UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

DOUGLAS EDUARDO BASSO

ANÁLISE DE SOLUÇÕES UTM E AMEAÇAS DIGITAIS

MONOGRAFIA

CURITIBA
2015

DOUGLAS EDUARDO BASSO

ANÁLISE DE SOLUÇÕES UTM E AMEAÇAS DIGITAIS

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de servidores e equipamentos de rede, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná – UTFPR.
Orientador: Prof. Dr. Augusto Foronda.

CURITIBA
2015

RESUMO

BASSO, Douglas E. **Análise de Soluções UTM e Ameaças Digitais.** 2015. 70 páginas. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

Num passado não tão distante, os usuários corporativos passivamente acessavam as informações da empresa em seus terminais e estações de trabalho. Com a chegada dos notebooks, foi possível ter uma maior mobilidade, que cresceu exponencialmente com a adoção dos smartphones e tablets pessoais, além de aumentarem a produtividade, trazem a tão sonhada “liberdade”, livre das políticas restritivas de segurança das empresas. A tecnologia cresceu, os computadores e os usuários evoluíram e a internet mudou. Essa mudança trouxe vários benefícios: serviços nas nuvens, redes sociais, comunicação entre pessoas, compras online, transações bancárias, dentre outros. Tudo isso não só no computador pessoal, mas também no ambiente corporativo. Algumas dessas aplicações se tornaram indispensáveis no nosso dia a dia, são elas: Skype,Google Docs, Facebook, Youtube, Twitter e muitos outros serviços. Mas como controlar tudo isso? Soluções separadas têm visões limitadas do tráfego, ou até mesmo a utilização de tecnologias antigas e atuais com o conceito “do tudo ou nada” não são mais eficientes. Não há mais como simplesmente bloquear o acesso corporativo a todas estas aplicações, porém permitir o acesso não inspecionado mesmo que para grupos específicos, como normalmente é realizado hoje em dia, representa uma séria ameaça à segurança das redes corporativas. Surgem então novas exigências para um firewall. Dentro desse contexto podemos destacar os firewalls UTM que é uma nova tecnologia abrangente de segurança de rede que se tornou a principal solução de proteção corporativa nos últimos anos. A segurança UTM é a evolução do tradicional firewall para uma solução de segurança mais robusta e completa, capaz de executar várias funções em um único dispositivo: firewall de rede, prevenção de intrusos de rede, antivírus, filtragem antispam, VPN, balanceamento de carga, prevenção de vazamento de dados, entre outros.

Palavras-chave: Redes de Computadores, Segurança da Informação, Firewall, UTM.

ABSTRACT

BASSO, Douglas E. **UTM solutions analysis and digital threats.** 2015. 70 pages. Monograph (Specialization in Configuration and Management of Servers and Network Equipments) - Federal Technological University of Paraná. Curitiba, 2015.

In a not-so-distant past, business users passively accessing the information of the company in its terminals and workstations. With the arrival of the notebooks, it was possible to have greater mobility, which grew exponentially with the adoption of smartphones and tablets, as well as increasing personal productivity, bring the much vaunted "freedom", free of restrictive security policies of companies. The technology grew, the computers and users have evolved and the internet has changed. This change brought many benefits: services in the cloud, social networks, communication between people, online shopping, banking, among others. All this not only in the personal computer, but also in the corporate environment. Some of these applications have become indispensable in our daily lives, they are: Skype, Google Docs, Facebook, Youtube, Twitter and many other services. But how to manage all this? Separate solutions have limited visions of traffic, or even the use of old technologies and current with the concept of "all or nothing" are no longer effective. There is no longer as simply block access to all these corporate applications, but allow access not inspected even if for specific groups, as is usually done nowadays, poses a serious threat to the security of enterprise networks. Arise then new requirements for a firewall. Within this context we can highlight the UTM firewalls which is a new comprehensive network security technology which became the main corporate protection solution in recent years. Roughly, the UTM security is the evolution of the traditional firewall for a more robust security solution and complete, able to perform multiple functions in a single device: network firewalling, network intrusion prevention, anti-virus, anti-spam filtering, VPN, load balancing, data leak prevention, among others.

Keywords: Networks, Firewall, Information Security, UTM.

LISTA DE SIGLAS

ARPA - Advanced Research Projects Agency

ARP - Address Resolution Protocol

ASP - Active Server Pages

CSS - Cascading Style Sheets

DLP - Data Loss Prevention

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

FTP – File Transfer Protocol

HTML – Hyper Text Markup Language

HTTP - Hypertext Transfer Protocol

ICMP - Internet Control Message Protocol

IDS - Intrusion Detection System

IP – Internet Protocol

ISO – International Organization for Standardization

JSP – Java Server Pages

LAN – Local Area Network

LLC - Logical Link Control

MAC - Media Access Control

Mbps - Megabits por Segundo

MPLS - Multi-Layer Protocol Label Switching

NAT - Network Address Translation

OSI - Open Systems Interconnection

OSPF - Open Shortest Path First

PCI - Protocol Control Information

PHP - Hypertext Preprocessor

POP - Post Office Protocol

QoS – Quality of Service

RFC - Request for Comments

RIP - Routing Information Protocol

SSH - Secure Shell

SSID - Service Set Identifier

SSL - Secure Sockets Layer

SMB - Server Message Block

SMTP - Simple Mail Transfer Protocol

TCP - Transmission Control Protocol

TCP/IP - Transmission Control Protocol over Internet Protocol

TI – Tecnologia da Informação

UDP - User Datagram Protocol

UTM - Unified Threat Management

VPN – Virtual Private Network

WAN - Wide Area Network

WEB - World Wide Web

WLAN – Wireless Local Area Network

LISTA DE ILUSTRAÇÕES

Figura 1 Comunicações e Redes de Dados 18
Figura 2 Serviços de Redes de Dados 18
Figura 3 Comunicação em Camadas e Modelo OSI 20
Figura 4 Aplicações e Serviços 20
Figura 5 Camadas do Modelo OSI 21
Figura 6 Camadas do Modelo TCP/IP 22
Figura 7 Funcionalidades UTM 36
Figura 8 Acelerador de WAN 43
Figura 9 Comparativo Firewalls UTM e Firewalls de Nova Geração 47
Figura 10 Quadrante Mágico para UTM (Unified Threat Manangement) 48
Figura 11 Logotipo Watchguard 49
Figura 12 Equipamentos Watchguard 49
Figura 13 Logotipo Sophos 50
Figura 14 Equipamentos Sophos 50
Figura 15 Logotipo Dell Sonicwall 51
Figura 16 Equipamentos Dell Sonicwall 52
Figura 17 Logotipo Aker 54
Figura 18 Equipamento Aker 54
Figura 19 Logotipo Stormshield 56
Figura 20 Equipamentos Stormshield 56
Figura 21 Stormshield Security Cloud 57
Figura 22 Logotipo Cyberoam 57
Figura 23 Equipamentos Cyberoam 58
Figura 24 Cyberoam Netgenie 58
Figura 25 Logotipo Cisco 59
Figura 26 Equipamentos Cisco 59
Figura 27 Logotipo Juniper Networks 60
Figura 28 Equipamentos Juniper Networks 61
Figura 29 Logotipo Palo Alto Networks 62
Figura 30 Equipamentos Palo Alto Networks 63

Figura 31 Logotipo Fortinet 63
Figura 33 Circuitos ASIC Fortinet..... 64
Figura 33 Portfólio de Produtos Fortinet..... 64
Figura 34 Equipamentos Fortinet 65

SUMÀRIO

1 INTRODUÇÃO 11
1.1 TEMA 11
1.2 PROBLEMAS E PREMISSAS 12
1.3 OBJETIVOS 14
1.3.1 OBJETIVO GERAL 14
1.3.2 OBJETIVOS ESPECÍFICOS 14
1.4 JUSTIFICATIVA 14
1.5 PROCEDIMENTOS METODOLÓGICOS 15
1.6 ESTRUTURA 16
2 REFERENCIAIS TEÓRICOS 17
2.1 REDES DE DADOS E A INTERNET 17
2.2 MODELO DE REFERÊNCIA OSI 19
2.3 MODELOO DE REFERÊNCA TCP/IP 21
2.4 UM POUCO DE SEGURANÇA DA INFORMAÇÃO 22
2.4.1 PRINCIPIO DA CONFIDENCIALIDADE 22
2.4.2 PRINCIPIO DA INTEGRIDADE 22
2.4.3 PRINCIPIO DA DISPONIBILIDADE 23
2.5 TESTES DE INSTRUSÃO 23
2.5.1 RECONHECIMENTO 23
2.5.2 VARREDURA 24
2.5.3 ENUMERAÇÃO 25
2.5.4 FALHAS E PROBLEMAS 26
2.5.5 BURLANDO PROTEÇÕES 28
2.5.6 ENGENHARIA SOCIAL 29
2.5.7 TRUQUES APLICADOS NA INFORMÁTICA 30
2.5.8 MALWARE 31
2.5.9 SENHAS 32
2.5.10 SNIFFERS 33
2.5.11 ATAQUE DE NEGAÇÃO OU RECUSA DE SERVIÇOS 34

3 UTM 36
3.1 EVOLUÇÃO DAS REDES 37
3.2 FUNCIONALIDADES DOS FIREWALLS UTM 39
3.2.1 CONTROLE DE APLICAÇÕES 39
3.2.2 ANTIVIRUS 40
3.2.3 FILTRO DE CONTEÚDO WEB 41
3.2.4 ANTISPAM 41
3.2.5 ACELERADOR DE WAN 42
3.2.6 VPN 43
3.2.7 IPS 44
3.2.8 DLP 44
3.2.8 RELATÓRIOS GERENCIAIS 44
3.3 UTM VS NGFW 45
3.4 FABRICANTES UTM 47
3.4.1 WATCHGUARD 48
3.4.2 SOPHOS 49
3.4.3 DELL 51
3.4.4 AKER SECURITY SOLUTIONS 54
3.4.5 STORMSHIELD 56
3.4.6 CYBEROAM 57
3.4.7 CISCO 59
3.4.8 JUNIPER 60
3.4.9 PALO ALTO NETWORKS 62
3.4.10 FORTINET 63
4 CONSIDERAÇÕES FINAIS 66
REFERÊNCIAS 68

1 INTRODUÇÃO

Neste capítulo serão tratados os elementos introdutórios relacionados ao estudo e análise sobre a utilização das redes de computadores e internet com uma ótica voltada para a questão da segurança da informação e as possíveis ameaças que o mundo digital apresenta a cada dia.

As mudanças no mundo acontecem rapidamente e se faz necessário responder a essas mudanças o mais rápido possível, com uma abordagem inovadora e eficaz para auxiliar a sua organização a gerenciar os riscos e mantendo o ritmo de crescimento com desenvolvimento tecnológico. As redes tornaram-se vulneráveis devido a alguns fatores fundamentais:

- Cenário dos aplicativos
- Comportamento dos usuários
- Dinâmica da segurança cibernética
- Mudanças na infraestrutura

A computação em nuvem, a evolução da internet, as plataformas sociais e a explosão de aplicativos estão presentes em todos os lugares do mundo. O uso dos dispositivos móveis e a virtualização de equipamentos estão mudando a arquitetura das infraestruturas de TI das corporações. A maneira como os usuários utilizam os recursos da rede e como a empresas gerenciam a área TI fizeram com que muitas redes de computadores ficassem mais vulneráveis a falhas de segurança, perda de dados e informações.

Os produtos tradicionais de segurança de redes são incapazes de controlar esse grande número de aplicativos de última geração, bem como os novos cenários de segurança da informação, os novos comportamentos dos usuários e a infraestrutura como um todo. É a hora de adotar uma abordagem totalmente nova para a segurança das redes corporativas.

1.1 TEMA

As guerras sempre fizeram parte da história da humanidade. A necessidade de defender-se dos inimigos, fez com que as técnicas de defesa fossem criadas e aprimoradas. Uma das mais antigas e utilizadas é a construção de um muro que serviria como barreira física para afastar invasores, demarcar territórios e evitar as derrotas [DIGITAL, 2012].

Vários muros caíram, uns virarão atração turística e outros permanecem de pé. No fim dos anos 80, foi criado o conceito de firewall devido à necessidade de criar restrições de acesso entre redes de dados. Naquela época, o perigo era externo, o medo principal era que um vírus derrubasse toda

a rede, como, aliás, aconteceu por diversas vezes. O perímetro era a referência de defesa.

Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local. Com as mudanças tecnológicas e com o uso de computadores de grande porte, a estrutura de segurança ficou um pouco mais sofisticada, englobando controles lógicos, porém ainda centralizados. Com a chegada dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes e de métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação também adquiriram importância vital para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável [BRASIL, 2007].

A internet cresceu e hoje o cenário é bem diferente. Hoje, as ameaças virtuais estão em qualquer lugar, o antigo perímetro já não existe mais. Foi necessária uma evolução nos firewalls e é preciso acompanhar essa mudança. A utilização de aplicações como o Skype, Google Docs, Facebook e muitos outros serviços estão agregando muito valor e melhorando a produtividade das organizações. A estratégia de negar tudo já não é muito eficiente.

1.2 PROBLEMAS E PREMISSAS

Todos os dias, milhões de brasileiros acessam a Internet, trocam informações e usam serviços tais como: operações bancárias, de comércio eletrônico, serviços públicos federais, estaduais e municipais, de ensino e pesquisa, das redes sociais, dentre outros, constituindo uma ampla rede de atividades digitais [BRASIL, 2010].

A segurança cibernética, desafio do século XXI, vem se destacando como função estratégica de Estado, e essencial à manutenção das infraestruturas críticas de um país, tais como Energia, Defesa, Transporte, Telecomunicações, Finanças, da própria Informação, dentre outras.

Diante de tais desafios, as Nações vêm se preparando, urgentemente, para evitar ou minimizar ataques cibernéticos às redes e sistemas de informação de governo, bem como de todos os demais segmentos da sociedade [BRASIL, 2010].

Dessa forma, o entendimento sobre a importância da segurança cibernética caracteriza-se cada vez mais como condição de desenvolvimento, requerendo para tanto, dentre outras ações, a promoção de diálogos e de intercâmbios de idéias, de iniciativas, de dados e informações, de melhores práticas, para a cooperação no tema, no país e entre países.

Segundo [BRASIL, 2010] entender, portanto, tais movimentos e as respectivas oportunidades e desafios são questões estratégicas que o Estado Brasileiro vem se aprimorando e se organizando para melhorar seu posicionamento tanto no nível nacional quanto, consequentemente, no que se refere à sua inserção internacional, no tema.

Chama a atenção que o chamado espaço cibernético, não tem suas fronteiras ainda claramente definidas, impacta o dia a dia de todos os dirigentes governamentais, de empreendimentos privados e dos próprios cidadãos.

Na nova conformação da Sociedade da Informação, vale destacar os seguintes fenômenos:

- ✓ Elevada convergência tecnológica;
- ✓ Aumento significativo de sistemas e redes de informação, bem como da interconexão e interdependência dos mesmos;
- ✓ Aumento crescente e bastante substantivo de acesso à Internet e das redes sociais;
- ✓ Avanços das tecnologias de informação e comunicação;
- ✓ Aumento das ameaças e das vulnerabilidades de segurança cibernética;
- ✓ Ambientes complexos, com múltiplos atores, diversidade de interesses, e em constantes e rápidas mudanças.

Neste contexto, as estratégias internacionais no tema apontam para o estabelecimento de parcerias e ações colaborativas efetivas entre países, que propicie a análise, a coordenação, e a integração dos conhecimentos, permitindo, além da correlação entre tais conhecimentos, o entendimento dos impactos que a convergência e a interdependência existentes, e ainda por vir, têm e terão no futuro. Há uma tendência de que tais esforços devam ser suportados por macrocoordenação e governança bem estabelecida, bem como baseados em modelos efetivos e eficazes de colaboração entre governo, setor privado e academia.

Ressaltam-se a transversalidade e particularidade da segurança cibernética, bem como a tendência mundial de destacar as diretrizes estratégicas, os planos e as ações neste tema, além do interesse do Brasil em protagonizar tal tema nos diferentes fóruns internacionais, sendo reconhecidamente um dos protagonistas na arena internacional.

Os desafios da segurança cibernética são muitos, e, portanto, é fundamental desenvolver um conjunto de ações colaborativas entre governo, setor privado, academia, terceiro setor e sociedade, para lidar com o mosaico de aspectos que perpassam a segurança cibernética.

1.3 OBJETIVOS

Nesta sessão serão trabalhados o objetivo geral e objetivos específicos.

