione **Ligar o sistema central a outro sistema central**. Clique em **Seguinte**.
7. Na página Política de Internet Key Exchange, seleccione **Criar uma nova política** e depois **Segurança mais elevada, rendimento inferior**. Clique em **Seguinte**.
8. Na página Certificado para Terminal de Ligação Remota, seleccione **Não**. Clique em **Seguinte**.
9. Na página Servidor de Chaves Locais, seleccione **Endereço de IP Versão 4** para o tipo de identificador. O endereço de IP associado deve ser 192.168.1.2. Clique em **Seguinte**. Para endereço IPv6, na página Servidor de Chaves Locais, seleccione **Endereço de IP Versão 6** para o tipo de identificador. O endereço IP associado deve ser 2001:DB8::2. Clique em **Seguinte**.
10. Na página Servidor de Chaves Remotas, seleccione **Qualquer endereço de IP** no campo **Tipo de Identificador**. No campo **Chave pré-partilhada**, introduza `chaveempresa`. Clique em **Seguinte**.
11. Na página Serviços de Dados, introduza `1701` para porta local. Depois seleccione `1701` para porta remota e **UDP** para protocolo. Clique em **Seguinte**.
12. Na página Política de Dados, seleccione **Criar uma nova política** e depois **Segurança mais elevada, rendimento inferior**. Clique em **Seguinte**.
13. Na página Interfaces Aplicáveis, seleccione **ETHLINE**. Clique em **Seguinte**.
14. Na página Resumo, reveja os objectos que o assistente irá criar para se assegurar de de que estão correctos.
15. Faça clique em **Terminar** para concluir a configuração. Quando se abrir a janela Activar Filtros de Políticas, seleccione **Não, as regras de pacotes serão activadas mais tarde**. Faça clique em **OK**.

Actualizar políticas de VPN para ligações remotas oriundas de clientes Windows XP e Windows 2000

Visto que o assistente cria uma ligação padrão que pode ser utilizada na maioria das configurações de VPN, terá de actualizar as políticas que são geradas pelo assistente de modo a garantir a interoperacionalidade com clientes Windows XP e Windows 2000.

Para actualizar estas políticas VPN, siga estas tarefas:

1. Em System i Navigator, expanda ***Sistema A*** → **Rede** → **Políticas de IP** → **Funcionamento em Rede Privada Virtual** → **Políticas de Segurança de IP**.

2. Clique duas vezes em **Políticas Internet Key Exchange** , clique com o botão direito do rato em **Qualquer endereço IP** e seleccione **Propriedades**.
3. Na página Transformações, clique em **Adicionar**.
4. Na página Adicionar Transformação Internet Key Exchange, seleccione as seguintes opções:
   - **Método de autenticação:** Chave pré-partilhada
   - **Algoritmo de Cálculo de Endereços:** MD5
   - **Algorimo de Codificação:** DES-CBC
   - **Grupo Diffie-Hellman:** Grupo 1
5. Faça clique em **OK**.
6. Em System i Navigator, expanda ***Sistema A*** → **Rede** → **Políticas de IP** → **Funcionamento em Rede Privada Virtual** → **Políticas de Segurança de IP**.
7. Clique duas vezes em **Políticas de Dados**, clique com o botão direito do rato em **SalestoRemote** e seleccione **Propriedades**.
8. Na página Geral, desmarque **Utilizar sigilo de reencaminhamento perfeito Diffie-Hellman**.
9. Seleccione **Proposta ESP**, clique em **Editar**.
10. Na página Proposta de Política de Dados, modifique as opções deste modo.
    - **Modo de Encapsulamento:** Transporte
    - **Expiração da Chave:** 15 minutos
    - **Expirar no limite de tamanho:** 100000
11. Na página Transformações, clique em **Adicionar**.
12. Na página Adicionar Transformação de Política de Dados, seleccione as seguintes opções:
    - **Protocolo:** Encapsulating security payload (ESP)
    - **Algoritmo de Autenticação:** MD5
    - **Algorimo de Codificação:** DES-CBC
13. Faça clique em **OK** duas vezes.

Activar regras de filtro

O assistente cria automaticamente as regras de pacotes necessárias para que a ligação funcione correctamente. Contudo, deve activá-las em ambos os sistemas antes de poder iniciar a ligação VPN.

Para activar regras de filtro no Sistema A, siga estes passos:

Importante: Os endereços IP utilizados neste cenário são meramente exemplificativos. Não reflectem nenhum esquema de endereços IP e não devem ser usados em nenhuma configuração verdadeira. Deverá utilizar os seus endereços de IP quando realizar tais tarefas.

1. Em System i Navigator, expanda ***Sistema A*** → **Rede** → **Políticas de IP**.
2. Faça clique com o botão direito do rato em **Regras de Pacotes** e seleccione **Activar Regras**.
3. Na página Activar Regras de Pacotes, seleccione **activar somente as regras geradas pela VPN** e também **ETHLINE** como interface onde pretende activar estas regras de filtro. Faça clique em **OK**.

Antes de os utilizadores remotos poderem configurar as suas estações de trabalho Windows, o administrador dá-lhes as seguintes informações para poderem configurar o seu lado da ligação. Dá a cada qual dos utilizadores remotos as seguintes informações:

- Nome da chave pré-partilhada: `chaveempresa`
- Endereço IP do Sistema A: 192.168.1.2 (2001:DB8::2 em IPv6)
- Nome de utilizador e palavra-passe para a ligação

Nota: Foram criados quando o administrador adicionou nomes de utilizador e palavras-passe a uma lista de validação, durante a configuração do perfil terminador Layer Two Tunneling Protocol (L2TP).

Configurar a VPN num cliente Windows XP

Utilize este procedimento para configurar a VPN num cliente Windows XP.

Os utilizadores remotos na Empresa, S.A., precisam de configurar o cliente Windows XP remoto seguindo estes passos:

1. No menu **Iniciar** do Windows XP, expanda **Todos os Programas** → **Acessórios** → **Comunicações** → **Assistente Nova Ligação**.
2. Na página Bem-vindo(a), leia as informações gerais. Clique em **Seguinte**.
3. Na página Tipo de Ligação de Rede, seleccione **Ligar à rede no meu local de trabalho**. Clique em **Seguinte**.
4. Na página Ligação de Rede, seleccione **Ligação rede Privada Virtual**. Clique em **Seguinte**.
5. Na página Nome da Ligação, introduza `Ligação à Sucursal` no campo **Nome da Empresa**. Clique em **Seguinte**.
6. Na página Rede Pública, seleccione **Não marcar a ligação inicial**. Clique em **Seguinte**.
7. Na página Selecção do Servidor VPN, introduza `192.168.1.2` (`2001:DB8::2` no campo **Nome de sistema central ou endereço IP**. Clique em **Seguinte**.
8. Na página Disponibilidade da Ligação, seleccione **Só para minha Utilização**. Clique em **Seguinte**.
9. Na página Resumo, clique em **Adicionar atalho a esta ligação no ambiente de trabalho**. Faça clique em **Terminar**.
10. Clique no ícone **Ligar Ligação a Empresa** que foi criado no ambiente de trabalho.
11. Na página Ligar Ligação a Empresa, introduza o nome de utilizador e a palavra-passe que o administrador indicou.
12. Seleccione **Guardar este nome de utilizador e palavra-passe para os utilizadores seguintes** e **Só para mim**. Faça clique em **Propriedades**.
13. Na página **Segurança**, assegure-se de que estão seleccionadas as seguintes **Opções de seguranç**:
    - **Típicas**
    - **Pedir palavra-passe protegida**
    - **Pedir codificação de dados**

    Clique em **Definições IPSec**.
14. Na página Definições IPSec, seleccione **Utilizar chave pré-partilhada para autenticação** e introduza `chaveempresa` no campo **Chave pré-partilhada**. Faça clique em **OK**.
15. Na página Funcionamento em Rede, seleccione **VPN IPSec L2TP** como **Tipo de VPN**. Faça clique em **OK**.
16. Inicie sessão com nome de utilizador e palavra-passe e clique em **Ligar**.

Para iniciar a ligação VPN do lado do cliente, clique no ícone que aparece no ambiente de trabalho depois de concluir o assistente de ligação.

Testar a ligação VPN entre terminais

Quando terminar de configurar a ligação entre o Sistema A e utilizadores remotos, e tiver iniciado a ligação, deve testar a conectividade para se assegurar de que os sistemas centrais remotos conseguem comunicar entre si.

Para testar a conectividade, siga estes passos:

1. Em System i Navigator, expanda ***Sistema A*** → **Rede**.

2. Faça clique com o botão direito do rato em **Configuração de TCP/IP**, seleccione **Utilitários** e depois **Ping**.
3. No diálogo **Ping a partir de**, introduza `10.1.1.101` (`2001:DA8::1:101` em IPv6) no campo **Ping**.

   Nota: 10.1.1.101 representa o endereço IP dinamicamente atribuído (ao cliente das vendas remotas) oriundo do conjunto de endereços especificado no perfil terminador L2TP (Layer Two Tunneling Protocol) no Sistema A.
4. Faça clique em **Efectuar Ping Agora** para verificar a conectividade do Sistema A a uma estação de trabalho remota. Faça clique em **OK**.

Para testar a ligação oriunda do sistema remoto, o funcionário remoto segue estes passos numa estação de trabalho que execute Windows:

1. Na linha de comandos, introduza `ping 10.1.1.2` (`ping 2001:DA8::2` em IPv6). Trata-se do endereço IP de uma das estações de trabalho da rede da empresa.
2. Repita estes passos para testar a conectividade da empresa à sucursal.

Cenário: Utilizar conversão de endereços de rede para a VPN

Neste cenário, a sua empresa pretende trocar dados sensíveis com um dos parceiros empresariais, por meio da VPN. Para proteger ainda mais a privacidade da estrutura de rede da sua empresa, também irá utilizar a NAT de VPN para ocultar o endereço de IP do sistema utilizado para hospedar as aplicações a que o parceiro de negócios tem acesso.

Situação

Suponha que é o administrador da rede de uma pequena fábrica no Porto. Um dos seus parceiros de negócios, um fornecedor de peças em Lisboa, 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. Para proteger ainda mais a privacidade da estrutura de rede da sua empresa, decide que irá necessitar de ocultar o endereço de IP privado do sistema que aloja as aplicações às quais o fornecedor tem acesso.

A VPN pode ser utilizada 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 de VPN executa a conversão de endereços antes da validação SA através da atribuição de um endereço quando a ligação é iniciada.

