

# Uma solução segura e escalável para acesso remoto VPN

Edmar Roberto Santana de Rezende, Paulo Lício de Geus

Instituto de Computação  
Universidade Estadual de Campinas  
Campinas, SP – Brasil  
{edmar,paulo}@las.ic.unicamp.br

## Resumo

Neste trabalho é apresentada uma solução de acesso remoto VPN utilizando o software FreeS/WAN, uma implementação Open Source do protocolo IPSec baseada em Linux. Tal solução visa atender a requisitos de autenticação, configuração do sistema remoto e da política de segurança, e passagem por intermediários apresentados pelos cenários comuns de acesso remoto utilizando IPSec. Devido à expressiva parcela de mercado ocupada por produtos Microsoft, também são abordadas soluções integradas de clientes VPN baseados em Windows.

PALAVRAS-CHAVE: acesso remoto, VPN, IPSec, segurança em redes.

## Abstract

This work presents a remote access VPN solution using FreeS/WAN software, an Open Source implementation of the IPSec protocol for Linux. This solution wants to address authentication, remote system and security policy configuration, and intermediary traversal requirements present in common remote access scenarios using IPSec. Due to the significant market share occupied by Microsoft products, some integrated Windows based VPN client solutions are also discussed.

KEYWORDS: remote access, VPN, IPSec, network security.

## 1 Introdução

Durante anos, o acesso remoto foi tipicamente caracterizado por usuários remotos acessando recursos privados de uma organização através de uma rede de telefonia pública, com a conexão discada terminando em um Servidor de Acesso Remoto (*Remote Access Server* – RAS) localizado na rede da organização.

A enorme difusão da Internet e a crescente disponibilidade do acesso de banda larga, em conjunto com o desejo de redução dos altos custos do acesso discado, têm conduzido ao desenvolvimento de mecanismos de acesso remoto baseados na Internet.

Esse tipo de acesso remoto, comumente chamado de acesso remoto VPN, utiliza a tecnologia de Redes Privadas Virtuais (VPN), possibilitando que uma infra-estrutura de rede pública, como a Internet, seja utilizada como backbone para a comunicação entre o usuário remoto e a rede privada.

Na maioria dos casos, o usuário remoto acessa primeiramente um Provedor de Acesso à Internet (*Internet Service Provider* – ISP), e em seguida estabelece uma conexão virtual adicional sobre a Internet até a rede privada, como mostrado na Figura 1. Isto significa que o endereço IP do cliente remoto será atribuído dinamicamente pelo ISP. O mesmo é

válido para muitos usuários remotos que acessam a Internet de suas casas através de uma conexão permanente DSL, onde freqüentemente uma mudança de endereço IP diária é forçada pelo operador da rede. De uma forma geral, na maioria dos cenários possíveis de acesso remoto, mesmo que o endereço IP do sistema cliente não seja totalmente dinâmico, raramente haverá garantias de utilização de um endereço IP fixo ou previamente conhecido.

Ao identificar essas características, bastante específicas dos cenários de acesso remoto VPN, surgem diversos requisitos importantes que devem ser tratados prioritariamente para o desenvolvimento de uma solução realmente segura e funcional de acesso remoto.

Tais requisitos podem ser agrupados em algumas categorias básicas, dentre as quais podemos destacar: (i) a autenticação dos extremos da comunicação, (ii) a configuração do sistema remoto, (iii) a configuração das políticas de segurança e (iv) a passagem por intermediários.

A autenticação dos extremos da comunicação (Seção 2) visa verificar as identidades dos participantes da comunicação, tanto do cliente quanto do gateway VPN. A configuração do sistema remoto (Seção 3) visa ajustar os parâmetros necessários de configuração de rede do sistema cliente. A configuração das políticas de segurança (Seção 4) remete à configuração das políticas de acesso em ambos, gateway VPN e cliente remoto. A passagem por intermediários (Seção 5) refere-se à capacidade de passar tráfego seguro através de intermediários, alguns dos quais podem modificar os pacotes de alguma maneira. Tais intermediários incluem os dispositivos de firewall e NAT.

Neste trabalho serão detalhados alguns dos aspectos específicos da configuração de uma solução de acesso remoto VPN baseada no uso do software FreeS/WAN<sup>1</sup>, uma implementação Open Source do protocolo IPSec para sistemas Linux, desenvolvida pelo *FreeS/WAN Project*. Além de ser uma alternativa de baixo custo, o FreeS/WAN é uma das implementações IPSec mais populares para plataformas Linux, que conta com a contribuição de desenvolvedores e grupos de pesquisa de diversos países, em um esforço conjunto visando agregar novas funcionalidades a este produto.

Devido à expressiva parcela de mercado ocupada por produtos Microsoft, serão abordadas também algumas soluções de clientes VPN baseados em Windows (Seção 6), principalmente nos sistemas Windows 2000 e Windows XP, devido à presença de suporte nativo ao IPSec nestes produtos.

<sup>1</sup><http://www.freeswan.org>

## 2 Autenticação dos extremos do túnel

Um dos principais requisitos do cenário de acesso remoto VPN é a autenticação dos extremos do túnel. Para que haja garantias de que os recursos da rede privada da organização estarão acessíveis somente aos usuários autorizados, é imprescindível que exista total confiança na identidade dos participantes da comunicação.

Para atender a tais necessidades de autenticação, o IPSec [Kent e Atkinson, 1998] faz uso dos mecanismos providos pelo IKE (*Internet Key Exchange*) [Harkins e Carrel, 1998], o protocolo para gerência de chaves criptográficas e estabelecimento de associações de segurança entre os extremos da comunicação.

As características dinâmicas dos cenários de acesso remoto utilizando IPSec impedem que um gateway VPN, que protege o acesso à rede da organização, identifique o cliente de acesso remoto com base no seu endereço IP. Isto impossibilita o uso de segredos pré-compartilhados como forma de autenticação durante o *Main Mode* do IKE, já que a chave de sessão usada para cifrar a identidade na mensagem 5 do IKE, mostrada na Figura 2, depende também do segredo pré-compartilhado. Sem o conhecimento a priori da identidade do cliente que inicia uma conexão, o gateway VPN não pode selecionar o segredo pré-compartilhado correto para decifrar a mensagem 5 do IKE que contém por sua vez a informação necessária para identificar o cliente.

