Software Livre na Implementação de uma Intranet Segura

Mércia Maria Rocha Costa[1] mercia.nat@zaz.com.br
Galileu Batista de Sousa[2] galileu@info.ufrn.br
Edgard de Faria Corrêa[3] edgard@info.ufrn.br

Resumo

Este artigo apresenta uma solução para a segurança interna da rede da Universidade Federal do Rio Grande do Norte, cuja implementação foi possível devido a utilização de softwares livres.

Palavras Chaves: Software Livre, Redes de Computadores, Intranet, VPN, SSH.

Abstract

This paper presents a solution to the internal security problem of the Federal University of Rio Grande do Norte's private network, and describes how this solution was implemented using free software.

Keywords: Free Software, Computer Networks, Intranet, VPN,SSH.

1. Introdução

O ambiente acadêmico, especialmente as universidades públicas brasileiras, tem uma carência de recursos financeiros. Na área de informática busca-se soluções que requeiram plataformas mais acessíveis e sempre que possível não-proprietárias. No caso dos *softwares* livres, além da questão econômica, existe o fator do acesso ao código que possibilita a customização.

No âmbito da Universidade Federal do Rio Grande do Norte, a expansão da rede de forma a atingir todos os setores foi possível através de investimentos de projetos específicos. No entanto, os custos de manutenção e de possíveis adequações a novas situações devem permanecer dentro de um patamar aceitável em virtude das razões já citadas.

Este trabalho apresenta um modelo que visa solucionar problema de segurança dentro da intranet da UFRN, e como essa solução foi possível devido a utilização de *softwares* livres.

2. O Problema

Atualmente, a Rede UFRN atinge todos os setores e todos os segmentos de sua comunidade universitária. Isso trouxe muitos benefícios no tocante a distribuição de informação. No entanto, acarretou também sérios problemas de segurança, uma vez que dados corporativos estão transitando na rede. Esses dados corporativos, mesmo quando em pouca quantidade, possuem um grande valor agregado.

O cenário de uma rede universitária é muito difuso, uma vez que a coordenação/administração e o uso são altamente distribuídos, os níveis de responsabilidade diversificados e parte dos usuários altamente qualificada. Soluções de controle de conexões com a Internet são pouco eficazes, pois o maior nível de risco está na Intranet, não o contrário. Desenvolvedores de software adicionam camada de segurança no próprio software, tipicamente usando SSL [1], contudo os softwares mais antigos não se preocupavam com esta questão.

A organização física da rede, com a presença expressiva de *hubs* e a relativa facilidade de acesso a pontos físicos, facilitam a execução de ataques com *sniffing*, sendo uma ameaça concreta a quebra de senhas em protocolos abertos, como *Telnet*, usados em sistemas corporativos. Um outro aspecto importante é a impossibilidade de fazer uma classificação distinta de máquinas corporativas e acadêmicas, pois a mesma máquina que acessa serviços corporativos pode perfeitamente ser usada por um professor, ou por seus alunos, para realizar trabalhos de natureza acadêmica.

Além disso, existem os campi do interior que se ligam ao Campus Central através de linhas públicas e precisam fazer parte da Intranet UFRN de uma forma segura e com desempenho adequado.

---

(1) Aluna do curso de Ciências da Computação da Universidade Federal do Rio Grande do Norte (UFRN)
(2) Professor do Departamento de Informática e Matemática Aplicada (DIMAp) da UFRN
Superintendente de Informática da UFRN
(3) Técnico da Diretoria de Redes da Superintendência de Informática da UFRN
Professor dos cursos Sistemas de Informação e Engenharia de Computação da Universidade Potiguar (UnP)

2.1 A Rede UFRN

A Rede UFRN (Figura 1) atualmente é composta dos campi do interior e das unidades remotas em Natal, ligados a rede do Campus Central. O Campus Central, por sua vez, está ligado a um Firewall, que interliga a Rede UFRN a Internet através do PoP-RN (RNP) e é também responsável pela segurança da rede, controlando o acesso externo. Um outro ponto de saída para a Internet é através da DMZ (*Demilitarized Zone*), que é interligada a Embratel, através do PoP. Também ligado ao Firewall está a rede da UFRNet, o provedor de acesso a Internet da UFRN, que permite aos usuários cadastrados o acesso residencial.