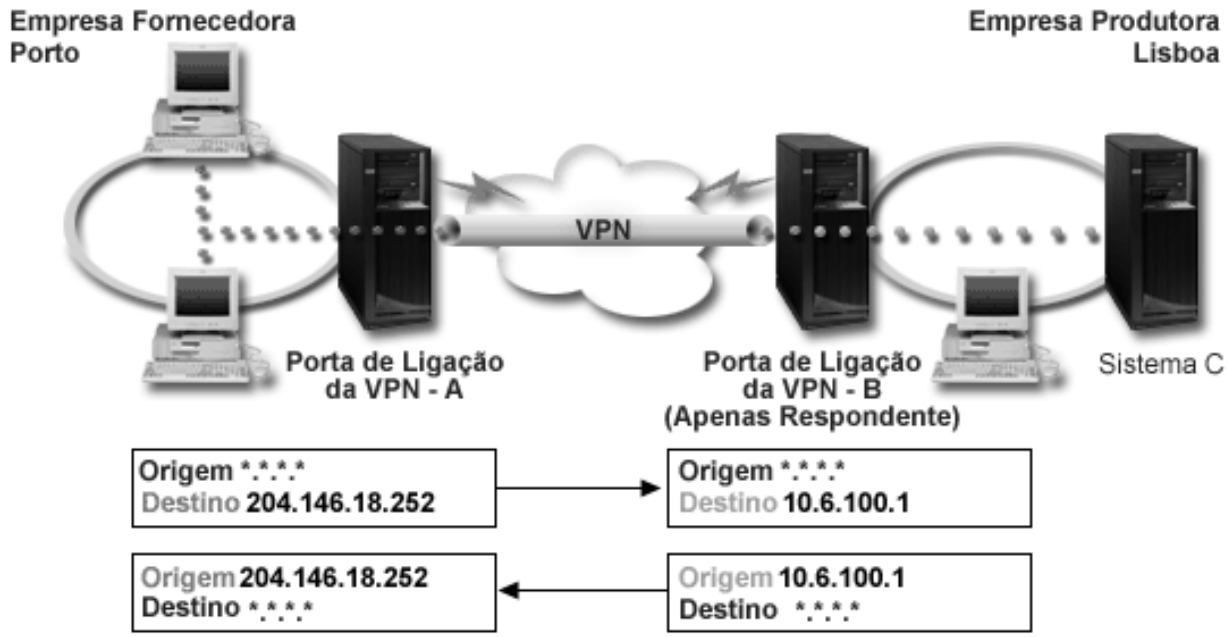
Objectivos

Os objectivos deste cenário são:

- permitir a todos os clientes na rede do fornecedor o acesso a um único sistema central na rede do fabricante via ligação VPN porta de ligação a porta de ligação.
- ocultar os endereços de IP do sistema central na rede do fabricante, convertendo-os em endereços de IP públicos, mediante conversão de endereços de rede para a VPN (NAT de 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 terminal destino para a ligação como 204.146.18.252 (o endereço público atribuído ao Sistema C).
- O Sistema C tem o endereço de IP privado 10.6.100.1 na rede do fabricante.
- Foi definido um endereço público 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 Sistema C.
- A porta de ligação B da VPN converte o endereço público do Sistema C no respectivo endereço privado, 10.6.100.1, para a chegada de datagramas. A porta de ligação B da VPN converte datagramas de regresso e de partida, oriundos do endereço 10.6.100.1 no o endereço público 204.146.18.252 do Sistema C. Em relação aos clientes na rede do fornecedor, o Sistema C tem o endereço de IP 204.146.18.252. Nunca se irão aperceber de que ocorreu esta conversão de endereços.

Tarefas de configuração

Tem de 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 **Sistema 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 relacionados

"Conversão de endereços de rede para a VPN" na página 9
A VPN fornece uma forma de executar a conversão de endereços da rede, denominada NAT de VPN. A NAT de 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.

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 a um consultor de planeamento que irá criar uma folha de trabalho personalizada de acordo com as suas especificações.

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
- Determinar que tipo de VPN deve criar
- 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

Depois de efectuar a planificação da VPN, pode iniciar a sua configuração.

Tarefas relacionadas

Utilize o consultor de planeamento da VPN

"Configurar a VPN" na página 50
A VPN proporciona várias formas diferentes para configurar ligações VPN. Pode configurar ligações manuais ou dinâmicas.

Requisitos de configuração da VPN

Para que uma ligação VPN funcione devidamente nos sistemas e com clientes de rede, terá de cumprir os requisitos mínimos

Segue-se uma lista dos requisitos mínimos para configurar uma ligação VPN:

Requisitos do sistema

- i5/OS Versão 5 Edição 3 ou posterior
- Gestor de Certificados Digitais
- System i Access for Windows
- System i Navigator
  - Componente de rede do System i Navigator
- Definir o valor do sistema de retenção de dados de segurança do servidor (QRETSVRSEC *SEC), para 1
- O TCP/IP tem de 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, devidamente ligado ao sistema e configurado para TCP/IP
- Uma unidade de processamento de 233 Mhz
- 32 MB RAM para clientes para Windows 95
- 64 MB RAM para cliente Windows NT 4.0 e Windows 2000
- System i Access for Windows e System i 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.

Tarefas relacionadas

"Iniciação à detecção e resolução de problemas da VPN" na página 64
Siga esta tarefa para saber os diversos métodos para determinar problemas de VPN que possa ter no 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 locais, como o servidor de chaves remotas desempenham na ligação.

Por exemplo, os terminais da *ligação* são diferentes dos terminais de *dados*? São iguais ou alguma combinação de ambos? Os terminais 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 terminais de dados, por outro lado, definem a ligação entre dois sistemas face ao tráfego de 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 terminais 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 terminais da ligação de ambos os sistemas são diferentes dos terminais 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 terminais da ligação são iguais aos terminais 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 terminal a terminal.

Preencher folhas de trabalho de planeamento 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.

Caso prefira, pode imprimir e preencher as folhas de trabalho de planeamento para recolher informações detalhadas sobre os planos de utilização da VPN.

Escolha a folha de trabalho para o tipo de ligação que pretende criar.

- Folha de trabalho de planeamento para ligações dinâmicas
- Folha de trabalho de planeamento para ligações manuais
- 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 o consultor de planeamento da VPN só 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 optar por definir as predefinições da VPN. Os valores predefinidos configurados permanecem nas folhas de propriedades da VPN. Isto significa que não tem de configurar as mesmas propriedades várias vezes. Para estabelecer os valores predefinidos da VPN, seleccione **Editar** no menu principal da VPN e depois **Predefinições**.

Informações relacionadas

Consultor de planeamento da VPN

Folha de trabalho de planeamento para ligações dinâmicas

Conclua esta folha de trabalho antes de configurar uma ligação dinâmica.

Antes de criar ligações VPN dinâmicas, preencha esta folha de trabalho. A folha de trabalho pressupõe que irá utilizar o Assistente Nova Ligação. O assistente permite configurar uma VPN com base nos seus requisitos de segurança básicos. Em alguns casos, poderá ter de especificar as propriedades que o assistente configura para a ligação. Por exemplo, poderá decidir que pretende registo em diário ou que o servidor VPN se inicie sempre que for iniciado o protocolo TCP/IP. 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.

Tabela 9. Requisitos do sistema

Lista de verificação de pré-requisitos	**Respostas**
O sistema operativo está na i5/OS V5R3 ou posterior?	Sim
A opção Gestor de Certificados Digitais está instalada?	Sim
O System i Access for Windows está instalado?	Sim
O System i Navigator está instalado?	Sim
O subcomponente de Rede do System i Navigator está instalado?	Sim
O IBM TCP/IP Connectivity Utilities for i5/OS 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 sistema (incluindo interfaces de IP, encaminhamentos, nome do sistema central local e nome do domínio local)?	Sim

Tabela 9. Requisitos do sistema (continuação)

Lista de verificação de pré-requisitos	**Respostas**
Foi estabelecida uma comunicação de TCP/IP normal entre os terminais necessários?	Sim
Aplicou as mais recentes correcções temporárias de programas (PTFs)?	Sim
Se o túnel de VPN passa por firewalls ou encaminhadores que implementem filtro de pacotes de IP, as regras de filtro da firewall ou dos encaminhadores suportam protocolos de 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

Tabela 10. Configuração da VPN

Necessita destas informações para configurar uma ligação dinâmica 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 • Equilibrar segurança e rendimento • 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 locais?	
Qual é o identificador do servidor de chaves locais?	
Qual é o identificador do servidor de chaves remotas?	
Qual é o identificador do terminal de dados remoto?	
De que tipo de segurança e de rendimento de sistema necessita para proteger os seus dados? • Segurança máxima, rendimento mínimo • Equilibrar segurança e rendimento • Segurança mínima e rendimento máximo	

Folha de trabalho de planeamento para ligações manuais

Preencha esta folha de trabalho antes de configurar uma ligação manual.

Preencha esta folha de trabalho para ajudar a criar as ligações da Rede privada virtual (VPN) que não utilizam IKE para gestão de chaves. Responda a cada uma destas questões antes de continuar com a configuração da VPN:

Tabela 11. Requisitos do sistema

Lista de verificação de pré-requisitos	**Respostas**
O sistema executa i5/OS V5R3 ou posterior?	
A opção Gestor de Certificados Digitais está instalada?	

Tabela 11. Requisitos do sistema (continuação)

O System i Access for Windows está instalado?	
O System i Navigator está instalado?	
O subcomponente de Rede do System i Navigator está instalado?	
O IBM TCP/IP Connectivity Utilities for i5/OS 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 sistema (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 terminais necessários?	
Aplicou as mais recentes correcções temporárias de programas (PTFs)?	
Se o túnel de VPN passa por firewalls ou encaminhadores que implementem filtragem de pacotes de IP, as regras de filtro da firewall ou dos encaminhadores suportam protocolos de 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?	

Tabela 12. Configuração da VPN

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 ligação?	
Qual é o identificador do terminal da ligação local?	
Qual é o identificador do terminal da ligação remota?	
Qual é o identificador do terminal de dados local?	
Qual é o identificador do terminal de dados remoto?	
Que tipo de tráfego irá permitir para esta ligação (porta local, porta remota e protocolo)?	
Precisa de conversão de endereços para esta ligação? Consulte Conversão de endereços de rede para VPN para mais informações.	
Irá utilizar o modo de túnel 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.	
Qual é a chave de chegada 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 chegada tem de corresponder exactamente à chave de partida do servidor remoto.	

Tabela 12. Configuração da VPN (continuação)

Qual é a chave de partida 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 partida tem de corresponder exactamente à chave de chegada do servidor remoto.	
Qual é a chave de chegada 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 chegada tem de corresponder exactamente à chave de partida do servidor remoto.	
Qual é a chave de partida 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 partida tem de corresponder exactamente à chave de chegada do servidor remoto.	
Qual é o SPI (Security Policy Index) de chegada? O SPI de chegada é uma cadeia hexadecimal de 4 bytes, em que o primeiro byte está definido como 00. O seu SPI de chegada tem de corresponder exactamente ao SPI de partida do servidor remoto.	
Qual é o SPI de partida? O SPI de partida é uma cadeia hexadecimal de 4 bytes. O seu SPI de partida tem de corresponder exactamente ao SPI de chegada do servidor remoto.	

Conceitos relacionados

"Conversão de endereços de rede para a VPN" na página 9
A VPN fornece uma forma de executar a conversão de endereços da rede, denominada NAT de VPN. A NAT de 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.

Configurar a VPN

A VPN proporciona várias formas diferentes para configurar ligações VPN. Pode configurar ligações manuais ou dinâmicas.

Uma ligação dinâmica gere e negoceia dinamicamente as chaves que a protegem, enquanto está activa, mediante 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.

No entanto, uma ligação manual não fornece suporte para negociações de IKE e, por conseguinte, gestão de chaves automática. Além disso, ambos os extremos da ligação exigem que configure vários atributos que têm de corresponder de forma exacta. As ligações manuais utilizam chaves estáticas que não são actualizadas ou alteradas enquanto a ligação estiver activa. Tem de parar uma ligação manual para alterar a respectiva chave associada. Se considerar este facto um risco para a segurança, poderá ser útil criar uma ligação dinâmica.

Conceitos relacionados

"Planear a VPN" na página 45
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 a um consultor de planeamento que irá criar uma folha de trabalho personalizada de acordo com as suas especificações.

Configurar ligações VPN com o assistente Nova Ligação

O assistente de Nova Ligação permite criar uma rede privada virtual (VPN) 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 (NAT de VPN), poderá sintonizar melhor a VPN com as folhas de propriedades da ligação ou do grupo de chaves dinâmicas apropriado(a). Para isso, tem de 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 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 System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Rede Privada Virtual**e seleccione **Nova Ligação** para iniciar o assistente.
3. Conclua o assistente para criar uma ligação básica VPN. Faça clique em **Ajuda** caso necessite de assistência.

