Universidade Federal do Rio de Janeiro

Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais

Humberto Ferreira Ramos Junior

Uma Arquitetura de Segurança de Redes Voltada ao Ambiente Corporativo

Rio de Janeiro

2016

Humberto Ferreira Ramos Junior

Uma Arquitetura de Segurança de Redes Voltada ao Ambiente Corporativo

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Claudio Miceli de Farias, D.Sc., UFRJ, Brasil

Rio de Janeiro

2016

Humberto Ferreira Ramos Junior

Uma Arquitetura de Segurança de Redes
Voltada ao Ambiente Corporativo

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2016.

Claudio Miceli de Farias, D.Sc., UFRJ, Brasil

Ao meu grande amor: Margareth, sempre ao meu lado. Fonte de pura inspiração.

AGRADECIMENTOS

Agradeço ao Sr. Antonio Carlos da Costa Pereira, uma das peças fundamentais na minha formação profissional e para a efetiva realização deste curso.

Agradeço também ao meu Orientador Prof. Claudio Miceli de Farias, amigo de longa caminhada. Obrigado pelo seu exemplo de correção de atitudes e pelos muitos ensinamentos que contribuíram sobremaneira para a realização deste trabalho.

Por fim, agradeço ao Prof. Moacyr Henrique Cruz de Azevedo pela maneira sábia e motivadora com a qual conduz suas atividades na coordenação do Programa MOT C.N. (Management of Technology in Computer Networks).

RESUMO

RAMOS JUNIOR, Humberto Ferreira. **Uma Arquitetura de Segurança de Redes Voltada ao Ambiente Corporativo**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2016.

Este trabalho descreve uma arquitetura de redes para ambientes corporativos cujo intuito é acelerar o processo de aprendizado de novos integrantes de uma equipe de segurança. Princípios fundamentais de funcionamento de dispositivos e serviços existentes são apresentados, além de importantes questões relacionadas à proteção da informação digital.

ABSTRACT

RAMOS JUNIOR, Humberto Ferreira. Uma Arquitetura de Segurança de Redes Voltada ao Ambiente Corporativo. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2016.

This paper describes a network architecture for enterprise environments which aims to accelerate the learning process for new members of a security team. Fundamental operating principles of devices and existing services are presented, as well as important issues related to protection of digital information.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ACL	*Access Control List*
AV	Antivírus
BD	Banco de Dados
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CSIRT	*Computer Security Incident Response Team*
DLP	*Data Loss Prevention*
DMZ	Zona Desmilitarizada (*DeMilitarized Zone*)
DDoS	*Distributed Denial of Service*
DoD	*Department of Defense*
DoS	*Denial of Service*
ET	Estação de Trabalho
HIPS	*Host Based Intrusion Prevention System*
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
IRC	*Internet Relay Chat*
MAC	*Media Access Control*
NIDS	*Network Based Intrusion Detection System*
NTP	*Network Time Protocol*
OSI	*Open systems interconection*
P2P	*Peer-to-Peer*
SD	Sistema Digital
SEM	*Security Event Management*
SID	Segurança da Informação Digital
SIEM	*Security Information and Event management*
SIM	*Security Information Management*
SSH	*Secure Shell*
TI	Tecnologia da Informação

SUMÁRIO

1 **INTRODUÇÃO**

Em redes de computadores, a área de segurança é responsável pelo provisionamento de políticas a serem adotadas no intuito de prevenir o uso e o acesso não autorizado a dados e recursos computacionais de uma organização. À medida que a Tecnologia da Informação (TI) avança, cresce também o número de ameças aos dados que trafegam ou são armazenados em uma rede.

Até recentemente, o único ponto de acesso à rede era um computador sobre uma mesa (*desktop*), mas com a popularização dos *notebooks*, *tablets* e *smartphones*, tornou-se comum o fato de um funcionário utilizar tais aparelhos e tentar conectá-los à sua rede local. Muitas das vezes, tal necessidade está intrinsecamente ligada à tentativa em aumentar sua produtividade, mas tal procedimento traz inúmeros riscos à segurança da rede da organização, deixando-a vulnerável à perda de dados ou infecção por códigos maliciosos.

Uma pesquisa divulgada pela Citrix (CITRIX SYSTEMS, 2012), empresa especializada em tecnologia móvel e de nuvem, revela que, até o ano de 2020, cada funcionário possuirá até seis aparelhos conectados à rede corporativa. Além disso, um terço dos trabalhadores da área de TI, estarão normalmente fora de seus escritórios tradicionais, gastando horas em outros locais, tais como hotéis e aeroportos, ou seja, trafegando informações da sua organização em redes públicas. Tal comportamento forçará as empresas a investirem cada vez mais em profissionais da área de segurança em redes em busca de soluções que protejam os dados de suas organizações.

Ao mesmo tempo, o número de incidentes em redes de computadores vem aumentando de maneira considerável nos últimos anos (CERT.BR, 2015a). Com isto, as instituições passaram a necessitar de equipes de TI cada vez mais capazes

a lutar contra eventos dessa natureza, impedindo que eles ocorram ou recebam tratamento rápido e adequado, quando inevitável.

De acordo com o **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil** (CERT.br), a figura abaixo apresenta o crescimento de incidentes em redes de computadores reportados à instituição.

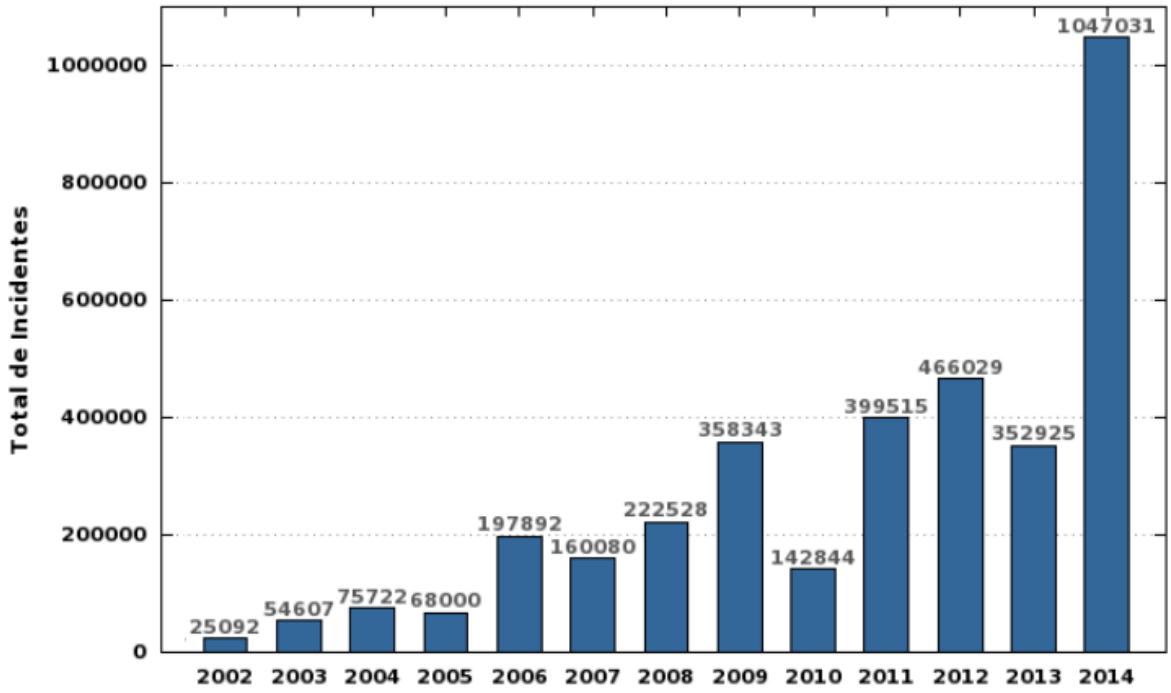

Figura 1.1 – Incidentes Reportados ao CERT.br - 2002 a 2014 (CERT.BR, 2015a).

Para chegarmos às categorias de ameças mais comuns existentes, levando-se em consideração as notificações enviadas ao CERT.br apenas no ano de 2014, poderíamos agrupar a maioria dos incidentes em redes nos seguintes tipos:

Worm: atividades relacionadas ao processo automatizado de propagação de códigos maliciosos na rede (CERT.BR, 2015b).

Negação de Serviço: atividade onde o atacante utiliza um computador (*Denial of Service - DoS*) ou um conjunto de computadores (*Distributed Denial of Service - DDoS*) no intuito de dificultar ou tornar inacessível uma rede ou serviço (CERT.BR, 2015b).

Invasão: ação maliciosa cujo objetivo é obter acesso não autorizado a um computador ou rede (CERT.BR, 2015b).

Web: ataque voltado especificamente ao comprometimento de servidores Web ou desfigurações de páginas na Internet (CERT.BR, 2015b).

Scan: varreduras realizadas em redes de computadores, no intuito de identificar máquinas e serviços ativos. É utilizado por atacantes para identificar potenciais alvos, pois permite associá-los a possíveis vulnerabilidades existentes (CERT.BR, 2015b).

Fraude: Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem do usuário da Internet (CERT.BR, 2015b).

A figura abaixo apresenta os percentuais de cada um dos tipos de ataques notificados ao CERT.br no ano de 2014 nas categorias acima descritas:

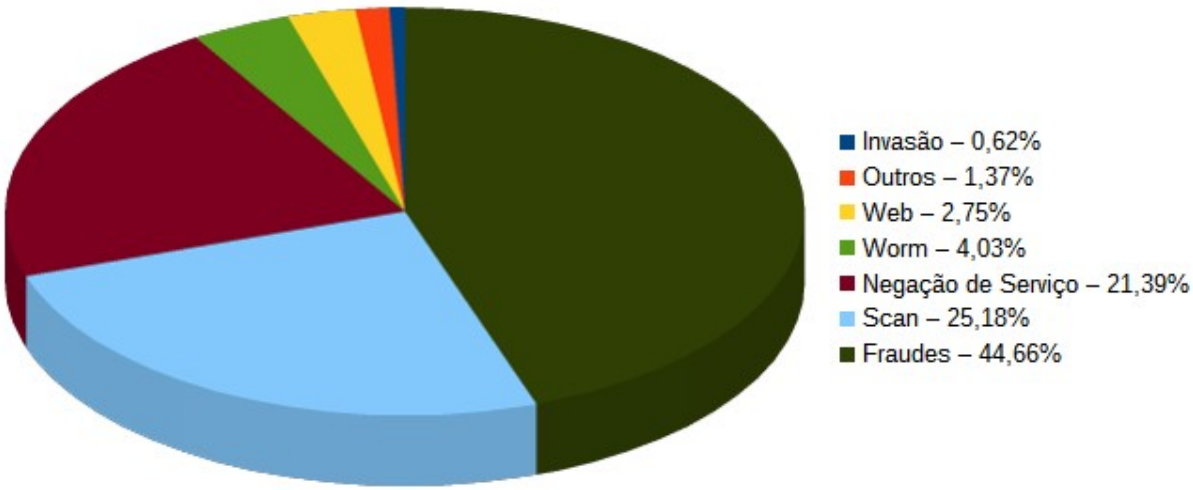

Figura 1.2 – Incidentes Reportados ao CERT.br em 2014 (CERT.BR, 2015b).

1.1 MOTIVAÇÃO

Desde o aparecimento do primeiro vírus, há uma constante evolução das técnicas empregadas por seus criadores no intuito de torná-los invisíveis aos programas antivírus voltados à proteção de computadores. As técnicas utilizadas evoluíram, partindo de métodos mais simples a estratégias bastante elaboradas e avançadas. Os profissionais de segurança necessitam estar atualizados no entendimento de como tais novas ameaças funcionam, entretanto é de suma importância analisar e compreender todos os métodos anteriormente utilizados, para que as ameaças vencidas no passado não retornem a ter êxito nos dias atuais (RAD *et al.*, 2011).

A formação de um profissional de segurança em redes tem como premissa fundamental a solidificação de conhecimentos básicos para que, a partir de um alicerce de competência em várias áreas, possa vislumbrar melhorias em ambientes corporativos que, em alguns casos, pode chegar a milhares de ativos computacionais conectados. O dia a dia do profissional de segurança varia de acordo com sua especialização, podendo atuar em duas áreas com focos distintos: forense computacional (análise de incidentes ocorridos) e analista de segurança (prevenção de incidentes).

O profissional de forense computacional deve possuir um amplo domínio das tecnologias utilizadas em seu ambiente corporativo, uma vez que exerce o papel de investigador, envolvendo-se, muitas das vezes, com a esfera jurídica e criminal no intuito de esclarecer situações onde membros de sua corporação pode estar envolvido. Nesta área, o objetivo é realizar a análise do incidente já ocorrido e verificar questões correlacionadas ao vazamento de informações, comprometimento dos ativos de redes e grau de envolvimentos dos usuários com o referido evento.

Por sua vez, o analista de segurança exerce um papel essencialmente técnico em sua organização. Podemos dizer, que o analista de segurança é a barreira a ser vencida pelo inimigo, pois atua na elaboração de estratégias, construção de políticas e implementação das tecnologias a serem adotadas em seu ambiente corporativo.

Ao analista, é atribuída a função de gerenciar políticas e ativos da área de segurança de redes, tais como: *Firewalls*, Sistemas de Detecção de Intrusos, Sistemas de Prevenção de Intrusos e *software* de Antivírus, além de diversas tarefas atinentes ao setor de Defesa Cibernética. Para isso, o analista deve compreender como toda a rede de sua organização trabalha e promover de maneira eficaz e eficiente a proteção de todo o fluxo de dados de sua instituição.

Para o correto gerenciamento das ferramentas de segurança, o analista tem a necessidade de conhecer o funcionamento de diversas aplicações e ativos de sua rede, inclusive quando gerenciados por outros setores, tais como: equipamentos de conectividades (*switches* e roteadores), *proxies* de acesso à Internet, servidores Web, acesso a Bancos de Dados (BD), soluções de segurança de e-mail, árvore de diretórios, sistemas operacionais, dentre outros. Esse conhecimento amplo é desejável, uma vez que a segurança deve ser proporcionada não só a um setor específico, mas a toda organização.

Em algumas instituições, como por exemplo: as Forças Armadas, a rotatividade de pessoal pode ser um empecilho para que o indivíduo alcance a maturidade e o conhecimento necessário para o pleno desempenho na área de Segurança de Redes. Em virtude do plano de carreira, pode haver mudanças no pessoal quase todos os anos e, com isso, sempre haverá a necessidade de treinamento para os novos integrantes dessa equipe.

1.2 JUSTIFICATIVA

Nas ocasiões onde há mudança de pessoal, a curva de aprendizado e o crescimento da equipe do setor de segurança é afetada basicamente de três maneiras:

1 – Perdas do conhecimento e da mão de obra qualificada do membro que deixou a equipe;

2 – Tempo gasto por um dos membros remanescentes na equipe no treinamento do novo integrante que, por ser advindo de uma Instituição de Ensino ou Centro de Formação, não possui o conhecimento dos ativos de segurança e da arquitetura de rede existente na organização; e

3 – Tempo que o novo integrante levará a atingir um nível de conhecimento semelhante ao do membro que anteriormente deixou a equipe.

Levando-se em consideração que muitos dos conhecimentos de redes já estão consolidados e que as tecnologias empregadas em uma instituição normalmente não sofrem alterações frequentes, uma publicação que concentre a base de conhecimento de todas as tecnologias empregadas em um ambiente corporativo aceleraria o aprendizado de cada novo integrante que venha a compor a equipe de segurança.

1.3 OBJETIVO

O intuito primordial desta obra é acelerar o processo de aprendizado de fundamentos básicos e necessários a novos integrantes de uma equipe de analistas de segurança. Para isso, é apresentada uma arquitetura de rede voltada a ambientes corporativos com a devida descrição do princípio de funcionamento das ferramentas e serviços existentes, tendo sempre como foco a proteção da Informação digital.

1.4 RESULTADOS ESPERADOS

Como resultado esperado deste trabalho, objetivamos reduzir o tempo médio de treinamento gasto com novos profissionais de segurança, uma vez que o período necessário para que se atinja o nível de conhecimento desejável está diretamente ligado à sua fase de inicial de treinamento.