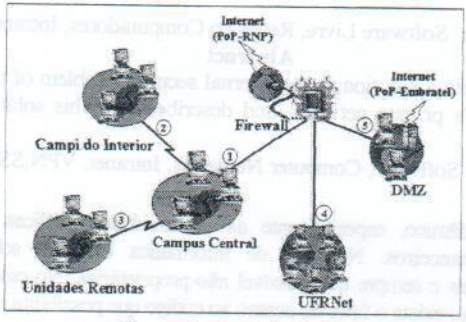

Figura 1 – A Rede UFRN

As unidade remotas em Natal, são ligadas ao Campus Central, através de linhas privadas, o que as tornam parte da mesma rede do ponto de vista de segurança. No caso dos campi do interior a utilização desta mesma solução teria um custo elevado. Optou-se então, pela utilização da ligação existente através da RNI (Rede Norte-Riograndense de Informática), o que trouxe o problema da falta de segurança, uma vez que os canais entre o PoP de Natal e os PoP do interior são canais públicos utilizados por outros usuários estranhos a UFRN.

3. A Solução Livre

A solução para a questão da expansão da rede teria que resolver a ligação com os campi do interior e garantir a segurança necessária no acesso aos servidores corporativos. Além disso, em virtude da carência de recursos, essa solução deveria ser a mais econômica possível, sem deixar de atender a todos os requisitos de segurança, tais como: proteção física, autenticação de usuários, controle de acesso aos recursos, confidencialidade (criptografia), dentre outros.

Conseguimos aliar a funcionalidade necessária e o baixo custo na solução adotada ao utilizarmos softwares livres disponíveis, conforme descrevemos a seguir.

3.1 A Ligação do Interior

Com o objetivo de resolver o problema da ligação dos campi do interior ao Campus Central, foi implementada uma solução baseada no conceito de VPN (*Virtual Private Network*). O conceito de VPN [2] utiliza tecnologias conhecidas de rede para estabelecer, sobre uma rede pública, uma conexão ponto-a-ponto virtual por onde os dados podem trafegar de forma segura. Esses pontos são, de preferência, localizados no limite da rede ou dentro da rede privada. A infra-estrutura da RNI, através do PoP-RN em Natal e dos PoP's nos interiores onde a UFRN possui unidades, foi utilizada para estabelecer a conexão.

Na rede do interior, um *gateway* define o limite entre a rede privada e a Internet, e este foi o ponto a partir do qual o túnel foi aberto. Na rede do Campus Central, por sua vez, uma máquina dentro da rede privada foi configurada como o ponto final do túnel (Figura 2).

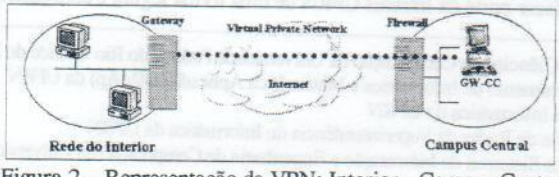

Figura 2 – Representação da VPN: Interior - Campus Central

O *Firewall* que protege a Rede UFRN faz a filtragem de pacotes e realiza o serviço de tradução de endereços de rede (NAT - *Network Address Translation*), que possibilita o acesso de forma totalmente transparente à interface interna da máquina no Campus Central responsável pelo estabelecimento do túnel.

