Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

KLEYTHON KELL VICENTE BEZERRA

FIREWALL DE NOVA GERAÇÃO: PRINCIPAIS CARACTERÍSTICAS E DIFERENCIAIS TECNOLÓGICOS

Brasília
2015

KLEYTHON KELL VICENTE BEZERRA

FIREWALL DE NOVA GERAÇÃO: PRINCIPAIS CARACTERÍSTICAS E DIFERENCIAIS TECNOLÓGICOS

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Redes de Computadores com Ênfase em Segurança

Orientador: Prof. José Eduardo Malta de Sá Brandão

Brasília
2015

KLEYTHON KELL VICENTE BEZERRA

FIREWALL DE NOVA GERAÇÃO: PRINCIPAIS CARACTERÍSTICAS E DIFERENCIAIS TECNOLÓGICOS

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Redes de Computadores com Ênfase em Segurança

Orientador: Prof. José Eduardo Malta de Sá Brandão

Brasília, 10 de dezembro de 2015.

Banca Examinadora

_____

Prof. José Eduardo Malta de Sá Brandão

_____

Prof. Sylas Rodrigues Mendes

_____

Prof. Gilson Ciarallo

À Deus, por me abençoar com muita saúde e determinação para buscar todos meus objetivos.

AGRADECIMENTOS

Agradeço a Deus, por me conceder saúde e muita determinação para conseguir concluir mais essa etapa.

Agradeço minha família e amigos por toda paciência e apoio a mim em todos os momentos.

Agradeço também ao meu orientador e professor José Eduardo Brandão por todo conhecimento compartilhado em sala de aula e na orientação desse trabalho.

“Sentir com inteligência, pensar com emoção”
Humberto Gessinger

RESUMO

Com a evolução das tecnologias, das formas de acesso das aplicações e juntamente, além de tudo isso, com a evolução dos ataques, um firewall tradicional, atualmente não é mais suficiente para uma proteção adequada de um ambiente corporativo. Para acompanhar todos esses avanços se faz necessário a utilização de um NGFW, Next Generation Firewall, ou Firewall de Nova Geração. Esse trabalho se baseia no Firewall Palo Alto, que segundo o Gartner está entre os líderes no seguimento de firewall de nova geração em ambientes corporativos. Será mostrado ainda, os pilares da segurança da informação e alguns conceitos importantes, de vulnerabilidades, riscos e ataques. E por fim, tendo como principal objetivo mostrar os diferenciais tecnológicos de um NGFW e mostrar a facilidade de criação de uma política orientada em aplicação e usuário. Concluindo que nenhum ambiente é 100% seguro, que tanto as ameaças quanto as soluções estão em constante evolução e que é preciso conhecer muito bem as necessidades de seu ambiente, para assim poder buscar a melhor solução que se adeque as suas necessidades, em meio a tantas opções e com características distintas, ofertadas no mercado.

Palavras-chave: Firewall. Geração. Ataques. APT. UTM

ABSTRACT

With the evolution of technologies, forms of access applications and along top of that, with the evolution of the attacks, a traditional firewall, it is now no longer enough for proper protection of a corporate environment. To keep up with all these developments it is necessary to use a NGFW, Next Generation Firewall. This work is based in Palo Alto Firewall, which according to Gartner is among the leaders in the new generation of firewall monitoring in enterprise environments. It will be shown further, the information security pillars and some important concepts, like vulnerabilities, risks and attacks. Finally, the main objective is to show technological advantages of a NGFW and show the ease of creating a policy based on application and user. Concluding that thare is no environment 100% safe, that both the threats and the solutions are constantly evolving and it is very good knowledge of the needs of their environment, so that could seek the best solution that fits your needs, amid so many options and with different characteristics, offered in the market.

Key words: Firewall. Generation. Attacks. APT. UTM

LISTA DE ABREVEATURAS E SIGLAS

APTs: Ameaças Persistentes Avançadas (*Advanced Persistent Threat*)

ARP: Protocolo de Resolução de Endereços (*Address Resolution Protocol*)

DOD: Departamento de Defesa Americano (*United States Department of Defense*)

FTP: Protocolo de Transferência de Arquivos (*File Transfer Protocol*)

HTTP: Protocolo de Transferência de hipertexto (*Hypertext Transfer Protocol*)

ICMP: Protocolo de Mensagem para Controle da Internet (*Internet Control Message Protocol*)

IP: Protocolo da Internet (Internet *Protocol*)

IPS: Sistema de Prevenção de Intrusos (*Intrusion Prevention System)*

ISO: Organização Internacional para Padronização (*International Organization for Standardization*)

NGFW: Firewall de Nova Geração (*Next Generation Firewall*)

QOS: Qualidade de Serviço (*Quality of Service*)

RFC: Pedido para Comentários (*Request for Comments*)

SMTP: Protocolo de transferência de correio simples (*Simple Mail Transfer Protocol*)

TCP: Protocolo de Controle de Transmissão (*Transmission Control Protocol*)

UDP: Protocolo de Datagrama de Usuário (*User Datagram Protocol*)

URL: Localizador Padrão de Recursos (*Uniform Resource Locator*)

UTM: Gerenciamento Unificado de Ameaças (*Unified Threat Management*)

VPNs: Redes Privadas Virtuais (*Virtual Private Networks*)

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Nesse trabalho serão abordados assuntos referentes a segurança da informação e seus pilares, além de uma definição e entendimento das soluções de firewall e de firewall de nova geração, com suas principais características e diferenciais.

Para facilitar o entendimento, implementação e a necessidade de uma dessas soluções devemos entender bem o que são as vulnerabilidades, as ameaças, os riscos e principalmente o avanço dos ataques. Partindo da explicação desses principais conceitos podemos entender o que são as soluções de firewall, passar pelas principais características em suas gerações até chegar nos atuais firewalls de nova geração, onde o foco é mostrar as principais características e diferenciais tecnológicos dessa solução, utilizando como base o firewall Palo Alto e a partir de então poder mostrar a forma de construção de políticas orientadas a aplicações.

Objetivos:

Objetivo Geral:

Apresentar um firewall tradicional e um firewall de nova geração.

Objetivos Específicos:

- Apresentar Firewall e principais características por todas suas gerações
- Apresentar Firewall de Nova Geração, suas principais características e diferenciais tecnológicos.
- Apresentar Comparativo entre Firewall de Nova Geração e Gerenciamento Unificado de Ameaças (UTM)
- Mostrar a forma prática de construção de políticas em um firewall de nova geração, orientada a aplicação.

Justificativa

Sabemos que nenhuma rede ou sistema é 100% seguro e que a simples instalação de um firewall não garante que a rede está segura contra invasores. Sabemos ainda que o firewall não é a única solução de segurança em um ambiente corporativo e que o mesmo trabalha em conjunto com várias outras soluções buscando, em conjuntos, uma maior proteção.

Com os passar dos anos, com a evolução das aplicações e juntamente com a evolução dos ataques sabemos que um firewall tradicional, que faz análise de cabeçalho não é mais suficiente para proteger eficientemente ambientes corporativos e por isso se faz necessário conhecer um Firewall de Nova Geração e todas novidades que essa solução traz para a segurança.

Procedimentos Metodológicos

Foi realizada uma pesquisa na literatura impressa como livros e normas técnicas. Realizado ainda uma pesquisa em literatura e artigos *online*, como sites de fabricantes e empresas relacionadas à segurança da informação, rede de computadores e firewall, buscando os tópicos mais relevantes para chegarmos no entendimento dos pilares da segurança da informação, dos conceitos de firewall e firewall de nova geração, assim como seus diferenciais.

Essa pesquisa ainda descreve algumas vulnerabilidades encontradas em firewalls com seus respectivos riscos.

Por fim foi mostrado de forma prática a forma de criação de uma política em um firewall de nova geração, onde a orientação é feita com base em aplicações e usuários, conseguindo assim uma facilidade e granularidade nas configurações.

A forma como as informações são expostas nessa pesquisa tem o objetivo de ajudar os profissionais de segurança da informação a conhecer melhor os diferentes tipos de firewall e com isso fazer uma escolha mais assertiva de acordo com as necessidades do ambiente onde o mesmo será inserido.

O presente trabalho foi então estruturado em 4 capítulos.

No primeiro capítulo, apresentam-se conceitos iniciais importantes para o melhor entendimento dos demais assuntos apresentados. O segundo capítulo proporciona uma apresentação dos pilares da segurança da informação. No terceiro capítulo é apresentado o conceito de *firewall* e suas gerações. No quarto e último capítulo é apresentado um *firewall* de nova geração, suas principais características e mostrado ainda como criar uma política orientada a aplicação.