1.3.1 OBJETIVO GERAL

O principal objetivo deste projeto é fazer uma pesquisa contextualizada em novas tecnologias e gerações de firewalls e centrais unificadas de gerenciamento de ameaças (UTM)

1.3.2 OBJETIVOS ESPECÍFICOS

- Identificar e destacar as necessidades de segurança digital que a sociedade da informação nos apresenta no panorama atual.
- Descrever os principais ambientes e cenários onde se faz importante à utilização de firewalls de nova geração e centrais unificadas de gerenciamento de ameaças.
- Apresentar o conceito de firewalls de nova geração e centrais unificadas de gerenciamento de ameaças (UTMs).
- Elencar as principais funcionalidades que os UTMs oferecem e como essas funcionalidades se ajusta a realidade das corporações.
- Destacar e analisar os fabricantes de firewalls de nova geração e equipamentos UTM que o mercado de tecnologia de informação oferece na atualidade.
- Comparar os principais equipamentos UTM em relação a funcionalidades e tecnologia.
- Avaliar a viabilidade de utilização dos UTMs nas redes de computadores.
- Fazer uma breve demonstração de acesso, configurações e funcionalidades de alguns UTMs através da utilização de máquinas virtuais.

1.4 JUSTIFICATIVA

Para [MITNICK, 2003] uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe.

Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis.

Segundo [TANENBAUM, 2011] apesar da indústria de informática ainda ser jovem em comparação a outros setores industriais (por exemplo, o de automóveis e o de transportes aéreos), foi simplesmente espetacular o progresso que os computadores conheceram em um curto período de tempo.

Durante as duas primeiras décadas de sua existência, os sistemas computacionais eram altamente centralizados, em geral instalados em uma grande sala com paredes de vidro, através das quais os visitantes podiam contemplar embevecidos, aquela maravilha eletrônica. Uma empresa de médio porte ou uma universidade contava apenas com um ou dois computadores, enquanto as grandes instituições tinham, no máximo, algumas dezenas. Era pura ficção científica a idéia de que, em apenas 20 anos, haveria milhões de computadores igualmente avançados do tamanho de um selo postal.

A fusão dos computadores e das comunicações teve uma profunda influência na forma como os sistemas computacionais eram organizados. O velho modelo de um único computador atendendo a todas as necessidades computacionais da organização foi substituído pelas chamadas redes de computadores, nas quais os trabalhos são realizados por um grande número de computadores separados, mas interconectados.

A segurança corporativa é uma questão de equilíbrio. Pouca ou nenhuma segurança deixa a sua empresa vulnerável, mas uma ênfase exagerada atrapalha a realização dos negócios e inibe o crescimento e a prosperidade da empresa. O desafio é atingir um equilíbrio entre a segurança e a produtividade.

Para [RODRIGUEZ, 2015] os agentes que criam ameaças continuam a demonstrar um alto nível de adaptação e inovação no desenvolvimento de novas e sofisticadas técnicas de ataque. Como resultado, a capacidade de implementar uma arquitetura robusta de segurança de informação exige soluções de segurança de rede que sejam flexíveis e que possam se expandir para incluir novos recursos de proteção e tecnologias de segurança ao longo do tempo.

1.5 PROCEDIMENTOS METODOLÓGICOS

Seguindo a linha de raciocínio de [GIL, 2010] sobre a classificação das pesquisas, levando em consideração os objetivos de cada uma, este trabalho de monografia estará seguindo os procedimentos técnicos de pesquisa

bibliográfica básica estratégica. Pesquisa bibliográfica, pois é uma pesquisa desenvolvida e voltada à aquisição de conhecimentos direcionados a ampla área de segurança de informação com vistas à solução de reconhecidos problemas de segurança digital, pesquisa essa constituída principalmente de livros, artigos científicos e revistas da área tecnológica. A principal vantagem da pesquisa bibliográfica reside no fato de permitir ao investigador a cobertura de uma gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente. Já a análise e os estudos definidos em relação aos firewalls e centrais unificadas de gerenciamento de segurança da informação mostram uma pesquisa exploratória que têm como propósito criar uma maior familiaridade com os problemas e ameaças digitais.

Como consequência, a análise e estudos em relação à gestão unificada de segurança de informação podem ajudar e contribuir com processo de evolução e pesquisa de novas tecnologias aplicadas a segurança da informação. Outra distinção é que no levantamento das informações procura-se identificar todos os componentes e fatores do universo pesquisado, possibilitando a caracterização dessas novas tecnologias de firewalls que chegam para reforçar ainda mais a segurança da informação dentro das redes corporativas e a internet.

1.6 ESTRUTURA

A monografia é composta por 4 capítulos. Primeiramente, o capítulo 1, tratará da parte introdutória, sendo apresentado o tema, os objetivos a serem atingidos, a justificativa da escolha e os problemas a serem resolvidos. Também nesta primeira parte, apresenta-se o embasamento teórico, procedimento metodológico e a estrutura da monografia.

O capítulo 2 trata do referencial teórico do projeto. Teoria sobre redes, modelos de referencia em camadas, conjunto de protocolos e conectividade. Os termos utilizados dentro do contexto de segurança digital, tipos de ataques, técnicas de hackerismo. Este capítulo trará de forma clara e objetiva os conceitos de rede que qualquer administrador deve conhecer antes de aprofundarmos no tema segurança de informação e controle de ameaças.

Partindo para a análise e estudo, o capítulo 3 mostrará as principais características dos firewalls UTM, suas funcionalidades e ferramentas que possibilitam uma gestão integrada de segurança digital contra invasões e ameaças.

Finalizando a monografia, o capítulo 4 traz as conclusões sobre o estudo e análise dos firewalls UTM como um todo e também quesitos comumente vistos após esta sessão, como as referências.

2 REFERENCIAIS TEÓRICOS

2.1 REDES DE DADOS E A INTERNET

Para [FILIPPETI, 2008] estamos em um ponto crucial no uso da tecnologia para estender e fortalecer nossa rede humana. A globalização da Internet tem tido mais sucesso do que jamais poderíamos imaginar. A maneira como as interações sociais, comerciais, políticas e pessoais ocorrem está mudando rapidamente para acompanhar a evolução dessa rede global. No próximo estágio de nosso desenvolvimento, as pessoas usarão a Internet como ponto de partida para seus esforços criando novos produtos e serviços especificamente projetados para tirar vantagem das capacidades da rede. À medida que desenvolvedores aumentam o limite do possível, as capacidades das redes que formam a Internet desempenharão um papel cada vez maior no sucesso desses projetos.

Entre tudo que é essencial para a existência humana, a necessidade de interagir com as outras pessoas está logo abaixo de nossa necessidade de manter a vida. A comunicação é quase tão importante para nós quanto nossa dependência de ar, água, comida e abrigo.

Os métodos que usamos para compartilhar idéias e informações estão em constante mudança e evolução. Enquanto as relações humanas antes eram limitadas a conversas cara a cara, inovações nos meios físicos continuam aumentando o alcance de nossas comunicações. Da imprensa à televisão, cada novidade tem melhorado e aperfeiçoado a nossa comunicação.

Assim como cada avanço na tecnologia da comunicação, a criação e conexão de redes de dados robustas tem tido profundo efeito. As primeiras redes de dados limitavam-se a trocar informações baseadas em caracteres entre sistemas de computadores conectados.

As redes atuais desenvolveram-se a ponto de transferir fluxos de voz, vídeo, texto e gráficos entre diferentes tipos de dispositivos. Formas de comunicação previamente separadas e distintas convergiram em uma plataforma comum. Esta plataforma fornece acesso a uma grande variedade de novos e alternativos métodos de comunicação que possibilitam que as pessoas interajam diretamente entre si quase instantaneamente.

A natureza imediata das comunicações na Internet favorece a formação de comunidades globais. E essas comunidades promovem uma interação social independente de localização ou fuso horário. A existência e a ampla adoção da Internet levaram a novas formas de comunicação que possibilitam que as pessoas criem informações que podem ser acessadas por um público global.

Nosso meio de vida é garantido pelos serviços fornecidos pelas redes de dados, sejam serviços como: reservas de passagens, mensagens instantâneas, entretenimento, jogos online, acesso a blogs, redes sociais, entre outras.

Figura 1: Comunicações e Redes de Dados
Fonte: Cisco Networking Academy – Fundamentos de Redes – Módulo1, Cap. 1, Slide 1.1.2.1, 2012.

Figura 2: Serviços de Redes de Dados
Fonte: Cisco Networking Academy – Fundamentos de Redes – Módulo1, Cap. 1, Slide 1.1.5.1, 2012.

2.2 MODELO DE REFERÊNCIA OSI

Quando as primeiras redes de dados surgiram, computadores de um mesmo fabricante podiam tipicamente comunicar-se entre si. Por exemplo, empresas escolhiam uma solução IBM ou uma solução DEC e nunca ambas, por uma questão de compatibilidade [FILIPPETTI, 2008].

No início da década de 80, a ISO (*International Standards Organization*), juntamente com representantes de diversos fabricantes existentes criou um grupo de trabalho para resolver o problema. Algum tempo depois, em 1984, surgia o primeiro resultado desse esforço: o Modelo de Referência OSI.

Esse modelo se baseia em uma proposta desenvolvida pela ISO como um primeiro passo em direção à padronização internacional dos protocolos empregados nas diversas camadas. Ele foi revisto em 1995. O modelo é chamado Modelo de Referência OSI (*Open Systems Interconnection*), pois ele trata da interconexão de sistemas abertos, ou seja, sistemas que estão abertos à comunicação com outros sistemas. Para abreviar, vamos denominá-lo simplesmente de modelo OSI [TANEMBAUM, 2011].

O modelo OSI tem sete camadas. Veja a seguir um resumo dos princípios aplicados para se chegar às sete camadas:

- Uma camada deve ser criada onde houver necessidade de outro grau de abstração.
- Cada camada deve executar uma função bem definida.
- A função de cada camada deve ser escolhida tendo em vista a definição de protocolos padronizados internacionalmente.
- Os limites de camadas devem ser escolhidos para minimizar o fluxo de informações pelas interfaces.
- O número de camadas deve ser grande o bastante para que funções distintas não precisem ser desnecessariamente colocadas na mesma camada e pequenas o suficiente para que a arquitetura não se torne difícil de controlar.

O modelo de referência Open Systems Interconnection (OSI) é uma representação abstrata em camadas criadas como diretriz para o design de protocolos de rede. O modelo OSI divide o processo de redes em sete camadas lógicas, cada uma com funcionalidades exclusivas e com serviços e protocolos específicos atribuídos a cada camada.

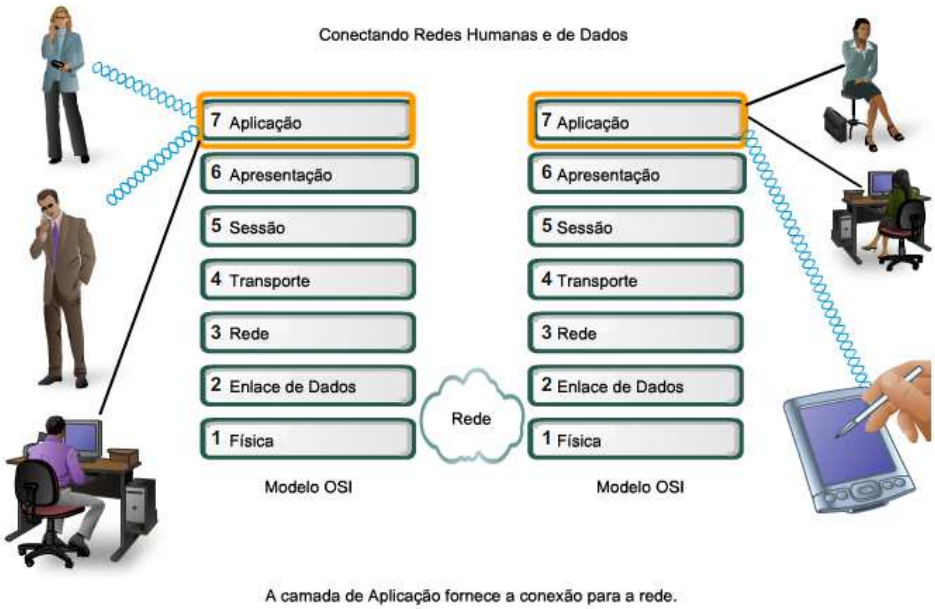

Figura 3: Comunicação em Camadas e Modelo OSI
Fonte: Cisco Networking Academy – Fundamentos de Redes – Módulo1, Cap. 3, Slide 3.0.1.1, 2012.

No modelo OSI, as aplicações que interagem diretamente com pessoas são considerados como estando no topo da pilha, assim como as próprias pessoas. Como todas as camadas dentro do modelo OSI, a camada de aplicação usa as funções nas camadas inferiores para completar o processo de comunicação. Dentro da camada de aplicação, os protocolos especificam que mensagens são trocadas entre os hosts de origem e destino, a sintaxe dos comandos de controle, o tipo e formato dos dados sendo transmitidos e os métodos adequados para notificação de erros e recuperação.

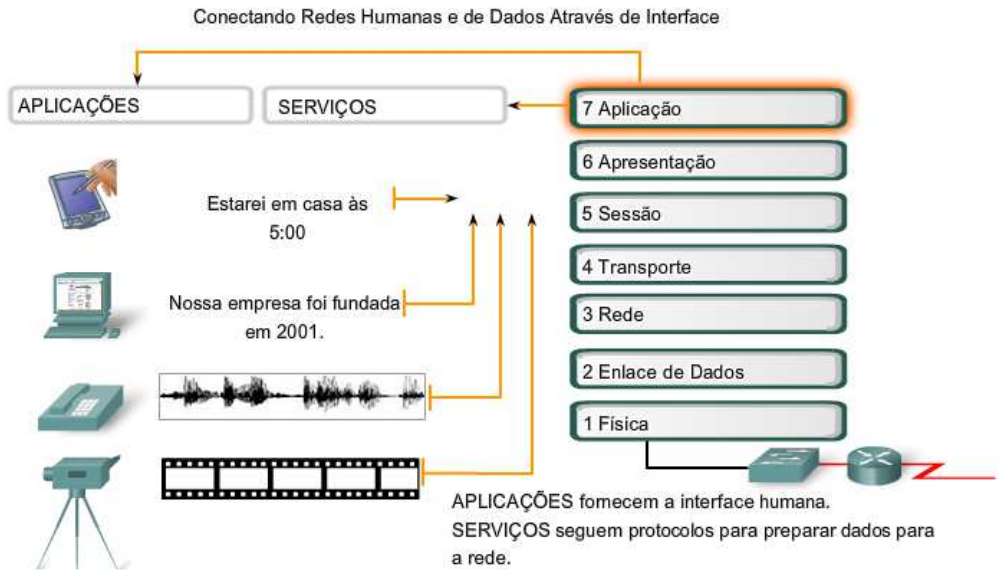

Figura 4: Aplicações e Serviços
Fonte: Cisco Networking Academy – Fundamentos de Redes – Módulo1, Cap. 3, Slide 3.0.1.2, 2012.

Cada protocolo implementa uma funcionalidade assinalada a uma determinada camada. Abaixo uma breve explicação sobre cada camada do modelo OSI:

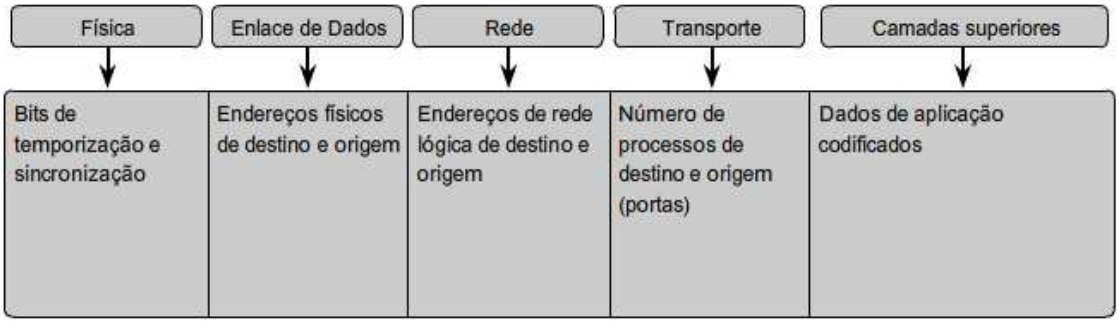

Figura 5: Camadas do Modelo OSI
Fonte: Cisco Networking Academy – Fundamentos de Redes – Módulo1, Cap. 2, Slide 2.5.1.1, 2012.

