UNIVERSIDADE FEDERAL DE SANTA CATARINA

Segurança de Rede em Ambientes de Instituições de Ensino

Paulo Alberto Macedo Vieira Violada

Florianópolis – SC

2006 / 2

UNIVERSIDADE FEDERAL DE SANTA CATARINA

DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

CURSO DE SISTEMAS DE INFORMAÇÃO

Segurança de Rede em Ambientes de Instituições de Ensino

Paulo Alberto Macedo Vieira Violada

Trabalho de conclusão de curso apresentado como parte dos requisitos para obtenção do grau de Bacharel em Sistemas de Informação

Florianópolis – SC

2006 / 2

Paulo Alberto Macedo Vieira Violada

Segurança de Rede em Ambientes de Instituições de Ensino

Trabalho de conclusão de curso apresentado como parte dos requisitos para obtenção do grau de Bacharel em Sistemas de Informação

Orientador(a): João Bosco Mangueira Sobral

Banca examinadora

Joelson de Alencar Degaspari

Luiz Carlos Zancanella

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÖNIMOS

TI	Tecnologia da Informação
IP	Internet Protocol
NAT	Network Address Translation
PAT	Port Address Translation
TCP	Transport Control Protocol
UDP	User Datagram Protocol
RFC	Request for Comment
VPN	Virtual Private Network
IPSEC	Internet Protocol Security
URL	Uniform Resource Locator
ACL	Access Control List
AH	Authentication Header
SPD	Security Policy Database
ESP	Encapsulating Security Payload
VLAN	Virtual Local Area Network
OSI	Open Systems Interconnect
SA	Security Association
WAN	Wide Area Network
LAN	Local Area Network
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
SSH	Secure Shell
DNS	Domain Name System
ERP	Enteprise Resource Planning
QoS	Quality of Service
PBR	Policy Based Routing
DMZ	Demilitarized Zone

RESUMO

As redes de instituições de ensino têm particularidades em relação a uma empresa comum, visto que além do colaborador da instituição existe a figura do aluno. Baseado neste cenário, são definidas sugestões de padronização da rede das organizações que se assemelham ao cenário proposto. Esta padronização envolve a segmentação dos ambientes administrativos, onde se encontram os colaboradores, e educacionais, que são os laboratórios, bibliotecas e salas de aula.

Além da segmentação, é proposto o desenvolvimento de um equipamento que adicione mecanismos de segurança, desempenho, redundância e gerenciamento. Neste equipamento são definidas regras de bloqueio e acesso, registro de atividades, e um plano de contingência para casos de falha nas redes.

Para que a solução de segurança seja efetiva, são definidas diretrizes básicas de uma política de segurança para este cenário.

Palavras-chave: Segurança de rede, Política de segurança, VLAN, Firewall.

I DEFINIÇÃO DO PROBLEMA

1. Introdução

Inicialmente as redes foram projetadas com finalidade de pesquisa e o objetivo principal era permitir diversas possibilidades de conectividade entre as partes que estivessem interagindo. Portanto, a interoperabilidade foi enfatizada, e não a segurança. Atualmente, com o crescimento da demanda comercial cada vez mais acentuado, a segurança passou a ser uma necessidade fundamental, consistindo foco de discussão das pessoas envolvidas com a tecnologia de redes.

A operação em rede possibilita, entre outras coisas, ganhos de produtividade pelo compartilhamento de recursos e propagação da informação, inclusive com a finalidade de divulgação. Contudo, esses benefícios trazem alguns riscos. Conectar-se em rede significa possibilitar, mesmo que sob condições específicas e com algum tipo de controle, o acesso externo aos recursos computacionais, inclusive às informações. Assim, falhas na especificação das condições e controle de acesso podem ser exploradas por usuários da rede, externos ou internos, para obtenção de acesso não autorizado aos recursos. Essas falhas nos sistemas podem causar impactos nos mais diferentes níveis, iniciando como um simples constrangimento, passando pelo desgaste da imagem corporativa, e chegando a perdas financeiras e de mercado.

É importante notar que um planejamento para que estes riscos sejam minimizados depende do grau de importância que a segurança é vista pela organização. Definido isto, todos os processos envolvidos em uma rede de computadores podem ser delimitados de acordo com a política definida para a segurança da rede.

2. Objetivo Geral

Este estudo objetiva definir um modelo de melhores práticas de segurança de rede em uma organização com abrangência estadual que atua no ramo educacional. Pode ser aplicável a qualquer instituição que se encontre em cenários semelhantes. Baseado nisto são definidas algumas premissas básicas de segurança em relação às redes das filiais e também ao ponto central da topologia.

3. Objetos Específicos

Serão abordados os seguintes tópicos no decorrer deste trabalho:

- Definir as melhores práticas para a estruturação da rede desta instituição, para que as regras de segurança sejam mais efetivas;
- Criar um modelo padrão de regras de *firewall* para as unidades da organização;
- Definir políticas de segurança para os usuários e administradores de rede;
    - Definir direitos e responsabilidades dos usuários no ambiente de rede;
    - Definir como os recursos computacionais da organização devem ser utilizados;
    - Definir as atribuições dos administradores de rede em relação à segurança dos recursos com os quais trabalham;
    - Definir política de segurança para desenvolvimento de *software* que será utilizado na instituição.

- Especificar métodos de conexão segura das filiais à sede;
- Definir uma estrutura de registros das atividades dos equipamentos de rede.

4. Formulação do Problema

Os problemas a serem resolvidos nos ambientes corporativos refletem fielmente a situação de muitas organizações que buscam a vantagem competitiva por meio da utilização da tecnologia. O ambiente corporativo é complexo, e a segurança necessária a ser implementada é igualmente complexa, envolvendo aspectos de negócios, humanos, tecnológicos, processuais e jurídicos.

A confiabilidade, integridade e disponibilidade da estrutura de rede passam a ser essenciais para o bom andamento das organizações, necessitando de proteção. Neste contexto, a segurança de redes é parte essencial para a proteção da informação.

A importância da segurança pode ser reforçada ainda mais quando se vêem as novas oportunidades de negócios que surgem no mundo digital, condicionando seu sucesso à eficiência da estratégia de segurança. Em alguns casos a falta de segurança é traduzida na negativa de ser usada uma novidade tecnológica (NAKAMURA, 2002).

Visando as características acima, é necessário realizar a padronização da segurança de rede em ambientes de instituições de ensino, como a que será desenvolvida neste trabalho. Criação e aplicação de políticas de segurança devem ser efetivadas, assim como a inserção e configuração correta dos equipamentos de rede.

5. Justificativas e Motivações

A justificativa deste projeto é a melhoria da segurança em redes locais e de longa distância de instituições de ensino, provendo mecanismos de segurança para as filiais e garantindo que o acesso destas à sede seja tolerante a falhas.

A proposta foi baseada em experiências relacionadas a algumas visitas a instituições de ensino, que não continham padrões de segurança de rede aplicados na organização.

6. Estrutura do Trabalho

Este trabalho está dividido em oito capítulos. O primeiro capítulo aborda as informações relacionadas à proposta do trabalho, os objetivos pretendidos e as justificativas e motivações para o estudo.

O capítulo dois traz os conceitos abordados no decorrer do trabalho, observando-se segurança de rede, políticas de segurança, tecnologias e dispositivos utilizados.

Na terceira etapa é apresentado o cenário utilizado na realização deste trabalho, sendo este a base para todo o desenvolvimento. Este capítulo versa sobre aspectos gerais da rede da organização.

O capítulo quatro trata da padronização das redes apresentadas no capítulo anterior. Esta padronização é necessária para que sejam inseridos os mecanismos de segurança nas redes citadas.

Após o capítulo quatro, são abordadas as políticas de segurança criadas para a organização, visando formalizar todos os procedimentos de segurança aplicados e tornando-as cientes para os envolvidos.

Resultados e testes da implantação do desenvolvimento apresentado nos capítulos anteriores podem ser vistos no capítulo seis.

No sétimo capítulo são apresentadas as conclusões obtidas no decorrer do trabalho, assim como sugestões para trabalhos futuros.

Na última etapa do trabalho estão as fontes utilizadas para o desenvolvimento de todo o trabalho.

II FUNDAMENTAÇÃO TEÓRICA

Este capítulo fornece uma base teórica para as diferentes tecnologias utilizadas no trabalho. Os diversos conceitos abordados são necessários para um melhor entendimento deste.

1. Segurança de rede

Segurança de rede é o processo de proteger informações digitais e seus recursos. Baseia-se em três objetivos principais (Cisco Systems, 2003):

- Confidencialidade: propriedade de que a informação não estará disponível ou será divulgada a indivíduos, entidades, ou processos sem autorização;
- Integridade: refere-se à garantia de que os dados não foram alterados ou destruídos de uma maneira não autorizada. A integridade é mantida quando um dado que é enviado é idêntico ao recebido;
- Disponibilidade: consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis sem autorização, assegurando ao usuário o acesso aos dados sempre que deles precisar.

Segurança de rede é um processo contínuo construído de acordo com a política de segurança, seguindo os seguintes passos (Cisco Systems, 2003):

1. Segurança - Os seguintes métodos são usados para tornar uma rede segura:
    - Autenticação;
    - Criptografia;
    - *Firewall*;
    - Correção de vulnerabilidades.
2. Monitoração – Para garantir que a rede permaneça segura é importante monitorar o estado em que a rede se encontra. Programas que fazem a varredura da rede em busca de vulnerabilidades podem, pró-ativamente, identificar áreas de fraqueza, e sistemas de detecção de intrusão podem monitorar e responder aos eventos de segurança caso eles ocorram. Usando soluções para monitorar a segurança as organizações podem obter visibilidades sem precedentes sobre os dados e a postura de segurança da rede;
3. Testes – Testar a segurança da rede é tão importante quanto monitorar. Sem soluções de testes de segurança de rede é impossível saber sobre novos ou existentes ataques;
4. Aprimoramento – Monitorar e testar provêem os dados necessários para a melhoria da segurança da rede. Administradores e engenheiros devem usar as informações provenientes da fase de monitoração e testes para que sejam feitas melhorias à implementação de segurança utilizada na rede, assim como ajustar a atual política de segurança assim que novas vulnerabilidades e riscos sejam identificados.

2. Política de segurança

De acordo com a RFC 2196 (Site Security Handbook), uma política de segurança é a expressão formal das regras pelas quais é fornecido acesso aos recursos tecnológicos da empresa.

Uma política de segurança é um instrumento importante para proteger a organização contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade. A política de segurança não define procedimentos específicos de manipulação e proteção da informação, mas atribui direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação. Desta forma, elas sabem quais as expectativas que podem ter e quais são as suas atribuições em relação à segurança dos recursos computacionais com os quais trabalham. Além disso, a política de segurança também estipula as penalidades às quais estão sujeitos aqueles que a descumprem (CERT.Br, 2006).

2.1 Planejamento

Segundo ABREU (2004), pode-se dividir a política de segurança em três níveis: nível estratégico, nível tático e nível operacional.

- Nível estratégico: Quando se fala em nível estratégico objetiva-se o alinhamento nos valores da empresa, ou seja, no rumo a ser seguido. Quando for necessário o profissional tomar uma decisão sobre uma situação nova, deve-se usar o bom senso na tomada da decisão seguindo os valores da empresa.

- Nível tático: para o nível tático deve-se pensar em padronização de ambiente. Equipamentos, *software*, senhas, utilização de correio eletrônico, cópias de segurança, segurança física, etc. Tudo isso precisa e deve ser padronizado.
- Nível operacional: a palavra chave no nível operacional é detalhamento, para garantir a perfeição no atendimento e continuidade dos negócios, independentemente do fator humano. Se a configuração está no papel, ou seja, se existe um padrão formalizado, então este padrão deve ser seguido e a configuração deve ser realizada de forma igual por todos.

Os elementos de uma política de segurança devem manter a disponibilidade da infra-estrutura da organização. Os elementos a seguir são essenciais para a definição e implantação da política de segurança:

- Vigilância: todos os funcionários da organização devem entender a importância da segurança para a mesma.
- Atitude: é a postura e a conduta em relação à segurança, é essencial que a política seja de fácil acesso e que seu conteúdo seja de conhecimento de todos os funcionários da organização.
- Estratégia: deve ser criativo quanto às definições da política e do plano de defesa contra intrusões, possuir a habilidade de se adaptar às mudanças.
- Tecnologia: a solução tecnológica deverá suprir as necessidades estratégicas da organização, deve-se tomar cuidado com qualquer tecnologia um pouco inferior, pois poderá causar uma falsa sensação de segurança, podendo colocar em risco toda a organização.

2.2 Definição

A política de segurança deve ser definida de acordo com os objetivos de negócios da organização. Existem algumas diretrizes para descrever a política de segurança (WADLOW, 2000):

- Mantenha-se compreensível: uma política de segurança deve ser de fácil entendimento para toda a organização;
- Mantenha-se relevante: se existir necessidade, a política de segurança poderá ser um documento extenso. Para que isto seja resolvido, podem ser criados módulos desta política, sendo estes direcionados a públicos específicos dentro da empresa;
- Saiba o que não é relevante: algumas partes da política terão tópicos que não deverão ser conhecidos por todas as pessoas.

Alguns detalhes relevantes em uma política de segurança podem ser inseridos em normas e procedimentos específicos e que podem ser definidos com base na análise do ambiente da rede e de seus riscos, são:

- A segurança é mais importante do que os serviços, caso não existir conciliação a segurança deve prevalecer;
- A política de segurança deve evoluir constantemente, de acordo com os riscos e as mudanças na estrutura da organização;
- Aquilo que não for expressamente permitido, será proibido;
- Nenhuma conexão direta com a rede interna, originária externamente, deverá ser permitida sem que um rígido controle de acesso seja definido e implementado;
- Os serviços devem ser implementados com a maior simplicidade possível;

- Devem ser realizados testes, a fim de garantir que todos os objetivos sejam alcançados;
- Nenhuma senha dever ser fornecida sem a utilização de criptografia.

As características de uma boa política de segurança são (RFC 2196):

1. Deve ser implementável através de procedimentos de administração, publicação das regras de uso aceitáveis ou outros métodos apropriados;
2. Deve ser exigida com ferramentas de segurança, onde apropriado, e com sanções onde a prevenção efetiva não seja tecnicamente possível;
3. Deve definir claramente as áreas de responsabilidade para os usuários, administradores e gerentes.

Os componentes de uma boa política de segurança incluem (RFC 2196):

1. Guias para a compra de tecnologia computacional que especifiquem os requisitos ou características que os produtos devem possuir;
2. Uma política de privacidade que defina expectativas razoáveis de privacidade relacionadas a aspectos como a monitoração de correio eletrônico, registros de atividades e acesso aos arquivos dos usuários;
3. Uma política de acesso que define os direitos e os privilégios para proteger a organização de danos, através da especificação de linhas de conduta dos usuários, pessoal e gerentes. Ela deve oferecer linhas de condutas para conexões externas, comunicação de dados, conexão de dispositivos a uma rede, adição de novos softwares, etc.

4. Uma política de contabilidade que defina as responsabilidades dos usuários. Deve especificar a capacidade de auditoria e oferecer a conduta no caso de incidentes (por exemplo, o que fazer e a quem contactar se for detectada uma possível intrusão);
5. Uma política de autenticação que estabeleça confiança através de uma política de senhas efetiva, e através da linha de conduta para autenticação de acessos remotos e o uso de dispositivos de autenticação;
6. Um documento de disponibilidade que define as expectativas dos usuários para a disponibilidade de recursos. Ele deve endereçar aspectos como redundância e recuperação, bem como especificar horários de operação e de manutenção. Ele também deve incluir informações para contato para relatar falhas de sistema e de rede;
7. Um sistema de tecnologia de informação e política de manutenção de rede que descreva como o pessoal de manutenção interno e externo devem manipular e acessar a tecnologia. Um tópico importante a ser tratado aqui é como a manutenção remota é permitida e como tal acesso é controlado. Outra área que deve ser considerada é a terceirização e como ele é gerenciada;
8. Uma política de relatório de violações que indique quais os tipos de violações que devem ser relatados e a quem estes relatos devem ser feitos. Uma atmosfera de não ameaça e a possibilidade de denúncias anônimas irá resultar uma grande probabilidade que uma violação seja relatada;

9. Suporte à informação que ofereça aos usuários informações para contato para cada tipo de violação; linha de conduta sobre como gerenciar consultas externas sobre um incidente de segurança, ou informação que seja considerada confidencial ou proprietária; referências cruzadas para procedimentos de segurança e informações relacionadas, tais como as políticas da companhia e leis e regulamentações governamentais.

2.3 Implementação

A implementação deve envolver toda a organização, todos os usuários devem conhecer e passar a utilizar a política.

Devem ser feitos programas de conscientização e divulgação da política, de modo que com a divulgação efetiva ela deverá tornar-se parte da cultura da organização.

Segundo a norma NBR ISO 17799, as seguintes análises críticas periódicas também devem ser agendadas:

- Verificação da efetividade da política, demonstrada pelo tipo, volume, e impacto dos incidentes de segurança registrados;
- Análise do custo e impacto dos controles na eficiência do negócio;
- Verificação dos efeitos de mudanças na tecnologia utilizada.

3. Virtual Local Area Network (VLAN)

Uma VLAN (Virtual Local Area Network – Rede local virtual) é um agrupamento lógico de estações, serviços e dispositivos de rede, criado por um ou mais *switches*, que não estão restritos a um segmento físico de uma rede local. As VLANs podem ser agrupadas por funções operacionais ou por

departamentos, independentemente do local físico dos usuários. Os dispositivos em uma VLAN só comunicam com os dispositivos existentes na mesma VLAN. Os roteadores providenciam a conectividade entre diferentes VLANs (Cisco Systems, 2003).

As VLANs aumentam o desempenho geral da rede pela agregação lógica dos usuários e recursos, diminuindo os domínios de *broadcast*[1]. Elas podem melhorar a escalabilidade, segurança e gerenciamento da rede (Cisco Systems, 2003).

Os *switches* criam uma tabela de endereços em separado para cada VLAN. Quando um quadro é recebido verifica-se o endereço de origem em relação à tabela de endereços, de forma que ele possa ser adicionado no caso de ainda ser desconhecido. O *switch* descobre os endereços e toma decisões de encaminhamento usando uma tabela de endereços por VLAN (ODOM, 2002).

Implementar VLANs com múltiplos *switches* acrescenta a necessidade de identificar a qual VLAN um quadro pertence. VLAN *Tagging* (ou *trunking*) é o processo de acrescentar um cabeçalho adicional a um quadro LAN com o intuito de identificar a qual VLAN o quadro pertence. O IEEE 802.1Q é um protocolo de entroncamento (*trunking*) utilizado para conseguir esse efeito (ODOM, 2002).

O entroncamento também pode ser utilizado entre um *switch* e um roteador. O entroncamento entre um *switch* e um roteador reduz o número necessário de interfaces do roteador. O mesmo método de *tagging*, usado entre switches, é utilizado para quadros enviados ao roteador, assim, o roteador pode saber de qual VLAN o quadro partiu. Quando trabalha entre duas VLANs, o

[1] Envio de mensagem para todos os computadores alocados no mesmo segmento de rede.

roteador atribui ao quadro que chega um ID de VLAN (como o faz com o quadro que sai), antes de enviar o quadro de volta ao *switch* (ODOM, 2002).

4. Firewall

O *firewall*, um dos principais componentes de segurança de qualquer organização (NAKAMURA, 2002; ACCARDI, 2005), serve como a primeira linha de defesa contra tráfego não autorizado e potencialmente malicioso.

Apesar de normalmente discutido no contexto de conectividade com a *Internet*, o *firewall* também, possui aplicabilidade em ambientes de rede que não incluem ou precisam desta conectividade. Muitas corporações implementam *firewalls* em sua rede empresarial para restringir conectividade de e para redes internas mais sensíveis (WACK, 2002).

A função de um *firewall* é mapear cada pacote que entra ou sai de uma dessas redes a um conjunto de decisões predefinidas, como aceitar ou descartar (GOUDA, 2005).

4.1 Filtro de Pacotes

Segundo WACK (2002), os *firewalls* baseados em filtro de pacotes são os mais básicos e fundamentais, sendo essencialmente dispositivos de roteamento que incluem a funcionalidade de controle de acesso para sessões de comunicação. Operam na camada de rede do modelo OSI, porém, podem utilizar campos da camada de transporte do mesmo modelo.

Os *firewalls* de filtro de pacotes realizam suas decisões de filtragem baseados no conteúdo do cabeçalho do segmento e em um conjunto de regras (ACCARDI, 2005). Alguns dos campos analisados são: endereço de origem,

endereço de destino, tipo de tráfego, porta de origem e porta de destino. Assim, as regras dos filtros de pacotes são definidas de acordo com endereços da camada de rede ou com os serviços (portas TCP/UDP relacionadas) permitidos ou proibidos (NAKAMURA, 2002).

Ainda segundo NAKAMURA (2002), por tomar decisões analisando apenas os pacotes em si, sem considerar informações de pacotes anteriores, este tipo de *firewall* é classificado como *firewall* sem estado. Os *firewalls* de filtro de pacotes deixam brechas permanentes no perímetro da rede, abrindo possibilidades de ataques, que podem ser minimizados pelo filtro de pacotes baseado em estados.