1 CONCEITOS INICIAIS

Para o melhor entendimento de vários assuntos que serão abordados nesse trabalho se faz necessário conhecer alguns conceitos iniciais.

1.1 Arquitetura TCP/IP (*Transmission Control Protocol / Internet Protocol)*

Segundo a RFC1594 (1994) TCP/IP é o nome comum para uma família com mais de 100 protocolos para comunicação de dados utilizados para organizar computadores e para comunicação de dados de equipamentos para redes de computadores. Ainda segundo a mesma RFC, TCP/IP é uma abreviação comum que se refere ao conjunto de protocolos de aplicação e de transporte que ocorrem sobre IP.

Segundo Filippetti (2008)**,** o padrão TCP/IP foi criado pelo Departamento de Defesa Americano (DoD) para garantir a preservação da integridade dos dados, assim como manter a comunicação de dados no advento de uma guerra. Se bem planejada uma rede baseada na combinação de protocolos (*suíte*) TCP/IP pode ser independente, confiável e muito eficiente.

O TCP/IP tem como referência um modelo de quatro camadas. Todos os protocolos que pertencem ao conjunto de protocolos TCP/IP estão localizados nas três camadas superiores desse modelo.

Segundo Tabenbaum (2003), as quatro camadas desse modelo são: aplicação, transporte, internet e host-rede.

1.2 Datagrama e Fragmentação

Segundo a RFC 1594 (1994) um Datagrama é uma entidade de dados completa e independente que contém informações suficientes para ser roteada da origem ao destino sem precisar confiar em trocas anteriores entre essa máquina de origem e destino e a rede de transporte.

Dessa forma a operação no modo datagrama é uma comunicação não confiável, não sendo usado nenhum tipo de reconhecimento fim a fim ou entre nós intermediários, nem qualquer tipo de controle de fluxo. No datagrama, o caminho através da rede é definido para cada pacote individualmente e é possível ainda tentar usar sempre o melhor caminho possível.

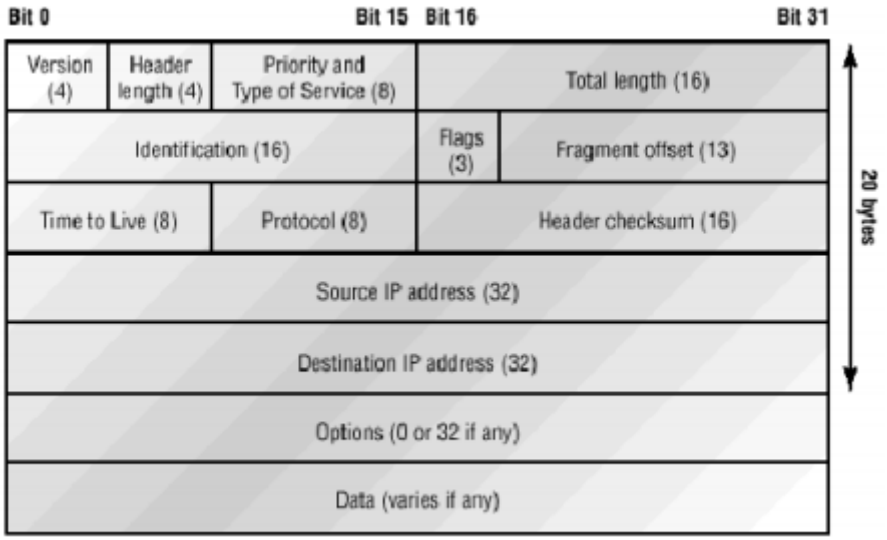
Algumas vezes é necessário fragmentar um datagrama. Isso ocorre quando ele tiver que, para chegar ao seu destino, transitar numa rede incapaz de transportar datagramas com a dimensão que aquele possui. A fragmentação pode ser feita no próprio computador de origem, e/ou em algum dos ativos onde o mesmo irá encontrar pelo caminho, como roteadores. A remontagem desses fragmentos acontecerá apenas no seu destino final.

1.3 Protocolo IP

Segundo Filippetti (2008)**,** Protocolo IP (*Internet Protocol*): O IP, poderia ser visto como um protocolo onipresente, no sentido de que está a par de todas as redes interconectadas. Isso é possível por que todos os dispositivos de rede possuem um endereço lógico chamado " endereço IP ". O protocolo IP efetua uma análise desse endereço para cada pacote de dados que recebe. Em seguida, utilizando uma tabela de roteamento, ele decide para onde o pacote deve ser enviado.

A identificação de dispositivos na rede requer que duas perguntas sejam respondidas: Em qual rede esse dispositivo se encontra? E qual seu endereço nessa rede? A primeira resposta é o endereço lógico (análogo ao nome de uma rua em um endereço de correspondência). A segunda, o endereço físico (a analogia agora seria o número da casa na rua). O IP recebe os segmentos, os encapsula em pacotes ou datagramas. No lado destinatário, o IP então remonta esses datagramas de volta em segmentos. Cada datagrama recebe o endereço IP do transmissor e do destinatário.

Figura 01 – Cabeçalho IP



Fonte FILIPPETI, Marco Aurélio

A figura acima ilustra os campos do cabeçalho ip.

Ainda segundo o mesmo autor, podemos definir esses campos:

Version**:** Número da versão do protocolo;

HLEN**:** Comprimento do cabeçalho;

Priority **ou ToS (** ***Type of service*****):** Indica como o datagrama deve ser manipulado. Os primeiros 3 bits definem a prioridade;

Total Lenght**:** Comprimento total do pacote, incluindo o cabeçalho;

Identification**:** Valor único para a identificação do pacote;

Flags**:** Especifica se a fragmentação deve ou não ocorrer;

Flag offset**:** Provê fragmentação e remontagem se um pacote de dados for muito extenso para ser colocado em um *frame*. Também permite diferentes

unidades máximas de transmissão (*Maximum Transmission Units* - MTUs) na internet.

TTL (*Time to Live*/ Tempo de Vida): O Valor TTL é estabelecido quando um pacote é originalmente gerado. Ele estebelece o tempo de vida do pacote através de diferentes métricas (número de saltos, tempo etc). Se o pacote não atingir seu destino antes de o timer TTL expirar, ele é descartado. Isso impede pacotes IPs de circularem continuamente pela internet, gerando loopings;

***Protocol*:** Número da porta lógica do protocolo de camada superior (Transporte). A porta TCP é 6 e a UDP é 17, em hexadecimal.

Header Checksum: Checagem de redundância (aplicada ao cabeçalho, apenas);

Source IP address: Endereço IP de origem (32-bits);

Destination IP address: Endereço ip de destino (32-bits);

IP option: Campo utilizado em testes de rede (debugging);

***Data*:** Dados enviados pela camada superior (Transporte).

1.4 Camada de Aplicação

Segundo Filippetti (2008)**,** a Camada de Aplicação é responsável pela definição dos protocolos necessários para a comunicação ponto a ponto pelas aplicações, bem como pelo controle e especificações da interface com o usuário.

Segundo Tabenbaum (2003), acima da camada de transporte, encontramos a camada de aplicação. Ela contém todos os protocolos de nível mais alto. Dentre eles estão o protocolo de terminal virtual (TELNET), o protocolo de transferência de arquivos (FTP) e o protocolo de correio eletrônico (SMTP). O protocolo de terminal virtual permite que um usuário de um computador se conecte a uma máquina distante e trabalhe nela. O protocolo de transferência de arquivos permite mover dados com eficiência de uma máquina para outra. Originalmente, o

correio eletrônico era um tipo de transferência de arquivos; no entanto, foi desenvolvido mais tarde um protocolo especializado para essa função (o SMTP).

2 SEGURANÇA DA INFORMAÇÃO

A segurança da informação está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

Segundo Sêmola (2003), a Segurança da Informação é uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

Caruso & Steffen (2006) afirmam que o bem mais valioso de uma empresa pode não ser o produto fabricado por seus operários ou o serviço prestado ao cliente, mas as informações relacionadas a esse bem de consumo ou serviço.

Como podemos encontrar na norma ISO 27001 (2013), a segurança engloba: as medidas físicas e as medidas lógica.

