# SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

AULA 6

Prof. Douglas Eduardo Basso

## CONVERSA INICIAL

Na aula de hoje, vamos falar sobre servidores proxies, as suas funções e funcionamento, o processo de tradução de endereços (NAT), conceitos de sistemas de detecção de ataques e detecção de intrusos, os tipos de IDS, as maneiras de identificação de ataques e intrusos, as diferenças entre IDS e IPS.

Nos temas posteriores, serão abordados o controle de conteúdo, o funcionamento dos filtros de conteúdo, os benefícios desses controles, a confiabilidade de acesso, os relatórios de acesso, categorização de conteúdo.

Em seguida, temos as proteções antimalware, o funcionamento dessas proteções, tipos de detecção baseadas em assinatura, comportamento e na heurística. As boas práticas relacionadas a proteção contra *malwares* e como será o futuro dessas soluções.

Por fim, vamos ter os conceitos de *firewall*, suas características, estrutura e os *firewalls* de nova geração, as soluções UTM. Como uma solução integrada de gestão de ameaças pode ser a chave para conter esse grande número de ameaças virtuais que se apresentam no ambiente computacional.

## TEMA 1 – *PROXY*

Para Galvão, no mundo digital, o tráfego de informações, isto é, dados que entram em uma rede e saem dela, não só devem ser controlados, como pontos específicos desse tráfego devem ser identificados. Para definir uma proteção de perímetro em uma rede, é importante que seja definido quais dados podem trafegar livremente e quais deverão ser bloqueados e barrados.

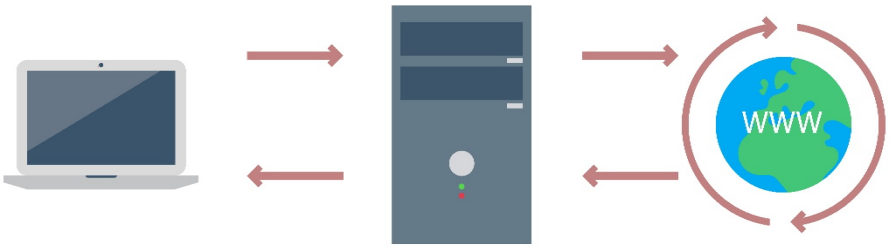
O *proxy* é um servidor que age como um intermediário para requisições de clientes solicitando recursos de outros servidores. Um cliente conecta-se ao servidor *proxy* solicitando algum serviço, como um arquivo, conexão, página *web* ou outros recursos disponíveis de um servidor diferente, o *proxy* avalia a solicitação como um meio de simplificar e controlar sua complexidade.

Os proxies foram criados para incrementar mais estrutura e encapsulamento a sistemas distribuídos. A maioria dos proxies são usados para *web*, facilitando e filtrando o acesso ao conteúdo da Internet, fornecem um acesso à Internet quase de maneira anônima (Fraga, 2019).

Um *proxy* é um servidor que recebe e encaminha uma série de requisições de acesso a *sites* de internet de máquinas clientes que estão conectadas à

Internet. Dessa maneira, o endereço IP e as páginas acessadas ficam registradas no servidor *proxy*. Assim, o endereço IP do cliente não fica exposto na rede, dificultando que seja possível rastrear os acessos, ele faz uma centralização do acesso à Internet.

Figura 1 – Servidor *Proxy*




Crédito: psv16/Shutterstock.

Ele também pode disponibilizar alguns recursos *web* armazenados no cache em redes de computadores. São máquinas que ficam interligadas a redes externas e fazem filtros, controle de conteúdo, registros de páginas acessadas além de outras regras de acesso. Pode prover conexões anônimas, armazenamento em cache de páginas *web*. É um equipamento dentro da estrutura de rede que atua entre os clientes de acesso e as redes externas.

## 1.1 Funções do *Proxy*

Conforme mencionado anteriormente, o *proxy* faz todo o intermédio de acesso à *web*, porém os servidores *proxy* podem desempenhar uma série de funções úteis. Vejamos as principais utilidades e funcionalidades dos proxies.

- *Firewall*: é uma solução de segurança com a função de bloquear acessos indevidos às redes que devem ser protegidas, possui ações de contramedidas contra vírus, malwares e tentativas de invasão e ataques. Como o *proxy* fica estrategicamente entre uma rede confiável e a internet, é uma posição ideal para implantar algumas funções de *firewall* para bloquear e aprovar o tráfego recebido e enviado a rede e seus clientes.
- Filtros de conteúdo: o *proxy* também pode fazer filtros e controles de conteúdo em relação a aplicações e *websites*. As organizações normalmente configuram servidores *proxy*, como filtros de conteúdo.

Alguns *proxys* possuem uma classificação de *sites* por categoria (jogos, redes sociais, organizacionais, acadêmicos, rádios *web*). Isso permite que os administradores filtrem os acessos dos colaboradores, controlando, assim, o conteúdo de acesso, podendo gerar relatórios de acesso para auditoria.

- Contorno de filtros de conteúdo: existem uma série de servidores *proxy* espalhados pelo mundo. Caso não exista um *firewall* bloqueando, é possível configurar um servidor *proxy* diferente para acessar a internet, sem os bloqueios do *proxy* corporativo.
- *Caching*: o *cache* é uma funcionalidade do *proxy* que armazena de maneira temporária dados dos *websites* mais acessados, o que torna mais ágil e rápido o acesso. Proxies têm a função de armazenar *sites* em *cache* para que eles sejam acessados de forma mais eficiente, pois, dessa maneira, não é necessário que todo o tráfego do *site* seja carregado novamente nos próximos acessos. Isso apresenta uma grande redução na latência, ou seja, no tempo que leva para que os dados sejam transferidos pela Internet.
- Segurança: o *proxy* pode ainda complementar a segurança servindo como o único equipamento ligado diretamente à Internet. Do ponto de vista de quem está fora, como o *proxy* centraliza o acesso de todos os usuários da rede, para quem enxerga de fora para dentro da rede, os acessos aparecem de maneira oculta, pois, nesse tipo de cenário, somente o endereço IP do proxy aparece na Internet. Caso um *hacker* queira invadir um dispositivo específico na rede, será uma tarefa bem difícil de executar.
- Compartilhamento e centralização de conexões de Internet: as organizações podem criar uma única conexão de internet e utilizar o *proxy* para fazer toda a centralização de acesso a todos os dispositivos da rede. Em redes sem fio, os *proxys* podem ser uma boa solução para concentrar os acessos à Internet passando por um servidor *proxy*.

## 1.2 Funcionamento do *Proxy*

Uma das principais arquiteturas computacionais utilizadas na Internet é a arquitetura cliente e servidor. Essa arquitetura permite a classificação dos elementos de tecnologia em duas categorias: os clientes e os servidores. Os

dispositivos com funções de cliente sempre fazem requisições, como um acesso à internet, por exemplo, navegando por servidores *web*, acessados por endereços *web*.

Os dispositivos com funções de servidores atendem as solicitações dos clientes e fazem a transmissão dos dados requisitados. Todo o *website* possui no mínimo um servidor que hospeda os dados e informações, normalmente, são grupos de servidores que armazenam essas informações, com alta disponibilidade, com a finalidade de oferecer os recursos para as solicitações do cliente. Essa troca de dados (entrada e saída) são conhecidas como tráfego *web*.

Quando a organização não possui um servidor *proxy*, os colaboradores acessam a Internet de maneira direta, sem filtros de conteúdo e controle. Todos os *sites* são acessados entre os navegadores (Chrome, Firefox, Edge) e se conectam diretamente com os servidores *web*. Dessa forma, a identificação do endereço IP do cliente é feita de maneira transparente, quase que de maneira pública, é facilmente identificado.

Um servidor *proxy* é um dispositivo de controle, filtros e intermediação de tráfego. O *proxy* tem duas interfaces de rede, uma conectada diretamente à Internet e outra à rede local da organização, fazendo uma tradução de endereços das requisições entre a rede local e a Internet. Os clientes se comunicam através do *proxy* até a Internet. Ele centraliza os acessos e faz os encaminhamentos de tráfego até a Internet.

No sentido inverso, quando os servidores da *web* responderem as solicitações encaminhadas pelo *proxy*, os proxies criam uma tabela de endereços de endereços públicos e locais e fazem todo o escalonamento de requisições e respostas. A maioria dos servidores proxies conseguem ocultar o endereço IP dos clientes, para que, dessa forma, os *websites* não consigam acessar e fazer qualquer tipo de identificação dos clientes. Ao empregar um *proxy* com endereço IP de outra localidade ou país, para fazer a interligação, é possível mascarar informações de origem, localização e nacionalidade.

## 1.3 *Proxy* Reverso

Os proxies reversos são empregados pelas organizações para aprimorar e consolidar a segurança de acessos as redes pela Internet. Um servidor *proxy* reverso apresenta algumas funções polivalentes. Ele centraliza todos as requisições externas de clientes e as encaminha aos destinatários certos,

criando um caminho seguro, evitando que *hackers* acessem a rede interna da organização.

Um *proxy* reverso geralmente atende às solicitações de um cliente da rede externa (Internet) e faz o encaminhamento para um servidor interno. Este responde às solicitações para o *proxy* reverso que devolve as informações ao cliente. Os proxies reversos têm três recursos interessantes: a segurança, o balanceamento de carga e a facilidade de manutenção.

Os proxies reversos desempenham um papel fundamental na melhoria e qualidade de acesso. Cria uma camada de segurança interessante, filtrando os acessos externos à rede interna. Um *proxy* reverso é eficiente e eficaz na proteção de sistemas contra vulnerabilidades da *Web*.

