Revista Científica UNAR (ISSN 1982-4920), Araras (SP), v.23, n.1, p.98-117, 2023.
DOI: 10.18762/1982-4920.20230007

FIREWALLS DE NOVA GERAÇÃO: FORTALECENDO A SEGURANÇA DA INFORMAÇÃO NO MUNDO DIGITAL

Alan Petrazzo, André Castro Rizo

RESUMO

Com o rápido avanço das tecnologias e a constante evolução dos ataques cibernéticos, um firewall tradicional já não é tão eficaz para proteção de uma rede computacional mais complexa, pois carece dos recursos e inteligências para inspecionar o fluxo de dados dos pacotes para distinguir diferentes tipos de tráfego na web, não sendo possível diferenciar dados legítimos de maliciosos. Para enfrentar esses desafios em constante mudança, é essencial adotar um NGFW (Next Generation Firewall), também conhecido como Firewall de Nova Geração. O firewall desempenha um papel importante como a primeira linha de defesa contra-ataques cibernéticos, garantindo a proteção da rede de dados corporativa. Ao longo do tempo, o firewall evoluiu significativamente para enfrentar as ameaças em constante evolução. O NGFW surgiu para lidar com as demandas avançadas de segurança sem comprometer a latência da rede. Esses firewalls foram desenvolvidos para atender às necessidades dos ambientes de computação atuais, nos quais os ataques de malware estão se tornando mais sofisticados e intensos, visando explorar as vulnerabilidades dos firewalls tradicionais. Além disso, é fundamental compreender os pilares da segurança da informação, bem como conceitos importantes como vulnerabilidades, riscos e ataques. O objetivo principal é destacar os diferenciais tecnológicos de um NGFW e demonstrar a facilidade de criar políticas orientadas por aplicação e usuário. Vale ressaltar que nenhum ambiente pode ser considerado totalmente seguro, pois tanto as ameaças quanto as soluções estão em constante evolução. Portanto, é necessário conhecer profundamente as necessidades específicas de cada ambiente e buscar a solução que melhor se adeque a elas.

Palavras-chave: NGFW; Next Generation Firewall; Firewall

Abstract

With the rapid advancement of technologies and the constant evolution of cyberattacks, a traditional firewall is no longer as effective for protecting more complex computational networks, as it lacks the necessary resources and intelligence to inspect the data flow of packets and distinguish between different types of web traffic. As a result, it is unable to differentiate legitimate data from malicious data. To address these ever-evolving challenges, it is essential to adopt a Next Generation Firewall (NGFW). The firewall plays a crucial role as the first line of defense against cyberattacks, ensuring the protection of corporate data networks. Over time, firewalls have significantly evolved to confront the continuously changing threats. The NGFW emerged to meet the advanced security demands without compromising network latency. These firewalls are designed to meet the needs of current computing environments,

where malware attacks are becoming more sophisticated and intense, aiming to exploit the vulnerabilities of traditional firewalls. Furthermore, it is essential to understand the pillars of information security, as well as important concepts such as vulnerabilities, risks, and attacks. The primary objective is to highlight the technological differentiators of an NGFW and demonstrate the ease of creating application- and user-oriented policies. It is important to emphasize that no environment can be considered completely secure, as both threats and solutions are constantly evolving. Therefore, it is necessary to have a deep understanding of the specific needs of each environment and seek the solution that best fits these requirements.

Keywords: NGFW; Next Generation Firewall; Firewall.

1 INTRODUÇÃO

O presente trabalho foi usado como metodologia a pesquisa bibliográfica, que consiste na comparação entre os firewalls tradicionais e os firewalls de nova geração. Para isso, foram utilizados livros, artigos, sites da Internet entre outras fontes.

A segurança das informações (SI), vem ganhando mais importância e jamais será alcançada se os três pilares PPT – Pessoas, Processos e Tecnologias – não for aplicada à estratégia de segurança. (ISO/IEC 27001, 2013).

Temos que cuidar das Pessoas e Processos através de treinamentos, conscientização, normas e procedimentos.

No pilar da Tecnologia temos que prover meios para suportar os 2 pilares da S.I, que são Pessoas e Processos.

A S.I é uma área dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidamente ou sua indisponibilidade.

Com a expansão das redes de computadores na década de 80, principalmente nas áreas acadêmicas e nas áreas militares, houve a necessidade da criação de um dispositivo que faria o controle de acessos entre essas redes, designado como Firewall.

O Firewall ajuda a preservar os princípios básicos da S.I, conforme demonstrado pela ISO 27001 (2013), sendo a Confidencialidade, Integridade e Disponibilidade.