4.2 Filtro de Pacotes Baseados em Estados

Filtros de pacotes baseados em estados são filtros de pacotes que incorporam a percepção adicional dos dados da camada de transporte do modelo OSI. Este tipo de *firewall* realiza suas decisões de filtragem baseado no conteúdo do cabeçalho do segmento, em um conjunto de regras e no estado obtido de pacotes anteriores (ACCARDI, 2005). Por analisar não somente os pacotes em si, mas também o estado de pacotes anteriores, este tipo de *firewall* é classificado como *firewall* com estados (GOUDA, 2005).

A análise de pacotes baseada em estados evoluiu da necessidade de acomodar certas características da pilha de protocolos TCP/IP que tornam difícil a implementação de um *firewall*. Quando uma aplicação TCP cria uma sessão com um servidor remoto, uma porta alta com número maior do que 1023, escolhida de forma aleatória, é criada no sistema de origem para o propósito de receber informações do sistema de destino (WACK, 2002). Permitindo a entrada destas

portas de uma forma estática cria-se um grande risco de intrusão por usuários não autorizados.

Com os *firewalls* de filtro de pacotes baseados em estados, o conjunto de regras pode levar em conta apenas os inícios das conexões, abrindo apenas temporariamente o perímetro da rede (NAKAMURA, 2002). Usando um *firewall* com estados para proteger a rede privada, pode-se obter um controle de acesso mais apurado através do acompanhamento das conexões entre a rede privada e a *Internet* (GOUDA, 2005).

5. Proxy Web

O *proxy web* tem sido considerado como a ferramenta principal para lidar com a sempre crescente demanda da busca da informação através da *Internet*, WWW sendo um exemplo típico (LI, 1999). Os *proxies web* encaminham requisições HTTP de uma rede interna para a *Internet* e retransmitem as respostas correspondentes às redes internas, assim agindo como um *firewall* (MALTZAHN, 1997; NAKAMURA, 2002). Também podem ser configurados para armazenar temporariamente (*cache*) estas respostas, melhorando a segurança, reduzindo o uso da banda disponível e reduzindo a latência da rede (MALTZAHN, 1997).

O princípio básico através do *caching* é que ele permite que documentos obtidos sejam mantidos perto dos clientes, reduzindo o tempo de resposta de serviços *web* e aliviando o congestionamento da rede em ambientes *web*. A melhor maneira de utilizar o princípio de *caching* para reduzir a latência geral é através do uso do *proxy web* (LI, 1999).

O *caching web* funciona da seguinte forma: quando um usuário faz uma requisição HTTP, esta requisição é analisada pela rede e redirecionada ao *cache* de rede local. Se o *cache* de rede local contiver a página solicitada, ele responderá com a sua cópia da página, caso contrário, ele fará uma requisição própria ao servidor *web* original. O servidor *web* então responde a solicitação ao servidor *proxy*, que armazena uma cópia e a repassa ao cliente que fez a solicitação original (Cisco Systems, 2001).

Os *proxies* podem ser utilizados para realizar uma filtragem mais apurada dos pacotes por atuar na camada de aplicação do modelo OSI, podendo, por exemplo, prevenir que funcionários acessem um conjunto específico de sites *web* (Cisco Systems, 2001). Também permitem que uma organização reforce requisitos de autenticação dos usuários, assim como um outro nível de registro do tráfego que passa por ele (WACK, 2002). A conexão direta entre um usuário interno e o servidor externo não é permitida por meio desta tecnologia e o reendereçamento do tráfego, ao fazer com que o tráfego pareça ter origem no *proxy*, mascara o endereço da máquina interna, garantindo assim uma maior segurança de rede interna da organização (NAKAMURA, 2002).

6. Network Address Translation (NAT)

Com o *Network Address Translation*, ou tradução de endereços de rede, um bloco de endereços públicos é utilizado para traduzir endereços de máquinas em um domínio privado enquanto elas originam sessões para domínios externos. Para pacotes originados dentro da rede privada, o endereço IP de origem é traduzido. Para pacotes originados fora da rede privada, o endereço IP de destino é traduzido (IETF – RFC2663, 1999). O NAT está limitado a utilizar apenas

endereços IP, tornando a tradução de um endereço público para apenas um endereço privado (IETF – RFC3022, 2001). O total de conexões com máquinas externas está limitado ao número de endereços públicos disponíveis (WACK, 2002).

6.1 Port Address Translation (PAT)

PAT (tradução de endereços de porta) estende a noção de tradução de endereços incluindo os identificadores da camada de transporte da arquitetura TCP/IP, como portas TCP e UDP e identificadores de requisições ICMP. Isto permite que os identificadores da camada de transporte de várias máquinas de rede privada sejam multiplexados para identificadores de camada de transporte de um único endereço IP público (IETF – RFC2663, 1999). O PAT permite que um conjunto de máquinas compartilhe um mesmo endereço IP público. Assim como o mapeamento de tuplas de tipo (endereço IP local, número de porta local) para tuplas do tipo (endereço IP público, número de porta atribuída) (IETF – RFC3022, 2001).

.

7. Virtual Private Network (VPN)

Uma VPN (rede privada virtual) é uma rede virtual construída em cima de uma rede existente que pode fornecer um mecanismo de comunicação seguro para dados e informações IP transmitidos entre redes (FRANKEL, 2005). Ela permite o envio de dados entre dois computadores através de uma rede compartilhada, ou pública, de uma maneira que emula as propriedades de um enlace privado ponto-a-ponto (DAVIES, 2004). Assim, quando a VPN é utilizada,

o serviço aparece para o usuário como se estivesse conectado diretamente à rede privada, quando na realidade utiliza uma infra-estrutura pública (NAKAMURA, 2002). Isto é normalmente mais barato que alternativas como linhas de telecomunicações dedicadas entre organizações ou filiais (FRANKEL, 2005).

Os conceitos que fundamentam a VPN são a criptografia e o tunelamento (NAKAMURA, 2002). Tunelamento é um mecanismo pelo qual as comunicações *site-to-site* de uma aplicação são protegidas de acesso não-autorizado através do encapsulamento dos dados dentro dos protocolos de transmissão de uma aplicação completamente diferente. Usando esta técnica, o fluxo de dados original também pode ser criptografado e autenticado para protegê-lo contra leitura e modificação não-autorizada (O'GUIN, 1999), sendo o IPSec o padrão *de facto* das VPNs (NAKAMURA, 2002). O tunelamento emula o enlace ponto-a-ponto e a criptografia emula o enlace privado (DAVIES, 2004).

Um túnel opera como um revestimento através do *backbone*, e o tráfego enviado através do túnel é opaco para o *backbone*. Um ponto final de uma VPN pode terminar múltiplos túneis ou encaminhar pacotes entre diferentes túneis. Túneis diferentes podem compartilhar o mesmo enlace físico e o tráfego pertencente a um mesmo túnel VPN pode ser carregado por diferentes enlaces físicos (LIANG, 2002).

A criptografia é utilizada para garantir a autenticidade, o sigilo e a integridade das conexões, e é a base da segurança dos túneis VPN (NAKAMURA, 2002). VPNs podem usar ambas as formas de criptografia, simétrica e assimétrica. A maioria dos dados trafegados em uma VPN normalmente são criptografados utilizando a criptografia simétrica, que requer

menor poder de processamento e é geralmente mais eficiente (FRANKEL, 2005). O único tráfego visível na WAN é o tráfego VPN criptografado e/ou autenticado, tornando-o ilegível e imutável por usuários não-autorizados. Esta proteção pode ser aplicada a todos os protocolos de *Internet* normalmente utilizados (O'GUIN, 1999).

Implementações VPN geralmente consistem em dois tipos de componentes: um *gateway* VPN que é instalado para servir todos os computadores em um único site, e um cliente VPN que permite a conexão de uma máquina à VPN. O *gateway* VPN é normalmente um sistema autônomo que permite comunicações VPN *site-to-site* e *site-to-host* de fora do *site*. O cliente VPN é um pacote de *software* separado que é instalado em máquinas convencionais para permitir que elas estabeleçam enlace*s* de comunicação *host-to-site* seguros com o *gateway* VPN (O'GUIN, 1999).

8. IP Security (IPSec)

O IPSec foi criado para prover segurança inter-operável e de alta qualidade baseada em criptografia para o IPv4 e o IPv6. Oferece controle de acesso, integridade sem conexão, autenticação de origem, proteção contra *replay* e confidencialidade. Estes serviços são providos na camada IP, oferecendo proteção para o IP e/ou protocolos de camadas superiores (IETF – RFC2401, 1998).

Um conceito chave que aparece tanto no mecanismo de autenticação quanto no de confidencialidade para o IP é a associação de segurança (AS – Security Association). Uma SA é uma relação de uma via entre o emissor e o

receptor que fornece serviços de segurança para o tráfego carregado nela. Uma SA pode utilizar o ESP[2] ou o AH[3], mas não ambos (STALLINGS, 2003).

De acordo com STALLINGS (2003), o *Security Policy Database*[4] (SPD) relaciona o tráfego IP a SAs específicas, ou nenhuma SA no caso de tráfego permitido para contornar o IPSec. Na sua forma mais simples, um SPD contém entradas, onde cada entrada define um subconjunto de tráfego IP e aponta uma SA para esse tráfego.

O AH e o ESP suportam dois modos de operação: modo túnel e modo transporte. No modo transporte o ESP protege apenas os dados do pacote IP e o AH protege os dados e alguns campos do cabeçalho IP. No modo túnel os protocolos protegem todo o pacote IP através do tunelamento deste pacote. Sempre que uma das pontas de uma SA for um *gateway* de segurança, a SA tem que ser de modo túnel (IETF – RFC2401, 1998).

No modo túnel, o ESP cria um novo cabeçalho IP para cada pacote. Este novo cabeçalho lista os pontos finais do túnel ESP (como dois *gateways* IPSec) como a origem e o destino do pacote. Por isto, o modo túnel pode ser utilizado para as VPNs. Este modo pode criptografar e/ou proteger a identidade dos dados e do cabeçalho IP original de cada pacote (FRANKEL, 2005).

A implementação difundida e o uso do IPSec requer um protocolo de gerenciamento de SA escalonável, automatizado e que seja padrão da *Internet*. O protocolo de gerenciamento de chaves automatizado padrão para uso com o IPSec é o *Internet Key Exchange* (IKE) (IETF – RFC2401, 1998). O IKE tem como base *o Internet Security Association and Key Management Protocol* (ISAKMP) e o Oakley, que é o responsável pela troca de chaves (NAKAMURA, 2002).

[2] Protocolo IPSec que provê confidencialidade dos dados em trânsito.
[3] Protocolo IPSec que verifica se os dados não foram modificados em trânsito.
[4] Retém as informações sobre as políticas de segurança de um dispositivo.

9. Host Intrusion Detection System (HIDS)

Host-based Intrusion Detection System, ou, Sistema de Detecção de Intrusão baseado em *Host* monitora parte, ou todo o comportamento dinâmico de um sistema. Assim como um Sistema de Detecção de Intrusão baseado em Rede, inspecionando dinamicamente os pacotes que trafegam na rede, um HIDS pode detectar modificações não autorizadas no sistema, sejam elas realizadas por pessoas ou por programas (Wikipedia, 2006).

O sistema de detecção de intrusão baseado em *host* faz o monitoramento do sistema, com base em informações de arquivos de *logs* ou de agentes de auditoria. O HIDS pode ser capaz de monitorar acessos e alterações em importantes arquivos do sistema, modificações nos privilégios dos usuários, processos do sistema, programas que estão sendo executados, uso da CPU, entre outros aspectos, como a detecção da atividade de varredura de portas (NAKAMURA, 2002).

O HIDS pode também realizar, por meio de *checksums*[5], a checagem da integridade dos arquivos do sistema. Essa característica é importante, porque os arquivos corrompidos, que podem ser *backdoors*[6], são detectados antes que causem problemas mais sérios (NAKAMURA, 2002).

Ao identificar alguma ocorrência suspeita, o HIDS pode enviar algum tipo de notificação ao administrador, que poderá tomar as devidas providências em relação ao ocorrido. Alguns HIDSs podem ser pró-ativos, baseados em regras pré-configuradas, podendo então informar ao administrador uma ocorrência suspeita, e, ao mesmo tempo, realizar algum tipo de operação para que essa ocorrência não seja concluída, prevenindo o sistema contra eventuais ataques.

[5] Valor calculado para testar a integridade do arquivo.
[6] Programa que permite a um invasor retornar a um computador comprometido.

III Cenário Atual

1. Visão Geral

O cenário de rede que será usado para definir este trabalho aborda a rede de uma instituição de ensino que detém uma rede privada de alta capilaridade, com pontos de presença de abrangência estadual, conectando-se a um ponto central onde está localizada a sede desta empresa.

Na sede estão localizados todos os serviços essenciais para a instituição, como sistema de ERP corporativo, que é acessado através de conexões remotas, servidores de *e-mail* e *web*, assim como o servidor de banco de dados que contém as informações cruciais para a sede e suas filiais.

O acesso à *Internet* desta organização se dá pela sede, sendo este usado tanto pelos funcionários da sede quanto das filiais. É por este enlace que as requisições externas aos servidores da empresa chegam.

Concentrar o acesso à *Internet* no ponto central pode ser considerado um risco para a organização já que:

- O uso exacerbado deste enlace pode comprometer o acesso externo aos serviços disponíveis;
- Caso este enlace venha a ter problemas, como queda ou problema com o equipamento que realiza a conexão, toda a organização (sede e filiais) tem seu acesso prejudicado.

Um esboço desta rede pode ser visto na figura 1:

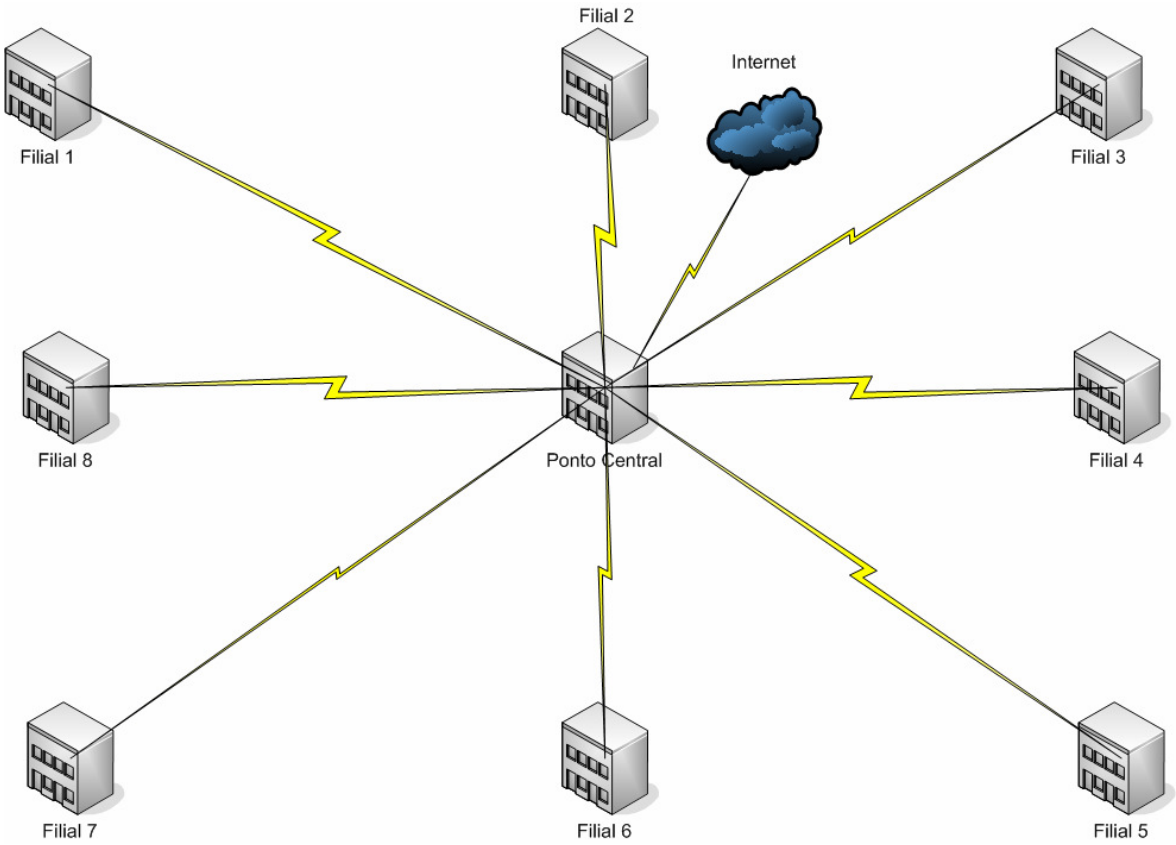

Figura 1 – Topologia de rede da organização

Para as conexões entre as filiais e o ponto central são utilizados enlaces *Frame Relay*, caracterizando-se uma rede privada desta organização. Os dados não trafegam pela *Internet* quando existe comunicação entre o ponto central e as unidades.

1.1 Filiais

Nas filiais estão localizados os alunos desta instituição de ensino, os professores e os colaboradores responsáveis pelo funcionamento da filial.

As dependências das filiais são organizadas em: áreas de colaboradores (funcionários da unidade), áreas para os professores (sala dos professores e laboratórios) e os laboratórios de informática para os alunos.

Uma descrição básica da rede destas filiais pode ser observada abaixo:

- Rede local contendo os colaboradores da unidade (ambiente administrativo) e salas de aula e laboratórios (ambiente educacional);
- Servidores de arquivos;
- Servidor de antivírus;
- Uma conexão com a rede privada até o ponto central da topologia (rede corporativa).

A topologia da rede pode ser verificada na figura 2:

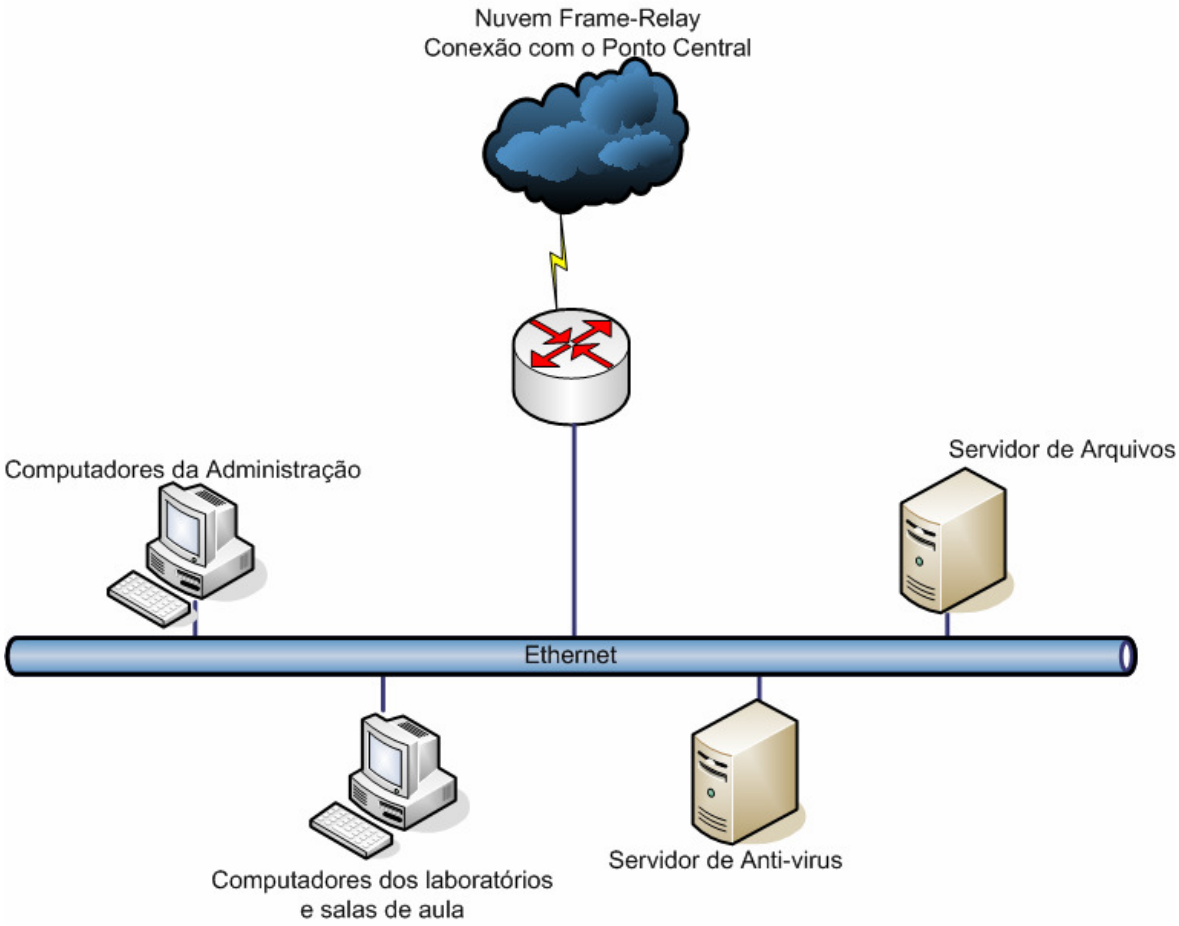

Figura 2 – Rede local das unidades

Algumas abordagens de segurança referentes a esta topologia são:

- Como todos os usuários e servidores estão em uma mesma rede podem existir acessos indevidos de pessoas não autorizadas a utilizar um recurso específico;
- Acessos aos sistemas corporativos podem ser realizados por qualquer pessoa que estiver na rede desta unidade, podendo ser aluno ou visitante (que não poderia ter esta permissão);

- É possível coletar informações sigilosas da organização de qualquer parte da rede.

