TUDO QUE VOCÊ PRECISA SABER SOBRE FIREWALLS

ostec
Segurança digital de resultados

Gerir de maneira eficiente o uso da internet é um passo importante, que não somente aumenta a segurança do ambiente corporativo e das pessoas, mas promove ganhos de produtividade.

ÍNDICE

INTRODUÇÃO

O termo firewall é comumente citado na literatura especializada e também no mercado de segurança da informação como um elemento básico e ao mesmo tempo super importante para proteger empresas das variadas ameaças da internet.

Neste e-book abordamos tudo aquilo que você deve conhecer sobre firewall, seja simplesmente para aumentar suas habilidades, seja para auxiliar nas suas atividades profissionais, mas especialmente, para facilitar uma decisão de compra ou reflexão acerca de sua solução.

Iniciaremos a abordam através da história, conceitos e terminologias, que formam a base de entendimento para as evoluções tecnológicas que houveram nas arquiteturas e características de firewalls ao longo de mais de 30 anos.

Traremos também aspectos mais técnicos que diferem recursos de filtragem de pacotes, bem como conceitos comerciais que foram adicionados à terminologia para melhor definir o escopo que os firewalls atingiram nesta última década.

Não abordaremos nenhum tópico específico de tomada de decisão para aquisição de firewalls, mas caso você esteja procurando sobre isso, recomendamos um excelente material que produzimos: 10 dicas essenciais para aquisição de firewalls.

HISTÓRIA

Firewall é um termo muito utilizado no mercado de segurança da informação, e com toda certeza, o ativo mais lembrado dentro de uma arquitetura de segurança. E não é para menos, o conceito não teve grandes alterações ao longo do tempo, no entanto, a abrangência passou por grandes modificações. esmo diante de tantas novidades no mercado de segurança de perímetro, os firewalls estão sempre presentes no mundo corporativo.

O QUE É

Firewall nada mais é do que um conceito, aplicado em um software, ou conjunto de software e hardware, que tem como objetivo oferecer recursos de segurança e interconexão de redes, regulamentando todo o tráfego que passa através dele, de acordo com as políticas previamente estabelecidas.

De forma complementar, o firewall é um ativo diante de uma infraestrutura, estrategicamente posicionado, por onde o tráfego é afunilado, e por conta disso, o mesmo pode permitir ou bloquear a continuidade da comunicação, se a mesma não apresentar nenhuma não conformidade ou ameaça para à rede.

Os firewalls são fortemente utilizados como estratégia de defesa em empresas dos mais variados portes e segmentados, e geralmente são posicionados em uma topologia entre redes públicas internet e redes privadas segmentos internos de rede.

Conhecer um pouco da história é entender como os desafios foram colocados ao longo do tempo, e como o mercado e as empresas se adaptaram e transformaram em um excelente modelo de negócios para um mundo cada vez mais interconectado.

LINHA DO TEMPO

Nas últimas 3 décadas tanto o conceito quanto a tecnologia evoluíram muito, e conhecer a linha do tempo é interessante para entender como as derivações e especialidades foram sendo construídas. Segmentamos em 3 grandes áreas, década de 80 e 90, e também as mudanças dos anos 2000 até 2015.

DÉCADA DE 80

Firewall não é um conceito novo, se popularizou especialmente com a disseminação da pilha de protocolos TCP/IP em decorrência de sua própria natureza. Uma vez que o protocolo IP tem a capacidade de intercomunicação, deixar redes com propósitos ou domínios empresas, universidades etc. diferentes sem qualquer controle, apresenta um risco potencial de acesso não autorizado, comprometimento de dados, entre outras possibilidades.

Por conta disso, defender o perímetro nada mais é do que criar uma barreira que separa a parte pública de interconexão oferecida pela internet, e operada por grandes empresas de telecomunicações até provedores locais, dos segmentos de rede privados.