Tarefas relacionadas

Consultor de planeamento da VPN

Configurar políticas de segurança da VPN

Depois de determinar a forma como irá utilizar a VPN, tem de definir as políticas de segurança da VPN.

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

Tarefas relacionadas

"Configurar uma ligação VPN segura" na página 53
Após a configuração das políticas de segurança para a ligação, tem de, em seguida, configurar a ligação segura.

Configurar uma política Internet Key Exchange

A política IKE define qual o nível de autenticação e de protecção de codificação é utilizado pelo IKE durante negociações de fase 1.

A fase 1 do IKE estabelece as chaves que protegem as mensagens que circulam nas negociações da fase 2 subsequentes. Não é necessário 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.

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, tem de configurá-los previamente através do Gestor de Certificados Digitais. A política de IKE também identifica qual o servidor de chaves remotas que irá utilizar esta política.

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

1. No System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP** → **Rede Privada Virtual** → **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 em **Políticas do Internet Key Exchange** na área de janela da esquerda, em seguida faça clique com o botão direito do rato sobre a política que pretende alterar na área de janela da direita e seleccione **Propriedades**.
3. Preencha cada uma das folhas de propriedades. Faça clique em **Ajuda** caso tenha questões acerca do preenchimento de uma página ou de qualquer um dos respectivos campos.
4. Faça clique em **OK** para guardar as alterações.

Recomenda-se que utilize a negociação de modo principal sempre que for utilizada uma chave partilhada para autenticação. Fornecem uma troca mais segura. Se tiver de utilizar chaves pré-partilhadas e um modo de negociação agressivo, seleccione palavras-passe obscuras que sejam difíceis de decifrar em ataques que fazem pesquisas no dicionário. Também se recomenda que mude periodicamente as suas palavras-passe. Para obrigar uma troca de chaves a utilizar a negociação de modo principal, execute as tarefas seguintes:

1. No System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP**.
2. Seleccione **Rede Privada Virtual** → **Políticas de Segurança de IP** → **Políticas de Troca de Chaves da Internet** para ver as políticas de troca de chaves definidas actualmente na área de janela da direita.
3. Faça clique com o botão direito do rato sobre uma determinada política de troca de chaves e seleccione **Propriedades**.
4. Na página Transformações, clique em **Política de Resposta**. Surge a caixa de diálogo Política de Troca de Chaves da Internet de Resposta.
5. No campo de Protecção de identidade, desmarque **negociação em modo agressivo IKE (sem protecção de identidade)**.
6. Faça clique em **OK** para voltar à caixa de diálogo Propriedades.
7. Faça clique em **OK** para guardar as alterações.

Nota: Quando definir o campo de protecção de identidade, a alteração entra em vigor para todas as trocas com servidores de chaves remotos, visto que apenas existe uma política de IKE respondente para todo o sistema. A negociação de modo principal assegura que o sistema em iniciação apenas pode solicitar uma troca de política de chaves de modo principal.

Conceitos relacionados

"Gestão de chaves" na página 6
Uma VPN dinâmica proporciona segurança adicional às comunicações, com o protocolo Internet Key Exchange (IKE) para a gestão de chaves. O IKE permite aos servidores VPN em cada extremo da ligação negociar novas chaves em intervalos específicos.

Tarefas relacionadas

Gestor de Certificados Digitais

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 em comunicação acordam estes atributos durante as negociações da fase 2 do protocolo Internet Key Exchange (IKE). Não é necessário 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.

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

1. No System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP** → **Rede Privada Virtual** → **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 em **Políticas de Dados** (na área de janela da esquerda), em seguida faça clique com o botão direito do rato sobre a política de dados que pretende alterar (na área de janela da direita) e seleccione **Propriedades**.
3. Preencha cada uma das folhas de propriedades. Faça clique em **Ajuda** caso tenha questões acerca do preenchimento de uma página ou de qualquer um dos respectivos campos.
4. Faça clique em **OK** para guardar as alterações.

Conceitos relacionados

"Gestão de chaves" na página 6
Uma VPN dinâmica proporciona segurança adicional às comunicações, com o protocolo Internet Key Exchange (IKE) para a gestão de chaves. O IKE permite aos servidores VPN em cada extremo da ligação negociar novas chaves em intervalos específicos.

Configurar uma ligação VPN segura

Após a configuração das políticas de segurança para a ligação, tem de, em seguida, configurar a ligação segura.

Para 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 VPN. Configurar um grupo de chaves dinâmicas permite utilizar as mesmas políticas, mas diferentes terminais de dados para cada ligação dentro do grupo. Os grupos de chaves dinâmicas permitem ainda negociar de forma bem sucedida com os iniciadores remotos, quando os terminais de dados propostos pelo sistema remoto não forem especificamente conhecidos com antecedência. Os grupos procedem a esta negociação associando as informações sobre políticas no grupo de chaves dinâmicas a uma regra de filtro de políticas com um tipo de acção IPSEC. Se os terminais de dados específicos facultados pelo iniciador remoto estiverem dentro do intervalo especificado na regra de filtro 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 terminais. 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, execute ambas as tarefas Parte 1 e Parte 2:

Conceitos relacionados

"Configurar políticas de segurança da VPN" na página 51
Depois de determinar a forma como irá utilizar a VPN, tem de definir as políticas de segurança da VPN.

"Configurar regras de pacotes da VPN" na página 55
Se estiver a criar uma ligação pela primeira vez, deve permitir que a VPN crie automaticamente as regras de pacotes da VPN. Pode fazê-lo com o assistente Nova Ligação ou nas páginas de propriedades da VPN para configurar a ligação.

Tarefas relacionadas

"Activar regras de pacotes da VPN" na página 59
Tem de activar as regras de pacotes da VPN antes de poder iniciar as ligações VPN.

Parte 1: Configurar um grupo de chaves dinâmicas

1. No System i Navigator, expanda **sistema → Rede → Políticas de IP → Rede Privada Virtual → Ligações Seguras**.
2. Faça clique com o botão direito do rato sobre **Por Grupo** e seleccione **Novo Grupo de Chaves Dinâmicas**.

3. Faça clique em **Ajuda** caso tenha questões acerca do preenchimento de uma página ou de qualquer um dos respectivos campos.
4. Faça clique em **OK** para guardar as alterações.

Parte 2: Configurar uma ligação de chaves dinâmicas

1. Em System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP** → **Rede Privada Virtual** → **Ligações Seguras** → **Por Grupo**.
2. Na área de janela da esquerda do System i 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 em **Ajuda** caso tenha questões acerca do preenchimento de uma página ou de qualquer um dos respectivos campos.
4. Faça clique em **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 maioria dos casos, deve permitir que a interface da VPN crie automaticamente as regras de pacotes de VPN, ao seleccionar a opção **Gerar a seguinte filtro de políticas para este grupo**, na página **Grupo de chaves Dinâmicas - Ligações**. Contudo, se seleccionar a opção **O filtro de políticas será definido nas Regras de Pacotes**, tem de configurar regras de pacotes da VPN utilizando o editor de Regras de Pacotes e, em seguida, activá-las.

Configurar uma ligação manual

Uma ligação manual é aquela em que deve configurar todas as propriedades da VPN sem recurso a assistentes.

Além disso, ambos os extremos da ligação exigem que configure vários elementos que têm de corresponder de forma *exacta*. Por exemplo, as chaves de chegada têm de corresponder às chaves de partida do sistema remoto ou a ligação falha.

As ligações manuais utilizam chaves estáticas que não são actualizadas nem alteradas enquanto a ligação estiver activa. Tem de parar uma ligação manual para alterar a respectiva chave associada. Se considerar este facto um risco para a segurança e que ambos 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 System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP** → **Rede Privada Virtual** → → **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 em **Ajuda** caso tenha questões acerca do preenchimento de uma página ou de qualquer um dos respectivos campos.
4. Faça clique em **OK** para guardar as alterações.

Nota: Na maioria dos casos, permita que a interface da crie automaticamente as regras de pacotes de VPN ao seleccionar a opção **Criar um filtro de políticas que corresponda aos terminais de dados**, na página **Ligação Manual - Ligação**. Contudo, se seleccionar a opção **A regra de filtro de políticas será definida nas Regras de Pacotes**, tem de configurar uma regra de filtro de políticas manualmente e, em seguida, activá-las.

Tarefas relacionadas

"Configurar uma regra de filtro de políticas" na página 57
Só deve concluir esta tarefa se tiver especificado que não pretende que a VPN faça automaticamente a gestão das regras de filtro de políticas.

Configurar uma ligação dinâmica

Uma ligação dinâmica gere e negoceia dinamicamente as chaves que a protegem, enquanto está activa, mediante utilização do protocolo Internet Key Exchange (IKE).

Siga o assistente Nova Ligação com Chaves Dinâmicas para configurar uma ligação dinâmica, nestes passos:

1. Em System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP** → **Rede Privada Virtual** → **Ligações Seguras** → **Por Grupo**.
2. Clique com o botão direito do rato no grupo de chaves dinâmicas específico e seleccione **Nova Ligação com Chaves Dinâmicas**.
3. Preencha cada uma das folhas de propriedades. Faça clique em **Ajuda** caso tenha questões acerca do preenchimento de uma página ou de qualquer um dos respectivos campos.
4. Faça clique em **OK** para guardar as alterações.

Configurar regras de pacotes da VPN

Se estiver a criar uma ligação pela primeira vez, deve permitir que a VPN crie automaticamente as regras de pacotes da VPN. Pode fazê-lo com o assistente Nova Ligação ou nas páginas de propriedades da VPN para configurar a ligação.

Caso decida criar as suas regras de pacote da VPN ao utilizar o editor de Regras de Pacotes no System i Navigator, crie as regras adicionais também desta forma. De modo oposto, se for a VPN a criar as regras de filtro de políticas, crie desta forma todas as regras de filtro de políticas adicionais.

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

- Configurar a regra de filtro pré-IPSec

  As regras pré-IPSec são regras existentes 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: Só 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 filtro especificamente escritas para permitir o tráfego IKE, o tráfego IKE estará implicitamente garantido.
- Configurar uma regra de filtro de políticas

  A regra de filtro 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 filtro a uma interface, o sistema adiciona automaticamente uma regra DENY predefinida a essa interface. Isto significa que qualquer tráfego que não seja expressamente permitido é recusado. Não é possível ver nem alterar esta regra. Desta forma, pode acontecer que tráfego que funcionava anteriormente falhe misteriosamente, após a activação das regras de filtro da VPN. Se pretender permitir outro tráfego na interface para além do da VPN, tem de adicionar regras PERMIT explícitas para fazê-lo.

Depois de configurar as regras de filtro adequadas, tem de definir a interface às quais são aplicadas e, em seguida, activá-las.

É fundamental que configure as regras de filtro de forma correcta. Caso contrário, as regras de filtro podem bloquear todo o tráfego IP que entra e sai do sistema. Inclui a ligação ao System i Navigator, utilizada para configurar as regras de filtro.

Se as regras de filtro não permitirem o tráfego no System i, o System i Navigator não pode comunicar com o sistema. Se porventura ficar nesta situação, terá de iniciar a sessão no sistema 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.

Conceitos relacionados

"Filtragem da VPN e IP" na página 12
A filtragem IP e a VPN estão estreitamente relacionadas. De facto, a maioria das ligações da VPN requerem regras de filtro para funcionarem correctamente. Este tópico, fornece informações sobre quais os filtros requeridos pela VPN, bem como outros conceitos de filtragem relacionados com a VPN.

