FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI
Curso Superior de Tecnologia em Segurança da Informação

Raul Misael De Lima

ENTENDENDO IPS E IDS

Uso de IPS e IDS em conjunto

Americana, SP
2021

FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI
Curso Superior de Tecnologia em Segurança da Informação

RAUL MISAEL DE LIMA

ENTENDENDO IPS E IDS

Uso de IPS e IDS em conjunto

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Dr. Daives Arakem Bergamasco.

Área de concentração: Segurança da Informação

Americana, SP

2021

L71e LIMA, Raul Misael de

Entendendo IPS e IDS: uso de IPS e IDS em conjunto. / Raul Misael de Lima. – Americana, 2021.

40f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Dr. Daives Arakem Bergamasco

1 Segurança em sistemas de informação I. BERGAMASCO, Daives Arakem II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

RAUL MISAEL DE LIMA

ENTENDENDO IPS E IDS

Uso de IPS e IDS em conjunto

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Banca Examinadora:

_____
Daives Arakem Bergamasco
Doutor
Faculdade de Tecnologia de Americana

_____
EDSON ROBERTO GASETA
Mestre
Faculdade de Tecnologia de Americana

_____
LUIZ CARLOS CAETANO
Especialista
Faculdade de Tecnologia de Americana

Americana, 01 de julho de 2021.

AGRADECIMENTOS

Agradeço à minha esposa que esteve comigo em todo o período de graduação.

DEDICATÓRIA

A Deus e ao meu pai, onde quer que ele esteja.

RESUMO

Muito pode ser visto em tópicos relacionados à segurança (sobre IPS e IDS). Porém, possuir essas tecnologias tem pouco valor agregado e aprofundar os conhecimentos, ainda existem algumas lacunas nesses tópicos. IPS e IDS podem trabalhar juntos de forma eficaz. O objetivo é abordar e valorizar essas duas ferramentas e como implementá-las juntas para fornecer segurança mais forte para o seu ambiente. Não será demonstrada a implementação dessas ferramentas, mas apenas mostrar um ponto de vista para reunir conhecimentos que possam melhorar o ambiente de sua empresa.

A configuração correta e a implementação do uso de IPS e IDS irão melhorar muito a segurança da empresa. Essas duas ferramentas fornecem elementos-chave para uma estratégia de defesa em profundidade. O propósito não é mostrar detalhes técnicos detalhados, mas cobrir os aspectos avançados de IPS e IDS em treinamento e técnicas de desempenho pessoal, implementação, aconselhamento e atenção.

Palavras-Chave: Sistema de detecção de intrusos; Sistema de prevenção de intrusão; Sistema de detecção de intrusão baseado em host; Conscientização de Rede em Tempo.

ABSTRACT

Much can be seen in security-related topics (about IPS and IDS). However, having these technologies has little added value and, when we want to deepen our knowledge, there are still gaps in these topics. IPS and IDS can work together effectively. In contrast, some forums are opposed to these technologies. Our goal is to address and value these two tools and how to implement them together to provide stronger security for your environment. We don't want to demonstrate the implementation of these tools, but just show a point of view to gather knowledge that can improve your company's environment.

The correct configuration and implementation of the use of IPS and IDS will greatly improve the security of the company. These two tools provide key elements for an in-depth defense strategy. Our purpose is not to show detailed technical details, but to cover the advanced aspects of IPS and IDS in training and techniques of personal performance, implementation, advice and attention.

Keywords: Intrusion Detection System; Intrusion Prevention System; Host-based Intrusion Detection; Real-time Network Awareness;

LISTA DE FIGURAS

TERMOS

IDS - Intrusion Detection System ou Sistema de detecção de intrusão

HIDS - Host-based Intrusion Detection System ou Sistema de detecção de intrusão baseado em host

IPS - Intrusion Prevention System ou Sistema de prevenção de intrusão

NIPS - Network Intrusion Prevention System ou Sistema de prevenção de intrusão baseado em rede

RNA - Real-time Network Awareness ou Conscientização de rede em tempo

SMA - Security Management Appliances ou Dispositivos de gerenciamento de segurança

HTTPS - Hyper Text Transfer Protocol Secure ou Protocolo de transferência de hipertexto seguro

TCP - Transmission Control Protocol ou Protocolo de controle de transmissão

SUMÁRIO

1. INTRODUÇÃO

As redes foram descobertas e construídas há muitos anos. Dependendo da profundidade da investigação, a ideia de redes de dados pode ser rastreada centenas de anos. O conteúdo abordado no texto, será concentrado no uso mais recente de redes decorrentes das décadas de 1960 e 1970. uma vez que as redes foram descobertas e construídas, o potencial de intrusão dessas redes também se tornou uma realidade. Da resposta à intrusão veio a ideia de detecção de intrusão. O termo IDS foi definido de muitas maneiras desde as primeiras descobertas, porque o inevitável requisito que decorre da descoberta de uma nova tecnologia é a necessidade e interesse em monitorar essa tecnologia.

