COLOCAÇÃO DO VPN NA CONFIGURAÇÃO DO *FIREWALL*.

RESUMO

Este artigo discute o correto posicionamento de um *gateway* VPN numa configuração de *firewall*, na qual estão presentes uma ou mais DMZs. São discutidos as vantagens e desvantagens de cada tipo de configuração. Além disso discute-se o papel da VPN quando se propõe uma topologia de *firewall* distribuído.

ABSTRACT

This paper discusses the right placement of a VPN gateway in a firewall configuration with one or more DMZs. The advantages and drawbacks of which configuration are discussed. Besides, the role of a VPN is discussed when a distributed firewall topology is proposed.

1 INTRODUÇÃO

Desde que as empresas começaram a usar computadores em mais de uma localidade, apareceu o desejo e a necessidade de conectá-las de maneira privada e segura para facilitar as comunicações corporativas. Instalar uma rede privada numa área contígua de prédios pode ser relativamente simples, mas a instalação de uma rede corporativa envolvendo outros escritórios ou plantas localizadas a quilômetros de distância, pode ser bastante difícil. Em muitos casos, não há outro recurso a não ser o de usar linhas dedicadas para ligar localidades separadas geograficamente. Contudo, este tipo de tecnologia e correlatas, oferece problemas operacionais importantes para as empresas, tais como: alto custo, dificuldades de escalabilidade e baixa flexibilidade.

Uma solução, para este tipo de problema, é o uso da infra-estrutura aberta e distribuída da Internet para transmissão de dados, de modo privado, entre localidades diversas de uma empresa. A isso chamamos de VPN – *Virtual Private Network* - Rede Privada Virtual.

Como a Internet é uma rede pública com transmissão aberta da maior parte dos dados, cabe às VPNs prover o suporte criptográfico necessário para se obter a privacidade desejada. Isto inclui o ciframento, a verificação e a assinatura dos dados que trafegam entre as localidades, protegendo os dados de escuta, alteração e impostura por parte de agentes não autorizados. Como vantagem adicional, a VPN permite conexões seguras para usuários móveis, em virtude das conexões discadas que os provedores de Internet oferecem em seus POPs (Kosiur, 1998).

Para tanto, deve-se atentar para os aspectos de segurança envolvidos, pois a instalação de funcionalidade VPN poderá implicar numa revisão das políticas de segurança e numa nova formulação da estrutura lógica e física dos componentes de um *firewall*.

2 OBJETIVO

Este trabalho visa discutir o estabelecimento de possíveis configurações seguras de uma VPN dentro de um *firewall*, além de discutir como a utilização de funcionalidade VPN dentro de uma configuração de segurança se encaixa com as definições mais recentes de *firewall* e das fronteiras de um perímetro de segurança

3 DEFINIÇÕES: FIREWALL – DMZ – VPN

Primeiramente, serão estabelecidos, alguns conceitos básicos.

O primeiro deles é o conceito de *firewall*. Será seguido, inicialmente, o conceito clássico de *firewall*, como apresentado em (Chapman e Zwicky, 1995) e em (Gonçalves, 199).

Segundo (Chapman e Zwicky, 1995) *firewall* é definido como “um componente ou conjunto de componentes que restringem o acesso entre uma rede protegida e a Internet, ou entre outros conjuntos de redes”. Similarmente (Gonçalves, 199) afirma que “um *firewall* separa a rede protegida daquela desprotegida: a Internet. Ele escrutina e filtra todas as conexões vindas da Internet para a rede protegida e vice-versa, através de um único *checkpoint* concentrado de segurança. Um *firewall* assegura que não possibilidade de acesso à Internet a partir da rede interna, nem vice-versa, a não ser que se passe por esse ponto”. Poderíamos continuar citando outras referências já clássicas (Cheswick e Bellovin, 1994; Ranum, 199) e veríamos que elas têm em comum a afirmação de que o *firewall* é o ponto divisor entre a rede interna e externa, no qual o tráfego que entra e sai da rede protegida pelo *firewall* é vigiado, filtrado e, algumas vezes, modificado. Fica claro também que ele é considerado como um “ponto”, quando observado a partir de um referencial afastado, levando em conta a totalidade da rede. Quando nos aproximamos, notamos que ele é uma estrutura muitas vezes complexa, com elementos que cumprem papéis fixos e bem conhecidos.