Confidencialidade: Protege os dados dos acessos não autorizados, garantindo a privacidade das informações.

Integridade: Mantém a exatidão e completeza da informação, prevenindo a alteração indevida.

Disponibilidade: Garantem que a informação esteja sempre disponível para que os usuários autorizados obtenham acesso sempre que necessário.

Inicialmente as regras de Firewall eram utilizadas com os roteadores, o qual separavam as redes externas com as redes internas, ou locais. Realizando controles baseados em IPs (Internet Protocol) e portas de comunicação. (UFRJ,2023).

Em 1987, engenheiros da Digital Equipment Corporation (DEC) publicava o primeiro artigo sobre Firewalls, conhecido como filtro de pacotes, enquanto Bill Cheswik e Steve Bellovin da AT&T Bell Labs, pesquisavam filtragem de pacotes e acabaram desenvolvendo um novo modelo de Firewall para Prova de Conceito. (INGHAM K.; FORREST S., 2012)

O modelo apresentado pelo Cheswik e Bellovin,(1994), da AT&T Bell Labs, se tratava de um filtro de pacotes (Packet Filters) que entre outras palavras é a inspeção de pacotes de dados transferidos entre computadores na internet. Ele é flexível, escalável, barato e rápido.

No início dos anos 90 surgia o Application Proxies: (Proxies de Aplicativos), que usavam proxies de aplicativos para filtrar em todos os níveis.

O proxy é um dispositivo intermediário entre a origem e o destino. Ele é executado no servidor, então eles exigiam um sistema operacional separado. Fornecia mais segurança do que os filtros de pacotes, mas eram mais complexos.

Em meados da década de 1990, surgia o Stateful Packet Inspection (SPI); Inspeção de pacote com estado. Ele fornece reconhecimento total da camada de aplicação sem quebrar o modelo cliente/servidor. Mais sofisticado do que a filtragem de pacotes. Por um periodo o SPI foi muito seguro e rápido.

Nos dias de hoje temos Deep Packet Inspection (DPI). O DPI é a inspeção profunda de pacotes: Ele atende a proteção de firewall em todas as 7 camadas. Funciona tanto na borda da rede (entre a internet e a rede local) quanto dentro da própria rede e usa muitos recursos, como por exemplo IDS (Intrusion Detection System), IPS (Intrusion Prevention System), e é muito mais seguro que a tecnologia de firewall SPI. (Noonan & Dubrawsky, 2006).

2 REFERENCIAL TEÓRICO

A seguir serão demonstrados alguns assuntos iniciais importantes para um melhor aproveitamento do trabalho.

2.1 Arquitetura TCP/IP (Transmission Control Protocol / Internet Protocol)

Conforme descrito na RFC 1594 (1994), TCP/IP é o nome comum para uma família de mais de 100 protocolos de comunicação de dados usados para organizar computadores e equipamentos de comunicação de dados em redes de computadores.

O TCP/IP foi desenvolvido para interconectar hosts na ARPANET, PRNET (rádio de pacote) e SATNET (satélite de pacote). Todas essas três redes já foram desativadas; mas o TCP/IP continua existindo. Atualmente é usado em uma grande rede internacional de redes chamada Internet, cujos membros incluem universidades, outras instituições de pesquisa, instalações governamentais e muitas corporações. Às vezes, o TCP/IP também é usado para outras redes, particularmente redes locais que unem vários tipos diferentes de computadores ou unem estações de trabalho de engenharia. (A.S Tanenbaum, 2013).

2.2 Datagrama e Fragmentação

Um datagrama é uma entidade independente de dados que transporta informações suficientes para serem roteadas do computador de origem para o computador de destino sem depender de trocas anteriores entre esse computador de origem e de destino e a rede de transporte. (RFC 1514,1994).

Com isso a operação no modo datagrama é uma comunicação não confiável, pois não usa nenhum modo de reconhecimento fim a fim ou entre nós intermediários e também não utiliza nenhum controle de fluxo.

O caminho através da rede no datagrama, é definido para cada pacote individualmente e é possível utilizar sempre o melhor caminho.

Quando o datagrama estiver um uma rede incapaz de transportar datagramas com um tamanho maior suportado, ele será fragmentado pelo próprio computador de origem ou até mesmo pelos roteadores durante o caminho. No destino final é feita a remontagem dos fragmentos.