O processo de tunelamento consistiu do encapsulamento e codificação dos pacotes que são transmitidos pela rede pública. Originalmente, o pacote transmitido possui em seu cabeçalho IP os endereços reais da origem e do destino. O encapsulamento do pacote original é feito no ponto onde o túnel é aberto, pelo protocolo PPP, que adiciona um novo cabeçalho com endereços IP virtuais. Finalmente, após ser encapsulado pelo PPP, o pacote é criptografado pelo SSH [3][4] e enviado pelo túnel. No ponto onde o túnel termina ocorre o processo inverso. O pacote é decifrado e desencapsulado restando, assim, o pacote original que é transmitido para o *host* de destino. Desta forma, tem-se a garantia de que os campi do interior têm acesso a Internet e a todos os recursos que a Rede UFRN oferece de forma segura e confiável.

O software utilizado para estabelecer a VPN entre os campi do interior e Campus Central foi o VTUN (*Virtual Tunnel over TCP/IP Networks*). Essa ferramenta cria túneis virtuais em redes TCP/IP, além de permitir compressão e criptografia nesses túneis. Outra vantagem é o fato de sua implementação ser feita completamente no nível do usuário, sem necessitar de modificações em quaisquer partes do *kernel* do sistema operacional, neste caso o Linux. O VTUN [5] é executado nos dois pontos finais da conexão, que são o *gateway* do interior (GW-Int) e o *gateway* do Campus Central (GW-CC). O GW-Int é o limite entre a rede privada e a rede pública e o GW-CC é uma máquina interna localizada dentro da rede do Campus Central.

3.2 Segurança dentro da Intranet

Com a impossibilidade de distinguir máquinas corporativas de máquinas acadêmicas, a falta de suporte à criptografia em alguns sistemas legados, entre outros fatores, chegou-se a conclusão de que deveria ser criado um modelo que seguisse a seguinte filosofia: o fluxo de dados terá que trafegar de forma clara, sem criptografia, nos pontos onde não podemos (caso de arquitetura proprietária onde não se tem suporte à criptografia) ou não devemos (caso onde o canal já é seguro) cifrar.

A solução encontrada foi isolar os servidores corporativos em um ambiente fisicamente seguro, dentro do qual o tráfego não precisa ser cifrado. Uma ou mais máquinas podem fazer a ligação entre a rede de servidores corporativos e o restante da Rede UFRN. Esta máquina não faz roteamento e somente aceita conexões seguras. Portanto, sua função será apenas receber e repassar pacotes destinados a um determinado servidor corporativo. Dessa forma, todo pacote que tem como destino final um servidor corporativo chega até a máquina intermediária de forma segura, onde então, pode ser repassado de forma limpa para o servidor de destino (Figura 3)

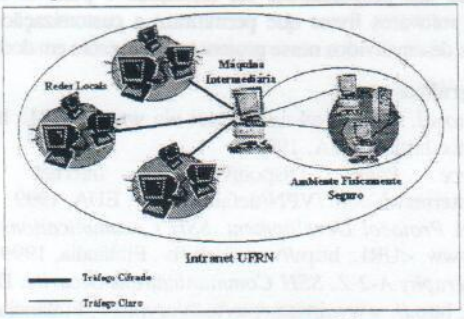

Figura 3 – Modelo de segurança para servidores corporativos

Existe uma sutil diferença no comportamento de um cliente localizado na rede do Campus Central e um cliente localizado em algumas das redes dos campi do interior quando um destes quiser se conectar a um servidor corporativo. Um cliente no Campus Central se conecta de forma segura a uma máquina também localizada no mesmo campus, que fará o papel de intermediária. Como as redes do interior estão ligadas ao Campus Central através de uma VPN, um cliente no interior, por sua vez, deve se conectar ao gateway do interior, de onde o tráfego é

repassado para o servidor corporativo de destino, através da VPN. Essa diferença se deve ao fato de querermos evitar a dupla criptografia no canal estabelecido pela VPN, o que tornaria o overhead muito significativo.