2.3 MODELO DE REFERÊNCIA TCP/IP

Segundo [ASSUNÇÃO, 2012] o conjunto de protocolos TCP/IP foi desenvolvido pela *Defense Advanced Research Projects Agency* (DARPA). Ele foi criado para fornecer comunicação através da DARPA. Posteriormente, o TCP/IP foi incluído no Berkeley Software Distribution da Unix. Os Estados Unidos desenvolveram o TCP/IP porque desejavam uma rede que pudesse sobreviver a qualquer guerra ou conflito. Seja qual for o meio físico (cabos, fibras ópticas, micro-ondas, satélites), a meta é que os pacotes cheguem sempre ao seu objetivo. Utilizando essa tecnologia, a Internet foi criada.

Para [GALVÃO, 2013] as regras (protocolos) para o funcionamento adequado das redes de computadores são definidas segundo o modelo estrutural utilizado. Na grande maioria das redes é utilizada a pilha de protocolos TCP/IP.

A pilha de protocolos TCP/IP, ou simplesmente TCP/IP, é um conjunto de protocolos de comunicação entre equipamentos computacionais e tem esse nome em função dos seus principais protocolos: o TCP (*protocolo de controle de transmissão*) e o IP (*protocolo de internet*).

Esse modelo é estruturado em camadas, em que cada camada é responsável por um conjunto de tarefas, fornecendo funcionalidades e serviços bem definidos para os protocolos das camadas adjacentes. As camadas superiores (mais próximas do usuário) manipulam dados mais abstratos, enquanto nas camadas mais inferiores as tarefas têm menor nível de abstração.

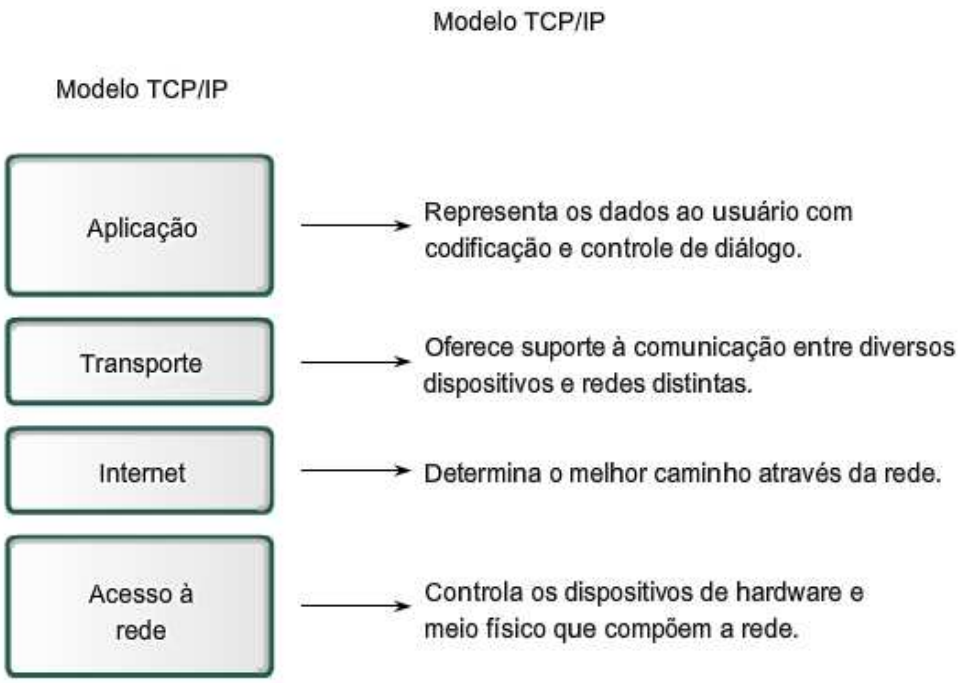

Figura 6: Camadas do Modelo TCP/IP
Fonte: Cisco Networking Academy – Fundamentos de Redes – Módulo1, Cap. 2, Slide 2.4.3.1, 2012.

2.4 UM POUCO DE SEGURANÇA DA INFORMAÇÃO

Para [GIAVAROTO, 2013] quando falamos de segurança da informação, estamos no referindo a um dos ativos mais importantes de uma organização. A informação embutida em todos os processos constitui elemento crucial na tomada de decisões e, consequentemente, pode gerar ganhos e perdas.

A tríade da segurança da informação se baseia nos princípios da Confidencialidade, Integridade e Disponibilidade. É de fundamental importância que administradores de rede e sistemas estejam envolvidos e que conheçam esses princípios de segurança da informação.

2.4.1 PRINCIPIO DA CONFIDENCIALIDADE

Define que somente pessoas autorizadas poderão acessar determinada informação, isso significa que, se alguém, intencionalmente ou não, acessar determinado sistema sem autorização, estará violando o princípio da confidencialidade.

2.4.2 PRINCIPIO DA INTEGRIDADE

Uma informação que esteja íntegra e sem alterações pode ser considerada confiável. Porém, a quebra da integridade pode ocorrer quando a

informação é adulterada, intencionalmente ou não, e, com isso, a informação perde a confiabilidade.

2.4.3 PRINCIPIO DA DISPONIBILIDADE

Define que a informação deverá estar disponível a quem esteja autorizado sempre que for necessário. Podemos citar como quebra da disponibilidade um ataque de negação de serviço contra um servidor, tal ataque faria com que o equipamento parasse de funcionar e, com isto, a informação ficaria indisponível.

2.5 TESTES DE INSTRUSÃO

Segundo [ASSUNÇÃO, 2012] antes de iniciar o ataque propriamente dito, um candidato a invasor tem que passar por algumas etapas nas quais irá conhecer mais sobre o alvo, descobrir computadores ativos, enumerar possíveis usuários e falhas ou mesmo rotas de acesso àquele sistema. Essas etapas anteriores ao ataque são determinantes do sucesso ou fracasso da tentativa.

Para realizar de modo eficiente um Teste de Penetração (*Penetration Test*), que é extremamente necessário para se mantiver uma boa segurança em um sistema, é importante seguir algumas as etapas para que um invasor consiga o máximo possível de eficiência.

2.5.1 RECONHECIMENTO

Segundo [GIAVAROTO, 2013], a técnica de reconhecimento advém de táticas militares em que o terreno deve ser estudado de forma estratégica antes que seja atacado. Nas táticas de reconhecimento, muitas informações podem ser extraídas através de recursos públicos disponíveis na Internet. Os tipos de reconhecimento podem ser passivos ou ativos:

- *Reconhecimento Passivo*: reúne informações relativas ao alvo através de ferramentas públicas disponíveis, como a Internet.

- *Reconhecimento Ativo*: reúne informações através de visitas, engenharia social, entrevistas ou questionários.

Incluímos recursos de mapeamento de redes e consultas a bancos de dados *Whois*, ferramentas que se destacam como: *Netifer, Fingerprint, Fierce, Dnsrecon, Dnsmap, Dnsenum, Genlist*, além de sites como o Google. Alguns dos inúmeros tipos de informações que um atacante poder coletar:

a) Informações envolvendo redes de computadores:

- ✓ Blocos (*ranges*) de IP.
- ✓ Serviços rodando em uma rede.
- ✓ Nomes de domínios.
- ✓ Protocolos.

b) Mecanismos de autenticação:

- ✓ Informações relacionadas a sistemas.
- ✓ Banners com descrição de versões.
- ✓ Informações sobre grupos e nomes de usuários.
- ✓ Arquitetura de sistemas.
- ✓ Senhas e chaves de acesso.

c) Informações relativas a colaboradores:

- ✓ Nome de empregados.
- ✓ Endereços e telefones.
- ✓ Sites.
- ✓ Artigos.
- ✓ Formação, especialização e etc.

Solução: O problema do reconhecimento não é fácil de ser resolvido, mas podem-se tomar alguns cuidados que minimizarão esse problema [ASSUNÇÃO, 2012]:

- ➢ Evitar que informações importantes sejam colocadas desnecessariamente nos websites corporativos, como e-mails e configurações de rede.
- ➢ Procurar sempre remover os scripts de instalação de uma ferramenta web, pois eles podem servir para o invasor tentar identificar todo o sistema.
- ➢ Estar sempre pesquisando no Google as informações do website corporativo. Se encontrar algum documento ou informação que não deveria ser acessada, seguir as instruções da ajuda do Google de como remover.

2.5.2 VARREDURA

A segunda fase está baseada em técnicas de varreduras, descoberta de computadores ativos na rede através do protocolo ICMP (*ping*) e rastreamento de portas de serviços abertas nesses sistemas são as técnicas mais comuns e usadas por atacantes para descobrir serviços vulneráveis em um sistema.

Quaisquer máquinas conectadas numa rede oferecem serviços que usam portas TCP e UDP.

Portanto, o rastreamento de portas consiste em enviar uma mensagem de cada vez para cada uma das portas, explorando as portas comuns e até as menos usadas. Com a análise de resposta de varredura pode se determinar se uma porta está sendo ou não usada e, caso esteja, o agressor poderá explorar através de outros testes [GIAVAROTO, 2013].

Existem três tipos de varredura: de porta, de vulnerabilidade e de redes. Na varredura de porta, são verificadas as portas ativas e serviços, na varredura de vulnerabilidades são detectadas as fraquezas e vulnerabilidades presentes no sistema, por fim, na varredura de rede são identificados computadores ativos. Existem vários programas de varreduras de portas que se destacam conforme suas características como: *Nmap, Amap, Netcat* e *Hping*.

Solução: não dá para impedir que alguém tente realizar varredura nos hosts da sua rede e nas portas do seu sistema. O que é possível fazer em relação a isso é [ASSUNÇÃO, 2012]:

- Configurar corretamente o firewall para não responder externamente a *ping* e outras chamadas ICMP, e restringir o acesso às portas do sistema, salvo àquelas de serviços muito usados (exemplo: servidor web).
- Utilizar um IDS para registrar às tentativas de varredura de portas. Assim você pode tentar bloquear tentativas futuras, impedindo o acesso daquele endereço IP, ou mesmo reportar a varredura para as autoridades competentes.

2.5.3 ENUMERAÇÃO

Com informações obtidas através de reconhecimento e varreduras, é possível então passar para a próxima fase do teste: a enumeração. Nesta fase o atacante atua de forma mais invasiva, nesse processo de enumeração são obtidos nomes de computadores, usuários, serviços, versões, compartilhamentos e etc. Nessa fase tudo é anotado e analisado pelo atacante, versão de serviços FTP, servidores web, serviços de e-mail, banco de dados, serviço de netbios, endereços físicos (*MAC address*). Algumas ferramentas utilizadas são: *Nbtscan, Snmpcheck, SmtpscaneHttprint*.

Solução: existem alguns passos que podem ser seguidos para evitar o problema da enumeração. Citarei alguns deles que podem ajudar a amenizar o problema [ASSUNÇÃO, 2012]:

- Nunca deixar páginas não indexadas no servidor web.
- Utilizar sempre serviços de rede criptografados (como SSH e SFTP) para evitar a captura de banners. Se for possível mudar ou ocultar o banner nas configurações de algum serviço, é sempre recomendável.
- Se possível, configurar o servidor SMTP para não informar quando o usuário não existe e também não enviar resposta quando um e-mail destinado a uma conta inexistente chegar (pelo menos, modifique a mensagem de resposta para uma que não informe qual era a conta).
- Desabilitar recursos que permitam sessão nula, como o compartilhamento Netbios IPC$.

2.5.4 FALHAS E PROBLEMAS

Após descobrir os hosts ativos e os serviços que estão rodando, identificar esses serviços e descobrir usuários e recursos no sistema, nessa fase são identificas possíveis falhas nesse sistema. Isso pode ser feito manualmente, através de pesquisa ou utilizando programas próprios para essa análise. Quando se sabe a versão exata dos servidores que estão rodando, a pesquisa manual costuma ser a mais eficiente. As falhas são classificadas em dois tipos, locais e remotas [ASSUNÇÃO, 2012]:

- *Falhas locais*: É um tipo de falha que só pode ser explorada localmente no sistema, ou seja, um invasor precisaria estar fisicamente usando esse computador ou já possuir acesso local pela Internet.

- *Falhas remotas*: Esse tipo de falha acontece em servidores que escutam conexões externas. Um serviço do servidor, como FTP, Web, POP3, SMTP, SMB, NetBIOS, *Universal Plugand Play*, X11 e etc. Como esses serviços fornecem acesso à Internet e, em quase 90% dos casos, eles requerem algum tipo de autenticação, podem vir a ter problemas no caso de alguma falha ser encontrada.

  Podemos destacar algumas falhas comuns em sistemas:

Buffer Overflow: é o chamado “estouro de buffer”, falha muito comum hoje. Tanto o stack overflow (overflow da pilha) quanto o heap overflow (overflow da memória heap) podem ser encontrados em diversos programas existentes no mercado.

Race Conditions: outro tipo interessante de falha. Uma *racecondition* (condição de corrida) é criada geralmente quando um programa com permissões de usuário comum gera algum recurso, como um arquivo temporário, com

permissão de usuário administrativo ou superusuário. Esse recurso é finito, geralmente durando no máximo até alguns segundos antes de ser apagado. A questão então é: se nesses poucos segundos alguém conseguir tomar controle desse recurso com permissões elevadas, poderia usá-los para aumentar seus privilégios dentro de um determinado sistema.

SQL Injection: um dos ataques mais comuns hoje é a injeção de comandos SQL (*Structured Query Language*). Para quem não sabe, SQL é um banco de dados muito utilizado atualmente, que possui várias versões: Microsoft SQL Server, MySQL etc. Esse tipo de falha não é do servidor de banco de dados e, sim, de um programa feito para interagir com esse banco. Seja ASP, PHP, JSP ou qualquer outro tipo de programação para a Web, se o programa não interpretar corretamente certos caracteres como barra (/) e aspas simples(‘), eles podem ser usados para “injetar” comandos naquele sistema, burlando sistemas de nome de usuário e senha, fornecendo acesso completo ao banco de dados muitas vezes.

Cross Site Scripting: também chamada simplesmente de CSS ou XSS, o *Cross Site Scripting* é uma técnica que visa roubar cookies de usuários através de seus navegadores. Geralmente o invasor injeta comandos HTML e Java Script em alguma função, conseguindo obter sessões de usuários mesmo sem ter autorização para isso. Qual a utilidade disso, então? Podemos ler o e-mail de uma pessoa no seu webmail, acessar o seu banco on-line etc. Tudo sem precisar saber a senha.

Nas fases anteriores são utilizadas ferramentas para varredura, enumeração e praticamente são utilizadas para descobrir computadores ativos na rede, portas e identificar os serviços nessas portas. Alguns vão além. Muitas ferramentas de varredura também têm um banco de dados de falhas e checam os serviços descobertos no computador-alvo para ver se descobrem alguma vulnerabilidade. É um processo completamente automatizado e extremamente simples, que não requer nenhum tipo de pesquisa manual, dentre elas podemos citar: *Languard, Shadow Security Scanner, Syhunt TrustSight, Retina para* sistemas operacionais Windows*. Nessus e Saint* para sistemas operacionais Linux.

Solução: as falhas sempre vão acontecer, por mais caro que os softwares possam ter custado. A melhor maneira, então, de se proteger é estar sempre realizando o *Penetration Test*. Assim é possível sempre estar corrigindo os problemas dos softwares antes que alguém possa se aproveitar dessas falhas e usá-las para ganhar controle do sistema [ASSUNÇÃO, 2012].

2.5.5 BURLANDO PROTEÇÕES

Com as fases anteriores executadas é possível se concentrar em como burlar três tipos de ferramentas: o antivírus, o firewall e o IDS. São as proteções mais importantes de uma rede e quando contornados abrem caminhos para novos ataques.

Antivírus: um passo muito importante é impedir um programa malicioso de ser detectado pelos antivírus de hoje. Outra coisa a ser lembrada é que, ao contrário de firewalls e IDS que são mais usados em ambientes corporativos, praticamente todo mundo usa antivírus. Técnicas como alterações em hexadecimal, apagando recursos do executável, compressão de executáveis e alterações de data streams podem ser usadas para despistar o antivírus. Ferramentas que são usadas para burlar o antivírus são: *Xvi32, PE Explorer, Petite, Aspack, Mewe*x*Upx.*

Firewall: geralmente, o firewall é configurado para uma excelente proteção de fora para dentro, deixando passar, muitas vezes, apenas conexões para servidores web, de correio e algum tipo de serviço remoto que possua boa autenticação, outros firewalls são configurados apenas para barrar endereços específicos. O uso de servidores proxy, técnicas de *spoofing* (arte de criar informações de rede falsas e utilizar para diversos propósitos), interceptar o tráfego de rede de requisições DNS, conexão reversa e tunelamento são técnicas utilizadas para driblar o firewall. Ferramentas para burlar o firewall: *Sterm, Netcat, Netwox*e *HTTP Tunnel*, entre outras.