Como uma alternativa, o *Aggressive Mode* é freqüentemente usado em soluções VPN, sendo a identidade do cliente enviada em claro. Infelizmente o hash da identidade também é transmitido em claro, o que cria uma potencial brecha de segurança, possibilitando um ataque de dicionário off-line sobre o segredo pré-compartilhado que foi usado para assinar o hash.

Assim, para evitar esta potencial fraqueza do *Aggressive Mode* e também proteger a identidade dos clientes de acesso remoto, deve ser usado o *Main Mode* do IKE com assinaturas e certificados digitais, como mostrado na Figura 3.

Neste cenário de chave pública, a chave de sessão simétrica que cifra a troca IKE iniciada com a mensagem 5 depende somente do segredo Diffie-Hellman estabelecido pelas mensagens 3 e 4. Isso possibilita que o receptor extraia a identidade cifrada, que desta forma pode ser usada para selecionar a chave

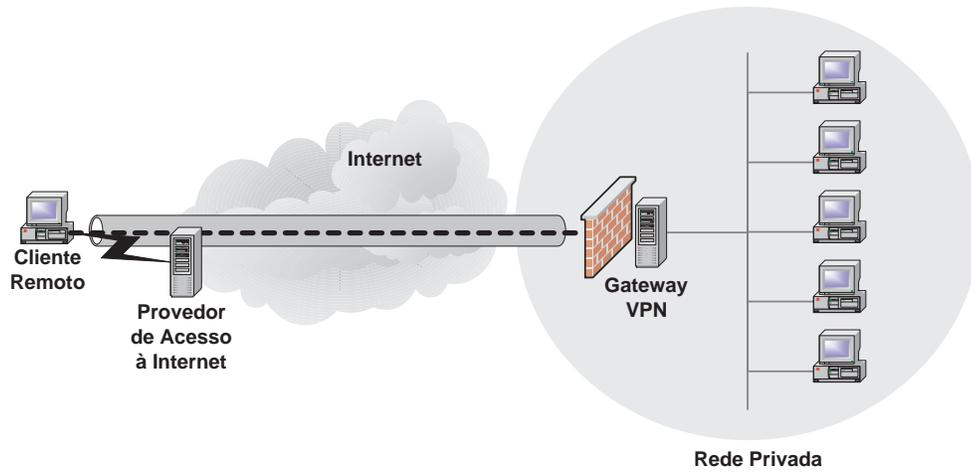


Figura 1. Acesso remoto VPN.

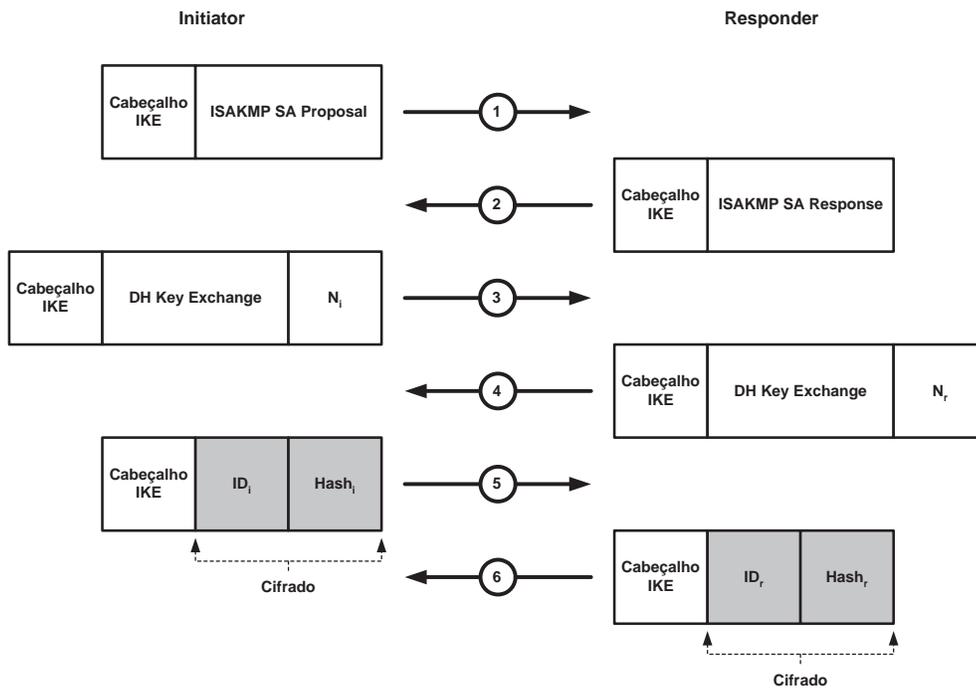


Figura 2. Main Mode do IKE usando chaves pré-compartilhadas.

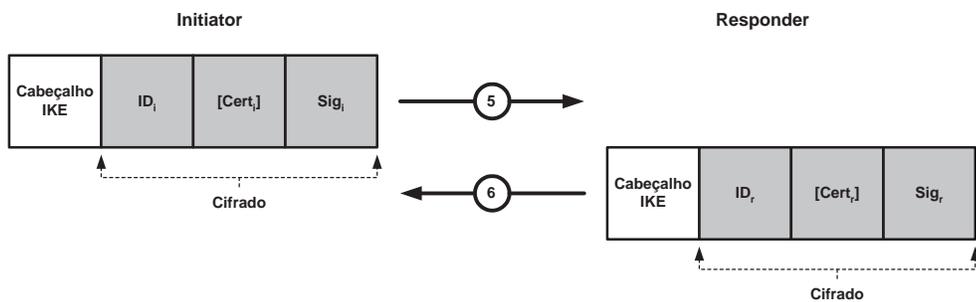


Figura 3. Main Mode do IKE usando certificados.

pública correta necessária para verificar a assinatura. Como uma conveniência, a maioria das implementações VPN envia junto um certificado X.509 contendo a chave pública exigida, de forma que não seja necessário obtê-la por outros meios, como por exemplo, uma requisição a um servidor LDAP.

O uso de certificados X.509 normalmente requer a existência de uma Infra-estrutura de Chaves Públicas (ICP) baseada em uma Autoridade Certificadora (AC) que emite e eventualmente revoga certificados de usuários e máquinas. A AC pode também ser executada dentro da empresa ou opcionalmente ser utilizado um centro de confiança oficial. Esta sobrecarga adicional impõe um fardo considerável no desenvolvimento inicial de uma solução VPN. Contudo, esse investimento é compensador, pois o gerenciamento de usuários baseado em certificados é mais escalável em relação a um número crescente de clientes VPN. O uso de certificados de usuário fornece a base ideal para um esquema de controle de acesso sofisticado.