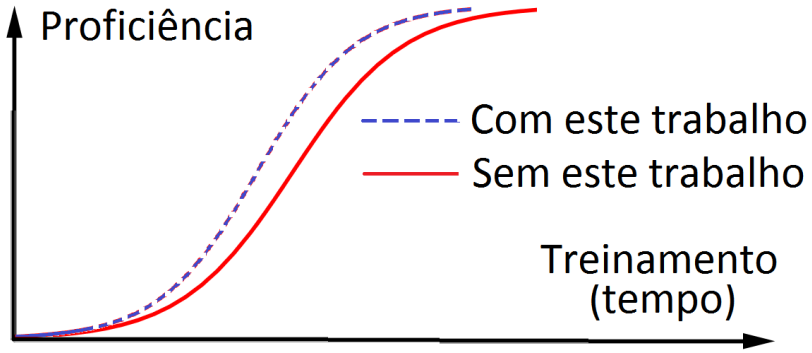

Figura 1.3 – Proficiência x Treinamento (tempo).

Além de acelerar a curva de aprendizagem de novos profissionais, esta obra passará a ser uma fonte de consulta para membros de outras áreas no intuito de que adquiram conhecimentos básicos sobre as ferramentas administradas pelo setor de segurança. Este conhecimento é importante e válido em situações onde a resolução de problemas relacionados à indisponibilidade momentânea de serviços (*troubleshooting*) envolvam outros setores.

Outro ganho substancial está no aumento da produtividade da organização. Na maioria das vezes, quando um novo dispositivo (ou tecnologia) passará a ser empregado, membros de diferentes setores reúnem-se no intuito de haver uma explanação de como os mecanismos de segurança comportar-se-ão em relação ao tráfego gerado pelo novo dispositivo. Em certos casos, uma consulta prévia a um documento interno que contenha a descrição de como os dispositivos de segurança são configurados e operacionalizados eliminaria a necessidade de uma reunião.

1.5 ORGANIZAÇÃO DO TRABALHO

O trabalho está organizado da seguinte forma:

O segundo capítulo exibe uma visão sobre espaço cibernético, suas ameaças inerentes e ataques na Internet. Apresenta os principais perigos à navegação na rede mundial de computadores e fomenta a necessidade de haver uma preocupação com a segurança da informação digital (SID).

O terceiro capítulo apresenta conceitos básicos sobre arquitetura de redes, ativos de conectividade, ferramentas de segurança e serviços corporativos voltados à SID, sendo subdividido em 3 seções:

→ A primeira seção apresenta um conjunto de sub-redes que compõem a arquitetura proposta neste trabalho, essencialmente divididas pela concepção de funcionamento de cada uma delas.

→ A segunda seção apresenta os ativos e ferramentas de rede existentes, levando em consideração: suas características, princípios de funcionamento e boas práticas de segurança.

→ A terceira seção apresenta os serviços corporativos capazes de prover uma segurança ativa e, além disso, contribuir para a identificação e rastreabilidade de ações maliciosas na rede.

O quarto capítulo propõe um modelo de arquitetura de redes para um ambiente corporativo, cujo arranjo das sub-redes existentes e posicionamento dos ativos e ferramentas utilizados têm o objetivo de prover uma defesa em profundidade a ataques originados na Internet. São adotas boas práticas na estruturação da rede, expondo, de uma maneira didática, os conceitos empregados, no intuito de facilitar a leitura para iniciantes na área de segurança da informação.

Por fim, o quinto capítulo apresenta as considerações finais sobre o trabalho.

2 O ESPAÇO CIBERNÉTICO E SUAS AMEAÇAS

Atualmente muitos confundem o conceito de cyberespaço ou espaço cibernético com a própria definição de Internet. Entretanto, Tanenbaum e Wetherall (2013) definem a Internet como uma vasta coleção de diferente redes que usam certos protocolos e fornecem determinados serviços comuns. É um sistema incomum, pois não foi planejado e nem é controlado por um único grupo de pessoas cooperando entre si, ou seja, cada um faz a sua parte e a rede assim funciona.

Quanto ao espaço cibernético, o Departamento de Defesa dos Estados Unidos (*Department of Defense - DoD*) o define como um domínio global dentro do ambiente de informação. Consiste na rede interdependente de infraestruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicações, sistemas de computador e processadores embutidos e controladores. No espaço cibernético, tanto a eletrônica quanto o espectro eletromagnético são utilizados para armazenar, modificar e trocar dados de diferentes de sistemas de rede (ANDRESS e WINTERFELD, 2013).

Em comum, ambas as definições acima envolvem uma enorme quantidade de usuários, computadores, sistemas e equipamentos de conectividade interligados entre si trocando dados dos mais variados tipos possíveis. Além do simples envio de mensagens de um ponto a outro da rede, é necessário prover uma comunicação segura e confiável, pois muitos dos dados contém informações particulares e sigilosas.

À medida que aumentam as capacidades de armazenamento, processamento e a banda disponível na Internet, aumentam também o número de ameças na rede que podem afetar nossos dados. A seguir, são apresentados várias ameças ao

espaço cibernético, cujas definições e informações adicionais podem ser encontradas na "*Cartilha de Segurança para a Internet"* do CERT.br.

2.1 *Malwares*

São programas desenvolvidos especificamente para executarem atividades maliciosas em um computador (CERT.BR, 2015c). Uma máquina pode ser infectada de várias formas:

- Ao executar um arquivo gravado em dispositivos removíveis de armazenamento em massa, tal como *pen-drives* e HD externos;
- Ao acessar um *link* ou executar um arquivo infectado anexado a uma mensagem de correio eletrônico;
- No acesso a conteúdo malicioso hospedado em *Websites*; e
- Por meio de ações específicas conduzidas por indivíduos que visam invadir e instalar programas dessa natureza em um computador.

Por meio de um *malware* instalado, um atacante pode realizar ações que vão desde simplesmente obter cópias de informações e arquivos existentes até o efetivo controle total da máquina. Com isso, pode haver prejuízos financeiros pela coleta indevida de dados sigilosos, além da possibilidade do computador ser utilizado por um atacante como origem para outros golpes e atividades maliciosas na Internet.

Dentre os *malwares* existentes, podem ser citados os seguintes tipos: Vírus, *Worm*, *Bot*, *Spyware*, *Backdoor*, Cavalo de troia (*Trojan*) e *Rootkit*.

2.1.1 Vírus

Código que se instala em um sistema computacional alterando programas existentes e em alguns casos, de maneira semelhante ao que acontece na biologia, faz cópias de si mesmo e busca a propagação pela rede (CERT.BR, 2015c). Entretanto, para que um vírus haja efetivamente em um computador, é necessária a execução do programa infectado por parte do usuário.

2.1.2 *Worm*

Diferente do vírus, para sua ação, o *worm* não necessita de uma ação prévia do usuário. Este tipo de código malicioso não apenas infecta outros programas, mas envia cópias de si mesmo para outras máquinas e busca por vulnerabilidades em *softwares* instalados (CERT.BR, 2015c).

Dentre algumas ações possíveis e no intuito de continuar sua propagação, após a infecção de uma máquina, um *worm* pode executar uma das seguintes tarefas: (i) varrer a rede em busca de outros alvos; (ii) buscar uma lista de endereços de e-mails e utilizá-la para o envio de anexos infectados; e (iii) esperar uma conexão e encaminhar uma cópia sua para a origem desta comunicação.

2.1.3 *Bot* (*Botnet*)

O *Bot* é um tipo de *malware* que permite o controle remoto de um computador por um invasor. A máquina infectada poderá ser utilizada na captura de dados de contas e senhas de seus usuários, realizar ações pré-agendadas ou receber tarefas maliciosas via canais de IRC (*Internet Relay Chat*) e redes P2P *(peer-to-peer)*, por exemplo (CERT.BR, 2015c).

Um computador infectado por um *bot,* normalmente denominado de *zumbi,* passar a ser um vetor de ataque poderoso, pois um indivíduo pode obter o controle de um conjunto de máquinas para a realização de atividades maliciosas coordenas. Esta rede formada por um aglomerado de zumbis é denominada de *Botnet*.

Uma ação muito comum é a utilização de *Botnets* para ataque de *DDoS*, onde milhares de máquinas realizam acessos simultâneos a um sítio de Internet, sobrecarregando-o e deixando-o inacessível.

2.1.4 *Spyware*

Os *Spywares* ou programas espiões visam coletar informações das atividades desempenhadas por usuários de um sistema e enviá-las a terceiros. Como exemplos dentro desta categoria, podemos citar o *Keylogger e o Screenlogger* (CERT.BR, 2015c). O primeiro tem a tarefa de gravar a sequência das teclas digitadas pelos usuários, enquanto o segundo é capaz de capturar a tela e a posição do *mouse* no momento do “clique” do usuário. Devido a este comportamento, o *Screenlogger* pode ser utilizado na captura de senhas de *Internet Banking* em teclados virtuais, por exemplo.

2.1.5 Cavalo de Troia

O Cavalo de troia, ou *trojan*, é um programa aparentemente legítimo com linhas de código que executam tarefas maléficas desconhecidas pelo usuário. Em alguns casos, os *trojans* alteram outros programas previamente instalados que, além de suas atividades legítimas, passarão a desempenhar ações maliciosos (CERT.BR, 2015c).

2.1.6 *Backdoor*

Os *Backdoors* são programas que tornam um computador acessível remotamente sem a devida permissão do usuário. Este acesso indevido pode ser realizado por meio da ação de códigos maliciosos ou devido a vulnerabilidades existentes em *softwares* instalados. Programas de administração remota, tais como *Radmin, SubSeven, VNC*, dentre outros, quando mal configurados, podem ser considerados como *backdoors* (CERT.BR, 2015c).

2.1.7 *Rootkit*

O *Rootkit* é um conjunto de técnicas e programas desenvolvidos especificamente para garantir, de maneira imperceptível ao usuário ou até mesmo a *softwares* de antivírus, a presença de um invasor em um computador (CERT.BR, 2015c). Embora uma máquina infectada não possua informações valiosas, poderá ser utilizada como vetor para outras ações, tais como ataques do tipo *DDoS* ou envio de e-mails maliciosos (*phishing*).

2.2 ATAQUES NA INTERNET

Os ataques na Internet ocorrem por diferentes motivações, normalmente relacionadas a busca por prestígio e motivações de cunho ideológico, financeiro ou comercial. Na busca por prestígio, atacantes buscam realizar atividades que propiciem notoriedade na Internet. Para isso, tentam invadir sites em ações de desconfiguração de páginas (*defacement*), substituindo a página inicial pela marca registrada do próprio atacante ou grupo ao qual pertence. Além disso, podem

também tornar serviços inacessíveis e reclamar a autoria de tal feito (CERT.BR, 2015d).

Nas ações de motivação ideológicas, normalmente estão presentes ações direcionadas a sites que possuem opinião oposta à do grupo atacante. São publicadas mensagens de apoio à causa defendida e contrárias à ideologia pregada na página desconfigurada.

Nas motivações de cunho financeiro, informações confidenciais são capturadas para posterior realização de compras na Internet. Outra ação possível é o roubo de dados sigilosos e a posterior chantagem pelo seu resgate.

Como motivação comercial, grupos *hackers* podem ser contratados no intuito de realizarem ataques a uma empresa concorrente, desconfigurando sua página inicial ou tornando o serviço inacessível, diminuindo seu crédito perante a sociedade. A partir de agora, abordaremos várias técnicas que podem ser empregadas por um atacante.

2.2.1 Varreduras

A varredura consiste em analisar uma rede em busca de ativos e computadores com serviços e programas acessíveis e vulneráveis. Tais informações podem ser posteriormente utilizadas como portais de entrada por um atacante (CERT.BR, 2015d).

Abaixo, é apresentada a saída de um dos mais famosos softwares de varredura, o *Nmap*. Em uma análise do hipotético sítio *www.x3map.com*, foram encontrados dois serviços ativos: o *ssh* (porta 22/TCP) e o *http* (porta 80/TCP).

```
# nmap  www.x3map.com

Starting Nmap 6.25 ( http://www.x3map.com ) at 2015-08-27 11:50 E. South America Standard Time

Nmap scan report for www.x3map.com  (45.33.32.156)

Host is up (0.16s latency).

Not shown: 995 closed ports

PORT        STATE        SERVICE

22/tcp      open         ssh

80/tcp      open         http

Nmap done: 1 IP address (1 host up) scanned in 5.79 seconds
```

2.2.2 Falsificação de e-mail

A Falsificação de e-mail, ou *e-mail spoofing*, consiste no envio de mensagens de correio eletrotônico que induzem seu destinatário a acreditar que o remetente da mensagem é legítimo. Aproveitando uma característica do protocolo SMTP (*Simple Mail Transfer Protocol*), um atacante consegue falsificar o campo "*From*:" (endereço de origem) no e-mail enviado a uma vítima (CERT.BR, 2015d).

Infelizmente, há vários sítios na Internet onde é possível fabricar estas mensagens de correio falsas e enviá-las com *hiperlinks* redirecionando o destinatário a páginas com conteúdo malicioso ou anexar um arquivo infectado ao e-mail.

Exemplos de falsificação de e-mail são mensagens recebidas solicitando que o usuário acesse um *link*, preencha dados sigilosos ou execute um arquivo anexo.

Os endereços forjados de origem, normalmente, são de pessoas conhecidas, do seu banco ou de serviços na Internet onde o indivíduo possui cadastro.

2.2.3 Interceptação de tráfego

A Interceptação de tráfego, ou *sniffing*, consiste em capturar dados que passam pela rede para posterior análise. A captura é feita com o uso de programas específicos, denominados *sniffers* (CERT.BR, 2015d). Alguns protocolos, tais como o *telnet* e o *ftp* são inseguros, pois trafegam seus dados de usuários e senhas em "modo claro" e os *sniffers* possuem processos automatizados que facilitam sua captura e exibição.

2.2.4 Força bruta (*Brute force*)

O ataque de força bruta, ou *brute force*, consiste em realizar repetitivas tentativas de acerto de usuário e senha de serviços na Internet ou ativos de rede, tais como *switches* e roteadores. Caso o atacante consiga descobrir um usuário e sua respectiva senha, ações poderão ser realizadas em seu nome (CERT.BR, 2015d).

Existem várias ferramentas disponíveis na Internet com uma série de dicionários já padronizados para o emprego de força bruta, o que facilita seu uso. Dentre várias ações possíveis, contas de correio podem ser invadidas e utilizadas para o envio de e-mails falsos, perfis de redes sociais podem ser utilizados para a distribuição de *links* maliciosos e roteadores podem ser comprometidos e suas tabelas de roteamento alteradas. Um ataque de força bruta pode deixar um serviço lento ou até mesmo indisponível, devido ao grande número de requisições feitas em um curto espaço de tempo.

2.2.5 Desfiguração (*Defacement)*

A Desfiguração, ou *defacement*, consiste em alterar o conteúdo legítimo de uma página na Internet. Normalmente, os atacantes visam ganhar notoriedade ou disseminar uma ideologia oposta à pregada pelo sítio alvo das ações. Para o sucesso do ataque, podem ser exploradas falhas na aplicação, vulnerabilidades existentes no SO devido a falta de atualizações ou erros de programação (CERT.BR, 2015d).

2.2.6 Negação de serviço (*DoS* e *DDoS*)

A negação de serviço, ou *Denial of Service* (DoS), tem o objetivo de causar uma sobrecarga em um servidor ou computador no intuito de tornar indisponível o acesso por outros utilizadores (CERT.BR, 2015d). No DoS, a partir de um computador, o atacante envia inúmeras requisições ao alvo de tal modo que esta máquina não consiga responder a solicitações lícitas de outros usuários. Quando este ataque é realizado de maneira organizada e com o emprego de várias máquinas, tal ação é denominada negação de serviço distribuída ou DDoS (*Distributed Denial of Service*).

Existem várias ferramentas que podem ser utilizadas para a realização destes ataques. Uma tática empregada é a infecção de vários computadores por *bots* (ver subseção 2.1.3), tornando-os zumbis e utilizando-os de maneira involuntária por parte de seus proprietários, formando uma *Botnet*.

2.2.7 *Phishing*

O *Phishing* é uma técnica onde o atacante visa obter dados pessoais ou financeiros para posterior obtenção de vantagens. Normalmente, ocorre por meio de mensagens de correio eletrônico onde o remetente tenta ludibriar o destinatário simulando comunicações enviadas de sites amplamente conhecidos, instituições financeiras ou órgão públicos, induzindo-o a fornecer informações particulares (CERT.BR, 2015e).