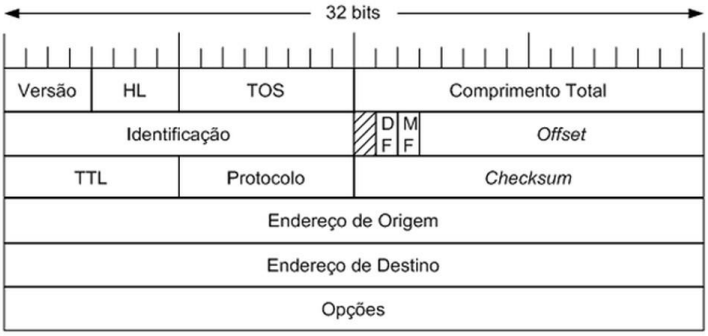
2.3 Protocolo IP

O Protocolo IP (Internet Protocol) está presente em todas as redes interconectadas. Todos os dispositivos de rede possuem um endereço lógico denominado “Endereço IP”. Ele realiza uma análise de endereçamento de cada pacote de rede que recebe e através de uma tabela de roteamento, ele redireciona os pacotes para o destino correto.

O IP recebe segmentos que são encapsulados em pacotes, ou datagramas.

De acordo com a Figura 1, apresentada por Tanenbaum (A.S Tanenbaum, 2013) é apresentado um cabeçalho IP para um melhor entendimento:

Figura 01.: Cabeçalho do Protocolo IP (Internet Protocol)



Fonte: Redes de Computadores (2003, p.461)

- 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 16 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).

2.4 Camada De Aplicação

A camada de Aplicação é responsável por definir os protocolos necessários para comunicação, controle e especificações da interface com o usuário.

Na camada de Aplicação temos os protocolos de níveis mais alto, como o FTP (File Transfer Protocol), protocolos de e-mails, POP, IMAP e SMTP. (Tanenbaum,2003).

2.5 Segurança da Informação

A informação entende-se como qualquer conteúdo que possa ser armazenado ou transferido, com o propósito de utilizada ao ser humano. Ela pode ser manipulada e visualizada de diversas maneiras, sendo um dos principais produtos da atual era digital, uma vez que o conhecimento é estratégico para governos, corporações e empresas.A segurança da informação é o conjunto de ações e recursos utilizados para manter a informação protegida contra riscos e ameaças.

De acordo com a ISO 27001 (2013), a segurança se compõe de medidas físicas e medidas lógicas.

Medidas físicas:

Organizações que possuem funções públicas como: Bibliotecas, prefeituras e que fazem o uso de controle de acesso.

Organizações privadas que estabelecem áreas restritas para proteger novos conhecimentos, como um novo lançamento ou novas tecnologias.

Medida lógica:

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.

Nesses ambientes existem riscos próprios, ameaças potenciais, controles aplicáveis e soluções de segurança que podemos minimizar o nível de exposição no qual um ambiente possa estar comprometido, com o intuído principal de garantir segurança para o produto mais valioso e imensurável: a informação.

3 TIPOS DE FIREWALL

3.1 Firewall

Firewall é um componente essencial da segurança de rede, que atua como uma barreira de proteção entre uma rede privada interna e redes externas não confiáveis, como a Internet. Ele controla o tráfego de rede com base em um conjunto de regras predefinidas, permitindo ou bloqueando o acesso a determinados recursos com base em critérios de segurança. (Noonan & Dubrawsky, 2006).

Em uma configuração mais restritiva, um firewall pode bloquear todo o tráfego de um computador ou rede, isolando-os. No entanto, é possível criar regras que exijam autorização do usuário ou administrador para liberar o acesso de um determinado aplicativo. Essa autorização pode ser permanente, ou seja, uma vez concedida, acessos subsequentes serão automaticamente permitidos.

Por outro lado, em uma configuração mais flexível, um firewall pode ser configurado para permitir automaticamente o tráfego de certos tipos de dados, como solicitações HTTP (Hypertext Transfer Protocol - protocolo usado para acessar páginas da web), enquanto bloqueia outros, como conexões a serviços de e-mail.

Esses exemplos mostram que as políticas de um firewall são baseadas em dois princípios iniciais: bloquear todo o tráfego, exceto o explicitamente autorizado, ou

permitir todo o tráfego, exceto o explicitamente bloqueado. Existem várias formas de realizar o trabalho de um firewall, e as principais categorias de funcionamento incluem filtragem de pacotes com ou sem inspeção de estados, bem como firewalls de aplicação. A escolha da metodologia depende de fatores como critérios do desenvolvedor, necessidades específicas de proteção, características do sistema operacional, estrutura da rede, entre outros. É por isso que existem diferentes tipos de firewalls disponíveis. (Strebe & Perkins, 2002).