Podemos citar como exemplos de medidas físicas:

- Organizações que possuem funções públicas como: Bibliotecas, prefeituras e que utilizam controle de acesso.
- Organizações privadas que estabelecem áreas restritas para proteger novos conhecimentos, como um novo lançamento ou novas tecnologias.

Como exemplo de medida lógica podemos citar:

- A Gestão de acesso lógico: Utilizada para permitir acesso a informação digital e a serviços de informação por pessoas autorizadas e impedir o acesso das que não são autorizadas.

Em cada um desses ambientes encontraremos riscos próprios, ameaças potenciais, controles aplicáveis e soluções de segurança que podem minimizar o nível de exposição no qual um ambiente possa estar comprometido, com o objetivo de garantir segurança para o seu principal patrimônio: a informação.

2.1 Princípios básicos da Segurança da Informação

Segundo Sêmola (2003) a segurança da informação é uma área de conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade, como pratica de gestão de riscos de incidentes que atinjam diretamente a confidencialidade, integridade e disponibilidade da informação. Segundo a norma NBR ISO/IEC 27002 (2013), podemos definir:

Confidencialidade: É a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso.

Integridade: é a garantia da exatidão e completeza da informação e dos métodos de processamento.

Disponibilidade: É a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2.2 Ameaças

O processo de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade, caracteriza-se como Segurança Informação. (BEAL, 2005).

A norma ISO 27002 (2013) afirma que a Segurança da Informação é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades.

Segundo Campos (2007), a ameaça pode ser considerada um agente externo ao ativo de informação, pois se aproveita de suas vulnerabilidades para quebrar a os princípios básicos da informação – a confidencialidade, integridade ou disponibilidade.

As ameaças podem ser, naturais: são aquelas que se originam de fenômenos da natureza; involuntárias: são as que resultam de ações desprovidas de intenção para causar algum dano, e intencionais: são aquelas deliberadas, que objetivam causar danos, tais como hacker. (DANTAS, 2011).

2.2.1 Ameaças Persistentes Avançadas (APTs)

Para Deloitte (2011) as APT's (ameaças persistentes avançadas) são uma versão automatizada da espionagem dita tradicional. Além de serem difíceis de detectar também o são de combater. Ao se introduzirem num sistema de informação da empresa ou organização, fazem-no de forma quase invisível e criam um modo para subtrair os dados de informação que pretendem.

Segundo a Kaspersky, APT´s são pouco intuitivas. Quando pensamos em cibercriminosos e outros disseminadores de malware imaginamos que o objetivo deles seja contaminar todos os computadores possíveis com suas credenciais de furtos, botnets ou outros softwares maliciosos. Quanto maior a rede, mais oportunidades para roubar dinheiro, benefícios e qualquer coisa que estejam procurando. Mas os agressores de APT estão interessados em atingir computadores específicos. O objetivo final de um ataque APT é atingir a máquina em que exista algum tipo de informação valiosa.

Segundo a Palo Alto Networks, ataques cibernéticos avançados estão empregando métodos sofisticados e persistentes para enganar a segurança tradicional. É preciso que as equipes modernas de segurança reavaliem suas crenças de que os sistemas tradicionais de prevenção de intrusão, antivírus e ferramentas de *sandbox* podem tranquilamente derrotar as APTs.

2.3 Vulnerabilidades

Segundo Wadlow (2000), as vulnerabilidades são os pontos fracos existentes nos ativos, que quando explorados por ameaças, afetam a confiabilidade, a disponibilidade e a integridade das informações de uma pessoa ou organização.

A ISO 27002 (2013) define a vulnerabilidade como uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Para Dantas (2001), As vulnerabilidades podem advir de vários aspectos: instalações físicas desprotegida contra incêndios, inundações e desastres naturais; material inadequado empregado nas construções; ausência de política de segurança para RH; funcionários sem treinamento e insatisfatório nos locais de trabalho; ausência de procedimento de controle de acesso e utilização de equipamentos por pessoal contratado; equipamento obsoletos, sem manutenção e sem restrições para sua utilização; software sem *patch* de atualização e sem licença de funcionamento.

Segundo a Cartilha de Segurança para Internet (versão 4.0 / CERT.br), uma vulnerabilidade e definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede. Um ataque de exploração de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.

Sabemos que não existem ambientes e soluções 100% seguras e com os firewalls isso não seria diferente. Nessas ferramentas também encontraremos falhas e vulnerabilidades.

Segundo Kamara et al. (2003), a vulnerabilidade do firewall é definida como um erro cometido durante o desempenho do firewall, implementação, configuração ou, que pode ser explorada para atacar a rede de confiança que o firewall é designado a proteger.

Segundo Geus e Pouw (1996), algumas vulnerabilidades na arquitetura do firewall são encontradas como: falhas no software; vulnerabilidade do meio físico; negação de serviços e ataques de baixo nível que possam afetar a disponibilidade, a confidencialidade e a integridade das informações.

É muito importante entendermos a definição das vulnerabilidades citadas e mais do que isso, compreender as possíveis consequências de suas explorações em firewalls.

2.3.1 Falhas de software

Segundo Geus e Pouw (1996), falhas de software são comportamentos inesperados de programas, quer seja por falha de projeto e/ou implementação. Quanto maior a complexidade e tamanho de um programa, mais difícil é " prever" seu comportamento e consequentemente garantir que este não apresente falhas que possam comprometer a segurança do sistema a qual pertença.

Consequências: Conforme Von Zuben e Henriques (2009), algumas falhas são de se esperar, com relação aos erros apresentados nos softwares, dentre elas se destacam: instalações indevidas: instalação não autorizada do software cliente, afetando com isso a Disponibilidade, a Integridade e a Confidencialidade das informações

2.3.2 Vulnerabilidades do meio físico

Conforme Geus e Pouw (1996), as deficiências da tecnologia ethernet, que constitui a maior parte das redes locais, expõem ainda mais as fragilidades da Internet. Os principais problemas estão relacionados com: a facilidade de se realizar grampo e o falso mapeamento entre endereço de rede (IP) e endereço fixo (ARP).

Consequências: Conforme Geus e Pouw (1996), podemos ter 2 consequências:

Grampeando a Rede: Sendo ethernet uma tecnologia de rede onde o meio físico é compartilhado, é possível configurar a interface de rede de uma máquina em modo "promíscuo", e assim receber todos os quadros transmitidos no meio. Geralmente tem-se por objetivo obter informações privilegiadas, como por exemplo senhas, mas também pode usar tal facilidade como passo na implementação de ataques mais sofisticados, afetando assim a Confidencialidade das informações.

Falso Mapeamento entre Endereço IP e Endereço Ethernet (ARP): o protocolo ARP (*Address Resolution Protocol*) mapeia um endereço IP em endereço ethernet enviando um broadcast com o endereço IP desejado. A máquina que tiver o endereço IP procurado, ou alguma outra agindo em nome daquela, responde com o

par: endereço IP- endereço ethernet. Uma máquina mal-intencionada pode então enviar respostas falsas, desviando todo o tráfego para si, tendo como objetivo personificar uma máquina, ou mais sutilmente, modificar os dados que estiverem sendo transmitidos entre duas outras máquinas, afetando com isso a Integridade das informações.

2.3.3 Negação de serviços

Segundo Kamara et al. (2003), isso ocorre quando uma vulnerabilidade é explorada para interromper um serviço prestado ao usuário legítimo. Serviços no contexto pode variar de encaminhamento de pacotes ou tradução de endereços de rede da administração.

Consequência: Conforme Geus e Pouw (1996), durante a negação de serviços há a interrupção de funcionamento de serviços de um computador ou sistema, por meio da saturação de seus recursos, afetando com isso a Disponibilidade e a Integridade das informações.

2.3.4 Ataques de baixo nível

Conforme Geus e Pouw (1996), os firewalls estão sujeitos a ataques de baixo nível que exploram deficiências nas implementações das camadas mais baixas do protocolo TCP/IP, e também por sondagens externas que procuram por tais vulnerabilidades.

Consequências: Através desse ataque pode-se afetar a Disponibilidade e a Integridade das informações.

2.4 Riscos

Segundo a norma ISO 27005 (2013), risco é a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, desta maneira prejudicando a organização.

Ainda de acordo com a norma, na etapa de análise de riscos, são identificados os eventos que podem causar perdas, ou seja, as ameaças. Logo após, devemos identificar os controles existentes e a sua eficácia em evitar que uma ameaça explore uma vulnerabilidade. Com a informação das ameaças e da efetividade dos controles, podemos identificar o nível de risco.