## 2.1 Certificados digitais

No desenvolvimento de VPNs em larga escala, uma maneira viável de realizar a autenticação mútua de ambos os pontos da VPN de uma forma segura e eficiente é usando esquemas baseados em criptografia de chave pública, utilizando certificados digitais. Nestes casos, cada extremo da VPN deve possuir um certificado de usuário ou um certificado de máquina que é enviado ao outro extremo como parte do processo de autenticação no *Main Mode* do IKE. Esta autenticação é baseada em uma assinatura digital gerada cifrando um valor de hash com a chave privada de um dos extremos da VPN. A outra ponta pode então facilmente verificar a assinatura decifrando-a com a chave pública contida no certificado e, em seguida, comparando os hashes.

Para que este processo de autenticação seja seguro, é crucial que exista uma confiança total no certificado da outra ponta. Isto pode ser feito através da inclusão do certificado da AC raiz que emitiu os certificados de usuário e máquina em cada extremo da VPN. A confiança é então transferida para o certificado da AC. Se autoridades certificadoras multinível são usadas, então toda a cadeia de certificação deve estar disponível para cada cliente VPN. Os certificados de ACs intermediárias podem ser carregados estaticamente ou ficarem disponíveis através do *Main Mode*.

O FreeS/WAN suporta o uso de certificados X.509 a partir de sua versão 1.99, através da instalação de um patch<sup>2</sup> desenvolvido pelo *Security*

<sup>2</sup><http://www.strongsec.com/freeswan>

*Group of the Zurich University of Applied Sciences.*

No exemplo apresentado na Figura 4, todos os certificados finais foram emitidos pela autoridade certificadora VPN CA. O certificado da VPN CA deve ser instalado em cada ponto final da VPN para que se estabeleça uma relação de confiança no certificado recebido da outra ponta. Dessa forma, o gateway VPN aceitará qualquer cliente remoto que apresente um certificado de usuário válido emitido pela VPN CA [Steffen, 2003a].

## 2.2 Identidades coringa

De acordo com as especificações do IETF [Piper, 1998], os seguintes tipos de identidade podem ser usados na autenticação do *Main Mode* baseada no uso de certificados X.509:

- ID\_IPV4\_ADDR / ID\_IPV6\_ADDR: Endereço IPv4 ou IPv6
- ID\_FQDN: Nome de domínio da máquina (*Fully Qualified Domain Name*)
- ID\_USER\_FQDN: Identificador de usuário (*Fully Qualified Username*)
- ID\_DER\_ASN1\_DN: X.500 *Distinguished Name*

Para clientes VPN com endereços de rede dinâmicos não faz muito sentido usar um endereço IP como identificador, portanto, somente os três últimos tipos de identidade são relevantes.

Identidades enviadas como parte das mensagens 5 e 6 do *Main Mode* devem estar presentes nos campos correspondentes do certificado X.509, já que a identidade deve estar vinculada a uma chave pública que pode ser usada para checar a assinatura. Se a identidade utilizada for do tipo ID\_DER\_ASN1\_DN, ela deve estar contida no campo *subject distinguished name* (DN) do certificado, enquanto que identidades do tipo ID\_FQDN ou ID\_USER\_FQDN devem estar contidas no campo *subjectAltName*, uma extensão do X.509v3.

Os exemplos a seguir mostram como identidades coringa, representadas pelo caracter “\*”, podem ser utilizadas para especificar políticas de controle de acesso mais detalhadas:

```
conn IC
    right=%any
    rightid="C=BR,O=UNICAMP,OU=IC,CN=*"
                                /* ID_DER_ASN1_DN */
    leftsubnet=10.1.1.0/24
```

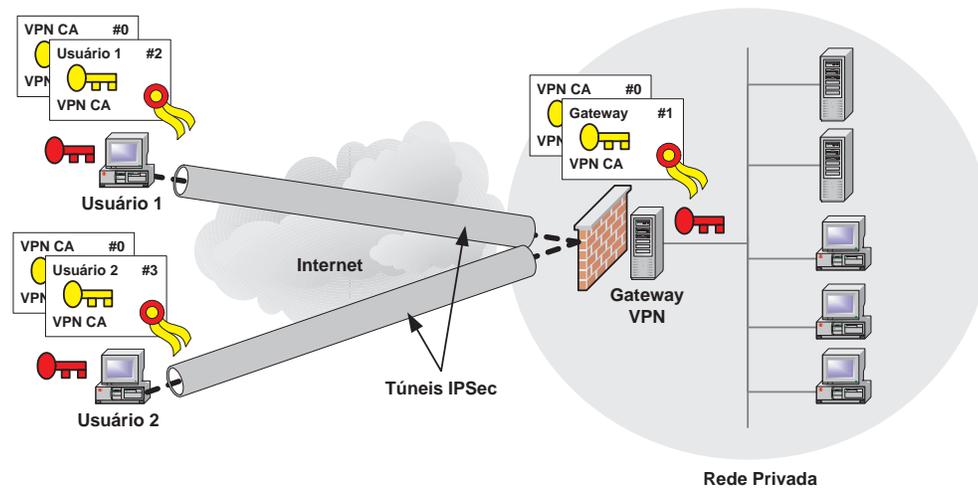


Figura 4. Autenticação baseada em certificados X.509.

```
conn DCC
    right=%any
    rightid=*@dcc.unicamp.br
                                /* ID_USER_FQDN */
    leftsubnet=10.1.2.0/24
```

A primeira definição de conexão (`conn IC`), mostrada neste exemplo, restringe o acesso à sub-rede 10.1.1.0/24 a qualquer usuário (`CN=*`) pertencente ao Instituto de Computação (`OU=IC`).

A segunda conexão (`conn DCC`) permite o acesso à sub-rede 10.1.2.0/24, a todos os usuários que possuem e-mail no domínio `dcc.unicamp.br` através do uso de um caractere coringa no endereço de e-mail (`*@dcc.unicamp.br`).

O FreeS/WAN também suporta caracteres coringa nos campos *relative distinguished name* (`C=`, `O=`, `OU=`, `CN=`, etc.) das identidades do tipo `ID_DER_ASN1_DN`.