O *proxy* reverso faz o intermédio de acesso entre clientes externos e serviços internos, criando uma barreira de acesso. Com uma estrutura menos exposta, menor é a chance de criminosos virtuais conseguirem sucesso em suas tentativas de invasão, garantindo a segurança dos ativos corporativos. Isso representa uma grande redução de riscos de ataques por duas questões.

- Os servidores ficam blindados e mais protegidos contra *hackers*.
- Os *hackers* normalmente buscam *websites* que apresentam muitas vulnerabilidades e, consequentemente, mais fáceis de invadir. Com o *proxy* reverso, cria-se uma barreira contra as tentativas de invasão e ataques virtuais.

Dentro da topologia de rede, o *proxy* fica localizado entre a rede interna e externa. Dessa forma, ele pode armazenar um certificado digital e prover uma comunicação criptografa utilizando o protocolo SSL. O *proxy* reverso deve ser o elo para todas as aplicações e todos os seus servidores internos. Assim, não seria necessário fazer a gerência de vários certificados nem criptografar sua rede interna.

O certificado SSL é um certificado digital que autentica a identidade de um *site* e possibilita uma conexão criptografada. A sigla SSL significa *Secure Sockets Layer* (camada de soquete seguro), um protocolo de segurança que cria um *link* criptografado entre um servidor *Web* e um navegador *Web*.

## 1.4 Tradução de endereços (NAT)

O serviço de tradução de endereço de rede que também é chamado NAT (*network address translation*) apresenta um conceito mais específico que fazer uma correlação de endereços lógico. Na prática, é uma tradução entre endereços IPs de redes diferentes. Normalmente, essa tradução envolve vários endereços de rede privados, sendo traduzidos em endereços públicos por meio da alteração das informações de rede e informações de endereço encontradas no cabeçalho IP dos pacotes de dados.

As redes LAN possuem diversos endereços IP de redes privadas que são atribuídos a dispositivos específicos na rede. Com o processo de NAT, esses endereços privados são traduzidos em um endereço IP público quando são enviadas solicitações de saída dos dispositivos de rede para a Internet.

Um processo inverso ocorre quando os dados recebidos, geralmente como uma resposta à solicitações específicas, são enviados para uma rede local. Neste caso, o NAT altera o endereço IP público para o endereço IP privado do dispositivo específico para o qual o pacote de dados é direcionado. O endereço IP público é usado repetidamente pelo roteador que conecta os computadores à Internet (Iplocation, 2021),

Com o crescimento das redes de computadores e o aumento cada vez maior de dispositivos conectados à Internet, os IPs públicos (IPv4) se tornaram recursos limitados e, atualmente, existe uma escassez. O processo de tradução de endereços (NAT) tem como finalidade minimizar a utilização de endereçamento público, fazendo essa tradução de endereços IPs privados.

Os endereços públicos são gerenciados por entidades reguladoras locais, são endereços pagos que permitem a identificação de maneira unívoca de dispositivos (computadores, roteadores, servidores e demais elementos) na Internet. Todavia, os endereços utilizados nas redes privadas apenas têm funcionalidade nos domínios de redes locais e não são reconhecidos na Internet. Equipamentos configurados com um IP de redes privadas só conseguem se conectar à Internet através de um IP público. Os servidores *Proxy* provêm esse tipo de tradução de endereços.

Segundo o *Speedcheck*, existem quatro maneiras de utilização do processo de NAT, podendo ser empregados para atender diferentes cenários de uso e situações. A seguir, vamos descrever esses quatro modelos.

- Tradução de Endereço Portuário ou Sobrecarga (PAT) – é o modelo mais empregado de NAT. Ele é capaz de mapear vários endereços IP privados para um único endereço IP público. Esse processo é possível uma vez que o equipamento de rede que implementa o PAT utiliza portas que identificam univocamente cada pedido das máquinas locais. Existe uma limitação de 65.536 conexões internas que podem ser traduzidas em um único IP público. Esse modelo acaba se tornando muito eficaz e eficiente em casos em que os provedores de serviços tenham disponibilizados apenas um único endereço IP público.
- NAT dinâmico – nessa configuração, o mapeamento é criado a partir de um endereço IP privado para um grupo de endereços IP públicos, chamado de grupo NAT (NAT *pool*). Esses endereços de IPs públicos são oferecidos e disponibilizados pelos provedores de serviços de Internet. O mapeamento público-privado pode variar de acordo com o endereço público disponível na *pool* do NAT.
- NAT estático – nesse modo, a configuração e o mapeamento dos endereços são feitos de maneira permanente de um endereço IP público para um endereço IP (um para um). É muito utilizado para equipamentos e dispositivos que necessitam ser acessados de redes externas. Usualmente, esse método de NAT é mais empregado para disponibilizar o acesso a servidores com funções específicas, como: serviços de mensagens (*e-mails*), servidores *web*, videoconferências, entre outros.
- Redirecionamento de Portas – o NAT na modalidade de redirecionamento de portas, disponibiliza uma funcionalidade em que um único endereço IP público consiga fazer encaminhamentos de portas de comunicação, e isso dá a possibilidade a vários servidores e serviços internos de diferentes aplicações serem acessados pelas portas de comunicação redirecionadas pela Internet.

## TEMA 2 – IDS/IPS

Visando o combate a ataques e invasões, existem algumas soluções de software e hardware de proteção para fazer a segurança da infraestrutura tecnológica das organizações, fazendo os controles de acesso e combatendo as tentativas de invasões e ataques. Essa categoria de soluções tem um papel

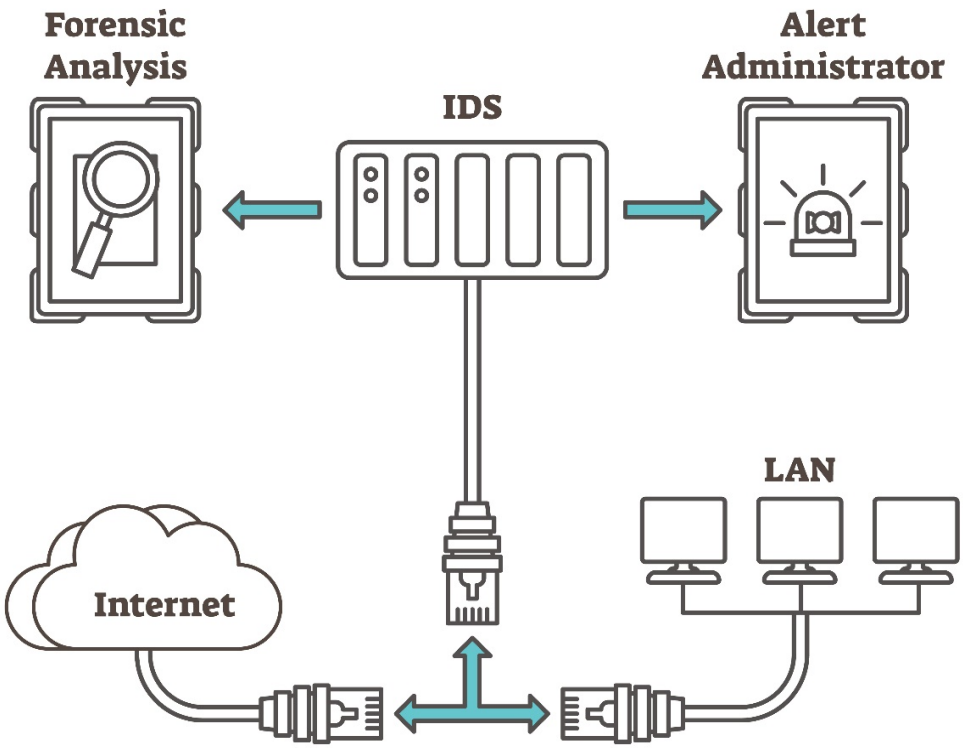
primordial na gestão de segurança, tendo em vista que o número de ataques virtuais tem crescido de maneira exponencial.

Nesse contexto, podemos elencar dois tipos de sistema utilizados para a prevenção de ataques: Sistema de Detecção de Intrusos (IDS) e Sistema de Prevenção de Intrusos (IPS). Essas duas aplicações trabalham de maneiras bem semelhantes, todavia, faz uma função específica. Ter o entendimento é essencial para a decisão de qual tecnologia é mais prioritária na estratégia de segurança de rede.

Os sistemas de detecção de intrusos (IDS) permitem fazer uma com detalhes de todo o tráfego de rede em diversos pontos da estrutura, sendo possível identificar vários tipos de atividade maliciosa. Ao localizar um evento que atente contra a política de segurança, o IDS faz a análise e armazena um registro detalhado do evento malicioso ao administrador de rede.

Com esse registro, é possível ser utilizado como evidência para uma tomada de ação ou contramedida. O IDS utiliza todos os registros de informações que servem como base, auxiliam e ajudam a compreender a todos esses eventos de violação de políticas de segurança que são elaboradas para defender toda a infraestrutura da rede. A Figura 2, a seguir, apresenta um cenário de utilização de um IDS:

Figura 2 – Sistema de Detecção de Intrusão




Crédito: VectorMine/Shutterstock.