1.2 Ponto Cental

O ponto central concentra todos os dados corporativos da organização, alocando os servidores que são acessados pela *Internet* e pelas filiais. A sede funciona como um braço gerencial das unidades, não contém alunos, laboratórios ou professores como nas filiais. É constituída basicamente dos diretores da organização e dos colaboradores que tratam as questões corporativas.

Como suas características se diferem bastante das filiais, a estrutura de rede da sede também contém suas especificidades e complexidades devido ao alto grau de importância na instituição.

Descrevendo brevemente o conteúdo da rede da sede, se obtém:

- Servidores *Web*;
- Servidor de *e-mail*;
- Servidor de antivírus;
- Servidor de banco de dados;
- Servidor de arquivos;
- Rede local com os colaboradores desta unidade.

A topologia de rede do ponto central da organização pode ser visualizada na figura 3:

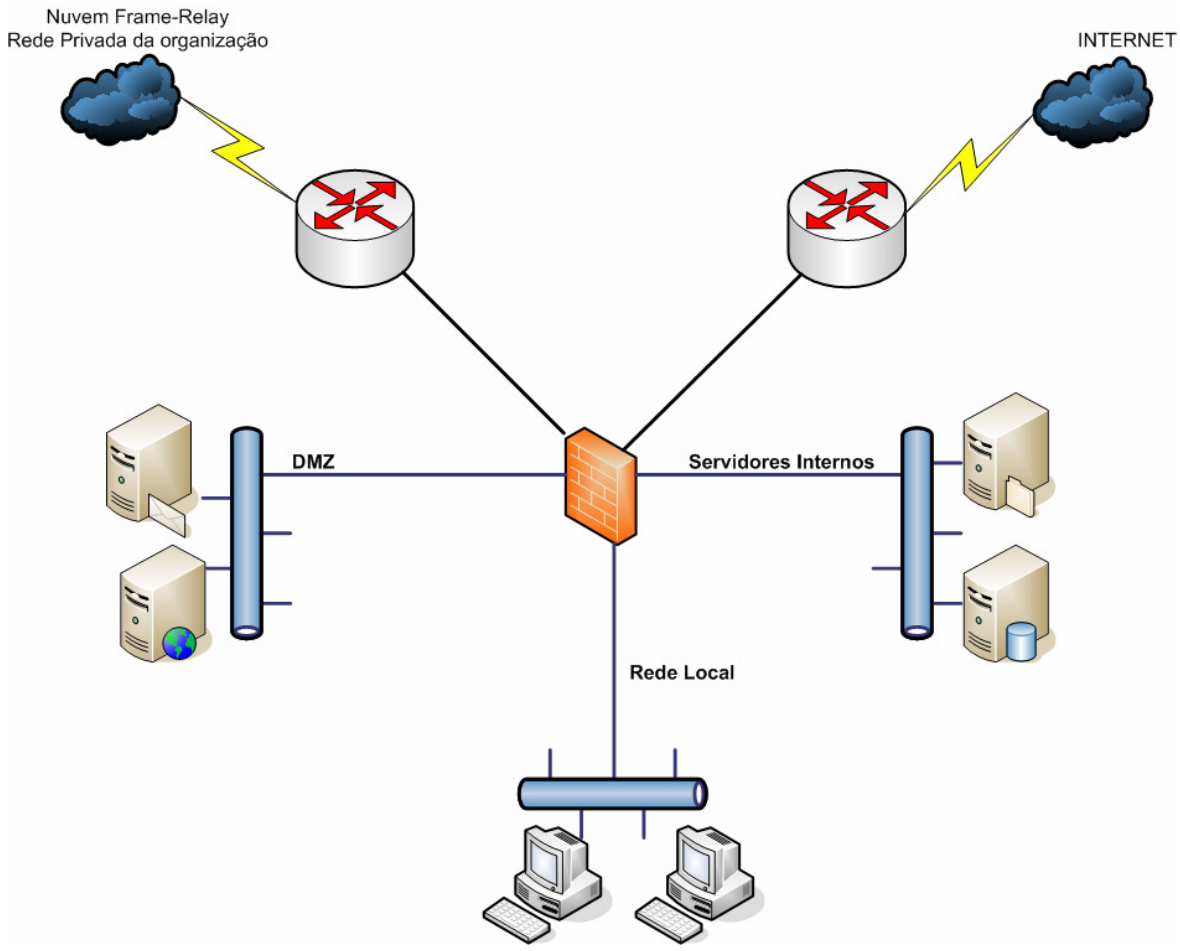

Figura 3 – Ponto central da topologia

De acordo com a figura 3, é possível notar que já existe uma segmentação lógica para garantir a segurança da rede da sede. Os servidores acessíveis via *Internet* e rede privada estão localizados em uma área desmilitarizada (DMZ), que contém regras de acesso localizadas no *firewall*, autorizando o acesso somente às portas específicas daqueles servidores.

Os servidores que estão localizados na DMZ são: servidor *Web* e servidor de e-mail. Qualquer tipo de acesso a estes servidores precisa ser liberado pelo

firewall da instituição, seja ele proveniente da *Internet*, rede privada, ou rede local. Isto garante que os servidores não fiquem expostos diretamente sem qualquer tipo de controle de acesso.

O intuito de utilizar uma DMZ na rede da sede é garantir que os servidores de *e-mail* e *Web* possam desempenhar suas funções, mas que o restante da rede continue protegido, já que os acessos externos só devem chegar até estes serviços, e jamais aos restantes na rede.

Os outros servidores localizados na rede são o servidor de arquivos e o servidor de banco de dados. Estes servidores estão separados de todos os outros servidores e máquinas clientes através de regras de *firewall*, e da segmentação lógica da rede. Novamente, qualquer tipo de acesso a estes servidores deve ser liberado pelas regras de controle de acesso que estão configuradas no *firewall* da rede. Para que o servidor *Web* possa utilizar os dados que estão no banco de dados, deve ser criada uma regra de *firewall* liberando o acesso ao recurso necessário. Qualquer outro tipo de comunicação entre os servidores da DMZ e as redes internas deve ser bloqueado.

O acesso dos colaboradores da sede à *Internet*, servidores de e-mail e *Web* e aos servidores internos está previamente liberado pelo *firewall*, garantindo assim, acesso aos recursos e dados da organização aos colaboradores da sede. Baseado no exposto, o enfoque deste trabalho está relacionado à segurança da rede das filiais desta instituição.

IV METODOLOGIA/DESENVOLVIMENTO

Neste capítulo será apresentada a solução adotada na padronização das redes das filiais, assim como os equipamentos utilizados. Esta padronização é necessária para que sejam implementados os mecanismos de segurança nas redes citadas.

1 Padronização das redes das filiais

Algumas considerações sobre as redes das filiais desta organização são:

- Falta de padronização da segurança de rede;
- Problemas de desempenho no acesso aos conteúdos corporativos e à *Internet* em momentos de uso intensivo da rede.

A solução encontrada para resolver estes problemas foi a inclusão de ativos de rede que possam garantir os níveis desejados na padronização da segurança, como exemplo, podem ser substituídos *hubs* por *switches,* incluir *firewalls* na rede e a criação de políticas de segurança.

Com estes padrões é possível obter um nível de segurança que não existia anteriormente, podendo a rede ser segmentada logicamente para que o tráfego corporativo, proveniente dos colaboradores não seja visível pelos alunos, que estão localizados em laboratórios de informática e bibliotecas.

Para permitir que as considerações de segurança apresentadas não permaneçam na instituição, foram definidas algumas novas características:

- Criação de VLANs para segmentar o tráfego entre as diferentes redes:

    - VLAN RC (Rede Corporativa) – VLAN que se conecta à Rede Corporativa da organização;
    - VLAN ADM (Administrativa) – VLAN que abrange a rede administrativa (colaboradores) da filial;
    - VLAN SRV (Servidores) – VLAN que abrange os servidores;
    - VLAN EDU (Educacional) – VLAN que abrange a rede educacional;
    - VLAN INET (*Internet*) – VLAN que se conecta com a *Internet*.
- Configuração de um equipamento que faça o roteamento entre as diferentes redes, denominado Gateway Multiuso;
- Inclusão de um enlace *Internet* para que os dados corporativos tenham maior performance no enlace privado;
- Criação de uma solução de redundância dos dados destinados à sede, utilizando VPN. Caso o enlace da rede privada venha a falhar, o tráfego pode ser roteado ao ponto central através de uma VPN utilizando IPSec.

Com a inclusão destas novas características na rede das filiais obtêm-se uma padronização visando atingir o nível de segurança de rede desejado.

A criação das VLANs permite que sejam os colaboradores agrupados em segmentos de rede diferente dos alunos, garantindo que o tráfego de uma rede não se misture com o tráfego de outra. Isto é feito através da configuração dos *switches*, criando redes locais virtuais, sem a necessidade de mais equipamentos físicos para tal segmentação.

A utilização das VLANs em um equipamento de camada 2, que é o caso dos *switches* que foram adquiridos para as unidades, garantem a segmentação de redes que se encontram em VLANs diferentes, fazendo com que uma não se comunique com outra. Porém, como foram criadas 5 VLANs, cada uma com endereçamentos de rede diferentes, é necessário um equipamento que realize a comunicação entre estas redes locais virtuais de forma segura. Para que isso ocorra é sugerida a implementação de um equipamento que seja o ponto central desta rede, fazendo a função de roteador e *firewall*, garantindo assim a segurança nas comunicações. Este equipamento terá várias funções na rede da unidade, sendo denominado Gateway Multiuso.

A VLAN denominada RC (rede corporativa) é a rede que se conecta ao ponto central da organização, utilizando para isso o enlace privado entre a sede e a filial. É por esta rede que trafegam os dados corporativos da organização. Assumindo que estes dados sejam sigilosos, nenhum outro tipo de tráfego pode estar nesta VLAN, assim como nenhum equipamento que não seja o Gateway Multiuso e o roteador utilizado para a conexão com a rede privada pode estar conectado nesta rede.

Os colaboradores da unidade serão alocados na VLAN denominada ADM (administrativo). Os equipamentos que devem estar conectados nesta rede são: Gateway Multiuso, computadores dos colaboradores utilizados no ambiente administrativo e impressoras de rede.

A utilização da VLAN SRV (servidores), é permitida somente aos servidores da filial, que são os servidores de arquivo e o servidor de antivírus. Qualquer novo servidor interno que a unidade venha a adquirir deve permanecer neste segmento de rede. O acesso a estes servidores deve ser previamente

liberado pelo *firewall*, que é uma das funções do Gateway. Os equipamentos que podem estar nesta rede são: Gateway Multiuso e os servidores.

Os laboratórios de informática, e as bibliotecas informatizadas devem ter seus computadores contidos na VLAN EDU (educacional). O acesso à *Internet* é liberado pelo *firewall*. Só podem estar conectados nesta rede o Gateway Multiuso e as impressoras utilizadas pelos alunos.

Para concluir a segmentação lógica da rede, foi criada a VLAN INET (*Internet*), que é a rede utilizada para que a unidade possa se conectar à *Internet*, utilizando o roteador e o enlace de comunicação adquiridos para esta padronização. Os equipamentos que pertencem a esta rede são: roteador, *switch* e Gateway.

A inclusão de um enlace *Internet* em conjunto com o Gateway Multiuso na topologia da rede garante maior desempenho para acesso aos dados corporativos da organização, pois todo tráfego que não seja corporativo utilizará este enlace, garantindo uso exclusivo do enlace corporativo para os dados destinados a este fim. O tratamento destas informações, indicando qual enlace deve ser utilizado será feito pelo Gateway Multiuso, utilizando *Policy Based Routing*[7] (Roteamento Baseado em Políticas).

A utilização deste enlace *Internet* também será de extrema importância em um momento de contingência para o enlace corporativo, que ocorre na queda do enlace com a rede privada. No caso específico deste tipo de falha será criada uma conexão VPN, que trafegará os dados corporativos através da *Internet.* Os dados estarão criptografados, pois a VPN utilizará IPSec.

[7] Técnica utilizada para decidir rotas de rede baseadas em políticas definidas pelo administrador.

A topologia lógica das filiais pode ser visualizada na figura 4:

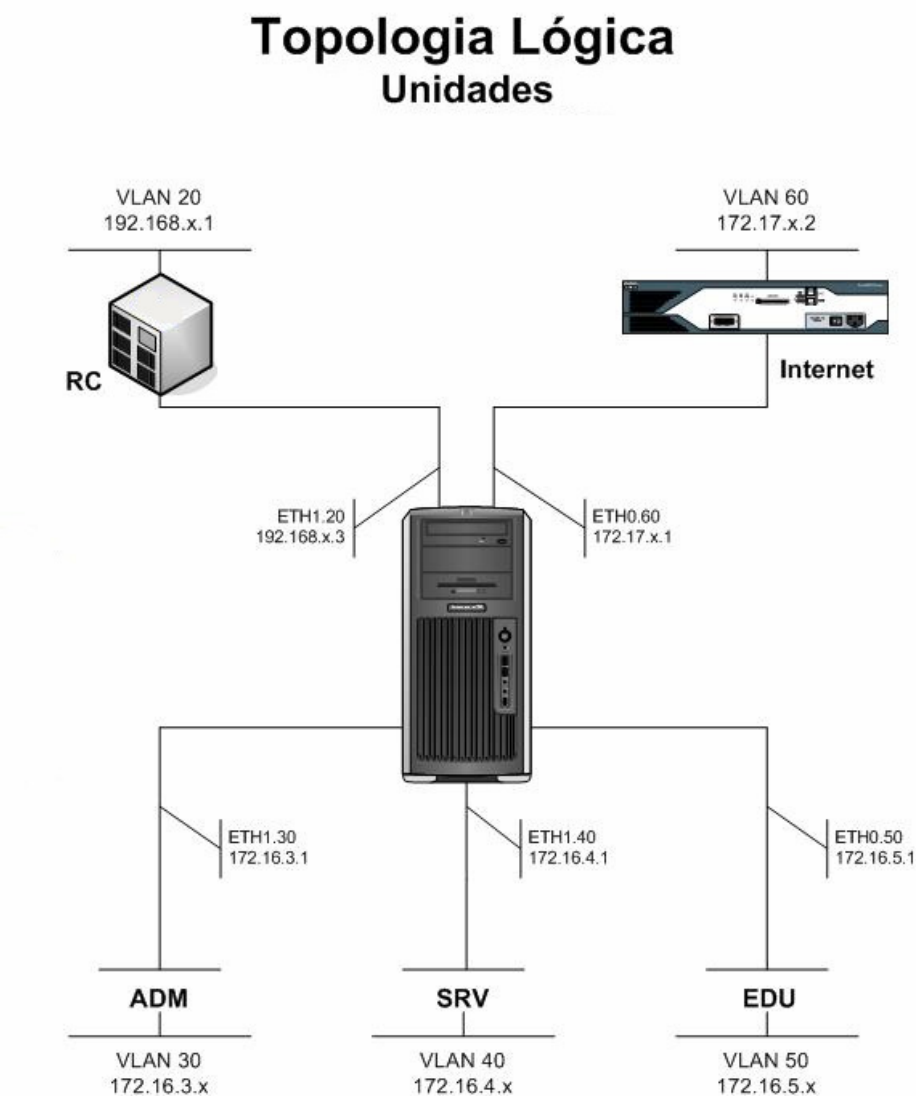

Figura 4 – Topologia lógica das unidades após a padronização

2 Gateway Multiuso

O Gateway Multiuso tem como principal função garantir a segurança da rede das filiais, sendo utilizados somente aplicativos e sistema operacional de código aberto. É uma solução de baixo custo porém de alto valor agregado, já que será considerado como o concentrador da rede, por onde toda comunicação entre redes diferentes deve passar.

O Gateway executará algumas funções na rede local, tais como: roteamento avançado (*policy based routing)*, filtro de pacotes (*firewall*), *proxy web*, gerenciamento de endereços IP (dhcpd), servidor *web* (httpd), gerenciamento de falhas e outros que serão detalhados no decorrer deste trabalho.

2.1 Roteamento avançado (*Policy Based Routing*)

O Gateway possui subinterfaces conectadas a todas as VLANs previamente definidas, agindo como o roteador destas redes. Com isso, todo o tráfego entre as diferentes VLANs deve, obrigatoriamente, utilizar o Gateway como roteador.

Para melhorar o desempenho e garantir a segurança dos dados corporativos foram criadas duas tabelas de roteamento, uma tendo como saída padrão a Rede Corporativa e outra tendo como saída padrão o roteador que se conecta com a *Internet*.

Como o Gateway é baseado no sistema operacional Linux, foram necessários incluir alguns pacotes de aplicativos para que o roteamento avançado pudesse ser configurado, um deles é o IPRoute2, que permite a criação de QoS, neste caso o PBR.

O IPRoute2 é uma coleção de utilitários para controlar configurações de rede TCP/IP e Controle de Tráfego no Linux (QoS).

Para que o roteamento avançado fosse realizado, foi utilizado em conjunto com o IPRoute2 o IPtables. O IPtables faz a identificação do tráfego e executa ações definidas pelo usuário, como marcação de pacotes e negação de tráfego. O *kernel* do Linux é inicializado com três listas de regras-padrão, que também são chamadas de *firewall chains* ou apenas *chains* (cadeias), que são: INPUT, OUTPUT e FORWARD. Cada cadeia possui seu próprio conjunto de regras de filtragem. Quando o pacote atinge uma das cadeias, é examinado pelas regras pertencentes a ela. Se a cadeira contiver uma regra que define que o pacote deve ser descartado, ele será descartado nesse ponto.

Cada uma dessas cadeias é constituída de um conjunto de regras que são examinadas uma a uma, sequencialmente. Se não houver regras em nenhuma cadeia, então a política padrão será utilizada, que no caso do Gateway é descartar o pacote. O Gateway utiliza a marcação de pacotes como regra para definir a qual tabela de roteamento pertence um determinado pacote, sendo esta marcação realizada através do IPtables.

Nesta etapa foram criadas duas tabelas de roteamento para que os pacotes sejam encaminhados aos seus destinos corretamente. Para tal, foram inseridas no arquivo /etc/iproute2/rt_tables as seguintes tabelas:

- Tabela 5: INET (*Internet*)
- Tabela 6: RC (Rede Corporativa)

A identificação e marcação dos pacotes ocorrem utilizando a tabela *mangle* do Netfilter (IPtables), tendo a seguinte regra básica:

- Tráfego destinado à Rede Corporativa deve ser encaminhado à tabela 6 (RC);
- Qualquer outra comunicação que não seja para as VLANs internas (ADM, EDU e SRV) deve ser encaminhada para a tabela 5 (INET).

Com essa estratégia, somente os dados corporativos utilizarão o enlace destinado a este fim. No caso de falha de algum dos enlaces, o Gateway será reconfigurado automaticamente para que nenhum acesso seja perdido.

A condição de *gateway* padrão das sub-redes ADM, EDU e SRV exige que o Gateway realize a tradução de endereços (NAT/PAT) para comunicações externas à rede local. Este tipo de tradução é realizado com o uso da ferramenta IPtables e sua funcionalidade de *masquerading*. *Masquerading,* ou PAT, é o processo de tradução do endereço de origem de um pacote pelo endereço da interface de saída, sendo o endereço da interface detectado automaticamente (EASTEP, 2006). São utilizadas as funções de *masquerading* nas interfaces que se conectam com a Rede Corporativa e com a *Internet*.