Em redes de computadores as informações trafegam através de pacotes de um lado para outro. Cada pacote é uma unidade que leva uma porção de identificação cabeçalho e de dados conteúdo , e são roteados de maneira independente através da internet.

A primeira proposta de firewall, ou filtro de pacotes, surgiu em 1991 por Jeff Mogul's da Digital Equipament Corp (DEC), marcando, portanto, a primeira geração.

DÉCADA DE 90

O Bell Labs da AT&T, através de Steve Bellovin e Bill Cheswick, desenvolveu o primeiro conceito do que se consolidaria adiante como filtragem de pacotes stateful, ou simplesmente firewall stateful. Esta etapa ficou marcada como segunda geração de firewalls.

Em um curto espaço de tempo, surgiu a terceira geração de firewalls, onde foi inicializada a comercialização do DEC SEAL, já contando com recursos mais modernos de proxies de aplicação. A combinação entre filtro de pacotes e proxy em uma única solução fez com que o nome firewall híbrido começasse a ser mais utilizado no mercado e academia.

Em 1994 a Checkpoint lança o Firewall-1 que teve extrema importância para o amadurecimento e desenvolvimento do mercado de segurança, introduzindo de forma pioneira o conceito de GUI (Graphic User Interface), além de outras tecnologias diretamente relacionadas à segurança.

Na segunda metade dos anos 90 surgem diversos projetos em paralelo, como Squid (1996), Snort (1998), que tinham como grande propósito não a comercialização, mas o desenvolvimento e amadurecimento das soluções e conceitos ao longo do tempo. Estes projetos tiveram e tem, até os dias atuais, grande utilização por soluções de segurança comerciais e gratuitas.

Nesta mesma época surgiram outras empresas, e outros recursos de segurança foram agregados às soluções, tornando-as cada vez mais híbridas. Surgiram características como VPN, filtros de URL, QoS, integração ou incorporação de soluções de antivírus, WAF e outros, permitindo maior robustez na construção de ambientes seguros para empresas.

ENTRE 2000 E 2015

Com a incorporação de soluções complementares de segurança para os firewalls, em 2004 apareceu pela primeira vez, através do IDC, o termo UTM (Unified Threat Management). O termo nada mais é do que uma melhor denominação para a evolução ocorrida aos firewalls ao longo dos anos.

Através da popularização da internet, muitos serviços e aplicações passaram a centralizar sua operação na web. Esse movimento aumentou consideravelmente a necessidade de proteger sistemas específicos baseado no protocolo HTTP. Em 2006 apareceram de forma mais concreta os Web Application Firewalls (WAF), como soluções independentes, mas também incorporadas como recurso para UTM.

Muito embora os UTMs estivessem em grande destaque, ao reunir diversas funcionalidades e recursos de segurança em uma única solução, tinha o lado negativo associado a performance, tendo em vista o montante de recursos. Em 2008, a Palo Alto Networks traz ao mercado o conceito de firewalls de próxima geração (NGFW), resolvendo basicamente o problema de performance apresentada por UTMs, e adicionando um recurso importante que é a visibilidade e controles baseado em aplicações.

Em seguida, no ano de 2009, o Gartner passa a definir o conceito de firewalls de próxima geração. Muitos vendedores passaram por reformulações técnicas e comerciais para acompanhar as tendências que seguiriam nos próximos anos. Muitos dos outros recursos conhecidos passaram a ter um upgrade, na maioria deles somente comercial, para o termo de próxima geração , como foi o caso de NGIPS.

As tecnologias por trás de soluções de firewall mudaram muito nos últimos anos, diretamente impulsionada pela convergência de informações e conhecimento para o mundo eletrônico, e a internet foi um grande impulso para que isso ocorresse. Nos próximos anos veremos grandes transformações com IoT (Internet of Things - Internet das Coisas) e tantos outros novos desafios para dispositivos móveis que já tem presença significativa no mundo corporativo. A história não pára de ser construída.