Já os sistemas de detecção de intrusos (IPS) são sistemas que fazem uma função de controle, que tem no *firewall* o seu complemento. Vamos falar de *firewall* mais adiante. Ele atua da seguinte maneira: o administrador cria e elabora uma série de regras e instruções de análise de tráfego que bloqueiem e rejeitem determinados pacotes de dados. Quando uma requisição de acesso chega à infraestrutura de rede, o IPS faz toda a checagem das regras criadas e possíveis instruções que possam bloquear ou rejeitar o pacote de dados da requisição que chega. Caso o pacote de dados não esteja nas regras de rejeição, o IPS permite o tráfego de dados.

## 2.1 Tipos de IDS

Os sistemas IDS têm como principal função a detecção de se algum criminoso virtual está tentando invadir algum sistema corporativo ou se alguém da equipe interna está fazendo um acesso indevido. O IDS é executado em segundo plano e gera diversos alertas e notificações em relação a ocorrências que apresentem algum tipo de suspeita. Ele pode ser classificado pela forma de

monitoramento que ele executa. Por meio da origem de dados e dos algoritmos de detecção utilizados, existem dois tipos de implementação de sistemas IDS.

- *Host Based IDS* (HIDS) – nesse tipo de IDS, o sistema é instalado nos servidores (*hosts*) para efetuar os alertas e fazer a identificação das tentativas de ataques. Esse modelo é empregado quando a segurança está estritamente focada e baseado nos equipamentos de rede e servidores.
- *Network Based IDS* (NIDS) – no IDS baseado em rede, o sistema é instalado em algumas máquinas responsáveis para fazer a identificação de tentativas de ataques. Fazem o monitoramento de pacotes de rede de maneira detalhada, analisando cabeçalhos e protocolos de rede.

Nos sistemas IDS baseado em rede, o monitoramento é executado de maneira simultânea, porém a eficiência e eficácia diminui à medida que escalabilidade de rede cresce. A necessidade de analisar muitos pacotes com as velocidades de rede cada vez maiores se torna uma tarefa difícil, a utilização de criptografia também é um fator que dificulta ainda mais esse monitoramento, diante desse cenário, a utilização de sistemas baseados em servidores é essencial em ambientes críticos. Alguns IDS conseguem trabalhar de maneira híbrida, combinando os dois modelos de sistemas.

## 2.2 Tipos de IPS

Os sistemas de detecção de intrusão (IPS), geralmente, ficam instalados na configuração no fluxo de dados que passa pelo *firewall* e fornece uma camada secundária de análise na filtragem de fluxo de dados, bloqueando os conteúdos nocivos à rede. De maneira diferente do sistema de detecção de intrusão (IDS) – que é um sistema que atua de maneira passiva, fazendo a verificação de tráfego e gerando alertas sobre ameaças –, o IPS é colocado em linha (no caminho de comunicação direta entre fonte e destino), analisando de forma ativa e executando ações automatizadas em todos os fluxos de tráfego que entram na rede. Especificamente, essas ações incluem:

- faz envios de alertas e alarmes ao administrador de rede;
- eliminação de ameaças;

- executa o bloqueio imediato do tráfego perigoso a rede, através do endereço de origem do fluxo de dados; e
- reativa a conexão de rede ao interpretar tráfegos legítimos como ameaças.

O IPS tem alguns métodos de detecção para identificar as explorações e tentativas de invasão, são elas: detecção baseada em assinatura, a detecção baseada em anomalias estatísticas e a detecção baseada em diretivas são os três métodos empregados pelos IPS.

- Detecção baseada em assinatura – esse método faz a utilização de um dicionário de padrões (ou assinaturas), são identificáveis no código e nas assinaturas de cada exploração. À medida que essas atividades são descobertas, a sua assinatura é registrada, gravada e armazenada em um dicionário de assinatura que segue crescendo e sendo incrementado continuamente. A detecção de assinatura para IPS é classificada em dois tipos: a exploração individual e a visibilidade de vulnerabilidade.
    - Exploração individual – nesse tipo de IPS, as assinaturas são checadas, conseguem identificar tentativas de invasão executadas com *exploits* individuais, elencando e classificando alguns padrões exclusivos de uma tentativa específica de exploração. O IPS pode identificar explorações específicas ao encontrar uma correspondência com uma assinatura que está registrada como uma exploração no fluxo de tráfego.
    - Visibilidade de vulnerabilidade – nesse tipo de IPS, as assinaturas com visibilidade de vulnerabilidades apresentam uma avaliação mais ampla que checam a vulnerabilidade inerente de alguns sistemas que está sendo direcionado à tentativa de ataque. Esse tipo de assinatura permite que as redes sejam protegidas e seguras contra algumas variantes de ataques ou alguma exploração que talvez ainda não tenha sido mapeada e observada diretamente dentro do ambiente de rede, mas é um método que pode aumentar o risco de falsos positivos, ou seja, bloquear conexões legítimas achando que é uma ameaça.
- Detecção baseada em anomalias – faz análise estatísticas, levando em conta algumas amostras de tráfego de rede e faz uma comparação com

o tráfego normal mapeado anteriormente. É possível fazer uma análise a um nível de desempenho levando como base o comportamento natural da rede. Quando a amostra da atividade de tráfego de rede está acima ou fora dos parâmetros do desempenho comparado com o tráfego padrão, o IPS toma medidas para lidar e contornar essa situação.

- Detecção baseada em diretivas – além dos métodos apresentados anteriormente, baseados em assinaturas e em anomalias, a detecção de intrusão do IPS pode ser criada e executada com base em diretivas configuradas pelos administradores de rede. Nesse método, o dispositivo deve ser configurado e programado com um conjunto de regras e normas de operação. Sempre que um tráfego em rede fizer alguma violação de uma das diretivas previamente configuradas e programadas, o IPS deve bloquear o tráfego de rede em questão e notificar ao administrador da rede sobre esse evento e gerar uma ocorrência.

## 2.3 Diferenças entre IDS e IPS

Os sistemas de intrusões podem ser conceituados como dispositivos criados e desenvolvidos com o intuito de fazer indicações ao administrador, quando algum evento fora dos padrões ou indevido ocorre, classificando como uma possível invasão. Para atender a essa tarefa, o IDS faz o monitoramento da rede e, quando necessário, faz a identificação de atividade suspeita, cria diversos alertas e alarmes para o administrador de rede. O administrador, dessa maneira, deve analisar a atividade identificada como suspeita e definir as soluções mais adequadas para lidar com ela.

Da mesma maneira que o IDS, os sistemas de prevenção contra intrusão monitoram e gerenciam as redes empresariais em busca de atividades suspeitas. O grande ponto de atenção é que esse dispositivo é configurado e é capaz de executar ações e medidas como prevenção, como restringir a atividade suspeita bloqueando o acesso do usuário responsável pela atividade maliciosa. Levando em conta as características dos dois dispositivos, podemos dizer que a maior diferença entre eles se encontra no elevado grau de autonomia do IPS, o que tende a tornar sua utilização a escolha mais eficiente e eficaz.

## TEMA 3 – CONTROLE DE CONTEÚDO

Com a evolução das tecnologias de informação e comunicações e com o advento da mobilidade e a Internet, a sua utilização se tornou frequente e obrigatória nas organizações. É praticamente inviável atualmente obter algum tipo de sucesso nos negócios sem a ajuda ou complemento dessa poderosa ferramenta. Com a Internet, podemos atualizar as mídias sociais, estabelecer conexão com aplicativos, programas servidores e uma série de fontes de dados, elaborar pesquisas, consultar dados e realizar pagamentos, acompanhar o mercado financeiro, as notícias, entre outras utilidades oferecidas.

Devido ao acesso maciço às diversas páginas da Internet, a dinâmica do espaço digital e as constantes troca de dados, as organizações têm buscado soluções que protejam suas informações, apresentem mais segurança aos colabores e minimizem os impactos de ataques e furtos cibernéticos. Controlar o conteúdo da Internet é uma das camadas dessa segurança da informação. Ou seja, é essencial aplicar um controle de conteúdo, um filtro *web*, de acordo com as políticas de segurança empresariais.

A utilização de maneira livre e liberada da Internet pode criar diversos reflexos positivos e negativos para as organizações. Tudo vai depender do modelo de negócio, do cenário de utilização, do perfil dos colaboradores, entre outros fatores. Podemos concluir que o acesso sem filtros à Internet pode trazer várias consequências, como perda de tempo e desempenho em páginas de Internet que não são de cunho empresarial e que não atentam quanto aos interesses da organização. Isso acaba comprometendo a produtividade e o desempenho de colaboradores e departamentos. De outra maneira, pode ajudar a estimular a criatividade, a variedade e o desempenho de determinados colaboradores.