A figura 5 demonstra o funcionamento do roteamento no Gateway Multiuso:

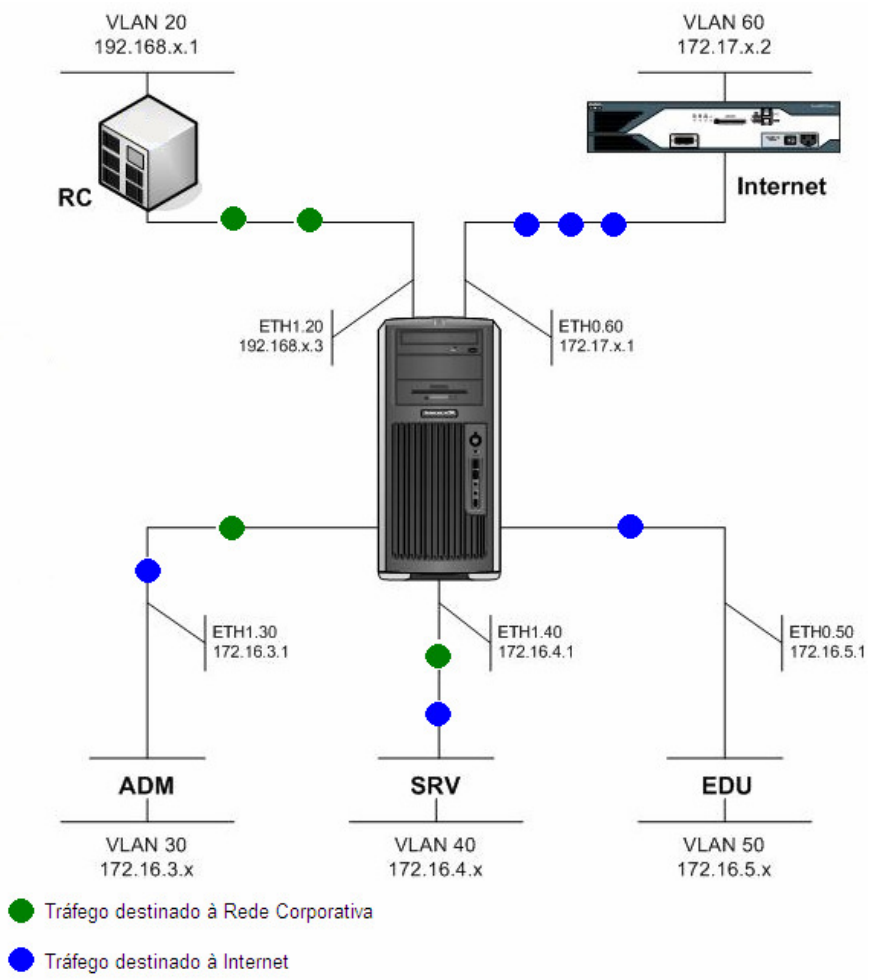

Figura 5 – Roteamento – Gateway Multiuso

2.2 DHCP

O DHCP (*Dynamic Host Configuration Protocol*) é utilizado para facilitar o gerenciamento dos endereços IP na rede local, facilitando o trabalho do administrador, evitando conflitos e configurações incorretas. O Gateway provê as seguintes informações para as máquinas das VLANs ADM e EDU: endereço IP, máscara de sub-rede, *gateway* padrão, servidor DNS, sufixo de DNS, tempo de concessão do endereço e tempo máximo de concessão.

As redes habilitadas neste serviço foram:

- 172.16.3.0/24 (ADM);
- 172.16.5.0/24 (EDU);

Algumas faixas de endereços foram excluídas da configuração automática para casos específicos, onde realmente são necessários IPs configurados estaticamente. São eles:

- 172.16.3.1 – 172.16.3.31/24 (ADM);
- 172.16.5.1 – 172.16.5.31/24 (EDU);

2.3 Proxy Web

O Squid é um *proxy-cache* para clientes *Web*, suportando protocolos *ftp*, *gopher* e *http*. Como *proxy*, atua como intermediário entre os clientes e servidores *Web*, dando maior segurança à rede interna. Como servidor *cache*, o Squid copia objetos solicitados recentemente para que uma próxima requisição destes objetos possa ser respondida por ele mesmo mais rapidamente, sem a necessidade de se conectar a um servidor externo, melhorando o desempenho da rede.

O Squid permite a filtragem de pacotes em nível de aplicativo para as requisições direcionadas a ele. O controle de acesso é feito através do uso de *Access Control Lists* (ACL), ou listas de controle de acesso. A solução proposta implementa o controle de acesso através de palavras na URL das requisições (utilizando expressões regulares), estas palavras são mantidas em um arquivo que pode ser atualizado pelos administradores através da interface de gerenciamento utilizada.

A sistemática de bloqueio de acesso aos *sites* na *Internet* pode ser resumida através do fluxograma da figura 6:

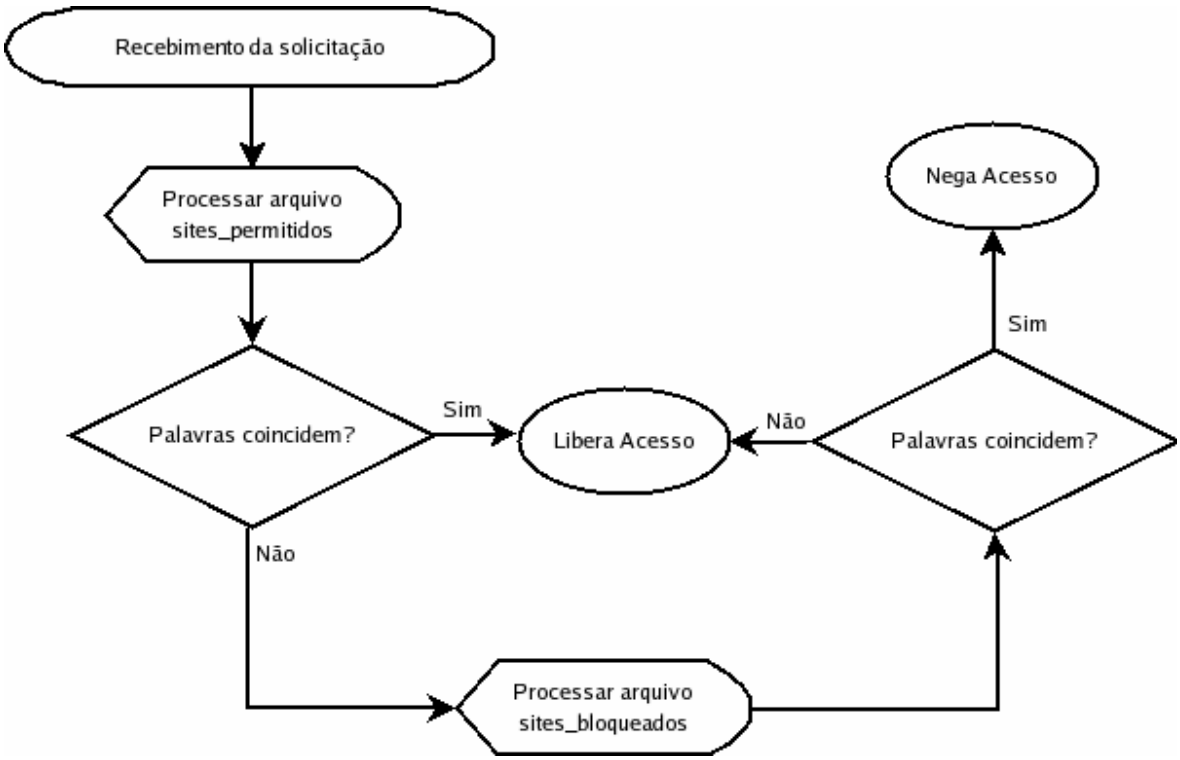

Figura 6 – Fluxograma de permissão de acesso do Squid

O *proxy* pode ser utilizado pelas redes ADM, SRV e EDU. Seu uso é obrigatório para as redes administrativa e educacional.

O acesso *web* a partir dos clientes da filial, independente de estar no ambiente administrativo ou educacional segue algumas premissas básicas definidas pelo Gateway. É necessário que os *browsers* (navegadores) estejam configurados com a opção “Detectar automaticamente as configurações de rede”, pois, como será visto adiante, é utilizado um conjunto de instruções para que os navegadores reconheçam o tipo de operação que deve ser adotado para que o cliente possa utilizar a *Internet* ou os *sites* da Rede Corporativa.

A navegação direta sem o uso do *proxy* do Gateway Multiuso não é permitida, garantindo assim que qualquer acesso poderá ser registrado e filtrado pelos administradores destas redes. Este tipo de bloqueio é feito através do *firewall*, obrigando que qualquer solicitação destinada às portas 80 e 443, que não têm como destino final o Gateway, sejam redirecionadas para o servidor *Web* deste equipamento, exibindo uma página que ilustra como o navegador deve estar configurado para atender os requisitos de navegação da rede, conforme figura 7:

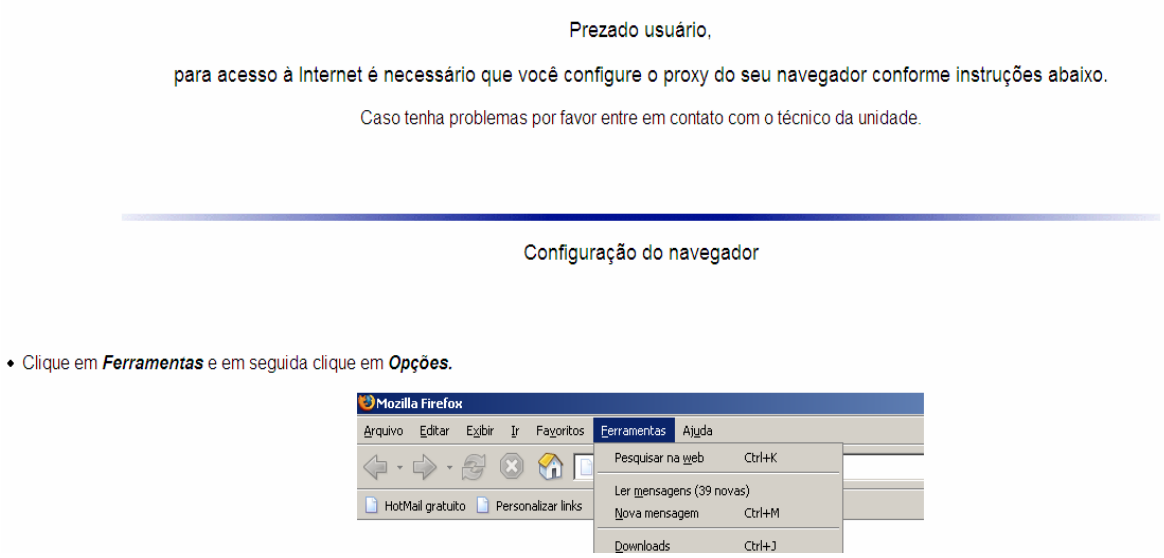

Figura 7 – Configurando o navegador

Esta abordagem difere do conceito de *Proxy* Transparente, que é largamente utilizada no mercado. A opção de *Proxy* Transparente utiliza o *firewall* para redirecionar os pacotes para o *proxy*, sem que o cliente ou o navegador estejam cientes.

Os principais motivos pelo não uso da operação por *Proxy* Transparente foi o fato de não ser possível utilizar o *proxy* para conteúdos criptografados (HTTPS), impedindo assim o registro e o filtro das páginas e arquivos que podem ser acessados na *Internet* e também não permitir autenticação de usuário.

2.4 WPAD

Web Proxy Auto-Discovery, ou, Detecção Automática de *Web Proxy*, foi a solução encontrada para que os navegadores dos clientes sejam configurados de forma automática. Isto visa desonerar os administradores de um trabalho repetitivo e muitas vezes causando má impressão para o cliente da instituição que quer utilizar os recursos que a empresa oferece.

Por padrão, os navegadores habilitados a utilizar a detecção automática executam a seguinte rotina:

- Procuram um servidor *web* contendo o seguinte nome: wpad.*sufixo_de_dns*;
- Se existir um servidor com este nome, o navegador solicitará o arquivo wpad.dat;
- Se obtiver êxito, o navegador processará este arquivo, e, se contiver informações válidas, irá utilizar os dados providos para configurar o *proxy* deste cliente.

O arquivo wpad.dat contém as configurações que serão utilizadas pelo navegador, tais como: Endereço do *proxy*, porta e endereços que não devem utilizar o *proxy*. Ficou definido o seguinte conteúdo para este arquivo:

```
function FindProxyForURL(url,host)
{
  if (isInNet(host, "127.0.0.0", "255.0.0.0")) {
              return "DIRECT";
  } else if (isInNet(host, "172.16.0.0", "255.255.0.0")) {
             return "DIRECT";
```

```
  } else  {
            return "PROXY 172.16.5.1:3128";
  }
}
```

Com isso é possível afirmar que as solicitações para a máquina local (rede 127.0.0.0/8) e para a rede 172.16.0.0/16 não utilizarão o *proxy*, tendo acesso direto aos recursos destas redes. O acesso a outras redes utilizará obrigatoriamente o *proxy* (endereço 172.16.5.1, porta 3128).

O processo de configuração automática é rápido e simples do ponto de vista do cliente, que não necessita digitar endereço IP e porta do *proxy* para utilizar a *Internet*.

2.4.1 HTTPD

Este serviço é utilizado para que os clientes das redes administrativa e educacional não realizem a configuração manual de seus navegadores *Web*, desonerando o administrador da rede local de eventuais problemas causados por usuários com dúvidas em relação à configuração de sua máquina.

O serviço disponibiliza aos usuários os seguintes arquivos:

- Página *Web* contendo um tutorial para que os clientes habilitem no navegador a opção “Auto detectar configurações de *proxy*”;
- Arquivo contendo um *JavaScript* que será utilizado pelo navegador para tomar conhecimento do *proxy* a ser utilizado (wpad.dat);

A sistemática desta solução funciona da seguinte maneira:

- Ao tentar conectar a uma página *Web*, sem utilizar o *proxy*, o cliente fará uma solicitação utilizando a porta de destino 80, do protocolo TCP;
- Esta solicitação será interceptada pelo Gateway, que irá repassar os dados ao servidor *Web* local (Apache);
- A solicitação HTTP será reescrita para que uma página contendo o tutorial de configuração seja exibida. Para este passo, foi utilizado o módulo *mod_rewrite* do Apache, que resultou nas seguintes linhas do arquivo httpd.conf:
    - RewriteEngine On
    - RewriteCond %{HTTP_HOST} !^wpad
    - RewriteCond %{HTTP_HOST} !^172.16.5.1
    - RewriteRule ^/(.*) http://wpad.organizacao.br/index.html

Qualquer solicitação HTTP que utilize a porta 80 e não seja destinada ao Gateway, será reescrita como http://wpad.organizacao.br/index.html. Isso garante que nenhum acesso direto à *Internet* será realizado, possibilitando realizar o bloqueio baseado nas políticas de segurança da instituição.

2.5 WEBMIN

O Webmin é uma interface *web* para administração de sistemas Unix. É composto por vários módulos, cada um com sua função específica. A administração a partir de um ambiente gráfico e centralizado permite uma maior

agilidade para um administrador que não possui conhecimento técnico elevado ao ponto de conhecer todos os serviços e configurações deste equipamento.

A interface de gerenciamento proporciona uma solução fácil via *web* para virtualmente realizar qualquer tarefa de administração Linux do dia-a-dia, protegendo o administrador de erros de sintaxe e outras falhas que são feitas editando arquivos de configuração diretamente, e alerta o administrador antes de tomar ações potencialmente perigosas (CAMERON, 2003).

Foram criados usuários especiais para que módulos de administração do sistema não sejam acessados por pessoas indevidas, ocorrendo assim, falhas de segurança e de integridade de arquivos do equipamento.

Por ser acessado através da *Web*, o Webmin pode ser utilizado pelo administrador a partir de qualquer computador de sua rede, desde que o computador possua permissão para tal. Isto também permite que eventuais suportes possam ser realizados remotamente à unidade pelos funcionários da sede da instituição, que têm gerência total sobre o equipamento.

A figura 8, ilustrando a configuração de um servidor DHCP de uma unidade, pode ser visualizada abaixo:

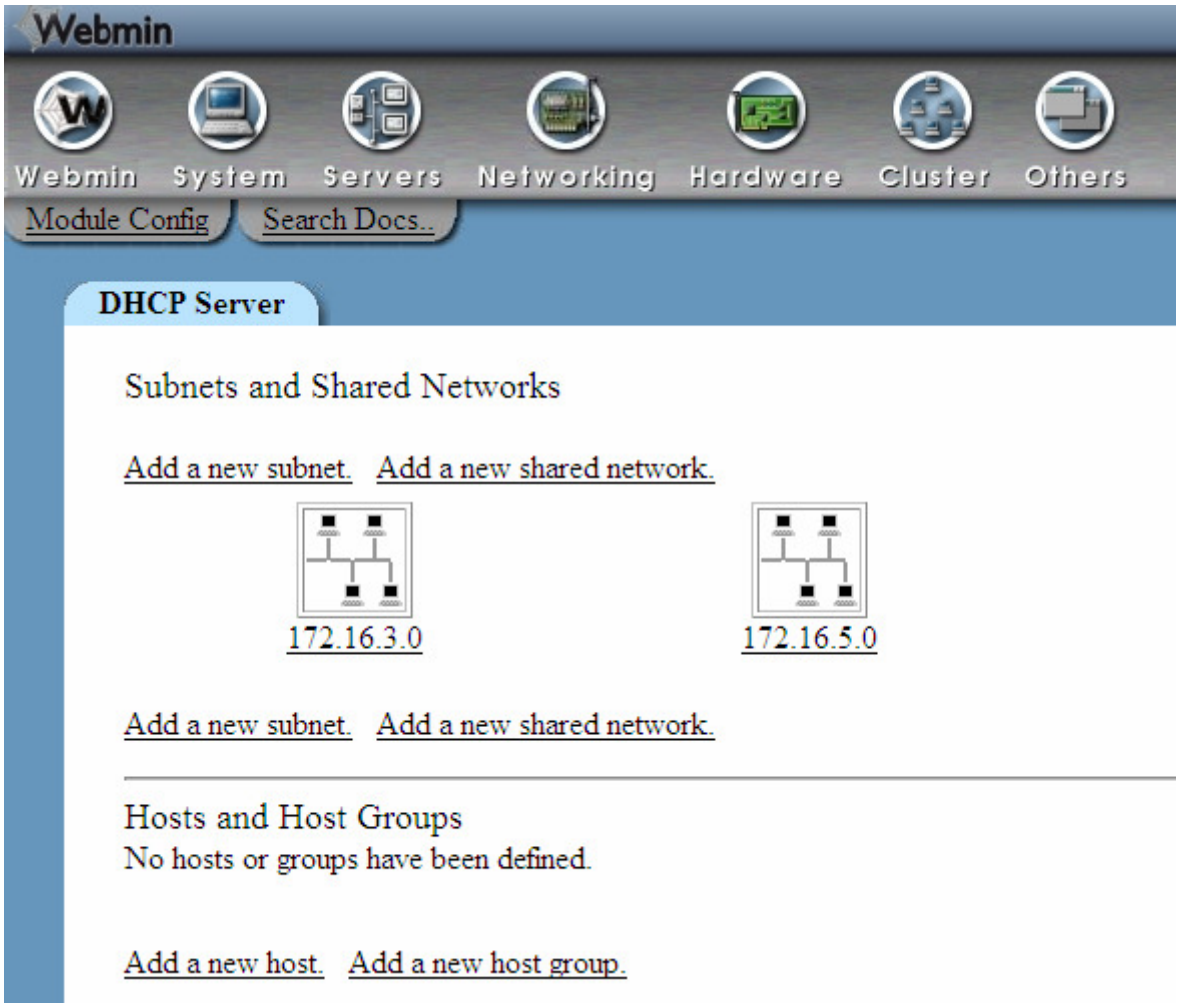

Figura 8 – Módulo de configuração do servidor DHCP

2.6 HIDS

Para realizar as funções de HIDS no Gateway Multiuso, optou-se a solução de código aberto chamado OSSEC HIDS. O aplicativo provê as seguintes funções:

- Análise de *logs*;
- Verificação de integridade dos arquivos;

- Detecção de *rootkits*;
- Alertas por email;
- Respostas pró-ativas, baseadas nos incidentes.

Caso o administrador tenha somente uma máquina a ser monitorada, o OSSEC pode ser instalado localmente neste equipamento. No entanto, se estão sendo administrados vários equipamentos, é possível eleger um como sendo o servidor, e os outros como sendo os agentes. Todos os eventos gerados pelos agentes são enviados ao servidor, que faz as análises necessárias. Um dos grandes benefícios do OSSEC HIDS é a escalabilidade, possibilitando ao administrador monitorar vários servidores a partir um ponto central.

Considerando a parte de análise de *logs*, o OSSEC é capaz de analisar os registros provenientes dos serviços listados abaixo, entre outros:

- Syslog;
- Apache;
- Squid;
- Snort-Full / Snort-Fast
- Windows EventLog / IIS Log

No caso do Gateway Multiuso são feitas as análises de *logs* dos serviços Syslog, Apache e Squid. Alguns casos de análise destes registros são detalhados a seguir:

1. Usuários internos com vírus

Alguns tipos de vírus são programados para acessarem páginas na *Internet*, colhendo ou enviando informações de/para seus desenvolvedores. Um exemplo é o vírus W32.Beagle, que tenta acessar páginas com extensões xxx3.php ou blst.php. O evento gerado após a identificação destes acessos seria exibida como:

```
OSSEC HIDS Notification.
2006 May 11 11:00:00
Received From: /var/log/squid/access.log
Rule: 5054 fired (level 12) -> "Infected machine with
W32.Beagle.DP.'"

Portion of the log(s):
524          192.168.2.204          TCP_MISS/404          590          GET
http://www.ordendeslichts.de/intern/xxx3.php? - DIRECT/81.201.107.6
3571          192.168.2.204          TCP_MISS/404          470          GET
http://www.levada.ru/htmlarea/images/xxx3.php? - DIRECT/62.118.252.213
```

2. Ataques com sucesso e falhos em aplicações web

Através da análise de *logs* é possível identificar alguns tipos de ataques destinados às aplicações *web* vulneráveis. Um exemplo é a aplicação NeoBoard, que continha um script chamado PJReview_neo.cgi que era vulnerável. Utilizando o OSSEC foi possível identificar estes ataques:

```
OSSEC HIDS Notification.
2006 Aug 24 21:33:31
Received From: /var/log/httpd/access_log
```

```
   Rule: 3153 fired (level 10) -> "Multiple common web attacks from
same souce ip.'"

Portion of the log(s):
172.16.5.72 - - [24/Aug/2006:21:33:30 -0300] "GET
/PJreview_Neo.cgi?p=../../../../../../../../../../etc/passwd HTTP/1.1"
302 375 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"
172.16.5.72 - - [24/Aug/2006:21:33:30 -0300] "GET
/cgi-bin/PJreview_Neo.cgi?p=../../../../../../../../../../etc/passwd
```

A verificação da integridade dos arquivos é feita utilizando MD5 ou SHA1. Periodicamente são gerados *hashes* dos arquivos de sistema, e comparados com o valor armazenado anteriormente. Caso os valores difiram, é gerado um evento, que pode ser armazenado nos registros do HIDS ou enviado por e-mail.