3.2 Firewall Stateless

De acordo com Strebe e Perkins (2002), os filtros podem ser configurados para operar com base em várias partes do cabeçalho do protocolo IP, mas geralmente são configurados para filtrar os campos mais relevantes, como o Tipo de protocolo, Endereço IP e Porta TCP/UDP.

a) Filtragem de protocolos: Essa forma de filtragem analisa o conteúdo do campo de tipo de protocolo IP nos pacotes. Com base nessa análise, é possível discriminar um conjunto de serviços, como UDP, TCP, ICMP e IGMP.

b) Filtragem de endereços IP: Essa filtragem permite limitar as conexões de e para hosts e redes específicas com base em seus endereços IP. É importante ressaltar que um filtro só pode restringir endereços com base no conteúdo do campo que identifica o endereço IP.

c) Portas TCP/UDP: Essas portas são frequentemente usadas na filtragem, pois o campo de dados delas indica especificamente a finalidade do pacote. Ao contrário da filtragem de endereços IP, bloquear determinadas portas ainda é útil, pois a maioria das atividades maliciosas se concentra em protocolos específicos.

O mesmo autor também destaca que os filtros de pacotes sem estados (stateless) apresentam duas limitações que impedem que sejam totalmente eficazes:

- Eles não verificam a parte útil de dados dos pacotes.
- Eles não mantêm o estado das conexões.

Essas limitações tornam os filtros sem estados insuficientes quando aplicados sozinhos para proteger uma rede.

3.3 Firewall Stateful

Os filtros de pacotes com estados têm a capacidade de lembrar o estado das conexões da rede e das camadas da sessão, registrando informações sobre o estabelecimento da sessão que passa pelo gateway do filtro. Essas informações são posteriormente utilizadas pelos filtros para distinguir pacotes de retorno válidos de tentativas de conexão inválidas ou invasões. No entanto, os filtros de pacotes com estados não permitem que nenhum serviço passe pelo firewall, a menos que seja programado para isso.

Por outro lado, os firewalls de inspeção analisam todo o tráfego de dados para identificar estados, ou seja, padrões aceitáveis de acordo com suas regras, que serão utilizados para manter a comunicação. Essas informações são mantidas pelo firewall e usadas como parâmetro para o tráfego subsequente.

Para entender melhor, imagine que um aplicativo inicia uma transferência de arquivos entre um cliente e um servidor. Os pacotes de dados iniciais informam quais portas TCP serão utilizadas para essa tarefa. Caso o tráfego comece a fluir por uma porta que não foi mencionada, o firewall pode detectar essa ocorrência como uma anormalidade e bloqueá-la. (Strebe & Perkins, 2002).

3.4 Firewall UTM

De acordo com Tam (2012), a Central Unificada de Gerenciamento de Ameaças (UTM) é uma solução completa desenvolvida para o setor de segurança de redes e tem se destacado como a opção mais procurada para a defesa digital das organizações. O UTM é considerado uma evolução do firewall tradicional, pois combina a execução de várias funções de segurança em um único dispositivo, como firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga, geração de relatórios informativos e gerenciais, além de funções como IPS e muito mais.

De acordo com a empresa Kaspersky (2023), a Gestão Unificada de Ameaças (UTM) é um termo relacionado à segurança da informação, que se refere a uma solução de segurança abrangente, geralmente um dispositivo único, que oferece várias funções de segurança em um único ponto da rede. A principal vantagem dessa solução é a sua simplicidade. As organizações podem optar por ter fornecedores ou

dispositivos individuais para cada tarefa de segurança específica, ou podem obter todas essas funções de um único fornecedor global, apoiado por uma equipe de TI, e gerenciá-las a partir de um console centralizado.

Segundo a empresa Sonicwall (2023), os hackers estão se tornando mais sofisticados e seus ataques estão se tornando mais direcionados. Muitos dos ataques atuais são combinações de técnicas diferentes, visando infiltrar-se em uma rede. No entanto, lidar com várias ferramentas de segurança separadas pode ser cansativo, ineficiente e caro para as organizações. O gerenciamento unificado de ameaças (UTM) é considerado a melhor abordagem de segurança para empresas de pequeno e médio porte, oferecendo um novo nível de eficiência em termos de segurança.

3.5 NGFW – Next Generation Firewall

Seguindo Kurose, J. F., & Ross, K. W. (2013), os firewalls de nova geração são uma evolução dos firewalls tradicionais, que foram desenvolvidos para enfrentar os desafios e as demandas cada vez maiores da segurança de redes. Eles combinam recursos de filtragem de pacotes com recursos adicionais, como inspeção profunda de pacotes, inteligência de ameaças, controle de aplicativos e gerenciamento unificado de ameaças.