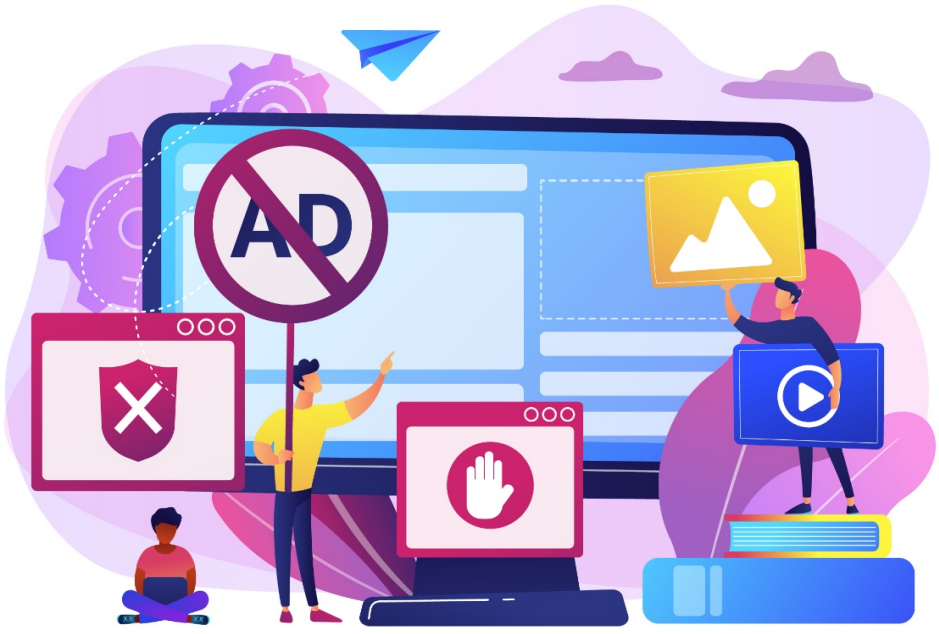
Nesse aspecto, é plausível que as organizações tenham em mãos alguns métodos e modelos capazes de melhorar o desempenho, a *performance* e a eficiência de seus colaboradores, implementando uma política de controle de conteúdo na internet de maneira equilibrada e benéfica à organização.

As conexões com a Internet abriram oportunidades infinitas de negócios, não só para as organizações produzirem mais em menos tempo e com mais produtividade, gerando mais resultados, todavia, por outro lado, aumentou a superfície de ataques para criminosos virtuais.

Para proteger colaboradores, parceiros, clientes, propriedades intelectuais, ativos de rede, informações críticas, as empresas precisam de uma segurança proativa em relação à Internet. Uma solução de controle de conteúdo de acesso na Internet é fundamental, um modelo não se limita apenas a bloquear apenas endereços de internet conhecidos como prejudiciais, aplicações maliciosas, ou até mesmo acessos que consomem muitos recursos (mídias sociais, conteúdos audiovisuais, rádios *web*), mas também acessos desconhecidos e ocultos amplamente difundidos na internet.

Ao compreender o comportamento de acesso aos conteúdos da Internet e o contexto em que ele se apresenta, podemos prever intenções maliciosas, bloqueando ameaças de segurança impedindo o acesso à rede. O uso irrestrito e totalmente liberado a Internet e aplicações pode tornar os colaboradores improdutivos, com baixo desempenho, além de gerar possíveis problemas jurídicos. Com um acesso liberado, o consumo de recursos computacionais é muito maior, como utilização alta do *link* Internet, aumento do armazenamento de dados, consumo de largura de banda, processamento de equipamentos de rede, servidores, entre outros. Isso pode impactar drasticamente na *performance* e desempenho dos recursos de rede e Internet, que são recursos indispensáveis às atividades diárias das organizações.

Figura 3 – Controle de conteúdo




Crédito: Visual Generation/Shutterstock.

## 3.1 Funcionamento dos filtros de conteúdo

Para a Kasperky, os filtros de conteúdo da Internet normalmente são chamados de software *de controle de conteúdo e aplicações*. São programas criados para restringir acesso a *sites*, aplicações e endereços de Internet. A aplicação desses filtros pode funcionar usando uma lista branca ou uma lista negra: a lista branca faz a permissão de acesso somente a *sites* especificamente escolhidos por quem criou e elaborou a lista, e a segunda faz a restrição do acesso a *sites* e aplicações indesejáveis, conforme determinado pelos padrões criados na lista negra e nos filtros de palavras-chave.

Esses programas analisam o endereço eletrônico do *site* desejado, portas de comunicação das aplicações, buscam palavras-chave, extensões restritas no conteúdo do *site* para fazer a decisão de bloqueio ou permissão de acesso. Os filtros de conteúdo são normalmente instalados como extensões do navegador de Internet, como um programa autônomo no computador ou como parte e complemento de uma solução global de segurança. Todavia, esses componentes podem ser instalados nos servidores de rede (*proxys*, *firewall*, soluções de filtro de conteúdo e aplicações), seja pelo provedor de Internet ou por uma empresa terceirizada que presta esse serviço de controle de conteúdo e aplicações para a restrição e, ao mesmo tempo, o acesso de vários usuários à Internet (Kaspersky, 2021).

- Software*s* de controle de conteúdo – as soluções de controle e filtro de conteúdo atuam em duas frentes principais: controle de conteúdo para pais que desejam filtrar o acesso de seus filhos, e organizações que desejam impedir que seus funcionários acessem *sites* e aplicações que não sejam do interesse da organização ou que não tenham relação com o trabalho. Os filtros de conteúdo de Internet também são utilizados como ferramenta de prevenção de *malwares* e vírus, pois bloqueiam o acesso a *sites* que costumam hospedar *malwares* e ameaças correlatas, *sites* com conteúdo pornográfico, jogos de azar, terrorismo, entre outros. As soluções mais avançadas podem até bloquear tráfegos de dados que são enviados pela Internet para garantir que seus dados sigilosos não sejam expostos e divulgados.

Existem algumas formas de burlar um software de controle de conteúdo, isso pode ser feito com a utilização de *proxy* de Internet (caso esteja liberado o acesso). Usar *sites* de outras localidades e em outros idiomas, às vezes, é possível acessar *sites* correlatos ou tentar acesso através de uma VPN contratada de forma privada. Por causa dessas falhas e vulnerabilidades, nem sempre é possível controlar o conteúdo.

As soluções de filtro de conteúdo e aplicações são uma maneira de aumentar a segurança contra as milhões de ameaças virtuais que encontramos na Internet. São soluções que dificultam e impedem que essas ameaças cheguem aos computadores dos usuários e faz também com que os usuários não acessem *sites* de procedência duvidosa ou armadilhas de Internet.

Ao longo de sua execução, os softwares de controle de conteúdo atuam da seguinte forma: a ferramenta faz a checagem e validação dos endereços eletrônicos acessados para analisar e verificar se esse endereço eletrônico está ou não na lista de possíveis vulnerabilidades. Se o endereço estiver, o usuário recebe um aviso e não consegue acessar o conteúdo. Todavia, se o *site* for liberado, é garantido o acesso ao ambiente seguro e o controle de conteúdo libera a conexão.

A análise é feita de maneira granular e considera informações de protocolos de acesso, domínio, portas de comunicação, entre outras variáveis antes de liberar o conteúdo.

## 3.2 Benefícios dos filtros de conteúdo

Existem diversos benefícios gerados pelas soluções de controle de conteúdo e aplicações. A implementação de um controle das conexões de Internet eficiente dentro de uma organização traz uma série vantagens. Aspectos relacionados ao aumento da segurança, da confiabilidade dos sistemas e menor risco, ameaças e vulnerabilidades a ataques por meio de falhas de sistema são apenas algumas das melhorias geradas por essas soluções de controle de conteúdo. Dessa forma, podemos destacar, também, o que se segue.

- Aumento da Segurança e Proteção – os avanços tecnológicos atrelados às inovações digitais tornaram os *websites* muito mais dinâmicos. Todavia, os mesmos códigos que oferecem uma navegação mais rápida, ao serem manipulados por algum criminoso virtual, podem causar sérios

impactos a segurança da informação. Soluções de filtro de conteúdo devem ser efetivas e capazes de mapear, identificar e bloquear qualquer conteúdo malicioso que esteja alojado dentro de uma página de Internet, protegendo a rede da organização de possíveis ataques. Além de apresentar mais agilidade no controle de uso da internet, os filtros de conteúdo *web* devem oferecer uma camada complementar de segurança. Os filtros de conteúdo conseguem categorizar de maneira completa os conteúdos, incluindo a classificação de *sites* que possuem conteúdos maliciosos. Com regras automáticas configuradas, esse tipo de conteúdo proporciona mais segurança a infraestrutura, facilitando o trabalho de analistas e gestores.

- Segurança e Proteção Conteúdos Impróprios – acesso a *sites* de pornografia, nudez, jogos de azar ou a *download* de conteúdos assegurados e protegidos por direitos autorais feitos de maneira ilegal podem causar sérios problemas para muitas organizações. Ao bloquear e impedir que esse tipo de acesso seja feito e que os dados originados desses acessos circulem pela rede corporativa com o filtro de conteúdo, diversos problemas de segurança de acesso a esse tipo de conteúdo podem ser evitados. Diante disso, a rede corporativa vai utilizar menos recursos computacionais (largura de banda, roteamento, tráfego de dados), e o acesso críticos ao negócio serão priorizados.
- Melhoria de Produtividade de Colaboradores – procurar e buscar métodos e ferramentas que aumentam o desempenho e produtividade dos colaboradores é um desafio para os administradores de empresas. Uma das principais causas de problemas de produtividade é o uso liberado da Internet. Além de gerar perda de lucros para as organizações, na prática, acaba elevando os custos operacionais e a utilização dos recursos computacionais de equipamentos da rede, *links* de internet, entre outros. Ao configurar de maneira correta sistemas de controle de tráfego, filtros de conteúdo e aplicações, os administradores de rede garantem que somente os dados relativos ao negócio estejam disponíveis para acesso a seus colaboradores, impedindo que conteúdos irrelevantes à atividade empresarial sejam visualizados. Buscar por soluções adequadas que aumentem a produtividade da equipe é um desafio constante. Com o uso da internet liberado, fica muito fácil para que os colaboradores se tornem

menos produtivos, causando danos representativos às empresas. Isso tem impacto direto na falta de produtividade.

