



Aprenda com quem faz

Segurança de Infraestrutura On-Premises

Prof. Maximiliano de Carvalho Jacomo
2022



SUMÁRIO

Capítulo 1. Defesa em Profundidade.....	5
1.1. De onde vêm a defesa em profundidade e como funciona?	7
1.2. Quais são os elementos de defesa em profundidade?	10
Capítulo 2. Arquitetura da Defesa em Profundidade	13
2.1. Camada: Política, procedimentos e conscientização.....	13
2.2. Camada: Segurança física	15
2.3. Camada: Segurança de perímetro	16
2.4. Camada: Segurança rede interna.....	17
2.5. Camada: Segurança de host.....	18
2.6. Camada: Segurança aplicação.....	19
2.7. Camada: Segurança dados.....	19
Capítulo 3. Proteção de Borda: Ferramentas/Sistemas de Proteção	22
3.1. Roteadores e regras ACLs	22
3.2. Firewall	27
3.3. DMZ – Zona Desmilitarizada (Demilitarized Zone).....	40
Capítulo 4. Proteção: Rede Interna (camada rede interna)	44
4.1. Switches Layer 2 e 3 (switches gerenciáveis).....	44
4.2. VLANs – Redes locais virtuais	46
4.3. Redes wireless – Protocolo 802.1x	49
4.4. Servidor proxy e proxy reverso	51
Capítulo 5. Camada: Proteção Hosts (Segurança de Host)	57
5.1. Baselines, bugs, atualizações e correções	58
5.2. Exploit, Antivírus, AntiSpam e Anti-Malware's	64
5.3. RootKits, BackDoors e HIDS	68
5.4. Whitelisting, Blacklist e EndPoint Security	70

Capítulo 6. Tópicos Especiais I – IPS, IDS e VPN	74
6.1. IPS e IDS (Prevenção ou Detecção de Intrusão)	74
6.2. VPN – Virtual Private Network	79
Capítulo 7. Tópicos Especiais II – Monitoramento, Logs e SIEM	84
7.1. SIEM (Centralizadores de Logs)	90
Referências	93



XPe

> Capítulo 1



Capítulo 1. Defesa em Profundidade

A cada dia, novos desafios passam a fazer parte do cotidiano do ambiente corporativo, principalmente os relacionados à segurança dos dados, informações, recursos computacionais e de suas infraestruturas telecomunicações.

Neste contexto, as equipes de segurança da informação precisam se adaptar rapidamente aos novos requisitos necessários para os negócios e, ao mesmo tempo, estar preparadas para lidar com um ambiente que se torna cada vez mais hostil. Ou seja, os profissionais da área da segurança da informação e segurança cibernética, precisam aprender a trabalhar com as últimas tendências de tecnologia para conseguir projetar, dimensionar e implementar estratégias e mecanismos de segurança da informação e segurança cibernética que sejam eficientes e eficazes há diversos riscos e ameaças que possam causar qualquer tipo de dano a tecnologia da informação e a todo o sistema corporativo. Porém, definir e manter a proteção de toda a tecnologia da informação de um ambiente corporativo, por menor que seja esse ambiente, não é uma tarefa fácil para as equipes de segurança da informação. Isto porque, envolve processos, tecnologias e pessoas.

Garantir a segurança da informação dentro de um ambiente corporativo, significa proteger os ativos de TI quanto a perda que qualquer um dos princípios básicos relacionados à segurança da informação, que são: confidencialidade, integridade, disponibilidade, autenticidade. Sendo assim, a segurança da informação não é uma única tecnologia fechada, mas sim um conjunto de ferramentas, estratégias e políticas de segurança que visam proteger a empresa de vários problemas, dos quais podemos destacar:

- Proteção e prevenção contra-ataques virtuais aos sistemas corporativos;

- Prevenção e detecção de vulnerabilidades na área de TI da empresa;
- Proteção dos dados e informações alocados em sistemas de informações;
- Proteção e prevenção de acessos físicos e lógicos de pessoas não autorizadas aos dados, informações e sistemas corporativos etc.

Dentre as diversas estratégias que podem ser adotadas para garantir a proteção dos ativos de TI dentro de um ambiente corporativo, a *Defense in Depth (DiD)* ou *Defesa em Profundidade*, torna-se uma das mais eficientes e eficazes contra diversos tipos de ameaças internas e externas que, ou seja contra diversos riscos associados a TI.

A Defesa em Profundidade é uma estratégia de segurança da informação e da segurança cibernética que se baseia na aplicação de uma série de medidas defensivas redundantes em camadas que tem como objetivo implementar políticas, controles, mecanismos e ferramentas tecnológicas redundantes disposta em camadas. Essa abordagem em várias camadas conhecida como “*segurança em camadas*” aumenta a segurança de uma infraestrutura de TI como um todo e aborda muitos vetores de ataque diferentes, tendo como princípio o conceito que: se um mecanismo de segurança falhar, outro será acionado imediatamente para impedir um ataque.

A Defesa em Profundidade é comumente referida como a “*abordagem do castelo*” porque reflete as defesas em camadas de um castelo medieval. Antes de poder penetrar em um castelo, você se depara com diversos mecanismos de defesa como o fosso e as muralhas em volta do castelo, a ponte levadiça, as torres de vigilância e os soldados arqueiros e assim por diante.

Figura 1 – Camadas de proteção de um castelo medieval.



O mundo digital revolucionou a forma como vivemos, trabalhamos e nos divertimos. No entanto, é um mundo digital constantemente aberto a ataques e, como existem muitos riscos e ameaças em potencial, precisamos garantir que temos a segurança certa para impedir que a infraestrutura de TI seja comprometida.

Infelizmente, não existe um método único que possa proteger com êxito contra todos os tipos de ameaças. É aqui que entra em cena a defesa em profundidade.

1.1. De onde vêm a defesa em profundidade e como funciona?

A defesa em profundidade vem da Agência de Segurança Nacional (NSA). Foi concebido como uma abordagem abrangente para segurança da informação e segurança cibernética. O termo foi inspirado por uma estratégia militar com o mesmo nome. Na prática, a estratégia militar e a estratégia de segurança da informação diferem.

A defesa em profundidade, como estratégia militar, gira em torno de ter uma defesa de perímetro mais fraca e ceder intencionalmente espaço para ganhar tempo para construir um contra-ataque.

Como estratégia de segurança da informação e segurança cibernética, a defesa em profundidade envolve sistemas paralelos de

contramedidas físicas, técnicas e administrativas que trabalham juntas, mas não cedem intencionalmente o controle a um invasor.

A coisa mais importante a entender sobre defesa em profundidade é que um ataque em potencial deve ser interrompido por vários métodos independentes. Isso significa que as soluções de segurança devem abordar vulnerabilidades de segurança durante o ciclo de vida do sistema, e não em um ponto no tempo.

A sofisticação crescente dos ataques cibernéticos significa que as empresas não podem mais confiar em um produto único de segurança para protegê-las. Os profissionais de segurança precisam aplicar a defesa em profundidade em todos os ativos de TI. Desde laptops de funcionários que precisam de proteção contra-ataques do tipo intermediário advindos das redes Wi-Fi até prevenção de sequestro de dados e informações.

Não existe uma única camada de segurança que proteja contra todas as ameaças cibernéticas. Os criminosos virtuais estão se tornando cada vez mais sofisticados em seus ataques e as organizações precisam responder melhorando suas defesas.

Controle de acesso inadequado, *phishing*, falsificação de e-mails, *ransomware*, violação de dados, vazamento de dados, negação de serviços e outros tipos diferentes de ameaças podem ser usados em conjunto para atacar um ambiente organizacional. Neste contexto, as organizações precisam de implementar várias camadas de segurança, cada qual com seus conjuntos de ferramentas de segurança específicas ao tratamento de cada vulnerabilidade e ameaça presente aquela camada.

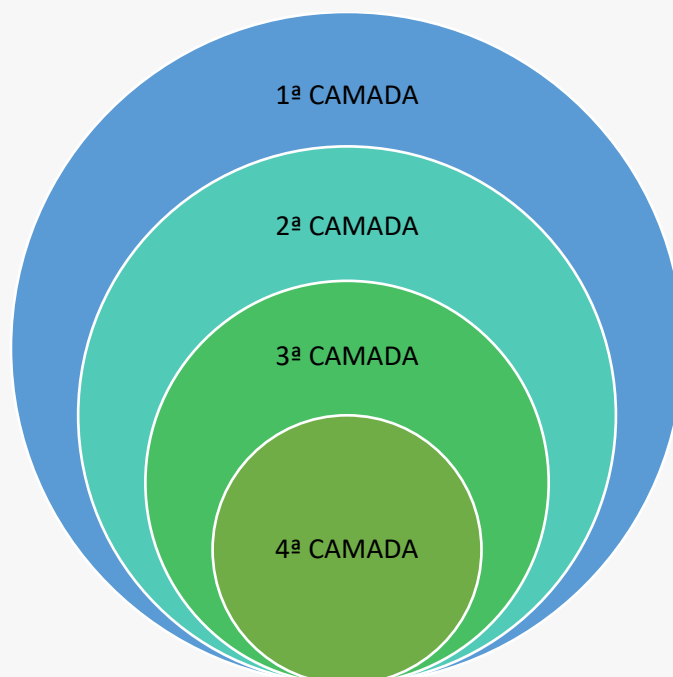
Para compreender melhor o funcionamento da estratégia de defesa em profundidade aplicada a segurança da informação e segurança cibernética, vamos voltar ao exemplo das proteções contidas em um castelo medieval. Um invasor se depara com diversos mecanismos de defesa como

o fosso e as muralhas em volta do castelo, a ponte levadiça, as torres de vigilância e os soldados arqueiros e assim por diante, conforme mencionado anteriormente. Cada um destes mecanismos de defesa estará distribuído em camadas e, cada camada será uma barreira responsável por realizar uma proteção específica para impedir que o invasor conquiste o castelo.

Por exemplo, os primeiros mecanismos de defesa a serem vencidos pelo invasor são os controles de acesso físico como os portões externos antes da ponte levadiça que podem conter soldados que exercem a função de identificar e controlar o primeiro acesso ao castelo. Temos ainda nesta primeira camada de proteção a ponte levadiça e o fosso d'água que são considerados outros mecanismos de segurança que limitam o acesso ao castelo. Caso o invasor consiga superar os mecanismos presentes na camada de segurança física do castelo, ele terá que enfrentar uma próxima camada de proteção, no caso podemos citar as torres externas de vigilância e os soldados arqueiros.

Podemos perceber neste momento que nesta segunda camada de proteção há a presença de outros mecanismos de segurança que possuem um grau de dificuldade maior se comparados aos primeiros mecanismos presentes na primeira camada de proteção. Isto faz com que o invasor tenha uma maior dificuldade em superá-los. Mas, caso ele consiga superar essa segunda camada de proteção, haverá uma terceira camada de proteção, composta por outros mecanismos de segurança com maiores níveis de dificuldade. Este aumento do nível de dificuldade irá se repetir de forma exponencial a cada camada de proteção. Ou seja, a próxima camada de proteção, a quarta camada, possuirá novos mecanismos de proteção superiores a terceira camada e, assim por diante, dificultado e impedindo o acesso do invasor ao tesouro contido dentro do interior do castelo, ou fazendo com que este invasor desista de invadir o castelo.

Figura 2 - Estratégia de camadas (defesa em profundidade).



Quanto mais funda for a camada de proteção, maior será o nível de proteção. Ou seja, maior será o fator dificultador para o invasor.

1.2. Quais são os elementos de defesa em profundidade?

Existem três partes principais de qualquer estratégia de defesa em profundidade, a saber:

1. Controles físicos: medidas de segurança que impedem o acesso físico a sistemas de TI, como guardas de segurança, cartões-chave e portas trancadas.
2. Controles técnicos: medidas de segurança que protegem a segurança da rede e outros recursos de TI usando hardware e software, como sistemas de proteção contra intrusões, firewalls de aplicativos da web, gerenciamento de configurações, proxy, scanners da web, gestão de identidades e acessos, antivírus e anti-malwares, sistemas de prevenção de perda de dados, sistemas de autenticação de dois fatores, biometria, gerenciadores de senhas,

redes privadas virtuais, criptografia de dados, sistemas de backups etc.

3. Controles administrativos: medidas de segurança que consistem em políticas e procedimentos direcionados aos funcionários de uma organização e seus fornecedores e parceiros comerciais. Os exemplos incluem: políticas de segurança da informação, políticas de segurança cibernética, políticas de privacidade e proteção de dados, gerenciamento de riscos de colaboradores terceiros, parceiros comerciais e fornecedores, estruturas de gerenciamento de riscos de terceiros, avaliações de riscos de segurança da informação e segurança cibernética, políticas de treinamento e conscientização, adoção de metodologias para promover a melhoria contínua e garantir as melhores práticas etc.

Juntos, os controles físicos, técnicos e administrativos constituem uma estratégia básica de defesa em profundidade. Além disso, muitos profissionais e equipes de segurança usam ferramentas de segurança que monitoram continuamente toda a infraestrutura de TI quanto a possíveis falhas em suas defesas de segurança.

Figura 3 – Elementos principais da defesa em profundidade.





XPe

> Capítulo 2

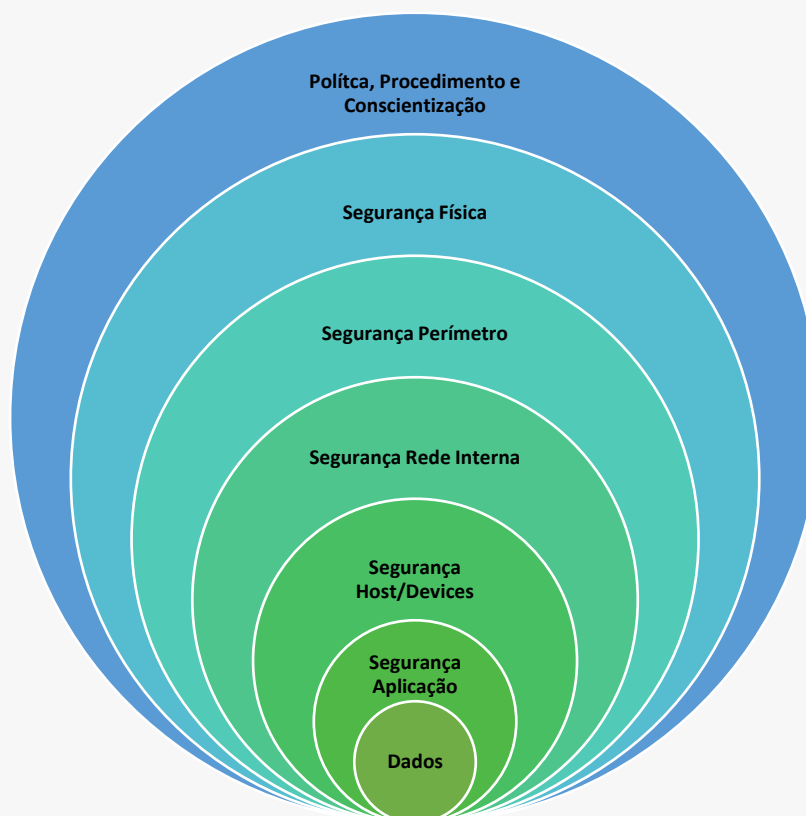


Capítulo 2. Arquitetura da Defesa em Profundidade

Conforme observamos no capítulo anterior, segurança de defesa em profundidade é baseada em camadas de proteção. Em cada camada, haverá um conjunto de controles, mecanismos e ferramentas tecnológicas de segurança projetados para proteger os aspectos físicos, técnicos e administrativos de uma infraestrutura de TI.

No geral, uma arquitetura de defesa em profundidade é composta por sete camadas de proteção.

Figura 4 – Arquitetura da defesa em profundidade.



2.1. Camada: Política, procedimentos e conscientização

Trata-se da camada responsável por implementar as políticas e os procedimentos que irão governar as práticas de segurança da informação e

segurança cibernética de uma empresa, bem como as ações de conscientização, treinamento e educação dessas práticas em geral que deverão ser seguidas e desempenhadas por todos os funcionários, fornecedores e parceiros comerciais da empresa.

Seja qual for a ação, controle, mecanismo ou ferramenta tecnológica que uma empresa adote em sua infraestrutura de TI e em seu ambiente corporativo, estes precisam de normas, políticas e procedimentos que irão garantir que todas as medidas de segurança estão sendo realizadas da forma correta ao longo do tempo por todos os funcionários, fornecedores e parceiros comerciais.

As políticas e procedimentos, precisam ser divulgados, seguidos e principalmente compreendidos pelos funcionários, fornecedores e parceiros comerciais e para tal é preciso que a alta administração da empresa em conjunto com a área de segurança e, por meio dos seus processos de governança corporativa, governança da tecnologia da informação e da gestão de segurança da informação, implemente programas de conscientização, treinamento e educação junto a todos os colaboradores internos e externos ligados a empresa.

Existem vários motivos para a criação e implementação de políticas e procedimentos voltados à segurança da informação e segurança cibernética, dentre os quais destacamos: estabelecer os requisitos necessários para impedir ou minimizar o acesso não autorizado acidental ou intencional aos ativos de TI – dados, informações, sistemas, dispositivos etc.; fornece diretrizes consistentes para as melhores práticas de segurança da informação e segurança cibernética; comunicar a importância da segurança da informação e segurança cibernética a todos os colaboradores; satisfazer aos requisitos legais inerentes ao modelo de negócio realizado pela empresa, tais como: normas e regulamentações de órgãos reguladores de mercado, leis e legislações impostas por órgãos municipais, estaduais e

federais, normas e regulamentações internas e de compliance, dentre outros.

Uma vez que as políticas e procedimentos estejam claramente definidos e divulgados, os programas de conscientização, treinamento e educação devidamente disseminados junto a todos os setores e colaboradores internos e externos à empresa, faz-se necessário a implementação de medidas de monitoramento das atividades realizadas por todos os membros que compõe o ambiente organizacional, para verificar se tais atividades estão de acordo com as políticas e procedimentos de segurança criados e vice-versa.

É importante que sejam definidos pela governança corporativa ou pela alta administração da empresa as ações e medidas disciplinares a serem aplicadas aos colaboradores que descumprirem as políticas e procedimentos de segurança da informação e segurança cibernética. Vale aqui ressaltar que os juristas costumam dizer que a lei é inócua se não houver uma punição definida para seu descumprimento.

2.2. Camada: Segurança física

Considerada a primeira barreira de proteção de uma infraestrutura de TI, a camada de segurança física tem como objetivo garantir que as ameaças não tenham acesso físico aos ativos tangíveis, como pessoas, servidores, desktops, dispositivos de rede – switches, roteadores, racks de telecomunicação, racks de redes – path panels, painéis de controle elétricos, painéis de controle de climatização, dispositivos de armazenamento de dados e outros recursos valiosos.

A ausência de controles e mecanismos de proteção física e redundante que impeçam as ameaças de acessarem fisicamente uma infraestrutura de TI e/ou o ambiente interno corporativo da empresa, bem como outros que impeçam que uma infraestrutura de TI se torne indisponível ou perca a sua integridade, pode afetar a sua confiabilidade e

causar danos financeiros e de imagem perante a seus produtos e serviços junto aos clientes e consumidores.