Complementar ao monitoramento é a capacidade para relatar sobre novas tecnologias e mostrar o valor delas para seus colegas e associados de negócios. Além disso, há sempre alguém que testará uma nova tecnologia para garantir que seja estável e consistente. O teste geralmente leva à identificação de vulnerabilidades que por sua vez leva à possibilidade de intrusão. O próximo passo, lógico, depois de descobrir uma tecnologia e a inevitáveis vulnerabilidades associadas é identificar os parâmetros de segurança. Uma maneira de ajudar a determinar esses parâmetros de segurança é construir uma fórmula para representar a ideia de segurança:

Segurança = visibilidade + controle

Tecnologia IDS, que monitora a rede em busca de eventos que possam violar alguma regra de segurança, fornece a visibilidade e oferece muitos outros benefícios diretamente relacionados ao monitoramento de nossas redes. Isso inclui a visibilidade ativa do que está acontecendo em nossas redes à medida que acontece, bem como a capacidade de armazenar essas informações para análise e relatórios em uma data posterior. A visibilidade é fundamental para a tomada de decisão. A visibilidade torna possível criar uma política de segurança baseada em dados quantificáveis do mundo real. A outra parte da fórmula é o controle e será abordada em mais detalhes por meio da pesquisa da tecnologia IPS. É a tecnologia IPS que fornece uma capacidade ativa de controlar nossas redes. O controle é fundamental para a aplicação, pois torna possível garantir a conformidade com a

segurança política. O termo IPS tem sido usado muito nos últimos anos e ainda está sendo definido com mais precisão à medida que a tecnologia amadurece.

A definição de IPS sendo usados para os fins deste TCC é a capacidade de detectar e prevenir atividades em ou ser apresentado a uma rede corporativa. Existem várias maneiras de fornecimento da capacidade do IPS e iremos cobrir alguns neste documento. Em particular, será mostrado os pontos fortes e fracos da combinação das tecnologias IPS e IDS juntos. Infelizmente, a maioria das organizações que operam grandes redes internas estão limitados pelo orçamento e de mão de obra capacitada e não têm recursos, de uma forma ou de outra, para implantar dezenas ou mesmo centenas de aparelhos individuais necessários para operar uma defesa eficaz em estratégia com profundidade.

À medida que dividimos as várias questões de recursos em torno de uma estratégia de defesa em profundidade relacionada à tecnologia IPS/IDS, descobrir por que o uso de ambas as tecnologias em harmonia é uma solução adequada para a maioria das médias e grandes corporações.

2. REVISÃO BIBLIOGRÁFICA

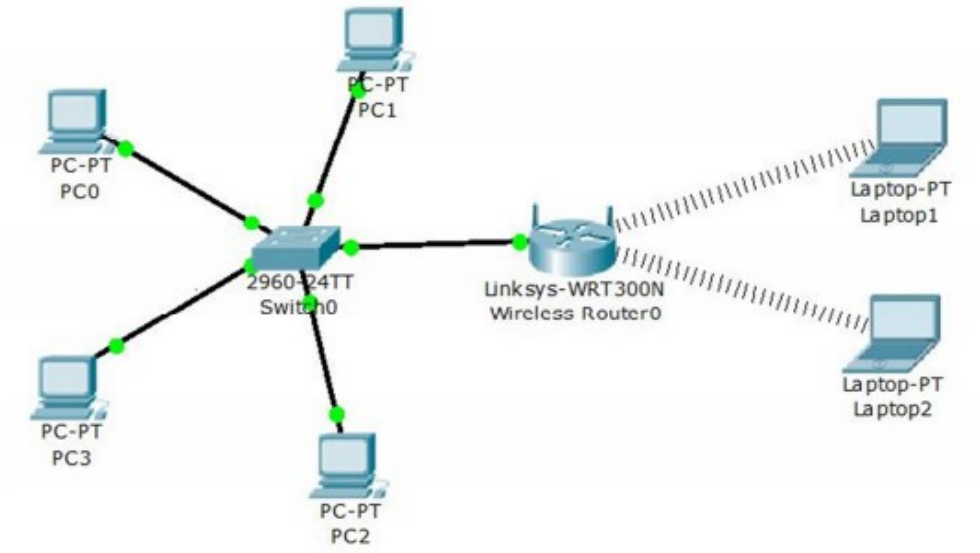
Há uma constante mudança e, com a globalização do mercado e o desenvolvimento da tecnologia da informação (TI), as organizações estão enfrentando novas realidades e métodos de desenvolvimento de negócios, e precisam ajustar sua estrutura, organização e planos para poder responder novos desafios e melhorar a tomada de decisão competitiva. A segurança da informação é um conjunto de processos, atividades, pessoal e tecnologias que envolvem a coleta de dados relevantes, o armazenamento necessário, o processamento de dados e o fornecimento de informações a quem delas precisa. A implantação de sistemas de informação em uma organização não traz benefícios e nem resolve todos os problemas por si só, é preciso estar atento ao treinamento dos usuários, procedimentos rotineiros, mudanças de regras e responsabilidades.