Dentre as táticas utilizadas, destacam-se a elaboração de: (i) *e-mails* de *Internet Bankig e* comércio eletrônico; (ii) *links* direcionados a páginas falsas onde serão solicitados dados de cartões de créditos e informações particulares; (iii) convites falsos para redes sociais; (iv) *e-mails* com *links* para *downloads* de arquivos maliciosos; e (v) *e-mails* falsos relacionados a promoções de grande repercussão na atualidade.

2.2.8 *Sql Injection*

A injeção de SQL ou *Sql Injection* é uma ação maliciosa voltada a aplicações Web onde o atacante envia comandos em SQL (*Structured Query Language*) para um campo de entrada existente no sítio a fim de obter acesso a dados cadastrados no banco de dados (KINDY e PATHAN, 2011). Podem ser utilizados comandos de manipulação de dados (*select, insert, update, delete*) ou comandos de definição de dados (*create, drop, alter*).

Para exemplificar tal técnica, imaginemos que um sítio possua dois campos de autenticação a serem preenchidos: campo_1 (*login*) e campo_2 (*senha*). A

fragilidade ocorre quando a aplicação está programada para validar internamente seus usuários com a seguinte instrução:

```
SELECT * FROM tabela_usuarios WHERE login = 'campo_1' AND senha = 'campo_2'
```

A instrução acima realiza uma busca no banco de dados (BD) para usuários digitados no campo ***login*** e sua respectiva ***senha***. Entretanto, caso um atacante insira no campo_1 os caracteres (123) e no campo_2 os caracteres (' or '1' = '1'), o resultado seria a seguinte expressão:

```
SELECT * FROM tabela_usuarios WHERE login = '123' AND senha = ' ' or '1' = '1'
```

Neste caso, em função do valor do campo_2, a condição acima será sempre verdadeira (**'1' = '1'**) e o acesso à aplicação será permitido, independente do usuário informado.

2.2.9 *Cross-site Scripting* (XSS)

O *Cross-site Scripting*, também conhecido como XSS ou CSS, permite ao invasor executar um *script* dinâmico no contexto da aplicação (BELARMINO e ARAÚJO, 2015). As falhas que possibilitam o XSS podem ocorrer quando a aplicação gera uma saída, a partir de dados fornecidos pelo usuário em uma página de entrada e essas informações são processados sem nenhum tipo de validação.

Falhas existentes em aplicações Web, com a utilização do XSS, podem levar a ações relacionadas ao roubo de sessões de usuários, desconfiguração de sítios, execução de códigos arbitrários na máquina do usuário e redirecionamento de navegadores para sites maliciosos, dentre outras (DE CARVALHO *et al.*, 2013).

2.3 CONCLUSÃO

O espaço cibernético trouxe inúmeros benefícios à sociedade, facilitando a troca de informações e conhecimentos entre indivíduos e organizações. Surgiram novas modalidades de comércio eletrônico e educação que contribuem com a economia e desenvolvimento da sociedade. Entretanto, ao mesmo passo desses avanços conseguidos, apareceram ameaças à navegação segura na Internet.

Instituições e organizações, no intuito de protegerem seus segredos econômicos e militares, realizaram estudos e criaram uma demanda de equipamentos e técnicas de proteção a seus negócios. Em virtude disso, o próximo capítulo apresenta um conjunto de definições sobre redes de computadores, ativos e equipamentos utilizados em conectividade e segurança, além de boas práticas de como empregá-los em prol da SID.

3 AS REDES, OS ATIVOS E OS SERVIÇOS CORPORATIVOS DE SEGURANÇA

Neste capítulo, há uma série de fundamentos que servirão de base para o entendimento da arquitetura de rede proposta neste trabalho. São apresentadas as sub-redes sugeridas para uma organização, boas práticas e funcionalidades presentes nos equipamento de conectividade e segurança. Além disso, conceitos sobre padronizações e serviços necessários na área de TI são abordados, a fim de proporcionar uma visão geral sobre o funcionamento de um ambiente corporativo.

3.1 AS REDES

Basicamente, um ambiente computacional de redes pode ser é dividido em três zonas: (i) a rede externa: Internet; (ii) a rede interna: Intranet; e (iiii) a zona desmilitarizada: DMZ (*Demilitarized Zone*) (BRUCKER *et al.*, 2015). Estas regiões estão representadas na Figura 3.1. É interessante que a rede interna possua duas sub-redes denominadas *Rede de Homologação* e *Rede de Serviços*. Cada uma destas redes será conceitualmente apresentada nas próximas subseções.

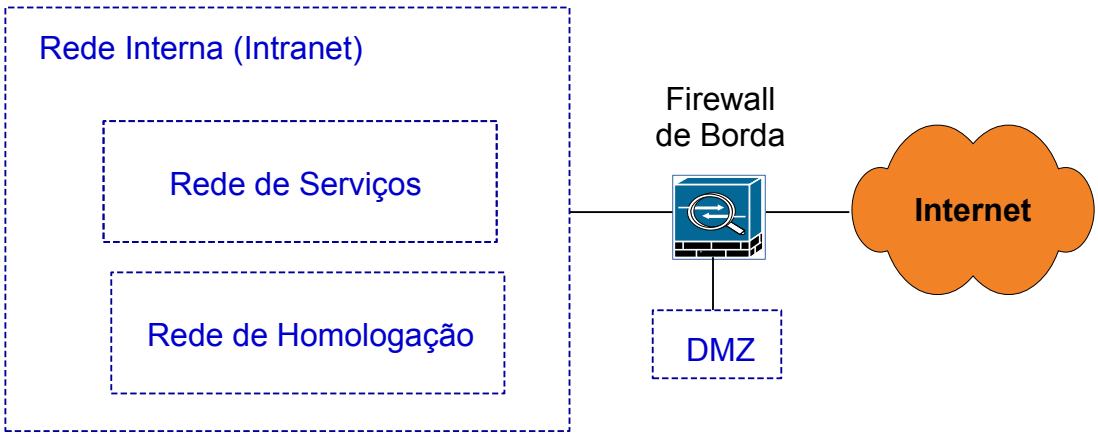

Figura 3.1 – Redes Organizacionais.

3.1.1 A Internet

É o ambiente de rede exterior à organização. É tudo aquilo que está além do *firewall* de borda (BRUCKER *et al.*, 2015). Às máquinas e ativos de rede presentes neste ambiente são identificadas por endereços IPv4 (normalmente) ou IPv6 públicos. Estes endereços, que são roteáveis na Internet, são gerenciados por uma entidade reguladora denominada *Internet Assigned Number Authority* (IANA).

3.1.2 A Rede Interna (Intranet)

É o ambiente de rede interior à organização. É nesta área que estão localizados os usuários, as estações de trabalho, servidores internos e as informações mais valiosas de todo o ambiente organizacional (BRUCKER *et al.*, 2015).

Atualmente, as máquinas situadas na Rede Interna são identificadas normalmente por endereços IPv4 privados (não roteáveis na Internet) e, via de regra, não podem ser acessados a partir da Internet. Para os endereços privados que excepcionalmente necessitam ter acesso a partir da Internet, normalmente situados em uma DMZ, é utilizado um mecanismos presentes em roteadores e *firewalls* denominado *Network Address Translation* (NAT), cuja função é traduzir um endereço privado para um endereço público. Os endereços privados são:

- 10.0.0.0 a 10.255.255.255 (10.0.0.0 / 8);
- 172.16.0.0 a 172.31.255.255 (172.16.0.0 / 12); e
- 192.168.0.0 a 192.168.255.255 (192.168.0.0 / 16).

Na Rede Interna, ainda podem coexistir duas sub-redes com funções específicas para uma organização: a Rede de Serviços e a Rede de Homologação.

3.1.2.1 A Rede de Serviços

Esta rede tem o propósito de hospedar serviços e aplicações que serão utilizados pelos usuários da organização. Neste ambiente podem ser inseridos, por exemplo, páginas Web para uso apenas da Intranet, os *Proxies, os Domain Name System (DNS)* internos, sistemas de monitoramento de ativos e serviços, servidores de Antivírus corporativo, concentradores e analisadores de registros de eventos (*Security Information and Event Management – SIEM*), dentre outros.

Dependendo do porte da organização, alguns servidores localizados na Rede de Serviços, tais como os que hospedam serviços da área de segurança, podem ter seu acesso limitado a certos usuários. Tal restrição pode ser conseguida com a utilização de um *firewall* ou roteador na entrada da rede, por meio da implementação de listas de controle de acesso (*Access Control List* - ACL).

3.1.2.2 A Rede de Homologação

Antes de um SD ser efetivamente colocado em produção, logo após sua aquisição ou desenvolvimento, deve ser iniciada a atividade de Homologação. A partir da documentação e especificações técnicas do SD, são estabelecidos requisitos mínimos de segurança a serem atingidos.

A avaliação técnica (homologação) do SD é realizada em uma sub-rede, logicamente segregada da rede local, denominada Rede de Homologação. Neste ambiente são realizadas varreduras no sistema, com ferramentas automatizadas, em busca de possíveis vulnerabilidades que poderiam ser exploradas por atacantes. Além disso, em função do sigilo das informações a serem armazenadas no SD, testes de penetração também podem ser realizados a fim de avaliar sua robustez a possíveis ataques *hackers* provenientes da internet.

Após as verificações acima descritas e correções das vulnerabilidades encontradas, o sistema está apto a entrar em produção e será hospedado: (i) na Rede de Serviços, caso seja disponibilizado apenas para a Intranet; ou (ii) na DMZ, caso o acesso passe a ser efetuado a partir da Internet.

3.1.3 A Zona Desmilitarizada (DMZ)

A DMZ surgiu com a ideia de trazer uma camada a mais de proteção para a rede de uma organização. Observando a Figura 3.2, é possível hospedar um servidor Web na DMZ com acessos simultâneos a partir da rede Interna e da Internet (BRUCKER *et al.*, 2015). É importante salientar que máquinas hospedadas na DMZ devem apenas responder a requisições originadas a partir de máquinas localizadas na Rede Interna, ou seja, o acesso à Rede Interna é restrito. Uma prática adotada é a utilização de vários *firewalls* em linha, para dificultar as chances de sucesso de um ataque a partir da Internet.

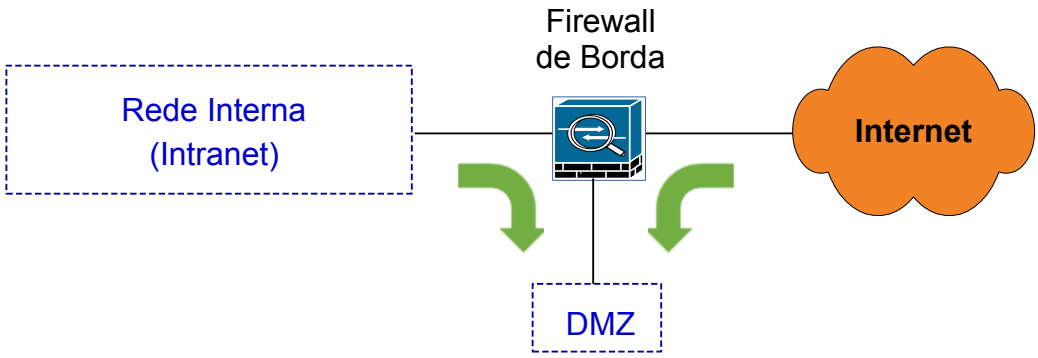

Figura 3.2 – Permissões de Fluxo de Dados.

A partir do *firewall* apresentado na Figura 3.2, as suas *interfaces* podem ser convencionadas da seguinte maneira:

- *Interface Inside*: ligada à Rede Interna;
- *Interface Outside*: ligada à Internet; e
- *Interface DMZ*: ligada à Rede DMZ.

As liberações de acesso à DMZ são realizadas no *firewall* de borda, normalmente em função dos endereços IP de origem e destino e das portas lógicas utilizadas pelo serviço.

Com relação à DMZ e regras de acesso envolvendo o *firewall* de borda, podemos destacar as seguintes orientações:

- Os servidores hospedados na DMZ e disponíveis para a Internet, antes de entrar em produção, devem passar por uma varredura de segurança em busca de vulnerabilidades que poderiam ser exploradas por atacantes;
- Os servidores hospedados na DMZ e disponíveis para a Internet devem ser rotineiramente atualizados, minimizando as chances de que vulnerabilidades descobertas sejam exploradas por atacantes;
- Deve haver regras nos *firewalls* de borda bloqueando o acesso direto (*sem Proxy*) de qualquer usuário interno à Internet. O acesso à Internet deve ser realizado por meio de um servidor *Proxy*, onde é possível criar um registro de navegação (*login*, endereço IP de origem, portas utilizadas, horário e páginas consultadas); e
- As regras existentes nos *firewalls* de borda devem ser rotineiramente auditadas. O objetivo é encontrar possíveis falhas de configuração que facilitem a um atacante invadir um servidor ou ter acesso à rede interna a partir da Internet.

3.2 OS ATIVOS DE REDE

Esta seção visa apresentar informações sobre os equipamentos de conectividade (*Switches* L2, *Switches* L3 e Roteadores) e os seguintes dispositivos

de segurança (*Firewalls*, Sistema de Detecção de Intrusos, Sistema de Prevenção de Intrusos, *Firewall* de Aplicação Web e *Security Information and Event Management*). A característica destes ativos é a de que suas regras de funcionamento e análise de registro de eventos (*logs*) são gerenciados normalmente por analistas de segurança.

3.2.1 *Switches* L2

Os *Switches* (Layer 2) são elementos capazes de comutar o tráfego de camada de enlace em uma LAN (*Local Area Networks*). Basicamente, o *switch L2* recebe um quadro e, em função do endereço MAC (endereço físico) de destino contido em seu cabeçalho, o envia para uma porta de saída (KUROSE e ROSS, 2013a).

A porta de saída do *switch* L2 é descoberta após uma busca em sua tabela MAC (*MAC Address Table*). À medida que quadros trafegam na rede, endereços MAC são armazenados nesta tabela. Quando o comutador não conhece a porta de saída, é enviada uma mensagem para todas as suas interfaces no intuito de descobrir em qual delas está localizada a máquina de destino.

No tocante a estes dispositivos, seguem algumas orientações de segurança (CSIRT-UNICAMP, 2015):

- Manter *backup* dos dispositivos de rede: uma considerável ajuda na recuperação em caso de desastres ou substituição dos equipamentos. Também serve como uma base de consulta com o histórico das mudanças de configurações;
- Sincronismo: É fundamental a sincronia de todos os equipamentos da rede com um servidor *NTP* (*Network Time Protocol*), para que nas

auditorias e análise de registros, os eventos possam ser corretamente correlacionados;

- Manter um armazenamento remoto dos registros de eventos *(logs):* permite o recebimento de alarmes e efetivamente analisar o que está ocorrendo com seu dispositivo;
- Desabilitar serviços desnecessários: verificar quais vem habilitados na configuração padrão e identificar quais não serão utilizados;
- Monitoramento: o SNMP (*Simple Network Management Protocol*) é um protocolo da camada de aplicação utilizado na gerência de dispositivos em rede com informações sobre vários parâmetros, tais como: estados de interfaces, processamento e memória. Deve ser empregado em sua última versão (atualmente SNMP v3). Além disso, devem ser desabilitadas as contas *default (snmp community public* e *snmp community private)* e configuradas novas contas;
- Gerenciamento: desabilitar as mudanças de configurações via protocolo *telnet*, pois as informações de usuário e senha trafegariam "em claro" na rede. Habilitar o SSH (*Secure Shell*) para tal fim. É recomendável também desabilitar o acesso Web. Além disso, devem ser desabilitadas as contas *default (admin, administrador)* e configurar novas contas;
- Endereçamento IP: É recomendável criar uma VLAN específica de gerência com endereçamento diferente dos utilizados na rede local; e
- Segurança Física: Não deixar o equipamento ao alcance de todos e desabilitar administrativamente as portas não utilizadas. Configurar senha de autenticação na porta *console* (porta de gerência local).

Algumas tecnologias permitem a utilização do *Port Security,* este recurso viabiliza um maior controle dos dispositivos que se conectam à rede local, pois o *switch* apenas encaminhará dados de endereços MAC registrados no equipamento. Os endereços MAC podem ser registrados de forma manual ou automática. Neste último caso, catalogando os equipamentos ligados à rede no momento de sua inicialização (CISCO, 2015).