Assumindo esse ponto de vista da proximidade, podemos distinguir nesse conjunto de elementos, uma rede que não é nem a rede externa, nem a

interna. Essa rede, situa-se no que chamamos "zona desmilitarizada" ou DMZ[1]. A DMZ tem como papel ser uma espécie de uma rede "tampão" entre as redes externas e interna. Os equipamentos situados numa DMZ têm como papel fornecer serviços aos usuários externos, de tal modo que estes não necessitem acessar a rede interna, proporcionando um certo grau de isolamento da rede interna em relação ao tráfego que vêm da parte externa (Nakamura, 2000). Os equipamentos colocados na DMZ devem ser configurados para funcionar com o mínimo de recursos possíveis para oferecer um determinado serviço. Além disso, o comprometimento de um equipamento qualquer situado numa DMZ, não deve servir de ponte para o comprometimento de equipamentos e/ou serviços da rede interna, ou seja, qualquer tentativa de ataque deve ficar confinada nos equipamentos situados na DMZ. Deste modo pode-se gerar um balanço satisfatório do clássico impasse da segurança *versus* disponibilização de serviços.

Pode-se definir VPN tomando-se como base as palavras que compõe o próprio acrônimo: Rede Privada Virtual (*Virtual Private Network*).

Dize-se, de maneira genérica, que uma rede é um conjunto de aparelhos (computadores, roteadores, etc), que podem se comunicar de algum modo, podendo transmitir e receber dados entre eles.

O termo "privado", numa acepção mais restritiva, significa a privacidade de comunicação entre dois ou mais equipamentos, privacidade essa assegurada através de algum mecanismo que torna essa comunicação secreta.

O aspecto virtual possui correlação com o aspecto privado. A comunicação privada é feita, utilizando-se a infra-estrutura de rede que é compartilhada por mais de uma organização. Deste modo, os recursos privados são construídos usando-se como base uma camada lógica de um recurso físico compartilhado, o que leva a afirmar que essa "rede" privada não possui qualquer relação com um sistema físico de telecomunicações privado. Ela é uma abstração, não representando um mapeamento direto da rede física que é seu substrato. Um conceito mais formal pode ser encontrado em (Ferguson e Huston, 1998) que afirma que a VPN é "um ambiente de comunicações no qual o acesso é controlado para permitir conexões entre pares somente dentro de uma comunidade de interesse, sendo construído através do particionamento de um meio de comunicação comum, no qual essa base de comunicação comum provê serviços à rede, numa base não exclusiva".

Um conceito envolvido na definição de VPN é o conceito de túnel, que possui relação estreita com o termo "virtual" da VPN. É o tunelamento que permite esconder dos elementos da rede privada, local ou remota, as infra-estruturas do provedor de Internet e da própria Internet (Ferguson e Huston, 1998).

O tunelamento cria uma conexão especial entre dois pontos. Para criar-se um túnel, a extremidade iniciadora encapsula os pacotes da rede privada para o trânsito através da Internet. Para as VPNs, sobre redes IP, esse encapsulamento pode significar cifrar o pacote original, adicionando um novo cabeçalho IP ao pacote. Na extremidade receptora, o *gateway* remove o cabeçalho IP convencional, do pacote usado como meio de transporte na Internet, e, se necessário, decifra o pacote; repassando o original para o seu destino (Ferguson e Huston, 1998) (Kosiur, 1998).

O protocolo de tunelamento mais utilizado é o IPsec, desenvolvido pelo IETF, que possui três componentes:

- AH (*Authentication Header*): fornece serviço de autenticação ao pacote IP, não alterando o conteúdo do *payload* do pacote. A autenticação é feita sobre todo o pacote (Kent e Atkinson, 1998a).
- ESP (*Encapsulating Security Payload*): fornece cifragem de pacotes, sendo que, opcionalmente, pode haver a autenticação do que foi cifrado. A cifragem é realizada somente sobre o conteúdo interno ao cabeçalho ESP (Kent e Atkinson, 1998b).
- IKE (*Internet Key Exchange*): negocia parâmetros de conexão para os outros dois, incluindo chaves (Harkins e Carrel, 1998).