### 2.3 Listas de certificados revogados

Confiar em um certificado de uma AC raiz significa confiar automaticamente em todos os certificados emitidos por essa AC. Assim, é de extrema importância que uma Lista de Certificados Revogados (LCR) seja mantida pela AC, que gerenciará então uma lista dos números de série de todos os certificados que tenham sido revogados.

A frequência com que uma LCR atualizada é emitida pela AC depende do que foi definido na política de segurança, de forma que os intervalos de emissão podem variar de acordo com a maior ou menor necessidade de impedir o acesso de usuários ou máquinas não-autorizados. O gateway e o cliente VPN devem periodicamente atualizar sua cópia local da LCR de

acordo com os intervalos de emissão, carregando-os de um servidor HTTP ou LDAP.

Um ou vários pontos de distribuição de LCRs (`crldistributionPoints`) podem ser inseridos como uma extensão em certificados X.509v3 para cada um dos certificados utilizados. Um `crldistributionPoint` usualmente tem a forma de uma URI (*Uniform Resource Indicator*), e pode ser usado para obter automaticamente uma LCR de um servidor HTTP ou LDAP.

Um exemplo de uma URI HTTP na notação do OpenSSL, seria:

```
crldistributionPoints=URI:
    http://www.vpnca.org/ca/cert.crl
```

A obtenção automática de LCRs baseadas em `crldistributionPoints` é suportada a partir da versão 2.00 do FreeS/WAN. Os certificados de máquina e usuário necessários podem ser gerados usando o pacote OpenSSL, através da definição de um ou mais `crldistributionPoints` no arquivo de configuração `openssl.cnf`.

### 2.4 Protocolo *online* de estado de certificado (OCSP)

Com um crescente número de usuários e a revogação frequente de certificados, os intervalos de emissão de LCRs podem se tornar inadequados para garantir que certificados recentemente revogados sejam rejeitados. Uma alternativa viável para complementar ou mesmo substituir as listas de certificados revogados pode ser o uso do Protocolo Online de Estado de Certificados (*Online Certificate Status Protocol – OCSP*) [Myers *et al.*, 1999].

Quando o OCSP é utilizado, um ponto da VPN envia uma requisição contendo o número de série do certificado da outra ponta para ser verificado por um servidor OCSP, que retorna uma resposta assinada contendo um dos indicadores: bom (*good*), revogado (*revoked*) ou desconhecido (*unknown*). A chave privada usada para assinar a resposta deve pertencer: à AC que emitiu o certificado em questão; a um *Trusted Responder* cuja chave pública é confiável; ou a uma *CA Designated Responder*, também denominada *Authorized Responder*, que possui um certificado especial emitido diretamente pela AC, indicando a permissão para emitir respostas OCSP em nome da AC.

Foi incorporado recentemente, na versão 1.5 do patch X.509, o suporte à verificação de certificados baseada em OCSP para o daemon IKE do FreeS/WAN, denominado Pluto. Um servidor OCSP também já está sendo disponibilizado a partir da versão 0.9.7 do pacote OpenSSL.

### 3 Configuração do sistema remoto

Pelo fato dos clientes remotos possuírem originalmente um endereço IP dinâmico atribuído por seus ISPs, muitas vezes é bastante desejável que eles utilizem endereços IP de um segmento de rede especial da faixa de endereços da rede privada, constituindo assim o que geralmente é denominado de “*extruded net*”. Isto pode ser conseguido atribuindo um endereço IP virtual ao sistema remoto estática ou dinamicamente como mostrado na Figura 5.

O uso do endereço IP virtual facilita tanto a filtragem realizada pelo gateway VPN de pacotes IP que saem do túnel VPN, quanto o roteamento dos pacotes que saem das máquinas da rede privada com destino aos clientes remotos.

Devido ao grande sucesso do protocolo PPP (*Point-to-Point Protocol*) e seus auxiliares, como o protocolo IPCP (*IP Control Protocol*), que permite a atribuição automática de um endereço IP ao cliente e também a especificação de servidores DNS e WINS, estes princípios foram prontamente herdados pelo protocolo L2TP (*Layer 2 Tunneling Protocol*) que encapsula quadros PPP em datagramas UDP para tunelá-los sobre a Internet, criando assim uma conexão virtual.

Pelo fato das funcionalidades do IPCP não serem diretamente suportadas pelo protocolo IKE, soluções baseadas no L2TP são frequentemente adotadas em cenários de acesso remoto. Para suprir a necessidade de segurança criptográfica deste protocolo, o L2TP deve ser adicionalmente protegido pelo IPsec, como

mostrado na parte superior da Figura 6. Esta é exatamente a abordagem escolhida pela Microsoft para sua solução de acesso remoto nos sistemas operacionais Windows 2000 e XP.

Apesar desta ser uma solução aparentemente viável, na prática ela apresenta diversos problemas causados pelo overhead de cabeçalhos na comunicação e pela própria natureza do protocolo PPP [de Rezende e de Geus, 2002]. A utilização de túneis IPsec, como mostrado na parte inferior da Figura 6, constitui uma excelente alternativa ao uso do L2TP, contanto que a atribuição dinâmica de endereços IP virtuais e servidores de informação DNS/WINS possa ser de alguma forma solucionada.

Uma abordagem proprietária chamada Mode-Config [Pereira *et al.*, 1999], introduz mensagens específicas proprietárias no protocolo IKE. Este conceito tem algumas vantagens convincentes quando informações de usuário, incluindo o endereço IP virtual que será atribuído, estão armazenadas em um servidor centralizado LDAP ou RADIUS. O gateway VPN pode então obter diretamente as informações de usuário do servidor de diretórios e encaminhar a informação para o cliente graças ao canal de comunicação IKE. Este argumento a favor do Mode-Config tem conduzido à sua inclusão oficial na proposta do protocolo IKEv2 [Kaufman, 2003] sendo especificado atualmente pelo *IPsec Working Group* do IETF.

Contudo, a necessidade de inclusão de novas mensagens no atual padrão do IKE em uso faz com que essa abordagem seja radicalmente evitada pelo IETF. Uma solução alternativa, recentemente padronizada pelo IETF, é o uso do protocolo DHCP sobre IPsec [Patel *et al.*, 2003].