3.2.2 Roteadores e *Switches* L3

Os Roteadores são dispositivos de camada de rede que encaminham pacotes em função de um endereço IP de destino (KUROSE e ROSS, 2013b). Para desempenhar funções de roteadores, também podem ser utilizados os *switches L3* que também encaminham pacotes em função do endereço de camada 3. Normalmente, os *switches L3* possuem hardware otimizado, sendo capazes de enviar dados mais rapidamente.

O mecanismo de roteamento presente nestes dispositivos de camada 3 segue um conjunto de regras que definem como dados devem trafegar entre sub-redes. Basicamente, dados são recebidos em uma interface e, em função de uma tabela de roteamento, são encaminhados para outra interface. Os modos de roteamento utilizados pode ser: o estático, o dinâmico e o *default* (FILIPPETTI, 2008).

No modo estático, as rotas de encaminhamento são configuradas pelo administrador da rede. Vantagens: redução no uso da CPU e ganho na segurança, pois o administrador controla o roteamento de pacotes. Desvantagem: O administrador deve conhecer detalhadamente toda a rede para inclusão e exclusão de cada rede, quando necessário (inviável para grandes redes).

No modo dinâmico, são utilizados protocolos de roteamento na distribuição das sub-redes existentes. Vantagem: Facilita o gerenciamento da rede, principalmente nas de grande porte. Desvantagens: Utiliza largura de banda dos *links* e aumenta o processamento da CPU.

O roteamento *default* é utilizado no encaminhamento de pacotes para redes que não estão presentes em sua tabela de roteamento. Por padrão, quando um pacote é destinado a uma rede que o roteador não conhece, ele o descarta. As rotas *default* são empregadas para que um pacote não seja simplesmente descartado, encaminhando-o para uma interface específica de saída. Por exemplo, a rota *default* poder ser configurada como a saída da rede para a Internet.

No caso da camada de rede, onde estão os roteadores, o controle do tráfego na rede pode ser implementado por meio de listas de controle de acesso (*Access Control Lists – ACL*). Uma ACL é uma lista com instruções de permissão ou negação com base em endereços e protocolos de camadas superiores. Na decisão a ser tomada pelo roteador para encaminhamento ou não de um pacote de dados, podem ser levadas em consideração os endereços IP de origem e destino e as portas lógicas utilizadas pelas aplicações (JUNG e PELLIS, 2013).

As precauções de segurança para os roteadores e *switches* L3 são semelhantes às adotadas para os *Switches* L2 (subseção 3.2.1).

3.2.3 *Firewalls*

O *Firewall* é uma solução baseada em hardware ou software cuja função é permitir ou negar o trafego de rede a partir de um conjunto de regras de segurança estabelecidas pelo seu administrador. É uma ferramenta que pode proteger uma máquina específica (*firewall* local) ou uma rede inteira (*firewall* de rede).

Os *firewalls* podem ser soluções prioritárias, como é o caso da *Check Point*, ou software de domínio público como o *IPTables,* nativo do Linux. Além disso, podem ser classificados em três categorias: os filtros de pacotes tradicionais (*stateless*), filtros de pacotes *stateful* e *gateways* de aplicação (KUROSE e ROSS, 2013c).

Os filtros de pacotes verificam o cabeçalho do tráfego de rede e, de acordo com as regras estabelecidas pelo administrador, permitem ou bloqueiam pacotes. As decisões sobre o encaminhamento são baseadas normalmente em: endereço IP de origem ou de destino, tipo de protocolo, portas lógicas (TCP ou UDP), *bits* de *flag* (*TCP SYN* e *ACK) e* tipo de mensagem ICMP. É comum seu emprego como barreira entre uma rede interna (endereçamento privado) e a Internet (ver figura 3.3).

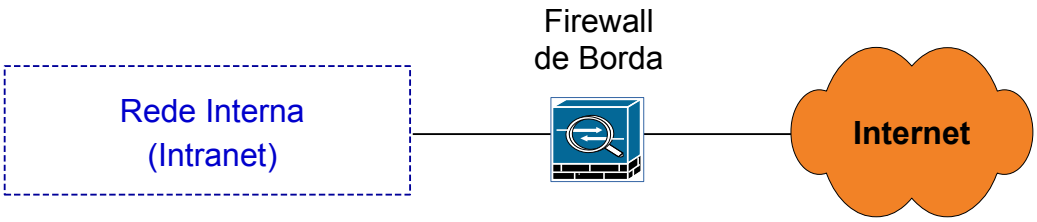

Figura 3.3 – *Firewall* de Borda.

Nos filtros de pacotes tradicionais, a decisão sobre o encaminhamento é feita individualmente com base em ACL, entretanto os filtros de pacotes *stateful* identificam as conexões TCP em andamento e levam isto em consideração para tomar decisões sobre os próximos processos de filtragem. A partir do estabelecimento de uma comunicação TCP (*three-way handshake* - SYN, SYN-ACK, e ACK), o estado de conexão é mantido até a chegada de um pacote FYN ou até que seja detectada inatividade na conexão.

Os *gateways* de aplicação conectam os usuários de uma organização à Internet por meio de servidores (*bastion hosts*). Estes servidores recebem as

solicitações dos usuários, realizam uma nova conexão para o destino, recebem os dados requisitados a partir da Internet e os entregam ao usuário que originou todo este processo. Nesta sistemática, a máquina do usuário inicial é protegida (mascarada) pelo *bastion host*, minimizando a possibilidade de ataques diretos a partir da Internet (MACÊDO, 2012).

Em seguida, serão vistas duas funcionalidades existentes no *firewalls* e roteadores L3: a tradução de endereço (*Network Address Translation* – NAT*)* e a utilização de redes privadas virtuais (*Virtual Private Network* - VPN).

3.2.3.1 *Network Address Translation - NAT*

O NAT permite que um dispositivo intermediário (roteador ou *firewall*) faça a tradução de um endereço da rede local para um endereço de outra rede externa. Normalmente é empregado na fronteira de uma organização com a Internet, permitindo que máquinas internas sejam traduzidas para endereços públicos, possibilitando a troca de pacotes com a Internet (BISWAS *et al.*, 2011).

Existem 3 diferentes tipos de NAT: (i) estático – onde cada endereço interno é traduzido para um endereço público; (ii) dinâmico – onde as máquinas internas são traduzidas para um endereço público dentro de um conjunto de N endereços possíveis; e (iii) *Overload* ou *Port Address Translation* (PAT) – onde, por apenas um endereço público, saem várias máquinas internas, mantendo o endereço externo fixo e variando a porta de saída para identificar a conexão (ex: 200.185.65.65: 53222, 200.185.65.65: 53223, …)

3.2.3.2 Rede Privada Virtual (*Virtual Private Network* - VPN)

A VPN é uma tecnologia empregada para conectar dois pontos na Internet com garantias de confidencialidade e privacidade das informações trocadas. Pode ser configurada entre computadores (*client-to-client*), entre um computador e um *gateway* (*client-to-site*) ou entre *gateways* (*site-to-site)* (ROŞU e DRĂGOI, 2011). O papel do *gateway* pode ser desempenhado por um *firewall* ou roteador.

O modelo *client-to-client* é utilizado normalmente para garantir a comunicação segura entre máquinas que trocam informações por meio de aplicações que utilizam protocolos nativamente inseguros. Cada informação é colocada dentro de um túnel virtual e enviada ao seu destino.

A VPN tipo *client-to-site* protege a troca de dados entre membros individualmente e uma organização. Por meio de um cliente-VPN instalado em um computador, é possível realizar a autenticação de um usuário em um *firewall* de borda. Assim, de qualquer lugar da Internet, torna-se possível acessar recursos corporativos de uma maneira segura.

A VPN tipo *site-to-site* visa proteger e integrar redes específicas em diferentes locais geográficos. Após sua implementação, os distintos ambientes computacionais passam a integrar logicamente a mesma rede corporativa. Esta solução pode ser empregada na comunicação entra filiais e a sede de uma empresa, por exemplo.

3.2.4 Sistema de Detecção de Intrusos e Sistema de Prevenção de Intrusos

Um Sistema de Detecção de Intrusos (*Intrusion Detection System* - IDS) é um equipamento cuja função é monitorar as atividades da rede a fim de identificar comportamentos maliciosos e violação de políticas, gerando relatórios sobre tais eventos (HOQUE *et al*., 2012). O principal objetivo do IDS é alertar os

administradores sobre o que acontece em seu ambiente, permitindo a adoção de medidas que venham a aumentar sua segurança.

No que se refere à identificação de ameaças, os IDS podem ser agrupados em três categorias: (i) Baseados em assinaturas: bastante eficazes contra ataques conhecidos, entretanto dependem do recebimento de atualizações regulares de padrões previamente conhecidos. São vulneráveis a ataques do tipo *zero-day*, ou seja, onde ainda não há uma particularidade que permita sua identificação*;* (ii) Baseados em Detecção de anomalias: agem em função de anomalias detetadas. Atuam em função de regas ou heurísticas, em vez de padrões ou assinaturas existentes; e (iii) Baseados em especificações: são responsáveis por monitorar processos específicos e combiná-los com dados reais em execução a fim de gerar alertas por ocasião da identificação de um comportamento anormal (ASHOOR e GORE, 2011).

Considerados como a segunda geração dos IDS, surgiram os Sistemas de Prevenção contra Intrusos (*Intrusion Prevention System* - IPS) com o objetivo de não apenas alertar aos administradores sobre o que está acontecendo em seu ambiente, mas, além disso, lançar automaticamente respostas a ataques e comportamentos anômalos identificados, a fim de proteger uma máquina ou uma rede.

Quanto à sua disposição na rede, tanto os IDS quanto os IPS podem ser de dois tipos: (i) *Network-Based* (NIDS ou NIPS, conforme o caso) – proveem segurança a uma rede; e (ii) *Host-Based* (HIDS ou HIPS, conforme o caso) – instalado em uma estação de trabalho ou servidor, provê segurança a esta máquina (RAGHAV *et al.*, 2013).

3.2.4.1 Solução NIPS, Regras e Quarentena

A solução *Network-based IPS* (NIPS) apresentada na Figura 3.4 é formada por uma *Manager* (Gerência Central) e sensores IPS espalhados estrategicamente pela rede. O processo de identificação e resposta a um ataque tem início na coleta e analise do tráfego em cada sensor IPS.

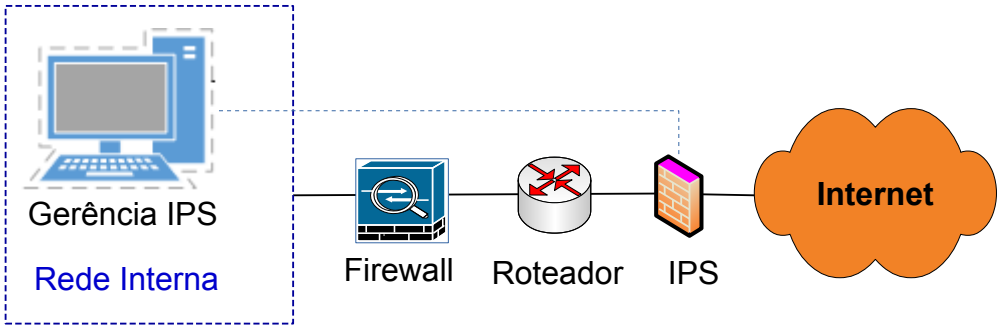

Figura 3.4 – Configuração *Network-based IPS* (NIPS).

Em cada sensor IPS podem ser configuradas diferentes políticas (conjunto de regras) que atuam em função do sentido do tráfego de dados. Por exemplo, é possível haver uma política “Servidores Web” que analisa o tráfego oriundo da Internet (*Inbound Direction*) e outra política “*Default IPS*” que verifica o tráfego proveniente da Rede Interna em direção à Internet (*Outbound Direction*). Utilizando regras configuradas nos dois sentidos, é possível reconhecer tentativas de ataques oriundas de computadores infectados pertencentes à organização.

Máquinas identificadas como origens de ações maliciosas, em ambos os sentidos do tráfego de dados, podem ser encaminhadas automaticamente para a *Quarentena*. Uma vez colocada em *Quarentena*, qualquer nova tentativa de comunicação a partir desta máquina será bloqueada.

3.2.5 *Firewall* de Aplicação Web

O *Firewall* de aplicação Web (*Web application firewall* – WAF) pode ser implementado como um *plug-in* para servidores ou filtro de rede com o objetivo de oferecer segurança à camada de aplicação. O WAF submete o tráfego HTTP/HTTPS a um conjunto de regas que visa identificar atividades maliciosas do tipo *SQL Injecton* e *cross site scripting* (XSS), dentre outras (OWASP, 2015).

O WAF trabalha de maneira semelhante a Sistema de Detecção de Intrusão (IDS), entretanto atua principalmente na camada 7 do modelo OSI (KHANDELWAL *et al.*, 2013). As regras existentes são configuráveis para diferentes tipos de aplicação (incluindo vários sistemas operacionais, tais como Linux, Windows e Mac OSX), permitindo assim um maior rendimento e acurácia na proteção dos ativos envolvidos.

Os WAF são capazes de impedir o sucesso de ataques que normalmente *firewalls* de rede e sistemas de detecção de intrusão (IDS) não percebem. Isso acontece porque são especialmente desenvolvidos para atuarem na camada de aplicação, filtrando dados e, principalmente, parâmetros existentes nas negociações HTTP/HTTPS (MACÊDO *et al.*, 2011).

3.2.6 *Security Information and Event Management* (SIEM)

O *SIEM* é a combinação de outras duas soluções: o *Security Information Management (*SIM*)* com o *Security Event Management (*SEM*).* A primeira solução analisa eventos reportados por ativos de rede e os armazenam em um banco de dados, para posterior análise, caso necessário. O objetivo da segunda é o monitoramento e a geração de alarmes, em tempo real, de eventos e sua correlação com possíveis incidentes de segurança (DORIGO, 2012).

O SIEM possibilita a análise de eventos gerados por vários dispositivos e aplicações, tais como: servidores, *proxies*, *firewalls*, roteadores e antivírus, no intuito de rapidamente identificar incidentes em redes, diminuindo o tempo de resposta da equipe de segurança. Geralmente, os eventos são capturados por coletores espalhados hierarquicamente pela rede e encaminhados para um console de gerência central (*mananger*).

Em algumas arquiteturas, pode haver uma análise prévia dos eventos nos coletores, deste modo o volume da comunicação com a *manager* seria reduzido, pois nem todas as informações capturadas são repassadas. Um risco existente neste caso, é o fato de que políticas existentes nos coletores podem filtrar eventos que seriam considerados relevantes pelo console de gerência central (STRONGSECURITY, 2015).

3.3 OS SERVIÇOS DE USO CORPORATIVO

Nesta seção, são abordados serviços corporativos utilizados pelos membros de uma organização que corroboram para a SID. São itens relacionados à navegação na Internet, recebimento de e-mail, resolução de nomes, agente de políticas de usuários, de antivírus e atualizações. Apesar de transparentes ao usuário, atuam diretamente na segurança de sua navegação e troca de dados com a Internet.

Neste tópico, também serão apresentadas questões refentes à homologação de sistemas digitais, atividade importante e que precede a publicação de um serviço Web. Além disso, é exposta a necessidade de uma Central de Suporte e Monitoramento, cujo objetivo é minimizar o tempo de resposta a incidentes em rede.

3.3.1 Os Servidores Web

Os servidores Web disponibilizados na Internet ficam suscetíveis a diversas atividades maliciosas, tais como: varreduras, força bruta, desfiguração e negação de serviço. Danos a sítios de Internet podem gerar descrédito e danos financeiros à organização. Devido a disso, o uso de ferramentas de segurança e o seu correto posicionamento dentro da infraestrutura da rede são essenciais.

Em uma arquitetura de redes, os servidores Web devem estar localizados em uma DMZ, pois caso uma máquina nesta zona seja comprometida (invadida), o invasor não conseguirá acesso à rede interna da organização, conforme demonstrado na figura 3.5.