O tunelamento com ciframento é feito usando-se o cabeçalho ESP à frente do pacote original, acrescentando-se a esse conjunto um cabeçalho IP externo.

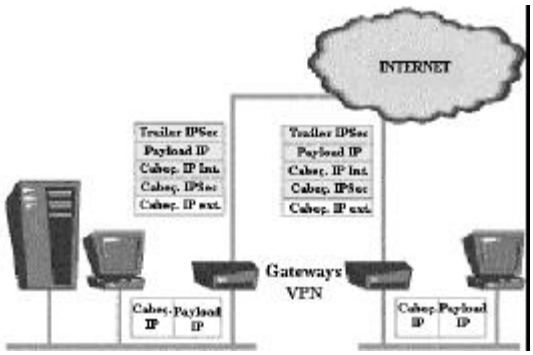

Figura 1 – Tunelamento IPSec usando ESP

4. POSICIONAMENTO DA VPN NA TOPOLOGIA DE SEGURANÇA

A colocação de uma VPN dentro de uma estrutura de segurança preexistente apresenta-se como um problema delicado. Uma configuração errada pode comprometer a segurança da rede como um todo. Deve-se estar atento a todos os aspectos envolvidos. Em geral, podemos enunciar algumas regras de colocação de um *gateway* VPN [??]:

- Não comprometer a política geral de segurança da rede.

[1] O termo vem da abreviatura do termo em inglês De-Militarized Zone

- A localização do *gateway* VPN não deve se constituir num único ponto de falha.
- *Gateway* VPN deve aceitar somente tráfego cifrado da rede não confiável[2].
- *Gateway* VPN deve aceitar tanto tráfego cifrado como não cifrado da rede confiável.
- *Gateway* VPN deve defender-se de ataques vindos da Internet.
- O restante do equipamento deve filtrar o tráfego após o deciframento por parte do *gateway* VPN.

Sabemos que a construção de uma política de segurança de uma rede deve se basear em conceitos mais genéricos do que seja uma rede segura, nos serviços que devem ser protegidos, nos serviços externos que devem estar disponíveis para os usuários internos e vice-versa. Do estudo desses fatores deve resultar uma topologia de equipamentos de segurança que seja reflexo da política de segurança anteriormente estabelecida. A colocação de um equipamento ou serviço VPN, numa rede já estabelecida, pode implicar numa revisão da topologia da rede de segurança, com o objetivo de assegurar as premissas da política de segurança. Para isso devem ser analisadas todas as alterações de tráfego introduzidas com a adição da funcionalidade VPN, efetuando-se as alterações de configuração necessárias nos equipamentos.

Como o *gateway* VPN deve receber tráfego da rede, não há qualquer sentido em que ele aceite qualquer outro tipo de tráfego, além daquele de controle, que não seja cifrado. Essa rejeição ou descarte de outros tipos de tráfegos é parte fundamental da política de autodefesa do próprio *gateway* VPN.

A colocação ao do *gateway* VPN em relação ao *firewall* é crucial, pois os *firewalls* não podem aplicar regras de filtragem a pacotes cifrados. Existem várias opções de colocação (King, 1999): em frente ao *firewall*, atrás do *firewall*, no *firewall*, paralelo ao *firewall*, ao lado do *firewall*. Tendo em vista as regras anteriormente descritas, vamos analisar cada uma delas:

- **Em frente ao firewall:** Um gateway VPN em frente a um firewall, como o ponto de conexão à Internet, apresenta um ponto único de falha, podendo ser explorado por um atacante. É algo sério, pois o *gateway* VPN pode conter erros de implementação que podem ser explorados. Com tal configuração permite-se a passagem tanto de tráfego cifrado quanto de não cifrado a partir da rede insegura (em alguns casos pacotes cifrados podem ser filtrados após o processo de deciframento); ou seja, o *gateway* VPN estaria recebendo tráfego que não estaria sendo destinado a ele, tráfego esse não submetido a qualquer tipo de análise. Além disso nunca se sabe se o *gateway* está ou não comprometido.
- **Atrás do firewall:** Nesta configuração a proteção é fornecida pelo firewall, que deve deixar passar pacotes IP do tipo 50(AH) e 51(ESP), e pacotes UDP na porta 500(IKE). Além disso o *firewall* não consegue efetuar qualquer tipo de filtragem no tráfego cifrado endereçado ao VPN. Como conseqüência, teremos um tráfego que, após o deciframento, adentrará a rede interna sem que sobre ele se tenha estabelecido qualquer tipo de controle. Esta configuração também implica em um único ponto de falha, gerando conseqüências parecidas com as citadas no item anterior.
- **No firewall:** Teoricamente é uma grande idéia, pois tal configuração uniformiza a administração e o gerenciamento dos componenetes da rede. Atualmente não é uma solução viável devido às limitações na habilidade em rotear, executar criptografia de chave pública e chavear entre sessões cifradas ao mesmo tempo em se realiza controle de acesso e geração de logs. Além disso também se constitui num único ponto de falha mais grave que os anteriores, pois um ataque ao VPN pode comprometer a toda a estrutura do *firewall*.
- **Paralelo ao *firewall*:** a maior parte dos produtores de VPN sugerem duas conexões com a rede não confiável: um para o *firewall*, outra para o *gateway* VPN. Nesta estrutura o VPN é configurado para aceitar somente tráfego cifrado. Embora tal arranjo evite um ponto único de falha, o equipamento VPN deve defender-se sozinho de ataques externos. Tal configuração é perigosa considerando-se que equipamentos de VPN não têm-se mostrado robustos quando conectados diretamente à Internet.
- **Ao lado do *firewall*:** Um *gateway* VPN numa interface dedicada de um *firewall* é considerado ao lado. Pode-se descrever a colocação do *gateway* VPN ao lado do *firewall* da seguinte forma: o *firewall* repassa o tráfego cifrado ao VPN, que o decifra e o reenvia ao firewall, que por sua vez o analisa e o envia à rede segura. Este arranjo protege o equipamento VPN de ataques da rede não confiável, enquanto filtra tráfego não cifrado. A interface externa do gateway VPN deve ser configurada para aceitar somente pacotes cifrados; todos os pacotes que entram pela interface interna (obviamente destinados ao prolongamento remoto da rede privada) devem ser cifrados antes de serem enviados a Internet.

Estudos preliminares parecem indicar que essa última configuração é a mais confiável (King, 1999).

A posição aconselhada no artigo é a colocação da VPN na interface dedicada do *firewall*, dado que numa configuração deste tipo todos os pacotes que chegam ao *gateway* VPN passam antes por um filtro de pacotes ou de estados, o que fornece uma certa proteção contra ataques diretos. Após passarem pelo *gateway*, terem os cabeçalhos de tunelamento retirados e serem decifrados, os pacotes originais

[2] Excetuando-se o tráfego de controle

podem passar agora por processo de filtragem, o que não podia ser feito ao entrarem no *firewall* por estarem completamente cifrados.

Apesar de (King, 1999) concluir que esta é a melhor configuração para a colocação de um *gateway* VPN dentro de um *firewall*, existem outros detalhes referentes à correta integração do *gateway* de VPN no *firewall*. Questões importantes nos aparecem quando pensamos na integração da funcionalidade VPN com as regras de *firewall*.

A colocação de uma VPN dentro de uma arquitetura de *firewall* deve levar em conta o possível aumento de complexidade das regras de filtragem, pois muitas vezes é necessário lidar com cenários complexos de acesso de clientes VPN, por exemplo: parceiros de *extranet*, funcionários com acesso remoto e filiais da própria corporação. Esta complexidade crescente pode comprometer a administração segura dos equipamentos, podendo gerar brechas que facilitem um ataque.

Essa preocupação nos leva a escolha de um software de filtragem que seja flexível o suficiente para acomodar as novas de filtragem do modo o mais transparente e simples possível, possibilitando o estabelecimento claro do escopo de cada bloco de regras. Em (Nakamura, 2000) temos exemplos de como pode ser difícil a análise da composição das regras num ambiente complexo.