- Confiabilidade de Acesso – a verificação e o encerramento de qualquer tipo de conexão insegura que um dispositivo conseguir fazer utilizando a rede da organização são uma das funcionalidades dos filtros de Internet. Além da checagem em relação a nomes de domínios pesquisados e acessados, o filtro analisará todo o tráfego de Internet, permitindo que somente conteúdos classificados como seguros sejam exibidos e mostrados na tela do computador do usuário. Dessa maneira, a organização terá mais confiabilidade dos acessos e dos dados que são transmitidos pelos pelas suas redes, trazendo para seus colaboradores um acesso seguro a conteúdos e livres de códigos maliciosos.
- Relatórios de acesso – uma das grandes vantagens do controle de conteúdo e filtros de acesso são os relatórios gerados pelas soluções. Isso permite que os administradores saibam de maneira exata o que cada colaborador está acessando, qual a taxa média de consumo de banda por cada equipamento ligado à rede, quanto tempo os colaboradores permanecem em cada *website*, o número de acessos, entre outras variáveis. Esses relatórios trazem a possibilidade para que analistas de TI atuem de forma proativa, antecipando algumas ações corretivas através do mapeamento e identificação de anormalidades no uso da internet. Algumas soluções de controle de conteúdo trazem ainda opções de envio de notificações automáticas por *e-mail*, facilitando a operação diária da infraestrutura de TI das organizações.
- Categorização de conteúdo – um dos maiores desafios enfrentados pelos analistas de segurança de informação se refere à listagem de *sites* e aplicações que ser criadas e atualizadas, com o alinhamento necessário às políticas de segurança corporativas, com a finalidade de impedir que a Internet seja a porta de entrada de ameaças digitais à organização. É muito difícil elaborar essas listas de maneira manual, pois o trabalho de atualização é extremamente trabalhoso, e o resultado atingido na prática tem pouca efetividade. Com ferramentas específicas e modernas de filtros de conteúdo, grande parte dessas dificuldades desaparecem. Essas soluções atualmente consultam bases gigantescas de endereços eletrônicos e são criadas uma série de base no conteúdo, propósito e

descrição. Essa forma de atuação e funcionamento diminui a complexidade associada à manutenção de listas de acesso, garantindo mais eficiência para a equipe de TI. Existem algumas listas de acessos disponíveis em ferramentas gratuitas de controle de conteúdo, mas nem sempre são as melhores soluções. Redes sociais, como o Facebook, têm uma infinidade de endereços específicos em seus servidores, tornando impossível identificar todos eles, todavia, ao executar a categorização de maneira correta de todos os conteúdos, torna-se muito mais fácil gerir e controlar o tempo dos funcionários em atividades corporativas úteis e alinhadas aos processos de negócio.

## TEMA 4 – PROTEÇÃO ANTI *MALWARE*

Um dos primeiros vírus de computador que foi registrado na década de 1980 foi um vírus de *boot* que infectou disquetes e se espalhou rapidamente. Desse período em diante, os vírus de computadores evoluíram muito. Com o advento da Internet, a proliferação de vírus é mais rápida e os números potenciais de vítimas é muito maior.

Como mencionado anteriormente, os *malwares* compreendem todos os tipos de códigos e software*s* maliciosos, sendo incluído os tipos mais conhecidos como: Cavalo de Tróia, *ransomware*, vírus, *worms* e *malwares*. As proteções anti *malware* são os elementos especiais de qualquer solução de segurança da informação para organizações. Os objetivos das proteções anti *malware* são fazer a identificação de ações e arquivos maliciosos, fazendo o bloqueio e impedindo que quaisquer danos ocorram com os equipamentos de TI.

Os criadores e autores de *malwares,* atualmente, agem de maneira muito criativa. Esses códigos maliciosos conseguem ser distribuídos, plantados e espalhados pelas vulnerabilidades em sistemas operacionais sem atualizações de segurança, conseguindo burlar algumas medidas de segurança. Eles conseguem se alojar na memória ou fazem réplicas e imitações de aplicativos legítimos apenas para conseguir permanecer indetectáveis às soluções anti *malware*.

## 4.1 Funcionamento da proteção anti *malware*

As soluções *antimalware* fazem a identificação das ameaças de diversas maneiras, ao depender da estrutura e característica de cada solução anti *malware* e do cenário de implementação. De maneira geral, esses softwares utilitários fazem análise de um determinado arquivo, código, *plugin*, aplicação ou amostra, fazendo uma investigação de se há algum tipo de risco ou perigo. Depois, fazem um reporte de resultados e, se necessário, fazem a paralização de execução da aplicação identificada como suspeita. Dessa forma, existem uma série de soluções de segurança que mantém um grande banco de dados de amostras maliciosas identificadas anteriormente, sendo empregadas múltiplas tecnologias de proteção como contramedidas aos novos *malwares*.

Na sequência, a solução anti *malware* faz um processamento sobre a amostra de arquivo avaliada. Com isso, a finalidade dessa atividade é avaliar e determinar se o arquivo é criptografado, qual é sua estrutura, elencando seu formato e outras características. A partir desses dados, o software determina como analisar o arquivo. A solução anti *malware* faz uso de vários filtros de checagem, detecção, verificação se há ou não uma ameaça no arquivo.

Algumas soluções anti *malware* têm a funcionalidade de abrir o arquivo em um ambiente monitorado restrito, uma espécie de *sandbox*. Se a solução for empregada em serviços de mensagens (*e-mail*), servidores *web*, *proxys*, sistemas de prevenção de invasão (IPS) e correlatos, processamentos adicionais podem ser requeridos antes que técnicas de detecção entrem em execução.

## 4.2 Tipos de detecção anti *malware*

As soluções anti *malware* fazem uso de várias ferramentas para checagem, detecção e escaneamento para fazer a identificação de *malwares* que já estejam hospedados nos dispositivos e, dessa forma, impedir que esse infecte os dispositivos. Os métodos e técnicas de detecção de vírus e *malwares* são elencados de diferentes maneiras. Vamos abordar os principais métodos.

- Detecção baseada na assinatura – esse método utiliza a estrutura do arquivo examinado para gerar uma espécie de impressão digital (um *hash* do arquivo) de *malwares* já identificados e documentados. Dessa

maneira, a assinatura pode apresentar tamanhos diversos dentro do arquivo. Esse método de detecção já foi o componente principal nas ferramentas anti *malware* e continua sendo parte integrante de várias soluções atuais, embora seu grau de importância tenha diminuído. Uma das desvantagens desse método é não conseguir detectar e alertar sobre novos arquivos maliciosos, cujas assinaturas ainda não foram mapeadas e identificadas. Portanto, essa limitação acaba possibilitando a ação e execução de códigos maliciosos novos por criminosos virtuais.

- Detecção baseada em heurística – nesse segundo método, é executada uma detecção generalizada de *malwares* e feita uma análise estatística em arquivos para buscar estruturas e características suspeitas. Uma ferramenta e proteção anti *malware* pode buscar por instruções incomuns ou códigos maliciosos nos arquivos checados. Podem ser feitas simulações de execução de um arquivo para avaliar seu comportamento. Nessa simulação, caso um único atributo seja identificado como suspeito, pode não ser suficiente que o arquivo seja classificado como nocivo ou malicioso. Todavia, uma série de características pode ultrapassar o limite estipulado de riscos, levando a solução a classificar o arquivo como nocivo ao sistema. O grande defeito da tecnologia heurística é que ela eventualmente pode identificar arquivos legítimos como suspeitos. É possível encontrar recursos integrados e complementares para checagem e investigações potenciais que indicam se houve algum tipo de comprometimento. Dessa forma, os certificados maliciosos que são usados na assinatura dos arquivos nessas detecções.
- Detecção comportamental – nesse método anti *malware*, é feita uma análise do processo de execução de um aplicativo ou programa. Esse tipo de detecção tem a finalidade de fazer a identificação de *malwares* ao avaliar e investigar possíveis comportamentos suspeitos. Notificar essas ações, de forma geral, habilita a ferramenta a detectar a presença de ameaças que já foram identificadas como legítimas e que não causam danos ao sistema. Para servir como base nesse processo de identificação e proteção contra *ransomware*, por exemplo, a detecção comportamental pode até mesmo fazer o impedimento que arquivos adicionais sejam criptografados. Da mesma forma que ocorre no método de heurística, cada grupo de ações não pode ser capaz de fazer a classificação de um

programa como um *malware*. Porém, se ações em conjunto são tomadas, esse modelo pode ser eficiente na identificação de arquivos maliciosos. Vale falar também que o emprego de técnicas de comportamento aproxima mais as soluções anti *malware* de serviços hospedados em provedores, que, naturalmente, já coexistiam como uma outra categoria de proteção de segurança.

- Detecção baseada em nuvem – nesse método de identificação e detecção de *malwares*, os dados são coletados e armazenados em uma *sandbox*. Em um segundo passado, são empregados métodos de análise e testes com os dados. Essa etapa é executada na infraestrutura de propriedade do provedor e podemos dizer que é feita análise localmente. A investigação normalmente é efetuada por intermédio de coleta e captura de parâmetros que tenham relevância sobre os arquivos e sua maneira de execução, sendo processados dentro da estrutura na nuvem. Todavia, esse processamento pode impactar na execução em potencial de um arquivo classificado como nocivo e malicioso, são feitas avaliações em relação a suas próximas ações. A nuvem possui um mecanismo capaz de buscar e derivar padrões relacionados às características, estruturas e comportamentos do *malware*, fazendo correlação com dados de múltiplos sistemas. É importante complementar que a maioria dos provedores dessas soluções já fez a inclusão de diversas tecnologias de que utilizam em sua estrutura inteligência artificial e aprendizado de máquina para a análise de *malwares*, criando uma automatização dessas atividades.
- Detecção de *malwares* invisíveis – nesse tipo de detecção, é possível identificar uma série de avanços no combate aos *malwares*. É um método recente que foi integrado às soluções anti *malware*. Nesse contexto, os *malwares* são identificados e detectados com base em um *script* ou conjunto de comandos, que são executados em um dispositivo.