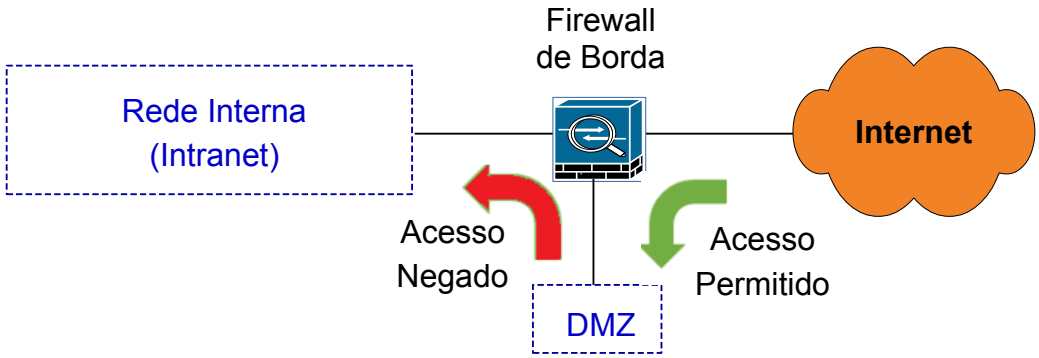

Figura 3.5 – Servidor Web (DMZ).

Além de sua localização na DMZ e da utilização de ferramentas na proteção, os desenvolvedores de sistemas Web devem estar atentos a possíveis falhas de segurança desde sua concepção. A tentativa de corrigi-las, quando o software já está próximo de ser finalizado, pode encarecer e trazer atrasos ao projeto (UTO e MELO, 2009).

Para que um serviço Web possa entrar em produção, sendo efetivamente disponibilizado para usuários, é necessário que o servidor atenda a requisitos mínimos de segurança e esteja de acordo com as boas práticas de desenvolvimento e usabilidade. A organização deve padronizar as configurações de sistema

operacional no intuito de facilitar a gestão dos recursos, controle de licenças e o gerenciamento da segurança. Por exemplo, podem ser padronizados servidores Web, servidores de correio eletrônico, servidores de banco de dados, servidores de virtualização, servidor de domínio e servidores de *patches* de atualização, dentre outros.

3.3.2 A Homologação de Sistemas Digitais (SD)

Antes de um SD ser efetivamente disponibilizado para acesso, é necessário realizar sua homologação. Para isso, devem ser verificadas questões relacionadas: (i) à produção dos manuais de utilização; (ii) ao seu desenvolvimento; (iii) ao correto funcionamento e usabilidade; e (iv) atendimento aos requisitos mínimos de segurança estabelecidos pela organização.

Quanto à avaliação de questões relativas ao desenvolvimento do SD, podem ser verificadas: (i) normas e padrões vigentes; (ii) linguagens de programação utilizada; (iii) sistemas operacionais utilizados; (iv) bancos de dados utilizados; (v) sistemas de backup; (vi) arquitetura do sistema; (vii) protocolos utilizados; (viii) resultados de testes de aceitação; e (ix) capacidade de escalabilidade, dentre outras.

No que tange aos requisitos mínimos de segurança, em caso de sistemas Web, e recomendável a utilização do protocolo HTTPS (*hypertext transfer protocol secure*), com certificados atualizados a serem empregados suas conexões, quando informações confidenciais são trafegadas em rede. Além disso, os sistemas Web devem ser compatíveis com os navegadores adotados pela organização.

Em sistemas que requeiram autenticação do usuário, as senhas devem conter um número mínimo de caracteres (letras, números e caracteres especiais,

preferencialmente). As senhas não devem ser armazenadas em claro e também não devem permitir sua recuperação e/ou leitura. Informações sensíveis que necessitem estar armazenados em BD, além de seus mecanismos intrínsecos de segurança, podem permanecer criptografados.

Como medida adicional, no processo de autenticação de usuário, um *hash* da senha digitada pode ser gerado e apenas comparado ao *hash* armazenado no BD. As medidas aqui descritas, são apenas algumas dicas de segurança. Como parte do processo de homologação, antes de ser disponibilizado na rede, devem ser realizadas varreduras no SD em busca de vulnerabilidades que poderiam comprometer o sistema quando este entrasse em produção.

3.3.3 As Estações de Trabalho

Os aplicativos e configurações das Estações de Trabalho (ET) devem ser padronizados pela organização no intuito de facilitar a gestão e economia de recursos, controle das licenças utilizadas e processos relacionados à segurança da informação. É recomendável haver uma especificação mínima de requisitos de sistema e programas homologados a serem instalados inicialmente, obtendo-se assim uma estação de trabalho padronizada.

A definição dos programas homologados para uso nas ET pode contemplar, por exemplo: Sistema Operacional (SO), navegador Web, compactador de arquivos, software antivírus, leitor de arquivos (.pdf*)* e suíte de programas para escritório. Antes da atualização de qualquer programa ou aplicativo, é interessante que os *softwares* em suas versões mais recentes sejam testados internamente e, só após isto, disponibilizados aos usuários, pois versões recém-lançadas podem trazer comportamentos indesejados, incidindo em lentidão ou indisponibilidade de algum

serviço corporativo. Por exemplo, uma solução de correio eletrônico pode ser incompatível com a última versão de um navegador Web, o que deixaria o serviço inacessível.

Outra medida importante é a utilização de softwares que impeçam a instalação de aplicativos não padronizados nas estações de trabalho. Auditorias internas e periódicas também podem auxiliar na identificação de máquinas com programas que podem colocar em risco a segurança digital da organização.

Nas estações de trabalho e servidores, no intuito de minimizar as chances de infecção por programas maliciosos, deve haver um software antivírus instalado. Outra medida importante é o Gerenciamento de Atualizações do SO e softwares instalados, bem como uma Política de Segurança aplicada aos Usuários.

3.3.3.1 O Antivírus

Embora haja uma enorme diversidade de processos existentes em uma organização, um antivírus corporativo é uma boa solução de segurança para seus usuários. Esta solução agrega várias vantagens relacionadas à facilidade de instalação, implantação, usabilidade, gestão, escalabilidade, apoio técnico e atualizações. Além disso, as soluções atualmente existentes normalmente atendem sistemas de plataformas Windows e Linux (GHARIBI e MIRZA, 2011)

A instalação e implantação de um antivírus é relativamente simples e rápida, a arquitetura é formada por um servidor principal com seu respectivo banco de dados e em cada uma das estações de trabalho e demais servidores da organização é instalado um agente do antivírus. Uma possível funcionalidade é a implementação de regras que bloqueiam a instalação de aplicativos que estejam em desacordo com a política de uso adotada pela organização. Os eventos (tentativas de instalação de

programas indevidos e/ou arquivos maliciosos) detectados pelos agentes são reportados ao servidor principal que, por sua vez, exibe uma interface de gerenciamento centralizada com recursos de monitoramento e detecções em tempo próximo ao real.

A solução é escalável, podendo atender organizações de tamanhos variados, desde redes onde todos os funcionários estão localizados em uma mesma sede a instituições com filiais em diferentes locais geográficos. Além disso, o sistema de antivírus corporativo recebe atualizações e apoio técnico do fornecedor do produto na resposta a eventuais problemas e incidentes encontrados.

3.3.3.2 O Gerenciamento de Atualizações

No intuito de manter uma padronização das estações de trabalho utilizadas, aos usuários não deve ser concedido o privilégio de ADMINISTRADOR. Isto facilita a gerência das máquinas e minimiza as chances de instalação de softwares indesejados na rede da organização.

Uma vez instalados o sistema operacional e os softwares homologados para uso interno, a estação de trabalho é entregue ao usuário. Entretanto, é necessário que as atualizações do SO (Windows ou Linux) e demais programas instalados continuem ocorrendo normalmente, por medida de segurança e desempenho. Para isso, devem haver repositórios internos que baixem as atualizações do SO a partir da Internet e as distribuam internamente.

O Windows utiliza o *Windows Server Update Services* (*WSUS*) para suas atualizações e o Linux faz uso de um servidor *mirror* que recebe esta denominação em função do conceito de “espelhamento” para a entrega de seus pacotes. Os

repositórios internos devem redistribuir as atualizações recebidas, após uma avaliação inicial do administrador da rede.

É interessante que as atualizações obtidas a partir da Internet sejam homologadas em máquinas de teste e só após isto, liberadas para toda a organização. Esta tarefa visa minimizar as chances de impactos negativos com atualizações defeituosas.

3.3.3.3 As Políticas de Segurança aplicadas aos Usuários

É possível criar políticas de segurança no intuito de restringir os recursos disponíveis da rede e as permissões de uso das estações de trabalho aos usuários. Um grande número de pessoas envolvidas nos processos que lidam com informações sensíveis, aliado ao fato de fragilidades existentes na política interna de segurança adotada, pode incidir em ações (intencionais ou não) diretamente correlacionadas à perda ou roubo de informações e sabotagem industrial (ALENCAR *et al.*, 2013).

ALVES e MOREIRA (2012) realizaram uma análise sobre o impacto da implementação de políticas de segurança em uma organização. Para o seu experimento, foi escolhida uma instituição que não possuía um plano de SID e grande desconhecimento de normas relacionado ao assunto. Após todo o processo de conscientização dos usuários e efetiva aplicação de sua proposta, os autores obtiveram o seguinte resultado: (i) aumento na produtividade de setores críticos, tais como tesouraria e contabilidade; (ii) diminuição do índice de contaminação por vírus; e (iii) aumento do desempenho da rede e facilidades na identificação de problemas. O estudo realizado concluiu que a adoção de políticas de segurança incide positivamente no desempenho de um ambiente corporativo.

Dentre as possibilidades existente, por exemplo, podem ser criadas políticas para controlar unidades leitoras de mídias removíveis (CD/DVD-ROM), controlar o uso de dispositivos de armazenamento em massa (Pen drive, HD externo, leitores MP3), aplicar permissões a partir da atual localização do usuário, solicitar periodicamente a troca de senhas de serviços e aplicações, criar uma política de senha forte (exigindo o uso de letras maiúsculas e minúsculas, números e caracteres especiais) e restringir o acesso a contas de e-mail particulares (algumas vezes associadas ao roubo de informações e entrada de vírus na rede).

3.3.4 O *Proxy*

Em ambientes corporativos, sua função é intermediar a comunicação HTTP/HTTPS/FTP entre uma estação de trabalho e o servidor de destino responsável pelo serviço solicitado (SOUZA e SOUSA, 2010). Em questões relacionadas à segurança, é função do *proxy*: (i) requerer a autenticação de usuários previamente cadastrados; e (ii) fazer restrições a endereços potencialmente perigosos ou que estejam em desacordo com a política da organização. A autenticação é importante a fim de permitir a rastreabilidade de acessos a sítios na Internet. Outra importante função do *proxy* é a de realizar o armazenamento local (*cache*) de páginas visitadas, o que torna a navegação mais rápida para os próximos indivíduos (RIBEIRO, 2007).

3.3.5 Os Filtros de E-mail

Um filtro de e-mail (*e-mail gateway)* é um servidor por onde passam as mensagens de correio eletrônico que entram e saem de uma organização. Os e-mail enviados e recebidos são processados e analisados no intuito que encontrar

arquivos maliciosos ou conteúdo que esteja em desacordo com sua política de utilização.

Dentre as possíveis funcionalidades, podem ser implementadas: (i) identificar arquivos maliciosos anexados; (ii) verificar se o remetente pertence a uma lista de domínios categorizados como maliciosos (*black list*); (iii) detectar imagens pornográficas, via *software*; (iv) prevenção contra perda de dados e documentos confidenciais, por meio de busca automatizada por palavras pré-configuradas; e (v) bloqueio a falsas notificações de mensagens não entregues (INFOMACH, 2015).

3.3.6 O *Domain Name System* (DNS)

O *Domain Name System* (DNS) é um sistema de gerenciamento hierárquico de nomes e endereçamentos cuja função é possibilitar a identificação de computadores na Internet de uma forma mais intuitiva. Por exemplo, quando um usuário acessa um endereço de URL, o endereço IP do servidor de destino é obtido com base no mapeamento (tradução) existente no DNS (CAMPISTA *et al.*, 2010).

Os DNS do tipo autoritativo e recursivo são bastante empregados e possuem funções distintas, embora possam ser configurados em um mesmo servidor. O Autoritativo é aquele que mantém todas as informações e responde por um domínio, sendo consultados por servidores externos quando necessário. O Recursivo é o DNS que normalmente configuramos nas estações de trabalho, sendo responsável por obter respostas internas ou externas de interesse para um usuário.

Um reconhecido problema de configuração e segurança é o chamado *DNS Recursivo Aberto*, isto acontece quando um DNS recursivo permite solicitações de resolução de nomes a partir de máquinas na Internet. Apenas os DNS autoritativos

devem responder a este tipo de consulta (CERT.BR, 2015f). O DNS utiliza as portas 53/TCP,UDP.

3.3.7 A Central de Suporte e Monitoramento

No intuito de manter o alto índice de disponibilidade dos sistemas, é importante a criação de uma Central de Suporte e Monitoramento dos principais ativos de Tecnologia da Informação (TI) a fim de atuar de forma rápida no diagnóstico e tratamento de eventos que incidam na indisponibilidade ou mal funcionamento de serviços oferecidos. Esta Central deve ser o ponto único de contato e suporte para usuários internos e externos.

A estrutura desta Central pode variar em função da dimensão do ambiente computacional. Em organizações de pequeno e médio porte, os profissionais da Central de Suporte e Monitoramento podem ser alocados em outras tarefas mais específicas, como por exemplo o tratamento de incidentes de segurança em redes.

Entretanto, em ambientes de grande porte, aos profissionais de primeiro nível, ficam alocadas apenas tarefas afetas à Central de Suporte e Monitoramento. Neste caso, atividades mais específicas, tal como o Gerenciamento de Incidentes deve ficar alocada a outra equipe, devido à quantidade de solicitações diariamente encaminhada à Central (FREITAS, 2013).

Para cada solicitação de usuário, evento detectado ou incidente em rede, pode ser criado um registro com todas as etapas desenroladas desde o início até a sua conclusão. Esta base de dados, com tais registros, tem duas finalidades: (i) servir de histórico da rede; e (ii) funcionar como fonte de pesquisa e busca de soluções a eventos possivelmente recorrentes.

A Central de Suporte e Monitoramento deve realizar uma avaliação preliminar das solicitações a serem atendidas, buscar uma solução inicial que esteja a seu alcance ou redirecioná-la a um próximo nível de suporte interno (conectividade, segurança, centro de dados ou acesso à Internet, por exemplo). Além disso, relatórios internos sobre solicitações de usuários e análise estatística de disponibilidade de serviços e ativos de rede podem facilitar a identificação e correção de pontos falhos na estrutura de TI da organização.

O uso de *scripts* e ferramentas automatizadas (CACTI, Nagios e Zabbix, por exemplo) auxiliam no gerenciamento e monitoramento de servidores e ativos de rede, tais como roteadores e *firewalls*. Abaixo, é apresentado um exemplo de programação em S*hell script* combinado o *sendEmail* para o envio automático de mensagens em caso de indisponibilidade de um equipamento.

```
#!/bin/bash
# Remetente
REMETENTE="humberto@dominio.com"
# Destinatários
DESTINATARIO="destinatario1@dominio.com, destinatario2@dominio.com"
# Quantidade de ping a serem enviados
COUNT=3
# Importante: Cadastrar a máquina de monitoramento como servidor de confiança
do # servidor de correio da organização
# Em <Svd_Correio>, substituir pelo endereço IP do servidor de correio da
# organização
# iniciando equipamento em estado "UP"
let estado_anterior_EQUIPAMENTO=1
```

```
while :
do
	let count_EQUIPAMENTO=$(ping -c $COUNT <Endereco_IP_Equipamento> |
grep 'received' | awk -F',' '{ print $2 }'| awk '{ print $1 }')
	if [ $count_EQUIPAMENTO = 0 ]
	then
		let estado_atual_EQUIPAMENTO=0
	fi
	if [ $count_EQUIPAMENTO != 0 ]
	then
		let estado_atual_EQUIPAMENTO=1
	fi
	if [ $estado_atual_EQUIPAMENTO != $estado_anterior_EQUIPAMENTO ]
	then
		if [ $estado_atual_EQUIPAMENTO = 0 ]
		then
			sendEmail -t $DESTINATARIO -f $REMETENTE -s <Svd_Correio>
-u "EQUIPAMENTO DOWN" -m "EQUIPAMENTO DOWN as $(date +%H:%M)h do
dia $(date "+%d de %B de %Y")"
			echo "EQUIPAMENTO DOWN as $(date +%H:%M)h do dia $(date
"+%d de %B de %Y")" >> ping.log
		fi
		if [ $estado_atual_EQUIPAMENTO = 1 ]
		then
			sendEmail -t $DESTINATARIO -f $REMETENTE -s <Svd_Correio>
```

```
-u "EQUIPAMENTO UP" -m "EQUIPAMENTO UP as $(date +%H:%M)h do dia $
(date "+%d de %B de %Y")"
                    echo "EQUIPAMENTO UP as $(date +%H:%M)h do dia $(date "+%d
de %B de %Y")" >> ping.log
            fi
            let  estado_anterior_EQUIPAMENTO=$estado_atual_EQUIPAMENTO
      fi
done
```

3.3.8 O Correio Eletrônico

O correio eletrônico é uma ferramenta utilizada para comunicação, via troca de e-mails, entre usuários de uma rede interna ou entre estes e a Internet. Podem ser enviados texto escrito, imagens, sons e arquivos digitais (MALTINTI e MALTINTI, 2010). Uma vantagem em relação às correspondências tradicionais é o fato da possibilidade do envio de mensagens para múltiplos destinatários simultaneamente.