A ideia principal desta camada é a de criar um perímetro de segurança física no qual busca-se estabelecer níveis de segurança física na infraestrutura de TI e em todo ambiente da empresa de forma segmentada. No geral, o perímetro de segurança física é composto por mecanismos de proteção e segurança tais como: muros, cercas e pontos de controle de acesso físico nas partes mais externas da empresa; sistemas de alarme, sensores de movimento, circuitos fechados de TVs, fechaduras eletrônicas, cartões de acesso, dispositivos de segurança biométrica, dentre outros nas partes internas da empresa.

2.3. Camada: Segurança de perímetro

A camada segurança de perímetro, tem como objetivo implementar a proteção necessária entre o mundo exterior e a infraestrutura de TI interna do ambiente corporativo. Ou seja, o perímetro é a fronteira da rede onde os dados fluem de e para outra rede, incluindo a internet. Portanto é essencial fortalecer as defesas ao longo da borda da rede para promover uma proteção mais abrangente. A defesa de perímetro permite a entrada de dados autorizados, bloqueando o tráfego suspeito e é composta por vários mecanismos e ferramentas tecnológicas diferentes.

É importante que as empresas criem um ponto de estrangulamento, ou seja, um funil ou ponto único, por onde todos os dados entrem e saiam de suas redes. Este caminho único tem como principal objetivo analisar em profundidade todos os dados que trafegam nesta única via, evitando que algum tipo de ameaça perpassasse para dentro da rede ou que algum dado ou informação vaze para fora, ou seja, para o ambiente externo.

Nesta camada encontramos como mecanismos e ferramentas de proteção, dispositivos de borda tais como: roteadores, switches layer 3, appliances de firewall, sistemas de IDS e IPS para detecção e prevenção de

intrusos, sistemas DLPs que previnem a perda de dados. Além de esquemas como DMZ – zonas desmilitarizadas de rede, sistemas de proxy e conversão de endereços de rede (NAT), VPN – redes virtuais privadas, dentre outras tecnologias de proteção.

É importante ressaltar que alguns desses mesmos dispositivos de proteção podem também estar presentes dentro da rede interna da empresa, realizando a proteção entre as redes e os ativos internos de TI da empresa.

2.4. Camada: Segurança rede interna

“Não pense nos oponentes que não estão atacando; se preocupe com sua própria falta de preparação”. Esta frase retirada do livro “Os Cinco Anéis” de Miyamoto Musashi ilustra bem, devemos considerar que não existem apenas ameaças externas. Ou seja, ameaças que vêm somente do lado de fora do ambiente corporativo. Mas, também podem existir ameaças internas, que vêm de dentro do próprio ambiente de rede corporativo.

A camada de segurança rede interna da estratégia de defesa em profundidade, deve possuir mecanismos e ferramentas de proteção capazes de lidar com a identidade e autenticação dos usuários da rede, autorizando ou não, o acesso destes usuários aos recursos computacionais e de redes disponíveis na infraestrutura de TI, protegendo os dados e informações que fluem pela rede, além de outros mecanismos e ferramentas que exerçam funções relacionadas a filtros que permitam analisar de forma consistente todos os pacotes de dados que circulam na rede e outros que também são utilizados na camada de segurança de perímetro como por exemplo, dispositivos de firewall internos, IPS e IDS, proxy que realizam a conversão de endereços (NAT), além de outras tecnologias como, sistemas que realizam autenticação de usuários e dispositivos baseados na no protocolo IEEE 802.1x; sistemas que implementam o protocolos IPSec (conjunto de protocolos que tem como objetivo proteger a comunicação IP, autenticando

e criptografando cada pacote IP de uma sessão de comunicação, NAC – protocolo que permite a restrição de disponibilidade de recursos de rede, VLANs – protocolos que permitem as equipes de segurança da informação realiza a segmentação de redes internas, dentre outros.

É importante ressaltar que, além dos mecanismos e ferramentas citada anteriormente, esta camada tem como missão realizar o levantamento, avaliação e o gerenciamento de vulnerabilidades presentes em um ambiente de infraestrutura de TI, permitindo as equipes de segurança da informação e segurança cibernética descobrir possíveis vetores de ataque e falhas de sistemas/aplicações que possam ser exploradas por ameaças e comprometer um ou todos os princípios relacionados à segurança da informação – disponibilidade, integridade, confidencialidade e autenticidade. Lembre-se, da mesma forma que as equipes de segurança da informação, realizam atualizações nos seus sistemas computacionais, tais como: os sistemas operacionais e sistemas aplicativos, é necessário que seja executado também as mesmas tarefas de atualização junto aos ativos de rede, tais como: roteadores, switches etc., para garantir a proteção deste, contra a exploração de vulnerabilidades que, porventura, podem estar presentes nestes dispositivos.

2.5. Camada: Segurança de host

A camada de segurança de host, concentra-se em manter a proteção dos hosts e respectivamente dos sistemas operacionais que controlam estes hosts. Para aqueles que não sabem a definição de host, podemos dizer que um “host” é qualquer dispositivo computacional – computador, servidor, impressora, ou outro qualquer que possua receber um endereçamento IP exclusivo, que realiza a interligação tais dispositivos entre si e a internet.

Prover mecanismos e ferramentas de proteção nessa camada, é uma tarefa especialmente desafiadora, pois esses dispositivos são projetados

para realizar multitarefas e interagir com vários outros dispositivos, aplicativos, protocolos e serviços simultaneamente.

Dentre os mecanismos e ferramentas tecnológicas que podem ser implementadas nessa camada, destacam-se: sistemas de firewall desenvolvidas para computadores pessoais; sistemas de detecção e prevenção de intrusão baseados em host (HIPS ou HIDS); sistemas de gestão ou gerenciamento de identidades e acessos; sistemas de detecção de vírus, malwares, Spyware e outras ameaças virtuais; sistemas de gerenciamento de patches e atualizações de segurança, sistemas de registro e auditoria de logs etc.

2.6. Camada: Segurança aplicação

A camada de segurança aplicação do modelo de defesa em profundidade tem como objetivo manter os aplicativos, os sistemas de informação e demais outras aplicações mais seguras e protegidas contra diversas ameaças. Vale lembrar que, os aplicativos são os softwares ou sistemas de informação, tais como: CRM, ERP, BI etc., que manipulam os dados e as informações, que é o objetivo final de qualquer ameaça.

Um aplicativo ou sistema de informação mal protegido dentro de um ambiente corporativo, podem fornecer para as ameaças o acesso e controle de forma fácil, há seus dados e informações.

Nesta camada, encontramos diversos mecanismos e ferramentas de proteção, tais como: gateway de aplicação (Proxy); sistemas de identificação e acesso a aplicativos; sistemas de filtragem de conteúdo, ACLs (regras) de liberação de acesso; entre outros.

2.7. Camada: Segurança dados

Trata-se da camada de segurança mais profunda da estratégia de defesa em profundidade e tem como principal objetivo proteger um dos ativos de TI mais valiosos que a empresa possui, os “dados”.

Atualmente, os dados são considerados o novo “petróleo” do mundo digital. Isto porque os dados são fonte essenciais para a formação de informações que permitem as empresas conhecer seus clientes e concorrentes, realizar o planejamento estratégico, conquistar novos mercados, criar produtos e serviços e, principalmente, garantir a sua sobrevivência em um mercado cada vez mais competitivo. Assim sendo, os dados são considerados o objetivo final de quase todas as medidas de segurança de TI e, alvo principal de vários tipos de ameaças e criminosos cibernéticos.

As estratégias de proteção nessa camada devem se concentrar nos dados armazenados, incluindo os dispositivos de armazenamento e nos dados em trânsito. Como exemplo de mecanismos e ferramentas de proteção que devem ser implementados nessa camada, podemos citar a criptografia, o controle de acesso e autenticação, os sistemas de prevenção de perda e vazamento de dados (DLPs), as ferramentas de backup e restore, entre outros.



XPe

> Capítulo 3



Capítulo 3. Proteção de Borda: Ferramentas/Sistemas de Proteção

Conforme observamos no capítulo anterior, a camada segurança de perímetro ou em alguns casos denominada proteção de borda, deve garantir a proteção necessária entre o mundo exterior e a infraestrutura de TI interna do ambiente corporativo. Essa proteção é realizada através da implementação de mecanismos e ferramentas tecnológicas que realizam o monitoramento e controle de todo o tráfego da rede. Ou seja, o monitoramento e controle do que entre e sai da empresa por meio das conexões existentes entre a rede pública “WAN” e a rede local privada “LAN”.

Denominados de “borda” a área mais externa da rede, onde, como mencionado anteriormente, é realizada a interligação das redes WAN e LAN. Os dispositivos utilizados para criar as barreiras de proteção são denominados de “dispositivos de borda”, nos quais destacamos: os roteadores e switches de bordas, os sistemas/appliance de firewall de borda, as zonas desmilitarizadas (DMZ), dentre outros.

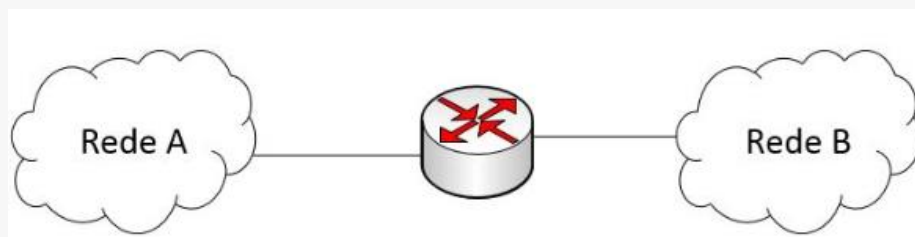
A seguir iremos estudar alguns dos dispositivos de bordas comumente mais utilizados na proteção de borda e na estratégia de defesa em profundidade.

3.1. Roteadores e regras ACLs

Um roteador (router, em inglês) é um equipamento de rede que efetua o encaminhamento de pacotes de dados entre redes de computadores distintas. Esses pacotes de dados são encaminhados de um roteador para outro até que atinjam o dispositivo de destino, ou sejam descartados. Os roteadores efetuem a leitura dos pacotes IP, podendo analisar o conteúdo de seus cabeçalhos, e então tomar decisões baseando-se nos lados lidos e os protocolos de transmissão implementados em suas configurações.

Os roteadores são conectados em redes distintas, efetuando a conexão entre essas redes, em contraste com um Switch, que efetua a conexão de dispositivos finais, como computadores e notebooks, dentro de uma mesma rede.

Figura 5 - Roteador como elemento central interligando duas redes distintas.

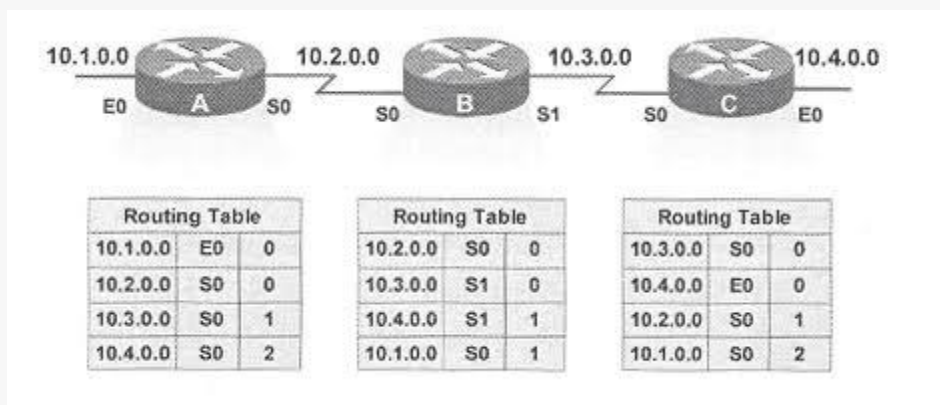


Os roteadores mantêm domínios de broadcast separados para cada rede que conectam, desta forma isolando-as. Assim, dados direcionados à rede local por um host qualquer permanecem nesta rede local, não sendo encaminhados para as outras redes que estejam conectadas ao roteador.

Por exemplo, no diagrama acima, se um host na rede A enviar um pacote a outro host na mesma rede A, o roteador não encaminhará o pacote para a rede B; o pacote permanece no domínio de broadcast a que pertence. Agora, se um host na rede A enviar um pacote para um host localizado na rede B, o router irá encaminhar o pacote de uma rede para outra, efetuando assim seu roteamento.

Os roteadores dependem de uma tabela de roteamento para identificar para onde um pacote de dados deve ser encaminhado. As tabelas de roteamento contêm informações sobre o destino, próximo salto, interface, métricas e rotas, que podem ser usadas para guiar o pacote de dados através das linhas de comunicação e em direção ao seu destino.

Figura 6 - Exemplo tabela roteamento.



Existem dois métodos pelos quais as tabelas de roteamento são atualizadas e mantidas em ordem. Isto pode ser feito de forma dinâmica ou estática. O método estático envolve a atualização manual das tabelas de roteamento. Por outro lado, os roteadores dinâmicos trocam automaticamente informações com dispositivos através de diferentes protocolos de roteamento. Com base nessas informações, as tabelas de roteamento são automaticamente atualizadas.

Todos os roteadores executam a função básica de receber e enviar dados entre a Internet e os dispositivos locais conectados a uma rede. No entanto, existem diferentes tipos de roteadores que existem com base em como eles se conectam aos dispositivos ou como funcionam dentro de uma rede. Especificamente, os tipos de roteadores comumente disponíveis incluem:

- Brouter – Um roteador B também é conhecido como roteador de ponte. Ele é um dispositivo de rede que executa tanto como uma ponte quanto como um roteador. Tanto uma ponte quanto um roteador conectam redes, entretanto, a ponte de rede envolve conectar 2 redes separadas para permitir que elas funcionem como uma única rede coesa. Considerando que um roteador fornece uma conexão que ainda mantém ambas as redes como redes privadas individuais;

- Core Router – Um roteador core estabelece uma conexão de rede e facilita a transmissão de dados dentro da rede privada. Os roteadores core funcionam dentro do núcleo ou dentro da rede e não podem enviar ou receber dados fora dela. A distribuição de dados está limitada à rede, uma vez que este tipo de encaminhador é incapaz de realizar o intercâmbio de informações com outros sistemas;
- Roteador de borda – Um roteador de borda é responsável pelas transferências de dados de condução entre várias redes. Ao contrário do roteador core, o roteador edge não facilita o intercâmbio de pacotes de dados dentro de uma rede privada, mas, em vez disso, gerencia a transmissão de dados para outros sistemas de rede separados;
- Roteador virtual – Geralmente, um roteador virtual consiste em um software que permite que um dispositivo funcione como um roteador físico padrão. É capaz de funcionar com o uso de um Protocolo de Redundância de Roteador Virtual (VRRP).
- Roteador sem fio – Um roteador sem fio ainda mantém uma conexão com fio com o modem onde recebe sinais de dados da internet. No entanto, não há necessidade de uma conexão com fio do roteador para os dispositivos que estão conectados à rede. Um roteador sem fio usa antenas que enviam ondas de rádio ou infravermelho que carregam os pacotes de dados. O exemplo mais comum de um roteador sem fio são os roteadores [wi-fi](#) de casa que são largamente usados em escritórios e casas residenciais.

Figura 7 - Esquema de interligação de roteadores de borda.



ACL – Access Control List ou Lista de Controle de Acessos, trata-se de uma lista sequencial de instruções de permissão ou negação que se aplicam a endereços ou protocolos de camada superior, fornecendo uma forma eficiente de controlar o tráfego dentro e fora de uma rede. No geral, as ACLs podem ser configuradas em todos os tipos de roteadores e, são principalmente encontradas nos roteadores de bordas.

A razão mais importante para configurar as ACLs é fornecer segurança para a rede. Porém, podemos ainda utilizar ACLs para outras finalidades em conjunto com a proteção, como por exemplo, a validação do tráfego de pacotes entre as redes LAN e a rede WAN ou a qualidade do serviço (QoS).

Uma das maneiras mais fáceis de se configurar ACLs em um roteador é memorizar o conceito dos três “Ps”, no qual uma ACL pode ser configura:

- 1.º P - Por Protocolo – no qual a ACL é utilizada para controlar o fluxo de tráfego em uma interface do roteador, devendo ser definida para cada um dos protocolos habilitados na interface;
- 2.º P – Por interface – no qual a ACL é utilizada para controlar o fluxo de tráfego de uma interface do roteador;

3.º P – Por direção – no qual a ACL é utilizada para controlar o fluxo de tráfego em uma direção por vez em uma interface. Neste caso deverá ser criada duas ACLs separadas para controlar o fluxo de entrada e saída dos dados.

Lembre-se de que uma ACL é uma lista sequencial de instruções de permissão ou negação que se aplicam a endereços IP ou protocolos de camada superior. A ACL pode extrair informações contidas no cabeçalho do pacote de dados e, testá-lo em relação às suas regras, tomando a decisão de “permitir” ou “negar” com base no endereço IP/Porta de origem TCP/UDP, no endereço IP/Porta de destino TCP/UDP ou tipo de mensagem ICMP.

Figura 8 - Exemplo de um conjunto da ACLs.

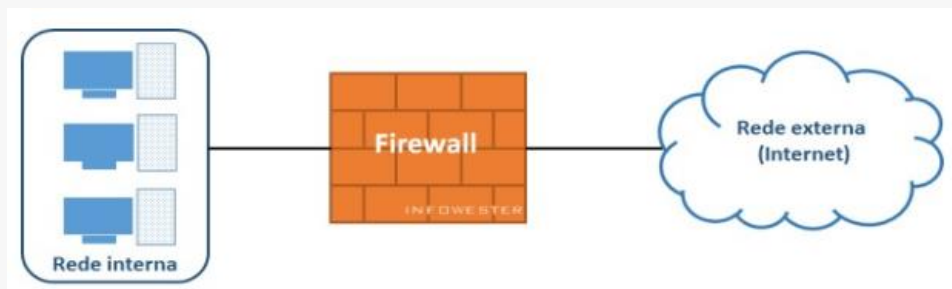
Regra	Ação	Ip de Origem	Ip de Destino	Protocolo	Porta de Origem	Porta de Destino
1	Permite	192.168.10.20	194.154.192.3	tcp	Qualquer Porta	25
2	Permite	Qualquer da rede any	192.168.10.3	tcp	Qualquer Porta	80
3	Permite	192.168.10.0/24	Qualquer da rede any	tcp	Qualquer Porta	80
4	Nega	Qualquer da rede any	Qualquer da rede any	Qualquer Protocolo	Qualquer Porta	Qualquer Porta

Por fim, podemos ainda configurar um conjunto de ACLs em outros dispositivos de segurança, tais como: Switches layer 3 e 2, Firewall e Gateways de Comunicação.

3.2. Firewall

O firewall é uma solução de segurança baseada em hardware e software que, a partir de um conjunto de regras ou instruções (ACLs), analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas. “Parede de Fogo”, a tradução literal do nome, já deixa claro que o firewall se enquadra em uma espécie de barreira de defesa. Seu objetivo assim por dizer, consiste basicamente em bloquear tráfego de dados indesejados e liberar acessos bem-vindos.

Figura 9 - Representação básica de um firewall.



Para que você possa compreender melhor o funcionamento de um firewall, imagine-o como sendo uma portaria de um prédio: para que você tenha acesso as salas ou apartamentos do prédio, é preciso obedecer a determinadas condições “regras”, como se identificar, ser esperado por um morador do prédio e não portar qualquer tipo de objeto que possa trazer risco à segurança; para sair, não se pode levar nada que pertence aos moradores ou ao prédio sem a devida autorização.