Os métodos de detecção de ameaças que são baseados em assinatura podem ser eficientes de alguma forma, entretanto, as proteções anti *malware* mais avançadas trazem a possibilidade de efetuar a identificação, classificação e detecção de ameaças fazendo uso de técnicas e métodos que têm o intuito de mapear e identificar elementos que sejam nocivos, danosos e maliciosos aos sistemas.

De outra forma, a detecção que tem como base a assinatura (a impressão digital dos arquivos) está buscando ameaças já identificadas. Ambas são ótimas formas de mapear as ameaças, porém, em caso de ameaças novas não catalogadas, isso se torna uma falha de segurança. Em soluções mais atuais anti *malware*, a identificação de ameaças ainda desconhecidas pode ser feita pela identificação de atividades suspeitas, analisando a estrutura e o comportamento do programa, tráfego de dados, entre outras.

De forma análoga, seria como monitorar um indivíduo que sempre está em locais frequentados por diversos outros criminosos e que ainda anda com ferramentas e *kits* para abrir fechaduras no bolso.

## 4.3 Boas práticas e recomendações contra malwares

Com a evolução da tecnologia e à medida que os *malwares* vêm se modificando e se tornando cada vez mais avançados, com grande parte dos dados sendo hospedados na Internet, as ameaças de *malwares* em relação aos dados privativos para fins nocivos e maliciosos têm sido uma grande preocupação, como manter o sigilo de informações e ter esses dados seguros.

Existem algumas formas se proteger. Logo a seguir, elencamos algumas recomendações para tentar minimizar as possíveis ações e evitar que *malwares* infectem seus dispositivos e consigam acessar informações sensíveis e preciosas.

- Utilizar proteção anti *malware* – utilizar softwares de proteção avançados para verificação automática de dispositivos com intuito de encontrar ameaças. Esses sistemas devem ser capazes de impedir a ação de *malwares* e, caso o dispositivo tenha sido infectado por um *malware*, é importante que a proteção tenha condições de remover a ameaça.
- Proteção em telefones celulares – os telefones celulares, em sua essência, são computadores pequenos e que cabem em nossos bolsos. Com tantos indivíduos utilizando celulares, muito mais do que *laptops* ou *desktops*, são dispositivos que apresentam muitas vulnerabilidades e estão suscetíveis a ameaças e infecções por *malwares*. Dessa forma, é essencial fazer a proteção adequada tanto nos telefones celulares como computadores e outros dispositivos que sejam alvos de ataques de *malware*.

- Aplicações legitimas e genuínas – para minimizar os riscos de ataques e infecções por *malwares*, é importante utilizar e baixar aplicativos, software*s* ou arquivos de mídia somente de *sites* autorizados, de fabricantes que sejam confiáveis. Quando falamos de celulares, as lojas, como a Google Play Store, no Android, ou a App Store, no iPhone, são os canais mais apropriados para isso. Utilizar instaladores e arquivos ou até mesmo aplicativos de *sites* desconhecidos é um grande risco, pois os *malwares* podem vir camuflados em software*s* que se dizem legítimos.
- Identificar detalhes de desenvolvimento – eventualmente, um software infectado por *malware* pode ser hospedado na rede legítima do desenvolvimento e acabar sendo armazenado em *sites* confiáveis. Detalhes de versão de software e do desenvolvedor na descrição podem ser checados e avaliados.
- Avaliações de utilizadores – ao buscar qualquer software ou aplicativo que será utilizado, é válido verificar as avaliações dos utilizadores. Os criminosos virtuais em algumas ocasiões conduzem usuários a baixar *malwares* forjando boas avaliações. Um aplicativo legítimo geralmente possui uma combinação de avaliações que mostram vantagens e desvantagens (Kaspersky, 2021).
- Número de *downloads* efetuadas – aplicativos que são infectados por *malware* provavelmente não possuem muitos *downloads*. Todavia, é menos provável que os aplicativos com milhares de *downloads* sejam algum tipo de *malware*. Se o aplicativo for popular (com muitas avaliações e *downloads*), então você não precisa ficar tão preocupado: as chances de ele ser um *malware* serão muito menores (Kaspersky, 2021).
- Solicitação de permissões – alguns aplicativos ou componentes de aplicativos solicitam várias permissões. É importante avaliar se o aplicativo realmente precisa ter acesso a ligações, câmeras, localização ou qualquer outro componente do dispositivo. É preciso ter cautela e evitar qualquer tipo de permissão não necessária.
- *Links* inseguros – clicar em *links* não checados em mensagens eletrônicas, em *e-mails* forjados, *spams* e outros tipos de mensagens ou *websites* desconhecidos pode ser um grande risco. Ao acessar *links* infectados, pode ser o início do *download* de um *malware*. Confirmações de dados, senhas, usuários, sistemas bancários, há uma série de

ameaças relacionadas a captura de dados importantes. Muitas mensagens parecem legítimas, em alguns casos, é importante contactar a instituição financeira em caso de suspeita de fraude e uso de dados bancários.

- Atualização de sistemas operacionais – as atualizações de sistemas operacionais devem ser feitas de maneira automática ou com grande frequência. É a maneira de minimizar as possíveis vulnerabilidades. Os dispositivos acabam se beneficiando com as atualizações recentes de segurança de sistema. É primordial manter as aplicações atualizadas nos dispositivos. Os fornecedores de aplicativos usam essas atualizações de segurança para aplicar medidas corretivas criadas pelos desenvolvedores para ajudar e auxiliar na proteção de dispositivos e dados. A grande maioria dos ataques cibernéticos partem da exploração de vulnerabilidades de s*oftwares* para ter acesso a dispositivos e sistemas.
- Cuidado com redes sem fio – ao utilizar redes sem fio de acesso à Internet em ambientes públicos, compartilhados, como universidades, aeroportos e outros locais, é importante ter cautela com acessos a redes sem fio gratuitas. Ter cuidado ao expor dados confidenciais por meio de compras na Internet e acessos a serviços bancários. Caso seja necessário, ao usar redes gratuitas, é recomendável utilizar algum tipo de conexão VPN, para que, dessa forma, seja possível proteger a conexão criptografando os dados no tráfego e transporte.
- Utilização de dispositivos removíveis – a conexão de *pendrives* desconhecidos em dispositivos é um grande risco à segurança. Muitas unidades removíveis podem estar infectadas por *malware*. É valido fazer uma checagem com uma ferramenta de varredura de *malwares*.

## 4.4 O futuro das proteções anti *malware*

A Inteligência Artificial (AI) e o aprendizado de máquinas são os novos elementos dos avanços da tecnologia anti *malware*. A AI traz a possibilidade de máquinas executarem algumas tarefas que não tenham sido pré-programadas especificamente. Ela não executa simplesmente uma sequência limitada de comandos de forma automática, como uma tarefa agendada.

O conceito e a estrutura da AI permitem que se façam análises mais minuciosas de situação, cenários e casos de uso e, por meio dessa análise de

estados, pode-se desenvolver ações de acordo com o objetivo a ser atingido, como a identificação de atividades de um *malware* como o *ransomware*. O aprendizado de máquina é outro elemento de programação capaz de fazer reconhecimento de padrões em dados novos, posteriormente, faz a classificação desses dados de maneira que o aprendizado ensine as máquinas a tomar decisões.

Em relação ao futuro das proteções anti *malware*, a Inteligência Artificial tem o foco na criação e desenvolvimento de equipamentos cada vez mais inteligentes, enquanto o aprendizado de máquina faz o emprego de algoritmos e programações que apresentam a possibilidade de que as máquinas aprendam com suas experiências e com a análise de ambientes e estados.

Esses dois elementos são perfeitos para serem aplicados de maneira mais intensa na segurança cibernética, principalmente depois da grande quantidade e a variedade de ameaças que tem sido criada e que está surgindo diariamente. Esse cenário de ameaças está se tornando cada vez mais complexo, estourando as capacidades dos métodos baseados em assinaturas. Tanto a AI quanto o aprendizado de máquina ainda requerem mais pesquisas e estudos, pois ainda estão em fase de desenvolvimento, mas são elementos promissores na área de segurança da informação.

Seguindo essa linha de evolução, segundo a *Malwarebytes*, outras duas formas relativamente novas de *malware* contribuíram para o avanço e o desenvolvimento de métodos de detecção sem assinatura: são os *exploits* e o *ransomware*. Por mais que essas ameaças sejam semelhantes a outros tipos de *malwares*, eles são muito mais difíceis de serem identificados e detectados. Em muitos casos, uma vez que os dispositivos foram infectados, é praticamente impossível fazer a remoção desse tipo de *malware*.

Os *exploits*, como o nome já diz, são exploradores de vulnerabilidades de sistemas, software*s* ou navegadores de Internet. Eles foram criados para injetar e instalar códigos maliciosos de diversas maneiras. As contramedidas de *exploits* foram elaboradas e desenvolvidas para proteger os dispositivos desses métodos de ataque. Muitos *malwares* do tipo *exploits* ainda não possuem soluções e atualizações de segurança capazes de neutralizarem essa ameaça.