O *ipchains* (Russel, 2000) (Nakamura, 2000) (Nakamura e Geus, 2000) possibilita a separação das regras em listas, chamadas "cadeias". Ele possui 3 cadeias básicas: *INPUT*, que cuida dos pacotes destinados a processos locais; *FORWARD*, que cuida dos pacotes

Porém, com o uso do *ipchains* (Russel, 2000) (Nakamura, 2000) (Nakamura e Geus, 2000) como software de filtragem, é possível construir as regras de modo que todas as filtragens referentes à VPN se localizem numa única cadeia. Ou ainda, caso a complexidade das regras específicas à VPN o justifique, pode-se quebrar tal cadeia em regras menores, sempre na tentativa de facilitar a administração da segurança.

4.1 Gateway VPN na DMZ

Outra questão a ser levantada refere-se à posição específica do *gateway* VPN: em conjunto com outros equipamentos de uma DMZ, numa DMZ separada, numa configuração de múltiplas DMZs, conforme descritas em (Chapman e Zwicky, 1995). A resposta a essa questão não é necessariamente única, vai depender da própria estrutura das redes que irão se comunicar através da VPN, se irão ser redes da mesma corporação ou de corporações cooperativas, se trata-se de acesso remoto ou de acesso de cliente de uma extranet. Iremos abordar cada um dos tipos de posicionamento, designando vantagens e desvantagens segundo a necessidade específica. Neste artigo não estaremos abordando o caso particular do acesso remoto como sendo pertencente à rede lógica da corporação. Este é um caso particular, que foi abordado em [Figueiredo e Geus, 2001].

4.1.1 Em Conjunto Com Outros Equipamentos De Uma DMZ.

Neste tipo de configuração o *gateway* VPN seria colocado em conjunto com os outros equipamentos de uma DMZ. Conforme colocado por (Chapman e Zwicky, 1995), estes equipamentos podem ser acessados por usuários não participantes da rede interna da corporação. Os desdobramentos deste tipo de colocação, depende do tipo de usuário que tem acesso à VPN.

Para o caso de VPN ligando parceiros de uma extranet, estes poderiam ter acesso a serviços acessíveis a qualquer usuário externo, porém de modo cifrado. Contudo os pacotes provenientes da rede desses parceiros, não seriam submetidos às regras de filtragem, pois os pacotes originais, antes da passagem pelo *gateway* VPN, estariam cifrados, impedindo a filtragem de seu conteúdo. Com isso, uma parte da política de segurança da organização, expressa através das regras de filtragem, não seria aplicada a uma parcela importante do tráfego da rede. No entanto, o tráfego oriundo do *gateway* VPN pode não estar destinado, a priori, a qualquer dos servidores situados na DMZ, mas sim para algum destino além. Neste caso, o tráfego decifrado seria passível de filtragem antes de alcançar seu destino. Isto não impediria que um usuário malicioso, situado na rede do parceiro, enviasse pacotes aos servidores situados na DMZ, violando a política de segurança da empresa, que determina que o tráfego oriundo da rede do parceiro, teria destino outro, que não algum equipamento situado na DMZ.

Se tivermos filial da empresa na outra extremidade da VPN, a situação é bastante parecida. O que torna este tipo de arquitetura é bastante estranha: estamos misturando tráfego oriundo de uma rede confiável, até o ponto que podemos considerar como confiável o tráfego vindo de uma rede que é uma subdivisão de nossa própria rede, com tráfego oriundo de usuários externos. Pois bem, esse tráfego "confiável", estaria acessando servidores configurados para o acesso de tráfego não confiável. Deste modo podemos estar restringindo, em muito, o acesso à informações importantes para membros de uma rede confiável. Por outro lado, o tráfego poderia ter como destino servidores situados em outros lugares que não a DMZ, e teríamos, como no caso anterior, filtragem do conteúdo dos pacotes que estavam anteriormente cifrados.

4.1.2 Numa DMZ Separada

Na DMZ separada não se tem muitos dos problemas anteriormente mencionados, pois teríamos um isolamento do tráfego decifrado com relação ao tráfego vindo direto da Internet.