3.2.1 O Caso Especial dos Sistemas Legados

Na UFRN existem sistemas que são executados em um *mainframe*. Com a interligação desta máquina a rede torna-se necessário implementar mecanismos que assegurem a privacidade e integridade dos dados corporativos. No entanto, não existe suporte a qualquer software de criptografia ou a qualquer outro mecanismo de segurança de redes, por parte do mainframe. Então, o modelo tem que garantir que o tráfego chegue ao mainframe de forma limpa, isto é, sem criptografia, e ainda assim de forma segura.

No caso dos sistemas legados eles são acessados através do protocolo *Telnet*, o que acarreta sérios problemas de segurança, pois este protocolo não possui mecanismos para a proteção dos dados que transmite. E quando o acesso é proveniente de um cliente no interior, esses dados trafegariam de forma limpa por uma rede pública, sem sofrer nenhum tipo de codificação. Assim, o aplicativo desenvolvido (Graph-SAU [6] - um emulador de terminal para *mainframes* UNISYS a partir de componentes abertos) para ser executado nos clientes e estes emularem terminais do mainframe foi adaptado para que permitisse uma conexão segura. Isto foi conseguido utilizando uma máquina intermediária para fazer uma conexão segura (cifrada) e o redirecionamento para o mainframe, que se encontra no mesmo ambiente físico seguro. No caso dos campi do interior a máquina intermediária é o gateway do interior que já é conectado de forma segura a máquina intermediária do Campus Central, através da VPN.

Para realizar o redirecionamento no GW-CC e no GW-Int para o mainframe, foi inicialmente desenvolvido um protótipo de um redirecionador de pacotes, depois substituído pelo RINETD [7], que é uma ferramenta que redireciona conexões internet de um endereço IP e uma porta para outro endereço IP e outra porta. Dessa forma o GW-CC redireciona as conexões para o mainframe e o GW-Int para a VPN, ou seja, para o GW-CC.

4. Considerações Finais

O modelo de segurança implementado conseguiu atender as necessidades da Rede UFRN. As redes do interior foram integradas a Intranet UFRN, permitindo o acesso a todos os serviços e recursos de forma segura e confiável. Os servidores corporativos ficaram protegidos das máquinas da própria rede interna, através do isolamento em um ambiente fisicamente seguro, de modo que o acesso a esses servidores somente é realizado por uma máquina intermediária acessada pelas demais máquinas internas somente de forma segura.

O objetivo a que nos propúnhamos foi alcançado e possível de ser implementado por causa da utilização dos softwares livres que permitiram a customização e a realização com um baixo custo. Os softwares desenvolvidos nesse projeto também estão em domínio público.

5. Referências Bibliográficas

[1] *The SSL Protocol*. Disponível na internet via www: <URL: http://home.netscape.com /eng/ssl3/ssl-toc.html>, EUA, 1999.

[2] *VPN Source Page*. Disponível na internet via www: <URL: http://www.internetwk.com /VPN/default.html>, EUA, 1999.

[3] *SSH, Network Protocol Development. SSH Communications Security*. Disponível na internet via www: <URL: http://www.ssh.fi>, Finlândia, 1999

[4] *SSH, Cryptography A-2-Z. SSH Communications Security*. Disponível na internet via www: <URL: http://: www.ipsec.com/tech/crypto/>, Finlândia, 1999.

[5] *VTUN: Virtual Tunnel over TCP/IP Networks*. Disponível na internet via www: <URL: http://vtun.netpedia.net>, EUA, 1999.

[6] Albuquerque, F. A. L de, *Graph-SAU: um ambiente GUI para o sistema acadêmico (SAU)*. Monografia de graduação DIMAp/UFRN, Natal/RN, fev 1999.

[7] *RINETD: an internet redirection server for UNIX*. Disponível na internet via www:: <URL: http://www.boutell.com/rinetd>, EUA, 1999.