**Configurando Túneis IPSec “Puros” com o ISA Server 2006**

**Por Rogério Silva**

**Data de criação: 08/11/2007**

**Resumo**

**Esta coluna descreve os passos para se configurar uma VPN Site-To-Site usando IPSec “Puro” no Microsoft ISA Server 2006, mostrando os benefícios do uso desta tecnologia.**

**Observação importante**

Este artigo técnico foi escrito por um membro da comunidade brasileira e não é um documento oficial Microsoft. A Microsoft Corporation e a Microsoft Brasil não fornecem quaisquer garantias, explícitas ou expressas, sobre o conteúdo deste documento, nem concorda necessariamente com opiniões pessoais dos colunistas, bem como não se responsabiliza por danos causados por procedimentos técnicos descritos nestas colunas.

**Este artigo aplica-se aos seguintes produtos e tecnologias:**

* Microsoft ISA Server 2006
* Windows Server 2003 com Service Pack 2
* VPN
* IPSec

**Introdução**

Os Túneis VPN IPSec trazem uma série de benefícios e vantagens inerentes a uma plataforma flexível onde podemos garantir a confidencialidade das informações por eles trafegados. Podemos relacionar vantagens como **autenticação**, **autorização**, **auditoria**, **integridade**, **não-repúdio** e **privacidade**.

Antes de prosseguirmos, é necessário ter conhecer mais alguns aspectos das conexões VPN.

Em redes TCP/IP temos basicamente três tipos mais comuns de VPN: **PPTP** – Fácil de configurar e com métodos simples (mas não inseguros) de autenticação, **L2TP sobre IPSec** – VPN tradicionalmente adotada por empresas que exigem um nível mais alto de segurança do que o PPTP através do uso de IPSec, e **Túneis IPSec “puros”** – Adotam um esquema de tunelamento mais enxuto do que o L2TP, mantendo a compatibilidade com outras soluções, mas reduzir a segurança.

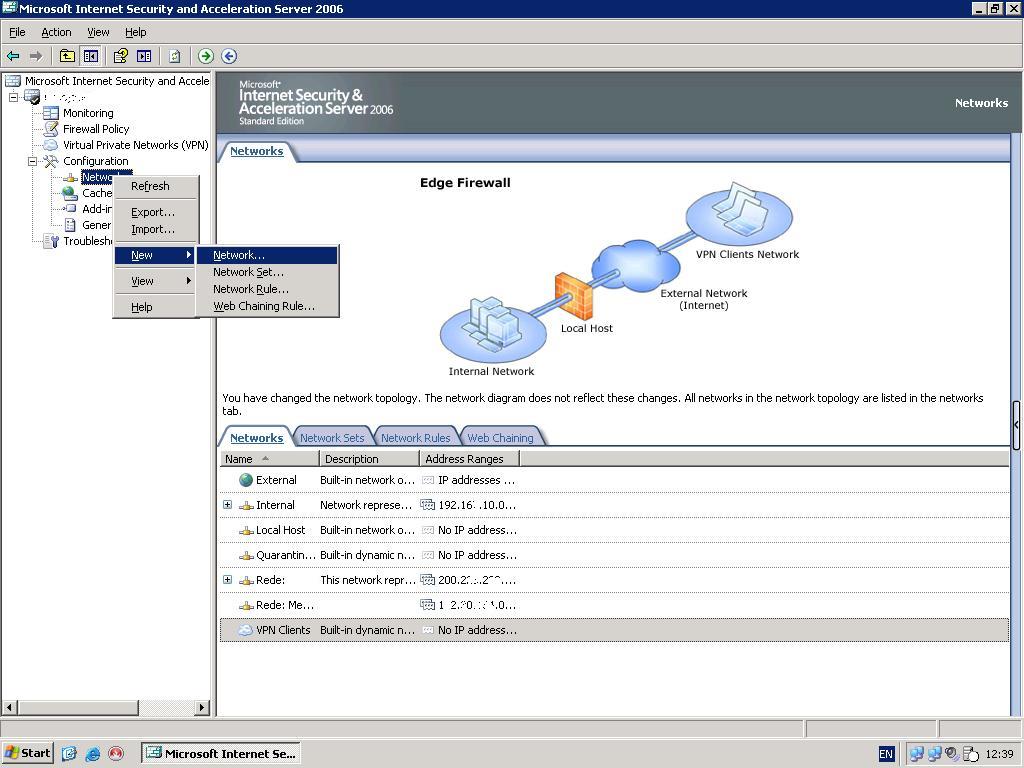
Os túneis puros IPSec adotam um esquema de conexão por “fases” (ou etapas), onde são estabelecidas as configurações de segurança para cada uma delas. A Fase 1, ou modo principal do IKE, define o canal inicial seguro para autenticação e por onde o restante das informações serão trafegadas. A Fase 2 é o modo rápido do IKE e é onde o tráfego é protegido através do ESP, o qual fica responsável pela confidencialidade, integridade e autenticação.