Quanto mais uma organização conhece os riscos mais ela pode decidir o que fazer em relação a cada um deles.

A mesma norma ainda trata da avaliação do risco (análise das consequências). Segunda ela, a avaliação de riscos tem como entrada uma lista de riscos com níveis de valores designados e como saída uma lista de riscos ordenados por prioridades.

2.5 Ataques

Segundo a Cartilha de Segurança para Internet (versão 4.0 / CERT.br), ataques costumam ocorrer na Internet com diversos objetivos, visando diferentes alvos e usando variadas técnicas. Qualquer serviço, computador ou rede que seja acessível via Internet pode ser alvo de um ataque, assim como qualquer computador com acesso à Internet pode participar de um ataque.

Os motivos que levam os atacantes a desferir ataques na Internet sao bastante diversos, variando da simples diversão até a realização de ações criminosas. Alguns exemplos são:

Demonstração de poder: mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente.

Prestıgio: vangloriar-se, perante outros atacantes, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar sites considerados visados ou difíceis de serem atacados; disputar com outros atacantes ou grupos de atacantes para revelar quem consegue realizar o maior número de ataques ou ser o primeiro a conseguir atingir um determinado alvo.

Motivações financeiras: coletar e utilizar informações confidenciais de usuários para aplicar golpes

Motivações ideológicas: tornar inacessível ou invadir sites que divulguem conteúdo contrário a opinião do atacante; divulgar mensagens de apoio ou contrarias a uma determinada ideologia.

Motivações comerciais: tornar inacessível ou invadir sites e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas.

3 DEFINIÇÃO DE FIREWALL

Segundo Gonçalves (1997) firewalls podem ser definidos como simples pontos de conexão entre duas redes não confiáveis que permitem que a comunicação entre elas seja monitorada e segura. Sua funcionalidade básica consiste em oferecer segurança para os componentes localizados dentro da rede sendo protegida, controlando e autenticando quem pode e quem não pode ter acesso à rede. Segundo Cheswick e Bellovin (1997), um *firewall* é composto por uma coleção de componentes localizados entre duas redes que coletivamente possuem as seguintes características:

- Todo tráfego de dentro para fora e de fora para dentro deve passar pelo *firewall*;
- Somente o tráfego autorizado, de acordo com alguma política de segurança local, poderá passar;

Para compreender melhor, você pode imaginar um *firewall* como sendo uma portaria de um condomínio: para entrar, é necessário obedecer a determinadas condições, como se identificar, ser esperado por um morador e não portar qualquer objeto que possa trazer riscos à segurança; para sair, não se pode levar nada que pertença aos condôminos sem a devida autorização.

Neste sentido, um *firewall* pode impedir uma série de ações maliciosas: por exemplo um código malicioso que utiliza determinada porta para se instalar em um computador sem o usuário saber, um programa que envia dados sigilosos para a internet, uma tentativa de acesso à rede a partir de computadores externos não autorizados, entre outros.

3.1 Funcionamento de um Firewall

Em um modo mais restritivo, um firewall pode ser configurado para bloquear todo e qualquer tráfego no computador ou na rede. O problema é que esta condição isola este computador ou esta rede, então pode-se criar uma regra para que, por exemplo, todo aplicativo aguarde autorização do usuário ou administrador para ter seu acesso liberado. Esta autorização poderá inclusive ser permanente: uma vez dada, os acessos seguintes serão automaticamente permitidos.

Em um modo mais versátil, um *firewall* pode ser configurado para permitir automaticamente o tráfego de determinados tipos de dados, como requisições HTTP (sigla para *Hypertext Transfer Protocol* - protocolo usado para acesso a páginas *Web* e definido pela RFC 2616), e bloquear outras, como conexões a serviços de e-mail.

Perceba, com estes exemplos, que as políticas de um *firewall* são baseadas, inicialmente, em dois princípios: todo tráfego é bloqueado, exceto o que está explicitamente autorizado; todo tráfego é permitido, exceto o que está explicitamente bloqueado.

O trabalho de um *firewall* pode ser realizado de várias formas. As principais categorias principais de funcionamento de um *firewall* são: filtro de pacotes com e sem inspeção de estados e *firewall* de aplicação. O que define uma metodologia ou outra são fatores como critérios do desenvolvedor, necessidades

específicas do que será protegido, características do sistema operacional que o mantém, estrutura da rede e assim por diante. É por isso que podemos encontrar mais de um tipo de *firewall*.

3.2 *Firewall Stateless*

Segundo Strebe e Perkins (2002), os filtros podem ser configurados para operar com base em qualquer parte do cabeçalho do protocolo IP, mas a maioria só pode ser configurada para filtrar os campos de dados mais úteis, como: o Tipo de protocolo, Endereço IP e Porta TCP/UDP

a) Filtragem de protocolos: essa filtragem filtra os pacotes com base no conteúdo do campo do tipo de protocolo IP. Então, o campo de protocolo pode ser utilizado para discriminar todo um conjunto de serviços, como: UDP, TCP, ICMP e IGMP.

b) Filtragem de endereços IP: permite limitar as conexões para e de hosts e rede específicos com base em seus endereços IP. Um ponto bem importante é que um filtro só pode limitar os endereços com base no conteúdo do campo que

Identifica o endereço IP.

c) Portas TCP/UDP: são aquelas habitualmente mais utilizadas na filtragem porque seu campo de dados indica mais especificamente para que serve o pacote. Diferentemente do que acontece na filtragem de IPs, o bloqueio de algumas portas ainda é útil, pois a maior parte das atividades dos atacantes se concentra somente em alguns protocolos específicos.

Ainda segundo o mesmo autor, os filtros de pacotes sem estados (*stateless*) sofrem de dois problemas que impedem que sejam totalmente eficazes:

• eles não verificam a parte útil de dados dos pacotes.

• eles não guardam o estado das conexões.

Esses problemas fazem com que os filtros sem estado sejam insuficientes se aplicados sozinhos para proteger uma rede.

3.3 *Firewall Stateful*

Segundo Strebe e Perkins (2002), os filtros de pacotes com estados lembram-se do estado das conexões da rede e das camadas da sessão gravando informações sobre o estabelecimento da sessão que passa através do *gateway* do filtro. Os filtros usam então essa informação para discriminar pacotes de retorno válido, das tentativas de conexão inválidas ou de invasão. Por outro lado, também, os filtros de pacotes com estados não permitem nenhum serviço passar pelo *firewall*, a não ser que esteja programado para isso.

Os *firewalls* de inspeção analisam todo o tráfego de dados para encontrar estados, isto é, padrões aceitáveis por suas regras e que, a princípio, serão usados para manter a comunicação. Estas informações são então mantidas pelo firewall e usadas como parâmetro para o tráfego subsequente.

Para entender melhor, suponha que um aplicativo iniciou um acesso para transferência de arquivos entre um cliente e um servidor. Os pacotes de dados iniciais informam quais portas TCP serão usadas para estas tarefas. Se de repente o tráfego começar a fluir por uma porta não mencionada, o *firewall* pode então detectar esta ocorrência como uma anormalidade e efetuar o bloqueio.

3.4 *Firewall* UTM

Para 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.

Segundo a empresa Kaspersky, A gestão unificada de ameaças, normalmente designada UTM, é um termo de segurança da informação que se

refere a uma solução de segurança única, e normalmente um aparelho de segurança único, que fornece diversas funções de segurança num ponto único da rede. A principal atração desta solução é a sua simplicidade. As organizações podem ter fornecedores ou aparelhos individuais para cada tarefa de segurança específica ou obtê-las todas de um fornecedor global, apoiado por uma equipa ou segmento de TI, executadas a partir de um console.

Para a empresa Sonicwall, 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.

4 FIREWALL DE NOVA GERAÇÃO

A internet cresceu muito e paralelo isso houve uma grande evolução das aplicações que nela trafegam e da dinâmica dentro dos ambientes corporativos. Hoje não é mais tão simples e seguro vincular as aplicações a portas específicas, assim como vincular usuários a endereços IPs. A maioria das aplicações mais utilizadas no dia a dia de uma empresa estão trafegando hoje nas portas 80(http)[1] e 443(https)[2], sabendo disso os ataques também se modernizaram e estão se aproveitando disso para serem cada vez mais efetivos.