CONCEITO E TERMINOLOGIA

Firewalls apresentam-se como um dos principais dispositivos em uma arquitetura de segurança, bem como em uma estratégia de segurança em profundidade, protegendo o perímetro fixo das empresas. A abrangência dos firewalls evoluiu muito ao longo do tempo, e especialmente por isso, conhecer os principais tipos e entender as diferenças são fundamentais para profissionais de segurança.

TIPOS DE FIREWALL

Os tipos de firewall estão associados a evolução técnica ao longo do tempo, e mais recentemente, também relacionadas ao marketing realizado por empresas para comunicar recursos de segurança em seus produtos. Isso é interessante e, ao mesmo tempo, inspira cuidados, especial ao comparar tecnologias, pois é comum fabricantes tratarem um determinado conceito com nomenclaturas totalmente diferentes.

Faremos um overview das terminologias utilizadas atualmente para diferenciar o propósito de cada uma delas. É importante destacar que muitos dos recursos, mesmo que de primeira ou segunda geração, continuam sendo utilizados por soluções atuais, pois formam a base de controle necessária para o funcionamento dos filtros.

STATELESS E STATEFUL

Apesar da idade avançada, em se tratando de aspectos tecnológicos, as filtragens sem e com estado, stateless e stateful, respectivamente, formaram a base para a construção e evolução de soluções de firewall, sendo utilizadas na atualidade.

Compreender o funcionamento destes mecanismos facilita o entendimento das novas tecnologias, além de auxiliar, de maneira substancial, na definição da melhor aplicação, de acordo com a necessidade do ambiente.

Mesmo com a complexidade por trás das soluções de segurança e firewall, os filtros stateful são utilizados com grande frequência na atualidade, contudo, quase sempre, de maneira transparente, não sendo gerenciável ou visível pelos administradores e analistas de segurança.

FILTRAGEM STATELESS OU SEM ESTADO

A filtragem sem estado oferece um recurso de avaliação de pacotes de maneira independente, onde não há conhecimento sobre a conexão. Isso quer dizer que cada pacote que passa pelo firewall, independente de ser uma nova conexão ou já existente, é avaliado pelas regras estabelecidas pelo administrador.

É comum nestas arquiteturas criar uma regra para cada direção de tráfego, prevendo tanto a saída (envio) de um pacote, quanto a entrada (recebimento) do mesmo, o que ocorre comumente em interfaces de rede diferentes. Como não há conhecimento das conexões, não é possível prever o retorno da conexão.

Os ambientes que possuem esse mecanismo de filtragem têm a tendência comum de ter um número maior de regras, por conta da necessidade de sempre se prever os dois sentidos de uma comunicação (entrada e saída).

Os firewalls stateless são cada vez menos utilizados, contudo ainda está presente em dispositivos de rede cujo principal foco não é segurança, garantindo que regras básicas de acesso ao mesmo possam ser criadas, evitando exposições desnecessárias.

O conceito mais importante a ser registrado sobre os firewalls stateless é que os mesmos não possuem conhecimento acerca das conexões, e por conta disso, aplicam suas regras em todos os pacotes que atravessam o dispositivo.

FILTRAGEM STATEFUL OU COM ESTADO

Os firewalls stateful foram concebidos posteriormente, a fim de solucionar aspectos de segurança que surgiram com a primeira geração, como por exemplo o caso de forjar spoof informações de conexão.

A importância fundamental foi de orientar a filtragem para conexão, permitindo que o mecanismo de filtragem passasse a conhecer as conexões e com base nisso legitimaria um pacote ou não. Esse recurso auxiliar ficou conhecido como tabela de conexões ou tabela de estados.

Com a tabela de estados, todo início de conexão é devidamente registrado (um novo estado é criado). Quando o pacote retorna, antes de iniciar o processo de avaliação das regras de acesso, o firewall verifica a tabela de estados, validando se há alguma conexão associada, e caso afirmativo, aceita a conexão, sem processar as regras. Do contrário, descarta o pacote.