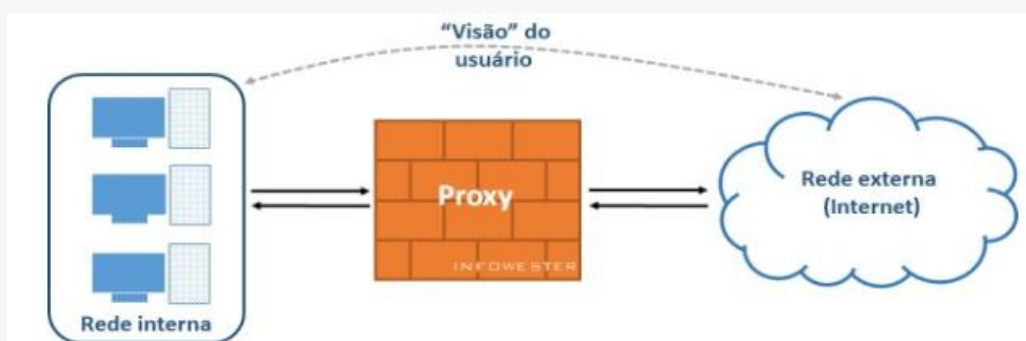
Neste contexto, um firewall pode impedir uma série de ações maliciosas: um malware que utiliza uma determinada porta para se instalar em um host da rede, sem o usuário saber, um aplicativo que envia dados sigilosos para a internet, uma tentativa de acesso à rede a partir de hosts externos não autorizados, entre outros.

O trabalho de um firewall pode ser realizado de várias formas. O que define uma metodologia ou outra são fatores como critérios do desenvolvedor, necessidades específicas do que será protegido, características do sistema operacional que o mantém, estrutura da rede e assim por diante. É por isso que podemos encontrar mais de um tipo de firewall. A seguir, iremos apresentar os mais conhecidos e utilizados.

Figura 10 - Firewall do tipo: Filtragem de pacotes.



Figura 11 - Firewall do tipo: Aplicação ou proxy de serviço.



3.2.1. Arquiteturas do firewall

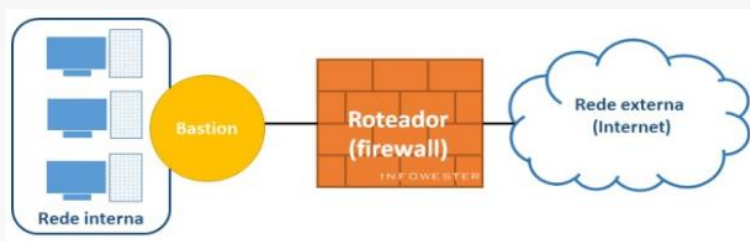
Percebe-se que, a julgar pela variedade de tipos, os firewalls podem ser implementados de várias formas para atender às mais diversas necessidades. Este aspecto leva a outra característica importante do assunto: a arquitetura de um firewall.

Quando falamos de arquitetura, nos referimos à forma como o firewall é projetado e implementado. Há, basicamente, três tipos de arquitetura. Veremos elas a seguir.

- **Arquitetura Dual-Homed Host** – nesta arquitetura, o firewall fica disposto entre a rede LAN e a rede WAN. O nome da arquitetura se deve ao fato de este firewall possuir ao menos duas interfaces de rede, uma para cada “lado”. Perceba que não há outro caminho de comunicação, portanto, todo o tráfego passa por este firewall, não havendo acesso da rede interna para a rede externa (e vice-versa) diretamente. A principal vantagem desta abordagem é que há

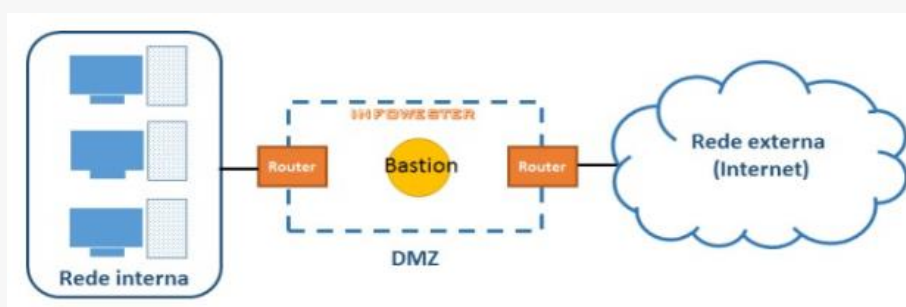
grande controle do tráfego. A desvantagem mais expressiva, por sua vez, é que qualquer problema com o dual-homed – uma invasão, por exemplo – pode pôr em risco a segurança da rede ou mesmo paralisar o tráfego. Por esta razão, o seu uso pode não ser adequado em redes cujo acesso à internet é essencial. Este tipo de arquitetura é bastante utilizado para firewalls do tipo proxy.

- **Arquitetura Screened Host** – na arquitetura Screened Host, em vez de haver um único firewall servindo de intermediador entre a rede LAN e a rede WAN, há duas: uma que faz o papel de roteador (*screening router*) e outra chamada de *bastion host*. O bastion host atua entre o roteador e a rede LAN, não permitindo comunicação direta entre ambos os lados. Perceba então que se trata de uma camada extra de segurança: a comunicação ocorre no sentido *rede interna – bastion host – screening router – rede externa* e vice-versa. O roteador normalmente trabalha efetuando filtragem de pacotes, sendo os filtros configurados para redirecionar o tráfego ao bastion host. Este, por sua vez, pode decidir se determinadas conexões devem ser permitidas ou não, mesmo que tenham passado pelos filtros do roteador. Sendo o ponto crítico da estrutura, o bastion host precisa ser bem protegido, do contrário, colocará em risco a segurança da rede interna ou ainda poderá torná-la inacessível.



- **Arquitetura Screened Subnet** – este tipo de arquitetura, também conta com a figura do bastion host, mas este fica dentro de uma área isolada de nome interessante: a *DMZ*, sigla para *Demilitarized Zone* – Zona Desmilitarizada. A DMZ, por sua vez, fica entre a rede

interna e a rede externa. Acontece que, entre a rede LAN e a DMZ há um roteador que normalmente trabalha com filtros de pacotes. Além disso, entre a DMZ e a rede WAN, há outro roteador do tipo. Note que esta arquitetura se mostra bastante segura, uma vez que, caso o invasor/ameaça passe no primeiro roteador, terá ainda que lidar com a zona desmilitarizada. Esta inclusive pode ser configurada de diversas formas, com a implementação de proxies ou com a adição de mais bastion hosts para lidar com requisições específicas, por exemplo. O nível segurança e a flexibilidade de configuração fazem da Screened Subnet uma arquitetura normalmente mais complexa e, conseqüentemente, mais cara.



3.2.2. Filtragem de pacotes (packet filtering)

As primeiras soluções de firewall surgiram na década de 1980 baseando-se em filtragem de pacotes de dados (*packet filtering*), uma metodologia mais simples e, por isso, mais limitada, embora ofereça um nível de proteção significativo.

Para compreender, é importante saber que cada pacote de dados transmitido ou recebido na rede, possui um cabeçalho com diversas informações a seu respeito, como endereço IP de origem, endereço IP do destino, tipo de serviço, tamanho, entre outros. O firewall então analisa estas informações de acordo com as regras estabelecidas para liberar ou não o pacote (seja para sair ou para entrar na máquina/rede), podendo também executar alguma tarefa relacionada, como registrar o acesso (ou tentativa de) em um arquivo de log.

A transmissão dos dados é feita com base no padrão TCP/IP (*Transmission Control Protocol/Internet Protocol*), que é organizado em camadas. A filtragem normalmente se limita às camadas de rede e de transporte: a primeira é onde ocorre o endereçamento dos equipamentos que fazem parte da rede e processos de roteamento, por exemplo; a segunda é onde estão os protocolos que permitem o tráfego de dados, como o TCP e o UDP.

Com base nisso, um firewall de filtragem pode ter, por exemplo, uma regra que permita todo o tráfego da rede local que utilize a porta UDP 123, assim como ter uma política que bloqueia qualquer acesso da rede local por meio da porta TCP 25.

Podemos encontrar dois tipos de firewall de filtragem de pacotes. O primeiro utiliza o que é conhecido como *filtros estáticos*, enquanto o segundo é um pouco mais evoluído, utilizando *filtros dinâmicos*.

Na filtragem estática, os dados são bloqueados ou liberados meramente com base nas regras, não importando a ligação que cada pacote tem com outro. A princípio, esta abordagem não é um problema, mas determinados serviços ou aplicativos podem depender de respostas ou requisições específicas para iniciar e manter a transmissão. É possível então que os filtros contenham regras que permitem o tráfego destes serviços, mas ao mesmo tempo bloqueiem as respostas/requisições necessárias, impedindo a execução da tarefa. Esta situação é capaz de ocasionar um sério enfraquecimento da segurança, uma vez que um administrador poderia se ver obrigado a criar regras menos rígidas para evitar que os serviços sejam impedidos de trabalhar, aumentando os riscos de o firewall não filtrar pacotes que deveriam ser, de fato, bloqueados.

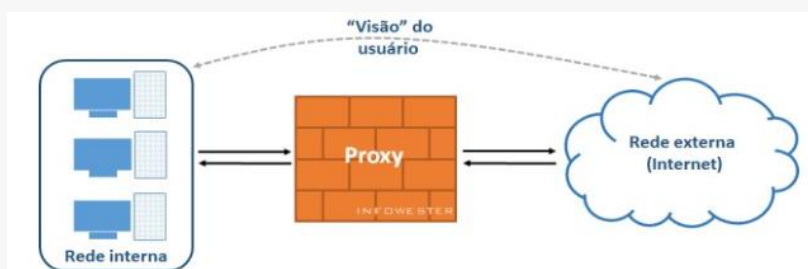
A filtragem dinâmica surgiu para superar as limitações dos filtros estáticos. Nesta categoria, os filtros consideram o contexto em que os pacotes estão inseridos para “criar” regras que se adaptam ao cenário,

permitindo que determinados pacotes trafeguem, mas somente quando necessário e durante o período correspondente. Desta forma, as chances de respostas de serviços serem barradas, por exemplo, cai consideravelmente.

3.2.3. Firewall de aplicação ou proxy de serviço (proxy services)

O firewall de aplicação, também conhecido como “proxy de serviços” ou apenas “proxy” é uma solução de proteção que atua como um ponto intermediário entre um host ou uma rede interna e outra rede, externa, no geral a internet. No geral, trata-se de um dispositivo “appliance” que possui um hardware com poder de processamento e memória superior, devido ao tratamento que deve ser realizado ao lidar com muitas requisições.

Firewall deste tipo são opções interessantes de segurança porque não permitem a comunicação direta entre origem e destino. Para entender melhor observe a figura a seguir. Perceba que em vez de a rede LAN (interna) se comunicar diretamente com a rede WAN (externa), há um dispositivo (proxy) entre ambas as redes, criando duas conexões – a primeira entre a LAN e o Proxy e, a segunda entre o Proxy e a WAN.



Perceba que todo o fluxo de dados necessita passar pelo proxy. Desta forma, é possível, por exemplo, estabelecer ACLs (regras) que impeçam o acesso de determinados endereços externos, assim como que proíbam a comunicação entre hosts internos e determinados serviços remotos. Este controle amplo também possibilita o uso do proxy para tarefas complementares: o equipamento pode registrar o tráfego de dados em um arquivo de log; conteúdo muito utilizado pode ser guardado em uma espécie de cache (uma página web muito acessada fica guardada temporariamente

no proxy, fazendo com que não seja necessário requisitá-la no endereço original a todo instante, por exemplo); determinados recursos podem ser liberados apenas mediante autenticação do usuário; entre outros.

A implementação de um proxy não é tarefa fácil, haja visto a enorme quantidade de serviços e protocolos existentes na internet, fazendo com que, dependendo das circunstâncias, este tipo de firewall não consiga ou exija muito trabalho de configuração para bloquear ou autorizar determinados acessos.

3.2.4. Proxy transparente

No que diz respeito a limitações, é conveniente mencionar uma solução denominada “proxy transparente”. O proxy “tradicional”, não raramente, exige que determinadas configurações sejam feitas nas ferramentas que utilizam a rede (por exemplo, um navegador de internet) para que a comunicação aconteça sem erros. O problema é, dependendo da aplicação, este trabalho de ajuste pode ser inviável ou custoso.

O proxy transparente surge como uma alternativa para estes casos porque as máquinas que fazem parte da rede não precisam saber de sua existência, dispensando qualquer configuração específica. Todo acesso é feito normalmente do cliente para a rede externa e vice-versa, mas o proxy transparente consegue interceptá-lo e responder adequadamente, como se a comunicação, de fato, fosse direta. É válido ressaltar que o proxy transparente também tem lá suas desvantagens, por exemplo: um proxy “normal” é capaz de barrar uma atividade maliciosa, como um malware enviando dados de um host para a internet; o proxy transparente, por sua vez, pode não bloquear este tráfego. Não é difícil entender: para conseguir se comunicar externamente, o malware teria que ser configurado para usar o proxy “normal” e isso geralmente não acontece; no proxy transparente não há esta limitação, portanto, o acesso aconteceria normalmente.

3.2.5. Firewall: Inspeção de estado (stateful inspection)

Sendo tratado por alguns especialistas no assunto como uma evolução dos filtros dinâmicos, os firewalls de inspeção de estado (*stateful inspection*) trabalham fazendo uma espécie de comparação entre o que está acontecendo e o que é esperado para acontecer.

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

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

3.2.6. Firewall de aplicações web (firewall application web - WAF)

O WAF é um novo tipo de firewall criado para combater as ameaças que estão além das capacidades dos firewalls tradicionais. Ele cria uma barreira entre o seu serviço baseado na web e todo o resto da internet, bloqueando e protegendo a aplicação de ações criminosas, como manipulação de conteúdo exibido, conhecida como “pichação”, injeções indevidas em banco de dados de padrão SQL ou simplesmente “SQL Injection”, determinados tipos de fraudes em acesso administrativo e várias outras espécies de ciberataques.

A maneira como o WAF atua garante que todos os tipos de negócio/empresas tenham suas redes protegidas adequadamente, ajudando as equipes de segurança da informação e segurança cibernética

no combate às principais ameaças e assegurando a continuidade das operações da empresa.

O web application firewall trabalha para impedir qualquer exposição de dados não autorizada em um site ou aplicativo baseado na web. Não é exagero algum dizer que um ataque organizado a um site é capaz de arruinar um modelo de negócio ou uma empresa, especialmente lojas virtuais que armazenam os dados dos usuários: sem a segurança adequada, essas informações podem facilmente cair nas mãos de criminosos cibernéticos.

Neste contexto, o WAF trabalha monitorando, filtrando e bloqueando automaticamente o tráfego de dados potencialmente maliciosos, liberando a TI da sua empresa para decidir quem terá o acesso impedido. Além disso, ele também é altamente escalável, permitindo a definição de um conjunto de regras para evitar os ataques mais comuns. O WAF pode ser executado como uma aplicação de rede, plug-in de servidor ou serviço na nuvem. Cada tipo apresenta suas vantagens e desvantagens, como você pode ver a seguir.

- **WAF de Rede** – esse modelo é normalmente baseado em hardware e, por ser instalado localmente, tende a ser mais rápido. Seu gerenciamento é normalmente oferecido como um serviço, o que pode tornar as coisas mais simples — e, por ter um conjunto central de assinaturas e opções de configuração, vários aplicativos podem ser protegidos com menos esforço. Como ponto negativo dos WAFs de rede, podemos apontar os altos custos não apenas do hardware necessário para a implementação da tecnologia, mas de todas as suas dependências, tais como contingência de energia por gerador e links redundantes de internet de altíssima largura;
- **WAF de Host** – a maior vantagem desse modelo é a possibilidade de incluir opções de personalização a um custo baixo — afinal, como é totalmente baseado em software, ele pode ser integrado no próprio

código do aplicativo. Porém, a tarefa de gerenciar os WAFs de host pode ser um tanto desafiadora, já que eles demandam bibliotecas locais, ambientes compatíveis (como Java ou .net) e são dependentes de recursos de [servidores](#) locais para funcionarem de forma eficaz;

- WAF na Nuvem – os WAFs hospedados na nuvem são geralmente administrados pelos provedores do serviço, que disponibilizam uma interface de configuração adequada às necessidades do cliente. Além de fáceis de implantar, são oferecidos em modelo de assinatura — o que os transforma na opção mais econômica e escalável de todas.

Independentemente do tipo de WAF que for implementado, é recomendável que a equipe de segurança faça alguns treinamentos de administração. Em muitos casos, quanto mais uma empresa desejar ter um papel profundo nas configurações de gerenciamento, mais treinos serão necessários. Seja quem for que administre o web application firewall, é importante ter ainda um time de desenvolvimento envolvido na tarefa, já que um WAF configurado incorretamente pode ter impacto negativo na performance e disponibilidade da aplicação que protege.

Uma alternativa para eliminar a necessidade desses esforços pela empresa é contratar os serviços de um IaaS (*Infrastructure as a Service*, ou Infraestrutura como um Serviço). Por uma taxa fixa mensal, você pode contar com o auxílio de profissionais especializados que cuidarão de todas as tarefas relacionadas ao WAF, liberando o seu time de TI para as tarefas estratégicas da companhia.

O WAF fornece proteção garantida contra as dez ameaças de segurança mais críticas identificadas pela comunidade on-line OWASP (*Open Web Application Security Project*, ou Projeto Aberto de Segurança em Aplicações Web). São elas:

1. Injection;
2. Broken Authentication and Session Management;
3. Cross-Site Scripting (XSS);
4. Broken Access Control;
5. Security Misconfiguration;
6. Sensitive Data Exposure
7. Insufficient Attack Protection;
8. Cross-Site Request Forgery (CSRF);
9. Using Components with Known Vulnerabilities;
10. Underprotected APIs.

O tráfego proveniente de ataques consome banda de internet, infraestrutura e recursos operacionais. Como o WAF bloqueia esses acessos inconvenientes, sua empresa acaba evitando todos esses gastos desnecessários.

Por fim é importante ressaltar que qualquer tipo de firewalls terá limitações, sendo que estas variam conforme o tipo de solução e a arquitetura utilizada. De fato, firewalls são recursos de segurança bastante importantes, mas não são perfeitos em todos os sentidos. Resumindo este aspecto, podemos mencionar as seguintes limitações:

- Um firewall pode oferecer a segurança desejada, mas comprometer o desempenho da rede (ou mesmo de um computador). Esta situação pode gerar mais gastos para uma ampliação de infraestrutura capaz de superar o problema;

- A verificação das políticas e regras contidas no firewall precisam ser revisadas periodicamente para não prejudicar o funcionamento de novos serviços;
- Novos serviços ou protocolos podem não ser devidamente tratados por proxies já implementados;
- Um firewall pode não ser capaz de impedir uma atividade maliciosa que se origina e se destina à rede LAN;
- Um firewall pode não ser capaz de identificar uma atividade maliciosa que acontece por descuido do usuário – quando este acessa um site falso de um banco ao clicar em um link de uma mensagem de e-mail, por exemplo;
- Firewalls precisam ser “vigiados”. Malwares ou atacantes experientes podem tentar descobrir ou explorar brechas de segurança em soluções do tipo;
- Um firewall não pode interceptar uma conexão que não passa por ele. Se, por exemplo, um usuário acessar a internet em seu computador a partir de uma conexão 4G (justamente para burlar as restrições da rede, talvez), o firewall não conseguirá interferir.