Esses firewalls oferecem uma abordagem mais avançada e abrangente para a proteção de redes, permitindo uma análise mais aprofundada do tráfego de rede. Eles podem identificar e bloquear ameaças sofisticadas, como malware, ataques de dia zero e ataques direcionados. Além disso, esses firewalls têm a capacidade de inspecionar o conteúdo dos pacotes, incluindo o tráfego criptografado, para detectar ameaças ocultas.

Uma característica importante dos firewalls de nova geração é o controle de aplicativos. Eles podem identificar os aplicativos e serviços específicos que estão sendo usados em uma rede, permitindo que as organizações definam políticas de acesso baseadas em aplicativos. Isso proporciona um controle mais granular sobre o tráfego de rede e ajuda a evitar o uso não autorizado de aplicativos ou serviços arriscados.

De acordo com o Gartner (2023), um firewall de nova geração deve ter algumas funcionalidades essenciais, que incluem as características de um firewall tradicional,

integração de um Sistema de Prevenção de Intrusões (IPS), controle de aplicação e capacidade de identificação de usuários. Essas funcionalidades mínimas foram definidas por grandes empresas que realizam testes nessa categoria de soluções, uma vez que não existe uma regulamentação específica para esse conceito.

Além dessas funcionalidades mínimas, cada fabricante pode adicionar novos recursos com o objetivo de oferecer uma solução mais completa e eficiente. Portanto, é de extrema importância analisar e conhecer as diversas soluções disponíveis no mercado, entender como cada uma opera e avaliar como cada uma pode atender às necessidades específicas da organização antes de tomar uma decisão sobre a escolha de um firewall de nova geração.

3.6 Principais características dos NGFW

- Recursos Avançados: Os firewalls de nova geração oferecem recursos mais sofisticados e avançados em comparação aos firewalls tradicionais.

- Funcionalidades Avançadas: Esses firewalls possuem funcionalidades mais aprimoradas e avançadas, indo além das capacidades básicas de um firewall convencional.

- Capacidades Ampliadas: Os firewalls de nova geração apresentam capacidades expandidas em termos de recursos e funcionalidades.

- Recursos de Próxima Geração: Esses firewalls possuem recursos inovadores e de última geração, que proporcionam uma proteção mais abrangente e eficiente.

- Funcionalidades de Segurança Avançadas: Esses firewalls incorporam funcionalidades de segurança mais sofisticadas, que vão além das funcionalidades tradicionais de um firewall.

- Recursos de Inspeção Profunda de Pacotes: Os firewalls de nova geração têm a capacidade de realizar uma análise mais detalhada e minuciosa dos pacotes de dados, identificando ameaças e comportamentos suspeitos.

- Controle de Aplicativos Avançado: Esses firewalls oferecem um controle mais abrangente e refinado sobre os aplicativos que são permitidos ou bloqueados na rede.

Cada fabricante incorpora novas funcionalidades com o objetivo de oferecer uma solução mais abrangente e eficaz. Portanto, é crucial que antes de tomar uma decisão sobre qual firewall de nova geração escolher, seja feito um estudo detalhado das

diversas opções disponíveis no mercado. É essencial compreender como cada solução opera, quais são seus recursos e como elas se alinham às necessidades específicas da organização. (KUROSE & Ross,2013).

4 RESULTADOS E DISCUSSÃO

4.1 Comparativo entre NGFW e UTM

O firewall de última geração (NGFW) é um conceito revolucionário no campo da segurança de redes, pois promete a integração e consolidação de tecnologias essenciais para proteger o perímetro de uma rede. No entanto, ainda existe uma considerável falta de clareza no mercado sobre o que exatamente o NGFW oferece, o que muitos clientes descobrem com surpresa quando percebem a ausência de recursos de segurança importantes. Em essência, as principais funcionalidades do NGFW incluem um firewall dinâmico, controle de aplicativos, controles baseados em usuário e um sistema de prevenção de invasões (IPS).

Em contraste, as soluções de gerenciamento unificado de ameaças (UTM) oferecem uma ampla gama de tecnologias de segurança de rede que vão além das funcionalidades do NGFW. As soluções de UTM incluem firewall dinâmico, sistema de prevenção de invasões (IPS), antivírus de gateway, segurança e filtragem de conteúdo da web, segurança de e-mails e prevenção contra vazamento de dados (DLP). O mais importante é que os fornecedores de UTM atualizaram com sucesso seus produtos para incluir as funcionalidades do NGFW, como controles de alerta de usuário e aplicativo.