IDS: um IDS nada mais é do que um *sniffer* com regras, muitas vezes simples e baseado em texto puro (*ASCII*). O objetivo de técnicas anti-IDS é modificar um pedido de tal maneira que os sistemas de detecção ficarão confusos, mas o servidor web ainda conseguirá entender o que é solicitado. As técnicas variam em outros protocolos e serviços, o uso de codificações de URL, barras duplas e triplas, travessias de diretórios e a combinação desses métodos são utilizadas para burlar o IDS. Ferramentas para burlar o IDS são: *Syhunt e HexEdit*.

Soluções: Podemos destacar algumas medidas para evitar que os sistemas de segurança sejam burlados:

- Não se pode confiar 100% nos softwares de antivírus. Caso ocorra desconfiança que alguém esteja acessando o seu sistema e antivírus como: Norton, McAfee, AVG ou outro não detectar, recomendado instalar um firewall pessoal e é necessário verificar se ele detecta alguma porta aberta que não deveria estar lá. Outros programas

interessantes são os monitoradores de registros, para verificar entradas suspeitas, e os monitoradores de conexões, como o *Active Ports*.

- Configurar uma proteção decente nas regras do firewall, não só para filtrar o que entra, mas também o que sai. Tentar somente permitir o acesso externo a servidores web através de um proxy. Se os funcionários necessitarem usar algum comunicador instantâneo, podem usar a versão online na página do fabricante. Isso evitaria a conexão reversa. Utilizar programas que detectem presença de ARP *poisoning* na rede interna, como o *ARP Guard*, evitando, assim, ataques de IP *spoofing*. Sobrando só o HTTP *tunneling*. Esse é o mais complicado de se proteger. A opção mais simples é baixar algumas regras novas para o IDS baseadas no formato, alteração e tamanho dos pacotes que trafegam na rede, possibilitando detectar pequenas alterações. Mas não é uma proteção muito eficiente. A opção perfeita, porém impossível de se implementar na maioria dos ambientes, seria permitir que o proxy acessasse somente endereços específicos (bancos, site da empresa, alguns sites de e-mail etc.) e bloqueasse todo o resto, inviável.

- Estar sempre atualizando as regras do IDS, definindo regras personalizadas para o seu ambiente corporativo e instalando módulos extras no sistema de detecção de intrusos, se disponíveis. Todo o cuidado é pouco para evitar que possíveis ataques passem despercebidos e causem um grande estrago no sistema e servidores.

2.5.6 ENGENHARIA SOCIAL

Para [MITNICK, 2003] a engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não e, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia.

Os engenheiros sociais são pessoas cultas, de um papo agradável e que conseguem fazer com que pessoas caiam em suas armadilhas. Utilizando meios digitais, telefônicos e até pessoalmente, observam e estudam sua rotina sem que sejam percebidos. E isso não é algo novo que surgiu com a informática, há décadas esses engenheiros vêm agindo [ASSUNÇÃO, 2012].

Geralmente, existem três maneiras básicas de agir:

- *Por e-mail ou carta*: O engenheiro social envia um e-mail ou carta para seu alvo contendo informações que ele quer. Pode ser pedindo um

documento importante ou fingindo ser do Centro de Processamento de Dados e requerendo uma mudança de senha.

- *Pessoalmente*: É o método mais arriscado, mas também o mais eficiente. O engenheiro social arruma um bom terno, um relógio com aparência de caro e uma maleta com um notebook. Pode se passar por um cliente, por um funcionário ou mesmo parceiro de negócios.

- *Pelo telefone*: O engenheiro social se passa por alguém importante, finge precisar de ajuda ou mesmo se oferece para ajudar.

O forte de um bom engenheiro social é manipular os sentimentos das pessoas, levando-as a fazerem o que ele quer. Os casos mais comuns de manipulação são: *curiosidade, confiança, simpatia, culpa* e *medo*.

2.5.7 TRUQUES APLICADOS NA INFORMATICA

Os engenheiros sociais também aplicam vários truques utilizando a informática, visando obter informações e dados importantes que, normalmente, não seriam tão facilmente entregues. Um desses truques é fazer com que alguma pessoa pense que está recebendo e-mail de um amigo qualquer com um anexo, quando, na realidade, é uma ferramenta de invasão.

E-mail Phising: a ferramenta mais utilizada da Internet hoje é de longe o e-mail. Correspondemo-nos instantaneamente com quem quisermos, na hora em que desejarmos. Justamente por isso ele é uma das principais ferramentas usadas pelos engenheiros sociais e vírus para ganhar acesso ao seu computador. Através de anexos de arquivos no e-mail isso pode acontecer. O mais comum é receber um e-mail estranho, de alguém que não conhece, com um arquivo anexado.

E-mail Falso: o e-mail falso é uma técnica muito utilizada hoje na Internet para se enviar e-mail sem ser identificado. Bom, pelo menos para o remetente, pois muitas vezes o endereço IP original ainda continua sendo mostrado no e-mail. Quais as vantagens disso para a Engenharia Social? Como a maioria dos usuários é leiga e nunca iriam conferir o endereço para ver se batem, os engenheiros sociais podem fingir ter vindo de qualquer e-mail.

Mensagens Instantâneas: tomar cuidado com comunicadores como Skype, Yahoo, Messengers. Um Engenheiro Social fará de tudo para lhe convencer a aceitar um determinado arquivo. Antigamente, usavam a desculpa de ser foto e, hoje, isso já não funciona tanto, pois a maioria desses *messengers* já mostra

automaticamente uma imagem da pessoa. Então, esses engenheiros se utilizam da sua confiança e simpatia para dizer que o arquivo é um jogo interessante, um projeto inacabado qualquer no qual ele quer a sua opinião, ou mesmo um programa para “magicamente” incluir créditos nos celulares.

Solução: se pode criar novas políticas de segurança e um controle maior do contato feito com os funcionários, mas se pegar muito pesado, deixará essas pessoas frustradas e a solução não é 100% eficiente. A melhor solução seria simplesmente o treinamento. Todas as pessoas de uma empresa que lidam com informações importantes devem passar por um treinamento no qual irão aprender a identificar os tipos de ataques e como reagir a cada um deles.

2.5.8 MALWARE

O termo *malware* é proveniente do inglês malicious software; é um software destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não). Alguns malwares que podemos citar são:

Backdoors: o nome “backdoor” significa porta dos fundos. É um software que, se instalado em algum sistema, permitirá posterior acesso a este. Isso é muito utilizado por invasores quando ganham acesso ao console de alguma máquina e querem manter um acesso para voltarem. Existem vários tipos de backdoors: de login, de telnet, protocolos incomuns e de servidor e *rootkits* que costumam substituir comando do sistema por versões “*hackeadas*”.

Cavalos de Tróia: um cavalo de tróia, ou trojan, é um programa que, quando instalado no sistema de alguém, geralmente abre uma porta TCP ou UDP para receber conexões externas, fornecendo normalmente o console (*prompt de comandos*) daquele sistema para um possível invasor. Isso não é regra geral, já que alguns backdoors podem fazer também conexão reversa e outros tipos de técnicas. Um cavalo de tróia nada mais é do que um backdoor disfarçado de um programa comum, como um jogo. Existem vários tipos de trojans como: *webdownloaders, de notificação, comerciais* e *joiners*, com o joiner é possível escolhe o arquivo da porta dos fundos, o programa onde você o deseja colocar e pronto.

Exploits: um exploit é um programa criado para testar uma falha de segurança, geralmente como prova de conceito, outras vezes feito com fins maliciosos para realmente explorar e invadir sistemas alheios. Existem técnicas de exploração (*exploiting*) para diversos tipos de falhas, como os stack overflows, heap overflows e outros. Vamos ver alguns desses tipos, como obter *exploits*,

como eles funcionam como utilizá-los, ferramentas para o desenvolvimento e utilização, entre outras.

2.5.9 SENHAS

Nunca devemos deixar uma conta de usuário ou algum outro serviço que dependa de autenticação sem senha. Os invasores podem se aproveitar disso. Mas também não adianta colocar senhas fáceis. Nunca utilizar senhas do tipo:

- *Data de nascimento* – Exemplo: 070275.
- *Nome de familiar ou amigo* – Exemplo: marcelo.
- *Local em que trabalha* – Exemplo: correios.
- *Nome de personagens/filmes* – Exemplo: matrix.
- *Outros nomes conhecidos* – Exemplo: cruzeiro.

Os programas de força bruta hoje conseguem fazer pequenas permutações quando tentam descobrir a senha (exemplo: tentar a senha ao contrário, com números na frente, com todos os caracteres minúsculos e todos maiúsculos e etc.). Então, essa é uma prática que deve ser evitada. Para se montar uma boa senha é importante utilizar:

- *Letras maiúsculas e minúsculas;*
- *Números;*
- *Caracteres especiais como /*+-*&@#{;*
- *Tamanhos de senha com no mínimo 10 caracteres.*

Outro detalhe é sempre estar alterando as senhas. Mesmo que a politica de segurança da empresa não exija que você faça essa mudança de tempos em tempos (o que já pode ser considerada uma má configuração do sistema, já que é essencial essa mudança), é importante mudar as senhas periodicamente.

Para [ASSUNÇÃO, 2012] existe ainda um problema mais grave em relação a isso com as senhas padrões. Senhas padrões geralmente são encontradas em dispositivos de rede como equipamentos de rede, sistemas operacionais e serviços de rede. O problema é que essas informações são comumente divulgadas na Internet, então, se você instala um recurso que vem com uma senha padrão para um usuário qualquer e esquece-se de mudar essa informação, qualquer pessoa que conseguir identificar o seu dispositivo (através dos processos de varredura e enumeração) como um roteador Cisco, por exemplo, poderá se conectar a ele e ter total acesso.

Existem algumas maneiras e técnicas para a descoberta de senhas, seguem alguns tipos:

Password Guessing: o famoso “chute”. Nada mais é do que tentar manualmente entrar com diversas senhas. O método menos eficaz de todos.

Engenharia Social: uma pessoa pode simplesmente se passar por alguém e pedir a senha.

Keyloggers: utilizar-se de programas capturadores de teclas para obter a tão desejada senha de acesso. Processo eficaz, mas ainda possui o defeito de depender de Engenharia Social para sua instalação.

Força-Bruta: parecida com o ataque de dicionários, mas esse método não utiliza palavras prontas em uma lista e, sim, gera todas as combinações possíveis de caracteres para tentar como senha. É, de longe, o método mais eficiente para senhas criptografadas locais e, remotamente, não dá muito resultado.

Criptoanálise: utilização de *rainbow tables*, uma espécie de *wordlist* contendo diversas palavras e números e com o seu equivalente criptografado, para apressar o processo da força-bruta (que, em alguns casos, levaria anos para terminar).

Ataque de dicionários: o ataque de dicionários consiste em criar uma lista de palavras (*wordlist*) ou senhas muito utilizadas e valer-se dessas informações. Se a pessoa utilizar uma senha simples ou fraca, esse processo costuma ser bem eficiente.

Sniffers: os “farejadores”. Também muito eficientes para capturar senhas em redes locais, mesmo quando essas redes são segmentadas.

Man in the middle: ataques de “*homem no meio*”. Especialmente interessantes para capturar senhas de ambientes criptografados como SSH e SSL.

2.5.10 SNIFFERS

Segundo [ASSUNÇÃO, 2012] o ato de farejar uma rede é um dos processos mais antigos do hackerismo e o mais interessante. Quando a rede utiliza um multirepetidor (*hub*) ou uma topologia que faça com que os dados sejam enviados a todos os sistemas ao mesmo tempo (através de *broadcast* e *multicast*, por exemplo), é possível utilizar o *sniffer*. Quando os frames (*quadros*) são direcionados a certa máquina, no caso do *hub*, eles são enviados para todas as máquinas ligadas a ele. Apenas a máquina à qual o pacote foi endereçado envia-o para suas camadas superiores para ser processado, o resto dos computadores simplesmente descarta o pacote. Seria interessante,

então, que você tivesse um programa que "capturasse" esses pacotes antes que o sistema os descartasse. Isso é o *sniffer*.

Wireless Sniffing: hoje em dia é moda também farejar tráfego de redes wireless, existem diversos programas interessantes para farejar redes sem fio. Bons exemplos são *AirSnort, Kismet, WireShark*, entre outros. Normalmente, o processo para se obtiver acesso a uma rede wireless é o seguinte:

- Encontrar o SSID da rede (identificador da rede)
- Se a rede tiver criptografia, deve utilizar a chave necessária.
- Somente aí, quando se conectar a ela, poderá farejar o tráfego.

Acontece que isso não é muito útil. Muitas vezes, as pessoas colocam a opção de não fazer o *broadcast* do SSID, ou seja, a rede nem é detectada. Em sistemas Linux, é possível colocar a placa de rede em um modo passivo especial que consegue farejar o tráfego de redes wireless mesmo que você não esteja autenticado a elas ou mesmo sem detectar o SSID. O Windows não tem suporte para esse tipo de utilização.

Solução: configurar corretamente o seu sistema. Estar atento para configurações de senhas, forçar os usuários a utilizarem senhas com, no mínimo, oito caracteres e misturando letras e números. Fazer com que o sistema peça a troca dessa senha em, no máximo, a cada três meses. Criar regras de bloqueio para contas de usuário após várias tentativas inválidas para evitar os ataques de força-bruta. Utilizar serviços criptografados na rede para evitar o *sniffing* (farejamento). Utilizar para acesso remoto o aplicativo SSH em vez de Telnet, SFTP em vez de FTP comum, buscar sempre utilizar os serviços de forma criptografada. Não permita que os usuários locais consigam dar boot no sistema por disquete, pendrives ou CD-ROM. Se isso acontecer, é possível facilmente alterar a senha administrativa do sistema. E, por último, não se esquecer de remover quaisquer compartilhamentos de *Netbios* que não estiverem sendo utilizados. Lembrar que cuidado nunca é demais.

2.5.11 ATAQUE DE NEGAÇÃO OU RECUSA DE SERVIÇOS

O *Denial of Service*, ou recusa de serviços, tem como objetivo derrubar um sistema da rede, consumindo os seus recursos. Isso pode ser feito de diversas maneiras [ASSUNÇÃO, 2012]. Alguns dos inúmeros tipos de ataques comuns de recusa de serviço são:

Ping da morte: técnica muito antiga e totalmente ineficaz, mas vale como referência histórica. Tratava-se de enviar um ping para um site, com um pacote muito grande, fazendo esse sistema travar.

Syn Flood: técnica que envia pacotes Syn para um sistema, mas não realiza a transação completa em três vias. O resultado é que o alvo vai recebendo inúmeros pacotes, fica aguardando o resto das respostas e, eventualmente, consome todos os seus recursos.

Smurf: técnica que utiliza os endereços de broadcast das redes para gerar tráfego excessivo e redirecionar todos esses dados em um único alvo, consumindo automaticamente a sua banda.

DDoS: a recusa de serviço distribuída é um poderoso recurso, pois soma todo o poder das conexões nos sistemas em que está instalada. Se for possível infectar cem computadores, cada um deles possuindo uma conexão de até 256 Kb, já é o suficiente para derrubar grandes servidores. Existem alguns programas para realizar isso, o mais conhecido deles é o *Tribal Flood Network*, ou TFN.

Solução: não existe uma solução definitiva para o problema do *Denial of Service*. Se um *DDoS* for feito, não haverá muita ação que possa ser tomada. Mas contra os ataques comuns e as falhas, esses sim são possíveis dar um jeito. Primeiro é bom sempre estar corrigindo possíveis bugs do sistema. Por exemplo: configurar o sistema para parar de responder a um determinado IP se ele receber desse endereço dez pacotes Syn em seqüência e nenhuma outra resposta. Isso evitaria o ataque de *Syn Flood*.

3 UTM

Os hackers se tornaram mais sofisticados e seus ataques também, mais direcionados inclusive. Muitos dos ataques atuais são ataques combinados, que usam várias técnicas para tentar se infiltrar em uma rede. Embora as organizações precisem de várias técnicas para combater ataques combinados, gerenciar várias ferramentas de segurança separadas pode ser cansativo, ineficiente e caro. O gerenciamento unificado de ameaças (*Unified Threat Management*) é a melhor abordagem de segurança para empresas de pequeno e médio porte, trazendo um novo nível de eficiência para a segurança.