3.2.7. Firewall pessoal e appliance de hardware

Conforme observamos, as arquiteturas de firewall nos mostram as opções de configuração de firewalls em redes. Mas, como você provavelmente sabe, há firewalls mais simples destinados a proteger o seu computador, seja ele um desktop, um laptop, um tablet, enfim. São os firewalls pessoais (ou domésticos), que DEVEM ser utilizados por qualquer pessoa.

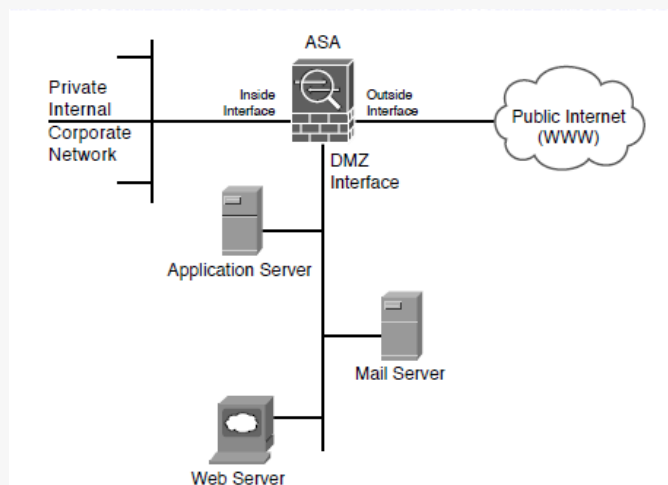
Felizmente, sistemas operacionais atuais para uso doméstico ou em escritório costumam conter firewall interno por padrão, como é o caso de

distribuições Linux, Windows ou Mac OS X. Além disso, é comum desenvolvedores de antivírus oferecerem outras opções de proteção junto ao software, entre elas, um firewall.

Existem ainda outras soluções de firewall que podem ser utilizadas para proteger a infraestrutura de TI da empresa. Estas por sua vez, são soluções “embarcadas”, ou seja, que possuem um conjunto de hardwares e softwares específicos e projetados exclusivamente para atuar com firewall. A grande vantagem de um firewall deste tipo “firewall de hardware” é que o equipamento, por ser desenvolvido especificamente para este fim, é preparado para lidar com grandes volumes de dados e não está sujeito a vulnerabilidades que eventualmente podem ser encontrados em um servidor convencional (por conta de uma falha em outro software, por exemplo).

3.3. DMZ – Zona Desmilitarizada (Demilitarized Zone)

DMZ é uma sigla para Demilitarized Zone (Zona Desmilitarizada em português), trata-se de uma sub-rede que se situa entre uma rede confiável (a rede da sua empresa, por exemplo) e uma rede não confiável (geralmente a internet), provendo assim isolamento físico entre as duas redes, garantido por uma série de regras de conectividade mantidas no firewall. O aspecto do isolamento físico do DMZ é importante pôr ele garantir que a rede WAN (a internet no caso) acesse apenas os servidores isolados no DMZ, ao invés de acessar diretamente a rede interna (LAN) da empresa, como pode ser visto a seguir. Os servidores mais comumente encontrados no DMZ são os que prestam algum tipo de serviço externo como por exemplo os servidores de e-mail, arquivos FTP e páginas HTML.

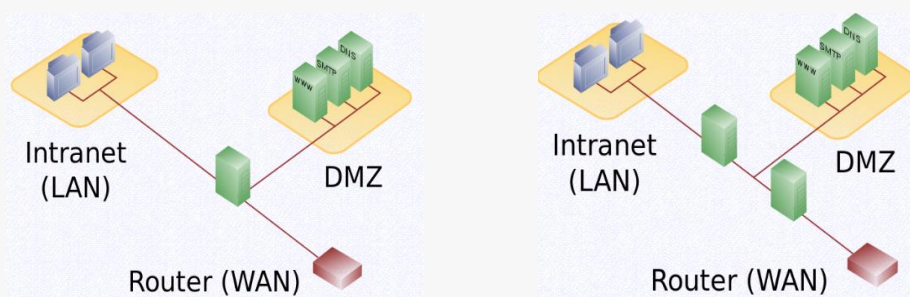


Apenas por curiosidade: O termo DMZ surgiu no meio militar, e significava uma área entre as áreas aliadas e inimigas. A DMZ (no sentido original, não computacional) mais famosa do mundo fica entre as fronteiras da Coreia do Norte e Coreia do Sul, que desde o fim da Guerra da Coreia (1953) ainda não assinaram um tratado de paz. Quanto as arquiteturas do DMZ, podemos implementar as seguintes:

- **Single Firewall** – trata-se de uma arquitetura comumente encontrada nas infraestruturas de TI das empresas. Qualquer firewall com pelo menos 3 interfaces de rede pode formar uma arquitetura desse tipo. Neste caso, a primeira interface de rede conecta o firewall à internet através do provedor de acesso (ISP), a segunda interface forma a rede interna (LAN) e a terceira interface é usada para criar a DMZ. Esse tipo de arquitetura é considerado vulnerável devido ao fato de o firewall ter que lidar com as requisições para a rede interna e o DMZ, sendo um ponto óbvio de ataque na arquitetura de segurança da rede.
- **Multiple Firewall** – considerada a arquitetura DMZ a mais segura. Utiliza mais de um firewall (geralmente dois), onde o primeiro, também chamado de firewall exterior ou de "front-end" é utilizado para direcionar o tráfego da internet para a DMZ apenas, enquanto os demais são utilizados para direcionar o tráfego da DMZ para a

rede interna (LAN). Esse tipo de arquitetura é considerado mais seguro pois para que a rede interna seja comprometida, é necessário que os dois firewalls sejam comprometidos. Por isso, quando essa arquitetura é utilizada, é comum que se usem firewalls de fabricantes diferentes, pois é mais difícil que as falhas de segurança encontradas no produto de um fabricante sejam encontradas no produto de outro, tornando assim a rede mais segura e confiável. Um exemplo dessa arquitetura pode ser visto na figura a seguir.

Figura 12 - DMZ: Single Firewall e Multiple Firewall.





XPe

> Capítulo 4



Capítulo 4. Proteção: Rede Interna (camada rede interna)

Nesta camada podemos adotar diversos tipos de mecanismos e ferramentas tecnológicas para garantir a proteção da rede LAN da empresa. A seguir iremos estudar os mais utilizados e implementados pelas equipes de segurança da informação e segurança cibernética.

4.1. Switches Layer 2 e 3 (switches gerenciáveis)

De acordo com a estratégia de defesa em profundidade “segurança em camadas”, precisamos garantir que a rede interna “LAN” da empresa possua barreiras que possam impedir, dificultar e inibir o acesso de ameaças (invasores) aos ativos de TI internos, caso as barreiras de proteção de borda sejam vencidas.

No passado as conexões locais entre os hosts da rede eram realizadas por meio de dispositivos denominados “HUBs” ou repetidores. Estes dispositivos eram extremamente inseguros e não possuíam inteligência para tratar os pacotes de dados que passam por eles. Ou seja, apenas realizam a repetição da transmissão dos pacotes de dados por toda a rede. E, o pior replicando essa transmissão aos hosts de toda rede. Isso sem dúvida apresentava um risco de segurança enorme, uma vez que uma ameaça poderia ser replicada a todos os hosts da rede.

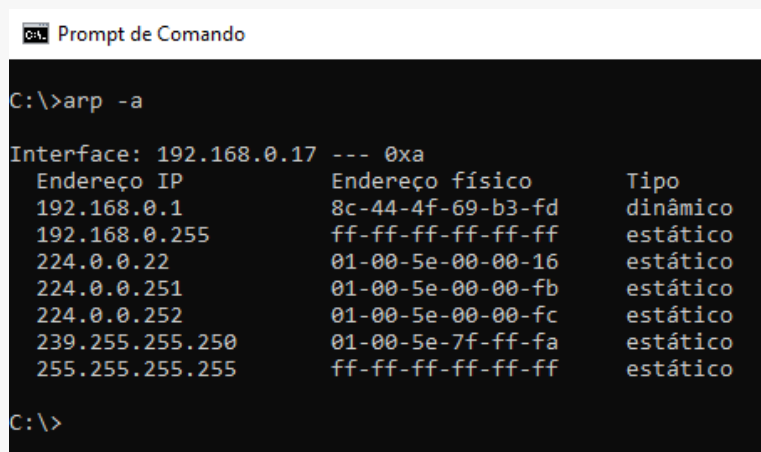
Atualmente o envio e recebimento dos pacotes de dados em uma rede local é realizada por roteadores ou switches, que por possuírem uma “inteligência” possibilitam a otimização de todo o tráfego da rede local, realizando a transmissão dos pacotes de dados de forma isolada, host a host sem mais replicar essa transmissão a todos os hosts da rede e, única exclusivamente, aquele host que requisitou a transmissão e está autorizado a recebê-la. Esse novo modelo proporcionou uma maior proteção e segurança as redes locais.

Os switches layer 2 e layer 3 são dispositivos que computacionais que possuem mecanismos de gerenciamento que podem ser configurados de acordo com as necessidades de proteção e segurança desenhadas pelas equipes de TI. São conhecidos comumente como switches gerenciáveis de camada 2 ou camada 3 do modelo de arquitetura TCP/IP.

A utilização de switches gerenciáveis como mecanismos de proteção a rede interna possibilita inúmeras vantagens, dentre as quais destacamos:

- Otimização das transmissões dos pacotes de dados por evitar problemas de colisão de dados durante a transmissão;
- Proteção da transmissão de pacotes de dados entre os host conectados à rede, através de um controle de endereçamento físico entre os hosts e as redes conhecido como endereços MAC – Media Access Control, um endereço físico configurado pelo fabricante em um hardware que possui conectividade à rede por meio do protocolo ethernet que fica armazenado em uma tabela denominada tabela ARP no switch que tem como função principal realizar o relacionamento entre o endereçamento IP utilizados junto as aplicações e o endereço físico “MAC” utilizado na camada enlace do modelo de arquitetura TCP/IP.

Figura 13 - Representação da tabela ARP contida em um host.



```
C:\> Prompt de Comando

C:\>arp -a

Interface: 192.168.0.17 --- 0xa
Endereço IP      Endereço físico  Tipo
192.168.0.1      8c-44-4f-69-b3-fd  dinâmico
192.168.0.255    ff-ff-ff-ff-ff-ff  estático
224.0.0.22       01-00-5e-00-00-16  estático
224.0.0.251      01-00-5e-00-00-fb  estático
224.0.0.252      01-00-5e-00-00-fc  estático
239.255.255.250  01-00-5e-7f-ff-fa  estático
255.255.255.255  ff-ff-ff-ff-ff-ff  estático

C:\>
```

- A criação de redes virtuais denominada VLANs – redes locais virtuais que possibilitam a criação de sub-redes (redes distintas), fortalecendo a proteção e a segurança da rede local, tema que iremos estudar a seguir.

4.2. VLANs – Redes locais virtuais

Existem inúmeras definições para uma rede local virtual, como pode ser observado na bibliografia.

- Varadarajan (2002) as define como "estruturas capazes de segmentar, logicamente, uma rede local em diferentes domínios de broadcast".
- Já Molinari (2002) diz que "uma rede virtual é um grupo de estações e servidores que se comunica independentemente de sua localização física ou topologia, como se fosse um único domínio broadcast, ou uma rede lógica."

De acordo com as definições apresentadas, a implantação de VLANs possibilita a partição de uma rede local em diferentes segmentos lógicos (criação de novos domínios broadcast), permitindo que usuários fisicamente distantes (por exemplo, um em cada local ou andar da empresa) estejam conectados à mesma rede.

Como fatores motivadores à criação de VLANs em uma infraestrutura de TI no ambiente corporativo, imagine uma empresa, cujo crescimento acelerado impossibilitou um projeto ordenado de expansão, que possua uma dezena de departamentos conectados a uma rede local interna. Ao contrário do que se pensa, os funcionários de cada departamento estão espalhados pelos andares da sede. Como organizar um domínio para cada setor da empresa? Uma solução possível seria a segmentação da rede interna em redes virtuais, uma para cada departamento.

Outro exemplo é a formação de grupos temporários de trabalho. Hoje em dia é comum o desenvolvimento de projetos envolvendo diversos setores de uma empresa, como marketing, vendas, contabilidade e comercial. Durante o período do projeto, a comunicação entre seus membros tende a ser alta. Para conter o tráfego broadcast, pode-se implementar uma VLAN para este grupo de trabalho.

Os exemplos anteriores mostram que as VLAN proporcionam uma alta flexibilidade a uma rede local. Isto é ideal para ambientes corporativos, onde a todo momento ocorrem mudanças de empregados, reestruturações internas, aumento do número de usuários, entre outras situações. Entre os benefícios proporcionados pela implantação de redes virtuais podemos citar:

- Controle do tráfego broadcast – as VLANs apresentam um desempenho superior as tradicionais redes locais, principalmente devido ao controle do tráfego broadcast. Tempestades de quadros broadcast (*broadcast storms*) podem ser causadas por mal funcionamento de placas de interface de rede, conexões de cabos malfeitas e aplicações ou protocolos que geram este tipo de tráfego, entre outros. Em redes onde o tráfego broadcast é responsável por grande parte do tráfego total, as VLANs reduzem o número de pacotes para endereços desnecessários, aumentando a capacidade de toda a rede. De um outro ponto de vista, em uma rede local segmentada, os domínios de broadcast são menores. Isto porque cada segmento possui um menor número de dispositivos conectados, comparado ao existente na rede sem segmentação. Com isso, trafegam menos quadros broadcast tanto em cada segmento, quanto em toda rede;
- Segmentação lógica da rede – como visto anteriormente, redes virtuais podem ser criadas com base na organização setorial de uma

empresa. Cada VLAN pode ser associada a um departamento ou grupo de trabalho, mesmo que seus membros estejam fisicamente distantes. Isto proporciona uma segmentação lógica da rede;

- Redução de custos e facilidade de gerenciamento – grande parte do custo de uma rede se deve ao fato da inclusão e da movimentação de usuários dela. Cada vez que um usuário se movimenta é necessário um novo cabeamento, um novo endereçamento para estação de trabalho e uma nova configuração de repetidores e roteadores. Em uma VLAN, a adição e movimentação de usuários pode ser feita remotamente pelo administrador da rede (da sua própria estação), sem a necessidade de modificações físicas, proporcionando uma alta flexibilidade;
- Independência da topologia física – VLANs proporcionam independência da topologia física da rede, permitindo que grupos de trabalho, fisicamente diversos, possam ser conectados logicamente a um único domínio broadcast.
- Maior segurança – as redes locais virtuais limitam o tráfego a domínios específicos proporcionando mais proteção e segurança a estes. O tráfego em uma VLAN não pode ser "escutado" por membros de outra rede virtual, já que estas não se comunicam sem que haja um dispositivo de rede desempenhando a função de roteador entre elas. Desta forma, o acesso a servidores que não estejam na mesma VLAN é restrito, criando assim "*domínios de segurança no acesso a recursos*".

Dispositivos em uma rede local virtual podem ser conectados de três maneiras diferentes, sendo:

- Enlace tronco (*Trunk Link*) – todos os dispositivos conectados a um enlace deste tipo, incluindo estações de trabalho, devem,

obrigatoriamente, ter suporte à VLANs. Todos os pacotes de dados transmitidos em quadros em um *trunk link* possuem um rótulo VLAN;

- Enlace de acesso (*Access Link*) – um enlace de acesso conecta um dispositivo sem suporte a VLAN a uma porta de um switch. Todos os pacotes de dados transmitidos em quadros neste tipo de enlace, obrigatoriamente, não devem possuir rótulo;
- Enlace híbrido (*Hybrid Link*) – este é uma combinação dos dois enlaces anteriores. Em um enlace híbrido são conectados tanto dispositivos com suporte a VLANs, quanto os sem. Num enlace desta natureza pode haver quadros com (*tagged frames*) e sem rótulo (*untagged frame*), mas todos os quadros para uma VLAN específica têm de ser com rótulo VLAN ou sem rótulo.

4.3. Redes wireless – Protocolo 802.1x

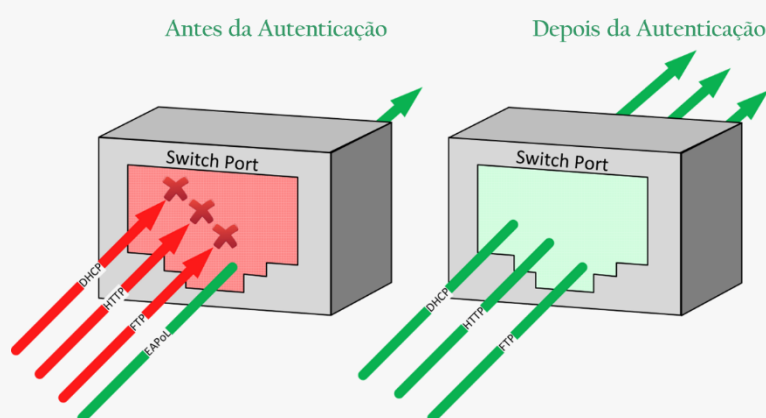
O 802.1x é um protocolo de controle de portas muito utilizado em redes wireless para admitir ou não uma estação dentro de uma rede, de acordo com o seu Mac Address e o status de sua autenticação. Os Switches incorporaram este protocolo para autenticar estações em redes locais, aumentando assim a segurança da rede como um todo.

O protocolo 802.1x pode bloquear ou permitir o acesso de um host à rede verificando se o seu Mac Address se encontra em uma tabela de hosts autorizados, mas como o Mac pode facilmente ser falsificado por meio da técnica spoofing, a melhor funcionalidade do protocolo é o bloqueio de toda a comunicação dos hosts não autenticados com a rede, exceto a comunicação de autenticação.

Uma vez que o host consegue se autenticar, os switches passam a transmitir todos os pacotes, sem exceções. Esta proteção é particularmente útil para evitar que pessoas mal-intencionadas, com acesso físico a um

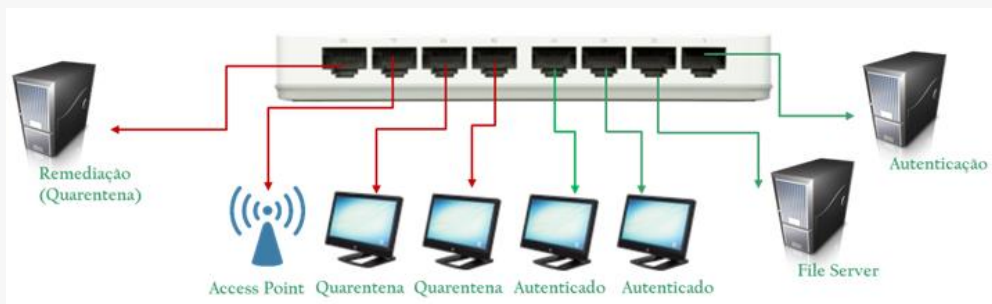
ponto da rede corporativa possa conectar um computador com a intenção de atacar os ativos e as estações da rede. Outra utilidade do 802.1x é designar um endereço IP de uma rede de quarentena para aos hosts que não se encontrarem em conformidade com a política de segurança da empresa. Podemos definir critérios de configuração, atualização de patches de segurança e atualização de antivírus como pré-requisitos para a entrada na rede principal da empresa.