O *ransomware* é um tipo de *malware* que ganhou muito destaque nos últimos anos ao fazer o sequestro e a criptografia de dados de diversos dispositivos de tecnologia da informação. É utilizado para manter os dados

criptografados como uma espécie de refém para promover extorsão e pedir resgates e pagamentos. Alguns criminosos virtuais costumam até fazer ameaças de deleção de dados caso o prazo do pagamento do resgate não seja efetuado. Atualmente, ambas as ameaças resultaram na criação, elaboração e no desenvolvimento de novos produtos dedicados a combater *malwares* do *exploit* e o *ransomware* (Malwarebytes, 2021).

## TEMA 5 – *FIREWALL* E *FIREWALL* DE NOVA GERAÇÃO

As guerras sempre fizeram parte da história da humanidade. A necessidade de defender-se dos inimigos fez com que as técnicas de defesa fossem criadas e aprimoradas. Uma das mais antigas e utilizadas é a construção de um muro que serviria como barreira física para afastar invasores, demarcar territórios e evitar as derrotas. Vários muros caíram, uns viraram atração turística e outros permanecem de pé.

No fim dos anos 1980, foi criado o conceito de *firewall* devido à necessidade de criar restrições de acesso entre redes de dados. Naquela época, o perigo era externo, o medo principal era que um vírus derrubasse toda a rede, como, aliás, aconteceu por diversas vezes. O perímetro era a referência de defesa.

Com a chegada dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes e de métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação também adquiriram importância vital para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável.

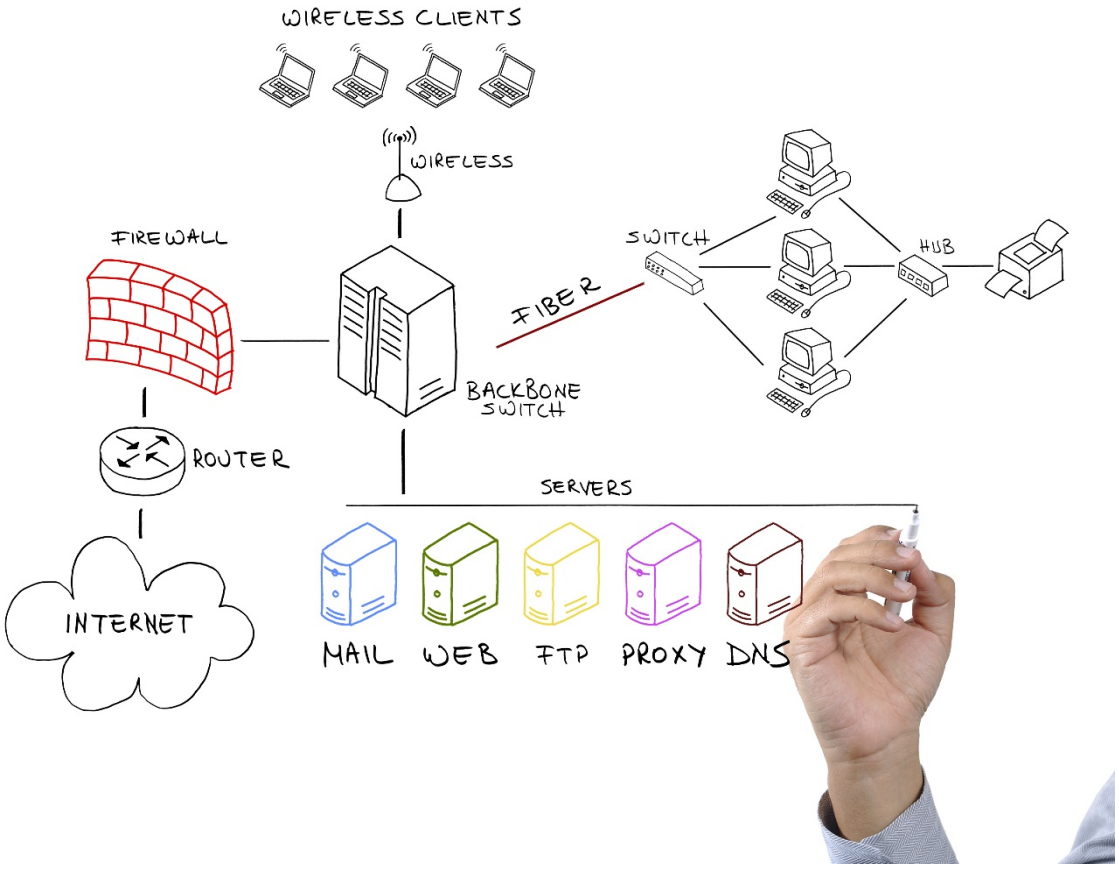
Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local. Com as mudanças tecnológicas e com o uso de computadores de grande porte, a estrutura de segurança ficou um pouco mais sofisticada, englobando controles lógicos, porém ainda centralizados.

Com a chegada dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, os aspectos de segurança

atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes e de métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação também adquiriram importância vital para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável.

A Internet cresceu e hoje o cenário é bem diferente. Atualmente, as ameaças virtuais estão em qualquer lugar, o antigo perímetro já não existe mais. Foi necessária uma evolução nos *firewalls* e é preciso acompanhar essa mudança. Os *hackers* se tornaram mais sofisticados e seus ataques também, mais direcionados inclusive. Muitos dos ataques atuais são ataques combinados, que usam várias técnicas para tentar se infiltrar em uma rede. A Figura 4 a seguir apresenta cenário de utilização de um *firewall*:

Figura 4 – Cenário de uso de *firewall*




Crédito: Oez/Shutterstock.

Embora as organizações precisem de várias técnicas para combater ataques combinados, gerenciar várias ferramentas de segurança separadas

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

## 5.1 *Firewall*

Um *firewall* é uma solução (software e/ou hardware) que tem a função de reforçar a segurança de informação entre uma rede privada interna segura e uma rede insegura e não muito confiável como a Internet. O *firewall* tem a responsabilidade de criar e manter uma barreira de segurança para todo os dados trafegados pela rede, criando um obstáculo contra ameaças que podem ser originadas das redes externas. Existem uma série de recursos empregados para esse mecanismo de segurança.

Os *firewalls* são visualizados como um elemento de proteção muito importante entre as redes internas e a Internet. Quando os *firewalls* não são utilizados nas redes e em computadores, os sistemas se tornam desprotegidos e muito vulneráveis a ataques cibernéticos, acessos indevidos, programas mal intencionados, deixando as portas de conexão expostas a qualquer tipo e investida criminosa.

Em relação à sua estrutura, um *firewall* pode ser um computador, um servidor, um roteador, um *mainframe* ou a combinação desses elementos. Normalmente, ele é implementado no ponto onde a rede interna e a rede externa se cruzam, fica no chamado perímetro da rede e tem a função de controlar e filtrar todo o tráfego.

É primordial lembrar que o *firewall* mais adequado para uma organização vai depender de uma série de variáveis, seja pela característica de navegação, tipo de tráfego, a escala da rede, o nível de segurança, as funcionalidades que devem ser aplicadas, estrutura de rede, sistemas operacionais utilizados, entre outros.

Os analistas de redes e infraestrutura têm a responsabilidade de, frequentemente, analisar todos os registros, alertas e eventos gerados pelo *firewall*. Normalmente, são encontrados diversos tipos de *firewalls* nas organizações, dependendo da estrutura do cenário de segurança, pois coexistem várias necessidades específicas de proteção.

## 5.2 Soluções UTM

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

Os UTM protegem a sua rede em tempo real contra ataques combinados e reduzem o custo total de operação. Seguem alguns benefícios dessa solução:

- reduz custo e gastos com a Internet pelo controle do uso dos *links* de dados;
- melhora o desempenho do seu *link* de Internet com filtros de navegação *web*;
- aumenta a disponibilidade dos *links* de Internet com balanceamento de *links*;
- protege os usuários com antivírus de navegação;
- conexão de qualquer lugar à sua rede com acesso seguro aos dados corporativos com VPN; e
- faz a integração de suas unidades remotas com maior segurança e confiabilidade.

## 5.3 Funcionalidades das soluções UTM

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

- Controle de Aplicações – uma importante característica do UTM é a maior visibilidade a aplicativos que geram tráfego na rede, juntamente com a capacidade de controlar essas aplicações. O controle de aplicativo pode identificar e controlar aplicativos, software*s*, programas, serviços de rede

e protocolos. A fim de proteger as redes contra as últimas ameaças criadas no mundo digital, o controle de aplicativo deve ser capaz de detectar e controlar todo o acesso a plataformas sociais, como Youtube, Facebook e Twitter, para controlar o uso de aplicações em toda a rede corporativa. Com esse recurso habilitado, é possível determinar quais aplicações podem ou não trafegar pelo seu *link* de Internet. É possível bloquear aplicações que compartilham arquivos, P2P, mensagens instantâneas, navegadores e milhares de aplicações conhecidas. O controle de aplicativo deve fornecer políticas granulares de permissões de acesso, possibilitando que seja permitido ou bloqueado o acesso a aplicativos com base no tipo de fornecedor da aplicação, comportamento e tecnologia utilizada. É possível bloquear, permitir ou apenas monitorar o uso das aplicações. É possível controlar o uso de novas aplicações *web*, por exemplo, liberar o Facebook, mas não permitir o uso do bate-papo ou de aplicativos de jogos dentro do Facebook, entre outros.