O OSSEC pode enviar *e-mail* aos administradores assim que ocorre um evento, possibilitando ações pró-ativas até mesmo na eventual falha de *hardware* em virtude da análise de *logs.*

2.7 DNS

Domain Name System (DNS) é um sistema distribuído de banco de dados que traduz nomes de domínio em endereços IP e endereços IP em nomes de domínio. A distribuição do sistema permite o controle local dos segmentos do banco de dados geral, mantendo os dados disponíveis por toda a rede através de um esquema cliente-servidor (ALBITZ, 2001).

Os servidores de nomes contêm informações sobre alguns segmentos do banco de dados e as disponibiliza para os clientes. As informações que o servidor de nomes local não possuir podem ser buscadas por ele contatando outros servidores de nomes.

O Gateway Multiuso também faz a função de servidor de nomes para as redes internas, ou seja, rede administrativa, servidores e educacional. É utilizada a implementação de DNS mantida pelo *Internet Software Consortium*, o BIND versão 9. Porém, não são configuradas zonas neste servidor. Sua atuação é definida em dois itens:

- *Cache-only*:
    - Utilizado para guardar em *cache* as solicitações de DNS;
- *Forwarder*:
    - Repassa as solicitações para os servidores do ponto central da topologia.

Com isso é possível obter um ganho de performance nas solicitações de DNS realizadas pelos clientes das redes internas. As solicitações são enviadas ao Gateway, que verifica se a informação está armazenada em memória, armazenamento este feito pela função de *cache*. Caso a informação não esteja disponível, uma solicitação nova é gerada para o servidor de nomes do ponto central da topologia, que está localizado na sede da empresa. Após receber a resposta, a mesma é armazenada localmente e enviada ao cliente solicitante.

2.8 SHOREWALL

O Shoreline Firewall, chamado de Shorewall, é uma aplicação de alto nível utilizada para administrar o IPtables de forma mais fácil e ágil. Utiliza vários arquivos de configuração para que as regras de permissão e bloqueio do Netfilter sejam criadas.

O Shorewall também utiliza o conceito de zonas, que no Gateway tem a mesma denominação das VLANs utilizadas, já que são as redes diretamente conectadas, ou seja, o Shorewall possui as seguintes zonas:

- RC (Conexão com a Rede Corporativa)
- ADM (Ambiente de administração)
- SRV (Ambiente dos servidores)
- EDU (Ambiente educacional)
- INET (Conexão com a *Internet*)
- Firewall (Zona que caracteriza o próprio equipamento)

As regras do Shorewall determinam a ação a ser tomada com determinadas conexões, e são definidas no arquivo *rules*. Estas conexões são identificadas por um sentido, com zona de origem e zona de destino, além de identificadores específicos como portas, protocolo, endereços. Caso nenhuma regra se aplicar a uma conexão específica, a política padrão, definida no arquivo *policy*, para aquele sentido de conexão, é utilizada.

O Gateway utiliza o Shorewall para facilitar o gerenciamento de configuração do *firewall*. Para auxiliar o gerenciamento do Shorewall é utilizada a interface de configuração Webmin.

2.8.1 Regras de Firewall

Firewalls de rede são dispositivos ou sistemas que controlam o fluxo de tráfego de rede entre redes que implementam posturas de segurança diferentes. Implementando um *firewall* para controlar a conectividade a estas redes, uma organização pode prevenir o acesso não-autorizado a sistemas e recursos (WACK, 2002).

Por prover uma camada adicional de segurança, a utilização de um *firewall* na estrutura proposta pelo Gateway se torna necessária.

O sistema operacional utilizado pelo Gateway implementa o NetFilter Firewall. O IPtables, utilizado em conjunto com o NetFilter, permite ao usuário definir as regras que governam a filtragem dos pacotes (ACCARDI, 2005). O Gateway ainda implementa o Shorewall, que visa facilitar o gerenciamento da configuração do IPtables.

Um modelo de regras de *firewall* foi desenvolvido como configuração mínima de regras para o Gateway. Este modelo considera todos os serviços implementados pelo Gateway e os aplicativos utilizados pela rede corporativa.

Este modelo considera que tudo aquilo que não é explicitamente permitido deve ser proibido. São permitidas apenas conexões entrantes a servidores específicos, limitando-as ao mínimo de serviços/portas necessárias, e também não são permitidos acessos externos às redes locais.

As tabelas a seguir foram divididas por interface de entrada, de onde se originam as conexões. As regras destinadas para a rede corporativa (interface eth1.20) são duplicadas para a interface eth0.60, que se conecta à *Internet*, pois,

em caso de contingência, o tráfego será roteado pela VPN, que é estabelecida através da *Internet*.

INTERFACE DE ORIGEM: ETH1.30 (Rede administrativa)						
Rede/IP de Origem	**Rede/IP de Destino**	**Interface de destino**	**Protocolo**	**Porta de Origem**	**Porta de Destino**	**Ação**
Qualquer	Qualquer	Firewall	UDP	Qualquer	53	Permitir
Qualquer	Qualquer	Firewall	TCP	Qualquer	22,80,3128,10000	Permitir
Qualquer	Servidor de Arquivos	Eth1.40	UDP	Qualquer	137,138,139	Permitir
Qualquer	Servidor de Antivírus	Eth1.40	TCP	Qualquer	8080	Permitir
Qualquer	Servidor de aplicação	Eth1.20	TCP	Qualquer	3389	Permitir
Qualquer	Servidor de aplicação	Eth0.60	TCP	Qualquer	3389	Permitir
Qualquer	Servidor de e-mail	Eth1.20	TCP	Qualquer	25, 110	Permitir
Qualquer	Qualquer	Eth0.60	TCP	Qualquer	25, 110	Permitir

Tabela 1 – Regras de Firewall – VLAN ADM

INTERFACE DE ORIGEM: ETH0.50 (Rede educacional)						
Rede/IP de Origem	**Rede/IP de Destino**	**Interface de destino**	**Protocolo**	**Porta de Origem**	**Porta de Destino**	**Ação**
Qualquer	Qualquer	Firewall	UDP	Qualquer	53	Permitir
Qualquer	Qualquer	Firewall	TCP	Qualquer	80,3128	Permitir
Qualquer	Servidor de Antivírus	Eth1.40	TCP	Qualquer	8080	Permitir

Tabela 2 – Regras de Firewall – VLAN EDU

INTERFACE DE ORIGEM: ETH1.40 (Rede dos servidores)						
Rede/IP de Origem	**Rede/IP de Destino**	**Interface de destino**	**Protocolo**	**Porta de Origem**	**Porta de Destino**	**Ação**
Qualquer	Qualquer	Firewall	UDP	Qualquer	53	Permitir
Qualquer	Qualquer	Firewall	TCP	Qualquer	80,3128	Permitir
Qualquer	Servidor de Antivírus	Eth1.40	TCP	Qualquer	8080	Permitir

Tabela 3 – Regras de Firewall – VLAN SRV

INTERFACE DE ORIGEM: Firewall						
Rede/IP de Origem	**Rede/IP de Destino**	**Interface de destino**	**Protocolo**	**Porta de Origem**	**Porta de Destino**	**Ação**
Qualquer	Qualquer	Eth1.20	TCP	Qualquer	21,25,80,443	Permitir
Qualquer	Qualquer	Eth0.60	TCP	Qualquer	21,25,80,443	Permitir
Qualquer	Qualquer	Eth0.60	UDP	Qualquer	53	Permitir
Qualquer	Qualquer	Eth1.20	UDP	Qualquer	53	Permitir

Tabela 4 – Regras de Firewall – Gateway

2.9 GERENCIAMENTO DE FALHAS

Uma falha é uma condição anormal cuja recuperação exige ação de gerenciamento. O impacto e a duração do estado de falha podem ser minimizados pelo uso de componentes redundantes e rotas de comunicação alternativas, reduzindo ao mínimo o dano ao usuário final.

Um componente crítico das redes das unidades é o enlace corporativo, pois toda comunicação administrativa da organização utiliza este caminho. No caso de falha deste enlace de comunicação, as operações normais das unidades ficam comprometidas, resultando em perda de tempo, e muitas vezes de dinheiro. Por esta razão, este trabalho define um meio de realizar automaticamente o gerenciamento de falha do enlace corporativo e um plano de contingência caso uma falha venha a ocorrer.

O gerenciamento de falhas é realizado através de um *Shell Script*. No caso mais simples, um *script* nada mais é que uma lista de comandos de sistemas armazenados em um arquivo. Um *shell* é um interpretador de comandos em sistemas UNIX e derivados. O *shell script* definido para o Gateway utiliza o Bash, um acrônimo para Bourne-Again Shell, que se tornou o padrão de *facto* para *shell scripting* em todas as derivações do UNIX (COOPER, 2005).

O *script* de gerenciamento de falhas dos enlaces de comunicação é executado a cada 2 minutos, através do processo *cron* do sistema Linux.

O funcionamento básico deste *script* consiste em realizar um *ping* de três pacotes para o salto seguinte da rede corporativa, armazenando o resultado deste comando em um arquivo temporário. Deste arquivo são retiradas as informações necessárias para verificar se o enlace está ativo ou inativo. Caso não tenha

recebido resposta do outro equipamento o processo é realizado novamente, visando garantir que não foi uma queda e retorno rápido. O mesmo processo ocorre com o enlace que conecta a unidade à *Internet*.

2.9.1 Plano de contingência

Sistemas de Tecnologia da Informação são vulneráveis a uma variedade de perturbações, variando de faltas de energia a destruição de um equipamento. Muitas vulnerabilidades podem ser minimizadas ou eliminadas através de soluções técnicas, administrativas ou operacionais como parte do esforço do gerenciamento de riscos de uma organização. O planejamento de contingência é designado para atenuar o risco de indisponibilidade de um serviço ou sistema focalizando soluções de recuperação eficientes e efetivas (SWANSON, 2002).

O plano de contingência definido para uma eventual falha do enlace corporativo de uma unidade consiste na utilização de VPN e roteamento adaptativo. Este plano é executado automaticamente assim que for detectada uma falha no enlace corporativo, através do *script* de gerenciamento de falhas.

Para que o plano de contingência seja efetivado é necessário estabelecer uma VPN do roteador que está ligado à *Internet* com o ponto central da topologia, no *firewall* externo que também realiza a função de concentrador de VPN. Este processo garante um enlace de comunicação seguro entre a unidade e o ponto central, pois utiliza IPSec para realizar a criptografia dos dados. Após este passo é preciso alterar a estrutura de roteamento do Gateway, indicando que o enlace corporativo não está mais disponível. O tráfego que antes utilizava o enlace

corporativo agora pode utilizar a VPN estabelecida para trafegar os dados, mantendo saída normal do tráfego destinado à *Internet*.

A queda do enlace que conecta a unidade à *Internet* resulta em um processo diferente do exposto acima. Neste caso, os aplicativos corporativos não sofrerão perdas, já que a comunicação com o ponto central, através do enlace corporativo, não foi afetado. No entanto, o tráfego destinado à *Internet* não alcançará o seu destino, resultando em perdas. Para que isso não ocorra, o plano de contingência foi definido para que o tráfego *Web* (portas TCP 80 e 443) utilize o enlace corporativo, e tenha saída à *Internet* no ponto central da instituição. Este caso também requer a reestruturação do roteamento do Gateway Multiuso.

Nos dois casos a disponibilidade das aplicações é assegurada, garantindo que não ocorram períodos de inatividade da unidade pela queda de algum enlace de comunicação.

A cada processo de contingência que é executado, um e-mail é enviado aos administradores de rede, para que possam tomar as devidas providências quanto à manutenção do enlace.

2.10 REGISTROS DE ATIVIDADES

Para que sejam comprovadas modificações feitas nos equipamentos e para validar configurações de *firewall*, por exemplo, foi instituído que qualquer equipamento de rede deveria registrar estas informações no Gateway Multiuso. Esta prática pode auxiliar na resolução de problemas de configuração e na identificação de ações incorretas realizadas por algum administrador de rede.

Registros incomuns de bloqueio de *firewall* podem demonstrar a atividade de um vírus na rede, ou, um usuário tentando realizar atividades não permitidas pela política de segurança da instituição.

Como este trabalho se concentra nas atividades do Gateway Multiuso, do *switch* utilizado na unidade e no roteador, serão demonstrados abaixo alguns exemplos de registros que cada um deles deve gerar.

2.10.1 Serviços de rede

Além das configurações padrões que o Linux traz com a instalação, como o registro para os arquivos */var/log/messages, /var/log/dmesg* e */var/log/secure*, alguns dados adicionais estão sendo registrados para visualização futura ou em tempo real.

2.10.1.1 HTTPD

A função do Apache no Gateway Multiuso é prover uma página contendo as configurações necessárias para que o *script* de configuração dos navegadores seja executado corretamente, além de servir o próprio *script*. Qualquer outra solicitação a este serviço estará realizando alguma atividade que não está de acordo com o processo normal de funcionamento da rede. Baseado nisto, são registradas as atividades normais de acesso ao serviço, assim como as atividades que resultaram em erros. Estes arquivos ficam armazenados em */var/log/httpd/access_log* e */var/log/httpd/error_log* respectivamente.

Alguns exemplos de utilização correta deste serviço podem ser vistas abaixo, onde é requisitado o arquivo de configuração dos navegadores:

```
172.16.3.130 - - [19/Dec/2006:18:43:11 -0200] "GET /wpad.dat HTTP/1.1"
304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Win32)"
172.16.3.114 - - [19/Dec/2006:18:47:53 -0200] "GET /wpad.dat HTTP/1.1"
200 180 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; pt-BR; rv:1.8.0.8)
Gecko/20061025 Firefox/1.5.0.8"
172.16.3.132 - - [19/Dec/2006:18:51:04 -0200] "GET /wpad.dat HTTP/1.1"
200 180 "-" "NSPlayer/4.7.0.3001"
```

Nestes casos é possível identificar o endereço IP do computador que solicita o arquivo de configuração e o navegador utilizado.

Para casos em que existe não conformidade no uso da rede, os registros podem aparecer como:

```
[Mon Dec 18 14:24:01 2006] [error] [client 172.16.3.152] File does not
exist: /var/www/html/avg7info.ctf
[Mon Dec 18 15:48:07 2006] [error] [client 172.16.3.54] Invalid URI in
request J\xc2w\x11a\x07\x07\xa3\xc6;\x97\xb8Q 4
```

No primeiro registro é possível identificar que o cliente de antivírus utilizado na máquina com IP 172.16.3.152 está tentando buscar um arquivo na *Internet*, porém, sem utilizar o *proxy*. Esta operação resulta em falha, já que a utilização do *proxy* é obrigatória para todos os aplicativos que desejam se conectar à *Internet*.

O segundo registro indica uma atividade inválida do cliente com IP 172.16.3.54, atividade esta que deve ser verificada com cautela pelo administrador da rede da unidade, já que pode ser uma incidência de vírus ou algum programa que esteja gerando tráfego incomum na rede.

2.10.1.2 Proxy

O registro de atividades gerado pelo *proxy* é útil para identificar usuários que não estão respeitando a política de uso aceitável da instituição. Com estes registros é possível identificar as páginas da *Internet* que estão sendo visualizadas pelos colaboradores e alunos, podendo-as bloquear utilizando o procedimento já descrito ou tomar providências administrativas em relação aos usuários.

Exemplos destes registros podem ser visualizados abaixo:

```
1166444919.821             208   172.16.5.6   TCP_MISS/200   5927   GET
http://www.uol.com.br/ - DIRECT/200.221.2.45 text/html
1166453112.697              11   172.16.5.5   TCP_DENIED/403   1352   GET
http://www.orkut.com/ - NONE/- text/html
1166453118.782              3   172.16.5.5   TCP_DENIED/403   1344   CONNECT
www.orkut.com:443 - NONE/- text/html
```

O primeiro registro listado acima indica um uso legítimo do usuário que está utilizando o computador com IP 172.16.5.6, visitando a página do Universo Online, já que esta página não está bloqueada pelo administrador de rede da unidade.

Nos dois casos seguintes é possível perceber que a ação realizada foi negada pelo *proxy* do Gateway Multiuso. A primeira ação negada indica uma tentativa de conexão à porta 80 do protocolo TCP destinada ao Orkut, um site de relacionamentos que está disponível na *Internet*. A segunda ação negada indica também uma tentativa de acesso ao Orkut, porém utilizando o protocolo HTTPS, com conexão criptografada, tentando burlar as regras de segurança da instituição.

Esta ação também não obteve sucesso, já que tanto o protocolo HTTP quanto o protocolo HTTPS são verificados pela configuração atual do *proxy*.

2.10.1.3 Shorewall

São registradas todas as tentativas de conexão bloqueadas pelo *firewall* do Gateway Multiuso, possibilitando aos administradores de rede resolver problemas de conexão de equipamentos ou identificar atividades anormais acontecendo na rede, como a presença de um vírus ou tentativas de ataque.

A utilização destes registros pode servir para a resolução de problemas, já que novas conexões podem ser identificadas pelos registros do *firewall,* possibilitando a identificação dos protocolos e portas utilizadas pelo aplicativo que está com problemas de conexão.

Exemplos de registros de bloqueio de conexões pelo *firewall* podem ser visualizados a seguir:

```
Dec 19 19:30:16 hostname kernel: Shorewall:EDU2INET:DROP:IN=eth0.50
OUT=eth0.60 SRC=172.16.5.180 DST=68.1.27.120 LEN=48 TOS=0x00 PREC=0x00
TTL=127 ID=4527 DF PROTO=TCP SPT=1875 DPT=52030 WINDOW=65535 RES=0x00 SYN
URGP=0
Dec 19 19:30:17 hostname kernel: Shorewall:EDU2INET:DROP:IN=eth0.50
OUT=eth0.60 SRC=172.16.5.180 DST=70.28.58.171 LEN=48 TOS=0x00 PREC=0x00
TTL=127 ID=4530 DF PROTO=TCP SPT=1876 DPT=23818 WINDOW=65535 RES=0x00 SYN
URGP=0
```

Do primeiro registro é possível visualizar alguns campos importantes para a identificação do tráfego de rede que foi bloqueado:

- Shorewall:EDU2INET:DROP (Zonas envolvidas – Origem para Destino, e ação tomada DROP, que é o descarte);
- IN=eth0.50 (Interface de entrada);
- OUT=eth0.60 (Interface de saída);
- SRC=172.16.5.180 (IP de origem);
- DST=68.1.27.120 (IP de destino);
- PROTO=TCP (Protocolo);
- SPT=1875 (Porta de origem);
- DPT=52030 (Porta de destino);

No caso de um uso legítimo dos recursos de rede, o administrador pode criar uma regra permitindo o estabelecimento desta conexão. Caso não seja permitido, é necessário realizar uma verificação para identificar qual o aplicativo que está tentando utilizar o serviço.