Tarefas relacionadas

"Configurar uma ligação VPN segura" na página 53
Após a configuração das políticas de segurança para a ligação, tem de, em seguida, configurar a ligação segura.

"Configurar a regra de filtro pré-IPSec"
Só deve concluir esta tarefa se tiver especificado que não pretende que a VPN faça automaticamente a gestão das regras de filtro de políticas.

"Configurar uma regra de filtro de políticas" na página 57
Só deve concluir esta tarefa se tiver especificado que não pretende que a VPN faça automaticamente a gestão das regras de filtro de políticas.

"Definir uma interface para as regras de filtro da VPN" na página 58
Depois de configurar as regras de pacotes da VPN e outras regras de que necessite para activar a ligação VPN, tem de definir a interface à qual se aplicam.

"Activar regras de pacotes da VPN" na página 59
Tem de activar as regras de pacotes da VPN antes de poder iniciar as ligações VPN.

Configurar a regra de filtro pré-IPSec

Só deve concluir esta tarefa se tiver especificado que não pretende que a VPN faça automaticamente a gestão das regras de filtro de políticas.

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

1. No System i Navigator, expanda **sistema** → **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 filtro para o sistema.
3. Na janela Bem-vindo(a), seleccione **Criar um novo ficheiro de regras de pacotes** e clique em **OK**.
4. No editor Regras de Pacotes, seleccione **Inserir** → **Filtrar**.
5. Na página **Geral**, especifique um nome do conjunto para as regras de filtro da VPN. É recomendada a criação de pelo menos três conjuntos diferentes: o primeiro para as regras de filtro pré-IPSec, o segundo para as regras de filtro de políticas e o último para regras de filtro PERMIT e DENY. Atribua um nome ao conjunto que contenha as regras de filtro pré-IPSec com um prefixo de *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 locais no segundo campo. Especificou o endereço de IP do servidor de chaves locais 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 remotas no segundo campo. Especificou também o endereço de IP do servidor de chaves remotas 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 em **OK**.
15. Repita estes passos para configurar o filtro INBOUND. Utilize o mesmo nome do conjunto e os mesmo endereços inversos, conforme necessário.

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 filtro de políticas para definir qual o tráfego IP protegido pela ligação VPN.

Conceitos relacionados

"Configurar regras de pacotes da VPN" na página 55
Se estiver a criar uma ligação pela primeira vez, deve permitir que a VPN crie automaticamente as regras de pacotes da VPN. Pode fazê-lo com o assistente Nova Ligação ou nas páginas de propriedades da VPN para configurar a ligação.

Tarefas relacionadas

"Configurar uma regra de filtro de políticas"
Só deve concluir esta tarefa se tiver especificado que não pretende que a VPN faça automaticamente a gestão das regras de filtro de políticas.

Configurar uma regra de filtro de políticas

Só deve concluir esta tarefa se tiver especificado que não pretende que a VPN faça automaticamente a gestão das regras de filtro de políticas.

A regra de filtro 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 VPN. Para configurar uma regra de filtro de políticas, siga estes passos:

Nota: Se acabou de configurar a regra pré-IPSec (apenas para ligações dinâmicas), o Editor de Regras de pacotes ainda vai estar aberto; siga para o passo 4.

1. No System i Navigator, expanda **sistema** → **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 filtro para o sistema.
3. Na janela Bem-vindo(a), seleccione **Criar um novo ficheiro de regras de pacotes** e clique em **OK**.
4. No editor Regras de Pacotes, seleccione **Inserir** → **Filtrar**.
5. Na página **Geral**, especifique um nome do conjunto para as regras de filtro da VPN. É recomendada a criação de pelo menos três conjuntos diferentes: o primeiro para as regras de filtro pré-IPSec, o segundo para as regras de filtro de políticas e o último para regras de filtro PERMIT e DENY. Por exemplo, `filtrospolíticas`

6. No campo **Acção**, seleccione **IPSEC** na lista pendente. O campo **Direcção** tem como predefinição OUTBOUND e não pode alterá-lo. Apesar de este campo ter como predefinição OUTBOUND, é, na verdade, bidireccional. OUTBOUND é apresentado para clarificar a semântica dos valores de entrada de dados. 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 terminal 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 os definir com a função **Definir Endereços**.
8. Para **Nome do endereço de destino**, seleccione **=** no primeiro campo e, em seguida, introduza o endereço de IP do terminal 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 os definir com a 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 filtro 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 utilize qualquer porta utilizar a VPN.
14. Faça clique em **OK**.

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

Nota: Quando adiciona regras de filtro a uma interface, o sistema adiciona automaticamente uma regra DENY predefinida a essa interface. Isto significa que qualquer tráfego que não seja expressamente permitido é recusado. Não é possível ver nem 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 quiser permitir outro tráfego na interface para além do da VPN, tem de adicionar regras PERMIT explícitas nesse sentido.

Conceitos relacionados

"Configurar regras de pacotes da VPN" na página 55
Se estiver a criar uma ligação pela primeira vez, deve permitir que a VPN crie automaticamente as regras de pacotes da VPN. Pode fazê-lo com o assistente Nova Ligação ou nas páginas de propriedades da VPN para configurar a ligação.

Tarefas relacionadas

"Configurar uma ligação manual" na página 54
Uma ligação manual é aquela em que deve configurar todas as propriedades da VPN sem recurso a assistentes.

"Configurar a regra de filtro pré-IPSec" na página 56
Só deve concluir esta tarefa se tiver especificado que não pretende que a VPN faça automaticamente a gestão das regras de filtro de políticas.

"Definir uma interface para as regras de filtro da VPN"
Depois de configurar as regras de pacotes da VPN e outras regras de que necessite para activar a ligação VPN, tem de definir a interface à qual se aplicam.

Definir uma interface para as regras de filtro da VPN

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

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

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

1. No System i Navigator, expanda **sistema** → **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 filtro para o sistema.
3. Na janela Bem-vindo(a), seleccione **Criar um novo ficheiro de regras de pacotes** e clique em **OK**.
4. No editor Regras de Pacotes, seleccione **Inserir** → **Interface de Filtro**.
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 em **Adicionar**, para adicionar cada nome do conjunto para o filtros configurados.
8. Faça clique em **OK**.
9. Guarde o ficheiro de regras. TO ficheiro é guardado no sistema de ficheiros integrado do sistema 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.

Após definir uma interface para as regras de filtro, tem de activá-las antes de poder iniciar a VPN.

Conceitos relacionados

"Configurar regras de pacotes da VPN" na página 55
Se estiver a criar uma ligação pela primeira vez, deve permitir que a VPN crie automaticamente as regras de pacotes da VPN. Pode fazê-lo com o assistente Nova Ligação ou nas páginas de propriedades da VPN para configurar a ligação.

Tarefas relacionadas

"Configurar uma regra de filtro de políticas" na página 57
Só deve concluir esta tarefa se tiver especificado que não pretende que a VPN faça automaticamente a gestão das regras de filtro de políticas.

"Activar regras de pacotes da VPN"
Tem de activar as regras de pacotes da VPN antes de poder iniciar as ligações VPN.

Activar regras de pacotes da VPN

Tem de activar as regras de pacotes da VPN antes de poder iniciar as ligações VPN.

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

Se tiver criado as ligações VPN com o assistente Nova Ligação, pode optar por 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 filtro de políticas da VPN.

Caso decida activar as regras criadas pela VPN utilizando o Editor de Regras de Pacote, siga estes passos:

1. No System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Regras de Pacotes** e seleccione **Activar**. Abre-se a caixa de diálogo **Activar Regras de Pacotes**.

3. Seleccione se pretende activar somente 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 aplicar 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 em **OK** na caixa de diálogo para confirmar que pretende verificar e activar as regras na interface ou 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 específicos, 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 filtro, pode iniciar a ligação VPN.

Conceitos relacionados

"Configurar regras de pacotes da VPN" na página 55
Se estiver a criar uma ligação pela primeira vez, deve permitir que a VPN crie automaticamente as regras de pacotes da VPN. Pode fazê-lo com o assistente Nova Ligação ou nas páginas de propriedades da VPN para configurar a ligação.

Tarefas relacionadas

"Configurar uma ligação VPN segura" na página 53
Após a configuração das políticas de segurança para a ligação, tem de, em seguida, configurar a ligação segura.

"Definir uma interface para as regras de filtro da VPN" na página 58
Depois de configurar as regras de pacotes da VPN e outras regras de que necessite para activar a ligação VPN, tem de definir a interface à qual se aplicam.

"Iniciar uma ligação VPN" na página 61
Conclua esta tarefa para iniciar ligações iniciadas localmente.

Configurar confidencialidade de fluxo de dados

Se a política de dados estiver configurada para modo de túnel, poderá utilizar TFC (traffic flow confidentiality) para ocultar o comprimento real dos pacotes de dados transferidos numa ligação VPN.

A TFC adiciona revestimento adicional aos pacotes enviados e envia pacotes fictícios com extensões diferentes a intervalos aleatórios, para ocultar a extensão real dos pacotes. Use a TFC para uma segurança adicional relativamente a intrusos que possam adivinhar o tipo de dados que estão a ser enviados, com base na extensão do pacote. Ao activar a TFC obtém mais segurança, mas o preço a pagar é o rendimento do sistema. Assim sendo, deverá verificar o rendimento do sistema antes e depois de activar a TFC numa ligação de VPN. A TFC não é negociada por IKE e o utilizador só deve activar a TFC se ambos os sistemas a suportarem.

Para activar TFC numa ligação de VPN, execute os passos seguintes:

1. No System i Navigator, expanda o servidor > **Rede** → **Políticas de IP** → **Rede Privada Virtual** → **Ligações Seguras** → **Todas as Ligações**.
2. Faça clique com o botão direito do rato sobre a ligação para a qual pretende activar TFC e seleccione **Propriedades**.
3. No separador **Geral**, seleccione **Usar Confidencialidade de Fluxo de Tráfego (TFC) quando estiver em Modo Túnel**.

Configurar número de sequência expandido

Pode utilizar o ESN (extended sequence number - número de sequência expandido) para aumentar a velocidade de transmissão de dados para uma ligação de VPN.

Se usar o protocolo AH ou o protocolo ESP e AES como algoritmo de codificação, é do seu interesse activar ESN. O ESN permite a transmissão de grandes volumes de dados a uma elevada velocidade sem ter de voltar a inserir as informações. A ligação de VPN usa uma sequência de números de 64 bits em vez de números de 32 bits através de IPSec. A utilização da sequência de números de 64 bits confere mais tempo antes de ter de voltar a inserir, o que evita a exaustão de sequências de números e minimiza o uso de recursos do sistema.

Para activar ESN numa ligação de VPN, execute os passos seguintes:

1. Em System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP** → **Funcionamento em Rede Privada Virtual**
2. Faça clique com o botão direito do rato sobre **Rede Privada Virtual** e seleccione **Propriedades**.
3. No separador **Geral**, seleccione **Usar o Número de Sequência Expandido (ESN)**.

Iniciar uma ligação VPN

Conclua esta tarefa para iniciar ligações iniciadas localmente.

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

1. No System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP**.
2. Se o servidor VPN não se tiver iniciado, faça clique com o botão direito do rato em **Rede Privada Virtual** e seleccione **Iniciar**.
3. Certifique-se de que as regras de pacotes estão activadas.
4. Expanda **Rede Privada Virtual** → **Ligações Seguras**.
5. Faça clique em **Todas as Ligações** para visualizar uma lista de ligações na área de janela 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 e seleccione **Iniciar**.

Tarefas relacionadas

"Activar regras de pacotes da VPN" na página 59
Tem de activar as regras de pacotes da VPN antes de poder iniciar as ligações VPN.