A segurança do ambiente é incrementada consideravelmente tendo em vista que há rastreabilidade de par metros utilizados para validar uma conexão ativa na estrutura. O nível e complexidade do tracking depende do fabricante. Alguns utilizam somente parâmetros de endereços e portas de origem e destino, enquanto outros utilizam número de sequência e reconhecimento, tamanho de janela e etc, no caso do protocolo TCP.

A medida que a conexão evolui em termos de trocas de pacotes, a tabela de estados é sempre atualizada com as informações para garantir a continuidade de segurança e integridade. Este processo também garante a validade da conexão, sem que seja necessário avaliar as regras de acesso definidas pelo administrador.

Em firewalls stateful há uma economia considerável de recursos computacionais, uma vez que há um esforço inicial para a criação de novas conexões, que é recompensado até o encerramento pela não necessidade de processar as regras de acesso. É muito comum encontrar esse mecanismo de filtragem nas mais modernas soluções, que continua sendo um elemento fundamental na estratégia de defesa em profundidade.

PROXY

O termo firewall proxy, ou simplesmente proxy, é aplicado para controles mais especializados sobre um determinado protocolo de aplicação. Os proxies funcionam de maneira complementar em uma arquitetura de segurança, oferecendo um controle mais aprofundado de acordo com os comportamentos e características do protocolo suportado.

O exemplo que podemos trazer como mais comum, facilitando o entendimento, trata-se do controle de navegação, onde pode-se gerenciar os acessos aos sites de acordo com diversos par metros, como usuários, endereços, horários e outros. Enquanto um firewall stateless e stateful atuaria permitindo ou bloqueando o acesso a porta utilizada para navegação (atuando até a camada 4), o proxy HTTP tem a visibilidade da última camada oferecendo, portanto, maior flexibilidade para aplicação de políticas de acesso.

Em muitos casos, os proxies de aplicação atuam de maneira transparente em uma arquitetura de segurança, onde o tráfego para a porta associada ao serviço é automaticamente direcionando para o proxy, onde os controles são aplicados de acordo com a necessidade da empresa. Em outros casos, porém, é necessário configuração, ou intervenção manual, para que se tenha acesso ao proxy e uso do serviço.

Outro exemplo interessante de integração e complementariedade de firewalls stateful com proxy é que, caso o último seja manual e não esteja devidamente configurado em um dispositivo (computador, tablet, smartphone etc.), o filtro de pacotes com estado pode bloquear o acesso, forçando que determinada aplicação só funcione através do proxy.

Pela diversidade de aplicações e serviços, não é comum e nem necessário haver proxies para cada serviço. Portanto, é mais comum visualizar proxies atuando de maneira especializada nos protocolos HTTP, FTP, IMAP, POP3, SMTP e outros. Os proxies podem atuar tanto no sentido de saída de conexões, quanto de

entrada, nestes casos mais conhecidos como proxies reversos.

Um proxy reverso permite centralizar um conjunto de aplicações e publicá-las para a rede, com base no que é requisitado, o proxy direciona para o ativo que tem determinada informação ou aplicação. Como todo tráfego acaba sendo afunilado no proxy, ataques podem ser detectados antes do pacote ser encaminhado para a aplicação de fato.

É bastante comum a utilização de proxy reverso para publicação de aplicações web na internet, onde o servidor não é diretamente exposto, e todo tráfego passa por uma camada intermediária de segurança. Outros recursos comumente utilizados em arquiteturas de proxy reverso é o balanceamento de carga, compactação de tráfego, que permitem a construção de ambientes altamente disponíveis e taxas consideráveis de economia de banda.

INSPEÇÃO PROFUNDA DE PACOTES (DPI)

Os desafios de segurança ao longo do tempo cresceram de tal forma que analisar e filtrar os pacotes com base nas informações do cabeçalho se tornaram insuficientes para garantir a integridade dos ambientes, uma vez que os ataques estavam cada vez mais direcionados para a camada de aplicação. Os sistemas de detecção de intrusão (IDS) e posteriormente a evolução para sistemas de prevenção de intrusão (IPS) adicionaram o conceito de inspeção profunda de pacote, ou inspeção profunda de conteúdo.