Figura 14 - Funcionamento do protocolo 802.1x.



Observa-se na figura 15, um switch segregando hosts através do protocolo 802.1x. Os hosts que ainda não se autenticaram ou que não cumpriram os requisitos de segurança ficam em uma rede separada, chamada rede de quarentena. Nesta rede, eles têm acesso a um servidor de remediação, que pode atualizar as configurações, os patches de segurança da estação e os clientes de antivírus. Após a estação entrar em conformidade, ela sai da rede de quarentena e ganha um IP da rede corporativa. Essa correção é necessária, mas o ideal é que tenhamos mecanismos e ferramentas de proteção nos hosts, para que estes não fiquem desatualizados nunca. Devemos considerar que durante o tempo que o host ficou desatualizado, ele pode ter sido comprometido, e uma atualização posterior não retirará os privilégios do invasor nesta máquina.

Figura 15 - Segmentação de rede através do protocolo 802.1x.

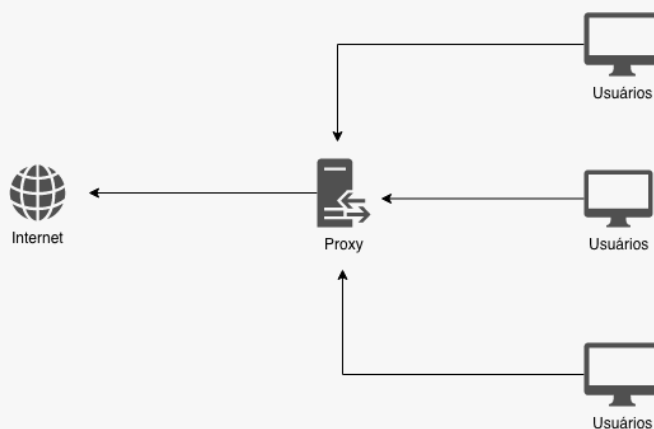


4.4. Servidor proxy e proxy reverso

Os servidores proxy foram criados no início da expansão da World Wide Web, quando a maioria das páginas eram estáticas e os links de comunicação trabalhavam a velocidades muito inferiores às disponíveis atualmente. Os proxies melhoram a eficiência das comunicações com a internet, fazendo um cache das páginas já acessadas e restringindo o acesso a sites não relacionados às atividades das empresas.

Com o passar do tempo as páginas web se tornaram cada vez mais dinâmicas, diminuindo a eficiência do cache de web, mas o proxy continua a ser uma ferramenta importante para a proteção de uma infraestrutura de TI. Isto porque permite bloquear o tráfego para websites não desejados pela empresa.

Figura 16 - Exemplo funcionamento proxy.



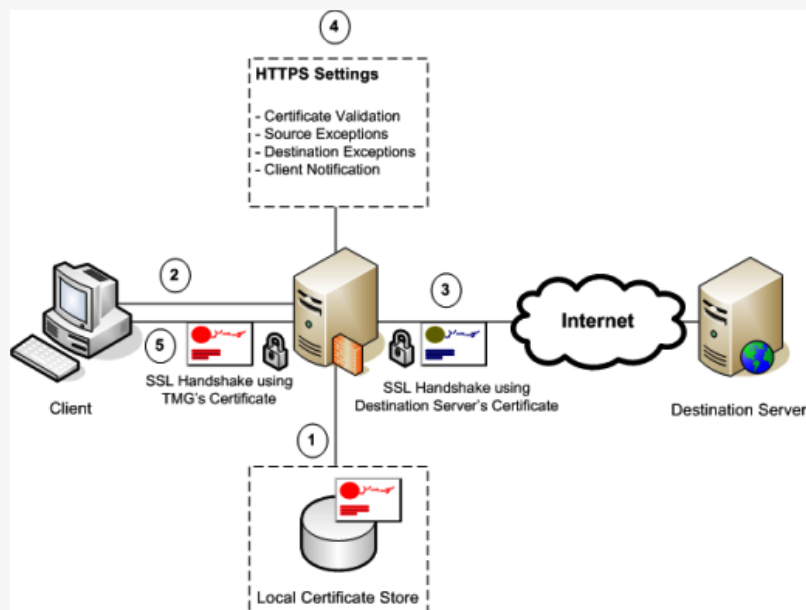
Observa-se na figura 16, alguns clientes da rede LAN conectando-se a um servidor proxy, que por sua vez, faz as solicitações a um servidor na

internet. Do ponto de vista do servidor externo, quem faz a solicitação é o servidor proxy e não a estação de trabalho. Essa ofuscação ajuda a proteger a estrutura interna da rede, uma vez que todas as solicitações de acesso a websites externos serão feitas pelo servidor proxy, que posteriormente analisará o conteúdo e o encaminhará para a estação que solicitou os dados.

Do ponto de vista do administrador de rede ou das equipes de segurança da informação e segurança cibernética, o proxy se torna um ponto de estrangulamento por onde passa todo o tráfego para a internet e onde eles podem aplicar as políticas de acesso de forma centralizada, protegendo todas os hosts em um ponto único. Além da URL, o administrador pode procurar por palavras-chave nas solicitações e registrar ou até mesmo bloquear o acesso a estes websites. Uma das vantagens de centralizar as configurações de acesso em um servidor proxy é a utilização de listas negras de websites, comumente conhecidas como blacklists, que podem ser alimentadas pelas equipes de segurança da informação ou segurança cibernética, ou baixadas de sites específicos na internet. Essas listas possuem URLs maliciosos, que trazem um perigo potencial não só para as estações da rede, mas também para todos os ativos de TI.

Um dos maiores desafios para os administradores de redes ou equipes de segurança da informação ou segurança cibernética, é lidar com o tráfego de pacotes de dados criptografados. Se os hosts estiverem criando conexões criptografadas diretamente com servidores na internet, o administrador ou a equipe de segurança perde o controle sobre os pacotes de dados que entram e saem da rede corporativa. Em um cenário como este, um colaborador pode enviar documentos com informações sensíveis para qualquer site na internet, e por outro lado um invasor pode controlar remotamente uma máquina que se encontra dentro da rede através de um malware instalado em um host, que cria uma conexão criptografada com seu controlador.

Figura 17 – Conexões criptografadas.



Na figura 17, observamos um proxy analisando uma conexão criptografada utilizando o protocolo SSL. Quando a estação pede para realizar a conexão, o servidor proxy solicita o certificado do servidor na internet e inicia uma comunicação criptografada entre os dois servidores. Uma vez que o proxy recebe os dados, ele os analisa e posteriormente envia para a estação que solicitou a conexão, através de uma conexão não criptografada ou de uma conexão criptografada entre a estação e o proxy, utilizando um certificado digital instalado no servidor proxy.

Por outro lado, o proxy reverso atende a uma finalidade completamente diferente da finalidade do forward proxy, ou simplesmente proxy comum. O proxy reverso recebe as conexões da internet como se fosse o servidor web da rede corporativa, analisa as requisições e posteriormente as envia ao servidor, ou um dos servidores capazes de atender à solicitação.

Do ponto de vista da segurança, a grande vantagem do proxy reverso é proteger os servidores contra possíveis ataques vindos de ameaças da web. Os proxies podem analisar o tráfego e verificar se existem padrões de ataques como os ataques de SQL Injection antes de passar os dados para

os servidores web, que podem conter aplicações vulneráveis a este tipo de ataque.

Quando o servidor web a ser protegido trabalha com conteúdo criptografado, o proxy reverso precisa abrir o conteúdo para examinar as solicitações e verificar se não trazem nenhuma ameaça para o servidor web. Neste caso em particular, é necessário instalar o certificado digital e a chave privada do servidor web no proxy reverso. A estação que se conectar ao proxy reverso pensará que está conversando com o servidor web e enviará os dados criptografados para o proxy reverso. Uma vez analisado o tráfego, o proxy reverso bloqueia as solicitações malformadas e encaminha as solicitações legítimas para o servidor web, através de uma conexão criptografada ou não, de acordo com a configuração escolhida pelo administrador de rede ou pela equipe de segurança da informação.

Figura 18 - Proxy reverso sem criptografia.

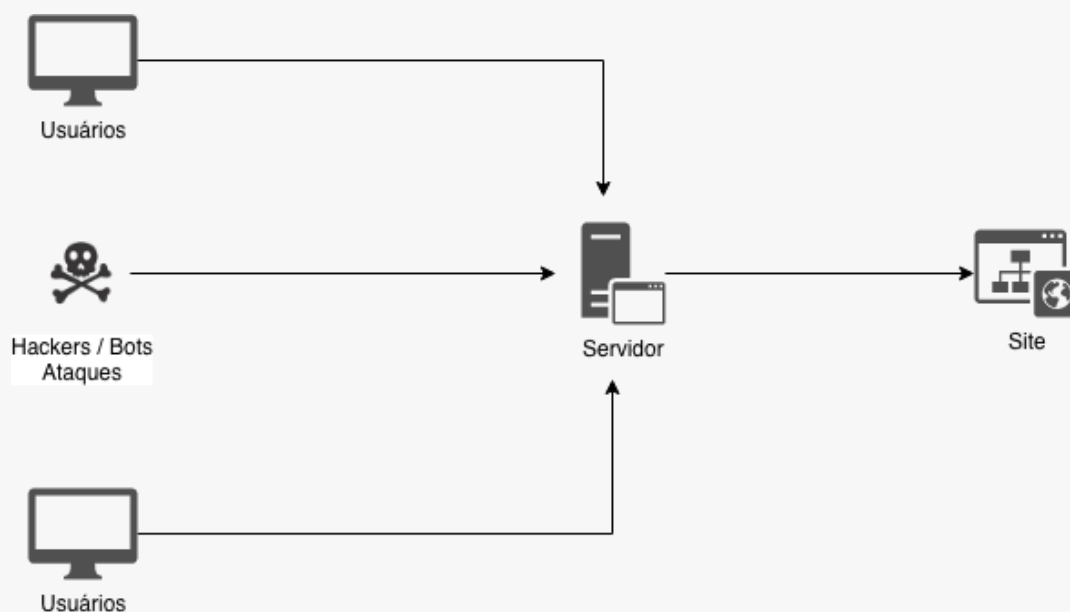
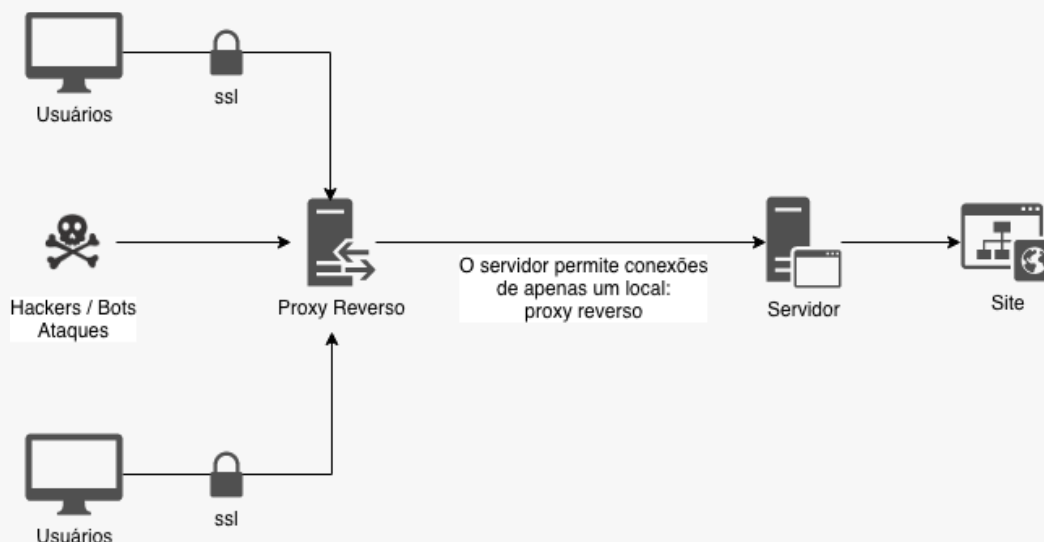


Figura 19 - Proxy reverso com criptografia.



É importante ressaltar que, como todas as informações externas passam por dentro do proxy reverso, o servidor de proxy reverso consegue tratar todas as informações que circulam na rede e pode oferecer diversas vantagens relacionadas à segurança, otimização e velocidade, entre as quais destacam-se:

- Proteção contra ameaças;
- Proteção contra spam;
- Criptografia: a criptografia SSL pode ser delegada ao proxy ao invés dos servidores internos;
- Balanceamento de carga: o servidor pode distribuir a carga para vários servidores da rede;
- Cache: Ele pode manter em cache o conteúdo estático. Dessa forma ele ajuda a diminuir a carga dos servidores da web;
- Velocidade: Através deste servidor, o acesso pode se tornar mais rápido pois ele comprime o conteúdo e pode distribuir esse conteúdo estático em redes CDN.



XPe

> Capítulo 5



Capítulo 5. Camada: Proteção Hosts (Segurança de Host)

Conforme estudamos no capítulo 2, a camada de segurança de host se concentra em manter a proteção dos hosts e respectivamente dos sistemas operacionais que controlam estes hosts. Porém, prover mecanismos e ferramentas de proteção nessa camada é uma tarefa especialmente desafiadora para as equipes de segurança da informação e segurança cibernética. Isto porque esses dispositivos são projetados para realizar multitarefas e interagir com vários outros dispositivos, aplicativos, protocolos e serviços simultaneamente.

Neste contexto, é importante que as equipes de segurança busquem implementar dispositivos de fabricantes de hardware e software, que seguem o conceito de segurança por design e segurança por default. Estes dois conceitos expressam a responsabilidade dos fabricantes de hardwares e desenvolvedores de softwares acerca da preocupação em aumentar os níveis de segurança no planejamento, fabricação e desenvolvimentos de dispositivos de hardware ou softwares.

Segurança por design significa que o hardware ou a aplicação (software) deve ser desenhado (planejado) para prover segurança desde sua concepção, passando por um processo de modelagem de ameaças como parte de sua análise, uma inspeção regular de código durante o término do desenvolvimento, e testes de invasão durante a homologação das versões. Já a segurança por default significa que o hardware ou a aplicação (software) quando é entregue ao usuário, deve ser configurado com a menor superfície de ataque possível, e seguindo a recomendação de privilégio mínimo, ou seja, com o mínimo de recursos habilitados e com usuários configurados para terem permissão de executar somente o necessário para a operação normal do sistema ou do dispositivo. Qualquer recurso ou

privilégio adicional deve ser habilitado pelo usuário administrador, de acordo com sua demanda ou políticas de segurança.

Outro exemplo sobre segurança por design e por default, vêm sendo divulgado e implementado quanto ao quesito “proteção à privacidade dos dados pessoais”. Neste caso, podemos citar como exemplo a Lei Geral de Proteção de Dados Pessoais brasileira – LGPD, que tem como um dos princípios a serem seguidos pelas empresas, a adoção de segurança baseada em privacidade por design e privacidade por default.

Bem, considerando que o fabricante de hardware ou o desenvolvedor de software teve o cuidado de seguir estes dois princípios, resta as equipes de segurança manter a infraestrutura de TI fortalecida, ou ainda, reforçar a proteção e a segurança dela, de acordo com a classificação de risco que esta infraestrutura receber. Para manter o host fortalecidos, ou seja, devidamente protegidos, devemos:

- Sempre manter atualizado todos os sistemas operacionais e ativos de rede;
- Eliminar todos os serviços desnecessários ou não utilizados pelos usuários;
- Utilizar baselines de fontes confiáveis;
- Dividir as funções entre servidores para reduzir a superfície de ataque;
- Remover funcionalidades ou recursos desnecessários ou não utilizados pelos usuários;

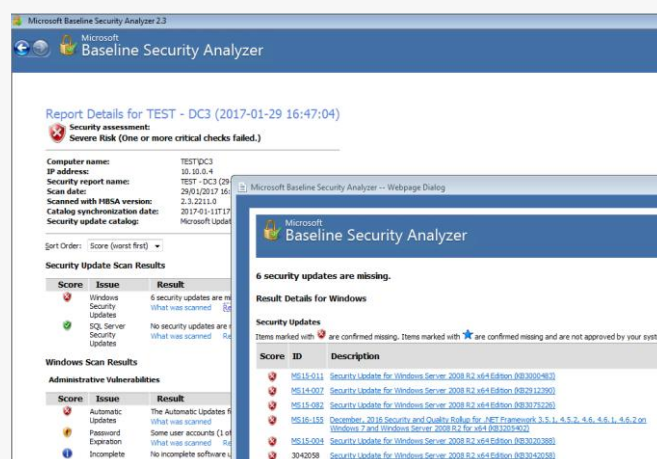
5.1. Baselines, bugs, atualizações e correções

Para que as equipes de segurança da informação e segurança cibernética possam fortalecer a proteção dos hosts existentes em suas

redes internas, existem diversos guias de que fornecem orientações sobre as melhores práticas para realizar configurações nos hosts, proporcionando aumentar a proteção e a segurança nos mesmos, sejam eles roteadores, switches, desktops, servidores ou servidores de alta criticidade. Porém, é importante termos em mente que cada configuração de segurança aplicada ao host pode dificultar a usabilidade dele, e até mesmo fazer com que algumas aplicações ou sistemas parem de funcionar. Por este motivo as equipes de segurança ou as equipes de TI, deve analisar estes guias de *Hardening* minuciosamente, verificando quais configurações podem ou não ser aplicadas em suas infraestruturas de TI e consecutivamente nos hosts pertencentes a mesma.

Além dos guias, existem alguns softwares que ajudam as equipes de segurança e de TI, na tarefa a verificar a configuração dos hosts e compará-las a um baseline estabelecido pelo fabricante do hardware ou software. Uma das ferramentas de baseline mais utilizadas por inúmeras equipes de TI, e que serve para tal propósito, é o MBSA (*Microsoft Baseline Security Analyser*), um programa gratuito que pode ser baixado do site da Microsoft, que permite a equipe de TI realizar uma análise acurada de um ou mais hosts na rede, indicando quais configurações estão de acordo com o baseline da Microsoft e quais não estão.

Figura 20 - Resultado obtido após a execução do MBSA.



Bugs são tão antigos como a própria computação e receberam este nome porque os primeiros defeitos nos computadores foram causados por pequenos insetos que causavam curtos nas placas de circuitos deles. Segundo a Wikipédia, um bug é um erro no funcionamento comum de um software ou hardware, também chamado de falha na lógica de um programa que pode causar comportamentos inesperados, como resultado incorreto ou comportamento indesejado. São, geralmente, causados por erros no próprio código-fonte, mas também podem ser causados por algum framework, interpretador, sistema operacional ou compilador.

O problema com os bugs é que eles podem levar ao comprometimento da segurança de todo o sistema. Quando um pesquisador consegue encontrar um bug em um sistema ele pode explorar este bug para fazer com que o sistema saia de seu comportamento normal e execute o código desejado pelo invasor.