Com esse avanço, tanto das aplicações quanto dos ataques, os *firewalls* stateful e UTM não são mais efetivos como eram no passado e com o avanço dessas soluções chegamos hoje ao que chamamos de Firewall de Nova Geração ou *Next Generation Firewall* (NGFW), que ainda não é um conceito regulamentado, mas que veremos várias características fundamentais para identificar essas soluções.

---

[1] HTTP, protocolo de transferência hipertexto, usado tradicionalmente para acesso as páginas web. Utiliza por padrão a porta 80.
[2] HTTPS, protocolo de transmissão segura. Permite transmitir dados de forma encriptada. Utiliza a porta 443.

Há algum tempo que o conceito de 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).

Para o Gartner[3], os Firewalls de Nova Geração são firewalls de inspeção de pacote em profundidade que vão além da inspeção de porta e protocolo e atua em nível de inspeção de aplicativo, prevenção de intrusão e trazem inteligência de fora 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.

Segundo a NSSLabs[4], Firewall de Nova Geração ou *Next-Generation Firewall* (NGFW) integra prevenção de intrusão, controle e identificação de aplicação e criação de regras por usuários e grupos.

4.1 Principais Características dos Firewalls de Nova Geração

Segundo o Gartner, as funcionalidades mínimas para um Firewall de Nova Geração, são:

- Funcionalidades de um *firewall* tradicional;
- IPS integrado;
- Controle de aplicação;
- Identificação de usuários.

Como não há uma regulamentação desse conceito, o que encontramos são requisitos mínimos definidos por grandes empresas que realizam testes nesses segmentos de soluções.

---

[3] http://www.gartner.com/it-glossary/next-generation-firewalls-ngfws
[4] http://www.nsslabs.com

Além das funcionalidades mínimas, cada fabricante adiciona novas *features* com intuito de ter uma solução mais completa e eficiente. Por isso, antes de decidir sobre a escolha de uma solução de *firewall* de nova geração é muito importante conhecer as várias soluções de mercado, como cada uma trabalha e como cada uma vai atender as suas necessidades.

4.2 Comparativo entre *Firewall* de Nova Geração e UTM

O presidente da *Anitian Enterprise Security*, Andrew Plato, desenvolveu um comparativo a fim de provar esse ponto de vista em relação conceitual das soluções de UTM e de NGFW, 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).

Figura 02 - Comparativo Firewalls UTM e Firewalls de Nova Geração.

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

Fonte: ITFriends, 2015.

Na figura abaixo, podemos verificar ainda de forma mais macro algumas funcionalidades de acordo com as gerações dos *firewalls*, sem levar em consideração um fabricante específico.

Figura 03 - Comparativo Gerações dos Firewalls

Gerações	Filtragem de Protocolos	Filtragem de Endereços IP	Filtro de Pacotes com Estados	IPS	VPN	Inspeção Camada 7
1a. Geração	✓	✓				
2a. Geração	✓	✓	✓			
UTM	✓	✓	✓	✓	✓	
NGFW	✓	✓	✓	✓	✓	✓

Fonte: Próprio Autor, 2015.

Após analisarmos o comparativo, fica evidente a similaridade entre essas duas soluções do ponto de vista de funcionalidades.

A maioria dos fornecedores de segurança de rede estão oferecendo controle e visibilidade de aplicativos, adicionando assinaturas de aplicativo ao mecanismo IPS ou oferecendo uma licença adicional para um módulo de controle de aplicativos. Em ambos os casos, estas opções são adicionais a um *firewall statefull* ou UTM.

4.3 Avaliação Do *Firewall* de Nova Geração Palo Alto

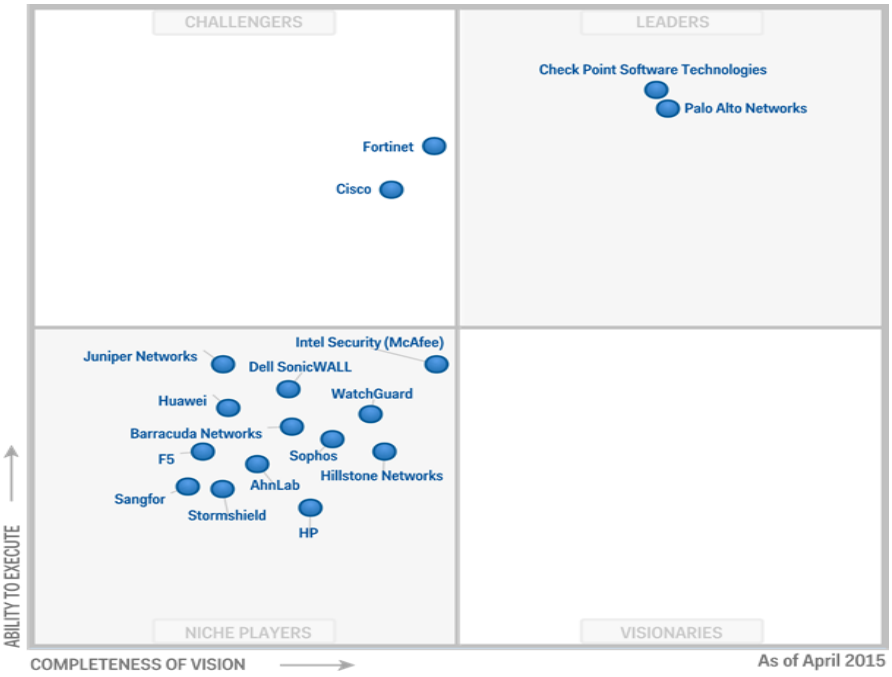
O *firewall* de última geração avaliado, inspeciona todo o tráfego, incluindo os aplicativos, ameaças e conteúdos relacionados com o usuário, independente da sua localização ou do tipo de dispositivo. Aplicativos, usuários e conteúdos são os elementos fundamentais para gerir os negócios e, portanto, componentes integrais da sua política de segurança empresarial. O resultado é a habilidade de alinhar a segurança com as principais iniciativas de negócios.

A empresa Gartner, que trabalha com consultoria, pesquisa e avaliação de soluções desenvolveu um gráfico matriz chamado de Quadrante Mágico. Essa matriz é dividida em quatro quadrantes: Líderes, Desafiadores, Visionários e Nichos de mercado, nessa ordem de importância. Esse gráfico é dividido em dois eixos. Na horizontal é avaliada a visão da empresa em termos de inovação tecnológica e

abrangência sobre as necessidades do mercado. Na vertical, o relatório traz o quanto as empresas têm habilidade de executar, implantar o que prometem.

O gráfico mostrado na figura abaixo traz o último relatório lançado para *Firewall* de Rede Corporativa, onde podemos ver a solução avaliada nesse trabalho no quadrante de líderes de mercado.

Figura 04 - Quadrante Mágico do Gartner para Enterprise Network Firewalls.



Fonte: Gartner 2015

Principais funcionalidades desta solução:

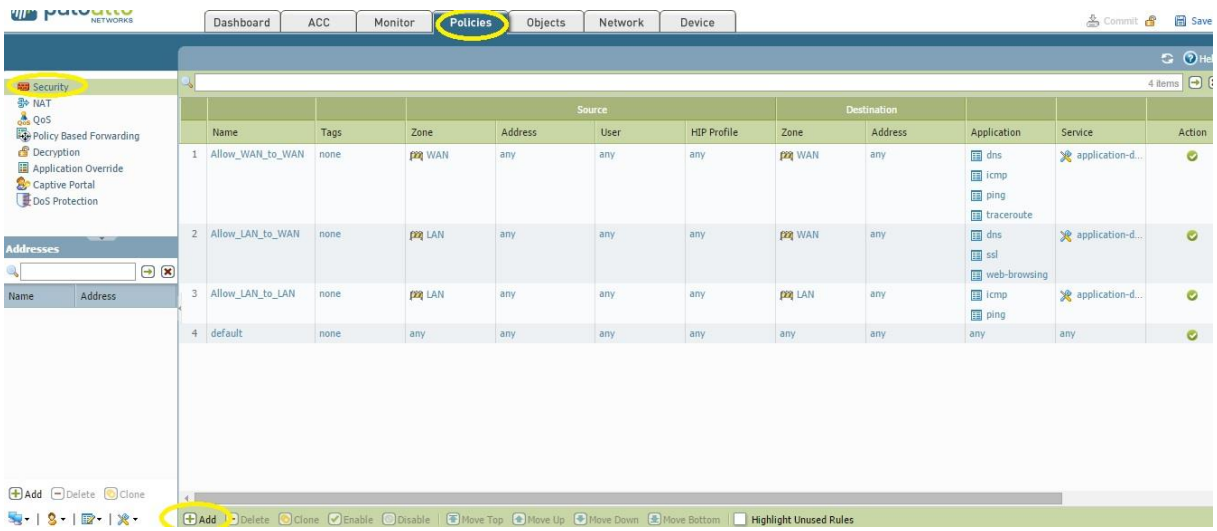
- Identificam aplicativos independente da porta, protocolo, tática evasiva ou criptografia.
- Identificam usuários independente do dispositivo ou endereço IP.
- Protegem em tempo real contra ameaças conhecidas e desconhecidas integradas aos aplicativos.
- Fornecem visibilidade e controle minucioso de políticas sobre os aplicativos, usuários e conteúdo.
- Fornecem implantação em linha previsível e multi-gigabit.