Ambas as pontas (endpoints) do túnel devem ter exatamente as mesmas configurações para que eles possam estabelecer o túnel e manter a conexão.

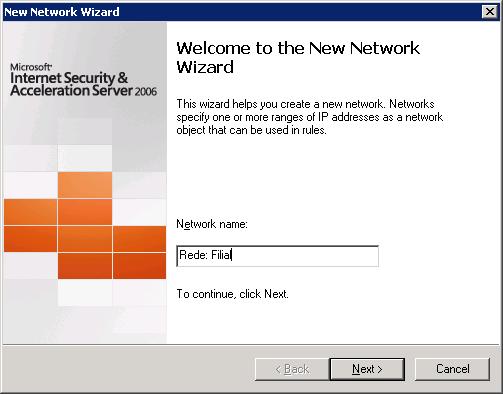
**Criando uma rede para IPSec VPN Site-To-Site**

Nesta etapa efetuaremos a configuração inicial do túnel VPN IPSec, usando chave pré-compartilhada para autenticação.

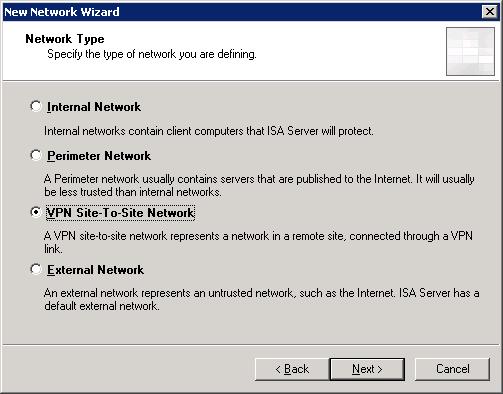
1. Abra o ISA Server Management
2. Expanda o nome do servidor
3. Expanda o nó Configuration
4. Clique com o botão esquerdo do mouse em Networks
5. Clique com o botão direito do mouse em Networks
6. Selecione New -> Network...



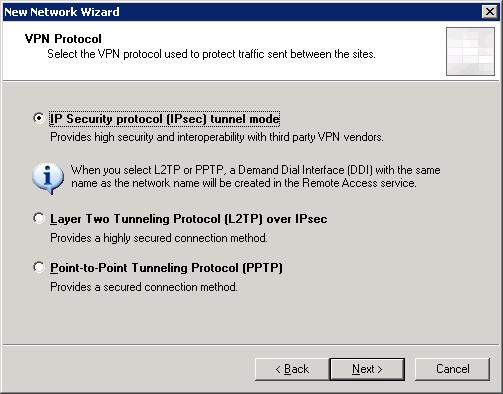
1. Na janela do New Network Wizard, digite o nome da rede remota e clique no botão Next.



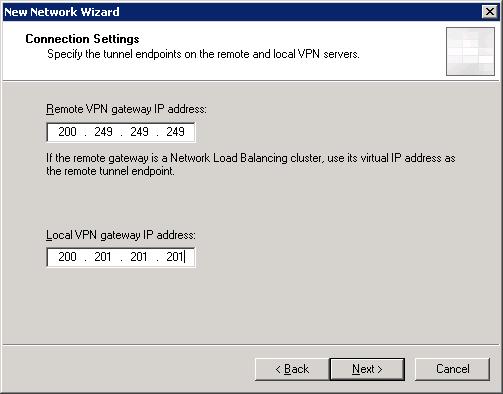
1. Selecione VPN Site-To-Site Network e clique no botão Next.



1. Na etapa VPN Protocol, selecione IP Security protocol (IPSec) tunnel mode e clique no botão Next.



1. Na etapa Connection Settings, em Remote VPN gateway IP address digite o endereço IP do gateway remoto (endpoint remoto) e em Local VPN Gateway IP address digite o endereço IP do firewall local que será usado para estabelecimento do túnel com o endpoint remoto (este endereço IP deve ser configurado como IP do gateway remoto no firewall da filial).



1. Na seção IPSec Authentication, selecione o método desejado para autenticação.
   1. Caso queira usar certificados digitais, selecione Use a certificate from this Certification Authority (CA)
   2. Clique no botão Browse
   3. Selecione o certificado desejado e clique no botão Select

Observação: Neste caso, os certificados devem estar instalados em ambos os endpoints.

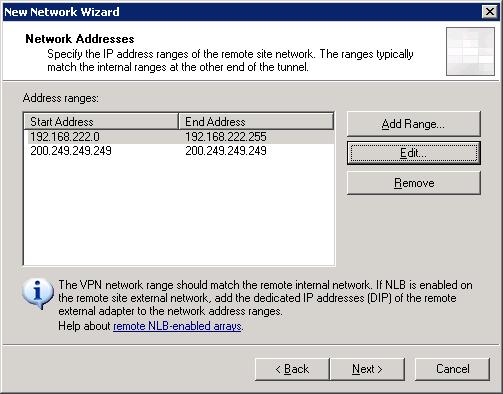


Para este artigo, utilizaremos chave pré-compartilhada como método de autenticação.