Um dos bugs mais comuns é o *Buffer Overflow*. O Buffer é a memória utilizada para guardar as entradas de um usuário e, geralmente, tem um tamanho pré-fixado. Quando um usuário envia mais dados que o Buffer foi programado para suportar, estes dados passam então a ocupar um espaço de memória destinado a guardar outras entradas de usuários e até mesmo um ponteiro, destinado a guardar o endereço de memória onde o programa deve executar a próxima instrução. Um buffer overflow é realizado em cima de uma função de uma aplicação e como consequência ele se apodera de todos os recursos que o sistema operacional destina àquele processo. Uma informação importante a ser feita para avaliar o impacto do buffer overflow em um programa é saber com quais privilégios este programa é executado. Para entender melhor como uma ameaça pode explorar um buffer overflow, observe a figura a seguir:

Gerenciador de Tarefas

Arquivo Opções Exibir

Processos Desempenho Histórico de aplicativos Inicializar Usuários Detalhes Serviços

Nome	PID	Status	Nome de usuário	CPU	Memória (conjunto de t...	Virtualização do U...
chrome.exe	4736	Em execução	Max Jacomo	00	19.012 K	Desabilitado
CMServer.exe	3604	Em execução	SISTEMA	00	1.104 K	Não permitido
conhost.exe	8384	Em execução	Max Jacomo	00	240 K	Não permitido
conhost.exe	6376	Em execução	Max Jacomo	00	248 K	Não permitido
csrss.exe	596	Em execução	SISTEMA	00	792 K	Não permitido
csrss.exe	712	Em execução	SISTEMA	00	816 K	Não permitido
ctfmon.exe	8144	Em execução	Max Jacomo	00	45.120 K	Desabilitado
dllhost.exe	7768	Em execução	Max Jacomo	00	2.816 K	Desabilitado
dllhost.exe	9140	Em execução	Max Jacomo	00	1.536 K	Desabilitado
dllhost.exe	11956	Em execução	SISTEMA	00	1.096 K	Não permitido
dwm.exe	1100	Em execução	DWM-1	00	37.276 K	Desabilitado
EasyTuneEngineServi...	4624	Em execução	SISTEMA	00	5.784 K	Não permitido
explorer.exe	6684	Em execução	Max Jacomo	01	51.220 K	Desabilitado
FileCoAuth.exe	12096	Em execução	Max Jacomo	00	1.296 K	Desabilitado
fontdrvhost.exe	928	Em execução	UMFD-0	00	1.188 K	Desabilitado
GCloud.exe	8444	Em execução	SISTEMA	00	4.744 K	Não permitido
gjagent.exe	9652	Em execução	Max Jacomo	00	2.580 K	Desabilitado
GoogleCrashHandler...	7784	Em execução	SISTEMA	00	360 K	Não permitido
GoogleCrashHandler...	7028	Em execução	SISTEMA	00	336 K	Não permitido
GraphicsCardEngine...	11408	Em execução	Max Jacomo	00	1.340 K	Não permitido
Interrupções do siste...	-	Em execução	SISTEMA	00	0 K	
LicenseServer.exe	3516	Em execução	SISTEMA	00	41.172 K	Não permitido

Menos detalhes Finalizar tarefa

Podemos perceber que em um sistema operacional de um host, haverá diversas aplicações, serviços e funcionalidades sendo executadas simultaneamente e que rodam de acordo com os privilégios de cada usuário. Como exemplo na figura a seguir é possível visualizar a aplicação “chrome.exe” sendo executada sob o privilégio do usuário “max jacomo”. Enquanto a aplicação “CMServer.exe” está sendo executado sob e com os privilégios do usuário “sistema”.

Figura 21 - Usuário privilegiado e não privilegiado.

Arquivo Opções Exibir

Processos Desempenho Histórico de aplicativos Inicializar Usuários Detalhes Serviços

Nome	PID	Status	Nome de usuário	CPU	Memória (conjunto de t...	Virtualização do U...
chrome.exe	4736	Em execução	Max Jacomo	00	19.012 K	Desabilitado
CMServer.exe	3604	Em execução	SISTEMA	00	1.104 K	Não permitido
conhost.exe	8384	Em execução	Max Jacomo	00	240 K	Não permitido
conhost.exe	6376	Em execução	Max Jacomo	00	248 K	Não permitido

No caso da primeira aplicação, como o usuário “max jacomo”, possui menos privilégios se comparado com um usuário do tipo sistema, caso este

usuário seja alvo de alguma ameaça, o impacto junto ao sistema operacional do host será menor, tendo em vista que o “max” não possui acesso privilegiado. Agora, caso ocorra um buffer overflow provocado por uma ameaça/invasor no aplicativo CMServer.exe, que por sua vez foi escalonado para ser utilizado pelo usuário “sistema”, que possui privilégios maiores se comparado com os privilégios configurados ao usuário “max jacom”, o resultado poderia ser catastrófico, visto que por se tratar de um aplicativo “serviço” que está escalonado para um usuário com “poder”, ou melhor, “acesso” privilegiado, este invasor ou ameaça poderia adquirir o acesso e controle total do sistema operacional, o que causaria uma grande falha de segurança no host.

No caso de atualizações e/ou correções, é comum que muitos dispositivos de hardware e aplicativos “softwares”, logo após o seu lançamento, possuam uma vulnerabilidade que não foi descoberta durante as fases de teste e homologação. Assim sendo, tal vulnerabilidade ficará em um estado latente até que algum pesquisador – geralmente um hacker – contratado ou não pelo fabricante ou desenvolvedor a encontre. A índole do pesquisador vai ditar as regras de quando ele irá publicar a vulnerabilidade encontrada. Se o pesquisador estiver apoiando o fabricante ou desenvolvedor, e este tratar segurança como algo sério, a vulnerabilidade somente será publicada após uma correção estar disponibilizada para os usuários. Caso ele não se importe com o fabricante ou com os usuários, a vulnerabilidade pode ser publicada assim que ele a descobrir ou quando ele já tiver um código que a explore.

Porém, existe ainda uma outra possibilidade, a que ele os “pesquisados” não venha a publicá-la, e sim disponibilizá-la para um criador de vírus que se utilizam de “O-days”, ou seja, exploração de vulnerabilidades zero ou menos dias antes da publicação da correção, para causar algum tipo de dano ao hardware ou ao software no intuito de obter algum benefício para si. Uma vez que a correção é publicada, inicia-se o período de homologação

por parte do usuário, que pode levar de horas a dias. Os últimos estudos mostram que os vírus baseados em 0-days ou em correções recém-lançadas têm tido uma penetração maior em empresas do que em usuários domésticos, porque estes contam com um serviço de atualização automática, e as organizações perdem um tempo valioso em seu processo de homologação, que apesar de importante deve ser tratado com prioridade para que essa não fique exposta a ameaças durante muito tempo. Como dica para o gerenciamento de atualizações e/ou correções de vulnerabilidades, destacam-se: (a) utilizar fontes externas confiáveis para identificar vulnerabilidades; (b) estabelecer uma escala de atualização de 24 horas a 30 dias de acordo com a exposição e criticidade do sistema; (c) possuir um ambiente completo de homologação e testes.

A título de curiosidade, as vulnerabilidades 0-day (ou de dia zero) são aquelas em que hackers encontram e que poderiam ser exploradas antes que os desenvolvedores tenham tempo de reagir a respeito. Mas é claro que nem todas as vulnerabilidades descobertas são do tipo 0-day. A maioria das falhas de segurança são descobertas por outros desenvolvedores ou hackers em programas de Bug Hunting, por exemplo. Grandes players desenvolvedores de softwares como a Microsoft e a Google, possuem projetos voltados a descobrir falhas de segurança em seus softwares e em softwares de outras empresas antes que elas se tornem públicas.

Estes projetos possuem como objetivo tornar a internet mais segura. Isso porque, com tempo suficiente para consertar as vulnerabilidades, os desenvolvedores podem lançar um patch de correção para que os usuários atualizem seus sistemas e fiquem seguros. Afinal, uma premissa muito atestada no universo da segurança da informação é de que o usuário é o elo mais fraco da corrente e isto, por si só, já justifica o porquê de os criminosos virtuais estarem aumentando significativamente o alvo em usuários finais, uma vez que a falta de conhecimento e educação necessária em relação às

boas práticas de segurança abrem diversas brechas para os criminosos virtuais adentrarem no ambiente corporativo das empresas.

5.2. Exploit, Antivírus, AntiSpam e Anti-Malware's

Me permita uma pergunta: você sabe o que é um exploit? Bem, as habituais definições falam de um programa ou código que se **aproveita de uma brecha de segurança** (vulnerabilidade) em um aplicativo ou sistema, de forma que um atacante pode usá-la em benefício próprio.

Passando para a vida real, seria como se um modelo de fechadura (sistema ou aplicativo) tivesse uma falha que permitisse criar chaves que a abrissem a fechadura (**exploit**), permitindo que alguém (malware) possa acessar ao local e realizar atos ilícitos. Existe muita confusão entre os usuários e certo mito de que um exploit pode considerar-se malware. A realidade é que, como vimos no exemplo acima, exploit não é um código malicioso em si mesmo, mas apenas uma “chave” para que algum malware acesse ao sistema. Dessa forma, podem ser dadas as permissões necessárias para que o exploit possa executar-se em um sistema, aproveitando-se de uma vulnerabilidade.

Agora que você já sabe o que é um exploit, podemos distingui-lo entre dois tipos: os conhecidos ou desconhecidos (O-day).

Os **exploits** conhecidos são aqueles que estão mais presentes e podemos tomar medidas efetivas de proteção para **evitar** que os sistemas sejam afetados. Na verdade, costumam ser os que aparecem na maioria das notícias sobre segurança e, além disso, a cada dia surgem novos, da mesma forma que também vão aparecendo novas vulnerabilidades.

Por este motivo, é importante que as equipes de segurança da informação e segurança cibernética estejam informadas sobre quais vulnerabilidades estão sendo aproveitadas pelos **exploits** e possam ter certeza de que estão com todos os seus hosts, **sistemas e aplicativos**

atualizados. Caso ainda não exista uma atualização disponível, a equipe de segurança deve buscar medidas técnicas que ajudem a **mitigar** as possíveis ameaças.

No geral, vários desenvolvedores de softwares de proteção e segurança, principalmente os desenvolvedores de sistemas de antivírus, disponibilizam ótimas ferramentas de informação, constantemente atualizada sobre as falhas, correções e novidades, embora também existam sites especializados em identificar e informar as mudanças que aparecem a cada dia, como o Exploit Data base.

Por outro lado, falamos dos **exploits** desconhecidos ou **0-days**, os quais vemos muitas vezes nas notícias sobre segurança. Estes se utilizam das vulnerabilidades que **ainda não tenham sido informadas** ao público em geral e, portanto, podem representar uma grave ameaça, especialmente quando utilizam **ataques dirigidos** às empresas ou governos. Quando são utilizados, não é comum haver medidas que possam bloquear o malware que o aproveita e isso os converte em uma ameaça **praticamente indetectável**. É por isso que são bastante utilizados entre os cibercriminosos, permitindo roubar informações importantes de uma empresa ou governo e, em casos extremos, atacar certo tipo de **infraestruturas críticas**.

Por fim, a seguir apresentamos algumas medidas que precisam ser adotadas pelas equipes de segurança da informação e segurança cibernética para evitar que suas infraestruturas de TI sejam contaminadas por meio de malwares que utilizam de exploit:

- Manter todos os aplicativos e sistemas atualizados – sabendo que os **exploits** se aproveitam das brechas de segurança, é fundamental fechá-las o quanto antes. Além disso, o ideal é manter uma política de atualizações eficaz, evitando deixar uma “janela de tempo” que possa ser aproveitada pelos atacantes;

- Diminuir os efeitos de possíveis *exploits* usados contra nós ou contra as empresas. Pode ser que o fabricante do sistema ou aplicativo vulnerável não tenha lançado ainda uma atualização que solucione o problema. Nesse caso, pode-se utilizar ferramentas específicas e destinadas ao reconhecimento de bugs e anomalias sistêmicas. Isso ajuda a evitar que o sistema seja infectado até que apareça uma solução definitiva.
- Contar com soluções de segurança avançadas, disponibilizadas por grandes players especializados em segurança da informação e segurança cibernética, que são capazes de detectar e bloquear *exploits* projetados para aproveitar vulnerabilidades em navegadores web e leitores de PDF, entre outros.
- Para compreendermos mais facilmente o grande número de definições referentes ao malware, é melhor dividi-lo em duas partes, sendo elas:
- Vetor de ataque é o método que o agente ameaçador utiliza para atacar um sistema. Como exemplos, podemos citar: Trojam, Phising etc.
- Payload é uma atividade mal-intencionada exercida pelo malware. O payload é uma ação separada da instalação e da propagação que o malware realiza. Como exemplo, podemos citar: Spyware, Ransomware, Rootkit etc.

Dessa forma, é comum encontramos duas classificações ao definir essas ameaças. Um malware pode ser, por exemplo, um Trojam-Ransomware.

Spam é o termo utilizado para se referir aos e-mails não solicitados, que geralmente são enviados para muitas pessoas. O nome spam é a

abreviação do nome de um produto alimentício, o Spiced Ham (presunto condimentado). Em 1970, a trupe do Monty Python fez um quadro onde a atendente tentava adicionar o SPAM a qualquer tipo de comida. Isso transformou o termo em uma gíria que significa uma coisa chata, que é empurrada para você.

Além de atentar contra a disponibilidade de banda das organizações, o spam também pode ser utilizado para enviar e-mails com trojans e vírus.

A pessoa que envia spam é chamada de spammer. Os spammers violam várias regras de conduta na web, inclusive a do W3C, consócio de empresas de tecnologia que regulamentam padrões para a web.

Phishing Scam trata-se de um tipo de spam que se passa por um presente ou comunicação de uma instituição conhecida, como um banco, empresa ou site popular, induzindo as pessoas a fornecer senhas, dados pessoais e financeiros, que posteriormente podem ser utilizados para roubo de identidade, operações fraudulentas etc.

Inicialmente, os phishings direcionavam as pessoas para páginas fraudulentas na internet, que apresentam formulários onde roubavam os dados pessoais e financeiros. Como essa tática passou a ser muito combatida pelos bancos e fabricantes de softwares, os phishings passaram a instalar trojans que roubam esses dados ou interceptam uma sessão de Home Banking sem o conhecimento do usuário.

Para proteger os equipamentos da organização é importante manter softwares de segurança nas estações (hosts), para protegê-las de ameaças como vírus e spams. Podemos ter soluções antivírus e antispam instaladas nos servidores de arquivos e de correio, assim como nas estações. O importante é certificar-se de que estão sempre ativos e atualizados.

5.3. RootKits, BackDoors e HIDS

Um rootkit é um pacote de programas maliciosos, que substituem os arquivos binários (programas compilados) por um kit de programas que mantém uma porta aberta sem que verdadeiro root (administrador do unix) perceba. Com a porta aberta o invasor pode voltar a qualquer momento e utilizar os privilégios do root (ou do usuário do serviço) que ele tenha utilizado, para realizar absolutamente qualquer ação dentro do computador, inclusive roubar, alterar ou destruir qualquer informação.

O nome rootkit é derivado do usuário root do Unix, ambiente onde essa prática se popularizou, mas existem rootkit para quase todas as plataformas. Existem rootkit para Solares, Mac OS, Linux e a maioria das versões do Windows, entre outros. Os rootkit ganharam publicidade em 2005, quando foi revelado que a gravadora Sony/BMG instalava um rootkit chamado XCP (*Extended Copy Protection*) em seus CDs de música com o objetivo de instalar um mecanismo anticópia.

Os rootkit são extremamente difíceis de serem detectados, e infectam o sistema sem que o usuário perceba nada. É difícil garantir a completa remoção dos rootkit de um sistema, esses programas são especializados em enganar as ferramentas de segurança para ficarem ocultos. A forma mais confiável de reaver seu computador é formatar o disco e reinstalar todo o sistema.

Já o backdoor é uma possível fonte de vazamento de informações sensível. São os canais secretos de comunicação, ou seja, canais que dos quais os usuários ignoram a existência. Estes canais são chamados de porta de manutenção ou backdoor, e são comumente utilizados por trojans para comunicar-se com seu controlador ou até mesmo fornecer acesso à máquina infectada.

São considerados backdoor os programas ou partes de códigos escondidos em outros programas, que permitem que um invasor entre ou

retorne a um computador comprometido por uma porta dos fundos, sem ter que passar pelo processo normal de autenticação. Nos primórdios da computação, os próprios programadores deixavam alguns backdoor em seus sistemas e os chamavam de “ganchos de manutenção”.

Nos sistemas Windows, os backdoor geralmente são trojans, instalados através de phishings, ou ainda programas instalados por worms, que após explorarem uma vulnerabilidade do sistema-alvo, infectam arquivos do sistema operacional e criam uma trilha adicional de execução, que mantém essa porta aberta. Esse tipo de malware também recebe o nome de rootkit no Windows.

Uma das soluções mais adequadas para detectar a ação de rootkit é o host IDS. Estes softwares salvam as informações sobre cada arquivo importante para a segurança do sistema e de tempos em tempos eles calculam novamente o hash destes arquivos para verificar se algum deles foi alterado. Além disso, os HIDS são capazes de realizar algumas funções como:

- Análise de logs;
- Correlação de eventos;
- Checagem de integridade;
- Aplicação de políticas de segurança;
- Detecção e alerta para rootkit;
- Podem detectar variações na configuração do sistema.

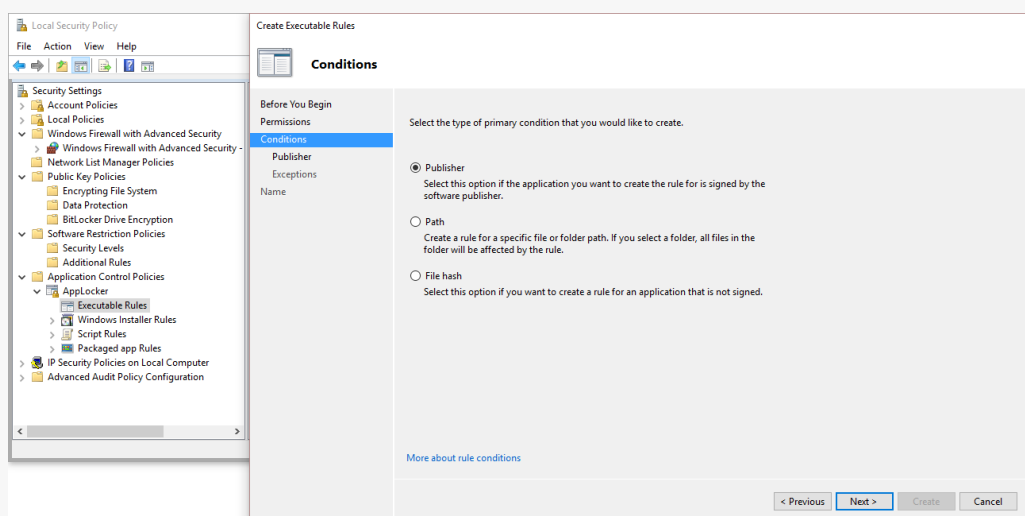
Como exemplo de ferramentas HIDS, citamos: SolarWinds Security Event Manager; Snort; Ossec; Fail2Ban; AIDE; Samhain e Suricata.

5.4. Whitelisting, Blacklist e EndPoint Security

Whitelisting ou lista de permissões, é a prática utilizada pelas equipes de segurança da informação e segurança cibernética para permitir explicitamente a algumas entidades identificadas (hosts) o acesso a um privilégio, serviço, mobilidade, acesso ou reconhecimento específico.