4.4 Criação de política baseada em aplicação e usuário

Para demonstrar a forma de criação de políticas nessa solução, será criada uma política para bloquear o acesso de todos usuários a aplicação facebook, sem informar ip dessa aplicação ou seu endereço para acesso (URL).

Os procedimentos abaixo ilustram os passos para criação dessa política em um firewall de nova geração da Palo Alto Networks, onde as políticas são orientadas a aplicação:

Figura 05 –Políticas de Segurança

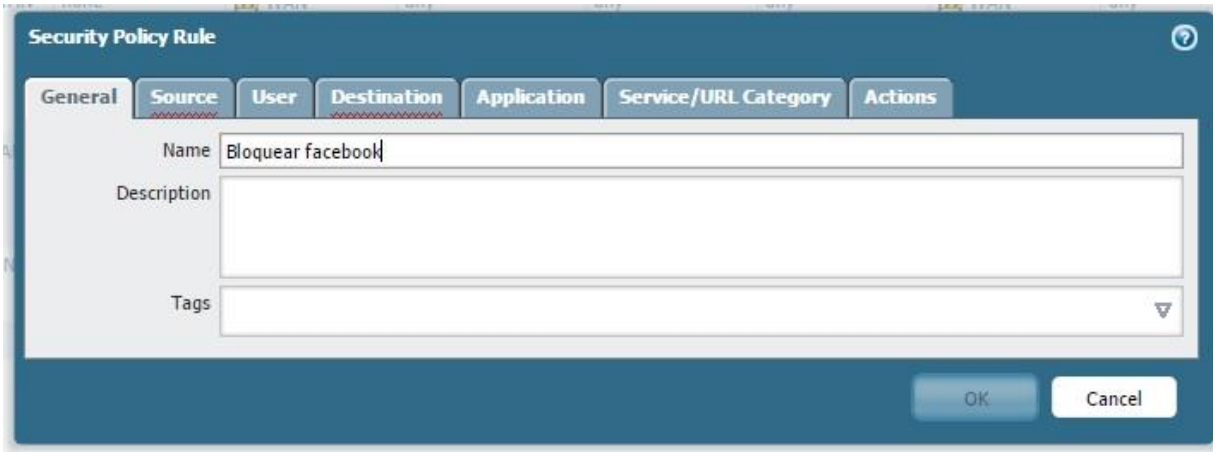


Fonte: Próprio Autor, 2015.

Na figura 05 temos a tela inicial de políticas de segurança. Para acessar essa área devemos inicialmente clicar em *Policies* (políticas), que se encontra no menu na parte superior, em seguida clicar em *Security*(segurança) que se encontra no menu ao lado esquerdo. Para iniciar a criação da nova política devemos clicar no botão *Add* que se encontra na parte inferior esquerda dessa tela.

Na tela inicial da criação da nova política, conforme a figura 06, devemos preencher as informações básicas, como nome da política e descrição da mesma, caso necessário.

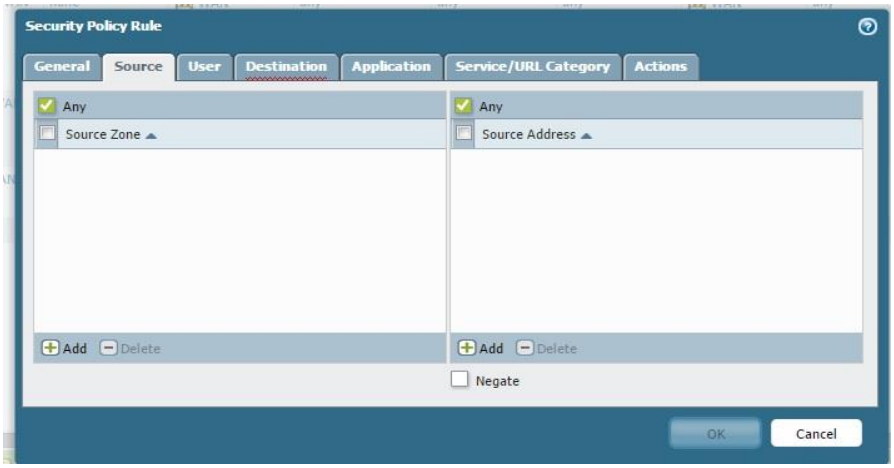
Figura 06 – Nome da política



Fonte: Próprio Autor, 2015.

Em seguida, na próxima aba *Source* (origem), podemos setar as origens para zonas, ips e redes. Iremos selecionar *any* (qualquer) para nossa política atuar em qualquer origem, conforme podemos ver na figura abaixo.

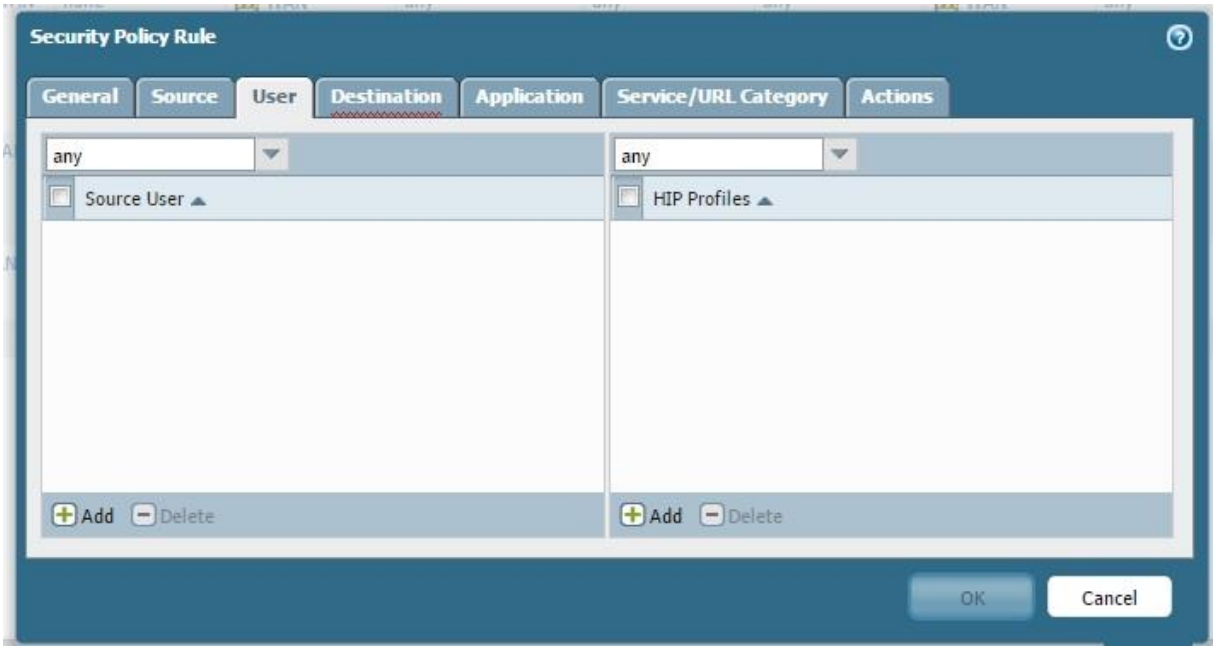
Figura 07 – Tela de origem da política



Fonte: Próprio Autor, 2015.

Na tela seguinte, *User* (usuários), em ambientes onde haja integração com alguma solução de gestão de usuários, se faz possível selecionar usuários ou grupos para uma política. Escolheremos o parâmetro *any* (qualquer), para a política ser aplicada a todos usuários, conforme figura 08.