Através deste conceito, os pacotes não passam mais a ser analisados somente baseados nas informações armazenadas em seus cabeçalhos, mas especialmente em seu conteúdo. Com um modelo baseado em assinaturas, os dados dos pacotes são analisados e caso seja identificado algum comportamento anômalo ou ataque, uma ação é tomada, registrando o evento, bloqueando a conexão, entre outras facilidades.

Similarmente aos proxies, a capacidade de analisar aplicações por parte de IDS/IPS não é necessariamente ampla, pois é mandatório conhecer o comportamento do protocolo para inserir as análises e comparações com base no conhecimento existente da solução (assinaturas). Como uma porção muito maior de informações são armazenadas na área de dados de um pacote, é comum que esse mecanismo ofereça maior consumo de recursos computacionais, especialmente CPU.

Ratificando a importância de vários elementos de segurança em uma arquitetura realmente robusta, mesmo os proxies atuando em sua grande parte na área de cabeçalho da camada de aplicação, a área de dados de maneira geral não é visualizada. O conceito de DPI, presente em IDS/IPS, permite acrescentar essa visibilidade e consequentemente ter um ambiente de segurança mais robusto, menos suscetível à ataques.

PRINCIPAIS TOPOLOGIAS DE FIREWALL

As topologias de firewall nada mais são do que representações físicas e lógicas do posicionamento dos ativos computacionais e dos dispositivos de segurança, neste caso, limitamos somente as principais aplicações para firewalls corporativos.

TOPOLOGIA BASTION HOST

As topologias de firewall nada mais são do que representações físicas e lógicas do posicionamento dos ativos computacionais e dos dispositivos de segurança, neste caso, limitamos somente as principais aplicações para firewalls corporativos.

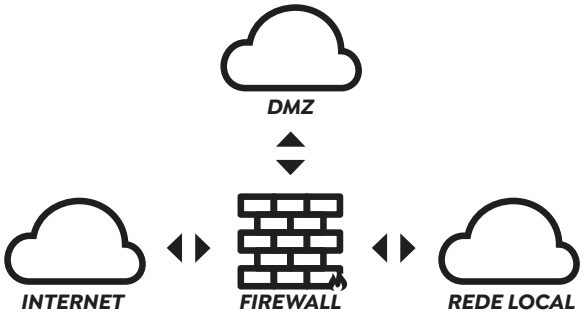
Apesar de extremamente simples, é possível visualizar que para o tráfego entrar ou sair da rede protegida, é obrigatório passar pelo firewall. Esta topologia oferece apenas uma camada de segurança real, por conta disso, é necessário avaliar com atenção os cenários onde é recomendada a utilização desta topologia.

Uma vez que o firewall seja comprometido, não há nenhum impedimento do atacante acessar a rede protegida. Independente das quantidades de camadas lógicas presentes no firewall, se o mesmo for comprometido, a rede local poderá ser potencialmente atacada.

Portanto, tenha em mente em utilizar essa arquitetura para pequenas necessidades de acesso à internet, onde não há servidores internos que sejam acessados publicamente pela internet, ou que ofereçam algum tipo de serviço interno valioso para a empresa, como banco de dados, arquivos e outros.

TOPOLOGIA DE SUBNET COM TRIAGEM

Uma topologia muito comum de firewall que preserva flexibilidade e ao mesmo tempo níveis de segurança adequados para boa parte dos ambientes é denominada screened subnet, ou subnet com triagem. Através desta topologia, empresas podem oferecer serviços para a internet, sem comprometer suas redes protegidas.