Segundo [TAM, 2012] o UTM ou Central Unificada de Gerenciamento de Ameaças é uma solução abrangente, criada para o setor de segurança de redes e ganhou notoriedade se tornando a solução mais procurada na defesa digital das organizações. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga, geração de relatórios informativos e gerenciais, funções como IPS e muito mais.

Os UTM ganharam muita reputação como primeira opção de defesa mais sofisticada sem a complexidade de integrar diversas soluções e recorrer a mais de um fabricante. Apesar de o mercado alvo ser as pequenas e médias empresas, existem grandes corporações que utilizam UTM como forma mais simplificada de lidar com diversas ameaças e problemas de segurança.

As vantagens apontadas são a redução de complexidade com o uso de uma solução única, um único fornecedor, uma única interface e uma única lógica de operação, a gerência facilitada e a ausência de problemas de compatibilidade entre plataformas diversas.

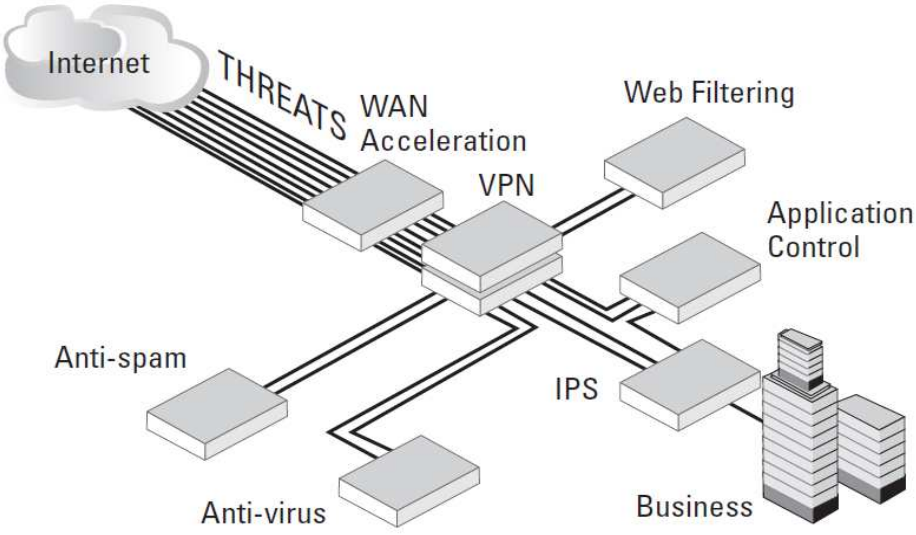

Figura 7: Funcionalidades UTM
Fonte: Tam, Kenneth. UTM Security with Fortinet: Mastering FortiOS, 2012.

Soluções de Segurança Integrada (UTM) que protegem a sua rede em tempo real contra ataques combinados e reduzem o custo total de operação. Seguem alguns benefícios dessa solução:

- Reduz o custo e gastos com a internet através de controle do uso dos links de dados;
- Melhora o desempenho do seu link de Internet com filtros de navegação web;
- Aumenta a disponibilidade dos links de Internet com balanceamento de links;
- Protege os usuários com antivírus de navegação;
- Conexão de qualquer lugar a sua rede com acesso seguro aos dados corporativos com VPN;
- Faz a integração de suas unidades remotas com maior segurança e confiabilidade.

3.1. A EVOLUÇÃO DAS REDES

As novas ondas tecnológicas como mobilidade, computação em nuvem, redes sociais e big data estão causando um grande impacto nas redes de dados bem como mostram novos desafios para que os administradores de rede mantenham o controle das políticas de segurança de rede, dentro desse contexto é necessário que as organizações adotem uma abordagem diferente em relação à segurança de rede. Dentro dessa evolução, podemos apontar alguns itens em relação à segurança de rede:

- *Disponibilidade*: a melhoria nos links de acesso a internet bem como o aumento muito grande das redes sem fio tem melhorado a disponibilidade e largura de banda dos acessos a dados e serviços de rede.
- *Acesso remoto*: o acesso a dados e sistemas corporativos através dos mais diversos dispositivos: notebooks, smartphones e tablets requer um firewall corporativo que comporte esses acessos de forma confiável e segura.
- *A explosão de aplicações*: a criação de novos softwares, aplicações, versões trabalhadas para plataformas móveis como *iOS* ou *Android*, os padrões de compatibilidade, protocolos de comunicação, as aplicações

e seu conteúdo evoluíram significativamente, os aplicativos podem estar localmente na rede ou na nuvem, hospedado por provedores e em alguns casos uma combinação entre rede local e nuvem.

- *Mídias sociais*: o crescente uso de mídias sociais como Youtube, Twitter, Facebook e Google no negócio e no dia-a-dia das empresas reflete uma mudança nas redes corporativas, surgem novas formas de acesso, novas formas de comunicação criando um nível maior de proteção e segurança em relação a essas novas modalidades de uso de mídias sociais.

- *Navegação insegura*: a explosão de aplicações que surgem sem planejamento ou até mesmo sem documentação apropriada podem potencialmente causar impactos nas redes de dados, seja no desempenho ou segurança com conteúdo malicioso, muitas vezes novos aplicativos passam despercebidos pelo radar dos administradores de rede.

- *Aplicativos que evitam detecção*: esse tipo de problema afeta organizações de todos os tamanhos, firewalls tradicionais dependem de números de portas ou identificadores para reconhecer e categorizar a rede e o tráfego. Aplicações maliciosas poderiam usar essas portas e protocolos específicos para se camuflar e operar dentro dessas redes de dados. Esses aplicativos podem trafegar dentro de um túnel e parecer legítimo, aplicações que utilizam algoritmos de criptografia que evitam inspeção e identificação do seu conteúdo, conexão com outros aplicativos através de portas de comunicação dinâmicas, *malwares* e *trojans* são ameaças famosas por utilizar essas técnicas que evitam a detecção dos firewalls.

- *Aplicações mal projetadas*: aplicativos, mas projetados que expõe informações importantes da rede da organização, vazamento de dados, informações sigilosas ou confidenciais, aplicativos que consomem muita largura de banda, compartilhamento de arquivos, tamanhos de arquivos grandes, trocas de arquivos indesejados, tudo isso são grandes riscos para as organizações.

- *Crimes online*: o cenário de ameaças hoje está repleto de novas ferramentas, hackers atuam na criação e desenvolvimento de ferramentas de ataque sejam elas para perda ou roubo de dados, comprometimento de sistemas, ataques de negação de serviço, redes

de terrorismo digital, divulgação de dados sigilosos, ataques por retaliação contra condições ou afiliações políticas e sociais.

3.2 FUNCIONALIDADES DOS FIREWALLS UTM

Os firewalls UTM são uma evolução dos firewalls tradicionais, um produto de segurança abrangente que inclui proteção contra várias ameaças, em uma plataforma unificada com diversas outras funcionalidades, vamos apresentar algumas dessas funcionalidades.

3.2.1 CONTROLE DE APLICAÇÕES

Uma importante característica do UTM é a maior visibilidade a aplicativos que geram tráfego na rede, juntamente com a capacidade de controlar essas aplicações. O controle de aplicativo pode identificar e controlar aplicativos, softwares, programas, serviços de rede e protocolos. A fim de proteger as redes contra as últimas ameaças criadas no mundo digital, o controle de aplicativo deve ser capaz de detectar e controlar todo o acesso a plataformas sociais como *Youtube, Facebook* e *Twitter*. Controlar o uso de aplicações em toda a rede corporativa. Com este recurso habilitado é possível determinar quais aplicações podem ou não trafegar pelo seu link de Internet. É possível bloquear aplicações que compartilham arquivos, *P2P*, *mensagens instantâneas*, *navegadores* e milhares de aplicações conhecidas.

O controle de aplicativo deve fornecer políticas granulares de permissões de acesso, possibilitando que seja permitido ou bloqueado o acesso a aplicativos com base no tipo de fornecedor da aplicação, comportamento e tecnologia utilizada.

É possível bloquear, permitir ou apenas monitorar o uso das aplicações. É possível controlar o uso de novas aplicações web como, por exemplo, liberar o *Facebook*, mas não permitir o uso do bate-papo ou de aplicativos de jogos como *Farmville*, entre outros.

Outra característica do controle do aplicativo é a capacidade de impor diretivas baseadas em identidade de usuários, fazendo filtros por endereços IP e grupos de usuário do *Active Directory* da Microsoft. Quando um usuário faz a autenticação no sistema e tenta acessar recursos de rede, o UTM aplica-se uma diretiva de firewall baseada em aplicativos. O acesso é permitido apenas se o usuário pertence a um dos grupos de usuários autorizados. *Traffic shaping*, um método de garantir a largura de banda de rede para determinados tipos de tráfego, dá prioridade a alguns aplicativos ao mesmo tempo em que limita a banda para outros. O controle de aplicativo fornece uma formatação de tráfego, que é acessível para manter a largura de banda aceitável para aplicações

como *Skype*, *iTunes* ou sites de compartilhamento de vídeos que dependem de uma largura de banda com mais qualidade.

3.2.2 ANTIVIRUS

A tecnologia do antivírus no UTM fornece proteção em várias camadas contra vírus, *spyware* e outros tipos de ataques de *malware*. É possível aplicar proteção antivírus para transferência de arquivos (FTP), mensagens instantâneas e conteúdo da web em todo o perímetro da rede. Algumas soluções suportam acesso seguro usando SSL e fazendo a varredura de conteúdo, que significa que você pode se proteger e criar conexões seguras para tráfegos como: HTTPS, SFTP, POP3S e assim por diante.

Essencialmente, um filtro de vírus UTM examina todos os arquivos de um banco de dados de assinaturas de vírus conhecidos e a padrões de arquivo utilizados para infectar os computadores. Se nenhuma ameaça é detectada, o arquivo é enviado para o destinatário. Se uma ameaça é detectada, a solução UTM exclui ou coloca em quarentena o arquivo infectado e notifica o usuário.

Algumas opções configuráveis em perfis antivírus incluem:

O banco de dados da assinatura antivírus: alguns fornecedores oferecem uma opção de assinatura de bases de dados, para que você possa determinar o equilíbrio certo entre desempenho e proteção. Um banco de dados maior aumenta a precisão, mas diminui o desempenho do sistema porque ele verifica um número maior de registros.

Padrão de arquivo: verifica o nome do arquivo contra as configurações padrão do arquivo configurado para o sistema.

Tamanho do arquivo: verifica se as mensagens ou anexos exceda um limite configurável pelo usuário.

Tipo de arquivo: aplica um filtro de reconhecimento de arquivos que verifica arquivos contra configurações criadas e configuradas pelo usuário.

Grayware: verifica todos os arquivos e faz relação com padrões de arquivo que correspondam a vírus scans e *spywares*.

Heurística: verifica os arquivos que apresentam comportamentos semelhantes a vírus ou outros indicadores de vírus conhecidos.

Verificação de vírus: verifica qualquer arquivo que tenha o padrão de arquivo similar a uma ameaça.

3.2.3 FILTRO DE CONTEÚDO WEB

A filtragem de conteúdo web permite que você controle quais os tipos de conteúdo web um usuário pode ter acesso. Usando a filtragem web, você pode reduzir significativamente a exposição a ameaças como *spyware, phishing*, *pharming*, sites de conteúdo inadequado, redirecionamentos de site e outras ameaças que encontramos diariamente na internet.

Um dos recursos do filtro de conteúdo web é a verificação completa de todo o conteúdo de cada web site que é aceito ou não por uma diretiva de firewall. Filtros de conteúdo permitem criar uma lista negra de palavras proibidas, frases e endereços web, bloqueando assim endereços de site não autorizados.

As categorias de web sites são o terceiro método de filtragem de conteúdos web, que se baseia em avaliações de URL para permitir ou bloquear por categoria, tais como: conteúdo adulto, sites de consumo de banda, rádios, pornografia, drogas, jogos, sites que tragam risco a segurança, sites de conteúdo pessoal, sites de conteúdo corporativo, governamental, entre outras. É possível criar categorias locais com os sites da empresa, parceiros e fornecedores. A categorização de sites é atualizada diariamente (na maioria dos UTMs funciona assim) e esse método diminui muito o trabalho dos administradores de rede em relação à filtragem de conteúdo web.

3.2.4 ANTISPAM

O *antispam* pode bloquear muitas ameaças que chegam por mensagens eletrônicas. Múltiplas tecnologias antispam incorporadas em UTM podem detectar ameaças através de uma variedade de técnicas, incluindo:

- Bloquear o IP de *spammers* conhecidos para evitar o recebimento de mensagens indevidas a partir desse remetente. O bloqueio de mensagens em qualquer URL que esteja no corpo da mensagem que possa estar associada com spam já conhecidos.

- Criação de um *hash* da mensagem e, em seguida, comparar esse valor para *hashes* de mensagens de spam conhecidos. Aqueles que correspondem um valor maior podem ser bloqueados sem saber detalhes sobre seu conteúdo.

- Utilização de listas brancas (lista de liberados) e listas negras (listas de bloqueados) de servidores de emails, remetentes, domínios de e-mails, IP de servidores, entre outros.

- Realização de DNS lookup do nome de domínio ao iniciar uma sessão de SMTP para ver se o domínio existe, é válido ou se está na lista negra.

- Bloqueio de emails com base em mensagem que tenha relação com conteúdo, palavras-chave ou padrões em caracterizam um spam, utilizando uma lista que serviria como filtro de palavras proibidas.

3.2.5 ACELERADOR DE WAN

Os usuários de uma rede corporativa que tem uma grande variedade de filiais esperam que a qualidade e velocidade de acesso estejam presentes em todo o ambiente da rede corporativa. Isso pode ser um problema porque as velocidades de Internet muitas vezes não são adequadas para aplicações que consomem muita largura de banda, ou mesmo pela qualidade dos links em locais mais distantes, sem falar no custo mais alto de links e conexões de alta velocidade.

Em tais situações, a otimização e aceleração de WAN desempenha um papel crítico, usando várias técnicas para melhorar o desempenho de acesso nas redes de longa distância da corporação. Estas técnicas incluem o protocolo de otimização, cache de byte, cache de web, descarregamento de SSL e encapsulamento seguro para entregar um melhor desempenho para aplicações e tornar mais eficiente o acesso para colaboradores que estejam conectando remotamente a rede corporativa.

Seguem abaixo alguns detalhes e mais informações sobre estas técnicas:

Otimização de protocolo: melhora a eficiência do tráfego que usa FTP, HTTP, TCP e outros protocolos, acelerando o desempenho da rede.

Byte cache: armazena arquivos e outros dados para reduzir a quantidade de dados transmitidos através dos links WAN.

Web cache: caches e arquivos temporários de páginas da web, reduzindo a latência e atrasos entre os servidores web e a rede WAN.

Descarregamento de SSL: descarrega a criptografia e descriptografia de SSL de servidores web para aceleração de hardware SSL, acelerando o desempenho dos servidores web.

Túnel de Acesso Seguro: protege o tráfego que passa pela rede WAN.

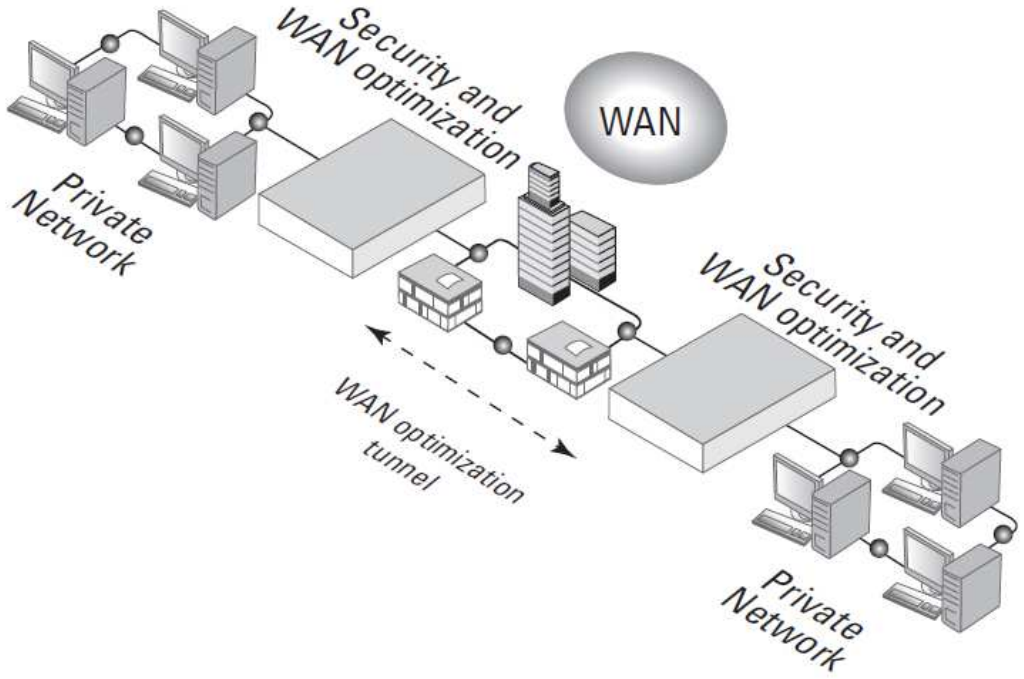

Figura 8: Acelerador de WAN
Fonte: Tam, Kenneth. UTM Security with Fortinet: Mastering FortiOS, 2012.