A proteção contra malware em uma infraestrutura de TI, em geral, depende de detecção das suas “assinaturas” por parte de um sistema de anti-malwares ou antivírus. No entanto, identificar um software malicioso é apenas uma das tantas missões que esses sistemas realizam. Na verdade, alguns especialistas diriam até que a detecção baseada em assinaturas – conhecida como blacklisting – é o lado menos importante do trabalho de um antivírus ou anti-malwares, por exemplo. Por outro lado, existe a tarefa da criação das whitelisting, que seria a pré-aprovação de softwares inofensivos ao contrário do bloqueio de softwares nocivos – papel da blacklisting.

Alguns sistemas operacionais possuem funções básicas de whitelisting. Como exemplo, podemos citar o aplicativo Windows AppLocker, que pode ser configurado para barrar ou permitir a execução de um software baseado no seu fabricante, seu caminho (pasta do executável) ou seu hash.



É possível também em servidores que possuem a função de controladores de domínios como por exemplo o Microsoft Windows Server, realizar a configuração de whitelisting e blacklisting por meio de GPOs (Group Policies ou Diretivas de Grupo), concedendo ou negando direitos como por exemplo: instalação de programas, acessos a endereços IPs, leitura, escrita ou execução de arquivos, entre outros esquemas que possibilitam aumentar a proteção dos hosts.

Com o aumento exponencial das ameaças em infraestruturas de TI, muitos fabricantes e desenvolvedores de soluções de segurança, perceberam que as empresas necessitavam de soluções integradas de proteção dos seus hosts e passaram a oferecer a seus clientes soluções completas, denominadas de soluções Endpoint Security. No geral, as soluções Endpoint Security oferecem em uma única suíte ou console, diversos mecanismos e ferramentas de segurança, a saber:

- Anti-malware;
- Antivírus;
- Firewall pessoais;
- Controle de listas (whitelisting);
- Aplicativos de baseline e avaliação de vulnerabilidades;
- Aplicativos de criptografia de arquivos e discos de armazenamento;
- Aplicativos de backup e restore
- IPS, IDS e DLP;
- Entre outros.
- Como exemplo de soluções endpoint security, citamos:

- Sophos Intercept X do fabricante Sophos;
- Kaspersky Endpoint Security do fabricante Kaspersky;
- Symantec Endpoint Security do fabricante Symantec;
- Bitdefender GravityZone Business Security do fabricante BitDefender;
- Entre outras.

Figura 22 - Endpoint Security no quadrante mágico do Gartner Group
(Ago, 2019).





XPe

> Capítulo 6



Capítulo 6. Tópicos Especiais I – IPS, IDS e VPN

Conforme os estudos realizados até o momento, podemos chegar à conclusão de que existem diversos tipos de ameaças rondando uma infraestrutura de TI. Algumas delas são conhecidas e outras não!

Neste contexto, implementar mecanismos de segurança e proteção que, de forma ativa ou passiva, realizem o monitoramento constante, torna-se uma solução de segurança eficiente e eficaz. Vamos deste ponto em diante conhecer alguma desses mecanismos.

6.1. IPS e IDS (Prevenção ou Detecção de Intrusão)

Com o objetivo de inspecionar dados e verificar a existência de fraudes ou erros, os sistemas financeiros começaram a introduzir, em meados da década de 60, a prática da auditoria. Contudo, surgiram algumas questões pertinentes sobre o que deveria ser detectado, como realizar uma análise nas descobertas e como proteger os diversos níveis de habilitação de segurança em uma mesma rede sem comprometer a segurança.

Entre 1984 e 1986, então, dois especialistas desenvolveram o primeiro modelo de IDS, chamado IDES (Sistema Especialista em Detecção de Intrusão). Ele é baseado na hipótese de que a base de comportamento de um intruso não é o mesmo de um usuário legítimo. Por isso, o modelo tenta criar um padrão de comportamento de usuários em relação a programas, arquivos e dispositivos, tanto em longo quanto em curto prazo. Depois do IDES, muitos outros sistemas foram desenvolvidos, baseados numa abordagem que combinava estatística e sistemas especialistas.

Conceitualmente, o IDS refere-se a um mecanismo capaz de identificar ou detectar a presença de atividades intrusivas. Em um conceito mais amplo, isto engloba todos os processos utilizados na descoberta de

utilizações não autorizadas de dispositivos de rede ou de computadores. Isto é feito através de um software projetado especificamente para tal propósito.

No entanto, devemos salientar a diferença entre IDS, IPS (Intrusion Prevention System) e IDPS. Enquanto o primeiro é um software que automatiza o processo de detecção de intrusão, o segundo faz a prevenção de intrusão, que tem por objetivo impedir possíveis ataques. Já o IDPS, por fim, é um recurso híbrido de detecção e prevenção acoplado como uma única solução. Mas, por que um sistema de detecção de intrusão é importante em uma infraestrutura de TI?

Então, a cada dia que passa, novas técnicas para comprometer ambientes computacionais são criadas, e é um grande desafio para o mercado de segurança da informação acompanhar esta velocidade, e até mesmo estar à frente para não atuar de forma reativa. O Brasil, por exemplo, é o país que mais sofre com ataques de ransomware na América Latina, com 55% do total.

Por isso, a implementação de uma boa política de IDS é fundamental em uma arquitetura de segurança. Este recurso se atualizado constantemente, é capaz de manter a infraestrutura distante de ataques oportunistas, seja sob uma perspectiva da rede, ou pelo próprio comprometimento de um computador.

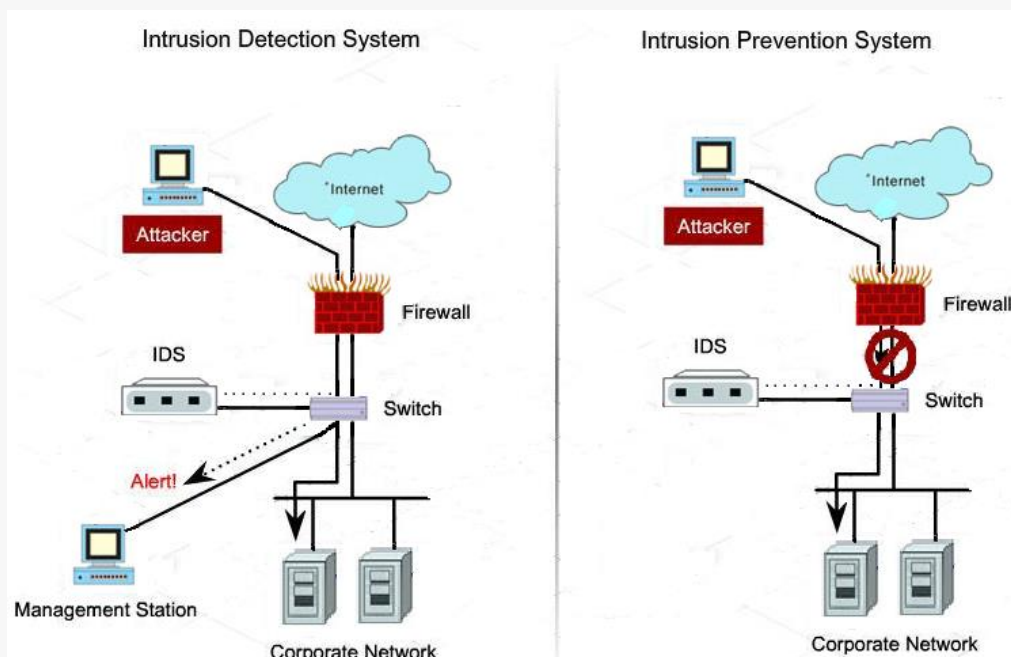
Combinar tantos sistemas de detecção e prevenção de intrusão baseados em rede (NDIS) e em host (HIDS) é essencial para uma boa saúde de segurança. Nenhum dos modelos apresentados é necessariamente excludente. Pelo contrário, eles devem ser tratados como complementares de acordo com a necessidade e criticidade de proteção exigidas por um ambiente corporativo e sua infraestrutura de TI. Os sistemas de detecção de intrusão podem ser categorizados em três grupos, dependendo do tipo de evento que monitoram e a maneira como são implantados. São eles:

1º grupo: IDS baseado em máquina e rede.

- Network Based – este tipo de IDS monitora o tráfego de rede em um segmento ou dispositivo, e analisa a rede e a atividade dos protocolos para identificar comportamentos suspeitos. Também é capaz de detectar inúmeros tipos de eventos de interesse, e geralmente é implantado em uma topologia de segurança como fronteira entre duas redes, por onde o tráfego é afunilado. Por causa disso, em muitos casos, o próprio recurso de IDS acaba sendo integrado diretamente no firewall.
- Host Based – podemos considerar um computador ou um servidor como host, pois o termo se refere a um equipamento ou ativo propriamente dito. A detecção de intrusão, neste formato, monitora características do dispositivo e os eventos que acontecem com ele em busca de atividades suspeitas. Geralmente, os IDS host based podem ser instalados de maneira individual, tanto para computadores corporativos dentro de uma rede empresarial, quanto para endpoints. Entre as principais características que ele acompanha, destacam-se o tráfego da rede para o dispositivo, os processos em execução, os logs do sistema, e o acesso e alteração em arquivos e aplicações.
- 2º grupo: IDS baseado em conhecimento e comportamento.
- Conhecimento – o IDS de conhecimento se baseia em um banco de dados que reconhece a assinatura de vulnerabilidades já identificadas anteriormente. Neste caso, é de suma importância que a estrutura tenha uma política de atualização contínua desse banco de dados, para garantir a continuidade de segurança do ambiente. Aquilo que não é conhecido não pode ser protegido.

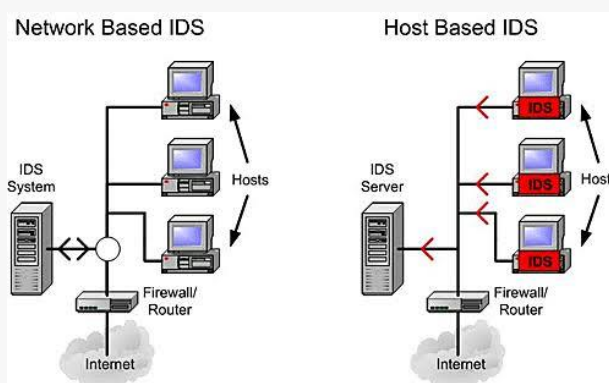
- Comportamento – este IDS, por outro lado, analisa o comportamento do tráfego e segue uma linha padrão de atividade normal do sistema. Caso haja desvios desse padrão – com a possibilidade de ser uma intrusão –, podem ser tomadas algumas ações, tais como o bloqueio temporário do tráfego ou alarmes para núcleos de operação de rede (NOC/SOC). Dessa forma, a anormalidade pode ser melhor investigada, liberada ou permanentemente bloqueada.
- 3º grupo: IDS ativo e passivo.
- Ativo – é definido como um IDS ativo, aquele que está programado para bloquear automaticamente ataques ou atividades suspeitas que sejam do seu conhecimento, sem qualquer necessidade de intervenção humana. Embora seja um modelo extremamente interessante, é importante uma padronização adequada nos ambientes protegidos a fim de minimizar falsos positivos – por exemplo, ao bloquear conexões que são legítimas, assim causando transtornos para a empresa.
- Passivo – um IDS passivo, por fim, faz o monitoramento do tráfego que passa através dele e assim identifica potenciais ataques ou anormalidades. Com base nisso, acaba gerando alertas para administradores e times de segurança – sem afetar em nada na comunicação. Trata-se de um modelo bastante interessante em uma arquitetura de segurança e, independente de não atuar diretamente na prevenção, serve como um excelente termômetro de ataques e tentativas de acesso não autorizados a infraestrutura de uma empresa.

Figura 23 - Diferença entre IDS e IPS.



Conforme podemos observar na figura 23, o IDS apenas executa a função de detectar e alertar as equipes de segurança no caso de uma tentativa de invasão ou ataque em uma rede. A equipe de segurança por sua vez realiza algum tipo de tratativa para inibir a invasão ou ataque. Ou seja, sua ação é “passiva” que depende de um segundo elemento de resposta. Já no caso do IPS, há uma ação “ativa”. Ou seja, não há a necessidade da ação do elemento de resposta (da equipe de segurança). Esta ação é realizada pelo próprio sistema, mitigando e repelindo a invasão e/ou ataque.

Figura 24 - Tipos IDS.



6.2. VPN – Virtual Private Network

À medida que uma empresa cresce, ela pode se expandir para várias localidades em sua cidade, país ou em todo o mundo. Para manter as coisas funcionando de maneira eficiente, as pessoas que trabalham nesses locais precisam de uma maneira rápida, segura e confiável de compartilhar informações nas redes de computadores. Funcionários em viagem, como vendedores, precisam de uma maneira igualmente segura e confiável de se conectar à rede de computadores de seus negócios a partir de locais remotos. Mesmo em lazer, as pessoas desejam manter seus computadores em segurança em uma rede desconhecida ou não segura.

Uma tecnologia popular para atingir esses objetivos é uma VPN (rede privada virtual). Uma VPN é uma rede privada que usa uma rede pública (geralmente a internet) para conectar sites ou usuários remotos. A VPN usa conexões "virtuais" roteadas pela internet da rede privada da empresa ou de um serviço VPN de terceiros para o site ou pessoa remota. As VPNs ajudam a garantir a segurança – qualquer pessoa que intercepte os dados criptografados não pode lê-los.

O objetivo de uma VPN é fornecer uma conexão privada segura e confiável entre redes de computadores em uma rede pública existente, geralmente a internet. Entre os benefícios que uma VPN pode oferecer à uma empresa, citamos:

- Conexões estendidas em várias localizações geográficas sem usar uma linha alugada;
- Segurança aprimorada para troca de dados;
- Flexibilidade para escritórios e funcionários remotos usarem a intranet comercial através de uma conexão de internet existente, como se estivessem diretamente conectados à rede;

- Economia de tempo e despesas para os funcionários comutarem se trabalharem em locais de trabalho virtuais;
- Maior produtividade para funcionários remotos.

Uma empresa pode não exigir todos esses benefícios de sua VPN, mas deve exigir os seguintes recursos essenciais de uma VPN:

- Segurança – a VPN deve proteger os dados enquanto viaja na rede pública. Se os invasores tentarem capturar os dados, eles não poderão lê-los ou usá-los;
- Confiabilidade – os funcionários e escritórios remotos devem poder se conectar à VPN sem problemas a qualquer momento (a menos que o horário seja restrito), e a VPN deve fornecer a mesma qualidade de conexão para cada usuário, mesmo quando estiver lidando com seu número máximo de simultâneas conexões;
- Escalabilidade – à medida que a empresa cresce, deve poder estender seus serviços VPN para lidar com esse crescimento sem substituir completamente a tecnologia VPN.

As equipes de segurança da informação e segurança cibernética, podem realizar a configuração de uma VPN de dois modos:

- VPN site to client: permite que usuários individuais estabeleçam conexões seguras com uma rede de computadores remotos. Esses usuários podem acessar os recursos seguros nessa rede como se estivessem diretamente conectados aos servidores da rede. Um exemplo de empresa que precisa de uma VPN de acesso remoto é uma grande empresa com centenas de vendedores em campo.
- VPN site a site: permite que escritórios em vários locais fixos estabeleçam conexões seguras entre si através de uma rede pública

como a internet. A VPN site a site estende a rede da empresa, disponibilizando recursos de computador de um local para funcionários de outros locais. Um exemplo de empresa que precisa de uma VPN site a site é uma empresa em crescimento, com dezenas de filiais em todo o mundo. As VPNs site a site, podem ser do tipo intranet – se uma empresa tiver um ou mais locais remotos nos quais deseja ingressar em uma única rede privada, poderá criar uma VPN na intranet para conectar cada LAN separada a uma única WAN ou do tipo extranet. Quando uma empresa tem um relacionamento próximo com outra empresa (como um parceiro, fornecedor ou cliente), pode criar uma VPN de extranet que conecta as LANs dessas empresas. Essa VPN de extranet permite que as empresas trabalhem juntas em um ambiente de rede compartilhado e seguro, impedindo o acesso às intranets separadas.

Figura 25 - Exemplo de VPN - Site to client.

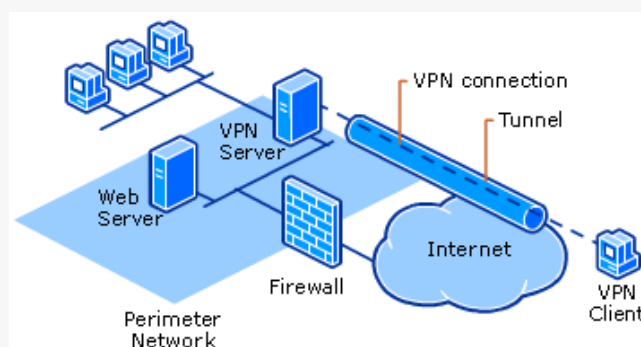
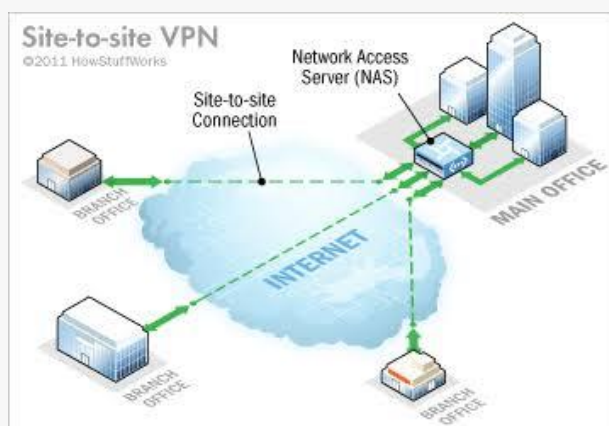


Figura 26 - Exemplo de VPN - Site to site.



Atualmente as VPNs são consideradas por muitos especialistas de segurança da informação e segurança cibernética, mecanismos confiáveis de proteção para a interligação de infraestruturas de TI distintas e dispostas em regiões físicas diferentes, pois além de prover uma segurança fim a fim de forma segura (criptografada), também fornecem economia. Atualmente os protocolos mais comuns utilizados em uma VPN são: PPTP, L2TP, SSTP, IKEV2 e OpenVPN.