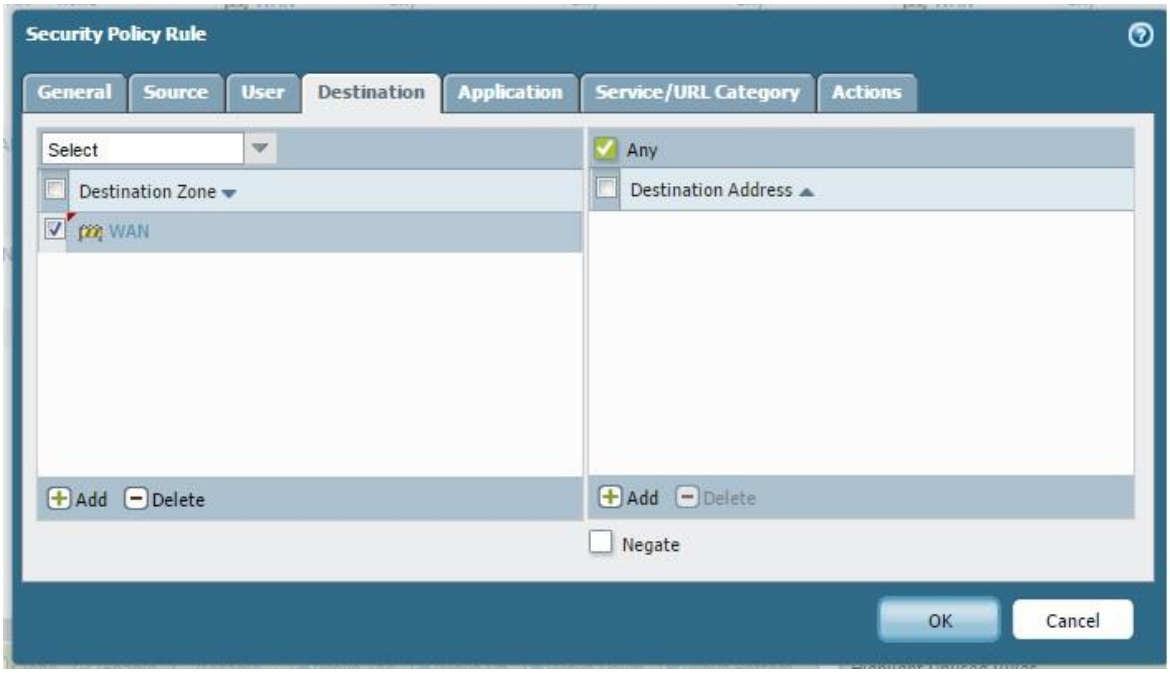
Figura 08 – Tela de definição de usuários.



Fonte: Próprio Autor, 2015.

Na aba de *Destination* (destino), podemos escolher zonas, ips e redes de destino. Para nosso ambiente escolhemos a zona WAN, que representa nossa saída para internet e setamos *any* (qualquer), para qualquer ip de destino, conforme figura 09.

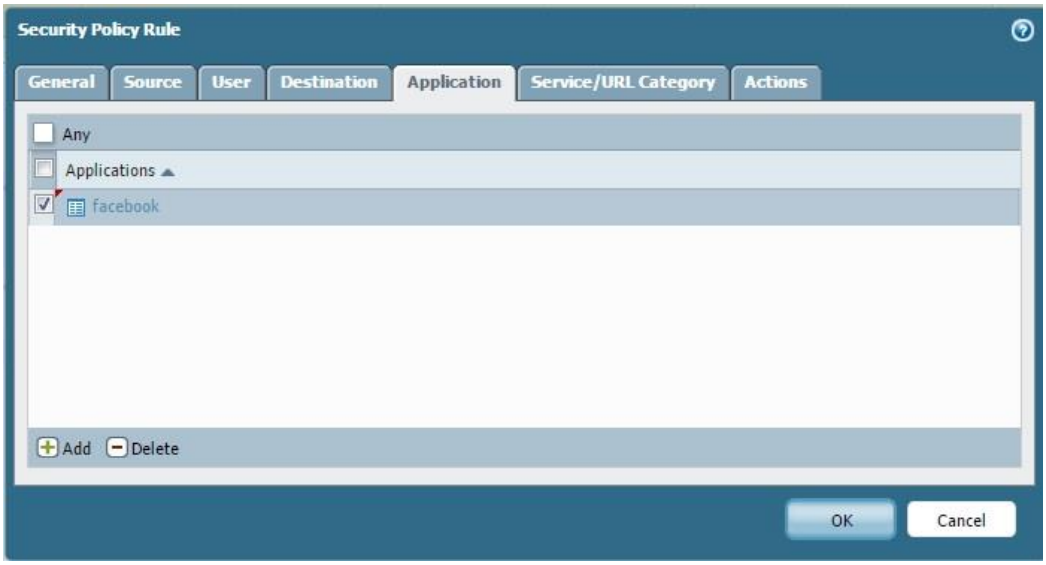
Figura 09 – Definição de destino.



Fonte: Próprio Autor, 2015.

A figura 10 representa a tela principal para a nossa política. Nessa tela escolhemos a aplicação facebook. Todas demais ações terão como base essa aplicação, independentemente de qual ip ou endereço ela utilize.

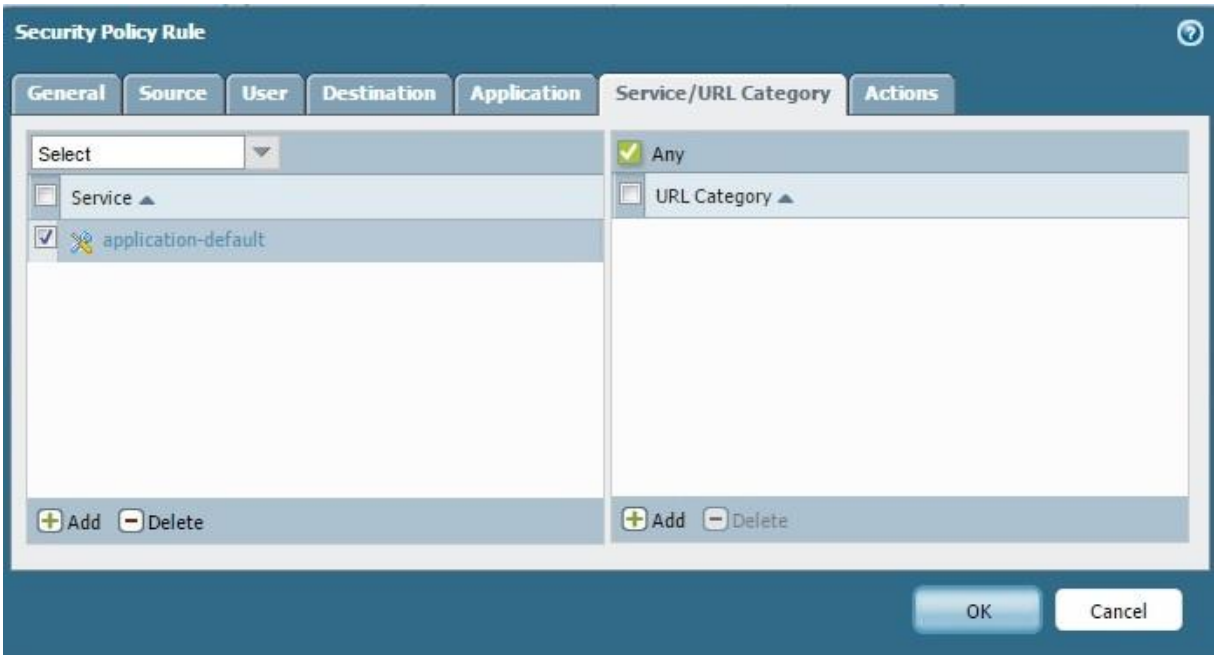
Figura 10 – Definição da aplicação.



Fonte: Próprio Autor, 2015.

Na tela seja, conforme figura 11, podemos fazer configurações de serviços e categorização URL. Para nossa política utilizaremos o serviço padrão, que engloba http e *any* (qualquer), para todas categorias de *url*.