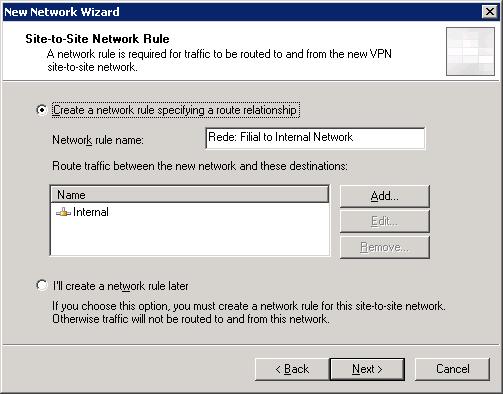
1. Clique em Use pre-shared key for authentication
2. Digite uma seqüência de caracteres para definir a chave e clique no botão Next. Atenção: esta chave deverá ser passada de forma segura ao administrador do outro endpoint para estabelecimento da autenticação.



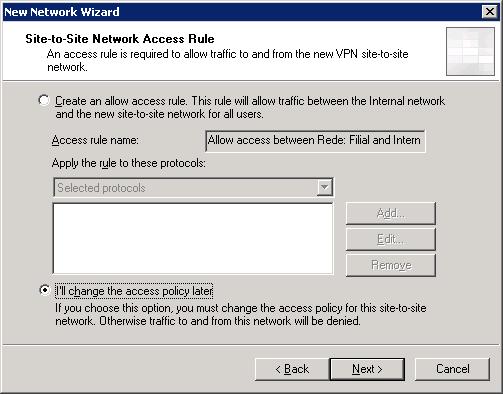
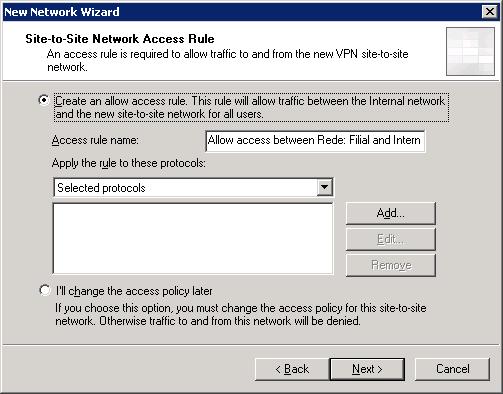
1. Na seção Network Addresses, adicione os endereços IP que fazem parte da rede remota.



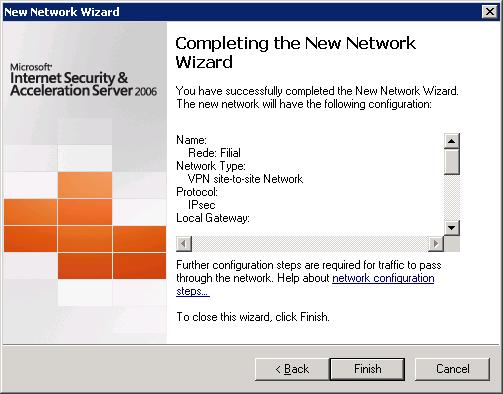
1. Na etapa Site-To-Site Network Rule, selecione Create a network rule specifying a route relationship para que o assistente possa criar de imediato uma regra de rede definindo o método de roteamento (que é Route).
2. Digite o nome da regra de rede no campo Network rule name.
3. Caso haja mais redes locais que precisem ter o tráfego roteado entre elas e a rede remota, clique no botão Add para adicioná-las. Ao finalizar, clique no botão Next.



1. Caso queira criar uma regra de acesso usando o assistente, clique em Create an allow access rule.
2. Clique no botão Add para adicionar os protocolos necessários.
3. Se preferir configurar uma regra de acesso posteriormente, clique em I’ll change the access policy later. Para este documento, utilizaremos esta opção. Ao terminar, clique no botão Next.



1. Revise suas escolhas no Completing the New Network Wizard e clique no botão Finish.



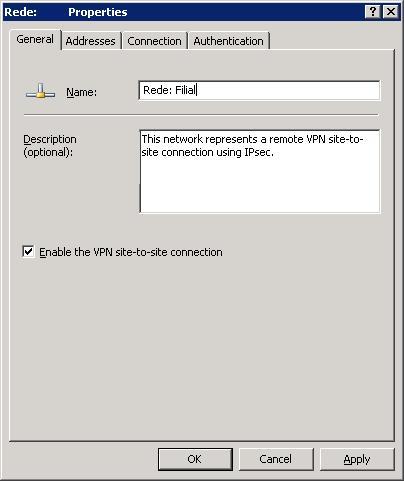
1. Clique no botão Apply e reinicie o ISA Server em seguida caso seja necessário.