XPe

> Capítulo 7



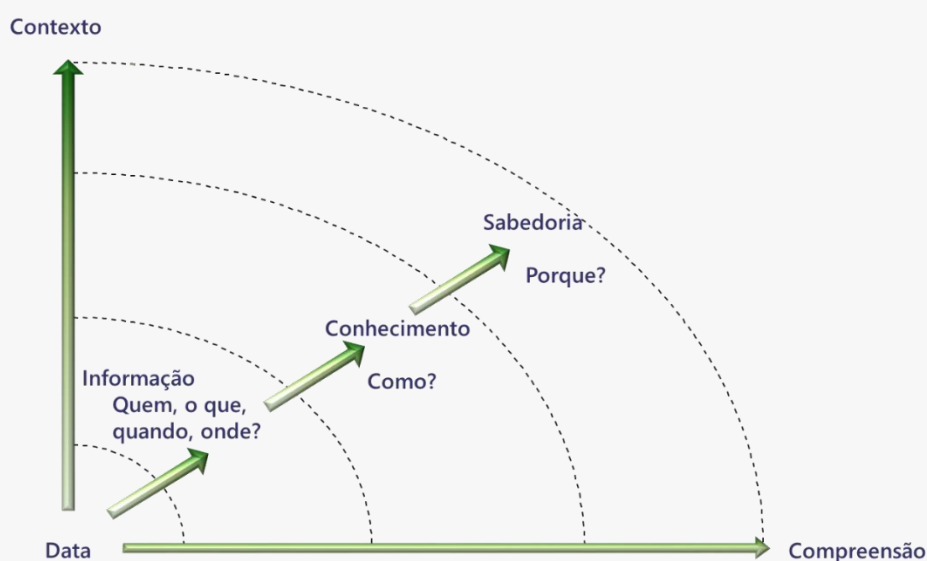
Capítulo 7. Tópicos Especiais II – Monitoramento, Logs e SIEM

Por definição, informação é o resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (pessoa, animal ou máquina). Podemos defini-la como “dados dotadas de significado e propósito”. Ela é a substância do conhecimento e deve responder a quatro perguntas: Quem? O quê? Quando? Onde?

A memória é o que faz o ser humano interiorizar suas experiências, relacioná-las, transformá-las em conhecimento e finalmente chegar à sabedoria (alguns nunca chegam). Chamamos este processo de DIKW (*Data-Information-Knowledge-Wisdom*), o acrônimo em inglês para Dados, Informação, Conhecimento e Sabedoria.

Este conceito, também conhecido como Pirâmide do Conhecimento, é uma hierarquia informacional utilizada principalmente nos campos da Ciência da Informação e da Gestão do Conhecimento, onde cada camada acrescenta certos atributos sobre a anterior, conforme a figura 27.

Figura 27 - Pirâmide do conhecimento (DIKW).



Imagine que você encontre um arquivo chamado mwnw.txt com a palavra “Gororoba”. Temos dois dados sem nenhum sentido, o nome do arquivo e seu conteúdo. Adicionando-se o contexto de que você procurava por senhas, temos a informação de que “Gororoba” é uma senha. Se você souber que está é a senha da rede MWNW, você tem conhecimento. Sabedoria é quando você sabe como utilizá-la para acessar a rede MWNW.

Os sistemas informatizados possuem as mesmas características. Qualquer “inteligência” que um sistema possua vem do registro, associação e interpretação dos eventos conhecidos por ele. Seguindo essa lógica, fica fácil compreender a importância da coleta, retenção e tratamento dos diversos tipos de registros gerados pelos sistemas informatizados de uma ou mais organizações. Mesmo as assinaturas de ataque encontradas em sistemas antivírus, IDS, IPS, Proxy Reversos, SIEMs etc., originam-se dos registros coletados por milhares, quando não milhões, de clientes espalhados pelo mundo.

O “Log” é o registro dos eventos que acontecem dentro de uma rede. Existem várias fontes de registro de logs, dentre eles podemos identificar aplicações, antivírus, servidores de acesso remoto, estações, servidores, switches, proxies, roteadores, IDS, IPS e firewalls.

Dentro da DIKW, o log algumas vezes pode representar apenas um dado e em outras pode representar uma informação, dependendo da forma como ele é construído. Existem três tipos de logs que são particularmente interessantes para a segurança da informação:

- Logs de software de segurança: trazem informações relevantes sobre os eventos ocorridos em toda a rede da organização. Nestes logs encontramos informações sobre eventos do firewall, do antivírus, do IDS e outros.

- Logs de sistema operacional: estes logs trazem informações sobre eventos ocorridos no sistema operacional. Estes eventos podem ter como fonte o próprio sistema (uma resolução DNS mal resolvida por exemplo) ou usuários do sistema (um administrador usando seus privilégios). Nesta categoria encontramos também os logs de segurança, que são os logs de auditoria de eventos. Dentro os eventos auditados temos, por exemplo, logon/logoff de usuário e criação acesso ou destruição de um objeto do sistema.
- Logs de aplicação: estes logs trazem informações sobre as aplicações que rodam no sistema operacional, como os bancos de dados, servidores web, aplicações web, e qualquer outra aplicação que esteja configurada para gerar registro de suas ações.

Um sistema que não possui registros de log é um sistema sem memória, incapaz de compreender a razão dos eventos. Um sistema sem memória nunca chegará ao conhecimento e muito menos à sabedoria, e seus gestores estarão fadados a inferir e presumir a origem dos eventos adversos que tendem a se proliferar, uma vez que sem o registro não podemos detectar a causa raiz e evitar uma reincidência.

O termo gestão fica incompleto quando se aplica a um ambiente de TI onde os gestores não têm registros e indicadores. Segundo uma frase atribuída a pelo menos dois grandes gurus da administração: O que não se mede, não se gerencia.

A integridade é outro aspecto importantíssimo a se considerar quanto aos logs é a necessidade absoluta de manter a integridade deles.

Por definição, integridade é a propriedade de manter a informação acurada, completa e atualizada. Garantir a precisão das informações e dos métodos de processamento aos quais ela é submetida. A quebra de integridade pode trazer prejuízos praticamente instantâneos para as

empresas e para os clientes dessas empresas. São exemplos de danos por quebra de integridade:

- Saldos de incorretos de correntistas de um banco.
- Venda de produtos por preços incompatíveis.
- Desabamentos devidos a cálculos incorretos.

Dos três princípios da segurança, a integridade é o mais abrangente e amplamente exigido em leis e regulamentações (ex.: Sarbanes-Oxley). A integridade pode ser definida em várias dimensões:

- Autenticidade (certeza de que uma informação pertence ao autor declarado): segundo o dicionário Aurélio, significa “o que é do autor a quem se atribui; a que se pode dar fé; que faz fé; legalizado, autenticado; verdadeiro, real, genuíno, legítimo”. Dentro da segurança da informação, a autenticidade nos fornece duas garantias fundamentais: o documento é realmente do autor declarado; o documento é o que diz ser;
- Não repúdio (impossibilidade de negar responsabilidade sobre seus atos): quando um documento é assinado de uma forma segura, dizemos que se estabeleceu o não repúdio, ou seja, a impossibilidade do assinante de negar a responsabilidade sobre seus atos. Um exemplo claro disso seria uma pessoa que usa um cartão com certificado digital (como o e-CPF) para assinar documentos. Devido ao grau de confiabilidade dessa tecnologia, essa pessoa não pode negar a autoria de uma transação na qual este cartão foi utilizado;
- Auditabilidade (grau de facilidade com que podemos checar a origem e consistência das informações): prevê a possibilidade de se checar os dados originários de determinada informação e reconstruí-la

através da recriação do processo original, validando assim toda a integridade da informação final;

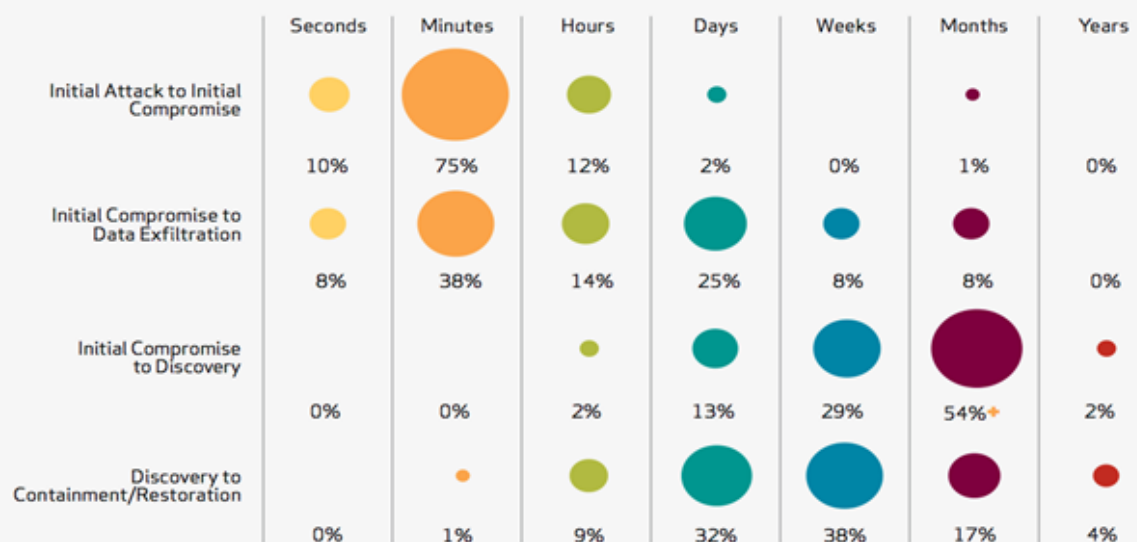
- **Exatidão** (capacidade de verificar e comprovar a exatidão das informações): é uma consequência da confiabilidade dos processos de entrada e processamento de dados, por isso a importância da possibilidade de verificação desses processos;
- **Precisão** (grau de variação de um resultado): é um componente importante da integridade, uma vez que um lapso de precisão pode causar uma inconsistência de dados;
- **Validade** (qualidade ou condição de válido): é alcançada quando os dados dos quais uma informação procede forem de alguma forma validados, eliminando a possibilidade de contaminação do resultado por dados incorretos;
- **Totalidade** (condição na qual um conjunto de informações se encontram por completo em um determinado sistema): é quando uma informação somente será confiável se todo o conjunto pré-estipulado de informações estiver totalmente disponível para processamento, caso contrário poderá haver impactos na exatidão e precisão das informações processadas.

A detecção de incidentes, é uma das variáveis com maior efeito na magnitude do dano total causado por um incidente, é o tempo de resposta a ele. Para ilustrar o raciocínio basta pensar em um incêndio. Se nada for feito, ele só vai parar de causar dano quando queimar tudo que for de alguma forma inflamável, e quanto antes reagirmos, menor o dano.

Os incidentes de segurança da informação acompanham a mesma lógica. O dano aumenta de forma diretamente proporcional ao tempo decorrido para a detecção do incidente. Na figura 28 vemos uma imagem retirada do Cisco Threat Report sobre a velocidade dos ataques atuais e o

tempo decorrido para a detecção de incidentes nas empresas de uma forma geral.

Figura 28 - Tempo de ataque e detecção de incidentes.



Os papéis e responsabilidades – as responsabilidades sobre a correta gestão de logs em uma organização podem recair sobre diversos profissionais, dependendo do tamanho e estrutura da empresa. De modo geral, os principais papéis e responsabilidade são:

- Desenvolvedores de aplicações: precisam desenhar as aplicações de forma que elas gerem os registros de forma consistente e segura, seguindo os requisitos de segurança do projeto do software;
- Administradores de redes e sistemas: responsáveis por configurar o registro de logs em sistemas operacionais, aplicações e dispositivos de rede, além de analisar o sucesso da atividade e realizar as manutenções necessárias para que os logs continuem íntegros;
- Administradores de segurança: responsáveis por criar as políticas e os procedimentos de gestão de logs, além de gerenciar e monitorar os indicadores para verificar a eficácia da política.

- Computer Security Incident Response Teams (times de resposta a incidentes de segurança): utilizam os dados dos logs para responder a incidentes de segurança;
- Auditores: utilizam os logs para realizar auditorias nos sistemas e devem auditar o próprio processo de gestão de logs.

Os logs e as fraudes – diversas pesquisas apontam que a maior parte das fraudes cometidas nas organizações são internas, e que estas fraudes internas representam as maiores perdas financeiras por fraude ao longo do ano.

A pesquisa realizada em 2018 pela KPMG da Austrália sobre fraude e má conduta mostra que 65% das fraudes foram realizadas por pessoas internas, e que estes 65% representaram 98% das perdas com fraudes.

Conforme dito anteriormente, uma empresa sem logs é uma empresa sem memória, e seus gestores andam às cegas. Sem uma gestão de logs apropriada fica muito difícil detectar ataques, contas de usuário comprometidas, abuso de privilégios e fraudes.

7.1. SIEM (Centralizadores de Logs)

Um host pode perder seus logs em caso de falhas de hardware/software e no caso de uma invasão, onde o atacante fará o possível para apagar os registros e encobrir os rastros de sua invasão ao sistema. Para garantir a integridade dos logs, a melhor abordagem é a de centralizar todos os logs em um único servidor, dedicado a tratar destes registros.

Centralizar os logs é um primeiro passo, visando manter a integridade de qualquer infraestrutura de TI. Veremos que estes logs centralizados podem ser correlacionados para que se descubra qualquer atividade anormal mais facilmente.

Existe um protocolo padrão para o redirecionamento de logs, o padrão do Syslog. O Syslog é muito utilizado nas variantes do UNIX e nos ativos de rede (roteadores, switches etc.). No entanto, existem diversos softwares que possuem um formato proprietário de logs. Nestes casos, é preciso instalar um cliente do software centralizador de log para que os mesmos cheguem ao centralizador. Já no caso dos sistemas operacionais Windows, o equivalente é o Windows Event Viewer.

As equipes de segurança da informação e segurança cibernética devem utilizar alguma ferramenta que facilite a realização de uma análise regular dos logs visando identificar problemas, incidentes e fraudes.

Existem diversas opções que vão desde a simples centralização do log até a correlação de eventos e geração de alertas automáticos. Quanto maior o investimento (tempo e/ou dinheiro) em criar o ambiente, maiores as chances de detecção.

A geração de arquivos de log é exigida por várias leis e regulamentações nacionais e internacionais, mas para que tenham valor legal, os arquivos de log precisam de proteção quanto à sua origem e sua integridade. Existem diversas formas de se garantir a integridade dos logs, sendo que as soluções mais avançadas de gerenciamento de log provêm desta garantia como parte de seu funcionamento.

Os logs são um componente essencial para uma análise forense bem-sucedida, e a garantia de que estes logs não foram alterados é o que dá credibilidade às evidências coletadas e pode significar a aceitação ou não de uma evidência em corte, o que em última instância pode significar a capacidade da organização de provar suas argumentações e ganhar a causa.

Os SIEMs coletam e agregam todos os eventos de segurança (logs de Firewall, Proxy, VPNs, IDS/IPS e outros dispositivos de perímetro como roteadores e switches de borda) e todos os eventos de gerenciamento de

segurança como os logs das estações, servidores, roteadores, switches, aplicações.

O SIEM oferece um console de acesso centralizado a todos os logs coletados, independente da tecnologia utilizada para gerar o log (um firewall proprietário, por exemplo), e possui a habilidade de correlacionar estes eventos tão diversos como uma mudança de configuração em um host e um anexo malicioso no antivírus, de forma que informações coletadas em vários sistemas gerem uma informação mais precisa sobre um possível ataque.

Costumamos dizer que no SIEM $1 + 1 = 3$, porque o sistema é capaz de detectar um possível incidente de maior magnitude (3) através da associação dois eventos de menor magnitude (1), que passariam despercebidos. Dentre as vantagens que um SIEM proporciona, podemos destacar as seguintes características:

- Detecta sistemas internos infectados;
- Identifica sistemas infectados tentando enviar informações para fora da empresa;
- Mitiga o impacto de sistemas infectados;
- Detecta a saída de dados sensíveis (DLP);
- Fundamental para algumas certificações, como o PCI, ISSO 27001 etc.

Os SIEMs estão se tornando o padrão de fato para o tratamento de todos os eventos dentro das organizações, e têm chamado a atenção da comunidade de software livre e de diversos fabricantes.

Referências

ABNT NBR ISO/IEC 27001:2013. Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação – Requisitos.

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

BUGS. In: *Wikipédia*, a enciclopédia livre. Flórida: Wikimedia Foudation, 2019. Disponível em: <<https://pt.wikipedia.org/wiki/Bug>>. Acesso em 07. Abr. 2022.

CERT.br. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <<https://www.cert.br/>>. Acesso em: 07. Abr. 2022.

COBB, Michael. *Using 802.1X to control physical access to LANs*. SearchMidmarketSecurity, 2009. Disponível em: <<https://searchmidmarketsecurity.techtarget.com/tip/Using-8021X-to-control-physical-access-to-LANs>>. Acesso em: 04 fev. 2019.

COMER, Douglas E. *Redes de Computadores e Internet*. 2. ed. São Paulo: Bookman, 2001.

DANTAS, Mário. *Tecnologia de Redes de Comunicação e Computadores*. Rio de Janeiro: Axcel Books, 2002.

HARRIS, Shon. *CISSP All-in-one*, 3. ed.: Mc Graw Hill, 2004.

INTRUSION DETECTION SYSTEM. In: *Wikipédia*, a enciclopédia livre. Flórida: Wikimedia Foudation, 2020. Disponível em: <https://en.wikipedia.org/wiki/Intrusion_detection_system>. Acesso em: 7. Abr. 2022

KIM, David; SOLOMON, Michael. *Fundamentos de Segurança de Sistemas de Informação*. 1.ed. São Paulo: LTC Exatas Didática, 2014.

MACHADO, Felipe R. Nery. *Segurança da Informação – Princípios e controle de ameaças*. 1.ed. Rio de Janeiro: Editora Érica, 2014.

MICROSOFT. VPN Tunneling Protocols. In: *Microsoft Docs*, 2012. Disponível em: <[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771298\(v=ws.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771298(v=ws.10)?redirectedfrom=MSDN)>. Acesso em: 07. Abr. 2022.

OUELLET, Eric; LITAN, Avivah; MCSHANE, Ian. *Magic Quadrant for Endpoint Protection Platforms*. Gartner, 2017. Disponível em: <<https://www.gartner.com/en/documents/3588017>>. Acesso em: 07. Abr. 2022.

RITTINGHOUSE, John W; RANSOME, F. James. *Cloud Computing. Implementation, Management and Security*. CRC PRESS, 2009.

SCARFONE, Karen; MELL, Peter. *Guide to Intrusion Detection and Prevention Systems*. CSRC, 2007. Disponível em: <<https://csrc.nist.gov/publications/detail/sp/800-94/final>>. Acesso em: 07. Abr. 2022.

SÊMOLA, Marcos. *Gestão da Segurança da Informação*. 2.ed. São Paulo: Gen-LTC, 2013.

SOARES, Luís Fernando; LEMOS, Guido; COLCHER, Sérgio. *Redes de computadores: das LANs, MANs e WANs às redes ATM*. Rio de Janeiro: Campus, 1995.

SPONH, Marco Aurélio. *Desenvolvimento e análise de desempenho de um “Packet Session Filter”*. Porto Alegre – RS: CPGCC/UFRGS, 1997.

STALLINGS, Willian. *Criptografia e Segurança de Redes – Princípios e Práticas*. 6.ed. São Paulo: Pearson, 2016.

STALLINGS, Willian; BROWN, Lawrie. *Segurança de Computadores – Princípios e Práticas*. 2.ed. São Paulo: Elsevier, 2017.

TANENBAUM, Andrew. S. *Redes de Computadores*. 4ª ed. Rio de Janeiro: Editora Campus (Elsevier), 2011.

V., John. *Overview*. Forward Proxy vs. Reverse Proxy. Blog Managed File Transfer and Network Solutions, 2012. Disponível em: <<https://www.jscape.com/blog/bid/87783/Forward-Proxy-vs-Reverse-Proxy>>. Acesso em: 07. Abr. 2022.

ZWICKY, Elizabeth D.; COOPER, Simon; CHAPMAN, D. Brent. *Building Internet Firewalls: Internet and Web Security*. 2. ed. O'Reilly Media, 2000.