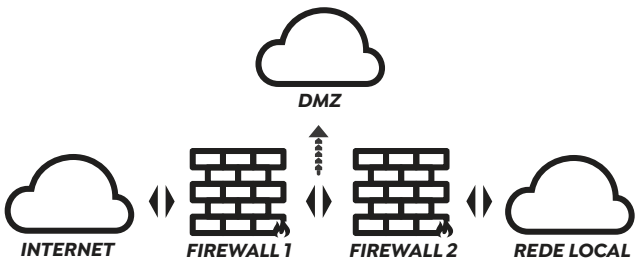


A base para o funcionamento de uma subnet com triagem é o firewall possuir pelo menos três interfaces de comunicação, para que se possa isolar a internet, as redes protegidas, e por fim, criar um local denominado de zona desmilitarizada, ou DMZ.

Os serviços de rede públicos, como servidores web, servidores de e-mail e outros, são estrategicamente posicionados na DMZ. Caso um atacante comprometa o acesso de algum destes servidores, ainda assim, ele não terá acesso direto às redes protegidas, pois o firewall está interposto nesta arquitetura.

Nos casos em que existirem múltiplas redes protegidas que devem ser diretamente interconectadas pelo firewall, pode-se trabalhar com VLANs associada a um número menor de interfaces físicas. Sobre o ponto de vista de segurança não há nenhum impacto, no entanto, é importante validar se haverá throughput suficiente para atender as demandas de tráfego.

TOPOLOGIA MULTI-HOMMED OU DUAL-FIREWALL



De maneira complementar a topologia de sub-rede com triagem, as arquiteturas mult-hommed são compostas por diversas conexões que permitem segmentar várias redes. Além disso, em muitos casos essas arquiteturas trabalham com dois equipamentos distintos, incrementando ainda mais a segurança do ambiente, uma vez que o comprometimento de um deles não significa o acesso para às redes protegidas.

A quantidade de conexões físicas (portas ou interfaces) e lógicas através de VLANs oferecidas por esta topologia permite definir, de maneira muito segregada, como criar a política de segurança adequada para proteger computadores, servidores e outros ativos importantes de uma organização.

É relevante destacar que a topologia final da arquitetura de segurança pode (e deve) misturar os conceitos abordados, permitindo criar uma verdadeira blindagem para sua infraestrutura. A defesa em profundidade, especialmente quando aplicada em dispositivos isolados, oferece níveis interessantes de resiliência em um ambiente diante de um ataque.

Não há uma topologia que possa ser considerada melhor, o entendimento está naquilo que é melhor para a realidade de proteção de sua empresa. Arquiteturas mais complexas exigem maior custo total de propriedade (TCO), tanto para aquisição de tecnologias produtos quanto mão de obra especializada para continuidade do ambiente.

FIREWALL UTM E NGFW

O mercado de firewalls nos últimos anos tem sido tomado por dois conceitos de soluções, que geram em alguns casos confusão no que diz respeito ao funcionamento, abrangência e especialmente diferença.

UNIFIED THREAT MANAGEMENT OU GERENCIAMENTO UNIFICADO DE AMEAÇAS

O conceito de Firewall UTM surgiu de forma natural, ao longo do tempo, de acordo com a necessidade e evolução do próprio mercado de segurança. A medida que novos ataques ou vulnerabilidades eram descobertas, incrementava-se o firewall com novos recursos e funcionalidades.

Por conta disso, um UTM pode ser facilmente identificado como um ativo de software e hardware, ou uma combinação entre os dois, que centraliza em plataforma única características de filtragem stateful, VPN, proxy web, antivírus, IDS/IPS, inspeção profunda de pacote (DPI) etc.

Como limitação ao Firewall UTM, podemos destacar problemas associados a performance, uma vez que todas as funções de segurança estão centralizadas em um único produto. O problema é evidenciado em ambientes corporativos, com alto volume de pacotes e hardware insuficiente, trazendo prejuízos no que tange processamento das regras de segurança aplicadas no ambiente.

Por outro lado, a centralização pode ser incrivelmente positiva para pequenos e médios negócios, onde um único dispositivo atenderá grande parte das necessidades de segurança, com valores altamente competitivos se comparados a aquisição de produtos individuais para atender separadamente as necessidades.