#### 3.1 DHCP sobre IPsec

Geralmente um ou mais servidores DHCP são responsáveis pela atribuição dinâmica de endereços IP e de informações auxiliares para máquinas de uma rede privada. Vários aspectos importantes como uma renovação periódica dos empréstimos (*leases*) de endereços, o gerenciamento eficiente dos endereços disponíveis e a reação apropriada aos *timeouts* podem ser tratados por servidores DHCP de forma estável e confiável.

Um cliente remoto acessando uma rede privada através de um túnel IPsec necessita do mesmo tipo de informação para a configuração de sua interface IP virtual. Dessa forma, um servidor DHCP pode ser utilizado para prover esses serviços, enquanto que o gateway VPN se restringirá somente ao repasse de informações DHCP sobre o canal IPsec.

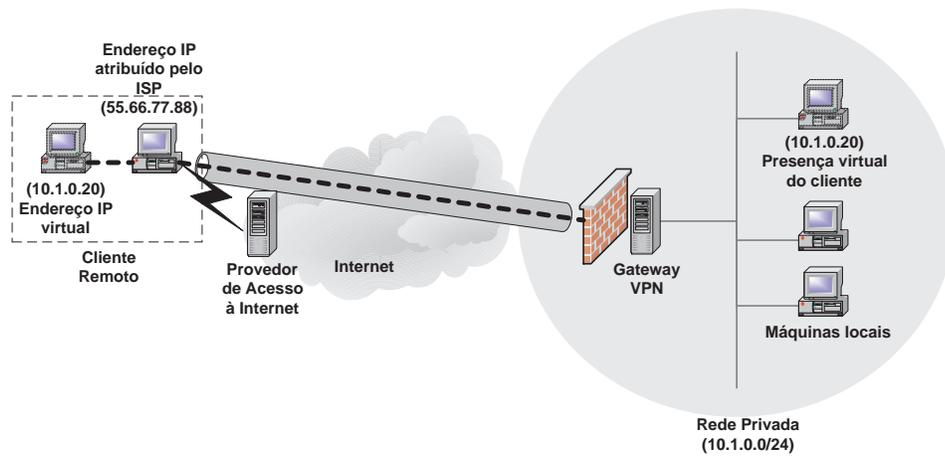


Figura 5. Atribuição de endereço IP virtual.

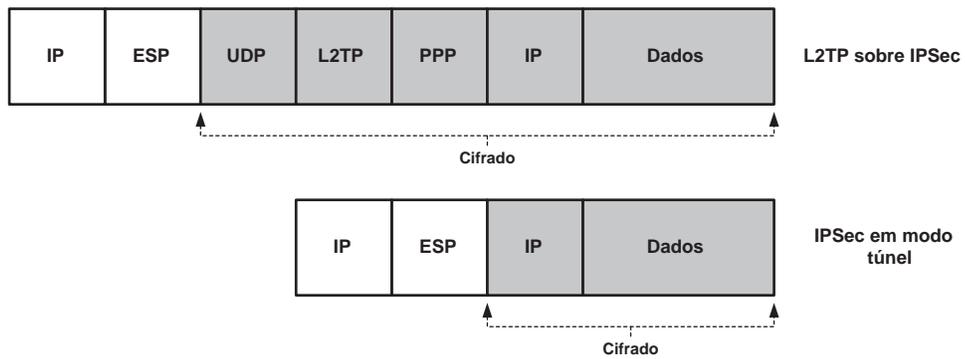


Figura 6. L2TP sobre IPsec vs. IPsec em modo túnel.

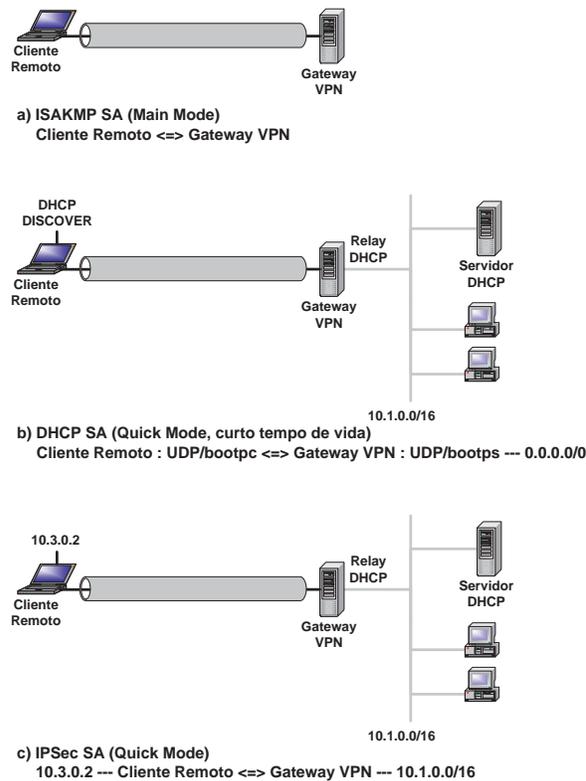


Figura 7. DHCP sobre IPsec.

A Figura 7 mostra como um esquema de atribuição dinâmica de endereço IP pode ser realizado usando o protocolo DHCP sobre IPsec:

- Na primeira fase uma negociação *Main Mode* do IKE é usada para criar uma associação de segurança ISAKMP (ISAKMP SA) estabelecendo uma relação de confiança entre o cliente remoto e o gateway VPN através de autenticação mútua. Esta ISAKMP SA é então a base para todas as IPsec SAs subsequentes que serão negociadas pelos extremos do túnel.
- Em seguida uma negociação *Quick Mode* do IKE configura uma IPsec SA com uma máscara de rede igual a 0.0.0.0/0, denominada DHCP SA, para que seja possível tunelar a mensagem broadcast DHCP DISCOVER subsequente originada pelo cliente remoto. Como tal máscara de rede global poderia implicar em um potencial risco de segurança, esta DHCP SA é restrita ao tráfego entre as portas UDP/bootpc e UDP/bootps, nos lados cliente e servidor respectivamente. Pelo fato do servidor DHCP de uma corporação usualmente não estar localizado na mesma rede que o gateway VPN, um relay DHCP é necessário no gateway para encaminhar a mensagem de DHCP DISCO-

VER ao servidor DHCP localizado em algum lugar na rede privada. Como uma medida adicional de segurança, o tempo de vida da DHCP SA será configurado como o mínimo de tempo absolutamente necessário para tratar a troca composta pelo broadcast DHCP DISCOVER inicial e pela mensagem de DHCP REPLY de retorno.