Na DMZ separada a complexidade de configuração nas regras do filtro escrutinador são

maiores: mais uma interface para administração e aplicação regras. Porém, como foi anteriormente colocado, com o uso de software como o *ipchains*, pode-se ter o conjunto de regras de filtragem a ser aplicado numa determinada interface em um único bloco separado, de modo a tornar a administração destas regras mais fácil, controlando-se de modo mais transparente os acessos aos recursos da VPN. Pode-se aproveitar a existência desta DMZ para inclusão de alguns outros serviços necessários aos usuários de extranet ou de redes externas cooperativas (Nakamura, 2000), evitando o acesso desnecessário à rede interna para responder a solicitações de HTTP, FTP e outras, de usuários não totalmente confiáveis. Note-se que não está sendo realizada novamente a filtragem pós passagem pelo VPN.

No caso de usuários de filiais da própria empresa, poderíamos também ter a colocação dos recursos necessários, de acordo com a confiança que tenhamos no tráfego oriundo dessas filiais. No caso de maior confiança neste tráfego, teríamos simplesmente o deciframento e seu encaminhamento para o roteador interno e a conseqüente filtragem.

Uma desvantagem seria a duplicação de recursos. Uma solução seria a instalação de *proxies* para esses recursos.

Uma solução mais radical seria a colocação somente do *gateway* VPN dentro dessa DMZ, sendo o tráfego oriundo dela encaminhado para seu destino, seja para outra DMZ, seja para a rede interna.

4.1.3 Numa Configuração De Múltiplas DMZs

Nesta situação têm-se um filtro externo e um interno exclusivamente para a VPN. As vantagens são a simplificação de endereçamento, a divisão entre o tráfego Internet comum e o tráfego para redes confiáveis via VPN e a possibilidade de uma filtragem exclusiva (no roteador interno) das solicitações de conexões oriunda da faixa de endereços internos atribuídos à máquinas de extranet, parceiros de redes corporativas, de filiais ou de acesso remoto.

Qualquer alteração na regras desse tipo de acesso não acarretam reflexo nas regras de filtragem mais geral, que estão no outro roteador. É claro que uma configuração deste tipo significa uma duplicação de recursos físicos necessários.

Todavia isto pode ser contornado quando colocado o filtro externo e a VPN num único equipamento. Tanto algumas soluções comerciais, quanto não comerciais podem atender este tipo de topologia, porém deve-se atentar para o enfraquecimento da segurança quando se tem um único ponto de falha

No caso de uma extranet ou de parceiros corporativos, teríamos também a possibilidade, da colocação dos recursos ou equipamentos necessários nessa DMZ, contudo perderíamos a grande vantagem deste tipo de configuração, que é a possibilidade de filtragem do tráfego recém decifrado, antes que ele alcance qualquer outro equipamento da rede.

Já o tráfego vindo das filiais poderia ser filtrado imediatamente após o seu deciframento, possibilitando a aplicação efetiva das regras colocadas no início do capítulo. Com isso aumentamos o nível de segurança em relação ao tráfego vindo das filiais

Qualquer que seja a configuração adotada, é importante estarmos atento às regras gerais enunciadas no início do capítulo.

Deve-se deixar bem claro que estas configurações são básicas, outras configurações podem ser originadas a partir destas, com objetivo de atender as necessidades de uma conexão segura.

Um exemplo disto é a configuração mostrada na figura seguinte.

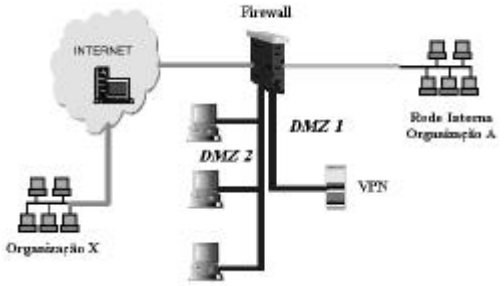

Figura 2 – Exemplo de colocação de VPN em DMZ

A partir desta figura podemos observar, que um parceiro de extranet (organização X) terá acesso aos serviços oferecidos pela organização A da seguinte forma. O tráfego cifrado com origem no gateway VPN da organização X passará pelo filtro externo, entrará na DMZ 1, será decifrado, sendo novamente submetido ao escrutínio do filtro, e só então terá acesso a DMZ 2, na qual estão localizados os serviços oferecidos pela organização A à organização X. Notemos que neste exemplo temos a aplicação clara das regras enunciadas: gateway VPN aceita somente tráfego cifrado da rede não confiável e tanto tráfego cifrado como não cifrado da rede confiável, e o restante do equipamento deve filtrar o tráfego após o deciframento por parte do gateway VPN.