3.2.6 VPN

VPN é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a Internet). O tráfego de dados é levado pela rede pública utilizando protocolos que seguem um padrão, não necessariamente seguro [GALVÃO, 2013].

Uma VPN é uma conexão estabelecida sobre uma infraestrutura pública ou compartilhada, usando tecnologias de tunelamento e criptografia para manter seguros os dados trafegados. VPNs seguras usam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementada, estes protocolos podem assegurar comunicações seguras através de redes inseguras.

Trabalhar remotamente, em *Home Office*, em viagem ou de qualquer local com acesso a Internet através de VPN é muito comum. Essa funcionalidade de VPN é encontrada na maioria dos firewalls UTM, através de dispositivos móveis é possível ter acesso aos dados corporativos da empresa com total segurança. O administrador pode definir quais dados podem ser acessados de fora da empresa e todo o acesso é documentado e registrado caso haja necessidade de auditoria. São utilizados softwares para clientes de VPN específicos com autenticação via *Active Directory*.

3.2.7 IPS

Este sistema detecta e impede invasões de sistemas publicados na rede pública como servidores web com vulnerabilidades não corrigidas, aplicações e seus protocolos, de forma simples de configurar e eficiente para a rede de dados e servidores, está presente na maioria dos firewalls UTM.

Um IPS atua como sistema de detecção de intrusos, à procura de padrões de tráfego rede, atividades e processos, registram todos os eventos que possam afetar a segurança. Um IPS emite alarmes ou alertas para os administradores e são capazes de bloquear tráfegos indesejados. Os IPS também rotineiramente registram informações quando os eventos ocorrem assim eles podem fornecer informações para análise de ameaças, ou fornecer provas para possíveis ações judiciais. Visto como uma extensão do firewall, o IPS possibilita decisões de acesso baseadas no conteúdo da aplicação e não apenas no endereço IP ou em portas, como os firewalls tradicionais trabalham.

3.2.8 DLP

Data Loss Prevention (DLP) é uma técnica utilizada na área de segurança da informação para se referir a sistemas e metodologias que possibilitam as empresas reduzir o risco do vazamento de informações confidenciais. Os sistemas DLPs podem identificar a perda de dados através da identificação do conteúdo, monitoramento e bloqueio de dados específicos, ou seja, identificar, monitorar e proteger as informações confidenciais que podem estar em uso (máquinas dos usuários), em movimento (na rede corporativa) ou armazenadas (banco de dados, planilhas, servidores, etc.).

Nos firewalls UTM o DLP procura por confidenciais, proprietários de arquivos, ou dados registrados que acabam saindo pela rede de computadores. O DLP pode impedir ou registrar essa “fuga” de dados, é possível habilitar os DLP em políticas de segurança e acesso, criar filtros e notificar ou impedir a saída de arquivos e informações confidenciais como planilhas, por exemplo.

3.2.9 RELATORIOS GERENCIAIS

Os firewalls UTM em sua maioria permitem a geração de relatórios de uso de praticamente todos os recursos oferecidos pelo equipamento. Exemplo: relatórios de sites acessados por um determinado colaborador, medição de tempos que ele ficou naquele site. Relatórios de tentativas de invasões,

estações infectadas por vírus entre outros. Os relatórios podem ser gerados em tela, em formato HTML, PDF e até mesmo enviados por e-mail.

3.3 UTM VS NGFW

O firewall de última geração (NGFW) é um conceito inovador no setor de segurança de rede, pois promete integração e consolidação de tecnologias fundamentais de proteção do perímetro de rede. No entanto, ainda há muita confusão no mercado em relação ao que o NGFW oferece, muitos clientes ficam surpresos quando descobrem que ele não apresenta recursos importantes de segurança.

Basicamente, a funcionalidade de NGFW inclui firewall dinâmico, controle de aplicativos, controles baseados no usuário e um sistema de prevenção contra invasão (IPS). Em comparação, as soluções de gerenciamento unificado de ameaças (UTM) oferecem uma gama abrangente de tecnologias de segurança de rede que vão além da funcionalidade do NGFW.

As soluções de UTM oferecem firewall dinâmico, um sistema de prevenção contra invasão (IPS), antivírus de gateway, segurança e filtragem do conteúdo da web, segurança de e-mails e prevenção contra vazamento de dados (DLP). De modo mais importante, os fornecedores de UTM atualizaram com sucesso seus produtos para incluir as funcionalidades de NGFW, como controles de alerta de usuário e de aplicativos.

Há algum tempo que o conceito de "*Next Generation Firewall*" (NGFW) vem sendo apresentado para empresas de análises de desempenho como a *Gartner* e empresas de segurança da informação como a *Palo Alto Networks*, dando a entender que NGFW está reinventando o atual modelo de firewall UTM. E os fabricantes de firewall estão posicionando seus produtos como "o próximo grande passo" na evolução de firewalls [ITFRIENDS, 2015].

Pesquisando nas literaturas o conceito das tecnologias chegamos aos seguintes resultados:

Unified Threat Management (UTM): é uma plataforma de convergência de produtos de segurança, particularmente adequado para pequenas e médias empresas e possuem conjuntos de recursos típicos de segurança que se dividem em três subgrupos principais, tudo dentro de um único dispositivo UTM: *Firewall / IPS / VPN, URL Filter / Content Filter / Antivírus e AntiSpam / Mail Antivírus*

Next-Generation Firewalls (NGFWs): são firewalls de inspeção de pacotes com maior complexidade que vão além da inspeção de portas de comunicação e protocolos, atua em nível de inspeção de aplicativo, prevenção de intrusão e trazem inteligência externas do firewall. Um NGFW não deve ser confundido

com um sistema de prevenção de intrusão de rede (IPS) independente, que inclui um firewall embarcado, ou um firewall e IPS no mesmo equipamento sem que estejam intimamente integrados.

Para a [ITFRIENDS, 2015] as duas soluções não as discriminam em produtos realmente diferentes, até porque as definições são bem vagas. Os NGFWs não são revolucionários e não existem diferenças entre os firewalls UTM, sendo assim, os NGFWs são literalmente firewalls UTM com uma nova nomenclatura de mercado. Isso não passa de uma estratégia para reposicionar um produto que ficou distante tecnicamente de outros produtos que se tornaram mais competitivos no mercado, deixando-os a frente em uma nova pesquisa com “outros critérios” que na verdade são os mesmos. Desta forma as características ruins ou questionáveis do produto ficam em segundo plano, pois teoricamente não se pode comparar um produto de uma classe com outra, sendo assim os NGFWs não são balizados com os UTM, criando um novo posicionamento.

Isso se dá devido aos grandes fabricantes de firewalls corporativos (aqueles firewalls tradicionais para ambientes corporativos como a *Checkpoint, Cisco* e *Juniper*) não terem adequado seus produtos para UTM quando o conceito surgiu no mercado, isso deixou estes fabricantes para traz na corrida, quando surgiu o conceito, ele precisou de uma evangelização e estes fabricantes se solidificaram na tradição, e quando tentava criar um UTM ele tinha pouca integração, o que os deixava muito inferiores a produtos como os da Fortinet e da Astaro (Sophos), além das empresas que estavam surgindo que não tinha todos os produtos de segurança de perímetro bem fundamentados ou completos como a *Sourcefire* e *Palo Alto Networks*.

Desta forma o conceito de UTM foi marginalizado como produtos de pequenas e médias empresas, afinal. O mais incrível disso tudo é como a indústria aceitou isso bem, inclusive os grandes fabricantes de UTM passam a se movimentar para aparecerem nos gráficos de NGFW ao invés de provar que não há diferenças, talvez até por causa da enxurrada de conceitos de NGFW que se teve nas mídias nos últimos tempos.

O presidente da *Anitian Enterprise Security*, Andrew Plato, desenvolveu um comparativo a fim de provar este ponto de vista, considerando o conjunto de recursos dos seguintes dispositivos: *Palo Alto Networks*, *Checkpoint, Sourcefire* e *McAfee*, onde todos afirmam ter um NGFW. Para os firewalls UTM foi considerado o conjunto de recursos dos seguintes dispositivos: *SonicWall, WatchGuard, Fortinet* e *Sophos (Astaro),* e para deixar o comparativo mais completo, foi considerado também os recursos de equipamentos da *Juniper e Cisco* já que são grandes fornecedores de equipamentos de rede que tendem a concorrer também neste nicho de mercado [ITFRIENDS, 2015].

Recursos → / ↓Produto	FW/VPN	IPS	AV	Web Filtering	Application Detection	Email Security	DLP
Next Generation Firewalls							
Checkpoint	Sim	Sim	Sim	Sim	Sim	Sim	Sim
McAfee	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Palo Alto Networks	Sim	Sim	Sim	Sim	Sim	???	Sim
Sourcefire	Sim	Sim	Sim	Sim	Sim	???	Sim
UTM							
Astaro	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Fortinet	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Sonicwall	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Watchguard	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Adicionais							
Cisco	Sim	Sim	Sim	Sim	Não	Sim	Não
Juniper	Sim	Sim	Sim	Sim	Sim	Sim	Não

Figura 9: Comparativo Firewalls UTM e Firewalls de Nova Geração
Fonte: ITFriends, 2015.

Cada fabricante tem seus pontos fortes e fracos. A qualidade e desempenho dos produtos variam amplamente, porém, a partir de uma perspectiva puramente de características, eles são todos iguais. As diferentes abordagens de inspeção de aplicativos, antivírus, IPS podem explicar seu desempenho ou precisão, porém não muda o fato de que o núcleo de recursos é o mesmo.

3.4 FABRICANTES UTM

Conceitos a parte, é uma tendência de mercado, As vantagens já apontadas são a redução de complexidade com o uso de uma solução única, um único fornecedor, uma única interface e uma única lógica de operação, a gerência facilitada e a ausência de problemas de compatibilidade entre plataformas diversas.

O modelo de proteção através de soluções UTM é uma forma de defesa estratégica contra ameaças virtuais, considerada um passo à frente do modelo convencional de firewalls, na medida em que o UTM carrega maior valor agregado, como funções de prevenção de intrusões de rede, antivírus, rede privada virtual, filtragem de conteúdo, balanceamento de carga e geração de relatórios para o gerenciamento da rede. Dentre os principais fabricantes de equipamentos UTM é possível verificar através do quadrante de Gartner para equipamentos UTM de 2014 quem são eles:

Figura 10: Quadrante Mágico para UTM (Unified Threat Manangement)
Fonte: Gartner, 2014.

As empresas apresentadas pela Gartner no quadrante de Líderes devem ter posição de vanguarda na fabricação e venda de produtos UTM. Os requisitos para constar nesta lista incluem uma ampla gama de modelos com condições de cobrir as diferentes necessidades de diferentes tipos de negócios.

As empresas neste quadrante lideram o mercado oferecendo soluções com alto grau de inovação tecnológica que podem ser implementados de forma barata, sem afetar de forma significativa a experiência do usuário final, eliminando a necessidade de novas contratações de pessoal especializado para sua gestão. O histórico da empresa em evitar vulnerabilidades em seus produtos é considerado nesta análise. Outras características que devem fazer parte dos produtos listados são confiabilidade, rendimento consistente e gestão e administração intuitivas.

3.4.1 WATCHGUARD

Figura 11: Logotipo Watchguard
Fonte: Watchguard, 2015.

A Mazana Software é uma empresa que desenvolve software de segurança de redes, fundada em Seattle em 1995 por David Bonn para criar produtos de segurança de Internet de fácil utilização baseada em sistemas operacionais Linux, em fevereiro de 1996 a *Mazana Software* fundiu-se com a *Seattle Software Labs* e o *Firebox*, dentre os dispositivos de segurança de rede amplamente disponível no mercado. A *Seattle Softwares Labs* tornou-se *Watchgard* no início de 1997, em julho de 1999 a empresa se tornou de capital aberto com bolsa na Nasdaq, em 2006 se tornou empresa privada, foi comprada por 151 milhões de dólares por *Francisco Partners* e *Vector Capital*. Em 2010 a Watchguard adquiriu a *Toronto Borderware Tecnologies* para seus produtos, incluindo funcionalidades de segurança de conteúdo de email e web, prevenção de perda de dados e criptografia de e-mail [WATCHGUARD, 2015].

Figura 12: Equipamentos Watchguard
Fonte: Watchguard, 2015.

A plataforma *Watchguard* integra as melhores tecnologias de segurança do mercado de fornecedores como *Websense, Kaspersky, AVG, Trendmicro e Sophos*. Essa estratégia centrada no parceiro permite que a Watchguard

ofereça o melhor valor e proteção aos seus clientes, com a flexibilidade de mudar de parceiros e acrescentar funcionalidades conforme a necessidade.

3.4.2 SOPHOS

Figura 13: Logotipo Sophos
Fonte: Sophos, 2015.

A Sophos é uma desenvolvedora e fornecedora de software e de hardware de segurança, incluindo antivírus, antispyware, antispam, controle de acesso de rede, software de criptografia e prevenção de perda de dados para desktops, servidores para proteção de sistemas de e-mail e filtragem para gateways de rede.

Fundada em 1985 pelo Dr. Peter Lammer e o Dr. Jan Hruska, Sophos é uma empresa privada e sediada em Abingdon, Oxfordshire, Inglaterra e Burlington, Massachusetts, Estados Unidos. A empresa tem subsidiárias e escritórios na Austrália, Benelux, Canadá, França, Alemanha, Áustria, Itália, Japão, Singapura e Espanha. A empresa tem aproximadamente 1.800 funcionários em todo o mundo. Ao contrário de outras empresas de segurança, a Sophos não produz antivírus e soluções antispam para usuários domésticos, mantendo seu foco sempre no mercado empresarial [SOPHOS, 2015].

Figura 14: Equipamentos Sophos
Fonte: Sophos, 2015.

O Sophos UTM integra um software de segurança completa em um único aparelho. Pode ser implantado na plataforma que melhor se adapta ao negócio: dispositivo de hardware (*appliance*), software ou virtual. Cada um oferece um recurso idêntico, independentemente se a proteção deve atingir 10 ou 5.000 usuários. O console de gerenciamento tem interface pela Web permite o gerenciamento simples e consolida toda a estrutura de segurança: Alguns módulos que o produto oferece:

Endpoint Protection – software antivírus para computadores, com definição de políticas para manter os usuários seguros.

Rede Firewall Essencial – um firewall para impedir ataques que levam à perda ou roubo de dados, infecções e outros incidentes que custam tempo e dinheiro. Os recursos de proteção do firewall são projetados para simplificar a entrada de dados e controle de tráfego de saída.

Rede de Proteção - permite a configuração flexível de site para site e de acesso remoto VPN, protege contra ataques de negação de serviço, worms e de ataques de hackers sofisticados com exploits através de uma proteção contra intrusão de forma totalmente integrada.

Email Protection – protege o e-mail corporativo de spams e vírus.

Web Shield – permite aplicar um filtro de navegação web para proteger os trabalhadores contra as ameaças da Web e controlar a forma como gastam seu tempo online.

Proteção de servidor Web – protege o seus servidores e aplicações web contra ataques sofisticados, perda de dados, entre outros.

Wireless Protection – Torna as redes sem fio mais segura e confiável.

Clientes VPN – criar um acesso facilitado para se conectar a uma VPN.

3.4.3 DELL

Figura 15: Logotipo Dell SonicWALL
Fonte: Sonicwall, 2015.

A Dell é uma empresa de hardware de computador dos Estados Unidos, empregando mais de 106.700 pessoas no mundo inteiro. A Dell desenvolve, produz, dá suporte e vende uma grande variedade de computadores pessoais, servidores, notebooks, dispositivos de armazenamento, switches de rede, PDAs, software, periféricos e mais. De acordo com a lista Fortune 500 de 2005, a Dell é a 28ª maior empresa nos Estados Unidos (em vendas). Em 2005, a Fortune Magazine classificou a Dell como a número 1 na sua lista anual das empresas mais admiradas nos Estados Unidos, tomando o lugar do Wal-Mart, que mantinha o lugar por dois anos. Sua sede fica em *Round Rock*, Texas nos Estados Unidos. Michael Dell fundou a empresa em 1984, aos 19 anos, quando estudava na Universidade do Texas, Estados Unidos [DELL, 2015].