Há algum tempo, o conceito de "Next Generation Firewall" (NGFW) tem sido apresentado a empresas de análise de desempenho, como a Gartner, e a empresas de segurança da informação, como a Palo Alto Networks, sugerindo que o NGFW está reinventando o atual modelo de firewall UTM. Os fabricantes de firewalls estão posicionando seus produtos como "o próximo grande passo" na evolução dos firewalls. Ao pesquisar sobre essas tecnologias, encontramos os seguintes resultados: o Unified Threat Management (UTM) é uma plataforma de convergência de produtos de segurança, especialmente adequada para pequenas e médias empresas. Ele combina recursos típicos de segurança em três principais subgrupos, tudo dentro de

um único dispositivo UTM: firewall, IPS e VPN; filtro de URL, filtro de conteúdo e antivírus; e antispam e antivírus de e-mail.

Por outro lado, os firewalls de próxima geração (NGFWs) são firewalls de inspeção de pacotes mais complexos, que vão além da simples inspeção de portas e protocolos de comunicação. Eles atuam no nível de inspeção de aplicativos, prevenção de invasões e incorporam inteligência externa ao firewall. É importante não confundir um NGFW com um sistema de prevenção de intrusões de rede (IPS) independente, que inclui um firewall embutido ou a combinação de um firewall e IPS no mesmo dispositivo, sem uma integração íntima entre eles.

Em resumo, o NGFW e o UTM são termos usados para descrever diferentes abordagens para proteção do perímetro de rede. Enquanto o NGFW se concentra em recursos avançados de firewall, controle de aplicativos e prevenção de invasões, o UTM oferece uma solução mais abrangente, incorporando recursos adicionais, como antivírus, filtragem de conteúdo e prevenção de vazamento de dados. É importante entender que o NGFW e o UTM são abordagens distintas para a segurança de rede e que cada uma delas possui suas vantagens e limitações. O NGFW oferece recursos avançados de inspeção de pacotes, focando em proteção de aplicativos e prevenção de invasões, enquanto o UTM é uma plataforma mais abrangente, adequada especialmente para pequenas e médias empresas, que combina diversos recursos de segurança em um único dispositivo.

No entanto, é essencial destacar que os fornecedores de UTM atualizaram seus produtos para incluir funcionalidades de NGFW, visando oferecer aos clientes o melhor dos dois mundos. Isso significa que os dispositivos UTM agora também são capazes de fornecer firewall dinâmico, prevenção de invasões e outros recursos avançados, anteriormente associados apenas aos firewalls de próxima geração.

A indústria de segurança de rede tem visto o NGFW como um passo adiante na evolução dos firewalls, trazendo maior inteligência e capacidades de inspeção para lidar com as ameaças modernas. No entanto, é importante ter em mente que a nomenclatura NGFW pode ser usada como uma estratégia de marketing, e que nem todos os dispositivos rotulados como NGFW oferecem necessariamente todas as funcionalidades esperadas. A Palo Alto Networks, a Checkpoint, a Sourcefire, a McAfee e outras empresas renomadas têm se destacado no mercado como fornecedoras de soluções de NGFW. Por outro lado, a SonicWall, a WatchGuard, a

Fortinet, a Sophos (Astaro) e também a Juniper e a Cisco são conhecidas por oferecerem soluções UTM de qualidade.

Em resumo, tanto o NGFW quanto o UTM desempenham papéis importantes na segurança de redes, cada um com suas próprias características e benefícios. O NGFW oferece recursos avançados de proteção de aplicativos e inspeção de pacotes, enquanto o UTM fornece uma plataforma abrangente de segurança em um único dispositivo. Com a evolução do mercado, muitos fornecedores de UTM têm incorporado as funcionalidades do NGFW em seus produtos, oferecendo uma solução mais completa e integrada aos clientes.

No final das contas, a escolha entre NGFW e UTM dependerá das necessidades específicas de segurança de cada organização, seu porte e recursos disponíveis. É recomendado avaliar cuidadosamente as opções oferecidas pelos fornecedores, considerando os recursos necessários, a facilidade de gerenciamento, a escalabilidade e o suporte técnico, para garantir a melhor proteção para a rede empresarial.