- Assim que o cliente remoto obtiver o endereço IP interno, uma negociação normal *Quick Mode* é iniciada, conectando o endereço IP interno virtual do cliente VPN à rede privada através do túnel IPsec. Frequentemente, quando o empréstimo DHCP (*DHCP lease*) requisitar uma renovação, a mensagem unicast DHCP REQUEST correspondente poderá ser tunelada para o gateway VPN usando a IPsec SA estabelecida, de forma que uma DHCP SA separada não tenha mais que ser configurada.

### 3.2 Servidor DHCP

Uma funcionalidade importante que deve ser provida pelo servidor DHCP é a diferenciação no tratamento das requisições feitas pelos clientes VPN e pelas demais máquinas da rede privada.

Para que isso se torne possível, é necessário que sejam levados em consideração parâmetros da requisição, como o DHCP Relay Agent Information Option ou o Gateway Address. O primeiro parâmetro contém o nome do dispositivo IPsec de onde se originou a requisição, neste caso, uma interface virtual ipsec0 criada pelo FreeS/WAN. O segundo parâmetro contém o endereço IP do gateway VPN. O exemplo a seguir ilustra a configuração de um servidor DHCP utilizando o primeiro parâmetro [Strasser, 2003]:

```
# Classe de clientes VPN class "vpn-clients"
{
  match if option agent.circuit-id = "ipsec0";
}

subnet ...
{# Demais máquinas da rede privada pool
  {
    deny members of "vpn-clients";
  }
  # Clientes VPN pool
  {
    allow members of "vpn-clients";
  }
}
```

### 3.3 Relay DHCP

Por razões de funcionalidade, o servidor DHCP de uma organização geralmente fica situado em sua rede privada. Já o gateway VPN, normalmente se encontra em uma interface de rede dedicada do firewall,

ou em muitos cenários em conjunto com o próprio firewall. O fato de ambos não estarem executando na mesma máquina, exige que o gateway VPN realize a função de Relay DHCP, encaminhando as mensagens de DHCP DISCOVER enviadas pelos clientes remotos ao servidor DHCP localizado em algum lugar na rede privada.

O Relay DHCP<sup>3</sup> desenvolvido por Mario Strasser (2003), utilizado em conjunto com o FreeS/WAN, permite a integração das funcionalidades de gateway VPN e Relay DHCP em um único equipamento, realizando todos os procedimentos descritos anteriormente. O arquivo de configuração do Relay DHCP contém quatro itens:

- LOGFILE: define o arquivo de log utilizado.
- DEVICES: contém uma lista das interfaces IP-Sec onde o Relay DHCP estará aguardando por requisições.
- SERVERDEVICE: define a interface que leva ao Servidor DHCP.
- DHCPSEVER: define o nome de máquina ou o endereço IP do Servidor DHCP. Se nenhum nome ou endereço forem fornecidos, os pacotes serão enviados em broadcast.

No exemplo a seguir é apresentada a configuração de um Relay DHCP, realizando o repasse das mensagens DHCP que chegam pela interface `ipsec0` ao servidor 10.1.1.3 acessível através da interface de rede `eth1`:

```
# Arquivo de configura\c{c}\~{a}o do Relay DHCP
LOGFILE="/var/log/relaydhcp.log" DEVICES="ipsec0"
SERVERDEVICE="eth1" DHCPSEVER="10.1.1.3"
```

### 3.3.1 Proxy ARP

Algumas questões relacionadas à faixa de endereços reservada aos clientes VPN merecem atenção especial. Existem basicamente dois cenários que devem ser considerados.

O primeiro é aquele onde clientes VPN recebem um endereço IP virtual de uma sub-rede separada. A principal vantagem desta opção é a facilidade de gerenciamento das políticas de segurança impostas aos clientes, já que estes pertencem a uma sub-rede bem definida. Além disso, o roteamento dos pacotes que retornam aos clientes remotos se torna mais simples.

Um segundo cenário possível é aquele onde são atribuídos aos clientes VPN endereços IP virtuais da mesma sub-rede que as máquinas da rede privada. A grande vantagem deste cenário é a possibilidade

do uso de aplicações que eventualmente necessitam enviar pacotes em broadcast para seu perfeito funcionamento. Nestes casos o suporte ao mecanismo de proxy ARP [Stevens, 1996] deve estar habilitado e devidamente configurado no gateway VPN, para que este consiga rotear os pacotes endereçados ao cliente apropriadamente.

Nas distribuições Linux mais populares isto pode ser feito através da configuração apropriada das rotas direcionadas ao cliente VPN, o que normalmente é feito automaticamente pelo FreeS/WAN, e da habilitação do suporte de kernel ao mecanismo de proxy ARP na interface de rede adequada, através da execução do comando:

```
echo 1 >
/proc/sys/net/ipv4/conf/eth*/proxy_arp
```

## 4 Configuração da política de segurança

Usando informações de identidade do usuário disponíveis em uma negociação IKE bem sucedida, um firewall pode dinamicamente abrir partes selecionadas da rede de acordo com um perfil de usuário pré-definido. Para implementar tal esquema comum, o firewall e o software VPN deveriam idealmente executar no mesmo computador, contudo uma variação onde um gateway VPN separado está conectado ao firewall através de uma interface de rede dedicada também pode ser possível.

A implementação IPsec do FreeS/WAN apresenta uma característica importante, onde há a possibilidade de definir um script qualquer que, imediatamente após a configuração bem sucedida de uma conexão VPN, deverá ser executado. Dessa forma, é possível inserir um conjunto de regras de firewall dinâmicas, possibilitando que ambos, cliente e gateway VPN, se protejam utilizando regras específicas durante a existência de uma determinada conexão VPN. Ao término do túnel VPN, as regras inseridas serão automaticamente removidas e o acesso à rede privada será fechado para aquele usuário específico.

A Figura 8 apresenta um cenário onde o firewall/gateway VPN permite a implementação de uma política de segurança comum que abrange a terminação do túnel VPN e o acesso seletivo a diferentes partes da rede privada controlado por regras de firewall dedicadas.