Entretanto, o correio eletrônico pode afetar a produtividade em virtude de seu uso em atividades de cunho particular, por servir de portal à entrada de vírus e *worms,* permitir o vazamento de informações e possibilitar o envio de mensagens com conteúdo pornográfico, dentre outras (FERREIRA, 2013). Além disso, em correios com interface Web, podem ocorrer tentativas de invasão à contas dos usuários, por meio de ataques de força bruta.

Uma medida de proteção às contas dos usuários é a adoção de uma politica de senha forte com os seguintes critérios:

- Mínimo de 8 e máximo de 20 caracteres;

- Conter os seguintes caracteres, pelo menos uma vez: letra maiúscula, letra minúscula, número e símbolo especial (!, @, #, $, %, &, por exemplo); e
- Troca periódica, sem a possibilidade de repetição das últimas senhas utilizadas.

3.3.9 O Serviço de Diretório

O serviço de diretório tem a função de centralizar a autenticação dos usuários e permitir a utilização dos computadores e demais recursos de uma rede corporativa. Além disso, armazena também as configurações dos serviços, zonas DNS, sub-redes DHCP, certificados digitais e arquivos binários, dentre outras informações pertinentes. Possui versões compatíveis com os sistemas Windows e Linux (CARRARA e BELLEZI, 2014).

O serviço de diretório deve estar configurado de modo que os dados estejam protegidos contra acessos indevidos, pois, além dos nomes de usuários e suas respectivas senhas, podem estar armazenados cadastros do setor de recursos humanos da empresa e várias informações particulares (BRITO *et al.*, 2012).

Utilizando o serviço de diretórios, permitimos a um usuário efetuar o "*login*" no domínio de sua organização. Caso haja ambientes computacionais localizados em diferentes localidades, pode ser construída uma infraestrutura com subdomínios distintos, com vínculos existentes e relações de confiança estabelecidas entre si. Como soluções de serviço de diretório, podem ser citadas: *Open Ldap* para Sistemas *Open Source*, *EDirectory* para Sistemas *Novell* e *Active Directory* para Sistemas *Microsoft* (MICROSOFT, 2015).

3.4 CONCLUSÃO

Foi apresentada a definição de espaço cibernético em conjunto com algumas abordagens sobre programas maliciosos (*malwares*) e ataques na Internet. O objetivo deste capítulo foi demonstrar uma noção de possíveis ações que podem ser empreendidas contra usuários, serviços e máquinas conectadas à rede mundial de computadores.

Além das definições expostas, ainda há uma grande variedade de ações maliciosas que não foram abordadas, mas que representam ameaças contínuas ao espaço cibernético, dentre as quais podem ser citadas: ataques na camada de aplicação (*Application-Layer Attack*), envenenamento do DNS (*DNS poisoning*), alteração de dados (*Data Modification*), ataques via protocolo ICMP (*ICMP Attack*), interceptação de comunicação entre dois computadores (*Man-in-the-Middle*), mascaramento de IP (*IP Spoofing*), roubo de sessão TCP (TCP *Hijacking*) e o uso da técnica *phishing* voltada a celulares via SMS (*SmiShing*).

No próximo capítulo, será apresentada uma arquitetura de redes baseada nos conceitos, ferramentas e serviços apresentados até o momento. A topologia contemplará uma organização de médio porte e está voltada à segurança da informação digital (SID), utilizando boas práticas e possíveis medidas contra as atuais atividades maliciosas existentes na Internet.

4 **A ARQUITETURA DE SEGURANÇA**

Neste capítulo, apresentaremos uma proposta de arquitetura de segurança para uma hipotética organização que possui uma sede e duas filiais localizadas em distantes locais geográficos. O objetivo não é explanar minuciosamente e/ou esgotar todas as possibilidades e questões inerentes à SID, mas utilizar a presente topologia para expor sugestões e orientações que tendem a manter um ambiente de rede protegido contra as ameças cibernéticas existentes em nosso cenário atual.

4.1 A TOPOLOGIA DA REDE

A arquitetura adotada levou em consideração uma suposta organização composta por uma sede e duas filiais. A instituição possui dois contratos de *links* de Internet com operadoras: (i) a Internet-1: conexão de rede onde ficam disponíveis os servidores Web; e (ii) a Internet-2: conexão utilizada para que os usuários internos possam navegar na Internet. Poderiam ser ainda elencadas questões sobre a redundância dos *links* MPLS e Internet, mas este não é o foco do presente trabalho.

A rede interna da organização possui duas sub-redes: Uma “Rede de Serviços” que hospeda os servidores empregados para fins específicos e corporativos e uma “Rede de Homologação” utilizada para a realização de testes de aceitação em sistemas desenvolvidos ou adquiridos comercialmente.

Na Figura 4.1, é apresentada a topologia proposta para a proteção da rede. A partir de agora, serão abordas questões relacionadas ao posicionamento dos equipamentos, regras e políticas de segurança atinentes ao uso das ferramentas de segurança.

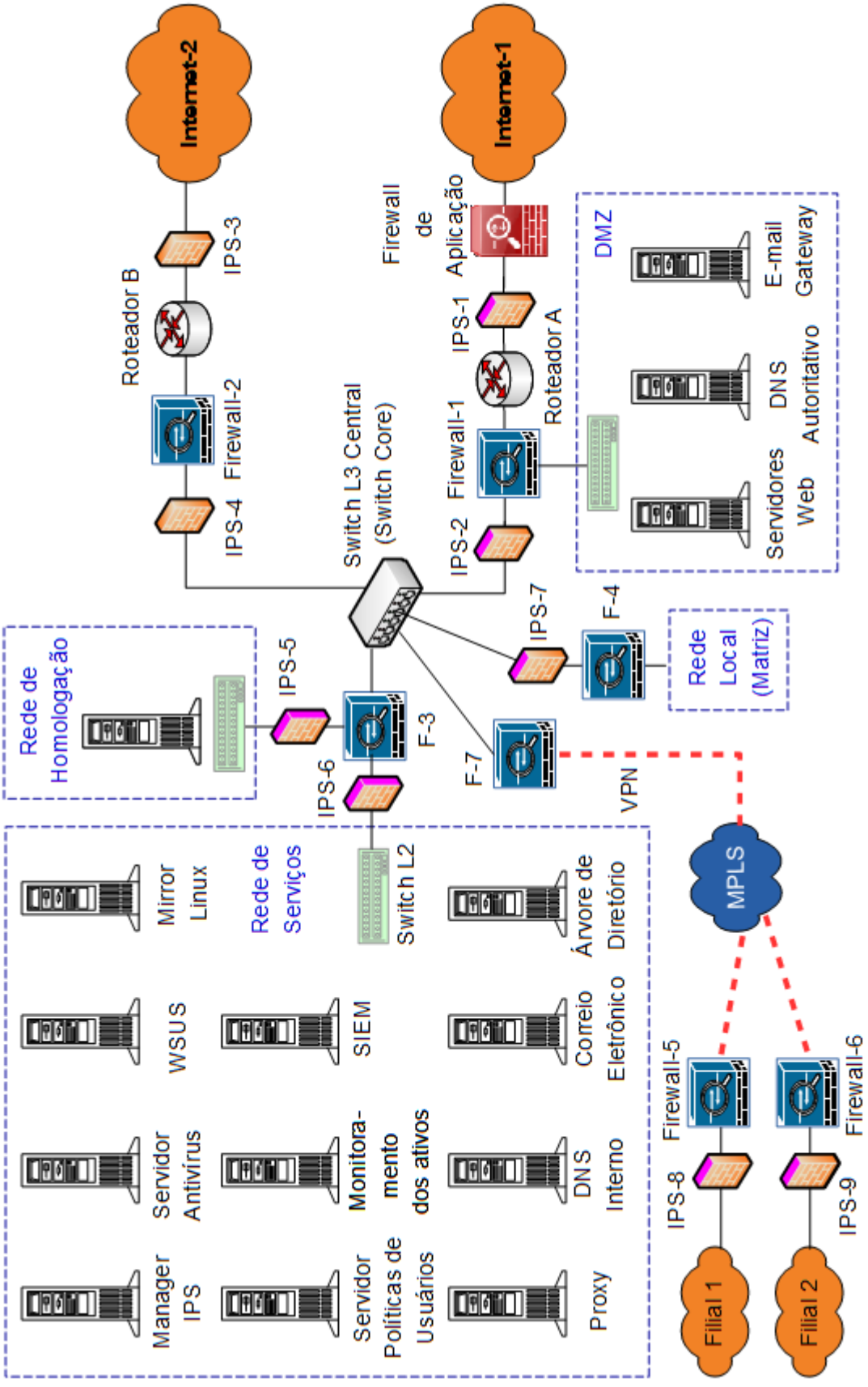

Figura 4.1 – A Topologia da Rede.

4.2 OS ROTEADORES DE BORDA COM A INTERNET

Os roteadores que interligam a organização com a Internet são, em alguns casos, a primeira barreira a ser vencida para que um atacante possa invadir a rede interna ou os servidores Web localizados na DMZ (Figura 4.2). Neste equipamento devem estar presentes, essencialmente, Listas de Controle de Acesso (ACL) ao ambiente da organizacional.

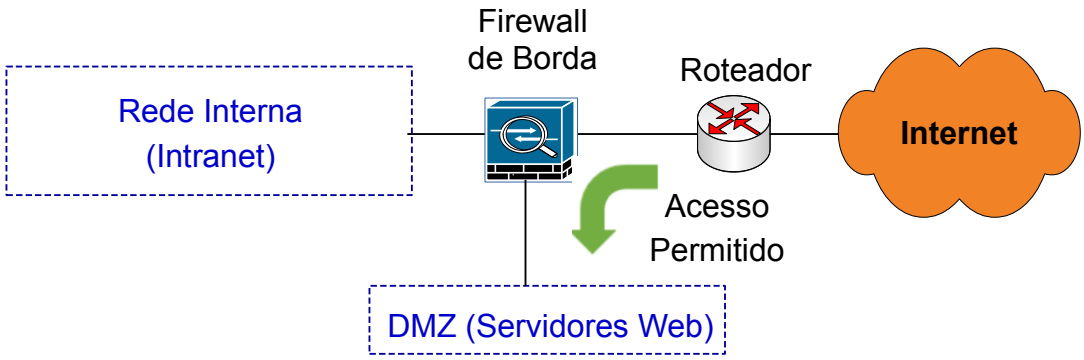

Figura 4.2 – Roteadores de Borda

É importante deixar configuradas apenas as portas lógicas que inerentemente serão utilizadas pelas aplicações e que devem ser acessadas a partir da Internet. Por exemplo, em organizações que oferecem páginas Web, o roteador de borda deve possuir as portas http (80/TCP) e https (443/TCP) liberadas. No caso de DNS Autoritativos, também torna-se necessária a liberação às portas 53/TCP,UDP. Para o recebimento de e-mail externos, é atribuída permissão para a entrada de pacotes direcionados às portas 25/ TCP (*Simple Mail Transfer Protocol*) (IANA, 2015).

A lista de portas lógicas com acesso liberado depende da realidade de cada organização. Via de regra, todas as portas não utilizadas devem estar configuradas com bloqueio (*deny*). Atenção especial deve ser dada às portas de gerência SSH (22/TCP) e TELNET (23/TCP). Este último, o TELNET, deve ser evitado devido ao fato do usuário e sua senha trafegarem em claro na rede (ARAVINDHAN e KARTHIGA, 2013), possibilitando que os dados senhas capturados por s*niffers* (ver

item 2.2.3). Outra medida importante é seguir as orientações de segurança contidas no item 3.2.1.

4.3 OS SENSORES DO SISTEMA DE PREVENÇÃO DE INTRUSOS

O Sistema de Prevenção de Intrusos visa monitorar e prover respostas adequadas contra tráfego de dados com características maliciosos. Basicamente é composto por uma *Manager* (Gerência Central) e sensores IPS distribuídos em pontos estratégicos. O posicionamento ideal de um sensor IPS é na entrada de uma rede com regras que atuam em ambos os sentidos (*Inbound*) e (*outbound*), analisando o tráfego em tempo real (STIAWAN *et al.*, 2013). As regras *Inbound* analisam o tráfego em direção à rede a ser protegida, enquanto as regras *Outbound* verificam o tráfego que sai da rede interna. As regras *Outbound* visam identificar computadores infectados lançando ataques a outras redes.

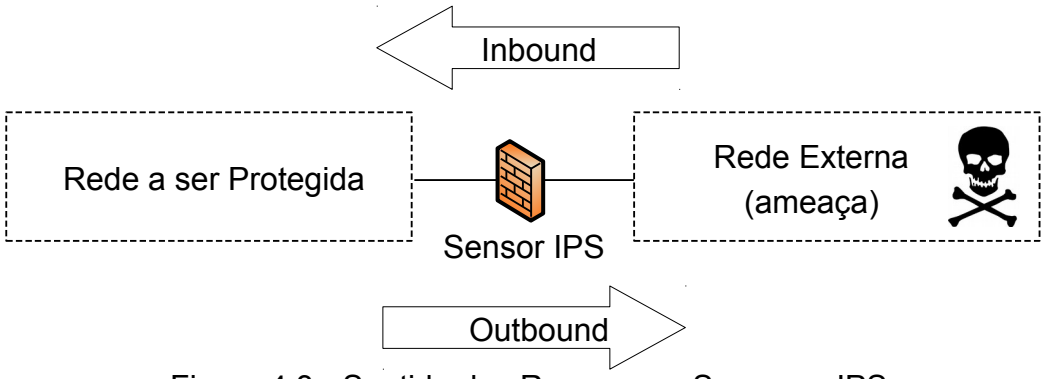

Figura 4.3 - Sentido das Regras nos Sensores IPS.

Na Figura 4.1, podemos observar que os sensores IPS 5, 6, 7, 8 e 9 estão protegendo redes internas da organização, assim como os pares de sensores IPS (1-2) e (3-4). Entretanto, estes dois últimos pares específicos trabalham em conjunto devido à existência de um *firewall* com *Port Address Translation* (PAT) que altera os endereços internos para um mesmo endereço público roteável na Internet. A

necessidade de pares de sensores IPS trabalhando em conjunto é explicado a seguir.

Na Figura 4.4, suponhamos que uma máquina de sua organização possua acesso sem proxy à Internet e realize uma varredura no endereço IP 8.8.8.8 (DNS Google). Caso o administrador do seu domínio receba uma notificação sobre este evento, provavelmente haveria referência ao endereço de origem e ao tipo de ação maliciosa (varredura) executada pela máquina.