Para finalizar, verifiquemos as configurações da VPN Site-To-Site.

1. Na árvore da console do ISA, clique em Virtual Private Networks (VPN).
2. Clique na aba Remote Sites



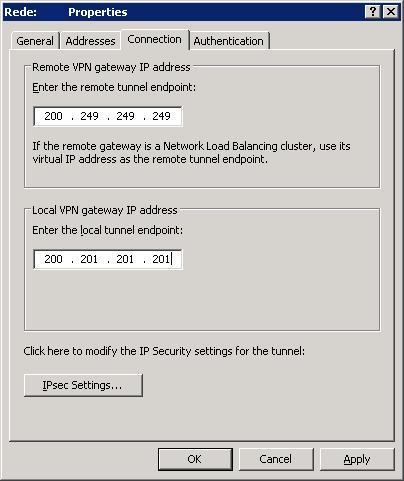
1. Clique com o botão direito na rede remota e em seguida em Properties



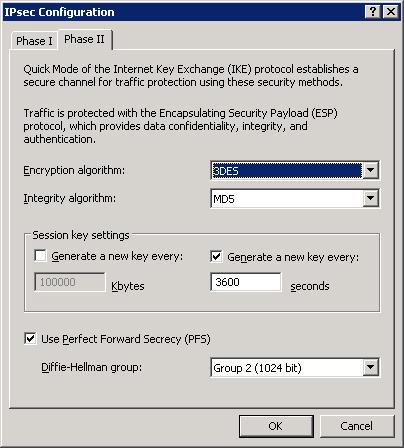
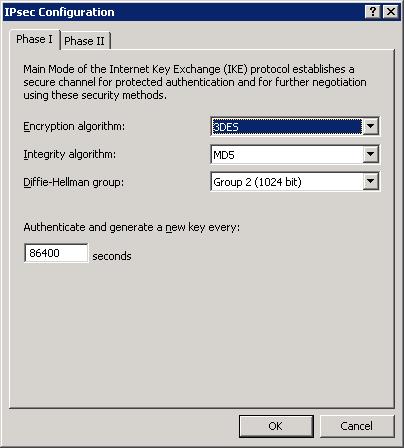
1. Clique na aba Addresses para visualizar a faixa de endereços IP da rede remota



1. Clique na aba Connection para visualizar os endereços IP dos endpoints do túnel
2. Ainda na aba Connection, clique no botão IPSec Settings... para visualizar as configurações de IPSec



1. Na janela IPSec Configuration, confirme se os parâmetros de segurança da Fase 1 e Fase 2 estão exatamente iguais tanto no ISA Server local (endpoint local) quanto no endpoint remoto



1. Clique no botão Ok
2. De volta à janela de propriedades da rede, clique na aba Authentication
3. Verifique se a opção Use pre-shared key for authentication está selecionada e se a chave digitada está de acordo com o que foi estabelecido.



**Links Relacionados**

* Public Key Infrastructure - http://en.wikipedia.org/wiki/Public\_key\_infrastructure
* The PKI page - http://www.pki-page.org/
* PKI – Public Key Infrastructure (Autor: Lino Sarlo da Silva, (c) Ed. Novatec Ltda., 2004, ISBN: 85-7522-046-2) - http://www.europanet.com.br/euro2003/index.php?cat\_id=1121&pag\_id=16202
* IPSec - http://technet.microsoft.com/en-us/network/bb531150.aspx
* How To Configure IPSec Tunneling in Windows Server 2003 - http://support.microsoft.com/kb/816514/en-us

**Conclusão**

Assim, com o uso do IPSec em conexões Site-To-Site, as organizações podem atingir a excelência no estabelecimento e manutenção de VPNs, tanto com a simplicidade de configuração no ISA Server 2006 quanto com o alto nível de segurança do protocolo IPSec.

*Rogério Silva atua no mercado há mais de 10 anos, especializando-se na área de infra-estrutura baseada em soluções Microsoft. Atuou em vários parceiros Microsoft da região como a Lanlink Informática, Allen Informática, ITECI, dentre outros. Como instrutor técnico, ministrou cursos de soluções Microsoft como o Windows Server e ISA Server para vários clientes, desde órgãos governamentais a empresas privadas. Em toda sua trajetória trabalhou em diversos projetos de implementação de soluções baseadas na plataforma Microsoft, porém, mais especificamente entre 2004 e 2007 atuou intensamente no ISA Server 2004/2006 e Microsoft Exchange Server 2003. É MCSE, MCSA e MCT, tendo investido na área acadêmica cursando em uma turma de Licenciatura em Computação.*