Figura 16: Equipamentos Dell SonicWALL
Fonte: Sonicwall, 2015.

Como uma plataforma multisserviços, a linha Dell *Sonicwall* de dispositivos de segurança de rede incorpora o nível mais abrangente de proteção disponível através de gestão unificada de ameaça (UTM). UTM combina vários recursos de segurança em uma única plataforma para proteger contra ataques, vírus, trojans, spyware e outras ameaças maliciosas. A complexidade de configuração é reduzida, administração e gestão são mais simplificadas, porque múltiplas camadas de proteção são entregues sob um único console de gerenciamento. Numa visão geral:

Proteção completa contra várias ameaças: os hackers se tornaram mais sofisticados e seus ataques, mais direcionados. Muitos dos ataques atuais são ataques combinados, que usam várias técnicas para tentar se infiltrar em uma rede. Embora as organizações precisem de várias técnicas para combater ataques combinados, gerenciar várias ferramentas de segurança separadas

pode ser cansativo, ineficiente e caro. O gerenciamento unificado de ameaças (UTM) é a melhor abordagem de segurança para empresas de pequeno e médio porte, trazendo um novo nível de eficiência para a segurança.

Proteção em camadas: a abordagem da Sonicwall para o UTM cria um ambiente de segurança que oferece firewall, proteção de conteúdo, antivírus, proteção contra invasões, inteligência de aplicativos, antispam, filtragem de conteúdo e SSL VPN em uma única plataforma de hardware. A proteção começa no gateway e bloqueia ameaças internas e externas em vários pontos de acesso e em todas as camadas de rede.

Reassembly-Free Deep Packet Inspection: a Sonicwall Reassembly-Free Deep Packet Inspection (RFDPI) vai além da inspeção de estado normal da camada de rede porque também inspeciona a camada de aplicativos em busca de ataques a vulnerabilidades de aplicativos. Essa tecnologia patenteada verifica mais de 50 tipos de aplicativos, além de vários protocolos, incluindo SMTP, POP3, IMAP, FTP, HTTP e Netbios. A RFDPI combina todos os arquivos obtidos por download, enviados por email e até mesmo compactos em um banco de dados de assinaturas amplo e atualizado de forma contínua, verificando todos os arquivos em tempo real para bloquear ameaças ocultas, como vírus em macros e executáveis compactados.

Desempenho superior: a Sonicwall oferece esse nível completo de proteção sem qualquer problema de desempenho. Muitas das outras soluções de UTM exigem o armazenamento em cache e a reinicialização de arquivos para suportar procedimentos de atualização de assinaturas de arquivos e verificação, o que diminui a velocidade do computador e afeta a produtividade. No entanto, como a Sonicwall pode verificar arquivos de qualquer tamanho sem armazená-los em cache e lidar com centenas de milhares de downloads simultâneos, ela oferece desempenho superior para redes de qualquer tamanho. Além disso, a Sonicwall acaba com a reinicialização depois da atualização de arquivos de assinatura, para que não haja necessidade de interromper a produtividade.

Segurança em tempo real: o UTM da Sonicwall adiciona recursos integrados de antivírus, antispyware e proteção contra invasões aos dispositivos de gateway *Sonicwall E-Class Network Security Appliance* (NSA), NSA e TZ Series. Esse nível robusto de proteção oferece segurança em tempo real contra uma ampla variedade de explorações, vulnerabilidades de software e códigos maliciosos. Ao oferecer o nível mais alto de segurança disponível, a Sonicwall combina proteção de gateway contra ataques externos com proteção de área de trabalho contra ataques internos de dentro da rede. O UTM da Sonicwall também oferece segurança de email e da Web, com proteção para emails recebidos e enviados, e conformidade reforçada com políticas internas e normas regulamentares externas.

3.4.4 AKER SECURITY SOLUTIONS

Figura 17: Logotipo Aker
Fonte: Aker, 2015.

Aker Security Solutions, fabricante de soluções de segurança da informação, é a primeira empresa brasileira a disponibilizar produtos e serviços que garantem a máxima proteção dos dados. Oferece soluções como: firewall, antispam, VPN, filtro de conteúdo e monitoramento remoto.

Seus produtos são comercializados por meio de revendas cadastradas e qualificadas. Hoje, a empresa conta com mais de 100 parceiros, distribuídos por todo Brasil, e atende clientes de portes variados em diversos segmentos das esferas públicas e privadas [AKER, 2015].

Além de softwares e hardwares, a Aker oferece também treinamentos, certificações, apoio a projetos e desenvolvimento personalizado. Importante ressaltar que todos os produtos e serviços Aker são totalmente adaptados à realidade brasileira.

A empresa é 100% nacional e orgulha-se disso porque acredita no potencial que o país tem para tornar-se um grande polo de produção tecnológica. A cada novo produto Aker desenvolvido, o Brasil avança alguns passos no caminho que o transformará em um dos líderes mundiais no setor de TI.

Figura 18: Equipamento Aker
Fonte: Aker 2015.

Algumas funcionalidades do Aker Firewall UTM:

Autenticação Clientless: acesso aos usuários que possuem permissão para utilizar a sua rede wireless de forma imediata e segura, sem a necessidade de cadastros e/ou registros complicados.

Kaspersky Antívirus: detecção, remoção e bloqueio de vírus nos arquivos trafegados na web pelo navegador, em aplicativos de comunicação online e em e-mails e é possível configurar alertas para aplicações e vulnerabilidade de programas que podem colocar a estrutura em risco. Com a assinatura da Kaspersky – solução líder de software antivírus e segurança web.

Soluções Wireless: WIDS – Segurança avançada com Sistema de Detecção e Prevenção de Intrusão Sem Fio; WDS – Permite que uma rede wireless alcance uma área geográfica maior com gerenciamento centralizado com Sistema de Distribuição Wireless.

Modo Bridge: esta funcionalidade permite que o Firewall funcione em modo transparente/oculto na rede, impossibilitando sua identificação por meio de saltos, otimizando o tempo de configuração e diminuindo a intervenção humana neste processo.

Link Aggregation: com este protocolo é possível criar uma forma padronizada para agrupar múltiplos links entre ativos (equipamentos de camada 2) fazendo com que estes se comportem como se fossem um único link, aumentando a velocidade do link na comunicação.

Filtro de Conteúdo Web: Controle o acesso a jogos, chats e aos mais diversos aplicativos em sites e redes sociais.

Cluster: alto desempenho, disponibilidade e escalabilidade. Com o cluster, você mantém os recursos da sua rede funcionando de forma eficiente e em tempo integral.

Antispam: previne contra a ação de spam bots e e-mails maliciosos.

VPN: acesso remoto seguro a rede corporativa via computador, *tablet* ou celular. Conta ainda com o VPN *failover*, que realiza a verificação de links específicos e permite que o administrador configure rotas seguras quando algum desses links ficarem inativos.

Balanceamento de Link: mantem a conexão online em tempo integral. Este recurso oferece alta disponibilidade, tolerando falhas em múltiplos links, como: 3G, 4G e ADSL.

IDS/IPS: detecção de tráfego de dados maliciosos entre a Internet e o ambiente computacional corporativo. O sistema tem a disposição uma base com mais 20.000 assinaturas de ataques.

QoS: classificação e priorização com os tipos de serviço da rede por grau de relevância. Assim, em caso de congestionamento, será possível priorizar determinados fluxos ou aplicações.

Filtro de Aplicações: controle de acessos a jogos, chats e aos mais diversos aplicativos em sites e redes sociais.

Controle de IM: permissão ou bloqueio a acessos a sistemas de comunicação instantânea. Isso melhora a produtividade dos colaboradores no ambiente corporativo.

3.4.5 STORMSHIELD

Figura 19: Logotipo Stormshield
Fonte: Stormshield, 2015.

Fundada em 2000, Arkoon Network Security é uma empresa francesa com sede em Lyon, na França, que é especializada em segurança da informação. A Arkoon cria soluções para proteção de informações, comunicações, infraestrutura e *appliances* UTM que integram os serviços de segurança, QoS e roteamento (aplicativo firewall, VPN, antivírus, antispam, filtragem de URL, entre outros), esses equipamentos seguem premissas de segurança como: confidencialidade, integridade e autenticidade de informações da empresa por meio de criptografia e técnicas de assinatura eletrônica. No final de 2009, a Arkoon adquire a empresa *SkyRecon Systems*, detentora da suíte de equipamentos *StormShield* (segurança de rede, segurança de dados e segurança de estação de trabalho) [STORMSHIELD, 2015].

Figura 20: Equipamentos Stormshield
Fonte: Stormshield, 2015.

Ambientes virtualizados em nuvens públicas ou privadas exigem proteção avançada contra ameaças que é equivalente a uma proteção dada em servidores físicos. A *Stormshield* trabalha com a segurança de rede para aplicação da nuvem, os clientes que tem estrutura na *Amazon Web Services* (AWS) podem controlar e garantir a segurança de seus ambientes de nuvem.

A segurança de rede Stormshield para aplicação da nuvem é similar a existente nos equipamentos físicos. Para uma transição segura para a nuvem, todas as características avançadas de segurança de equipamentos físicos estão disponíveis. A segurança de rede na nuvem Stormshield permite proteger servidores virtuais (EC2) e redes virtuais (VPC) hospedadas em uma nuvem da *Amazon Web Services*. É possível criar uma conexão de VPN entre um equipamento Stormshield corporativo local com a segurança de rede na nuvem *Stormshield*, é possível criar uma rede de dados estendida na nuvem com segurança [STORMSHIELD, 2015].

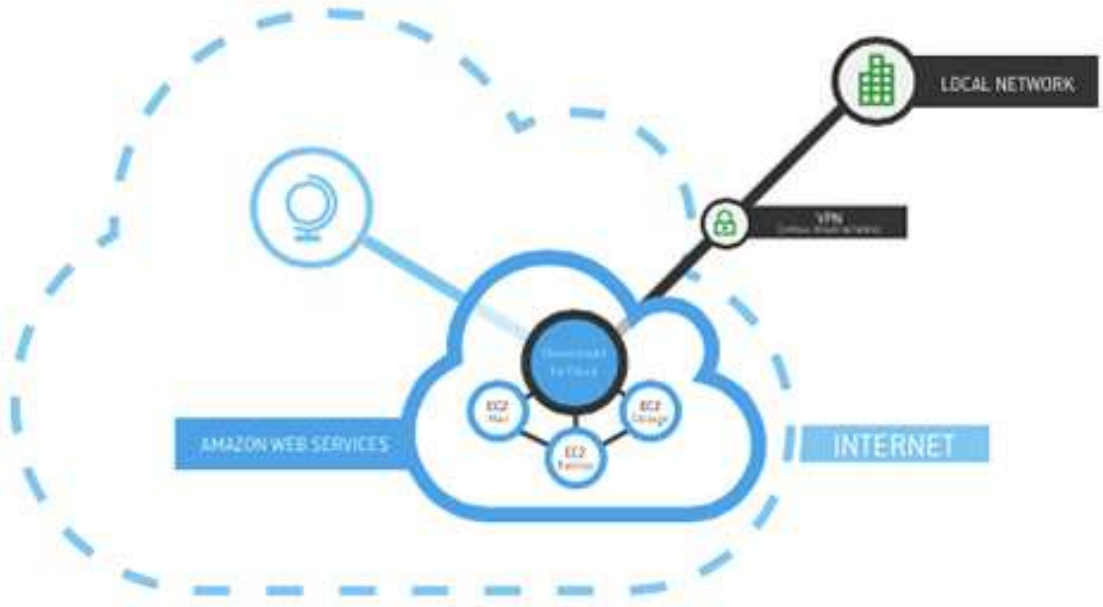

Figura 21: Stormshield Security Cloud
Fonte: Stormshield, 2015.

3.4.6 CYBEROAM

Figura 22: Logotipo Cyberoam
Fonte: Cyberoam, 2015.

A *Cyberoam Technologies*, uma empresa Sophos, é um fornecedor de aparelhos de segurança de rede global, com presença em mais de 125 países. A empresa oferece a segurança de rede *Unified Threat Management*, permitindo visibilidade e controle granular para de segurança de rede em ambientes corporativos. A empresa tem seu suporte ao cliente e desenvolvimento na Índia e possui 550 funcionários em todo o globo. Tem um

canal de vendas com mais de 4500 parceiros. A empresa também realiza programas de treinamento para seus clientes e parceiros [CYBEROAM, 2015].

Figura 23: Equipamentos Cyberoam
Fonte: Cyberoam, 2015.

O Cyberoam NG Firewall UTM (Unified Threat Management) oferece algumas funções de segurança de rede, dentro de um appliance de hardware. Inclui: firewall, VPN, antivírus, antispam, proteção contra intrusos, controle de acessos, filtragem de conteúdos web, controle de aplicações, gestão de largura de banda e muito mais.

Figura 24: Cyberoam Netgenie
Fonte: Cyberoam, 2015.

Possui também o *Cyberoam Netgenie* funciona como uma appliance UTM (Unified Threat Management) wireless para pequenos escritórios e utilizadores domésticos. Este produto é capaz de criar uma zona wireless que fornece diversos benefícios: firewall, VPN, antivírus, IPS, 3G e controle de uso da Internet sobre websites e aplicações, tudo isto em roteador wireless.

3.4.7 CISCO

Figura 25: Logotipo Cisco
Fonte: Cisco, 2015.

A empresa Cisco Systems é uma companhia multinacional sediada em San José, Califórnia, Estados Unidos da América, com 47.000 empregados em todo o mundo. A atividade principal da Cisco é o oferecimento de soluções para redes e comunicações quer seja na fabricação e venda (destacando-se fortemente no mercado de roteadores e switches) ou mesmo na prestação de serviços por meio de suas subsidiárias: *Linksys, WebEx, IronPort e Scientific Atlanta* [CISCO, 2015].

Figura 26: Equipamentos Cisco
Fonte: Cisco, 2015.

O Dispositivo de Segurança Adaptativo da Cisco ASA é uma plataforma modular que fornece a próxima geração de segurança e serviços VPN para ambientes que variam de pequenas empresas e escritórios domésticos a empresas de pequeno e médio porte [CISCO, 2015]. Dentre os principais recursos estão:

Serviços de segurança: combinando com funcionalidades da Trend Micro na proteção contra ameaças e controle de conteúdo no campo da Internet, com soluções comprovadas Cisco para fornecer antivírus, antispyware, bloqueio de

arquivos, antispam, antiphishing, bloqueio e filtragem de URL e filtragem de conteúdos abrangentes.

Serviços de prevenção: previne contra invasões e atua de forma proativa para bloquear uma ampla gama de ameaças, incluindo worms, ataques na camada de aplicativos, ataques ao sistema operacional, rootkits, spyware, compartilhamento de arquivos *peer-to-peer* e sistemas de mensagens instantâneas.

Serviços de gerenciamento e monitoramento: de forma intuitiva e em um único dispositivo por meio do ASDM (*Cisco Adaptive Security Device Manager*) e serviços de gerenciamento de vários dispositivos, de classe empresarial, por meio do *Cisco Security Manager*.

Aumenta a produtividade do funcionário: previne a perda de produtividade impedindo a entrada de spams, spywares e navegação inapropriada na Web.

Habilita o acesso remoto seguro – funcionalidades para acesso remoto a rede sem a introdução de ameaças que coloquem em risco os negócios, usando as capacidades VPN exclusivas e protegidas contra ameaças da solução.

3.4.8 JUNIPER

Figura 27: Logotipo Juniper Networks
Fonte: Juniper Networks, 2015.

A Juniper Networks é uma empresa de TI e fabricante de produtos e equipamentos de rede, fundada em 1996. Ela é sediada em Sunnyvale, Califórnia, EUA. A empresa desenvolve e vende protocolos de internet. Os principais produtos da Juniper incluem roteadores, T-série, série M, série E, MX-séries e série J, switches da série EX e produtos de segurança da série SRX [JUNIPER NETWORKS, 2015].

Figura 28: Equipamentos Juniper Networks
Fonte: Juniper Networks, 2015.

O gerenciamento unificado de ameaças (UTM) é uma função opcional para a série SRX da Juniper que fornece um conjunto integrado de funcionalidades de segurança de rede, recursos de segurança para proteger contra vários tipos de ameaça, incluindo ataques de spam e phishing, vírus, trojans e arquivos infectados de spyware, controle de conteúdo na web.