<sup>3</sup><http://www.strongsec.com/freeswan/dhcrelay>

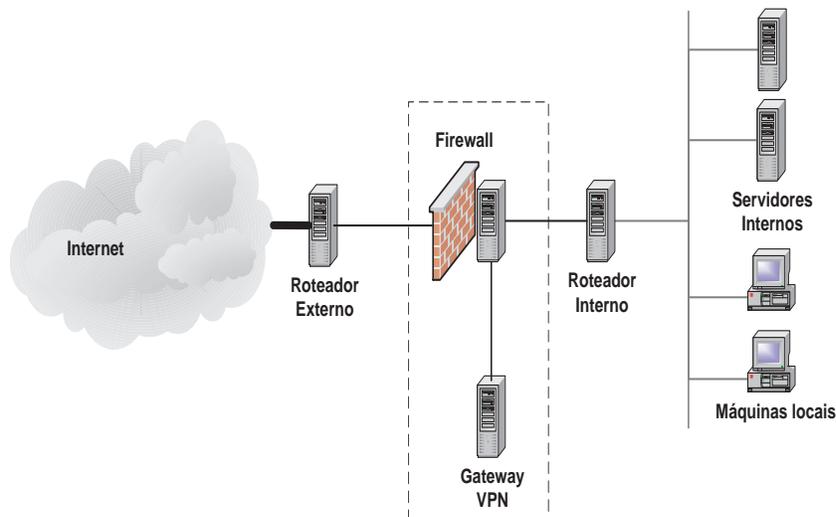


Figura 8. Firewall/gateway VPN implementando controle de acesso.

Outra forma de implementar uma política de segurança comum é através de um acesso seletivo baseado em identidades coringa, como descrito anteriormente. Tal mecanismo foi recentemente padronizado, através de sua inclusão na especificação de um Modelo de Informação de Configuração de Políticas IPsec [Jason *et al.*, 2003] desenvolvido pelo *IP Security Policy Working Group* do IETF.

Uma grande vantagem dessa abordagem baseada em identidades coringa é o fato de poder utilizar uma hierarquia de confiança bastante simplificada, sem a necessidade de diferentes níveis de autoridades certificadoras. Por outro lado, requer um planejamento cuidadoso na estrutura dos campos *Distinguished Name* do certificado no caso de identidades `ID_DER_ASN1_DN` ou na estrutura dos sub-domínios se os tipos `ID_FQDN` ou `ID_USER_FQDN` forem utilizados. Uma vez desenvolvido, torna-se extremamente difícil introduzir grandes modificações nesse esquema de controle de acesso sem substituir todos os certificados emitidos.

Alguns trabalhos estão sendo desenvolvidos com o intuito de criar outros métodos de controle de acesso seletivo baseados em aspectos distintos, como autoridades de certificação intermediárias, certificados de atributos, e tickets Kerberos [Steffen, 2003a].

## 5 Passagem por intermediário

Em muitos cenários de acesso remoto VPN, é comum a existência de equipamentos que realizam a

<sup>4</sup><http://open-source.arkoon.net>

tradução de endereços de rede (NAT) situados ao longo do caminho entre o cliente e o gateway VPN.

Estes mecanismos interferem no funcionamento normal das VPNs baseadas em IPsec, ao efetuarem modificações nos cabeçalhos dos pacotes que passam por eles, ocasionando falhas na verificação de integridade dos pacotes.

O que agrava a situação é que esses dispositivos de NAT estão amplamente difundidos, sendo necessários ao pleno funcionamento das redes envolvidas, e dificilmente podem ser modificados para a adequação a um tráfego de VPN.

Como alternativa, umas das propostas apresentadas ao IETF, o NAT Traversal (NAT-T) [Kivinen *et al.*, 2003], tem se mostrado uma solução promissora para os conflitos existentes entre NAT e IPsec. Esta solução se baseia no encapsulamento do tráfego da VPN em datagramas UDP, permitindo assim que um cliente remoto e um gateway VPN, ambos com suporte ao NAT-T, utilizem um túnel IPsec para o acesso remoto VPN sem serem afetados pelos inconvenientes causados pelo dispositivo de NAT.

O suporte ao mecanismo de NAT-T no FreeS/WAN é feito através da instalação de um patch<sup>4</sup> desenvolvido por Mathieu Lafon da Arkoon Network Security.

Para que o uso do NAT-T seja habilitado, é necessária a inserção de apenas três novos parâmetros no arquivo de configuração `ipsec.conf` do FreeS/WAN, como mostrado no exemplo a seguir:

```
config setup nat_traversal=yes
virtual_private=%v4:10.0.0.0/8, %v4:172.16.0.0/12
conn AcessoRemoto rightsubnet=vnet:%priv
```

Na seção de definição dos parâmetros de configuração (`config setup`) é habilitado o suporte ao mecanismo de NAT-T (`nat_traversal=yes`), sendo em seguida definida a faixa de endereços privados que será aceita como válida (`virtual_private=`), sendo suportados endereços IPv4 (`%v4:`) ou IPv6 (`%v6:`).

Em seguida, na definição da conexão do acesso remoto (`conn AcessoRemoto`) define-se que qualquer cliente VPN com endereço IP pertencente à faixa de rede privada definida anteriormente terá acesso permitido (`rightsubnet=vnet:%priv`).

O FreeS/WAN também suporta outros tipos de endereço, sendo `vnet` a definição de uma faixa de rede e `vhost` a definição de um endereço de máquina, e também diferentes métodos, como `%no` indicando que somente endereços IP públicos são aceitos, `%all` indicando que qualquer endereço IP é aceito, `%priv` como mostrado anteriormente.

## 6 Suporte a clientes *Windows*

Os sistemas operacionais da família Windows, desenvolvidos pela Microsoft, ocupam uma parcela significativa do mercado de sistemas operacionais domésticos. Tal popularidade também se traduz em realidade nos ambientes corporativos, onde grande parte do parque computacional das organizações utiliza os sistemas da Microsoft, especialmente os Windows 2000 e XP, devido à maior disponibilidade de recursos e mecanismos internos de segurança mais capazes.

O suporte nativo ao protocolo IPSec nesses dois sistemas operacionais permite o desenvolvimento de uma solução de baixo custo para o acesso remoto VPN, que apesar de não suportar algumas funcionalidades desejáveis, oferece ao usuário remoto uma conectividade segura com a rede da organização, através de um túnel IPSec, com autenticação baseada em certificados digitais.