- Antivírus – a tecnologia do antivírus no UTM fornece proteção em várias camadas contra vírus, *spyware* e outros tipos de ataques de *malware*. É possível aplicar proteção antivírus para transferência de arquivos (FTP), mensagens instantâneas e conteúdo da *web* em todo o perímetro da rede. Algumas soluções suportam acesso seguro usando SSL e fazendo a varredura de conteúdo, que significa que você pode se proteger e criar conexões seguras para tráfegos como: HTTPS, SFTP, POP3S, e assim por diante. Essencialmente, um filtro de vírus UTM examina todos os arquivos de um banco de dados de assinaturas de vírus conhecidos e a padrões de arquivo utilizados para infectar os computadores. Se nenhuma ameaça é detectada, o arquivo é enviado para o destinatário. Se uma ameaça é detectada, a solução UTM exclui ou coloca em quarentena o arquivo infectado e notifica o usuário.
- Filtragem de conteúdo – a filtragem de conteúdo *web* permite que você controle quais os tipos de conteúdo *web* um usuário pode ter acesso. Usando a filtragem *web*, você pode reduzir significativamente a exposição a ameaças, como *spyware*, *phishing*, *pharming*, *sites* de conteúdo inadequado, redirecionamentos de *site* e outras ameaças que encontramos diariamente na internet. Um dos recursos do filtro de conteúdo *web* é a verificação completa de todo o conteúdo de cada *web*

*site* que é aceito ou não por uma diretiva de *firewall*. Filtros de conteúdo permitem criar uma lista negra de palavras proibidas, frases e endereços *web*, bloqueando, assim, endereços de *site* não autorizados. As categorias de *web sites* são o terceiro método de filtragem de conteúdo *web*, que se baseia em avaliações de URL para permitir ou bloquear por categoria, tais como: conteúdo adulto, *sites* de consumo de banda, rádios, pornografia, drogas, jogos, *sites* que tragam risco à segurança, *sites* de conteúdo pessoal, *sites* de conteúdo corporativo, governamental, entre outras. É possível criar categorias locais com os *sites* da empresa, parceiros e fornecedores.

- *Antispam* – pode bloquear muitas ameaças que chegam por mensagens eletrônicas. Múltiplas tecnologias *antispam* incorporadas em UTM podem detectar ameaças por meio de uma variedade de técnicas, incluindo: bloqueio de IP de *spammers* conhecidos para evitar o recebimento de mensagens indevidas a partir desse remetente. O bloqueio de mensagens em qualquer URL que esteja no corpo da mensagem que possa estar associada com *spam* já conhecidos. Criação de um *hash* da mensagem e, em seguida, comparar esse valor para *hashes* de mensagens de *spam* conhecidos. Aqueles que correspondem a um valor maior podem ter bloqueados sem saber detalhes sobre seu conteúdo. Utilização de listas brancas (lista de liberados) e listas negras (listas de bloqueados) de servidores de *e-mails*, remetentes, domínios de *e-mails*, IP de servidores, entre outros. Realização de DNS *lookup* do nome de domínio ao iniciar uma sessão de SMTP para ver se o domínio existe é válido ou se está na lista negra. Bloqueio de *e-mails* com base em mensagem que tenha relação com conteúdo, palavras-chave ou padrões que caracterizam um *spam*, utilizando uma lista que serviria como filtro de palavras proibidas.
- Acelerador de WAN – os usuários de uma rede corporativa que tem uma grande variedade de filiais esperam que a qualidade e velocidade de acesso estejam presentes em todo o ambiente da rede corporativa. Isso pode ser um problema porque as velocidades de Internet, muitas vezes, não são adequadas para aplicações que consomem muita largura de banda, ou mesmo pela qualidade dos *links* em locais mais distantes, sem falar no custo mais alto de *links* e conexões de alta velocidade. Em tais situações, a otimização e aceleração de WAN desempenha um papel

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

- VPN – essa funcionalidade de VPN é encontrada na maioria dos *firewalls* UTM. Por meio de dispositivos móveis, é possível ter acesso aos dados corporativos da empresa com total segurança. O administrador de rede pode definir quais dados podem ser acessados de fora da empresa, e todo o acesso é documentado e registrado caso haja necessidade de auditoria. São utilizados software*s* para clientes de VPN específicos com autenticação via *Active Directory*.
- IPS – esse sistema detecta e impede invasões de sistemas publicados na rede pública, como servidores *web* com vulnerabilidades não corrigidas, aplicações e seus protocolos, de forma simples de configurar e eficiente para a rede de dados e servidores e está presente na maioria dos firewalls UTM. Um IPS atua como sistema de detecção de intrusos, à procura de padrões de tráfego rede, atividades e processos, registram todos os eventos que possam afetar a segurança. Um IPS emite alarmes ou alertas para os administradores e são capazes de bloquear tráfegos indesejados. Os IPS, também, rotineiramente registram informações. Quando os eventos ocorrem assim, eles podem fornecer informações para análise de ameaças, ou fornecer provas para possíveis ações judiciais. Visto como uma extensão *do firewall*, o IPS possibilita decisões de acesso baseadas no conteúdo da aplicação e não apenas no endereço IP ou em portas, como os *firewalls* tradicionais trabalham.
- DLP – é uma técnica utilizada na área de segurança da informação para se referir a sistemas e metodologias que possibilitam as empresas a reduzir o risco do vazamento de informações confidenciais. Os sistemas DLPs podem identificar a perda de dados por meio da identificação do conteúdo, monitoramento o bloqueio de dados específicos, ou seja, identificar, monitorar e proteger as informações confidenciais que podem estar em uso (máquinas dos usuários), em movimento (na rede corporativa) ou armazenadas (banco de dados, planilhas, servidores etc.).

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

- Relatórios gerenciais – os *firewalls* UTM, em sua maioria, permitem a geração de relatórios de uso de praticamente todos os recursos oferecidos pelo equipamento. Exemplo: relatórios de *sites* acessados por um determinado colaborador, medição de tempos que ele ficou naquele *site*. Relatórios de tentativas de invasões, estações infectadas por vírus entre outros. Os relatórios podem ser gerados em tela, em formato HTML, PDF e até mesmo enviados por *e-mail*.

## 5.4 Principais fabricantes de soluções UTM

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

O modelo de proteção pelas soluções UTM é uma forma de defesa estratégica contra ameaças virtuais, considerada um passo à frente do modelo convencional de *firewalls*, à medida que o UTM carrega maior valor agregado, como funções de prevenção de intrusões de rede, antivírus, rede privada virtual, filtragem de conteúdo, balanceamento de carga e geração de relatórios para o gerenciamento da rede. Entre os principais fabricantes de equipamentos UTM, é possível verificar pelo quadrante de Gartner, mostrado na figura a seguir, para equipamentos UTM de 2021:

Figura 5 – Quadrante de Gartner para *firewall* UTM 2021


Fonte: Gartner, 2021.

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

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

As empresas nesse quadrante lideram o mercado, oferecendo soluções com alto grau de inovação tecnológica que podem ser implementados de forma barata, sem afetar de forma significativa a experiência do usuário final, eliminando a necessidade de novas contratações de pessoal especializado para sua gestão. O histórico da empresa em evitar vulnerabilidades em seus produtos

é considerado nesta análise. Outras características que devem fazer parte dos produtos listados são confiabilidade, rendimento consistente e gestão e administração intuitivas.

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

## FINALIZANDO

Nesta aula, conseguimos entender uma série de elementos importantes empregados na árdua tarefa de ter um ambiente computacional com uma boa segurança da informação. Os servidores proxies que fazem um controle centralizado do acesso à Internet, os filtros de conteúdo que têm o objetivo de manter os colaboradores focados em conteúdos que têm relação com as atividades corporativas, as proteções contra *malwares* que precisam acompanhar todo esse dinamismo do ambiente digital.

Os *firewalls* são a primeira barreira entre a rede interna e a Internet, são verdadeiros muros que precisam estar blindados contra os diversos ataques cibernéticos provenientes da Internet. Soluções integradas podem ser um caminho para ter um ambiente seguro e resiliente.

Uma lição que podemos tirar de tantas mudanças é que precisamos realmente pensar à frente do nosso tempo, investir em soluções não só para suprir as necessidades do momento, mas, sim, investir em soluções que venham agregar valor para o ambiente atual e futuro. Não precisamos ser videntes para saber realmente o que vem pela frente. Ameaças mais sofisticadas, acessos mais intensos e, com tudo isso, precisamos garantir a tão sonhada segurança no ambiente corporativo.

## REFERÊNCIAS


ALVES, D.; PEIXOTO, M.; ROSA, T. **Internet das Coisas (IoT)**: segurança e privacidade de dados pessoais. Rio de Janeiro: Alta Books, 2021.

FRAGA, B. **Técnicas de invasão**: aprenda as técnicas usadas por *hackers* em invasões reais. Compilação de Thompson Vangller. São Paulo: Labrador, 2019.

GALVÃO, M. da C. **Fundamentos em Segurança da Informação**. São Paulo: Pearson Education do Brasil, 2015.

IPLOCATION. **Alocação de Endereços Lógicos de Rede (IP)**. Disponível em: <https://www.iplocation.net/nat>. Acesso em: 18 dez. 2021.

KASPERSKY. **Tecnologia e softwares de segurança**. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/web-filter>. Acesso em: 18 dez. 2021.

MALWAREBYTES. **Segurança Cibernética**. Disponível em: <https://br.malwarebytes.com/antivirus/>. Acesso em: 18 dez. 2021.

SPEEDCHECK. **Ferramenta de checagem de redes**. Disponível em: <https://www.speedcheck.org/pt/wiki/nat/>. Acesso em: 18 dez. 2021.

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