"Unified threat management (UTM) is a converged platform of point security products, particularly suited to small and midsize businesses (SMBs). Typical feature sets fall into three main subsets, all within the UTM: firewall/intrusion prevention system (IPS)/virtual private network, secure Web gateway security (URL filtering, Web antivirus [AV]) and messaging security (anti-spam, mail AV)."

NEXT GENERATION FIREWALL OU FIREWALL DE PRÓXIMA GERAÇÃO

Firewall de Próxima Geração ou NGFW foram desenvolvidos com a motivação de resolver a deficiência de performance apresentada nos UTMs, entregando recursos de controle de aplicação e inspeção profunda de pacotes em uma arquitetura altamente performática e coesa.

Recursos complementares como proxy web, proteção contra vírus e malwares e outros presentes em Firewall UTM não fazem parte da arquitetura de um NGFW, estas características foram removidas e

terceirizadas, garantindo altas taxas de escalabilidade para grandes ambientes.

A principal contribuição do NGFW, está nos avanços tecnológicos gerados a partir da inspeção profunda de pacotes e na visibilidade de aplicações, independente de protocolos e portas. Esses recursos, em conjunto, permitem não somente que ataques possam ser evitados, mas principalmente criam políticas de controle de acesso mais dinâmicas e eficientes para os desafios atuais de segurança.

"Next-generation firewalls (NGFWs) are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall. An NGFW should not be confused with a stand-alone network intrusion prevention system (IPS), which includes a commodity or nonenterprise firewall, or a firewall and IPS in the same appliance that are not closely integrated."