Com UTM é possível configurar um conjunto abrangente de recursos de segurança que incluem antispam, antivírus, filtragem de conteúdo web e proteção de filtragem. As características UTM fornecem a capacidade de prevenir ameaças no dispositivo da série SRX, antes que as ameaças entrem na rede. Os seguintes módulos UTM são suportados [JUNIPER NETWORKS, 2015]:

Antispam: bloqueio e filtro de todo o tráfego de correio eletrônico, lista de quarentena com mensagens indesejadas pela verificação de entrada e bloqueio de tráfego de e-mail SMTP de saída usando uma combinação de spam e listas (SBL), sendo possível configurar manualmente listas negras e listas brancas.

Antivírus: recurso de antivírus que utilizam um mecanismo de varredura integrado e bancos de dados de assinatura de vírus atualizado para proteção contra vírus, trojans, rootkits, worms e outros tipos de códigos maliciosos que possam atingir os dispositivos da rede corporativa.

Filtragem da Web: filtragem de conteúdo permite que sejam definidas políticas de permissão ou bloqueio de acesso a sites específicos individualmente ou com base em categorias ao qual pertence o site. A filtragem de conteúdo fornece funcionalidade de prevenção de perda de dados também. A filtragem de conteúdo controla todo o tráfego baseado em MIME tipo, extensão de arquivo e tipos de protocolo.

A série SRX tem predefinidos perfis de sistema (antispam, antivírus ou filtragem de Web) projetados para fornecer proteção básica. É possível usar um perfil predefinido para habilitar as políticas de UTM ou criar de forma granular um componente (antispam, antivírus, filtragem da Web ou filtragem de conteúdo) em cada perfil.

3.4.9 PALO ALTO NETWORKS

Figura 29: Logotipo Palo Alto Networks
Fonte: Palo Alto Networks, 2015.

A Palo Alto Networks é uma empresa de segurança de rede americana com sede em Santa Clara, Califórnia. Os principais produtos da empresa são avançados firewalls, projetados para fornecer segurança de rede, visibilidade e controle granular da estrutura de rede com base na identificação do conteúdo, usuário e aplicativo. Seus produtos com o conceito "*Next Generation Firewall*" permitem uma visibilidade sem precedentes e controle granular de políticas de aplicações e conteúdo, por usuário, não apenas endereço IP, sem degradação de desempenho. Os firewalls Palo Alto Networks identificam com precisão e controlam as aplicações independentemente de porta, protocolo, tática evasiva ou criptografia SSL e examina o conteúdo para bloquear as ameaças e impedir vazamento de dados. A empresa oferece uma completa visibilidade e controle, reduzindo significativamente o custo total de propriedade através da consolidação de diversos dispositivos como IPS/IDS, SSL-VPN, filtros web, entre outros [PALO ALTO NETWORKS, 2015].

A plataforma de última geração da Palo Alto Networks, com o seu firewall, pode habilitar com segurança aplicativos para certos usuários, enquanto protege a rede contra o crescente número de ameaças. Desenvolvido a partir de uma tecnologia totalmente nova, seu firewall fornece funcionalidades exclusivas, buscando sempre por inovações.

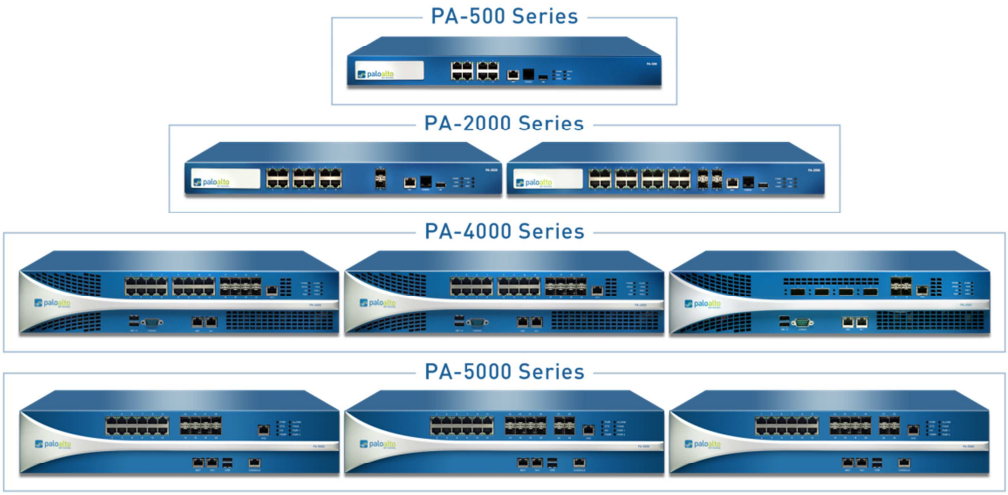

Figura 30: Equipamentos Palo Alto Networks
Fonte: Palo Alto Networks, 2015.

Inovação é o foco de tudo que a Palo Alto Networks faz. É a primeira empresa a definir e liderar a transição do firewall tradicional para o firewall de última geração, bem como a primeira a definir e liderar a transição de detecção para prevenção de malwares.

3.4.10 FORTINET

Figura 31: Logotipo Fortinet
Fonte: Fortinet, 2015.

A Fortinet é uma empresa mundial provedora de appliances para segurança de redes em alto desempenho fundada no ano 2000. Líder de mercado em gerenciamento unificado de ameaças (*UTM - unified threat management*) e nos firewalls de nova geração (*NGFW - next generation firewall*). Seus produtos e serviços oferecem proteção ampla, integrada e de alto desempenho contra ameaças dinâmicas (*ATP - advanced persistent threat*), simplificando a infraestrutura de segurança de TI. A Fortinet possui sede em Sunnyvale, Califórnia nos Estados Unidos com escritórios ao redor do mundo.

O principal produto da empresa o appliance de segurança Fortigate possui sua arquitetura baseada em circuitos específicos integrados para aplicações (*ASIC - Application-specific integrated circuit*) e integra múltiplas camadas de segurança projetadas para proteger contra ameaças de rede e aplicações [LDC, 2015].

Figura 32: Circuitos ASIC Fortinet
Fonte: LDC, 2015.

Figura 33: Portfólio de Produtos Fortinet
Fonte: LDC, 2015.

O sistema operacional do Fortigate, o *FortiOS*, possui recursos de firewalls de novas geração como: controle de aplicações, antivírus, IPS, filtro web, aceleração de WAN, otimização de tráfego de rede, VPN, DLP, controle de wireless e roteamento dinâmico [LDC, 2015].

A linha de soluções Fortinet complementares de produtos vai além do UTM para ajudar a proteger toda a rede corporativa. A suíte de soluções enquadra além do Fortigate: *rede sem fio gerenciada, gateway antispam, switches de rede, web application firewall, proteção de banco de dados, analise*

de vulnerabilidade de redes, gerenciamento de acesso e autenticação forte, application delivery control, VoIP, cache, proteção contra DDoS, entre outros.

Figura 34: Equipamentos Fortinet
Fonte: Fortinet, 2015.

A Fortinet desde 2009 é líder absoluta no quadrante mágico do Gartner na área de gerenciamento unificado de ameaças (UTM). Seus produtos são reconhecidos mundialmente através de diversos prêmios conquistados. O Fortigate é o produto de segurança com maior número de certificações de diversos órgãos independentes do mercado e seu modelo baseado em Chassi com *Blades* é reconhecido como o firewall mais rápido do mundo. A Fortinet se encontra hoje entre as três maiores empresas de Segurança da Informação no mercado de Network Security Appliance [FORTINET, 2015].

4 CONSIDERAÇÕES FINAIS

Uma lição que podemos tirar de tantas mudanças é que precisamos realmente pensar a frente do nosso tempo, investir em soluções não só para suprir as necessidades do momento, mas sim investir em soluções que venham agregar valor para o ambiente atual e futuro.

Não precisamos ser videntes pra saber realmente o que vem pela frente. Ameaças mais sofisticadas, acessos mais intensos e com tudo isso precisamos garantir a tão sonhada segurança no ambiente corporativo. Na próxima atualização das soluções de segurança na sua empresa, procure informações mais detalhadas sobre essas tecnologias de nova geração, que não só vão aumentar seu controle como também vão garantir a visibilidade e melhorar sua segurança digital.

A facilidade de uso e a geração de relatórios significativos no UTM serão fatores competitivos importantes à medida que os clientes buscam maximizar o valor de seus investimentos pela eliminação de práticas ineficientes e redução dos riscos de negócios. As empresas devem pré-selecionar os fornecedores dessas tecnologias que demonstraram um comprometimento com o desenvolvimento contínuo de seus produtos a fim de assegurar que seus investimentos sejam garantidos em relação às tecnologias em constante mudança e às ameaças digitais emergentes.

Em relação aos fabricantes de UTM podemos fazer alguns destaques:

- O UTM da Sophos apresentou políticas de firewall para aplicativos web como IIS e Apache, se mostrou polivalente, o filtro web é simples de configurar, é possível configurar uma gestão flexível do equipamento, podendo delegar controle de gerenciamento de algumas funcionalidades, é possível imprimir toda a configuração do equipamento para auditoria, a criação de relatórios é bem simplificada, o equipamento é bem recomendado para pequenas e médias empresas.

- A Cisco não tem um verdadeiro firewall UTM, os equipamentos da linha ASA ainda não possuem todas as funcionalidades e aplicações de um UTM, porém é um fornecedor conhecimento mundialmente e suas soluções podem ser implantadas em todos os tipos e tamanhos de rede.

- Nos dispositivos SRX da Juniper faltam alguns recursos importantes, como a inspeção HTTPS e recursos SSL VPN integrados. Como a Cisco, a Juniper também precisa melhorar seus firewalls e incorporar todas as funcionalidades de firewalls de UTM ou fornecer alguns recursos adicionais, como por exemplo, o controle da aplicação. Porém o sistema

operacional Junos que opera os equipamentos da Juniper apresenta progressos na área de comutação, roteamento e segurança.

- O Sonicwall, da Dell oferece boas soluções UTM tais como: e-mail, filtro web, SSL VPN e backup. Os equipamentos Sonicwall de pequeno e médio porte apresentam bons recursos de UTM, foram feitas excelentes melhores e o gerenciamento de rede sem fio integrado aos pontos de acesso Dell mostraram boa qualidade.

- ✓ WatchGuard é um fornecedor de segurança de com uma bom firewall UTM. WatchGuard não poupou esforços para simplificar processos dentro da interface de gerenciamento como o fornecimento de funcionaliade como arrastar e soltar dentro do console. A Watchguard têm uma solução madura, nos últimos anos tem sido um dos principais fornecedores de UTM, a Watchguard fornece um serviço de suporte e documentação útil, além de ter uma forte presença no mercado UTM.

- ✓ A Fortinet é líder de mercado, estão expandindo sua suíte de soluções para redes de computadores, tem boas funcionalidades como NAT, sniffer, recursos de prevenção de ameaças granular como: AV, DLP, controles de aplicações, IPS, NAC, boa capacidade de gerenciamento de pontos de acesso, consegue mapear tráfegos com base no país, domínios virtuais, tecnologia de aceleração de hardware patenteada e muitos outros recursos. A Fortinet também apresenta bom nível de inovação e é entre os firewalls corporativos também está entre os melhores.

REFERÊNCIAS

TANENBAUM, Andrew. S. **Redes de Computadores**. 4ª ed. São Paulo: Pearson Prentice Hall, 2011.

COMER, Douglas E. **Redes de Computadores e Internet**. 4ª ed. Porto Alegre: Bookman, 2007.

GIAVAROTO, Silvio César Roxo. **Backtrack Linux – Auditoria e Teste de Invasão em Redes de Computadores**, Rio de Janeiro: Editora Ciência Moderna Ltda, 2013.

GALVÃO, Ricardo Kléber M. **Introdução à Análise Forense em Redes de Computadores**, São Paulo: Novatec Editora, 2013.

ELEUTERIO, Pedro Monteiro da Silva. **Desvendando a Computação Forense**, São Paulo: Novatec Editora, 2010.

FILIPPETI, Marco Aurélio. **CCNA 4.1 Guia Completo de Estudo**, Florianópolis: Visual Books, 2008.

ASSUNÇÃO, Marcos Flávio Araújo. **Guia do Hacker Brasileiro**, São Paulo: VisualBooks, 2002.

ASSUNÇÃO, Marcos Flávio Araújo. **Segredos do Hacker Ético**. São Paulo: VisualBooks, 2012.

MITNICK - Kevin D.; **A Arte de Enganar**. Tradução: Kátia Aparecida Roque, São Paulo: Pearson Education, 2003.

TAM, Kenneth. **UTM Security with Fortinet: Mastering FortiOS**, Waltham: Syngress, 2012.

CAMERON, Rob. **Junos Security**, Sebastopol: O'Reilly, 2010.

FORTINET, **The Fortigate Cookbook**. **A Practical Guide to Getting the best from Your FortiGate**, Sunnyvale, 2012.

TORRES, Gabriel. **Redes de Computadores**, Rio de Janeiro: Novaterra Editora e Distribuidora Ltda, 2010.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa**, São Paulo: Atlas, 2010.

CISCO, Networking Academy. **CCNA Exploration – Fundamentos de Rede.** Cisco Systems, Inc., 2012-2014.

DIGITAL, **Revista Segurança Digital**, Edição 006, Maio 2012. Disponível em <www.segurancadigital.info>, acessado em 30/11/2014, 13:30.

BRASIL. Tribunal de Contas da União. **Boas Práticas em Segurança da Informação** / Tribunal de Contas da União. – 2. ed. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2007. Disponível em <http://portal2.tcu.gov.br/portal/pls/portal/docs/2059162.pdf>, acessado em 05/12/2015, 9:20.

BRASIL. Livro Verde: **Segurança Cibernética no Brasil** / Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização de Claudia Canongia e Raphael Mandarino Junior. – Brasília: GSIPR/SE/DSIC, 2010. Disponível em <http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf>, acessado em 10/12/2015, 15:15.

RODRIGUEZ, Chris. **Compreensão do gerenciamento unificado de ameaças (UTM) e dos firewalls de última geração (NGFWs)**. Disponível em <https://www.watchguard.com/international/br/resources/wg_frost-sullivan-report.pdf>, acessado em 10/01/2015, 10:45.

ITFRIENDS, **NGFW VS UTM.** Disponível em <http://www.itfriends.org/ngfw-vs-utm>, acessado em 31/03/2015, 17:00**.**

WATCHGUARD, **Informações da Watchguard e dos seus equipamentos UTM**. Disponível em <https://www.watchguard.com>, acessado em 02/04/2015, 8:45.

SOPHOS, **Informações da Sophos e dos seus equipamentos UTM**. Disponível em <https://www.sophos.com>, acessado em 03/04/2015, 10:30.

LDC, **Informações da Fortinet e dos seus equipamentos UTM**. Disponível em <http://www.ldc.com.br/fabricante/22/fortinet>, em 10/04/2015, 16:20

JUNIPER NETWORKS, **Informações da Juniper Networks e dos seus equipamentos UTM**. Disponível em <http://www.juniper.net/us/en/>, acessado em 04/04/2015, 9:15.

DELL**, Informações sobre a fabricante de equipamentos Dell**. Disponível em <http://www.dell.com/learn/us/en/uscorp1/about-dell>, acessado em 04/04/2015, 17:15.

SONICWALL, **Informações do Sonicwall equipamento UTM da Dell**. Disponível em <http://www.sonicwall.com/br/pt/solutions/Solutions-Unified-Threat-Management.html>, acessado em 05/04/2015, 14:50.

AKER, **Informações sobre a Aker Security Solutions e dos seus equipamentos UTM**. Disponível em <http://www.aker.com.br>, acessado em 05/04/2015, 16:30.

STORMSHIELD, **Informações sobre a Stormshield e dos seus equipamentos UTM**. Disponível em <http://www.stormshield.eu/network-protection/>, acessado em 06/04/2015, 8:20.

CYBEROAM, **Informações sobre a Cyberoam e dos seus equipamentos UTM**. Disponível em <http://www.cyberoam.com/>, acessado em 06/04/2015, 13:40.

CISCO, **Informações sobre a empresa Cisco e dos seus equipamentos UTM**. Disponível em <http://www.cisco.com/c/en/us/products/security/small-business-sa500-series-security-appliances/index.html>, acessado em 07/04/2015, 15:10.

PALO ALTO NETWORKS, **Informações sobre a empresa Palo Alto Networks e dos seus equipamentos NFGW**. Dísponivel em <https://www.paloaltonetworks.com/>, acessado em 08/04/2015, 08:25.

FORTINET, **Informações sobre a Fortinet e dos seus equipamentos UTM**. Dísponivel em <http://www.fortinet.com/>, acessado em 09/04/2015, 17:05.