Figura 02: Comparativo NGFW e UTM

Parameters	NGFW	UTM
Abbreviation for	Next generation firewall	Unified Threat Management
Stateful Inspection	Supported	Supported
Target customer	Enterprise grade	SMBs
Throughput and performance	Higher than UTM	Lower than NGFW
Traffic filtering (Port, IP Address and protocol based)	Supported	Supported
NAT	Supported	Supported
VPN	Supported	Supported
Application level awareness	Supported	Supported
Reputation and identity services	Supported	Supported
Bandwidth management	Supported	Supported
IPS	Supported	Supported
Antivirus and Antispam	Not Supported	Supported
Email Security	Not Supported	Supported
DLP	Not Supported	Supported
Content/Web filtering	Not Supported	Supported

Fonte: Ipwithease, 2023

Após examinar a comparação, torna-se claro que essas duas soluções são semelhantes em termos de funcionalidades. A maioria dos provedores de segurança de rede está fornecendo controle e visibilidade de aplicativos, seja incorporando assinaturas de aplicativos ao mecanismo IPS ou oferecendo uma licença adicional para um módulo de controle de aplicativos. Em ambos os casos, essas opções são complementares a um firewall stateful ou UTM.

4.2 Análise de um NGFW - Palo Alto

Em nossa pesquisa foi estudada a análise de um NGFW da Palo Alto.

O firewall de nova geração analisado tem a capacidade de inspecionar todo o tráfego, incluindo aplicativos, ameaças e conteúdos relacionados aos usuários, independentemente de sua localização ou tipo de dispositivo. Aplicativos, usuários e conteúdos são elementos essenciais para gerenciar os negócios e, portanto, fazem parte integrante da política de segurança corporativa. Isso resulta na habilidade de alinhar a segurança com as principais iniciativas empresariais. (PaloAlto,2023).

A empresa Gartner, especializada em consultoria, pesquisa e avaliação de soluções, desenvolveu uma matriz gráfica chamada Quadrante Mágico. Essa matriz é dividida em quatro quadrantes: Líderes, Desafiadores, Visionários e Nichos de mercado, classificados em ordem de importância. O gráfico é composto por dois eixos. No eixo horizontal, é avaliada a visão da empresa em termos de inovação tecnológica e atendimento às necessidades do mercado. No eixo vertical, o relatório avalia a capacidade das empresas de executar e implementar o que prometem.

A figura abaixo mostra o último relatório lançado para firewalls de rede corporativa, no qual a solução avaliada neste trabalho está posicionada no quadrante de líderes de mercado.

Figura 03: Magic Quadrant for Network Firewall

Fonte: Gartner, 2022

4.3 Principais recursos desta solução

- Reconhecimento de aplicativos, independentemente da porta, protocolo, tática de evasão ou criptografia.

- Identificação de usuários, independentemente do dispositivo ou endereço IP.

- Proteção em tempo real contra ameaças conhecidas e desconhecidas, integrada aos aplicativos.

- Oferecem visibilidade e controle abrangentes de políticas sobre aplicativos, usuários e conteúdo.

- Implantação em linha de alta velocidade e previsível, com suporte a múltiplos gigabits.

Na próxima figura ilustra as políticas de um firewall de nova geração da Palo Alto Networks, onde as políticas são orientadas a aplicação:

Figura 04.: Regras de Segurança NGFW

		Source				Destination							
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Options
Rule X	none	Untrust	any	any	any	DMZ	192.0.2.10	any	Web-Server_Ports	any		none	
Rule Y	none	Trust	any	any	any	Untrust	any	web-browsing	application-default	adult-and-pornography		none	
Rule Z	none	Trust	any	any	any	Untrust	any	any	any	any		none	

			Source				Destination							
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Options
1	Dependency Apps rule	none	Trust	any	any	any	Untrust	any	citrix ssl web-browsing	any	any		none	
2	Rule 10	none	Trust	any	any	any	Untrust	any	gotomeeting youtube	any	any		none	
3	Rule 11	none	Guest	any	any	any	Untrust	any	facebook gmail-base	any	any		none	
4	Rule 12	none	Guest	any	any	any	Untrust	any	web-browsing	any	any		none	

Fonte: PaloAlto Networks, 2023

A figura acima se trata de políticas totalmente orientada a aplicação, como por exemplo Citrix, independente do ip ou porta que essa aplicação utilize o Firewall é capaz de analisar o cabeçalho e validar se realmente aquele tráfego é pertencente aquela determinada aplicação, sendo capaz de permitir ou negar acesso baseada nessas informações. Essa é justamente uma das principais características de um *Firewall* de Nova Geração.