Este exemplo serve também para demonstrar o casamento entre uma configuração específica de DMZ e a colocação do gateway VPN dentro de um firewall. Podemos notar claramente que a colocação de um gateway VPN numa DMZ própria casa-se perfeitamente com a recomendação que o gateway VPN seja colocado ao lado do firewall (ou na interface dedicada do firewall, conforme (Nakamura, 2000)).

4.2 VPN e Firewalls Distribuídos

Das recomendações abordadas uma ainda não foi abordada: o gateway deve ser capaz de defender-se.

Este tipo de preocupação, presente de forma difusa nos vários meios que tratam sobre segurança na Internet, está claramente enunciado em (Bellovin, 1999) e em [Loannidis e Keromytis, 2000]

Nestes artigos os autores questionam as implementações tradicionais de *firewall*, utilizando os seguintes argumentos:

- Aumento na velocidade das linhas e a presença de protocolos computacionalmente intensivos tendem a transformar o *firewall* em um ponto de congestionamento.
- A existência de extranets, de acesso remoto de participantes de uma organização quebram com a noção tradicional de perímetro de segurança
- Tendência no crescimento no número de pontos de entradas de uma rede.
- Aparecimento do ciframento fim-a-fim, com o qual o firewall convencional não pode lidar.
- Necessidade de um controle mais granular do acesso a rede interna, controle esse que só pode ser exercido pelo modelo tradicional às expensas do aumento de complexidade e da capacidade de processamento do *firewall*.

Com isso os autores propõe como solução o *firewall* distribuído, no qual, além de termos as funções tradicionais de um firewall, teríamos também um mecanismo de controle da política de segurança externa, no qual a política é definida centralizadamente, sendo aplicada em cada ponto da rede. Para isto são necessários vários quesitos: uma linguagem de política de segurança, ferramentas de gerenciamento e a utilização de IPSec em todas as conexões. Contudo outros mecanismos podem ser propostos.

Dentre as soluções propostas para este problema, encontra-se a dos *firewalls* híbridos (Bellovin, 1999): na qual alguns *hosts* vivem exclusivamente atrás de um firewall convencional, enquanto que outros vivem fora. Um *gateway* IPSec no rede central proporciona a conectividade com as máquinas externas.

A estrutura de *firewall* distribuído preconiza que cada máquina, individualmente, tenha capacidade de defesa. Porém não se pensa numa solução do tipo "*firewall* pessoal" simples. A solução deve contemplar a aplicação da política de segurança da corporação naquele ponto específico. Deste modo quando dizemos que o *gateway* VPN deve se defender de ataques vindos da Internet temos em mente duas coisas: o *gateway* VPN, e suas conexões com o mundo, como um "prolongamento" do perímetro de segurança[3]; e a conseqüente necessidade de se cumprir a política geral de segurança.

O mesmo argumento é válido quando falamos da necessidade de filtragem do tráfego pós decifrамento: existe a obrigação de se aplicar a política de segurança da corporação a um tipo de tráfego que não sofreu este crivo anteriormente, dado que estava cifrado.

Como conclusão desta faceta da colocação de uma VPN num ambiente de *firewall*, pode-se dizer que ela aparece como conseqüência da implementação da política de segurança da rede.

Com todas essas considerações pode-se propor como melhor configuração aquela na qual o *gateway* VPN é colocado numa DMZ separada, a qual nos garante a proteção do equipamento pré filtragem e a consequente filtragem do tráfego pós decifrамento.

Podemos propor como alternativa um modelo no qual a filtragem pós decifrамento seja incorporada no próprio *gateway* VPN. Este tipo de solução gera algumas conseqüências: a necessidade de que esse filtro integrado ao *gateway* siga a política geral de segurança; flexibilidade na escolha da configuração de DMZ, pois uma desvantagem das outras configurações era a dificuldade de filtragem pós decifrамento; não deve excluir a filtragem realizada no tráfego que sai da DMZ, pois este tráfego é formado tanto pela parte recém decifrada pelo *gateway* VPN, quanto pelo tráfego oriundo dos outros equipamentos da DMZ[4].