"Iniciação à detecção e resolução de problemas da VPN" na página 64
Siga esta tarefa para saber os diversos métodos para determinar problemas de VPN que possa ter no sistema.

Gerir a VPN

Pode utilizar a interface VPN em System i Navigator para tratar de todas as tarefas de gestão da VPN como, por exemplo, parar uma ligação e ver atributos de ligação.

Use a interface da VPN no System i Navigator para processar todas as tarefas de gestão, incluindo:

Estabelecer atributos predefinidos para as ligações

Os valores predefinidos gerem os painéis utilizados para criar novas políticas e ligações. Pode definir valores predefinidos para níveis de segurança, gestão de sessões chave, validades das chaves e das ligações.

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

Para estabelecer valores de segurança predefinidos para as ligações VPN, siga estes passos:

1. No System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP**.

2. Faça clique com o botão direito do rato sobre **Rede Privada Virtual** e, em seguida, seleccione **Predefinições**.
3. Faça clique em **Ajuda** caso tenha questões acerca do preenchimento de uma página ou de qualquer um dos respectivos campos.
4. Faça clique em **OK** após o preenchimento de cada uma das folhas de propriedades.

Repor ligações em estado de erro

Repor ligações com erro devolve-as ao estado de inactividade.

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

1. Em System i Navigator, expanda **servidor** → **Rede** → **Políticas de IP** → **Rede Privada Virtual** → **Ligações Seguras**
2. Faça clique em **Todas as Ligações** para visualizar uma lista de ligações na área de janela 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 que estejam em estado de erro, seleccione cada ligação que pretenda repor, faça clique com o botão direito do rato e seleccione **Repor**.

Ver informações de erro

Conclua esta tarefa para ajudar a determinar a razão do erro na ligação.

Para ver informações sobre ligações com erros, siga estes passos:

1. Em System i Navigator, expanda **servidor** → **Rede** → **Políticas de IP** → **Rede Privada Virtual** → **Ligações Seguras**
2. Faça clique em **Todas as Ligações** para ver uma lista de ligações na área de janela da direita.
3. Faça clique com o botão direito do rato na ligação com erros que quiser ver e seleccione **Informações de Erros**.

Tarefas relacionadas

"Iniciação à detecção e resolução de problemas da VPN" na página 64
Siga esta tarefa para saber os diversos métodos para determinar problemas de VPN que possa ter no sistema.

Ver atributos de ligações activas

Conclua esta tarefa para verificar o estado e outros atributos das ligações activas.

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

1. Em System i Navigator, expanda **servidor** → **Rede** → **Políticas de IP** → **Rede Privada Virtual** → **Ligações Seguras**
2. Faça clique em **Todas as Ligações** para visualizar uma lista de ligações na área de janela da direita.
3. Faça clique com o botão direito do rato sobre a ligação activa ou a pedido que pretende visualizar e seleccione **Propriedades**.
4. Siga para a página **Atributos Actuais** para visualizar os atributos da ligação.

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

1. Em System i Navigator, expanda **servidor** → **Rede** → **Políticas de IP** → **Rede Privada Virtual** → **Ligações Seguras**
2. Faça clique em **Todas as Ligações** para visualizar uma lista de ligações na área de janela 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 System i 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.

Conceitos relacionados

"Mensagens de erro comuns do Gestor de Ligações VPN" na página 78
O Gestor de Ligações VPN regista duas mensagens no ficheiro de registo de trabalhos QTOVMAN quando ocorre um erro numa ligação VPN.

Ver o rastreio do servidor VPN

Permite configurar, iniciar, parar e visualizar os rastreios dos servidores do Gestor de Ligações e de Chaves da VPN. É semelhante à utilização do comando TRCTCPAPP *VPN na interface baseada em caracteres, excepto que pode visualizar o rastreio enquanto a ligação está activa.

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

1. No System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Rede Privada Virtual**, 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 VPN gerem, siga estes passos:

1. Na janela **Rastreio da Rede Privada Virtual**, clique no ícone  (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 em **Ajuda** caso tenha questões acerca do preenchimento de uma página ou de qualquer um dos respectivos campos.
5. Faça clique em **OK** para guardar as alterações.
6. Faça clique em  (Iniciar) para iniciar o rastreio. Clique no  (Actualizar) para ver as informações de rastreio mais recentes.

Ver ficheiros de registo de trabalho do servidor VPN

Siga estas instruções para ver os ficheiros de registo de trabalhos para o Gestor de Chaves e o de Ligações VPN.

Para ver os ficheiros de registo de trabalhos actuais do Gestor de Chaves ou do Gestor de Ligações VPN, siga estes passos:

1. No System i Navigator, expanda **sistema** → **Rede** → **Políticas de IP**.
2. Faça clique com o botão direito do rato sobre **Rede Privada Virtual** e seleccione **Ferramentas de Diagnóstico** e, em seguida, seleccione o ficheiro de registo de trabalhos que pretende ver.

Ver atributos de Associações de Segurança

Conclua esta tarefa para ver os atributos das Associações de Segurança (SAs - Security Associations) associados a uma ligação activada.

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

1. Em System i Navigator, expanda **servidor** → **Rede** → **Políticas de IP** → **Rede Privada Virtual** → **Ligações Seguras**
2. Faça clique em **Todas as Ligações** para visualizar uma lista de ligações na área de janela 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 VPN

Conclua esta tarefa para parar ligações activas.

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

1. Em System i Navigator, expanda **servidor** → **Rede** → **Políticas de IP** → **Rede Privada Virtual** → **Ligações Seguras**
2. Faça clique em **Todas as Ligações** para visualizar uma lista de ligações na área de janela 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 e seleccione **Parar**.

Eliminar objectos da configuração da VPN

Antes de eliminar um objecto da configuração da VPN da base de dados de políticas da VPN, familiarize-se com a maneira em que tal afecta outras ligações e grupos de ligações VPN.

Se tiver a certeza de que necessita de eliminar uma ligação VPN da base de dados de políticas da VPN, siga estes passos:

1. Em System i Navigator, expanda **servidor** → **Rede** → **Políticas de IP** → **Rede Privada Virtual** → **Ligações Seguras**
2. Faça clique em **Todas as Ligações** para ver uma lista de ligações na área de janela da direita.
3. Faça clique com o botão direito do rato sobre a ligação que pretende eliminar e seleccione **Eliminar**.

Detecção e correcção de problemas na VPN

Utilize os seguintes métodos de Detecção e correcção de problemas para resolver alguns problemas básicos com que poderá deparar na configuração de uma ligação VPN.

A VPN é uma tecnologia complexa e em rápida mudança que obriga a pelo menos um conhecimento básico de tecnologias IPSec padrão. Também terá de se familiarizar com as regras de pacote de IP porque a VPN exige várias regras de filtro para funcionar devidamente. Devido a esta complexidade, poderá deparar com problemas nas ligações 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 os gerir. Os tópicos que se seguem fornecem sugestões para a resolução dos vários problemas que pode encontrar durante a utilização da VPN:

Iniciação à detecção e resolução de problemas da VPN

Siga esta tarefa para saber os diversos métodos para determinar problemas de VPN que possa ter no sistema.

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. Não deixe de respeitar os requisitos mínimos de configuração da VPN.
3. Consulte as mensagens de erro que possam existir na janela Informações de Erros ou nos ficheiros de registo de trabalhos do servidor VPN para os sistemas local e remoto. De facto, quando está a resolver problemas na ligação VPN, é muitas vezes necessário olhar para ambos os extremos da ligação. Além disso, é necessário ter em conta que existem quatro endereços que tem de verificar: os terminais de ligações local e remoto, que são os endereços onde a IPSec é aplicada aos pacotes de IP, e os terminais de dados local e remoto, que são os endereços origem e destino dos pacotes de IP.

4. Se as mensagens de erro que encontrar não fornecerem informações suficientes para resolver o problema, consulte o diário do Filtro de IP.
5. O rastreio de comunicações no sistema proporciona outra hipótese de encontrar informações de carácter geral sobre se o sistema local recebe ou envia pedidos de ligação.
6. O comando Trace TCP Application (TRCTCPAPP) proporciona ainda outra forma de isolar os problemas. Normalmente, a Assistência da IBM utiliza TRCTCPAPP para obter saída de dados de rastreio, por forma a analisar problemas de ligação.

Conceitos relacionados

"Requisitos de configuração da VPN" na página 45
Para que uma ligação VPN funcione devidamente nos sistemas e com clientes de rede, terá de cumprir os requisitos mínimos

"Detecção e resolução de problemas da VPN com ficheiros de registo de trabalhos da VPN" na página 77
Quando se deparar com problemas nas ligações VPN, é sempre aconselhável analisar os ficheiros de registo de trabalhos. De facto, existem vários ficheiros de registo de trabalhos que contêm mensagens de erro e outras informações relacionadas com o ambiente de uma VPN.

"Detecção e correcção de problemas da VPN com o rastreio de comunicações" na página 83
O IBM i5/OS fornece a capacidade de rastrear dados numa linha de comunicações, como por exemplo 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.

Tarefas relacionadas

"Ver informações de erro" na página 62
Conclua esta tarefa para ajudar a determinar a razão do erro na ligação.

"Detecção e resolução de problemas da VPN com o diário QIPFILTER" na página 71
Consulte estas informações para saber as regras de filtro da VPN.

"Iniciar uma ligação VPN" na página 61
Conclua esta tarefa para iniciar ligações iniciadas localmente.

Outros 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 VPN em simultâneo, comece com a própria ligação IP. A lista seguinte faculta algumas directrizes básicas para começar a análise dos problemas da VPN, desde a ligação IP mais simples até à ligação VPN mais complexa:

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

   Nota: Lembre-se de facultar informações no comando PING; insira o endereço do sistema remoto e utilize PF10 para parâmetros adicionais, inserindo em seguida o endereço de IP 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 efectuem a filtragem de pacotes de pacotes e que possam estar a filtrar os pacotes PING. O comando PING baseia-se normalmente no protocolo ICMP. Se o comando PING for satisfatório, quer dizer que existe

conectividade. Se o comando PING não for satisfatório, só é possível saber que falhou. Pode optar por tentar outros protocolos IP entre os dois sistemas, tal como Telnet ou FTP para verificar a conectividade.

2. Verifique as regras de filtro 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 System i Navigator. Certifique-se de que as regras de filtro não especificam Conversão de Endereços de Rede (NAT) para qualquer tráfego na VPN.
3. Inicie a ligação 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 têm de 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 VPN.
4. Consegue activar uma sessão de utilizadores na ligação VPN? Se responder **sim**, a ligação VPN funciona como pretendido. Se responder **não**, verifique nas regras de pacotes e nos grupos e ligações de chaves dinâmicas as definições de filtro que não permitem o tráfego de utilizador que pretende.

Erros de configuração comuns da VPN e correcção dos mesmos

Utilize estas informações para rever mensagens de erro de VPN comuns e saber quais as resoluções possíveis.

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 de Segurança do IP e as Ligações Seguras. Assim, quando estas informações se referem a um objecto, referem-se a uma ou mais destas partes da VPN.

Mensagem de erro da VPN: TCP5B28

Quando tenta activar regras de filtro numa interface, recebe esta mensagem: violação da ordem TCP5B28 CONNECTION_DEFINITION

Sintoma:

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

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

Possível resolução:

As regras de filtro 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: Artigo 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 **Artigo não encontrado**.