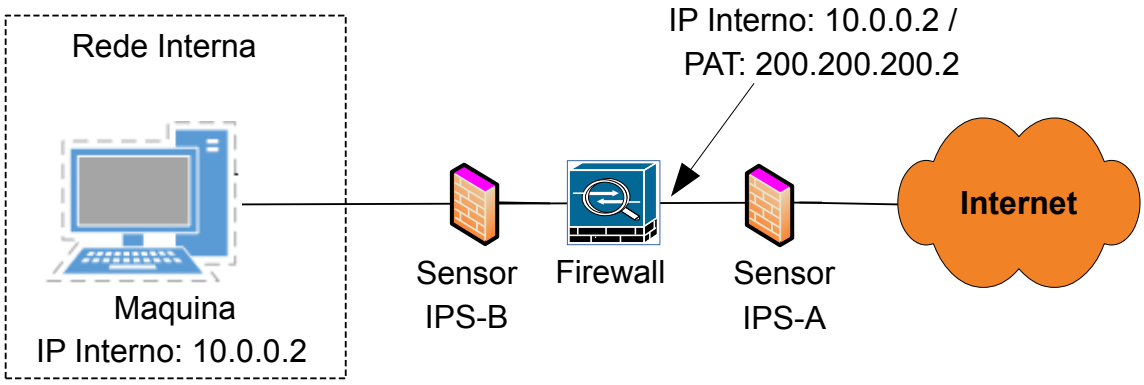

Figura 4.4 –Sensores IPS e *Firewall* com PAT.

De posse da notificação da Google, inicialmente o administrador verificaria nos registros (*logs*) do Sensor IPS-A a confirmação do tráfego saindo da sua rede e encontraria:

**** Sensor A ****			
Data	*Tipo*	*IP NAT*	*IP Externo*
10/27 02:20:17	*NMAP: XMAS with SYN Probe*	*200.200.200.2*	*8.8.8.8*

Após a confirmação de que a varredura realmente saiu de sua rede (a partir da informação acima), o administrador realizaria uma segunda busca no Sensor IPS-B e encontraria o registro abaixo que possibilitaria a identificação do endereço interno, confrontando o mesmo horário e o mesmo tipo de assinatura registrado nos

dois sensores A e B. Caso não houvesse o Sensor IPS-B, esse diagnóstico não seria possível.

**** Sensor B ****			
Data	*Tipo*	*IP Interno*	*IP Externo*
10/27 02:20:17	*NMAP: XMAS with SYN Probe*	*10.0.0.2*	*8.8.8.8*

Quanto à quantidade de sensores IPS a serem utilizados na organização, cabe salientar que existem modelos no mercado que possuem vários pares de portas disponíveis em um mesmo equipamento. Ou seja, dependendo da sua topologia, vários *links* de rede podem ser agrupados em um mesmo sensor, economizando recursos financeiros.

Uma observação pertinente, é o fato da colocação do Sensor IPS-1 antes do roteador da Internet-1 (Figura 4.4). Esta escolha, quando aplicável, pode ser utilizada para a proteção do roteador contra ataques provenientes da Internet. Quando não for possível, o IPS deve ser colocado antes do *Firewall*.

4.4 O *FIREWALL* DE APLICAÇÃO

Observando a Figura 4.5, verificamos que o *firewall* de aplicação (WAF) está posicionado como a primeira barreira contra ataques da Internet, seguido do sensor IPS-1. Os WAF são configurados com regras e políticas específicas para os serviços oferecidos na Internet. Em sua concepção, este equipamento foi particularmente concebido para oferecer proteção adicional às aplicações Web, onde, em certos casos, o IPS não consegue atuar (KHANDELWAL *et al.*, 2013).

Teoricamente, todos os ataques efetuados na camada de aplicação devem ser bloqueados pelo WAF. Quando um ataque é realizado nesta camada é identificado pelo IPS (que está após o WAF), é sinal de que houve uma falha de

configuração no WAF ou este ainda não possui a devida assinatura de identificação. Nestes casos, as regras do WAF devem ser revistas e melhoradas. Tal situação pode ocorrer, pois o IPS atua em várias camadas, inclusive identificando ataques na camada de aplicação não bloqueados pelo WAF.

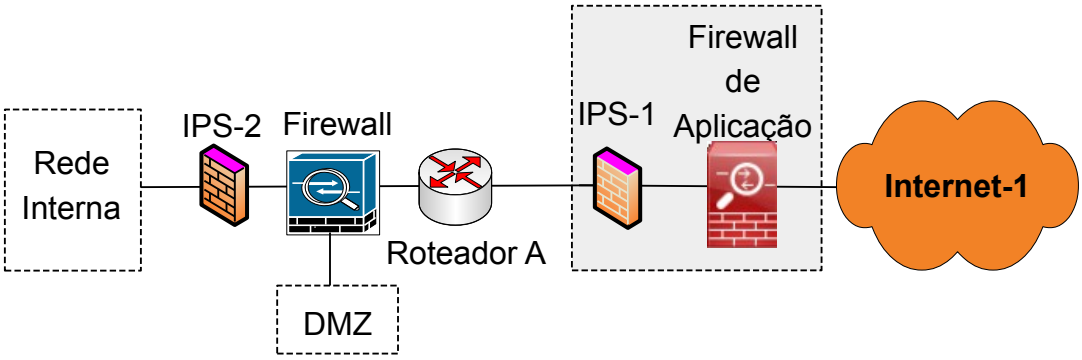

Figura 4.5 - Posicionamento do Firewall de Aplicação.

Cabe salientar que na topologia da rede (Figura 4.1), o *firewall* de aplicação apenas foi implementado na Internet-1 devido ao fato de que somente esta conexão possui sistemas corporativos disponibilizados na Internet. O outro *link* (Internet-2) é utilizado exclusivamente pelos *proxies* para a navegação dos usuários na Web.

4.5 OS *FIREWALLS*

O Firewall-1 posicionado no *link* onde estão hospedados os serviços disponibilizados para a Internet requer especial atenção, pois regras mal configuradas podem facilitar o acesso indevido a máquinas internas da organização. O ideal é que todos os computadores internos naveguem na Web por meio de *proxies* via Internet-2 (ver Figura 4.1), mas aplicações específicas podem não permitir tal funcionalidade, sendo necessária a liberação de endereços IP via Internet-1 (sem o uso de *proxy*).

Ainda no *firewall* da Internet-1, via de regra, os serviços oferecidos para a Internet ficam hospedados na rede DMZ e possuem NAT para os endereços IP

públicos sob o domínio da organização. Para o endereço público de cada servidor, devem ser liberadas apenas as portas específicas necessárias. O acesso à DMZ por usuários internos também deve ser controlado, de tal maneira que apenas as portas lógicas vitais sejam liberadas.

Na Internet-2, um ou mais endereços públicos devem ser disponibilizados para os *proxies* da organização. Cada *proxy* deve possuir um NAT no Firewall-2 de modo a permitir sua saída para a Internet. Cabe salientar que os endereços internos com NAT ou PAT (nos *Firewalls* 1 e 2), devem ser configurados de tal maneira a receberem apenas as respostas de solicitações por eles geradas.

De uma maneira geral, novas conexões originadas na Internet com destino aos endereços IP públicos da organização devem ser bloqueadas. Exceção a esta regra, são as portas dos serviços realmente necessários, tais como: servidores web, correio eletrônico e DNS autoritativo. Além disso, quando possível, o endereço de Internet deve ser levado em consideração na criação das regras (ACL) nos *firewalls*.

No Firewall-3, é importante estarem mapeadas todas as portas utilizadas pelos servidores da Rede de Serviços, bem como com quais máquinas cada um deve realizar comunicação. Por exemplo, com a Manager do IPS, apenas os endereços dos sensores IPS e as máquinas do departamento de segurança devem possuir acesso garantido. Por outro lado, ao servidor de atualizações WSUS, todos os computadores internos devem ter acesso: (i) no WSUS 3.2 e versões anteriores - na porta 80 para HTTP e 443 para HTTPS; e (ii) no WSUS 6.2 e posteriores (pelo menos *Windows Server* 2012) - na porta 8530 para HTTP e 8531 para HTTPS (MICROSOFT, 2015b).

Ainda no Firewall-3, quando houver a necessidade da realização de testes de aceitação em sistemas, devem ser configuradas as regras necessárias para o seu

correto funcionamento na Rede de Homologação. Neste caso, serão liberadas para acessos as portas de gerência e comunicação utilizadas pela aplicação hospedada.

Os *Firewalls* 4, 5 e 6 são utilizados para proteção respectivamente da rede da sede e das filiais 1 e 2. As regras implementadas nestes equipamentos visam bloquear tentativas de varreduras e acessos indevidos originados de redes distintas às protegidas. Nestes equipamentos, as comunicações com os servidores hospedados na rede de serviços e as conexões originadas a partir de cada uma das redes locais têm seu tráfego permitido.

As filiais 1 e 2, por estarem distantes da sede, são integradas à rede da organização via MPLS (*Multi-Protocol Label Switching*). Uma nuvem MPLS oferece um encaminhamento do tráfego de forma bastante eficiente, pois os roteadores de borda analisam os pacotes recebidos, atribuindo-lhes rótulos que são utilizados pelos demais roteadores internos para o encaminhamento por meio de circuitos virtuais estabelecidos. Ou seja, dentro da nuvem, não há a necessidade dos roteadores verificarem o cabeçalho IP de cada pacote e realizarem um busca em sua tabela de roteamento, diminuindo assim o tempo de processamento (FIGUEIREDO, 2011).

No intuito de proteger o sigilo das informações que trafegam na rede MPLS que é gerenciada por terceiros, entre os Firewalls 5, 6 e 7 são configuradas redes virtuais privadas (VPN). Após o tráfego ser entregue aos Firewalls 5 e 6, os sensores IPS 8 e 9, respectivamente, podem analisá-lo, pois já estará descriptografado.

Como medida adicional de segurança, convém criar uma ACL para liberar o acesso à gerência de todos os *firewalls* apenas para os endereços IP das estações de trabalho de seus administradores. Além disso, é recomendável a utilização de senhas que possuam um número razoável de caracteres com letras maiúsculas,

minúsculas, números e caracteres especiais. Outra medida importante é seguir as orientações de segurança aplicáveis e contidas no item 3.2.1.

4.5 O ANTIVÍRUS

A equipe de segurança deve manter o acompanhamento diário dos relatórios de eventos gerados pelo sistema de antivírus corporativo. Por exemplo, avisos de tentativas de instalação de softwares indevidos apontadas pelo antivírus ajudam a identificar indivíduos que devem receber orientações adicionais sobre a política de SID da empresa.

Dependendo do método de contratação do suporte de antivírus, seu servidor central receberá atualizações diárias contra novas ameaças cibernéticas. Entretanto, eventualmente, seu ambiente de rede pode ser infectado por um vírus que sua base de dados não possua a assinatura de identificação correspondente. Neste caso, torna-se importante identificar o executável malicioso e enviá-lo ao laboratório do suporte de antivírus para que a “vacina” específica seja gerada e aplicada ao servidor Central, para posterior distribuição automatizada aos computadores da organização.

É importante identificar quais portas são utilizadas pelo agente do antivírus na comunicação com seu servidor central. A partir disso, periodicamente deve-se realizar uma varredura na rede local no intuito de averiguar máquinas que, por ventura, estejam com tal porta lógica fechada. Isto é um indício de que estão desprotegidas por não possuírem o agente AV instalado.

Por exemplo, supondo que os agentes instalados utilizem a porta lógica 7749/TCP, uma opção é utilizar o Nmap (https://nmap.org) na identificação de

máquinas sem o referido agente. No exemplo abaixo, está sendo realizada uma busca da rede 192.168.0.0/24:

```
# nmap -p 7749 192.168.0.0/24
Starting Nmap 6.25 ( http://nmap.org ) at 2015-11-19 11:33 E. South America
Daylight Time
Nmap scan report for 192.168.0.101
Host is up (0.0030s latency).
PORT   STATE SERVICE
7749/tcp open  unknown    ( ← Porta 7749 aberta )
MAC Address: 00:21:29:A8:C5:D4 (Cisco-Linksys)
Nmap scan report for 192.168.0.102
Host is up (0.066s latency).
PORT   STATE  SERVICE
7749/tcp closed unknown    ( ← Porta 7749 fechada )
MAC Address: 00:24:8D:F3:91:11 (Sony Computer Entertainment)
Nmap done: 256 IP addresses (3 hosts up) scanned in 9.41 seconds
```

Cabe salientar novamente que o status “7749/tcp open” apenas é um indício de que a máquina possui o agente AV instalado, pois a porta pode estar sendo utilizada por outra aplicação. No caso de uma resposta “7749/tcp closed”, isto significa que o agente não está presente ou não foi corretamente instalado.

Outro cuidado importante é a integração do seu servidor AV com outros produtos. Caso seja tomada esta decisão, é necessário acompanhar o crescimento do banco de dados do AV, pois à medida que são realizadas interações com outras soluções, o BD pode crescer abruptamente e diminuir o desempenho da aplicação.

No intuito de garantir que somente agentes legítimos do antivírus estabeleçam comunicação com o servidor central, algumas soluções compartilham chaves de autenticação entre este e os agentes instalados nas demais máquinas. Na ocasião de mudança de hardware ou atualização da versão do servidor central de gerenciamento, é crucial o fiel cumprimento do processo de migração das chaves utilizadas. Em caso de falha, as chaves de autenticação compartilhadas com os agentes podem ser perdidas ou corrompidas, gerando assim a necessidade de reinstalação dos agentes AV em todas as máquinas da organização.

4.6 O *SECURITY INFORMATION AND EVENT MANAGEMENT* (SIEM)

Antes de adquirir um SIEM, é necessário realizar um estudo e identificar quais ativos de rede deverão ter seus eventos (*logs*) enviados e analisados por esta ferramenta, pois normalmente os módulos são dimensionados em eventos por segundo (capacidade para capturar, analisar e armazenar corretamente). Além disso, sua configuração demanda tempo e o pleno entendimento da atuação normal da rede. A partir disso, regras e políticas de identificação de comportamento anômalo podem ser criadas de tal maneira que a quantidade de alarmes gerados com falsos positivos tenda a ser reduzida.

O intuito do SIEM é receber eventos gerados por roteadores, *firewalls*, *proxies*, servidores antivírus, sistemas de detecção de intrusos, dentre outros equipamentos, agregá-los, correlacioná-los e apresentar uma informação útil ao administrador da rede. As regras de correlação contêm condições definidas que correlacionam eventos à medida que estes são processados na ferramenta (SILVA, 2011).

Devido a esta variedade e quantidade de dados a serem trabalhados, a escolha de membros com relevante conhecimento da rede tende a facilitar o trabalho da equipe. Com o SIEM, podem ser gerados relatórios, alarmes e respostas automatizadas. Por exemplo, repetitivas tentativas sem sucesso de acesso remoto a um *firewall* podem ser identificadas e, com isso, sua origem pode ser bloqueada com a utilização desta funcionalidade.

O posicionamento físico do SIEM deve levar em consideração dois aspectos fundamentais. O primeiro está relacionado à quantidade de tráfego (*logs*) que será enviada, pois em função da distância onde estão instalados os ativos de rede que enviaram suas informações, este fluxo de dados poderá sobrecarregar a rede, deixando-a lenta. O outro fator tem correlação de como trafegam os dados na rede, pois as informações enviadas (*logs*) ficam passíveis de serem interceptadas com o uso de *sniffers* (ver item 2.2.3) e analisadas por terceiros.

Segundo Michael Gabriel, CISO da *Career Education Corporation,* no processo de seleção de eventos a serem monitorados pelo SIEM, um administrador deve levar em consideração as informações advindas dos ativos utilizados no perímetro de rede, dos sistemas operacionais, de bancos de dados existentes e dados de camada de aplicação. Estas informações são bastante relevantes quando desejamos ter uma correta visão situacional da segurança da rede (DUBIE, 2015).

4.7 AS POLÍTICAS DE SEGURANÇA APLICADAS AOS USUÁRIOS

As políticas de segurança são gerenciadas em um servidor central e aplicadas aos computadores da organização, por meio de um agente instalado, sem a necessidade de intervenção do usuário. Por razões de segurança, a falta de conectividade desses agentes com o servidor de políticas, impede que o computador

seja disponibilizado ao usuário no momento do seu *login*, por isso a arquitetura deve prever a existência de servidores secundários em filiais remotas.

Por meio desse agente instalado, é oferecida uma camada de proteção adicional aos computadores, controlando as permissões de sua utilização pelos usuários. Um exemplo desta aplicação, é o controle de dispositivos USB (a partir do número de série) que podem propagar vários programas maliciosos (vírus e *worms*), quando infectados. Além disso, com a utilização de dispositivos USB, dados sigilosos poder cair em mão de terceiros, seja pela cópia indevida (intencional) ou pela sua perda com dados armazenados sem a devida criptografia aplicada.