Esta alternativa gera um incremento na proposta de colocação do *gateway* VPN numa DMZ separada: além do tráfego egresso da cifragem ser filtrado, temos também o isolamento desse tráfego em relação aos outros tipos, podendo-se proporcionar serviços exclusivos e adequados a extranet, a redes cooperativas e a filiais.

CONCLUSÕES

Neste artigo procurou-se discutir a problemática da inserção de um *gateway* dentro de uma estrutura de segurança.

Analisaram-se várias alternativas de posicionamento de um *gateway* VPN dentro de uma estrutura de *firewall*.

Chegou-se a conclusão à conclusão que a melhor alternativa é a colocação do *gateway* VPN numa DMZ separada das demais.

Como alternativa, e seguindo a tendência dos "*firewalls* distribuídos", sugeriu-se a incorporação no *gateway* VPN, de mecanismos que permitissem a filtragem pós decifrамento no próprio *gateway*, permitindo uma maior flexibilidade no posicionamento do *gateway* dentro das configurações de DMZ possíveis. Ainda assim a colocação numa DMZ separada parece ser a alternativa mais atraente.

[3] Neste caso não estaríamos pensando o perímetro de segurança como as rígidas muralhas de um castelo, mas sim como possuindo uma estrutura parecida com a de um protozoário, cujos limites físicos alongam-se ou se encolhem conforme a necessidade.

[4] É importante ressaltar que a incorporação da filtragem pós decifrамento no gateway VPN possibilita o uso de uma gama maior de configurações de DMZs.

BIBLIOGRAFIA

BELLOVIN, S. M., *Distributed Firewalls*, ;login: magazine, special issue on security. November 1999

CHESWICK, William R.; BELLOVIN, Steven M.. *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley, 1994.

CHAPMAN, D.B.; ZWICKY, E.D, *Building Internet Firewalls*, O'Reilly & Associates, 1995.

FERGUSON, P.; HUSTON, G., What is a VPN?, *http://www.employees.org/ ferguson/ vpn.pdf*, Abril 1999

FIGUEIREDO, F.J.C.; GEUS, P.L., Acesso Remoto em Firewalls e Topologia para Gateways VPN. In: *Workshop em Segurança de Sistemas Computacionais*. Anais do WSeg'2001. Florianópolis, 5 e 6 de Março, 2001, P. 49-54.

GONÇALVES, M., *Firewalls Complete*. New York, McGraw Hill Trade, 1998.

HARKINS, D.; CARREL, D., *The Internet Key Exchange*, RFC 2409, Novembro 1998, ftp://ftp.isi.edu/in-notes/rfc2409.txt

KENT ,S.; ATKINSON, R., *IP Authentication Header*, RFC 2402, IETF, Novembro 1998, ftp://ftp.isi.edu/in-notes/rfc2402.txt

KENT,S.; ATKINSON, R., *IP Encapsulating Security Payload (ESP)*, RFC 2406, IETF, Novembro 1998, ftp://ftp.isi.edu/in-notes/rfc2406.txt

KING, Christopher M., *Information Security*. *The 8 Hurdles to VPN Deployment*. March, 1999. http://www.infosecuritymag.com/ mar99/cover.htm.

KOSIUR, D., *Building and Managing Virtual Private Networks*, John Wiley & Sons, Inc, 1998

LOANNIDIS, S., KEROMYTIS, A. D., *Implementing Distributed Firewalls*, http://www.upenn.edu/ ~angelos/Papers/ df.ps.gz, 2000

NAKAMURA, E. T., *Um Modelo de Segurança de Redes para Ambientes Cooperativos*, Tese de Mestrado, IC – UNICAMP, Campinas, Setembro 2000

NAKAMURA, E. T.; GEUS, P. L., Análise de Segurança do Acesso Remoto VPN. In: *II Simpósio sobre Segurança em Informática* Anais do SSI'2000, , S. José dos Campos, SP, 24-26/10/2000, pp29-37.

RANUM, M. *Thinking About Firewalls V2.0: Beyond Perimeter Security*, http://pubweb.nfr.net/~mjr/pubs/think/ index.htm, 1997

RUSSEL, R. *Linux IP Firewalling Chains*, http://netfilter.filewatcher.org/ipchains/