Abaixo um modelo de regra em um firewall comum, não orientado a aplicação, com a utilização somente de IPs e portas:

Figura 05: Regras Firewall IP e Porta

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☐ ✔	0/0 B	IPv4 TCP/UDP	10.0.0.0/8	*	LAN address	53 (DNS)	*	none		Allow internal network to query the DNS Resolver
☐ ✔	0/0 B	IPv4 ICMP echoreq	10.0.0.0/8	*	LAN address	*	*	none		Allow internal network to ping the LAN IP Address
☐ ✔	0/0 B	IPv4 TCP	RemoteAdmin	*	LAN address	RemoteAdminPorts	*	none		Allow access to firewall management
☐	0/0 B	IPv4 *	*	*	LAN address	*	*	none		Reject everything else to the LAN IP address
☐ ✔	0/2.59 MiB	IPv4 *	10.0.0.0/8	*	*	*	*	none		LAN Traffic

Fonte: Pfsense, 2023

Nesse modelo, independente se for uma aplicação segura ou não, o firewall poderá permitir o acesso baseado nos IPS e portas, independentemente se for uma aplicação WEB na porta 80 ou não.

5 CONSIDERAÇÕES FINAIS

A pesquisa permitiu uma compreensão abrangente de que um firewall é essencial para garantir a segurança em ambientes corporativos, no entanto, tornou-se evidente que é necessário muito mais do que apenas um firewall para estabelecer uma segurança efetiva.

Foi possível adquirir um melhor conhecimento sobre diferentes tipos de firewalls e reconhecer as semelhanças entre os firewalls UTM e os firewalls de nova geração. Além disso, foram identificadas características distintivas de renomados fabricantes, líderes do mercado, que comprovam suas vantagens competitivas.

Com esse estudo, também foi possível apresentar os pilares fundamentais da segurança da informação, compreender a definição de ataques e vulnerabilidades, explorar as diferentes gerações de firewalls e abordar a criação de políticas em firewalls de nova geração. Essas políticas são desenvolvidas com foco nas aplicações, pois regras baseadas em endereços IP e portas não são mais eficazes nos dias atuais, especialmente considerando o aumento do uso de aplicativos baseados na web, que geralmente utilizam portas tradicionais, como 80 e 443.

Após analisar todos esses aspectos abordados, fica evidente a importância de conhecer profundamente as soluções disponíveis no mercado, compreender suas características, funcionalidades e limitações, além de ter um entendimento claro das necessidades específicas do ambiente em questão. Somente assim será possível buscar a melhor solução que atenda plenamente às demandas e requisitos do ambiente em que será implementada.

REFERÊNCIAS

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

Comparativo NGFW UTM: https://ipwithease.com/ngfw-vs-utm/. Acesso em: 01 de maio de 2023.

Wesley J Noonan, Ido Dubrawsky. Firewall Fundamentals, Cisco Press, 2006.

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

FONTES, E. Praticando a Segurança da Informação. Rio de Janeiro: Brasport, 2008.

Fortinet: Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/brasil-e-o-segundo-pais-que-mais-sofre-ataques-ciberneticos-na-a. Acesso em: 10/04/2023.

HARRIS, S. CISSP All-in-One ExamGuide. 5.ed. McGraw-Hill Osborne Media, 2010.

Ingham, K., Forrest, S.: A History and Survey of Network Firewalls, A history and survey of network firewalls. Tech. Rep. TR-CS-2002-37, University of New Mexico Computer Science Department (2002)

UFRJ - História do Firewall: Disponível em: https://www.gta.ufrj.br/grad/07_1/firewall/index_files/Page350.htm. Acesso em: 10/04/2023

Kaspersky, O que é gerenciamento unificado de ameaça: https://www.kaspersky.com.br/resource-center/definitions/utm

KUROSE, J. F.; Ross, K. W. Redes de Computadores e a Internet: uma abordagem-topdown. 6. Ed. São Paulo: Addison Wesley, 2013.
Magic Quadrant for Network Firewall: https://www.fortinet.com/solutions/gartner-network-firewalls. Acesso em: 10 de maio de 2023.

PaloAlto. Disponível em: https://www.paloaltonetworks.com/content/dam/paloaltonetworkscom/en_US/assets/pdf/datasheets/firewall-features-overview/firewall-featuresoverview-pt.pdf Acesso em: 20/04/2023.

Sonicwall. Disponível em: https://www.internationalit.com/post/sonicwall-relat%C3%B3rio-de-amea%C3%A7as-cibern%C3%A9ticas-2023

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

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

Regras Firewall IP e Porta**:** Disponível em: https://docs.netgate.com/pfsense/en/latest/firewall/rule-methodology.html. Acesso em: 20/04/2023

RFC 1594. Disponível em: http://www.rfc-base.org/txt/rfc-1594.txt. Acesso em: 20/04/2023.

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

VACCA, J. Computer and Information Security Handbook. MorganKaufmann,2009.