Para isso, é necessária a instalação de dois ítems adicionais. O primeiro é a ferramenta `ipsecpol.exe`<sup>5</sup>, que faz parte do *Resource Kit* do Windows 2000, ou sua correspondente `ipseccmd.exe` no Windows XP, cuja função é permitir a adição, remoção e alteração de políticas IPSec por meio de linhas de comando, sem a necessidade de uma interação com interfaces gráficas. O segundo item é uma ferramenta desenvolvida por Marcus Müller<sup>6</sup>, que permite a utilização de um arquivo de configuração baseado na sintaxe do FreeS/WAN e

também o estabelecimento, monitoramento e encerramento do túnel VPN através de linhas de comando.

Um exemplo de configuração para uma conexão de acesso remoto VPN em um cliente Windows utilizando essas ferramentas é mostrado a seguir:

```
conn AcessoRemoto
left=%any
right=143.106.60.15
rightsubnet=10.1.1.0/255.255.255.0
rightca="C=BR,O=Unicamp,OU=IC,CN=VPNCA"
network=auto
auto=start
```

Na definição da conexão de acesso remoto (`conn AcessoRemoto`) um cliente remoto com endereço IP qualquer (`left=%any`) estabelece um túnel IPSec com o gateway VPN 143.106.60.15 (`right=`) que permite o acesso à rede privada 10.1.1.0/255.255.255.0 (`rightsubnet=`) com a autenticação sendo feita por certificados emitidos pela autoridade certificadora VPNCA (`rightca=`). Os parâmetros adicionais servem para definir a interface de rede utilizada e a inicialização automática do túnel, respectivamente.

Após a configuração adequada dos parâmetros da conexão VPN e a instalação do certificado do usuário remoto através do *Microsoft Management Console* (MMC) do Windows, basta executar a aplicação `ipsec.exe` para o estabelecimento do túnel IPSec com o gateway VPN informado e o conseqüente acesso aos recursos da rede privada desejada.

Tal solução não possui suporte a muitas das funcionalidades descritas anteriormente, como a atribuição de endereços IP virtuais e suporte ao NAT-T.

Apesar desta ser uma solução um tanto restrita, apresenta a vantagem de não necessitar de softwares comerciais, com exceção do próprio sistema operacional da Microsoft, sendo portanto uma alternativa de baixo custo para clientes VPN utilizando tal plataforma.

É importante frisar que gateways VPN utilizando FreeS/WAN possuem compatibilidade conhecida com clientes FreeS/WAN, PGP-net, SafeNet/Soft-PK, SafeNet/SoftRemote, SSH Sentinel, Microsoft Windows 2000 e Windows XP [Steffen, 2003b]. Dentre esses clientes VPN, o SSH Sentinel, desenvolvido pela SSH Communications Security, é o que suporta o maior número de funcionalidades, além de ser o único a suportar a atribuição de endereços IP virtuais, constituindo portanto uma excelente opção de software comercial para a plataforma Windows.

<sup>5</sup><http://www.microsoft.com>

<sup>6</sup><http://vpn.ebootis.de>

## 7 Conclusões

O acesso remoto VPN possui uma grande aplicabilidade em um ambiente corporativo, ao permitir que usuários remotos deixem de realizar ligações interurbanas, acessando os recursos da organização utilizando um túnel virtual criado através da Internet.

Devido às características particulares apresentadas pelos cenários de acesso remoto, algumas categorias básicas de requisitos como a autenticação dos extremos do túnel, a configuração do sistema remoto, a configuração da política de segurança e a passagem por intermediários, devem ser tratadas prioritariamente para o desenvolvimento de uma solução segura e funcional.

Como resultado deste trabalho, é apresentada uma solução de acesso remoto VPN baseada no software FreeS/WAN sobre sistemas Linux. Tal solução abrange diversas tecnologias recentes e promissoras, incorporando várias características não suportadas nativamente pelo FreeS/WAN, como o suporte a autenticação e controle de acesso baseados em certificados digitais, a configuração do sistema remoto utilizando o protocolo DHCP sobre IPsec e o suporte a NAT-T para a passagem por dispositivos de NAT intermediários.

Dessa forma foi possível desenvolver uma solução viável de acesso remoto VPN que, além de ser uma alternativa de baixo custo, por ser baseada em um software Open Source como o FreeS/WAN, possui ainda compatibilidade com o software cliente VPN nativo dos sistemas operacionais Windows e também com alguns softwares comerciais.

## Agradecimentos

À empresa Robert Bosch Ltda pelo apoio financeiro durante a realização deste trabalho.

## Referências

- DE REZENDE, E. R. S. e DE GEUS, P. L. 2002 *Análise de segurança dos protocolos utilizados para acesso remoto VPN em plataformas Windows*. In: Anais do IV Simpósio sobre Segurança em Informática, p. 1-8.
- HARKINS, D. e CARREL, D. 1998. The internet key exchange (IKE). RFC 2409.
- JASON, J., RAFALOW, L. e VYNCKE, E. 2003. IPsec configuration policy information model. RFC 3585.
- KAUFMAN, C. 2003. Internet key exchange (IKEv2) protocol. Internet Draft.
- KENT, S. e ATKINSON, R. 1998. Security architecture for the internet protocol. RFC 2401.
- KIVINEN, T., SWANDER, B., HUTTUNEN, A. e VOLPE, V. 2003. Negotiation of NAT-traversal in the IKE. Internet Draft.
- MYERS, M., ANKNEY, R., MALPANI, A., GALPERIN, S. e ADAMS, C. 1999. X.509 internet public key infrastructure online certificate status protocol – OCSP. RFC 2560.
- PATEL, B., ABOBA, B., KELLY, S. e GUPTA, V. 2003. Dynamic host configuration protocol configuration of IPsec tunnel mode. RFC 3456.
- PEREIRA, R., ANAND, S. e PATEL, B. 1999. The ISAKMP configuration method. Internet Draft.
- PIPER, D. 1998. The internet IP security domain of interpretation for ISAKMP. RFC 2407.
- STEFFEN, A. 2003a. *Virtual private networks – coping with complexity*. In: Proceedings of the 17th DFN-Workshop on Communications Networks.
- STEFFEN, A. 2003b. X.509 FreeS/WAN patch – instalation and configuration guide. <http://www.strongsec.com/freeswan/>.
- STEVENS, W. R. 1996. *TCP/IP Illustrated*. 2ª ed. Reading: Addison-Wesley.
- STRASSER, M. 2003. DHCPv4 configuration of IPsec tunnel mode howto. <http://www.strongsec.com/freeswan/dhcprelay>.

Submitted in 26/07/2004

Accepted in 31/09/2004