Sintoma:

Quando faz clique com o botão direito do rato sobre um objecto da janela Rede Privada Virtual e selecciona **Propriedades** ou **Eliminar**, surge a mensagem seguinte:

Possível resolução:

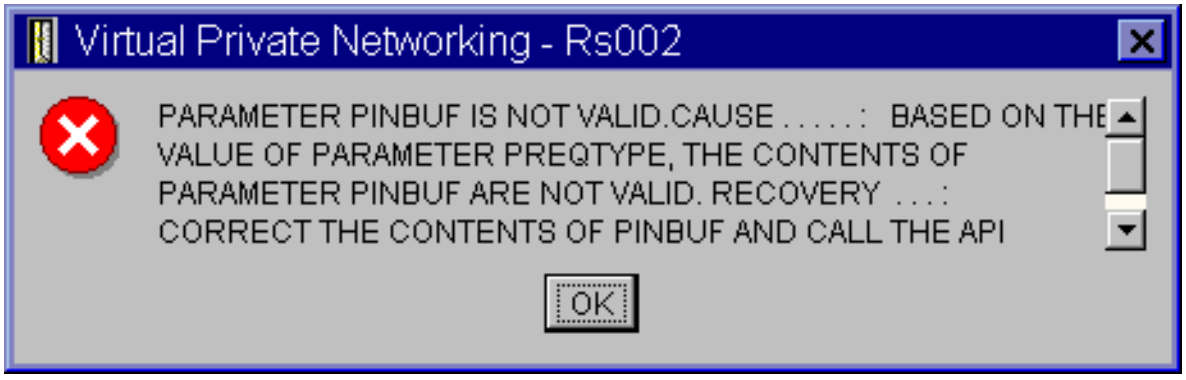
- Poderá ter eliminado o objecto ou mudado o nome do mesmo e ainda não actualizou a janela. Desta forma, o objecto ainda é apresentado na janela Rede Privada Virtual. Para verificar se é este o caso, no menu **Ver**, seleccione **Actualizar**. Se o objecto ainda surgir na janela Rede Privada Virtual, prossiga para o próximo artigo da lista.
- Quando configurou as propriedades do objecto, poderá ter ocorrido um erro de comunicação entre o servidor VPN e o seu sistema. Muitos dos objectos que são apresentados na janela VPN 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 predefinições). 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. Tal actualiza todas as ligações à base de dados de políticas VPN que se perderam. Pode agora eliminar o objecto.

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

Quando tenta iniciar uma ligação, recebe uma mensagem que diz: **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: Artigo não encontrado, Servidor de chaves remotas...

Quando seleccionar **Propriedades** para uma ligação de chaves dinâmicas, recebe um erro que diz que o servidor não consegue encontrar o servidor de chaves especificado.

Sintoma:

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

Possível resolução:

Tal acontece quando se cria uma ligação a determinado identificador de servidor de chaves remotas e depois o servidor de chaves remotas é removido do respectivo grupo de chaves dinâmicas. Para corrigir este erro, faça clique em **OK** na mensagem de erro. Abre a folha de propriedades da ligação de chaves dinâmicas que tem erro. A partir daqui, pode voltar adicionar o servidor de chaves remotas ao grupo de chaves dinâmicas ou seleccionar outro identificador de servidor de chaves remotas. Faça clique em **OK** na folha de propriedades, para guardar as alterações.

Mensagem de erro da VPN: Não foi 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.

Sintoma:

Ao seleccionar **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 foi possível codificar a chave...

Recebe uma mensagem em como o sistema não consegue consegue codificar as chaves, porque o valor QRETSVRSEC tem de estar definido como 1.

Sintoma:

Surge 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 como 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**.

Conceitos relacionados

"Erro da VPN: 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.

Mensagem de erro da VPN: CPF9821

Quando tentar expandir ou abrir o contentor Políticas de IP no System i Navigator, aparece a mensagem CPF9821- Não tem autorização para programar QTFRPRS na biblioteca QSYS.

Sintoma:

Quando tentar expandir o contentor Políticas de IP no System i Navigator, aparece a mensagem `CPF9821- Não tem autorização para 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 VPN. Assegure-se de que tem autoridade *IOSYSCFG para ter acesso às funções das Regras de Pacotes no System i Navigator.

Erro da VPN: 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.

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. A definição deste valor de sistema como 0 apaga todas as chaves da base de dados da política da VPN. Para corrigir este problema, tem de definir o valor de sistema como 1 e, depois, voltar a inserir todas as chaves. Consulte a Mensagem de Erro: Não é possível codificar chaves, para obter mais informações sobre a forma como proceder.

Conceitos relacionados

"Mensagem de erro da VPN: Não foi possível codificar a chave..." na página 68
Recebe uma mensagem em como o sistema não consegue consegue codificar as chaves, porque o valor QRETSVRSEC tem de estar definido como 1.

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

A primeira que utiliza a interface Regras de Pacotes no System i Navigator, é apresentado um ecrã de início de sessão num sistema diferente do actual.

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 System i Access for Windows obter a tabela de conversão apropriada para Unicode. Tal só acontecerá uma vez.

Erro da VPN: Estado da ligação em branco na janela do System i Navigator

Uma ligação não tem nenhuma valor na coluna **Estado** na janela System i Navigator.

Sintoma:

Uma ligação não tem nenhuma valor na coluna **Estado** na janela System i Navigator.

Possível resolução:

O valor de estado em branco indica que o início da ligação está em curso. Por outras palavras, ainda não está a ser executada, mas também ainda não teve erro algum. Quando actualizar a janela, a ligação vai apresentar estado `Erro`, `Activa`, `A Pedido` ou `Inactiva`.

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

Depois de parar uma ligação, a janela System i Navigator indica que a ligação ainda está activa.

Sintoma:

Depois de parar uma ligação, a janela System i Navigator indica que a ligação ainda está activa.

Possível resolução:

Isto acontece, normalmente, por ainda não ter actualizado a janela do System i 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

Não é possível escolher uma codificação de algoritmo 3DES quando trabalha com uma transformação de políticas de IKE, uma transformação de políticas de dados ou uma ligação manual.

Sintoma:

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

Possível resolução:

O mais provável é que tenha apenas o Cryptographic Access Provider (5722-AC2) instalado no sistema e não o Cryptographic Access Provider (5722-AC3). O Cryptographic Access Provider (5722-AC2) só permite o algoritmo de codificação Data Encryption Standard (DES), devido a restrições impostas ao comprimento das chaves. Os Cryptographic Access Provider (5722-AC2) e (5722-AC3) já não são necessários para activar codificação de dados em sistemas que executem i5/OS V5R4 ou posterior.

Erro da VPN: São apresentadas colunas inesperadas na janela System i Navigator

Defina as colunas que pretende visualizar na janela System i Navigator para as ligações VPN; quando mais tarde as visualizar, serão apresentadas colunas diferentes.

Sintoma:

Configurou as colunas que pretende visualizar na janela System i Navigator para as ligações VPN; quando mais tarde as visualizou, foram apresentadas colunas diferentes.

Possível resolução:

Quando altera as colunas para visualização, as alterações não são específicas a uma determinado utilizador ou PC, englobam sim o 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 filtro activas não foram desactivadas

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

Sintoma:

Quando tenta desactivar o conjunto de regras de filtro 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 VPN activa. Tem de parar cada uma das ligações com estado `activada`. Para o fazer, faça clique com o botão direito do rato em cada ligação activa e seleccione **Parar**. Pode agora desactivar as regras de filtro.

Erro da VPN: O grupo de ligações por chaves de uma ligação foi alterado

Quando criar uma ligação de chave dinâmica, irá especificar um grupo de chaves dinâmicas e um identificador para o servidor de chaves remotas. Mais tarde, quando vir as propriedades do objecto da ligação associado, a página Geral da folha de propriedades apresenta o mesmo identificador do servidor de chaves remotas, mas um grupo de chaves dinâmicas diferentes.

Sintoma:

Quando criar uma ligação de chave dinâmica, irá especificar um grupo de chaves dinâmicas e um identificador para o servidor de chaves remotas. Mais tarde, quando seleccionar **Propriedades** no objecto de ligação associado, a página **Geral** da folha de propriedades apresenta o mesmo identificador de servidor de chaves remotas, 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 remotas da ligação de chave dinâmica. Quando a VPN procura uma política para um servidor de chaves remotas, procura o primeiro grupo de chaves dinâmicas que tiver esse identificador de servidor de chaves remotas. Por isso, quando vir as propriedades de uma destas ligações, esta utiliza o mesmo grupo de chaves dinâmicas que a VPN encontrou. Se não quiser associar o grupo de chaves dinâmicas àquele servidor de chaves remotas, pode proceder de uma das seguintes formas:

1. Remova o servidor de chaves remotas do grupo de chaves dinâmicas.
2. Expanda **Por Grupos** na área de janela da esquerda da interface de VPN e seleccione e arraste o grupo de chaves dinâmicas pretendido para a parte superior da tabela no área de janela da direita. Tal garante que a VPN verifica primeiro este grupo de chaves dinâmicas para o servidor de chaves remotas.

Detecção e resolução de problemas da VPN com o diário QIPFILTER

Consulte estas informações para saber as regras de filtro da VPN.

O diário QIPFILTER está localizado na biblioteca QUSRSYS e contém informações sobre conjuntos de regras de filtro, 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 filtro.

Tarefas relacionadas

"Iniciação à detecção e resolução de problemas da VPN" na página 64
Siga esta tarefa para saber os diversos métodos para determinar problemas de VPN que possa ter no sistema.

Activar o diário QIPFILTER

Utilize o editor de Regras de Pacotes no System i Navigator para activar o diário QIPFILTER.

| Tem de activar a função de registo para cada regra de filtro 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 têm de estar desactivados.

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

| 1. No System i Navigator, expanda **sistema** → **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 filtro existentes.
| 4. Faça duplo clique sobre a regra de filtro que pretende registar em diário.
| 5. Na página **Geral**, seleccione **FULL** no campo **Registo em diário** conforme a caixa de diálogo
| apresentada acima. Esta acção activa o registo desta regra de filtro específica.
| 6. Faça clique em **OK**.
| 7. Guarde e active o ficheiro de regras de filtro alterado.

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

Utilizar o diário QIPFILTER

O i5/OS cria automaticamente o diário da primeira vez que activar a filtro do pacote de IP.

Para visualizar os detalhes específicos de uma entrada do diário, pode visualizar as entradas do diário no ecrã ou utilizar um ficheiro de saída de dados. Ao copiar as entradas do diário para um ficheiro de saída de dados, pode facilmente ver 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 saída de dados.

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 saída de dados:

1. Crie uma cópia do ficheiro de saída de dados 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 saída de dados que criou no passo anterior.

Se copiar o DSPJRN para um ficheiro de saída de dados que não existe, o sistema cria um ficheiro, mas este não contém as descrições de campo correctas.

Nota: O diário QIPFILTER contém apenas entradas de permissão e recusa das regras de filtro em que a opção de registo em diário está definida como FULL. Por exemplo, se configurar apenas as regras de filtro PERMIT, os datagramas de IP que não forem explicitamente autorizados são recusados. Para os datagramas recusados, não é adicionada nenhuma entrada no diário. Para a análise de problemas, poderá adicionar uma regra de filtro que recuse explicitamente qualquer outro tráfego e execute um registo em diário FULL. Assim, 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 filtro. Assim que os conjuntos de filtros forem testados, reduza o registo em diário para um subconjunto de entradas útil.