2.10.1.4 Roteador

Registros de alterações de configuração e quedas nos enlaces de comunicação são enviados para o Gateway Multiuso, possibilitando a visualização destas informações pela interface de gerenciamento Webmin, sem a necessidade de se conectar a este equipamento diretamente. Alguns exemplos de registros deste equipamento são:

```
Jul 27 19:06:21 172.17.2.2 22602: Jul 27 19:06:20.149 GMT-3: %SSH-5-
SSH2_SESSION: SSH2 Session request from 172.17.2.1 (tty = 0) using crypto
cipher 'aes128-cbc', hmac 'hmac-md5' Succeeded
```

```
Jul 27 19:06:25 172.17.2.2 22603: Jul 27 19:06:24.181 GMT-3: %SSH-5-
SSH2_USERAUTH: User 'admin' authentication for SSH2 Session from
172.17.2.1 (tty = 0) using crypto cipher 'aes128-cbc', hmac 'hmac-md5'
Succeeded
Jul 27 19:32:24 172.17.2.2 22604: Jul 27 19:32:23.586 GMT-3: %SSH-5-
SSH2_CLOSE: SSH2 Session from 172.17.2.1 (tty = 0) for user 'admin' using
crypto cipher 'aes128-cbc', hmac 'hmac-md5' closed
Dec  6 13:31:30 172.17.2.2 28: *Dec  6 13:31:22.332 GMT-2: %LINEPROTO-5-
UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
Dec  6 13:31:37 172.17.2.2 28: *Dec  6 13:31:22.332 GMT-2: %LINEPROTO-5-
UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

Os três primeiros registros indicam uma conexão ao roteador utilizando o protocolo SSH, sendo realizada pelo usuário *admin*, que encerra esta conexão sem realizar nenhum tipo de configuração do equipamento.

Os dois últimos registros caracterizam uma queda de comunicação do enlace que está conectado à interface serial deste equipamento. É possível notar que esta queda dura somente sete segundos, não iniciando o plano de contingência configurado pelo Gateway Multiuso.

2.10.1.5 Switch

Este equipamento também registra suas atividades no Gateway Multiuso, não necessitando de conexão direta do administrador a este equipamento, já que é possível visualizar suas atividades pela interface de gerenciamento.

São registradas informações como conexões de usuários ao equipamento, alterações de configuração e alteração do estado das portas, como registrado

abaixo, onde a interface FastEthernet0/3 perde comunicação com o equipamento da outra ponta, porém, restabelece rapidamente:

```
Dec 17 11:12:55 172.17.2.4 15965: Dec 17 13:12:54.118 UTC: %ENLACE-3-
UPDOWN: Interface FastEthernet0/3, changed state to down
Dec 17 11:12:57 172.17.2.4 15966: Dec 17 13:12:56.310 UTC: %ENLACE-3-
UPDOWN: Interface FastEthernet0/3, changed state to up
```

V Políticas de segurança

A cada ano novos incidentes de segurança são reportados na mídia. Consequentemente, os responsáveis por proteger os recursos críticos da organização vêem a necessidade de atentar com mais rigidez aos incidentes de segurança enfrentados pelo negócio da instituição, que é fortemente baseado em suas informações.

Instituições de ensino têm particularidades em relação a uma empresa comum, principalmente relacionada às pessoas que freqüentam tal instituição. Além do colaborador, temos a figura do aluno, que pode estar assistindo às aulas em determinados momentos, e em outros estar utilizando os recursos disponibilizados pela instituição para realizar seus trabalhos escolares.

Uma política de segurança voltada para instituições de ensino deve ser criada de forma a estabelecer regras a serem seguidas por todos os usuários dos recursos de informática, de maneira que todos sejam envolvidos e conscientizados da importância da segurança das informações na organização.

Para criação do modelo de política de segurança apresentado neste estudo foram utilizadas algumas informações como:

- A norma NBR ISO 17799 como referência, sendo que esta norma é o código de prática para a gestão da segurança da informação;
- Modelo de política de segurança, Cisco Systems;
- Informações sobre instituições de ensino.

1. Objetivos da política de segurança

O principal objetivo da política de segurança é garantir que os recursos e as informações estarão sendo utilizados da maneira correta. Cada usuário deve ter ciência da utilização e manipulação dos dados da empresa, evitando colocar em risco qualquer tipo de informação que possa ser prejudicial para a instituição no futuro.

Os documentos que descrevem as políticas de segurança da organização devem ser claros o suficiente para que o leitor possa saber se a informação lida é aplicável a ele ou não. Sendo assim, as informações disponibilizadas nestes documentos devem conter uma linguagem clara e de fácil entendimento, permitindo que qualquer usuário entenda e compreenda os objetivos descritos.

Na elaboração de uma política de segurança devem ser levados aspectos como a implementação de controles para preservar os interesses dos colaboradores, parceiros, clientes e da instituição contra danos que alguma falha de segurança possa vir a causar. Descrições de normas de utilização e atividades que possam ser consideradas como violações de uso dos recursos disponibilizados devem ser explícitas nestes documentos. Caso os procedimentos ou normas estabelecidos sejam violados os usuários poderão sofrer punições que serão esclarecidas e detalhadas posteriormente.

2. Políticas

2.1 POLÍTICA DE USO ACEITÁVEL

A política de uso aceitável não tem como objetivo impor restrições que são contrárias a outras políticas da Instituição, mas sim, estabelecer uma cultura de confiança e integridade. A instituição está comprometida em proteger seus empregados, parceiros e a própria organização quanto a ações ilegais ou danosas cometidas por algum indivíduo dentro desta, tendo conhecimento ou não de seus atos.

Intranet, *Internet* e sistemas relacionados de uso corporativo, incluindo, mas não limitando a computadores, aplicativos, sistemas operacionais, mídias de armazenamento, contas de *e-mail*, navegação na *Internet* ou outras atividades relacionadas são de propriedade da Instituição. O uso destes recursos deve ser de caráter somente corporativo, excluindo-se então o uso para fins pessoais, preservando-se os interesses da instituição, dos clientes e parceiros.

Para que a segurança da informação seja efetiva, é preciso realizar um trabalho em conjunto com todos os funcionários e parceiros da instituição que lidam com informação ou sistemas de informação. É responsabilidade de cada usuário conhecer e agir de acordo com as políticas estabelecidas por esta empresa.

Finalidade

Este documento contém as diretrizes de uso aceitável dos equipamentos computacionais da instituição. Estas regras protegem os usuários e a instituição de danos que possam ser causados. O uso inapropriado dos recursos expõe a

instituição a riscos, incluindo o comprometimento de todos os recursos de rede, ataques de vírus e questões legais.

Escopo

Esta política se aplica aos colaboradores, alunos, terceiros, consultores, empregados temporários e outros que tenham vínculo de trabalho com a instituição, incluindo todos os indivíduos que têm relacionamento com a instituição através de terceiros. Também se aplica a todos os equipamentos que são de posse ou alugados pela instituição.

Política

Uso geral:

1. Cada área da instituição é responsável por criar diretrizes para o uso pessoal da *Internet*. Em conjunto com as diretrizes aqui abordadas você deve seguir os procedimentos ditados pelo facilitador de sua área. Caso existam dúvidas, não hesite em consultar o responsável pela sua área;
2. Esta instituição recomenda que qualquer informação que você considere sensível ou vulnerável deve ser criptografada ou protegida por senha;
3. Para segurança e gerenciamento dos recursos de rede, pessoas autorizadas pela instituição podem monitorar equipamentos, sistemas e dados que trafegam na rede a qualquer momento;

4. Esta instituição se reserva ao direito de realizar auditoria nas redes locais e nos sistemas para garantir que as políticas de segurança estão sendo cumpridas;
5. Você deve tomar as precauções necessárias para que pessoas não autorizadas não tenham acesso a informações confidenciais;
6. Memorize suas senhas, lembrando que estas são pessoais e intransferíveis. Como um usuário autorizado, você é responsável pela segurança de suas senhas e contas. Tenha como hábito trocar suas senhas periodicamente;
7. Deixe seu computador ou *laptop* com uma proteção de tela protegida por senha, com ativação automática a cada 10 minutos de inatividade, ou menos, ou efetivando a retirada de suas credenciais (*logoff)* do computador quando se ausentar;
8. Postagens em listas de discussão devem conter explicitamente a informação de que a opinião difundida é pessoal e não necessariamente reflete a opinião da instituição;
9. Todos os equipamentos utilizados por sua pessoa, seja de posse da instituição ou pessoal devem ter todos os requisitos de segurança, como antivírus aprovado pela instituição, atualizados;
10. É necessário ter extrema cautela ao utilizar e-mail. Arquivos anexados podem conter vírus, cavalos de tróia ou outros aplicativos que podem causar danos à rede da instituição.

Uso inaceitável

As atividades abaixo são, geralmente, proibidas. Em casos especiais, você pode se exaurir destas restrições durante uma atividade legítima de seu trabalho (por exemplo, administradores de rede podem desabilitar o acesso à rede de um computador que está degradando a rede da instituição).

Em nenhuma circunstância um colaborador da instituição está autorizado a realizar atividades que sejam ilegais perante as leis locais, estaduais, federais ou internacionais quando estiver utilizando os recursos da organização.

Atividades na rede ou sistemas

As atividades abaixo são estritamente proibidas:

1. Violação dos direitos de qualquer pessoa ou organização protegidos por *copyright*, patentes ou outra propriedade intelectual, incluindo, mas não limitando a instalação de aplicativos “piratas”, ou outros produtos em que a instituição não tenha a devida licença para uso;
2. Cópia não autorizada de materiais, como digitalização de documentos, distribuição de fotografias de revistas, livros, músicas ou outros documentos protegidos por lei em que a instituição ou o usuário final não tenha uma licença ativa;
3. Introdução de programas maliciosos na rede, nos computadores, ou nos servidores, por exemplo: vírus, cavalos de tróia, capturadores de senhas;

4. Exposição de senhas de contas ou permissão de uso destas por outras pessoas. Isto inclui familiares ou outros membros enquanto estiver trabalhando em casa;
5. Utilizar os computadores da instituição para produzir ou repassar materiais que tenham teor sexual ou hostil;
6. Produção fraudulenta de ofertas dos produtos ou serviços oferecidos pela instituição através de sua conta;
7. Efetuar quebras nos procedimentos de segurança da rede, incluindo, mas não se limitando a acessar dados que você não deveria ter permissão. Conectar-se aos servidores utilizando a conta de outro colaborador, a não ser nos casos em que sua posição tenha permissão para tal;
8. Utilizar programas que possam degradar a performance da rede, *scanners* de portas e interceptadores de tráfego;
9. Prover informações ou listas dos colaboradores da instituição para pessoas que não estão autorizadas a receber tais dados;
10. É vedada a abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo deverá ocorrer pelo departamento técnico.

2.2 POLÍTICA PARA COMUNICAÇÕES DE E-MAIL

A política define os padrões para condução das comunicações de e-mail da instituição. Estes padrões minimizam a potencial exposição desnecessária da instituição, incluindo a perda de informações sensíveis, confidenciais ou de propriedade intelectual e degradação da imagem pública da instituição.

Escopo

Esta política se aplica aos colaboradores, alunos, terceiros, consultores, empregados temporários e outros que tenham vínculo de trabalho com a instituição, incluindo todos os indivíduos que têm relacionamento com a instituição através de terceiros.

Política

Os itens a seguir estão proibidos nesta instituição:

1. Envio de e-mails não solicitados, incluindo o envio de materiais de propaganda para pessoas que não requisitaram explicitamente tal informação (*spam*);
2. Envio de e-mails contendo informações confidenciais ou restritas à instituição;
3. Utilização do e-mail da instituição para fins pessoais;
4. Não utilização da assinatura de e-mail padronizada pela instituição;
5. Qualquer tipo de ofensa a um indivíduo ou organização por e-mail desta instituição.;

6. Uso forjado das informações contidas no cabeçalho de e-mail disponibilizado por esta instituição;
7. Criação ou replicação de “correntes”, “pirâmides” ou outros variações da mesma natureza;
8. Utilização indevida da linguagem em respostas aos e-mails comerciais, como abreviações de palavras, uso de gírias;
9. Não execute ou abra arquivos anexados enviados por remetentes desconhecidos ou suspeitos;
10. Visando racionalizar o uso e a distribuição do espaço em disco, cada usuário terá uma quota para armazenamento de suas mensagens, limitada a 15MB para colaboradores e professores e 10MB para alunos. Caso o usuário exceda essa quota, as mensagens recebidas serão devolvidas ao remetente. Para evitar que isto ocorra, o usuário deve acessar periodicamente sua caixa postal e transferir as mensagens para o seu microcomputador de trabalho;
11. Caso a instituição julgue necessário haverá bloqueios de e-mail com arquivos anexos, de e-mail para destinatários ou domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos.

Qualquer colaborador que viole as diretrizes desta política pode estar sujeito a sanções administrativas, incluindo rescisão do contrato de trabalho.

Definições

Termo	Definição
Spam	Mensagens não autorizadas ou não solicitadas.

2.3 POLÍTICA PARA USO DE INTERNET

Esse tópico visa definir as normas de utilização da *Internet,* que engloba desde a navegação a *sites*, *downloads* e *uploads* de arquivos.

Escopo

Esta política se aplica aos colaboradores, alunos, terceiros, consultores, empregados temporários e outros que tenham vínculo de trabalho com a instituição, incluindo todos os indivíduos que têm relacionamento com a instituição através de terceiros.

Política

1. É proibido utilizar os recursos da instituição para fazer o *download* ou distribuição de *software* ou dados não legalizados;
2. Poderá ser utilizada a *Internet* para atividades não relacionadas com os negócios durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta política;
3. Os colaboradores com acesso à *Internet* podem baixar somente programas ligados diretamente às atividades da instituição e devem providenciar o que for necessário para regularizar a licença e o registro desses programas;
4. Caso a instituição julgue necessário haverá bloqueios de acesso a arquivos e domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos.

Qualquer colaborador que viole as diretrizes desta política pode estar sujeito a sanções administrativas, incluindo rescisão do contrato de trabalho.

2.4 POLÍTICA PARA PREVENÇÃO DE VÍRUS

Esta política define padrões para proteger a rede e os sistemas da instituição de qualquer ameaça relacionada a vírus, cavalos de tróia ou qualquer ameaça semelhante. Estes padrões minimizam a potencial exposição da instituição a riscos que podem resultar em danos à rede da organização.

Escopo

Esta política se aplica aos colaboradores, alunos, terceiros, consultores, empregados temporários e outros que tenham vínculo de trabalho com a instituição, incluindo todos os indivíduos que têm relacionamento com a instituição através de terceiros.

Política

1. Caso seu computador não tenha um *software* de anti-vírus instalado entre em contato com o técnico de informática da sua unidade. Não utilize o equipamento até que a situação esteja normalizada;
2. Nunca abra arquivos recebidos de fontes desconhecidas ou suspeitas, seja através de *e-mail*, *cds* ou outros. Exclua estes arquivos imediatamente, verifique se o mesmo não permanece na "lixeira" de seu computador;

3. Apague *spam*s, correntes, ou qualquer outro tipo de e-mail não solicitado sem encaminhá-los, conforme a política de uso aceitável da instituição;
4. Nunca copie arquivos de fontes não confiáveis ou suspeitas;
5. Evite o compartilhamento de disco com permissão de leitura e escrita a menos que isso seja a única opção para troca de arquivos e autorizada pelo administrador de rede de sua unidade;
6. Sempre realize a verificação de vírus em dispositivos de armazenamento de dados, como disquetes e *cds*.

2.5 POLÍTICA PARA SENHAS

Descrição

Senhas são um aspecto importante da segurança computacional. Elas estão na linha de frente de proteção de sua conta. Uma senha mal escolhida pode resultar no comprometimento da rede da instituição. Diante disto, todos os colaboradores da instituição (incluindo parceiros e alunos que tenham acesso aos sistemas) são responsáveis por obedecer os passos abaixo.

Objetivo

O objetivo desta política é estabelecer um padrão para criação de senhas seguras.

Escopo

Esta política se aplica a todos os indivíduos que são responsáveis por uma conta (ou qualquer tipo de acesso que requer uma senha) em qualquer sistema ou dispositivo de rede que seja da instituição.

Política

1. Senhas de usuários comuns devem ser trocadas a cada três meses, enquanto senhas de acesso restrito devem ser trocadas a cada mês;
2. Contas que receberem senhas incorretas por três vezes consecutivas serão bloqueadas, tendo liberação somente aprovada pela administração da rede da instituição;
3. Não insira sua senha em mensagens de e-mail ou qualquer outro tipo de comunicação eletrônica;
4. Todas as senhas desta instituição devem seguir as regras abaixo.

Guia para construção de senhas

Esta instituição possui senhas para vários tipos de acesso. Os mais comuns incluem: senhas de e-mail, *intranet*, proteção de tela, acesso à rede, etc. Para que estes sistemas não fiquem comprometidos, todos os colaboradores devem estar cientes da criação de senhas seguras.

Para exemplificar, seguem abaixo algumas características de senhas fracas:

1. Contêm menos que oito caracteres;

2. São palavras encontradas em dicionários;
3. Nomes de parentes, animais de estimação, amigos, colegas de trabalho, etc;
4. Nomes de computadores, termos computacionais, comandos, páginas da *Internet*, aplicativos;
5. Inclusão do nome da instituição, localização, ou qualquer derivado;
6. Datas de nascimento, endereços e telefones;
7. Palavras ou números que seguem padrões, como *aaabbb, qwerty, 123321;*
8. Qualquer alternativa acima, escrita de forma inversa;
9. Qualquer alternativa acima, precedida ou seguida de um dígito (exemplo: senha1, 1senha).

Senhas seguras contém:

1. Tanto letras minúsculas quanto maiúsculas (exemplo: a-z, A-Z);
2. Dígitos e caracteres de pontuação (exemplo: 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./);
3. No mínimo oito caracteres alfa-numéricos;
4. Não são baseadas em palavras de nenhuma linguagem, gíria ou dialeto;
5. Não são baseadas em informações pessoais, familiares ou da instituição;
6. Não são escritas ou armazenadas em arquivos pessoais.

É possível criar senhas que podem ser facilmente lembradas. Um exemplo para criação são senhas baseadas em músicas, frases ou afirmações. Considere a frase “Esta é uma senha fácil de ser lembrada”. Esta frase pode ser transformada na seguinte senha: “Ee1sFdSl!” ou qualquer variação desta forma. NOTA: não utilize este exemplo para sua própria senha.

Padrões para proteção das senhas

1. Não use a mesma senha da instituição para acesso a outros recursos, como e-mail pessoal, conta de acesso doméstico à Internet, bancos, etc;
2. Não compartilhe sua senha com ninguém, nem mesmo com sua secretária ou assistente administrativo da sua área. Todas as senhas são confidenciais, pessoais e intransferíveis;
3. Não revele sua senha para ninguém;
4. Nunca escreva sua senha em documentos eletrônicos ou e-mails;
5. Não fale sua senha na frente de outras pessoas;
6. Não exponha dicas sobre o formato de sua senha;
7. Não revele sua senha em questionários;
8. Não compartilhe sua senha com familiares;
9. Não deixe sua senha com colegas de trabalho quando estiver em período de férias;
10. Não utilize a opção “Salvar senha” em aplicativos utilizados pela instituição.

Caso alguém necessite de uma senha para acessar um recurso da instituição encaminhe-o para o administrador de rede de sua unidade.

Se você suspeitar que sua senha foi descoberta, comunique o administrador de rede da sua unidade e troque sua senha imediatamente.

Administradores de rede podem utilizar *softwares* especializados para tentar descobrir senhas automaticamente. Caso sua senha seja descoberta será necessário substituí-la imediatamente.

2.6 POLÍTICA PARA VIRTUAL PRIVATE NETWORK (VPN)

A proposta desta política é definir padrões a serem seguidos na utilização de acesso remoto via VPN para a rede da instituição.

Escopo

Esta política se aplica a todos os empregados, terceiros, empregados temporários e parceiros que utilizam VPNs para se conectarem a esta instituição.

Política

1. É responsabilidade do usuário não permitir o uso do recurso por pessoas não autorizadas pela instituição;
2. A conexão de VPN só deve ser feita através do aplicativo disponibilizado por esta instituição. Em nenhum caso outro aplicativo poderá ser utilizado;
3. Para que a conexão seja concluída é necessário informar seu usuário e senha, sendo que esta deve seguir a política de senhas da instituição;

4. O aplicativo disponibilizado pela instituição contém embutido um *firewall*, este que não deve, em hipótese nenhuma, ser desabilitado;
5. A gerência dos acessos via VPN é da área central de TI desta instituição, e está autorizada a negar qualquer tipo de acesso caso seja encontrada alguma irregularidade, independente de horário ou comunicação;
6. Qualquer computador que seja utilizado para conexão VPN com esta instituição deve possuir antivírus instalado e atualizado;
7. As conexões VPN inativas por mais de 15 minutos serão desconectadas. *Pings* ou qualquer outro processo artificial para manter a conexão ativa não poderão ser utilizados;
8. O concentrador de VPNs está configurado para manter uma conexão por 24 (vinte e quatro) horas de tempo total, caso este tempo se exceda é necessário realizar uma nova conexão;
9. Ao utilizar a VPN desta instituição com equipamentos pessoais, os usuários devem entender que seus equipamentos são de fato uma extensão da rede desta instituição, estando sujeitos às mesmas normas e políticas que outros equipamentos.

Qualquer colaborador que viole as diretrizes desta política pode estar sujeito a sanções administrativas, incluindo rescisão do contrato de trabalho.

Definições

Termo	**Definição**
Firewall	Dispositivo de rede que tem como função regular o tráfego entre redes distintas.
Ping	Comando utilizado para realizar testes em redes de computadores.

2.7 POLÍTICA PARA DESENVOLVIMENTO DE APLICAÇÕES

Esta política tem como objetivo definir diretrizes básicas para que os sistemas desenvolvidos dentro ou fora desta instituição contenham níveis básicos de segurança, evitando que vulnerabilidades sejam inseridas na rede através destas aplicações.

Escopo

Esta política se aplica aos colaboradores, terceiros, consultores, empregados temporários e outros que tenham vínculo de trabalho com a instituição, incluindo todos os indivíduos que têm relacionamento com a instituição através de terceiros, que desenvolvam aplicações para esta instituição.

Política

1. Aplicações devem suportar autenticação individual de usuários, e não de grupos;
2. Em hipótese nenhuma as aplicações devem guardar senhas em texto plano ou qualquer outra forma que a senha possa ser descoberta;
3. As aplicações devem suportar autenticação via LDAP, para que possam ser integradas com os sistemas atualmente utilizados;
4. Os desenvolvedores devem se preocupar com a segurança das aplicações contra qualquer tipo de ataque que possa ser realizado através da mesma. Como exemplos de vulnerabilidades são destacadas:

    - Cross Site Scripting;

- *SQL Injection;*
- *Session Hijacking;*
- *Parameter Tampering;*
- *Privilege Escalation;*
- *Brute Force.*

5. Para os fornecedores externos os acessos aos servidores de aplicação serão somente via FTP e HTTP, utilizando a VPN desta instituição. Em hipótese nenhuma, serão disponibilizados outros tipos de acesso aos servidores;
6. Esta instituição poderá realizar testes periódicos de segurança das aplicações, seja desenvolvida interna ou externamente, sem notificação dos desenvolveres. Caso seja encontrada alguma vulnerabilidade, esta deve ser prontamente corrigida.

2.8 POLÍTICA PARA ADMINISTRADORES DE REDE

A proposta desta política é definir padrões a serem seguidos na administração dos equipamentos de rede da instituição.

Escopo

Esta política se aplica a todos os empregados, terceiros, empregados temporários e parceiros que administram equipamentos de rede desta instituição.

Política

1. É responsabilidade do administrador de rede não permitir o uso de recursos computacionais por pessoas não autorizadas pela instituição;

2. Não é permitida a instalação de novos servidores/serviços de rede que não tenham autorização prévia da equipe de informática da sede da instituição;
3. A monitoração dos equipamentos é de responsabilidade do administrador de rede;
4. É dever zelar pela segurança de rede da sua unidade, visando a maior restrição possível quanto aos acessos à rede;
5. A gerência sobre o acesso à *Internet* deve ser executada através do Gateway Multiuso, bloqueando e permitindo tráfego *Web* quando necessário;
6. Vulnerabilidades descobertas e intrusões de rede devem ser notificadas à equipe de informática da sede da instituição;
7. É responsabilidade do administrador garantir que as regras de segurança por ele implementadas devem ser efetivas e documentadas;
8. Novas políticas podem ser implementadas desde que sejam bem documentadas e com autorização da sede da instituição.

Qualquer colaborador que viole as diretrizes desta política pode estar sujeito a sanções administrativas, incluindo rescisão do contrato de trabalho.

2.9 POLÍTICA DE SEGURANÇA FÍSICA

O objetivo desta política é prevenir o acesso não-autorizado às instalações físicas desta instituição, evitando perdas ou danos às informações. Algumas áreas precisam receber mais atenção em relação ao controle de acesso, pois podem conter informações ou equipamentos que deve estar bem protegidos.

Instalações da equipe de TI desta instituição devem minimizar o acesso público direto a estas dependências.

Escopo

Esta política se aplica aos colaboradores, alunos, terceiros, consultores, empregados temporários e outros que tenham vínculo de trabalho com a instituição, incluindo todos os indivíduos que têm relacionamento com a instituição através de terceiros.

Política

1. Apenas pessoas autorizadas pela instituição podem acessar as instalações de TI, sendo que os colaboradores devem estar devidamente identificados com crachás;
2. Áreas que contenham informações confidenciais de alunos e da instituição não devem permitir acesso de pessoas não autorizadas, incluindo colaboradores;
3. Na entrada de alunos e visitantes aos laboratórios de informática e bibliotecas pelo menos um colaborador deve estar presente no recinto, sendo este nomeado como responsável nesta ocasião;
4. É de responsabilidade do colaborador que utilizar o laboratório de informática zelar pelas instalações ali presentes;
5. No caso de algum tipo de dano ou mau funcionamento dos equipamentos a equipe técnica de TI da unidade deve ser informada;

6. Nenhum tipo de equipamento deve ser conectado à rede sem autorização prévia do responsável de TI da unidade;
7. Qualquer tipo de material nocivo aos equipamentos, tais como alimentos, bebidas e fumo está proibido em qualquer laboratório. Celulares também deverão ser desligados para não perturbar outras pessoas que estiverem usufruindo dos recursos.

VI Resultados

Para realizar os testes necessários para efetivação dos procedimentos de segurança utilizados no Gateway Multiuso utilizou-se uma estrutura composta por quatro computadores (dois clientes, um servidor de arquivos e um com função de roteador), um *switch* Cisco Catalyst 2950, dois roteadores Cisco 2821, um *firewall* e concentrador de VPN Cisco ASA 5520 e o próprio Gateway Multiuso.

Os computadores clientes estavam utilizando o sistema operacional Windows XP, enquanto o servidor de arquivos e o computador que fazia papel de roteador da rede corporativa estavam utilizando Linux.

Os dois computadores com Windows foram utilizados como clientes de rede, um da VLAN ADM e outro da VLAN EDU, visando testar toda a conectividade e segurança da solução.

O computador que estava utilizando Linux foi configurado para ser o roteador que se conecta à rede corporativa, realizando funções de PAT na interface que se conecta ao *firewall* da estrutura utilizada.

O roteador Cisco 2821 conectado ao Gateway Multiuso foi configurado para realizar a conexão VPN com o *firewall* quando necessário, ou seja, em momento de contingência devido a falha do enlace corporativo.

O *firewall* Cisco ASA 5520 foi configurado para aceitar conexões VPN do roteador em questão, assim como foram criadas regras para permitir os acessos provenientes do enlace *Internet* e também do enlace corporativo, encaminhando as requisições para o roteador que está realizando a conexão com a *Internet.*

A figura 9 ilustra a estrutura utilizada para realizar os testes realizados neste trabalho.

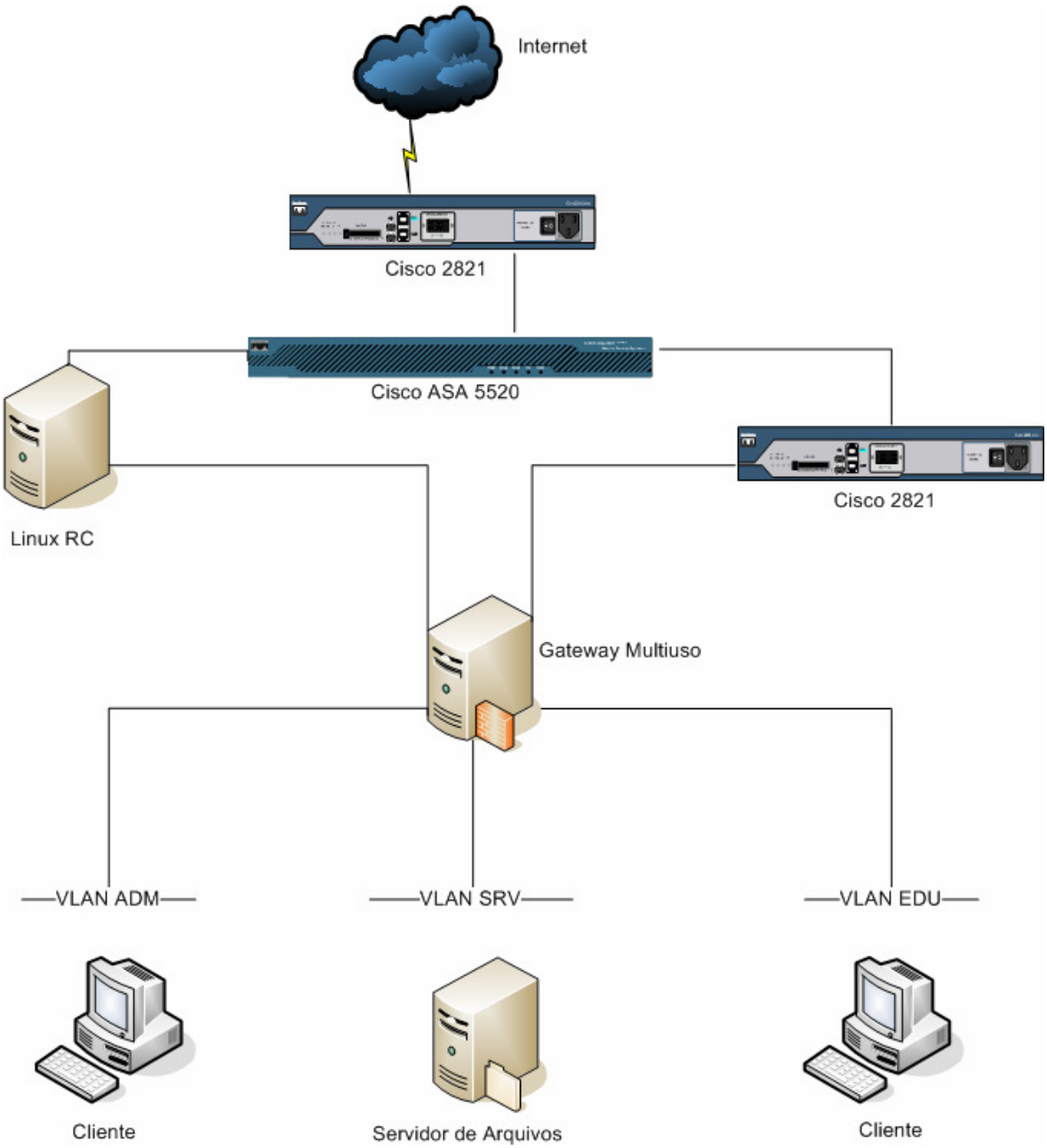

Figura 9 – Estrutura utilizada para testes

Os primeiros testes foram realizados para testar a marcação dos pacotes e o roteamento. Pacotes enviados ao ponto central da instituição foram enviados para a tabela RC, garantindo que teriam como destino a rede corporativa da instituição. O mesmo aconteceu com os pacotes enviados à *Internet*, em que foram destinados à tabela correta (INET), vide figura 5.

Após verificar o correto funcionamento do roteamento, a nova etapa de testes foi a verificação da configuração automática do navegador utilizado. Sem a utilização da opção “Detectar automaticamente as configurações de rede”, a página para configuração do navegador foi exibida, conforme figura 7 deste trabalho. O resultado desta operação pode ser visto nos registros abaixo, onde o cliente recebe a página de configuração do navegador, e, após configurá-lo corretamente, recebe o *script* com os dados necessários para utilizar a *Internet*:

```
172.16.3.16 - - [03/Jan/2007:15:05:51 -0200] "GET /index.html HTTP/1.1"
172.16.3.16 - - [03/Jan/2007:15:10:02 -0200] "GET /wpad.dat HTTP/1.1"
```

Nos testes de segurança o *firewall* realizou o bloqueio de tudo o que não estava explicitamente permitido. Como pode ser visto abaixo, foi negado o envio de pacotes UDP para a *Internet*, oriundo da rede educacional:

```
Jan  3 14:36:11 gateway kernel: Shorewall:EDU2INET:DROP:IN=eth0.50
OUT=eth0.60 SRC=172.16.5.5 DST=129.6.15.29 LEN=76 TOS=0x00 PREC=0x00
TTL=63 ID=21784 PROTO=UDP SPT=2930 DPT=123 LEN=56
Jan  3 14:37:11 gateway kernel: Shorewall:EDU2INET:DROP:IN=eth0.50
OUT=eth0.60 SRC=172.16.5.5 DST=131.107.1.10 LEN=76 TOS=0x00 PREC=0x00
TTL=63 ID=21785 PROTO=UDP SPT=2931 DPT=123 LEN=56
```

A implementação de regras de acesso ao Squid também foi validada, garantindo que o fluxograma exibido na figura 6 estava implementado corretamente. Os testes garantiram que os acessos a páginas que continham palavras proibidas foram realmente bloqueados pelo Gateway, exibindo a seguinte mensagem ao tentar acessar um *site* de relacionamentos na *Internet*:

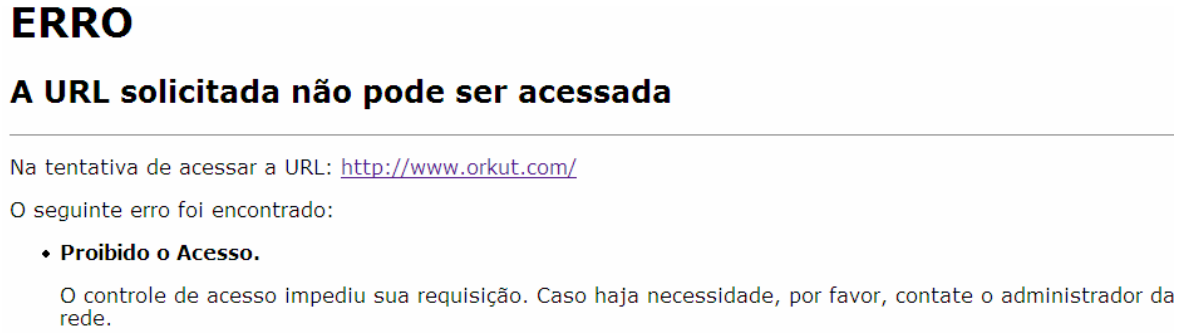

Figura 10 – Bloqueio de acesso

Dando continuidade aos testes, o próximo passo foi validar a atuação do HIDS do Gateway Multiuso. Testes realizados com ferramentas de análise automatizada de segurança, procurando por aplicações vulneráveis, revelaram que o Gateway se comportou como proposto, identificando o autor do ataque e reportando aos administradores. Neste caso também era possível configurar o HIDS para que efetuasse uma ação assim que o ataque fosse identificado. No registro abaixo é possível visualizar a atuação do HIDS:

```
Received From: /etc/httpd/logs/access_log
    Rule: 3153 fired (level 10) -> "Multiple common web attacks from same
souce ip.'"
    Portion of the log(s):

     172.16.5.72   -   -   [24/Aug/2006:21:33:26   -0300]   "GET   /cgi-
bin/eboard40//index2.cgi?
frames=yes&board=demo&mode=Current&threads=Collapse&message=../../../../.
./../../../../../etc/passwd%00 HTTP/1.1" 302 454       "-" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.0)"
    172.16.5.72  -  -  [24/Aug/2006:21:33:26  -0300]  "GET  /index2.cgi?
frames=yes&board=demo&mode=Current&threads=Collapse&message=../../../../.
```

```
./../../../../../etc/passwd%00 HTTP/1.1" 302 454 "-" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.0)"
```

Finalmente, o gerenciamento de falhas e o plano de contingência foram testados, utilizando o seguinte método: O computador que faz a função de roteador e que se conecta à rede corporativa da instituição foi configurado para descartar todos os pacotes, fazendo com que o Gateway Multiuso o identificasse como um enlace inativo. Após o tempo previsto, o equipamento entrou em modo de contingência, utilizando o enlace conectado à *Internet* para trafegar os dados corporativos. O roteador estava configurado para iniciar uma conexão VPN com o *firewall*, garantindo assim a segurança dos dados. Os testes foram registrados nos arquivos de *log* e enviados aos administradores:

```
Entrou em contingência em: Sat Nov 11 14:31:09 BRST 2006
Motivo: Enlace RC com problemas.
------------
Saiu da contingência em: Sat Nov 11 17:57:44 BRST 2006
```

O mesmo ocorreu com o teste de contingência quando o enlace *Internet* foi desativado. As conexões HTTP que estavam utilizando o enlace em questão foram redirecionadas para o enlace corporativo, garantindo que o acesso à *Internet* não ficasse indisponível. Após a detecção pelo Gateway da falha do enlace, a estrutura de roteamento foi alterada automaticamente e foram registrados nos *logs* os dados da operação. Estes dados também foram enviados aos administradores por *e-mail.*

Os registros podem ser visualizados no exemplo seguinte:

```
Entrou em contingência em: Sat Nov 11 18:21:14 BRST 2006
Motivo: Enlace Internet com problemas.
------------
Saiu da contingência em: Sat Nov 11 18:47:25 BRST 2006
```

Nos dois casos, após a realização dos testes necessários para validar o plano de contingência, os enlaces foram reconfigurados para voltar ao estado normal. Assim, o Gateway Multiuso identificou que os enlaces estavam ativos novamente e a estrutura de roteamento voltou ao seu padrão sem problemas.

O equipamento desenvolvido para garantir a segurança e desempenho das redes de instituições de ensino foi validado com os testes acima descritos, garantindo assim, sua eficácia quanto ao objetivo proposto.

VII Conclusões

De acordo com os objetivos estabelecidos no início do trabalho, a metodologia proposta mostrou-se um importante instrumento de padronização da segurança de rede em ambientes de instituições de ensino, sendo possível, a partir de sua aplicação, garantir que a segurança de rede seja efetiva e bem planejada.

No tocante ao aspecto acadêmico do trabalho foi de grande valia para analisar os aspectos teóricos e conhecer melhor não só a solução adotada, mas também, outras formas de uso de ferramentas de segurança. Combinando o conhecimento teórico com o conhecimento prático, adquirido no desenvolver deste trabalho, considero que tenho mais subsídios para a implementação de novos recursos de segurança de rede, quando se fizerem necessários.

O desenvolvimento do Gateway Multiuso proporcionou um conhecimento mais aprofundado do sistema operacional Linux e seus serviços, concedendo mais confiança na implementação de novas soluções de segurança utilizando esta plataforma.

A definição das regras de *firewall* para estes ambientes garantem que somente o tráfego explicitamente permitido será liberado, prevenindo a difusão sem limites de vírus que utilizam a rede para se propagar, utilizando portas não comuns.

No desenvolvimento deste trabalho foi possível notar que o mapeamento de todo o tráfego de uma rede não é uma tarefa tão simples quanto se pensava, pois podem existir tráfegos esporádicos que não eram esperados, mas que

precisavam ser contemplados nas regras de *firewall* e também nas políticas de segurança.

A definição automática das configurações de *proxy* nos navegadores dos computadores clientes garante um trabalho mínimo para os administradores de rede, ou aos responsáveis pela informática destas instituições. O processo de configuração é rápido e eficaz, garantindo que todas as conexões realizadas pelos navegadores sejam direcionadas ao *proxy*, que realiza as funções de *cache* e controla o tráfego através de listas de controle de acesso.

O Gateway Multiuso possui implementações que considero muito interessantes, que são o roteamento avançado e o plano de contingência. Este último garante que apesar de existirem falhas em um dos dois enlaces de comunicação, o tráfego será redirecionado para o enlace que continua operante.

O tráfego corporativo estará sempre seguro, já que em seu estado normal de funcionamento, o Gateway o direciona ao enlace corporativo, que é uma rede privada, sem acessos externos. No modo de contingência, causado pela falha do enlace corporativo, o tráfego corporativo será enviado para o ponto central da topologia através da *Internet,* porém, será criptografado através da VPN realizada entre o roteador do enlace *Internet* com o *firewall* da instituição.

Os registros de atividades dos usuários e dos equipamentos, assim como o HIDS utilizado no Gateway Multiuso garantem ao administrador maior segurança no gerenciamento dos recursos utilizados, das vulnerabilidades exploradas, e de possíveis tentativas de invasão de sua rede. Alarmes podem ser disparados aos administradores com um conjunto de registros do ocorrido, fazendo com que ações possam ser tomadas rapidamente, visando evitar qualquer tentativa de operação não permitida na rede.

No tocante aos problemas encontrados no desenvolvimento deste trabalho, podem ser citados os erros encontrados no plano de contingência em situações específicas e a configuração de VPNs, que resultavam em tabelas de roteamento errôneas, não garantindo o sucesso esperado.

A definição da política de segurança é importante em qualquer instituição, porém, em ambientes de instituições de ensino são encontradas particularidades devido à variedade de públicos que freqüentam estas instituições. A implantação desta política é necessária para que as definições de segurança sejam conhecidas por todas as pessoas que utilizam os recursos de informática disponibilizados por estas instituições. Garantir que os acessos aos dados da organização sejam seguros, íntegros e confiáveis envolve também a conscientização das pessoas que utilizam estes recursos. Nesta fase, que considero a parte mais delicada deste trabalho, é preciso prever que situações de rejeição serão encontradas na sua implantação, já que mudanças na cultura das pessoas e instituições são tarefas que exigem paciência e compreensão dos envolvidos.

Acredito que com a implantação do modelo de padronização de redes ambientado neste trabalho, em conjunto com o Gateway Multiuso e as políticas de segurança demonstradas, o nível de segurança de uma rede em ambientes de instituições de ensino pode ser considerado mais adequado aos problemas enfrentados atualmente.

Certamente, a solução é considerada definitiva, mas não imutável, até porque as necessidades das redes mudam, as vulnerabilidades aumentam, e os níveis de segurança precisam ser revistos.

Para trabalhos futuros, sugiro a definição de níveis de qualidade de serviço (QoS) para estas redes, seja este implementado no Gateway Multiuso ou nos roteadores, garantindo assim, um consumo mais ciente da largura de banda disponível para estes ambientes. Na linha de segurança pode ser implementado autenticação de camada dois, utilizando 802.1x, garantindo acesso à rede somente após autenticação de máquina e usuário.

VIII Referências Bibliográficas

1. WACK, J.; CUTLER, K.; POLE, J. **Guidelines on Firewalls and Firewall Policy**. NIST Special Publication 800-41, 2002.
2. NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos**. 3.ed. São Paulo: Futura, 2002.
3. ACCARDI, K.; et. al. **Network Processor Acceleration for a Linux Netfilter Firewall**. *ACM Proceedings of the symposium on Architecture for networking and communications systems.* p. 115-123. out. 2005.
4. GOUDA, M. G.; LIU, A. X.. **A Model of Stateful Firewalls and its Properties**. *IEEE Proceedings of the International Conference on Dependable Systems and Networks*, p. 128-137, jul. 2005.
5. GANJAM, A.; ZHANG, H.. **Connectivity Restrictions in Overlay Multicast.** *ACM Proceedings of the 14th international workshop on Network and operating systems support for digital audio and video*. p. 54-59. jun. 2004.
6. *INTERNET ENGINEERING TASK FORCE*. **RFC3022:** *Traditional IP Network Address Translator*. New York, 2001. 16p.
7. *INTERNET ENGINEERING TASK FORCE*. **RFC 2663**: *IP Network Address Translator (NAT) Terminology and Considerations*. New York, 1999. 30p.
8. LI, B.; et.al. **On the Optimal Placement of Web Proxies in the Internet**. *IEEE Proceedings on INFOCOM*, v. 3, p. 1282-1290. mar. 1999.

9. MALTZAHN, C.; RICHARDSON, K. J.; GRUNWALD, D. **Performance Issues of Enterprise Level Web Proxies**. *ACM Proceedings of SIGMETRICS.* p. 13-23. jun. 1997.
10. Cisco Systems, et. al. **Internetworking Technologies Handbook**. 3. ed**.** EUA: Cisco Press, 2001.
11. FRANKEL, S.; et. al. **Guide to IPsec VPNs**. NIST Draft Special Publication 800-77, 2005.
12. ABREU, D. **Melhores práticas para classificar informações.** 2004. Disponível em <http://www.modulo.com.br>. Acesso em: 22 de Janeiro de 2006.
13. WIKIPEDIA. **Sistema de detecção de intrusos.** 2006. Disponível em <http://pt.wikipedia.org>. Acesso em: 01 de fevereiro de 2006.
14. DAVIES, J.; LEWIS E. **Deploying Virtual Private Networks with Microsoft Windows Server 2003**. 1. ed. EUA: Microsoft Press. 2004.
15. O'GUIN, S.; WILLIAMS, C. K.; SELIMIS, N. **Application of Virtual Private Networking Technology to Standards-Based Management Protocols Across Heterogeneous Firewall-Protected Networks**. *IEEE Proceedings on Military Communications*, v. 2, p. 1251-1255, nov. 1999.
16. LIANG, H.; et. al. **Minimal Cost Design of Virtual Private Networks**. *IEEE Canadian Conference on Electrical and Computer Engineering*, v. 3, p. 1610-1615, maio 2002.
17. *INTERNET ENGINEERING TASK FORCE*. **RFC 2401:** *Security Architecture for the Internet Protocol.* New York, 1998. 66p.
18. STALLINGS, W. **Cryptography and Network Security: Principles and Practices.** 3.ed. EUA: Prentice Hall, 2003.

19. J. Wen, X. Lu. **The Design of QoS Guarantee Network Subsystem**. *ACM SIGOPS Operating Systems Review*, v. 36, n .1, p. 81-87. jan. 2002.
20. Cisco Systems, et. al. **CCNA 3: Conceitos Básicos de Switching e Roteamento Intermediário v3.1.1**. Cisco Systems, Inc: 2003.
21. Cisco Systems, et. al. **FNS: Fundamentals of Network Security v1.0.** Cisco Systems, Inc: 2003.
22. ODOM, W. **Cisco CCNA #640-607 Exam Certification Guide**. EUA: Cisco Press, 2002.
23. CERT.BR. **Práticas de segurança para administradores de redes Internet.** 2006. Disponível em <http://www.cert.br>. Acesso em: 13 de Janeiro de 2006.
24. HUBERT, B.; et. al. **Linux Advanced Routing & Traffic Control HOWTO**. 2003. Disponível em: <http://lartc.org/howto/>. Acesso em: 15 janeiro 2006.
25. EASTEP, T. **Shorewall 3.x Documentation**. 2005. Disponível em: <http://www.shorewall.net/Documentation_Index.html>. Acessado em: 15 janeiro 2006.
26. CAMERON, J. **Managing Linux Systems with Webmin: System Administration and Module Development**. EUA: Addison Wesley, 2003.
27. COOPER, M. **Advanced Bash-Scripting Guide: An in-depth exploration of the art of shell scripting**. 2005. Disponível em: <http://www.tldp.org/LDP/abs/html/>. Acesso em 15 janeiro 2006.
28. ABREU, D. **Melhores práticas para classificar as informações**. Disponível em: <http://www.modulo.com.br>. Acesso em 10 julho 2006.
29. WADLOW, T. A. **Segurança de redes: Projeto e gerenciamento de redes seguras.** São Paulo: Campus, 2000.

30. SWANSON, M.; et. al. **Contingency Planning Guide for Information Technology Systems**. NIST Special Publication 800-34, 2002.
31. VALENZUELA, J. L; et. al. **A Hierarchical Token Bucket Algorithm to Enhance QoS in IEEE 802.11:Proposal, Implementation and Evaluation**. *IEEE 60th Vehicular Technology Conference*, v. 4, p. 2659-2662, Set. 2004.
32. ALBITZ, P.; LIU, C. **DNS and BIND, 4th Edition.** EUA: O'Reilly, 2001.
33. BAUER, M. D. **Building Secure Servers with Linux**. EUA: O'Reilly, 2002.

ANEXOS

Anexo 1: Artigo

SEGURANÇA DE REDE EM AMBIENTES DE INSTITUIÇÕES DE ENSINO

VIOLADA, P. A. M. V.

RESUMO

Foram definidas sugestões de padronização das redes de instituições de ensino. Esta padronização envolve a segmentação dos ambientes administrativos, onde se encontram os colaboradores, e educacionais, que são os laboratórios, bibliotecas e salas de aula. Além da segmentação, é proposto o desenvolvimento de um equipamento que adicione mecanismos de segurança, desempenho, redundância e gerenciamento. Neste equipamento são definidas regras de bloqueio e acesso, registro de atividades, e um plano de contingência para casos de falha nas redes. Para que a solução de segurança seja efetiva, são definidas diretrizes básicas de uma política de segurança para este cenário.

Palavras-chave: Segurança de rede, Política de segurança, VLAN, Firewall.

1. Introdução

A operação em rede possibilita, entre outras coisas, ganhos de produtividade pelo compartilhamento de recursos e propagação da informação, inclusive com a finalidade de divulgação. Contudo, esses benefícios trazem alguns riscos. Conectar-se em rede significa possibilitar, mesmo que sob condições específicas e com algum tipo de controle, o acesso externo aos recursos computacionais, inclusive às informações. Assim, falhas na especificação das condições e controle de acesso podem ser exploradas por usuários da rede, externos ou internos, para obtenção de acesso não autorizado aos recursos. Essas falhas nos sistemas podem causar impactos nos mais diferentes níveis, iniciando como um simples constrangimento, passando pelo desgaste da imagem corporativa, e chegando a perdas financeiras e de mercado.

2. Contexto Inicial

O cenário de rede que será usado para definir este trabalho aborda a rede de uma instituição de ensino que detém uma rede privada de alta capilaridade, com pontos de presença de abrangência estadual, conectando-se a um ponto central onde está localizada a sede desta empresa.

Na sede estão localizados todos os serviços essenciais para a instituição, como sistema de ERP

corporativo, que é acessado através de conexões remotas, servidores de e-mail e web, assim como o servidor de banco de dados que contém as informações cruciais para a sede e suas filiais.

O acesso à Internet desta organização se dá pela sede, sendo este usado tanto pelos funcionários da sede quanto das filiais. É por este enlace que as requisições externas aos servidores da empresa chegam.

Concentrar o acesso à Internet no ponto central pode ser considerado um risco para a organização já que:

- O uso exacerbado deste enlace pode comprometer o acesso externo aos serviços disponíveis;
- Caso este enlace venha a ter problemas, como queda ou problema com o equipamento que realiza a conexão, toda a organização (sede e filiais) tem seu acesso prejudicado.

Nas filiais estão localizados os alunos desta instituição de ensino, os professores e os colaboradores responsáveis pelo funcionamento da filial.

As dependências das filiais são organizadas em: áreas de colaboradores (funcionários da unidade), áreas para os professores (sala dos professores e laboratórios) e os laboratórios de informática para os alunos.

Uma descrição básica da rede destas filiais pode ser observada abaixo:

- Rede local contendo os colaboradores da unidade (ambiente administrativo) e salas de aula e laboratórios (ambiente educacional);
- Servidores de arquivos;
- Servidor de antivírus;
- Uma conexão com a rede privada até o ponto central da topologia (rede corporativa).

3. Padronização das redes

Algumas considerações sobre as redes das filiais desta organização são:

- Falta de padronização da segurança de rede;
- Problemas de desempenho no acesso aos conteúdos corporativos e à Internet em momentos de uso intensivo da rede.

A solução encontrada para resolver estes problemas foi a inclusão de ativos de rede que possam garantir os níveis desejados na padronização da segurança, como exemplo, podem ser substituídos hubs por switches, incluir firewalls na rede e a criação de políticas de segurança.

Com estes padrões é possível obter um nível de segurança que não existia anteriormente, podendo a rede ser segmentada logicamente para que o tráfego corporativo, proveniente dos colaboradores não seja visível pelos alunos, que estão localizados em laboratórios de informática e bibliotecas.

Para permitir que as considerações de segurança apresentadas não permaneçam na instituição, foram definidas novas características, entre elas a criação de VLANs para segmentar o tráfego entre as diferentes redes:

- VLAN RC (Rede Corporativa) – VLAN que se conecta à Rede Corporativa da organização;
- VLAN ADM (Administrativa) – VLAN que abrange a rede administrativa (colaboradores) da filial;

- VLAN SRV (Servidores) – VLAN que abrange os servidores;
- VLAN EDU (Educacional) – VLAN que abrange a rede educacional;
- VLAN INET (Internet) – VLAN que se conecta com a Internet.

Outras características são:

- Configuração de um equipamento que faça o roteamento entre as diferentes redes, denominado Gateway Multiuso;
- Inclusão de um enlace Internet para que os dados corporativos tenham maior performance no enlace privado;
- Criação de uma solução de redundância dos dados destinados à sede, utilizando VPN. Caso o enlace da rede privada venha a falhar, o tráfego pode ser roteado ao ponto central através de uma VPN utilizando IPSec.

4. Gateway Multiuso

O Gateway Multiuso tem como principal função garantir a segurança da rede das filiais, sendo utilizados somente aplicativos e sistema operacional de código aberto. É uma solução de baixo custo porém de alto valor agregado, já que será considerado como o concentrador da rede, por onde toda comunicação entre redes diferentes deve passar.

O Gateway executará algumas funções na rede local, tais como: roteamento avançado (policy based routing), filtro de pacotes (firewall), proxy web, gerenciamento de endereços IP (dhcpd), servidor web (httpd), gerenciamento de falhas e outros.

4.1 Roteamento avançado

O Gateway possui subinterfaces conectadas a todas as VLANs previamente definidas, agindo como o roteador destas redes. Com isso, todo o tráfego entre as diferentes VLANs deve, obrigatoriamente, utilizar o Gateway como roteador.

Foram criadas duas tabelas de roteamento para que os pacotes sejam encaminhados aos seus destinos corretamente. Para tal, foram inseridas no arquivo /etc/iproute2/rt_tables as seguintes tabelas:

- Tabela 5: INET (Internet)
- Tabela 6: RC (Rede Corporativa)

A identificação e marcação dos pacotes ocorrem utilizando a tabela mangle do Netfilter (IPtables), tendo a seguinte regra básica:

- Tráfego destinado à Rede Corporativa deve ser encaminhado à tabela 6 (RC);
- Qualquer outra comunicação que não seja para as VLANs internas (ADM, EDU e SRV) deve ser encaminhada para a tabela 5 (INET).

Com essa estratégia, somente os dados corporativos utilizarão o enlace destinado a este fim. No caso de falha de algum dos enlaces, o Gateway será reconfigurado automaticamente para que nenhum acesso seja perdido.

4.2 HIDS

Para realizar as funções de HIDS no Gateway Multiuso, optou-se a solução de código aberto chamado OSSEC HIDS. O aplicativo provê as seguintes funções:

- Análise de logs;
- Verificação de integridade dos arquivos;

- Detecção de rootkits;
- Alertas por email;
- Respostas pró-ativas, baseadas nos incidentes.

No caso do Gateway Multiuso são feitas as análises de logs dos serviços Syslog, Apache e Squid.

A verificação da integridade dos arquivos é feita utilizando MD5 ou SHA1. Periodicamente são gerados hashes dos arquivos de sistema, e comparados com o valor armazenado anteriormente. Caso os valores difiram, é gerado um evento, que pode ser armazenado nos registros do HIDS ou enviado por e-mail.

O OSSEC pode enviar e-mail aos administradores assim que ocorre um evento, possibilitando ações pró-ativas até mesmo na eventual falha de hardware em virtude da análise de logs.

4.3 Firewall

Para realizar a função de Firewall foi configurado o serviço Shorewall, que é uma aplicação de alto nível utilizada para administrar o IPtables de forma mais fácil e ágil.

O Shorewall também utiliza o conceito de zonas, que no Gateway tem a mesma denominação das VLANs utilizadas, já que são as redes diretamente conectadas, ou seja, o Shorewall possui as seguintes zonas:

- RC (Conexão com a Rede Corporativa);
- ADM (Ambiente de administração);
- SRV (Ambiente dos servidores);
- EDU (Ambiente educacional);
- INET (Conexão com a Internet);
- Firewall (Zona que caracteriza o próprio equipamento).

Um modelo de regras de firewall foi desenvolvido como configuração mínima de regras para o Gateway. Este modelo considera todos os serviços implementados pelo Gateway e os aplicativos utilizados pela rede corporativa.

Este modelo considera que tudo aquilo que não é explicitamente permitido deve ser proibido. São permitidas apenas conexões entrantes a servidores específicos, limitando-as ao mínimo de serviços/portas necessárias, e também não são permitidos acessos externos às redes locais.

4.4 Plano de contingência

Um componente crítico das redes das unidades é o enlace corporativo, pois toda comunicação administrativa da organização utiliza este caminho. No caso de falha deste enlace de comunicação, as operações normais das unidades ficam comprometidas, resultando em perda de tempo, e muitas vezes de dinheiro. Por esta razão, define-se um meio de realizar automaticamente o gerenciamento de falha do enlace corporativo e um plano de contingência caso uma falha venha a ocorrer.

O plano de contingência definido para uma eventual falha do enlace corporativo de uma unidade consiste na utilização de VPN e roteamento adaptativo. Este plano é executado automaticamente assim que for detectada uma falha no enlace corporativo, através do script de gerenciamento de falhas.

Para que o plano de contingência seja efetivado é necessário estabelecer uma VPN do roteador que está ligado à Internet com o ponto central da topologia, no firewall externo que também realiza a função de concentrador de VPN. Este

processo garante um enlace de comunicação seguro entre a unidade e o ponto central, pois utiliza IPSec para realizar a criptografia dos dados. Após este passo é preciso alterar a estrutura de roteamento do Gateway, indicando que o enlace corporativo não está mais disponível. O tráfego que antes utilizava o enlace corporativo agora pode utilizar a VPN estabelecida para trafegar os dados, mantendo saída normal do tráfego destinado à Internet.

A queda do enlace que conecta a unidade à Internet resulta em um processo diferente do exposto acima. Neste caso, os aplicativos corporativos não sofrerão perdas, já que a comunicação com o ponto central, através do enlace corporativo, não foi afetado. No entanto, o tráfego destinado à Internet não alcançará o seu destino, resultando em perdas. Para que isso não ocorra, o plano de contingência foi definido para que o tráfego Web (portas TCP 80 e 443) utilize o enlace corporativo, e tenha saída à Internet no ponto central da instituição. Este caso também requer a reestruturação do roteamento do Gateway Multiuso.

Nos dois casos a disponibilidade das aplicações é assegurada, garantindo que não ocorram períodos de inatividade da unidade pela queda de algum enlace de comunicação.

A cada processo de contingência que é executado, um e-mail é enviado aos administradores de rede, para que possam tomar as devidas providências quanto à manutenção do enlace.

5. Políticas de segurança

Instituições de ensino têm particularidades em relação a uma empresa comum, principalmente relacionada às pessoas que freqüentam tal instituição. Além do colaborador, temos a figura do aluno, que pode estar assistindo às aulas em determinados momentos, e em outros estar utilizando os recursos disponibilizados pela instituição para realizar seus trabalhos escolares.

Uma política de segurança voltada para instituições de ensino deve ser criada de forma a estabelecer regras a serem seguidas por todos os usuários dos recursos de informática, de maneira que todos sejam envolvidos e conscientizados da importância da segurança das informações na organização.

O principal objetivo da política de segurança é garantir que os recursos e as informações estarão sendo utilizados da maneira correta.

Cada usuário deve ter ciência da utilização e manipulação dos dados da empresa, evitando colocar em risco qualquer tipo de informação que possa ser prejudicial para a instituição no futuro.

5.1 Política de uso aceitável

A política de uso aceitável não tem como objetivo impor restrições que são contrárias a outras políticas da Instituição, mas sim, estabelecer uma cultura de confiança e integridade. A instituição está comprometida em proteger seus empregados, parceiros e a própria organização quanto a ações ilegais ou danosas cometidas por algum indivíduo dentro desta, tendo conhecimento ou não de seus atos.

5.2 Política para comunicações de e-mail

A política define os padrões para condução das comunicações de e-mail da instituição. Estes padrões minimizam a potencial exposição desnecessária da instituição,

incluindo a perda de informações sensíveis, confidenciais ou de propriedade intelectual e degradação da imagem pública da instituição.

5.3 Política para uso de Internet

Essa política visa definir as normas de utilização da Internet, que engloba desde a navegação a sites, downloads e uploads de arquivos.

5.4 Política para prevenção de vírus

Esta política define padrões para proteger a rede e os sistemas da instituição de qualquer ameaça relacionada a vírus, cavalos de tróia ou qualquer ameaça semelhante. Estes padrões minimizam a potencial exposição da instituição a riscos que podem resultar em danos à rede da mesma.

5.5 Política para senhas

As instituições possuem senhas para vários tipos de acesso. Os mais comuns incluem: senhas de e-mail, intranet, proteção de tela, acesso à rede, etc. Para que estes sistemas não fiquem comprometidos, todos os colaboradores devem estar cientes da criação de senhas seguras.

Senhas são um aspecto importante da segurança computacional. Elas estão na linha de frente de proteção de sua conta. Uma senha mal escolhida pode resultar no comprometimento da rede da instituição. Diante disto, todos os colaboradores da instituição (incluindo parceiros e alunos que tenham acesso aos sistemas) são responsáveis por obedecer esta política de segurança.

5.6 Política para Virtual Private Network (VPN)

A proposta desta política é definir padrões a serem seguidos na utilização de acesso remoto via VPN para a rede da instituição, sendo esta utilizada por colaboradores ou parceiros.

5.7 Política para desenvolvimento de aplicações

Esta política tem como objetivo definir diretrizes básicas para que os sistemas desenvolvidos dentro ou fora desta instituição contenham níveis básicos de segurança, evitando que vulnerabilidades sejam inseridas na rede através destas aplicações.

6. Conclusões

De acordo com os objetivos estabelecidos no início do trabalho, a metodologia proposta mostrou-se um importante instrumento de padronização da segurança de rede em ambientes de instituições de ensino, sendo possível, a partir de sua aplicação, garantir que a segurança de rede seja efetiva e bem planejada.

A definição das regras de firewall para estes ambientes garantem que somente o tráfego explicitamente permitido será liberado, prevenindo a difusão sem limites de vírus que utilizam a rede para se propagar, utilizando portas não comuns.

No desenvolvimento deste trabalho foi possível notar que o mapeamento de todo o tráfego de uma rede não é uma tarefa tão simples quanto se pensava, pois podem existir tráfegos esporádicos que não eram esperados, mas que precisavam ser contemplados nas

regras de firewall e também nas políticas de segurança.

A definição da política de segurança é importante em qualquer instituição, porém, em ambientes de instituições de ensino são encontradas particularidades devido à variedade de públicos que freqüentam estas instituições. A implantação desta política é necessária para que as definições de segurança sejam conhecidas por todas as pessoas que utilizam os recursos de informática disponibilizados por estas instituições. Garantir que os acessos aos dados da organização sejam seguros, íntegros e confiáveis envolve também a conscientização das pessoas que utilizam estes recursos.

Certamente, a solução é considerada definitiva, mas não imutável, até porque as necessidades das redes mudam, as vulnerabilidades aumentam, e os níveis de segurança precisam ser revistos.