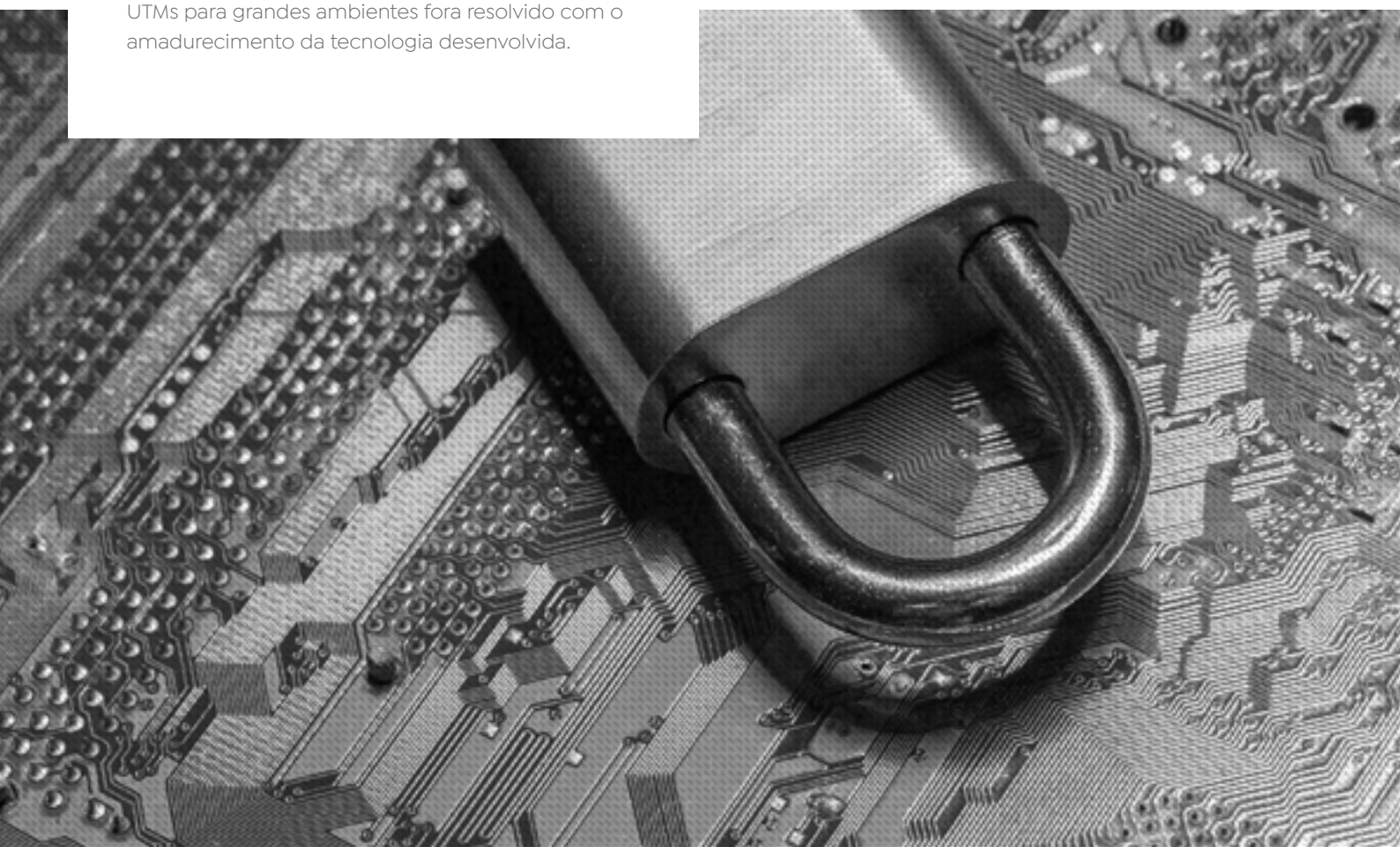
PRINCIPAIS DIFERENÇAS ENTRE UTM E NGFW

Apesar dos conceitos apresentarem diferenças substanciais, ainda assim existe uma certa dificuldade no entendimento dos mesmos. Muitos escritores e fornecedores defendem que atualmente não existe diferença, na prática, entre os dois tipos de produtos. Isso por que, o principal desafio de UTMs para grandes ambientes fora resolvido com o amadurecimento da tecnologia desenvolvida.

Existem outros formadores de opinião que defendem que NGFW são indicados para ambientes de grande intensidade de tráfego, especialmente empresas complexas, telecomunicações e outras que centralizam uma quantidade grande de trânsito de dados. Nestes casos, separar os ativos de segurança é fundamental para a escalabilidade e resiliência do ambiente. Sendo assim, um Firewall UTM seria recomendado para o mercado de pequenas e médias empresas (SMBs), onde o fluxo de dados é inferior.

O fato é que, independente do termo utilizado e do porte da empresa, o mais importante a ser analisado durante o processo de compra de uma solução de segurança de perímetro, é se os recursos oferecidos atendem aos requisitos funcionais e de crescimento do ambiente, sendo este o ponto mais relevante, independente do conceito utilizado UTM ou NGFW.

Outro aspecto de fundamental importância é analisar a tecnologia que está sendo empregue para oferecer os recursos de Firewall UTM e NGFW. Ambos trouxeram, de fato, grandes contribuições para o mercado de segurança em diversos fabricantes. Outros, no entanto, apenas trataram de mudar sua nomenclatura, sem agregar tecnologia de fato aos produtos entregues ao mercado.



CONTINUE LENDO

SE VOCÊ GOSTOU DO ASSUNTO E GOSTARIA DE NOVAS LEITURAS, FIQUE A VONTADE PARA CONSULTAR ATRAVÉS DOS LINKS ABAIXO TEMAS RELACIONADOS EM NOSSO PORTAL.

VOCÊ SE INTERESSOU PELO CONTEÚDO?

ESCLAREÇA SUAS DÚVIDAS COM ESPECIALISTAS NO ASSUNTO

CONVERSE COM ESPECIALISTA

facebook.com/ostec

linkedin.com/company/ostec-business-security

contato@ostec.com.br

www.ostec.com.br

ostec.blog

ostec

Segurança digital de resultados