Conceitos relacionados

"Campos do diário QIPFILTER"
Reveja a tabela seguinte que descreve os campos do ficheiro de saída de dados do QIPFILTER

Campos do diário QIPFILTER

Reveja a tabela seguinte que descreve os campos do ficheiro de saída de dados do QIPFILTER

Nome do Campo	Comprimento do Campo	Numérico	Descrição	Comentários
TFENTL	5	S	Comprimento da Entrada	
TFSEQN	10	S	Número da sequência	
TFCODE	1	N	Código do 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 de 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 da 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 filtro
TFPDIR	1	N	Direcção de Pacotes IP	O é de partida, I é de chegada
TFRNUM	5	N	Número da regra	Aplica-se ao número da regra no ficheiro de regras activas
TFACT	6	N	Acção de filtro efectuada	PERMIT, DENY ou IPSEC

Nome do Campo	Comprimento do Campo	Numérico	Descrição	Comentários
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 de 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*

Tarefas relacionadas

"Utilizar o diário QIPFILTER" na página 72
O i5/OS cria automaticamente o diário da primeira vez que activar a filtro do pacote de IP.

Detecção e resolução de problemas da VPN com o diário QVPN

Este tópico fornece informações acerca do tráfego IP e das ligações.

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.

Activar o diário QVPN

Utilize a interface da rede privada virtual no System i Navigator para activar o diário da VPN.

Não existe uma função que permita o registo em todas as ligações VPN. Deste modo, tem de activar a função de registo em diário para cada grupo de chaves dinâmicas individual ou ligação manual.

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 System i Navigator, expanda **sistema → Rede → Políticas de IP → Rede Privada Virtual → 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 nenhum 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, 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 filtro. O sistema grava as informações de tráfego IP no diário QIPFILTER, que se encontra na biblioteca QUSRSYS.

5. Faça clique em **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.

Utilizar o diário QVPN

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

Ao copiar as entradas do diário para o ficheiro de saída de dados, pode facilmente ver 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 saída de dados. 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 saída de dados:

.

1. Crie uma cópia do ficheiro de saída de dados 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 saída de dados que criou no passo anterior. Se tentar copiar DSPJRN para um ficheiro de saída de dados que não existe, o sistema cria um ficheiro para si, mas este não contém as descrições do campo apropriadas.

   Conceitos relacionados

   "Campos do diário QVPN"
   Reveja a tabela seguinte que descreve os campos do ficheiro de saída de dados QVPN.

Campos do diário QVPN

Reveja a tabela seguinte que descreve os campos do ficheiro de saída de dados QVPN.

Nome do Campo	Comprimento do Campo	Numérico	Descrição	Comentários
TSENTL	5	S	Comprimento da Entrada	

Nome do Campo	Comprimento do Campo	Numérico	Descrição	Comentários
TSSEQN	10	S	Número da sequência	
TSCODE	1	N	Código do diário	Sempre M
TSENTT	2	N	Tipo de entrada	Sempre TS
TSTIME	26	N	Marca de hora 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 de 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	Terminal local	
TSREP	43	N	Terminal remoto	
TSCORF	6	N	Número de actualizações	
TSRFDA	8	N	Data da próxima actualização	
TSRFTI	6	N	Hora da próxima actualização	

Nome do Campo	Comprimento do Campo	Numérico	Descrição	Comentários
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	

Tarefas relacionadas

"Utilizar o diário QVPN" na página 75
Para visualizar os detalhes específicos de uma entrada do diário da VPN, pode visualizar as entradas no ecrã ou utilizar o ficheiro de saída de dados.

Detecção e resolução de problemas da VPN com ficheiros de registo de trabalhos da VPN

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

É importante que analise os ficheiros de registo de trabalhos de ambos os extremos da ligação, caso estes sejam ambos modelos System i. Quando uma ligação dinâmica não iniciar, será útil perceber o que está a acontecer no sistema remoto.

Os ficheiros de registo de trabalhos da VPN, QTOVMAN e QTOKVPNIKE, são executados no subsistema QSYSWRK. Pode visualizar os respectivos ficheiros de registo de trabalhos no System i 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 TCP/IP em geral, analise o ficheiro de registo de trabalhos QTCPIP.

QTOKVPNIKE
O trabalho QTOKVPNIKE é o trabalho do gestor de chaves da VPN. O gestor de chaves 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 VPN. O registo de trabalhos associado contém mensagens de todas as tentativas de ligação falhadas.

QTPPANS*xxx*
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 Layer Two Tunneling Protocol (L2TP). Se tiver problemas na configuração de um túnel de L2TP, verifique a existência de mensagens neste registo de trabalhos.

Tarefas relacionadas

"Iniciação à detecção e resolução de problemas da VPN" na página 64
Siga esta tarefa para saber os diversos métodos para determinar problemas de VPN que possa ter no sistema.

Mensagens de erro comuns do Gestor de Ligações VPN

O Gestor de Ligações VPN regista duas mensagens no ficheiro de registo de trabalhos QTOVMAN quando ocorre um erro numa ligação VPN.

A primeira mensagem fornece detalhes relacionados com o erro. Pode ver informações sobre estes erros no System i Navigator fazendo clique com o botão direito do rato na ligação com erros e seleccionando **Informações de 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 VPN

Mensagem	Causa	Recuperação
TCP8601 Não foi possível iniciar a ligação VPN [*nome da ligação*]	Não foi possível iniciar esta ligação VPN devido a um destes códigos de razão: *0* - Uma mensagem anterior no registo de trabalhos com o mesmo nome de ligação 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 terminal remoto para esta ligação não está configurado correctamente. *5* - O Gestor de Chaves da VPN não conseguiu responder ao Gestor de Ligações VPN. *6* - Falha no carregamento da ligação VPN no Componente IP Security. *7* - Falha no Componente PPP.	1. Verifique se existem mensagens adicionais nos ficheiros de registo de trabalhos. 2. Corrija os erros e repita o pedido. 3. Com o System i Navigator, veja o estado da ligação. As ligações que não conseguiram iniciar apresentam estado de erro.
TCP8602 Ocorreu um erro ao parar a ligação VPN [*nome da ligação*]	Foi feito um pedido para que a ligação 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 VPN tem informações mais detalhadas. *1* - A ligação 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 terminal remoto da ligação VPN.	1. Verifique se existem mensagens adicionais nos ficheiros de registo de trabalhos. 2. Corrija os erros e repita o pedido. 3. Com o System i Navigator, veja o estado da ligação. As ligações que não conseguiram iniciar apresentam estado com erro.

Mensagens de erro do Gestor de Ligações VPN

Mensagem	Causa	Recuperação
TCP8604 Ocorreu uma falha ao iniciar a ligação VPN [*nome da ligação*]	Ocorreu uma falha ao iniciar esta ligação VPN devido a um destes códigos de razão: *1* - Não foi possível converter o nome do sistema central remoto num endereço de IP. *2* - Não foi possível converter o nome do sistema central local num endereço de IP. *3* - A regra de filtro de políticas da VPN associada a esta ligação 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 VPN não permite a acção especificada. *6* - Uma função do sistema para a ligação VPN é incoerente com informações do grupo de ligações. *7* - Reservado. *8* - Os terminais de dados (endereços e serviços locais e remotos) desta ligação VPN estão incoerentes com informações do grupo de ligações. *9* - Tipo de identificador não válido.	1. Verifique se existem mensagens adicionais nos ficheiros de registo de trabalhos. 2. Corrija os erros e repita o pedido. 3. Utilize o System i Navigator para verificar ou corrigir a configuração de 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 VPN não conseguiu comunicar com o Gestor de Chaves da VPN	O Gestor de Ligações VPN requer os serviços do Gestor de Chaves da VPN para estabelecer associações de segurança para ligações dinâmicas VPN. O Gestor de Ligações VPN não conseguiu comunicar com o Gestor de Chaves da VPN.	1. Verifique se existem mensagens adicionais nos ficheiros de registo de trabalhos. 2. Verifique se a interface *LOOPBACK está activa com o comando NETSTAT OPTION(*IFC). 3. Termine o servidor VPN com o comando ENDTCPSVR SERVER(*VPN). Em seguida, reinicie o servidor VPN com o comando STRTCPSRV SERVER(*VPN). **Nota:** Esta acção termina todas as ligações VPN.

Mensagens de erro do Gestor de Ligações VPN

Mensagem	Causa	Recuperação
TCP8606 O Gestor de Chaves da VPN não conseguiu estabelecer a associação de segurança solicitada para a ligação, [*nome da ligação*]	O Gestor de Chaves da VPN não conseguiu estabelecer a associação de segurança solicitada devido a um destes códigos de razão: *24* - A autenticação da ligação de chaves do Gestor de Chaves da VPN não foi bem sucedida. *8300* - Ocorrência de falha durante as negociações de ligações de chaves do Gestor de Chaves da VPN. *8306* - Não foi encontrada nenhuma chave pré-partilhada local. *8307* - Não foi encontrada nenhuma política de fase 1 do IKE remoto. *8308* - Não foi encontrada nenhuma 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 VPN do Gestor de Chaves da VPN. *8407* - Não foi encontrada nenhuma política de fase 2 do IKE remoto. *8408* - O tempo de espera das negociações da ligação 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 ficheiros de registo de trabalhos. 2. Corrija os erros e repita o pedido. 3. Utilize o System i Navigator para verificar ou corrigir a configuração de política da VPN. Certifique-se de que o grupo de chaves dinâmicas associado a esta ligação tem valores aceitáveis configurados.
TCP8608 A ligação 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 aplicar a NAT não é um endereço único de IP. *2* - Todos os endereços disponíveis foram utilizados.	1. Verifique se existem mensagens adicionais nos ficheiros de registo de trabalhos. 2. Corrija os erros e repita o pedido. 3. Com o System i Navigator pode verificar ou corrigir a política de VPN. Certifique-se de que o grupo de chaves dinâmicas associado a esta ligação tem valores aceitáveis para endereços configurados.
TCP8620 O terminal da ligação local não está disponível	Não foi possível activar esta ligação VPN, uma vez que o terminal da ligação local não estava disponível.	1. Verifique se existem mensagens adicionais nos ficheiros de registo de trabalhos referentes a esta ligação. 2. Certifique-se de que o terminal da ligação local está definido e que foi iniciado com o comando NETSTAT OPTION(*IFC). 3. Corrija erros e repita o pedido.

Mensagens de erro do Gestor de Ligações VPN

Mensagem	Causa	Recuperação
TCP8621 O terminal de dados local não está disponível	Não foi possível activar esta ligação VPN, uma vez que o terminal de dados local não estava disponível.	1. Verifique se existem mensagens adicionais nos ficheiros de registo de trabalhos referentes a esta ligação. 2. Certifique-se de que o terminal da ligação local está definido e que foi iniciado com o comando NETSTAT OPTION(*IFC). 3. Corrija erros e repita o pedido.
TCP8622 O encapsulamento de transporte não é permitido com uma porta de ligação	Não foi possível activar esta ligação VPN, uma vez que a política negociada especificou o modo de encapsulamento de transporte e esta ligação está definida como porta de ligação de segurança.	1. Verifique se existem mensagens adicionais nos ficheiros de registo de trabalhos referentes a esta ligação. 2. Utilize o System i Navigator para alterar a política da VPN associada a esta ligação. 3. Corrija erros e repita o pedido.
TCP8623 A ligação VPN sobrepõe-se a uma existente	Não foi possível activar esta ligação VPN, uma vez que uma ligação VPN existente já está activada. Esta ligação tem um terminal de dados local de [*valor do terminal de dados local*] e um terminal de dados remoto de [*valor do terminal de dados remoto*].	1. Verifique se existem mensagens adicionais nos ficheiros de registo de trabalhos referentes a esta ligação. 2. Utilize o System i Navigator para ver todas as ligações activadas com terminais de dados locais e remotos que se sobreponham à ligação. Altere a política da ligação existente se ambas as ligações forem necessárias. 3. Corrija erros e repita o pedido.
TCP8624 A ligação VPN não se encontra dentro do âmbito da regra de filtro de políticas associada	Não foi possível activar esta ligação VPN, uma vez que os terminais de dados não se encontram dentro da regra de filtro de políticas definida.	1. Verifique se existem mensagens adicionais nos ficheiros de registo de trabalhos referentes a esta ligação. 2. Utilize o System i Navigator para ver as restrições do terminal de dados para esta ligação ou para este grupo de chaves dinâmicas. Se a opção **Subconjunto de filtros de políticas** ou **Personalizar para corresponder ao filtro de políticas** estiver seleccionada, verifique os terminais de dados da ligação. Estes têm de caber na regra de filtro activa com uma acção IPSEC e um nome de ligação VPN associado a esta ligação. Altere a política da ligação existente ou a regra de filtro para activar esta ligação. 3. Corrija erros e repita o pedido.