Para redes sem fios, há soluções que possibilitam aplicar permissões levando em consideração a localização do usuário, desabilitar a *interface* de redes sem fio quando o computador estiver conectado via cabo e criar uma lista de pontos de acesso *wireless* permitidos.

Podem ser criadas ainda políticas de acesso a arquivos locais, gerenciamento de energia, gerenciamento de impressoras, acesso remoto (execução de sessão), grupos do Windows, dentre outras. A política de bloqueio de dispositivos de mídia removível é especialmente útil no contexto militar, governamental e em outros contextos sensíveis a espionagem e roubo de informações sigilosas (BEACHEM, 2014).

4.8 AS FILIAIS

Na presente topologia, há duas filiais conectadas à Matriz por meio de uma infraestrutura de rede MPLS. Foi criada uma VPN gerenciada pelo administrador da organização, no intuito de prover uma camada de criptografia ao tráfegos de dados no MPLS, a fim de atender ao requisito confidencialidade das informações.

Apesar de redes MPLS apresentarem alta disponibilidade, *links* redundantes de internet podem ser contratados. Além disso, deve ser prevista uma infraestrutura mínima de rede que permita a continuidade de trabalho nas filiais remotas, caso seja perdida a conectividade com a matriz. Para esta situação, as filiais podem possuir serviços secundários de DNS, correio eletrônico, árvore de diretório e servidor de política de usuários, por exemplo.

O serviço de árvore de diretório é necessário para que um usuário consiga conectar-se ao domínio da organização. Cabe salientar que, após efetuar este *login* na rede, o computador compulsoriamente consulta o servidor de políticas de segurança aplicadas aos usuários para verificar quais permissões o indivíduo possui e, só assim, disponibilizar a máquina ao indivíduo. O serviço de DNS local, propiciaria a resolução de nomes de serviços existentes na filial e o correio permitiria o acesso às mensagens de e-mail atualmente existentes.

4.9 CONCLUSÃO

O objetivo deste capítulo foi elencar questões relevantes à SID em função da arquitetura apresentada na seção 4.1. Existem outras possíveis topologias e tecnologias disponíveis que poderiam ser empregadas, mas as elencadas nesta obra forem escolhidas no intuito de apresentar conceitos iniciais a profissionais de segurança de redes.

Todos os equipamentos utilizados na segurança devem ter suas configurações e regras criteriosamente realizadas e, se possível, revistas por um segundo profissional, principalmente aquelas presentes nos equipamentos de borda com a Internet. Falhas de configuração nestes dispositivos podem comprometer ou colocar em risco ativos importantes do ambiente corporativo.

5 **CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS**

A segurança em redes é uma atividade contínua pela busca de melhorias, uma vez que as técnicas e ferramentas utilizadas por potenciais invasores estão em constante evolução. A topologia, princípios e ferramentas expostos neste trabalho visam servir de alicerce para que cada administrador busque a topologia e ferramentas adequadas a sua realidade.

Em organizações onde, devido ao fluxo de carreira, há uma rotatividade considerável dos membros que ocupam função específica na segurança da rede, é necessário acelerar o aprendizado de novos indivíduos que venham a ocupar lugar nesta área. Cotidianamente, são divulgadas novas falhas e vulnerabilidades em programas e sistemas operacionais, entretanto o ambiente computacional de uma organização deve estar sempre pronto a resistir a tal situação.

5.1 CONSIDERAÇÕES FINAIS

A sequência dos assuntos abordados neste trabalho procurou inicialmente inserir o leitor no espaço cibernético, demonstrando possíveis técnicas de ataques e golpe utilizados na Internet. Assim, o profissional de TI que, por ventura, seja designado para trabalhar com segurança de redes ambientar-se-á com os perigos aos quais estará submerso.

Em seguida, são apresentados conceitos sobre dispositivos de redes, ferramentas de segurança e serviços que podem estar presentes em um ambiente corporativo. Para cada um destes, quando aplicável, são apresentadas concepções básicas e orientações sobre seus princípios de funcionamento.

Por fim, é exposta uma topologia que visa demonstrar como as funcionalidades dos diversos dispositivos de rede podem ser utilizados de forma complementar, aumentando a SID da organização. Em várias oportunidades, serviços de rede deixam de exercer seu papel a contento e a culpa logo recai sobre os *firewalls* e demais mecanismos de segurança. Neste caso, um entendimento global do ambiente computacional tende a facilitar a resolução de problemas (*troubleshooting*).

5.2 TRABALHOS FUTUROS

Quanto aos trabalhos futuros, o intuito é realizar pesquisas relacionadas à prevenção contra perda de dados (*Data Loss Prevention* – DLP), utilização de códigos (*scripts)* que automatizem tarefas recorrentes de segurança e monitoramento e o estudo de políticas de correlação de eventos relacionadas a dispositivos SIEM (*Security Information and Event Management*).

A cultura de prevenção contra perda de dados vem crescendo no intuito de bloquear o envio de dados sigilosos para fora da organização. Uma possível opção é a adoção de uma política de bloqueio a serviços de correio Web (Gmail e Yahoo Mail, por exemplo), onde arquivos podem ser facilmente anexados e enviados. Entretanto, soluções de DLP mais poderosas e complexas baseadas em software e hardware podem ser utilizadas a fim de proibir tais fluxos de informações.

Por sua vez, o uso de *scripts* tende a facilitar a vida de um administrador de redes. Por exemplo, o *Shell script* é uma poderosa ferramenta que pode ser utilizada na automatização de vários processos, tais como: análise contínua de páginas Web contra alterações maliciosas (*defacement*), monitoramento de ativos de rede, análise de eventos (*logs*) de diversos ativos e realização de teste de penetração. Existem

inúmeras tarefas em segurança que podem ser supervisionadas com a utilização de códigos, cabendo ao analista identificá-las e utilizar a programação a seu favor.

Por fim, o SIEM é encarado por muitos como uma ferramenta essencial para a gestão da segurança. Um estudo sobre como criar políticas que analisem uma grande quantidade de eventos enviados por diversos dispositivos de rede, minimizando a taxa de falsos positivos gerados é crucial. Para o analista de segurança, é essencial entender como seu ambiente de rede funciona e, a partir disso, configurar regras adequadas e eficazes, de modo a identificar comportamentos maliciosos eficazmente.

REFERÊNCIAS

ALVES, L. C. M.; MOREIRA, J.. **Gerenciamento da Política da Segurança da Informação.** Revista TIS, v. 1, n. 2, 2012.

ANDRESS, J.; WINTERFELD, S. **Cyber warfare: techniques, tactics and tools for security practitioners**. Elsevier, 2013. p. 2.

ARAVINDHAN, K.; KARTHIGA, R. R. **One Time Password: A Survey.** International Journal of Emerging Trends in Engineering and Development, v. 1, n. 3, p. 613-623, 2013.

ASHOOR, A. S.; GORE, S. **Importance of Intrusion Detection system (IDS).** International Journal of Scientific and Engineering Research, v. 2, n. 1, p. 1-4, 2011.

BEACHEM, B. R. **Securing a network connection by way of an endpoint computing device.** U.S. Patent n. 8,838,804, 16 set. 2014.

BELARMINO, V. F.; ARAÚJO, W. J. **Análisis de vulnerabilidades computacionales en repositórios digitales**. Revista de Bibliotecología y Ciencias de la Información, n. 56, p. 1-18, 2015.

Biswas, K. P. *et al.* **Method and apparatus for making end-host network address translation (NAT) global address and port ranges aware.** U.S. Patent n. 8,019,889, 13 set. 2011.

BRITO, C. T.; *et al.* **Single Sign-On: um estudo de caso em banco de dados Oracle.** Revista Brasileira de Computação Aplicada, v. 4, n. 2, p. 28-41, 2012.

BRUCKER, A. D.; BRÜGGER, L.; WOLFF, B. **Formal firewall conformance testing: an application of test and proof techniques.** Software Testing, Verification and Reliability, v. 25, n. 1, p. 34-71, 2015.

CAMPISTA, M. E. M. et al. I**nterconexão de Redes na Internet do Futuro: Desafios e Soluções.** Minicursos do Simpósio Brasileiro de Redes de Computadores-SBRC, v. 2010, p. 47-101, 2010.

CARRARA, L. H.; BELLEZI, M. A. **Gerenciamento Centralizado de Servidor com OpenLDAP e Interface GOsa.** Revista TIS, v. 3, n. 1, 2014.

CERT.BR, **Estatísticas dos Incidentes Reportados ao CERT.br.** Disponível em http://www.cert.br/stats/incidentes/. Acesso em 04 jun. 2015a.

_____. **Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2014.** Disponível em http://www.cert.br/stats/incidentes/2014-jan-dec/tipos-ataque.html. Acesso em 05 jun. 2015b.

_____. **Cartilha de Segurança para Internet - Parte IV: Códigos maliciosos (Malware).** Disponível em http://cartilha.cert.br/malware/. Acesso em 02 nov. 2015c.

_____. **Cartilha de Segurança para Internet - Parte III: Ataques na Internet.** Disponível em http://cartilha.cert.br/ataques/ . Acesso em 02 nov. 2015d.

_____. **Cartilha de Segurança para Internet - Parte II: Golpes na Internet.** Disponível em http://cartilha.cert.br/golpes/. Acesso em 02 nov. 2015e.

_____. **Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos**. Disponível em http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/. Acesso em 03 out. 2015f.

CISCO. **Características e configurações básicas do Port Security.** 2015. Disponível em https://supportforums.cisco.com/pt/document/111081. Acesso em 13 set. 2015.

CITRIX SYSTEMS, **Workplace of the Future: A Global Market Research Report,** Fort Lauderdale, Florida, 2012. Disponível em https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/workplace-of-the-future-a-global-market-research-report.pdf. Acesso em 04 jun. 2015.

CSIRT-UNICAMP. **Boas Práticas em Configuração de switches de camada 2.** 2015. Disponível em https://www.security.unicamp.br/89-boas-praticas-em-configuracao-de-switches-de-camada-2.html Acesso em 13 set. 2015.

DE CARVALHO, F. R. et al. **Vulnerabilidades em aplicações Web.** RE3C-Revista Eletrônica Científica de Ciência da Computação, v. 8, n. 1, 2013.

DORIGO, S. **Security Information and Event Management.** Dissertação. (Mestrado em Segurança da Informação) Nijmegen, Holanda .2012.

DUBIE, D. **Best practices for a successful SIM deployment.** Disponível em http://www.pcworld.com/article/144638/guide_security_information_management.html. Acesso em 19 nov. 2015.

FERREIRA, A. S. **O Monitoramento Eletrônico do Teletrabalhador Brasileiro.** Instituto Brasileiro de Direito Eletrônico. Disponível em: http://www.telework2010.tic.org.ar/papers/simeao%20ferreira%20portugues.pdf. Acesso em abril de 2013.

FIGUEIREDO, R. N. **Avaliação de algoritmos de controle de congestionamento como controle de admissão em um modelo de servidores web com diferenciação de serviços.** Tese de Doutorado. Universidade de São Paulo, 2011.

FILIPPETTI, M. A. **CCNA 4.1 Guia Completo de Estudo.** Visual Books, Florianópolis, p. 242, 2008. F

FREITAS, M. A. S. **Fundamentos do gerenciamento de serviços de TI.** 2a. Ed. Brasport, 2013. p 343.

GHARIBI, W; MIRZA, A. **Security Risks and Modern Cyber Security Technologies for Corporate Networks.** (IJCSIS) International Journal of Computer Science and Information Security, Vol. 9, No. 1, p. 166. 2011

HOQUE, M. S.; MUKIT, M. A.; BIKAS, A. N. **An implementation of intrusion detection system using genetic algorithm.** International Journal of Network Security & Its Applications, Volume 4, Number 2, pages 109 - 120, March 2012.

IANA. **Service Name and Transport Protocol Port Number Registry.** Disponível em http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml. Acesso em 17 nov. 2015.

INFOMACH. **Proteção total de e-mail para as grandes empresas.** Disponível em http://www.infomach.com.br/produtos/EmailGateway.php?aba=0. Acesso em 23 OUT. 2015.

JUNG, E. V. ; PELLIS, R. R. **Aplicando segurança em redes locais através de gerenciamento de ativos de rede.** Disponível em: www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS11/Edson%20Venicius %20Jung%20_%20Edson%20Venicius%20Jung.pdf. Acesso em 04 jun. 2015.

KHANDELWAL, et al. **Frontline techniques to prevent web application vulnerability.** International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), v. 2, n. 2, p. pp: 208-213, 2013.

KINDY, D. A.; PATHAN, A. K. **A Survey on SQL Injection: Vulnerabilities, attacks, and Prevention Techniques.** IEEE 15th International Symposium on Consumer Electronics, pp 468-471, 2011.

KUROSE, J. F.; ROSS, K. W. **Computer networking : a top-down approach.** 6a Ed. Pearson, p. 476, 2013a.

_____. **Computer networking : a top-down approach.** 6a Ed. Pearson, p. 480, 2013b.

_____. **Computer networking : a top-down approach.** 6a Ed. Pearson, p. 732, 2013c.

MACÊDO, D. **Conceito de Filtragem de Pacotes e Firewall.** 2012. Disponível em http://www.diegomacedo.com.br/conceito-de-filtragem-de-pacotes-e-firewall. Acesso em 06 jan. 2016.

MACÊDO, M. A.; QUEIROZ, R. J. G. B.; DAMASCENO, J. C. **Uma Ferramenta Adaptativa Baseada em Agentes Móveis Inteligentes para Segurança de Aplicações Web.** VII Simpósio Brasileiro de Sistemas de Informação, p. 105-116, 2011.

MALTINTI, L. C.; MALTINTI, J. C. **Monitoramento do Correio Eletrônico nas Relações de Trabalho.** XIX Encontro Nacional do CONPENDI, 2010.

MICROSOFT. **O que é Active Directory, topologia física e lógica?** Disponível em https://technet.microsoft.com/pt-br/library/jj206711.aspx. Acesso em 16 nov. 2015.

_____. **Etapa 3: Configurar o WSUS.** Disponível em https://technet.microsoft.com/pt-br/library/hh852346.aspx. Acesso em 17 nov. 2015b.

OWASP, **Web Application Firewall.** Disponível em https://www.owasp.org/index.php/Web_Application_Firewall. Acesso em 12 out. 2015.

RAD, B.B.; MASROM, M.; IBRAHIN, S. **Evolution of computer virus concealment and anti-virus techniques: a short survey.** International Journal of Computer Science Issues - IJCSI Volume 8, Ed. 1, 2011.

RAGHAV, I; CHHIKARA, S.; HASTEER, N. **Intrusion Detection and Prevention in Cloud Environment: A Systematic Review.** International Journal of Computer Applications, v. 68, n. 24, p. 7-11, 2013.

RIBEIRO, C. H. **Implantação de um sistema integrado para autenticação segura de usuários e permissão de acesso em um proxy transparente.** Monografia. Universidade Federal de Lavras, MG. 2007.

ROŞU, M. S.; DRĂGOI, G. **VPN solutions and network monitoring to support virtual teams work in virtual enterprises.** Computer Science and Information Systems, v. 8, n. 1, p. 1-26, 2011.

SILVA, N. R. L. **Método de implementação de SIEMs: resultados de experiências práticas.** Tese de Mestrado. Universidade do Minho, Braga, Portugal. 2011.

SOUZA, P. R; SOUSA, J. R. **Segurança em redes: Implementando Servidores Proxy e Firewall em GNU/Linux.** Engenharia de Computação em Revista, v. 1, n. 4, Belém – PA. 2010.

STIAWAN, D.; ABDULLAH, A. H.; IDRIS M. Y. **Characterizing Network Intrusion Prevention System.** International Journal of Computer Applications, v. 14, n. 1, p. 11-18, 2011.

STRONGSECURITY, **O que é um SIEM?.** Disponível em http://www.strongsecurity.com.br/portal/o-que-e-um-siem/. Acesso em 05 OUT. 2015.

TANENBAUM, A. S.; WETHERALL, D. J. **Computer Networks: Pearson New International Edition.** University of Hertfordshire. Pearson Higher Ed, 2013, p. 54.

UTO, N.; MELO, S.P. **Vulnerabilidades em Aplicações Web e Mecanismos de Proteção.** Minicursos SBSeg 2009. IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, Campinas, São Paulo, Brazil, 2009. p. 237.