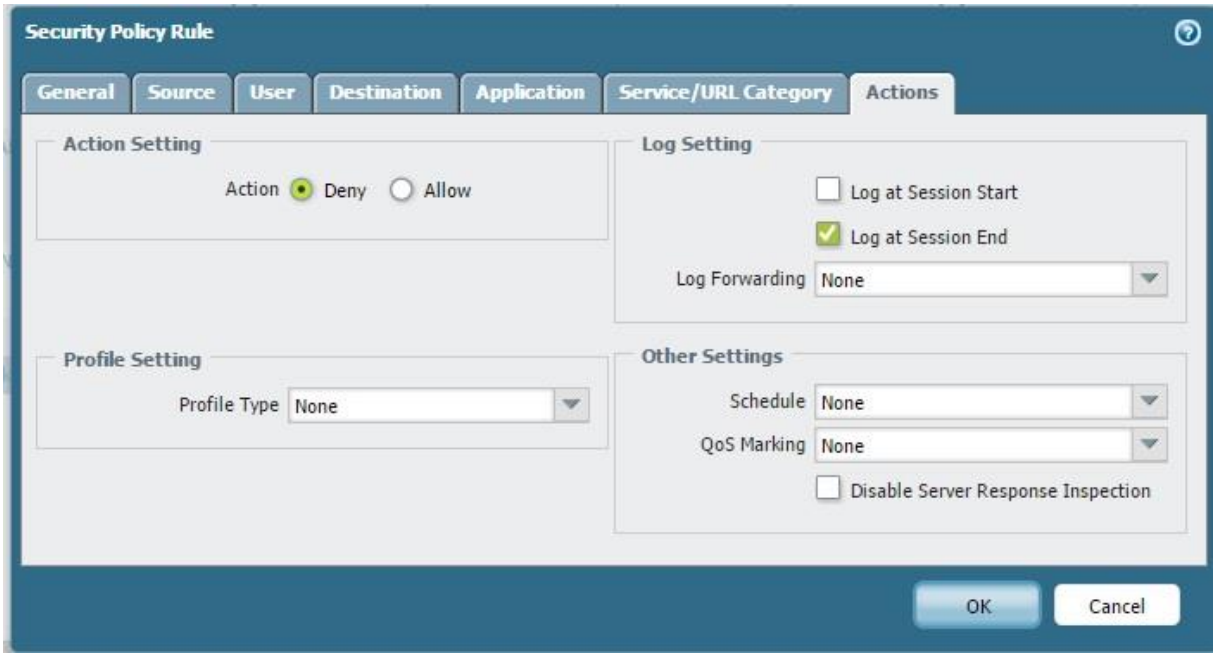
Figura 11 – Definição de Serviço e Categorização de URL.



Fonte: Próprio Autor, 2015.

Na última aba, referente as ações, definiremos se será uma política de bloqueio ou de liberação. Setamos como *Deny* (negar), para ser uma política de bloqueio. Nessa tela também é possível fazer configurações adicionais de *logs*, QoS e agendamento da política, conforme podemos ver na figura 12.

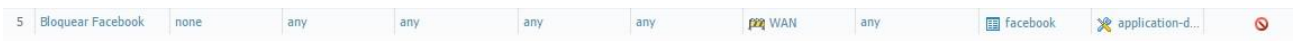
Figura 12 – Tela de definição de ações.



Fonte: Próprio Autor, 2015.

Após seguir esses passos, temos a política criada, conforme figura 13. Se trata de uma política totalmente orientada a aplicação, no caso em questão facebook, independente do ip ou porta que essa aplicação utilize. Essa é justamente uma das principais características de um *Firewall* de Nova Geração.

Figura 13 – Regra criada.



Fonte: Próprio Autor, 2015.

CONCLUSÃO

O estudo permitiu compreender que o *firewall* realmente é uma solução de segurança indispensável em ambientes corporativos, no entanto fica claro também, que se precisa muito mais do que um *firewall* para se ter uma segurança efetiva.

Foi possível conhecer melhor alguns tipos de *firewalls* e entender a semelhança entre os *firewalls* UTM e os *firewall* de nova geração, conhecendo ainda características de grandes fabricantes, líderes de mercado, que comprovam tais diferenciais.

Com esse trabalho foi possível ainda, apresentar os pilares da segurança da informação, a definição de ataques e vulnerabilidade, as gerações dos *firewalls* e ainda abordar a forma de criação de uma política em um *firewall* de nova geração, onde as mesmas são criadas orientadas a aplicação, algo muito mais eficiente nos dias atuais onde regras orientadas a ip e portas não são mais eficientes, principalmente levando em consideração a evolução de utilização das aplicações mais usadas hoje em dia, onde a maioria foram migradas para a *web*, onde se utilizam, na maioria das vezes, portas tradicionais, como 80 e 443.

Após a análise de todos esses aspectos apresentados, fica clara a necessidade de se conhecer bem as soluções ofertadas no mercado, todas suas características, funcionalidades e limitações e conhecer muito bem as necessidades de seu ambiente, para assim poder buscar a melhor solução que se adeque as suas necessidades.

Trabalhos Futuros

Espera-se com a contribuição desse trabalho que testes sejam sugeridos e que seja possível aplicar juntamente com toda teoria apresentada, aspectos práticos, para demonstrar melhor a aplicabilidades de diversas funcionalidades comentadas.

Espera-se também que futuras pesquisas possam focar em um estudo mais aprofundado acerca de algumas funcionalidades específicas de um *firewall* de nova geração, como por exemplo o sistema de detecção de intrusão.

Por fim, como trabalho futuro, pode-se propor a implantação de um *firewall* UTM e de um *firewall* de nova geração e comparar a utilização de recursos em cada uma das soluções para desempenhar funcionalidades em comum para ambos e também medir a utilização de recursos com todas funcionalidades habilitadas em cada uma das soluções.

REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2013 – **Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação — Requisitos**.

ABNT NBR ISO/IEC 27002:2013 – **Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação**.

Cert Br **– Cartilha de Segurança para Internet**. Disponível em: http://cartilha.cert.br/ataques/ . Acesso em:28 out.2015

CAMPOS, A. **SISTEMAS DE SEGURANÇA DA INFORMAÇÃO**. 2 ed. Florianopolis: Visual Books, 2007

CARUSO, C. A.A; STEFFEN, F. D. **Segurança em Informática e Informações**. São Paulo:SENAC,2006.

CHESWICK, W.R., BELLOVIN, S.M. **Firewalls and Internet Security**. Addison-Wesley Publishing Company, 1997.

DANTAS, M. **Segurança da Informação:** Uma abordagem Focada em Gestão de Riscos. 1 ed. Olinda: Livro rápido, 2011

DELOITTE - **Cyber Espionage:** The harsh reality of advanced security threats - Center for Security & Privacy Solutions. 2011. Disponível em: https://www.isaca.org/chapters1/phoenix/events/Documents/cyber_espionage.pdf Acesso em: 28 Out.2015

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

Gartner. Disponível em: http://www.gartner.com/it-glossary/next-generation-firewalls-ngfws - Acesso em:28 out.2015

GEUS, Paulo Lício de; POUW, Keesje Duarte.**Uma análise das vulnerabilidades dos firewalls**. 1996

ITFRIENDS**, NGFW VS UTM**. Disponível em <http://www.itfriends.org/ngfw-vs-utm/>, acesso em 09 nov.2015

KAMARA, Seny et al. **Analysis of vulnerabilities in internet firewalls.Computers & Security**. 2003

Kaspersky. Disponível em: https://blog.kaspersky.com.br/o-que-e-apt/754/ Acesso em:28 out.2015

NSSLabs. Disponível em: www.nsslabs.com - Acesso em:28 out.2015

PaloAlto. Disponível em: https://www.paloaltonetworks.com.br/products/technologies/wildfire.html Acesso em:28 out.2015

PaloAlto. Disponível em: https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/datasheets/firewall-features-overview/firewall-features-overview-pt.pdf . Acesso em:28 out.2015

RFC 1594. Disponível em: http://www.rfc-base.org/txt/rfc-1594.txt . Acessado em: 16 dez.2015

SÊMOLA, Marcos. **Gestão da Segurança da Informação, Uma visão Executiva**. Rio de Janeiro: Elsevier,2003

STREBE, Matthew; PERKINS,Charles. **Firewalls**: uma fonte indispensável de recursos para os administradores de sistemas.São Paulo:Makron Books, 2002.

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

TANENBAUM, Andrew S. **Redes de Computadores**. Tradução da 4 ed. Campus, 2003

VON ZUBEN, Miriam; HENRIQUES, Marco Aurélio de Amaral; **Análise de vulnerabilidades e incidentes de segurança em grids de computação voluntária**, Vol. CD-ROM, Campinas, SP, Brasil, 2009

WADLOW, Thomas. **Segurança de Redes**. Rio de Janeiro: Campus, 2000.