Mensagens de erro do Gestor de Ligações VPN

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

Mensagens de erro do Gestor de Ligações VPN

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

Tarefas relacionadas

"Ver atributos de ligações activas" na página 62
Conclua esta tarefa para verificar o estado e outros atributos das ligações activas.

Detecção e correcção de problemas da VPN com o rastreio de comunicações

O IBM i5/OS fornece a capacidade de rastrear dados numa linha de comunicações, como por exemplo 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 de 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. A predefinição 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 partida (*SND), apenas tráfego de chegada (*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. A predefinição 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. 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 nenhumas informações importantes.

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

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

Parar o rastreio de comunicações

Se não existirem indicações em contrário, o rastreio pára assim que ocorrer a condição que estiver a ser rastreada. 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 de 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, dispõe de diversas opções de filtros para geração de saída de dados. Tente que o ficheiro em spool se mantenha tão pequeno quanto o possível. Isto torna a análise mais rápida e eficiente. No caso de ocorrer um problema com a VPN, apenas deve filtrar o tráfego de 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 de 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 predefinido é sim. Se não quiser, por exemplo, pedidos Address Resolution Protocol (ARP), especifique *NO; caso contrário, pode ficar sobrecarregado com mensagens de difusão.

Tarefas relacionadas

"Iniciação à detecção e resolução de problemas da VPN" na página 64
Siga esta tarefa para saber os diversos métodos para determinar problemas de VPN que possa ter no sistema.

Informações relacionadas com a VPN

As publicações e os sítios na Web IBM Redbooks contêm informações relacionadas com o conjunto de tópicos Funcionamento em Rede Privada Virtual. Poderá ver ou imprimir qualquer dos ficheiros PDF.

IBM Redbooks

- IBM System i Security Guide for IBM i5/OS Version 5 Release 4
- AS/400 Internet Security: Implementing AS/400 Virtual Private Networks
- AS/400 Internet Security Scenarios: A Practical Approach
- OS/400 V5R2 Virtual Private Networks: Remote Access to the IBM eServer iSeries Server with Windows 2000 VPN Clients

Sítios na Web

- TCP/IP for i5/OS: Virtual Private Networking
- TCP/IP for i5/OS: RFC Documents

Apêndice. Avisos

Estas informações foram desenvolvidas para produtos e serviços disponibilizados nos E.U.A.

Os produtos, serviços ou funções descritos neste documento poderão não ser disponibilizados pelo fabricante noutros países. Consulte o representante do fabricante para obter informações sobre os produtos e serviços actualmente disponíveis na sua área. Quaisquer referências, nesta publicação, a produtos, programas ou serviços do fabricante, não significam que apenas esses produtos, programas ou serviços possam ser utilizados. Qualquer outro produto, programa ou serviço, funcionalmente equivalente, poderá ser utilizado em substituição daqueles, desde que não infrinja qualquer direito de propriedade intelectual do fabricante. No entanto, é da inteira responsabilidade do utilizador avaliar e verificar o funcionamento de qualquer produto, programa ou serviço alheio à IBM.

Nesta publicação, podem ser feitas referências a patentes ou a pedidos de patente pendentes. O facto de este documento lhe ser fornecido não lhe confere quaisquer direitos sobre essas patentes. Todos os pedidos de informação sobre licenças deverão ser endereçados ao fabricante, para:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Para pedidos de licença relativos a informações de duplo byte (DBCS), contacte o IBM Intellectual Property Department do seu país ou envie pedidos por escrito para:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

O parágrafo seguinte não se aplica ao Reino Unido nem a qualquer outro país onde estas cláusulas sejam incompatíveis com a lei local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO ""TAL COMO ESTÁ"" SEM GARANTIA DE QUALQUER ESPÉCIE, QUER EXPLÍCITA QUER IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE NÃO INFRACÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO FIM. Alguns Estados não permitem a exclusão de garantias, quer explícitas quer implícitas, em determinadas transacções; esta declaração pode, portanto, não se aplicar ao seu caso.

É possível que estas informações contenham imprecisões técnicas ou erros de tipografia. O fabricante permite-se fazer alterações periódicas às informações aqui contidas; essas alterações serão incluídas nas posteriores edições desta publicação. O fabricante pode introduzir melhorias e/ou alterações ao(s) produto(s) e/ou programa(s) descrito(s) nesta publicação em qualquer altura sem aviso prévio.

Quaisquer referências, nesta publicação, a sítios da Web que não sejam propriedade do fabricante são fornecidas apenas para conveniência e não deverão nunca servir como aprovação desses sítios da Web. Os materiais existentes nesses sítios da Web não fazem parte dos materiais destinados a este produto e a utilização desses sítios da Web será da exclusiva responsabilidade do utilizador.

O fabricante pode utilizar ou distribuir qualquer informação que lhe seja fornecida pelo utilizador, de qualquer forma que julgue apropriada, sem incorrer em qualquer obrigação para com o autor dessa informação.

Os Licenciados deste programa que pretendam obter informações sobre o mesmo com o objectivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) a utilização recíproca das informações que tenham sido trocadas, deverão contactar a IBM através do seguinte endereço:

IBM Portuguesa
Edifício Office Oriente
Rua do Mar da China, Lote 1.07.2.3
Parque das Nações
1990-039 Lisboa

Tais informações poderão estar disponíveis, sujeitas aos termos e às condições adequados, incluindo, em alguns casos, o pagamento de um encargo.

O programa licenciado descrito neste documento e todo o material licenciado disponível para o programa são fornecidos pela IBM nos termos das Condições Gerais IBM (IBM Customer Agreement), Acordo de Licença Internacional para Programas IBM (IPLA, IBM International Program License Agreement), Acordo de Licença para Código Máquina IBM (IBM License Agreement for Machine Code) ou de qualquer acordo equivalente entre ambas as partes.

Quaisquer dados de desempenho aqui contidos foram determinados num ambiente controlado. Assim sendo, os resultados obtidos noutros ambientes operativos podem variar significativamente. Algumas medições podem ter sido efectuadas em sistemas ao nível do desenvolvimento, pelo que não existem garantias de que estas medições sejam iguais nos sistemas disponíveis habitualmente. Para além disso, algumas medições podem ter sido calculadas por extrapolação. Os resultados reais podem variar. Os utilizadores deste documento devem verificar os dados aplicáveis ao seu ambiente específico.

As informações relativas a produtos não IBM foram obtidas junto dos fornecedores desses produtos, dos seus anúncios publicados ou de outras fontes de divulgação ao público. A IBM não testou esses produtos e não pode confirmar a exactidão do desempenho, da compatibilidade ou de quaisquer outras afirmações relacionadas com produtos não IBM. Todas as questões sobre as capacidades dos produtos não IBM deverão ser endereçadas aos fornecedores desses produtos.

Todas as afirmações relativas às directivas ou tendências futuras da IBM estão sujeitas a alterações ou descontinuação sem aviso prévio, representando apenas metas e objectivos.

Estas informações contêm exemplos de dados e relatórios utilizados em operações comerciais diárias. Para os ilustrar o melhor possível, os exemplos incluem nomes de indivíduos, firmas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com nomes e moradas reais é mera coincidência.

LICENÇA DE COPYRIGHT:

Esta publicação contém programas de aplicações exemplo em linguagem de origem, os quais pretendem ilustrar técnicas de programação em diversas plataformas operativas. Poderá copiar, modificar e distribuir estes programas exemplo sem qualquer encargo para com a IBM, no intuito de desenvolver, utilizar, comercializar ou distribuir programas de aplicação conformes à interface de programação de aplicações relativa à plataforma operativa para a qual tais programas exemplo foram escritos. Estes exemplos não foram testados exaustivamente nem em todas as condições. Por conseguinte, a IBM não pode garantir a fiabilidade ou o funcionamento destes programas.

Cada cópia ou qualquer parte destes programas exemplo ou qualquer trabalho derivado dos mesmos tem de incluir um aviso de direitos de autor, do seguinte modo:

© (o nome da sua empresa) (ano). Algumas partes deste código são derivadas de Programas Exemplo da IBM Corporation. © Copyright IBM Corp. _introduza o(s) ano(s)_. Todos os direitos reservados.

Se estiver a consultar as informações neste documento electrónico, é possível que as fotografias e as ilustrações a cores não estejam visíveis.

Informações sobre interfaces de programação

Esta publicação sobre redes privadas virtuais documenta as Interfaces de Programação que permitem ao cliente escrever programas para obter serviços do IBM i5/OS.

Marcas comerciais

Os termos seguintes são marcas comerciais da International Business Machines Corporation nos Estados Unidos e/ou noutros países:

Approach
AS/400
Balance
eServer
i5/OS
IBM
iSeries
OS/400
SAA
System i

Adobe, o logótipo Adobe, PostScript e o logótipo PostScript são marcas comerciais ou registadas da Adobe Systems Incorporated nos Estados Unidos e/ou noutros países.

Microsoft, Windows, Windows NT e o logótipo do Windows são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou noutros países.

Outros nomes de empresas, produtos e serviços podem ser marcas comerciais ou marcas de serviço de terceiros.

Termos e condições

As permissões de utilização destas publicações são concedidas sujeitas aos termos e condições seguintes.

Utilização pessoal: Pode reproduzir estas publicações para uso pessoal e não comercial, desde que mantenha todas as informações de propriedade. Não pode executar qualquer trabalho derivado destas publicações, nem reproduzir, distribuir ou apresentar qualquer parte das mesmas, sem o expresso consentimento do fabricante.

Utilização comercial: Pode reproduzir, distribuir e apresentar estas publicações exclusivamente no âmbito da sua empresa, desde que mantenha todas as informações de propriedade. Não pode executar qualquer trabalho derivado destas publicações, nem reproduzir, distribuir ou apresentar estas publicações, ou qualquer parte das mesmas fora das instalações da empresa, sem o expresso consentimento do fabricante.

À excepção das concessões expressas nesta permissão, não são concedidos outros direitos, permissões ou licenças, quer explícitos, quer implícitos, sobre as publicações ou quaisquer informações, dados, software ou outra propriedade intelectual contidos nesta publicação.

O fabricante reserva-se o direito de retirar as permissões concedidas nesta publicação sempre que considerar que a utilização das publicações pode ser prejudicial aos seus interesses ou, tal como determinado pelo fabricante, sempre que as instruções acima referidas não estejam a ser devidamente cumpridas.

Não pode descarregar, exportar ou reexportar estas informações, excepto quando em total conformidade com todas as leis e regulamentos aplicáveis, incluindo todas as leis e regulamentos de exportação em vigor nos E.U.A.

O FABRICANTE NÃO GARANTE O CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS ″TAL COMO ESTÃO″ (AS IS) E SEM GARANTIAS DE QUALQUER ESPÉCIE, QUER EXPLÍCITAS, QUER IMPLÍCITAS, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO, NÃO INFRACÇÃO E ADEQUAÇÃO A UM DETERMINADO FIM.