2.1 Redes de Computadores

Morimoto (2008), diz que a primeira rede de computadores teve início na década de 1960, para transferir informações de um computador ao outro. Nessa época, eram utilizados cartões perfurados como forma de armazenamento. Com o desenvolvimento da tecnologia, hoje é utilizado até uma rede sem fio para transferir os dados. A figura 1 mostra uma rede de quatro computadores conectados através de um switch, por cabo de rede, e uma rede sem fio para conectar os notebooks e

o roteador wireless. Nessa topologia é possível que os dados sejam transferidos entre todos os hosts

Figura 1 – Redes de computadores cabeada e sem fio



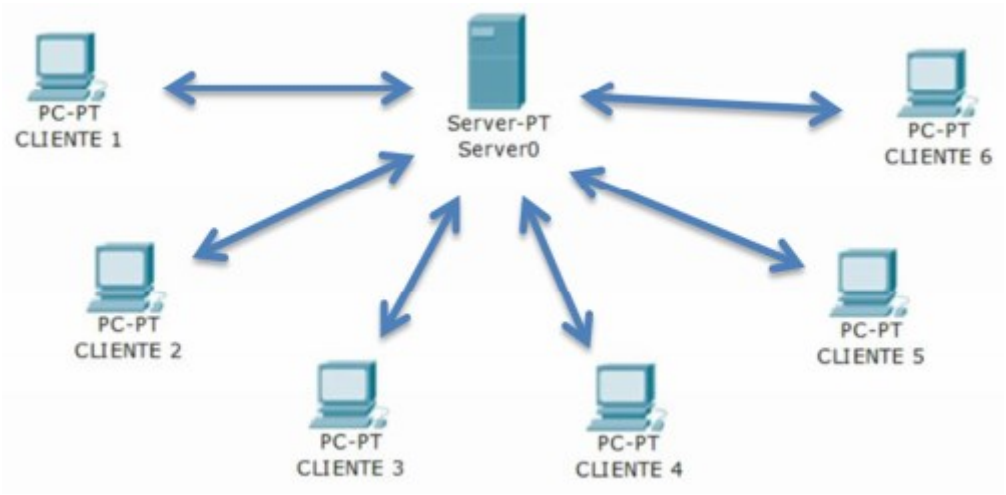
Fonte: Autor, utilizando a ferramenta packet tracer (CISCO)

Para Miranda(2008), uma rede de computadores é um conjunto de computadores conectados entre si, de maneira que possa haver comunicação de dados localmente e/ou remotamente, incluindo todos os equipamentos eletrônicos, como microcomputadores e impressoras.

Cantú(2003) explica que elas possem suas aplicações, que vão desde comercial, utilizando os recursos de compartilhamentos, programas, impressoras, e-mails, telefones IP dentre outros, e também para aplicações domésticas, que

podem ser compartilhamentos de arquivos, impressoras, informações educativas e redes sociais, músicas, filmes e jogos, comunicadores instantâneos etc.

Figura 2 – Modelo cliente-servidor – Compartilhamento de informações



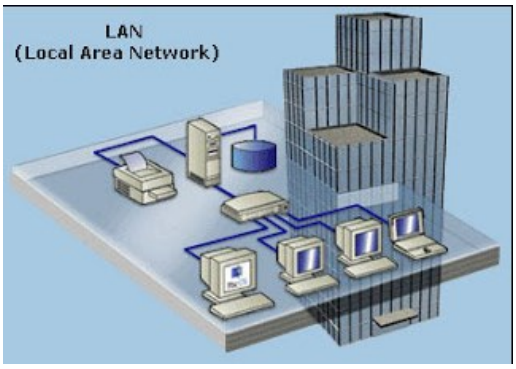
Fonte: Autor, utilizando a ferramenta packet tracer (CISCO)

O mundo corporativo não pode existir sem uma rede de computadores, pois há a necessidade de compartilhamento de dados, comunicação entre funcionários e equipamentos. Entretanto, as redes de computadores existem de diversas formas, conforme será descrito abaixo.

2.1.1 LAN (Local Area Networks)

É o modelo mais habitual que utilizado, até mesmo dentro de casa. Conecta dispositivos próximos em um mesmo ambiente, por meio de cabos.

Figura 3 – Rede LAN

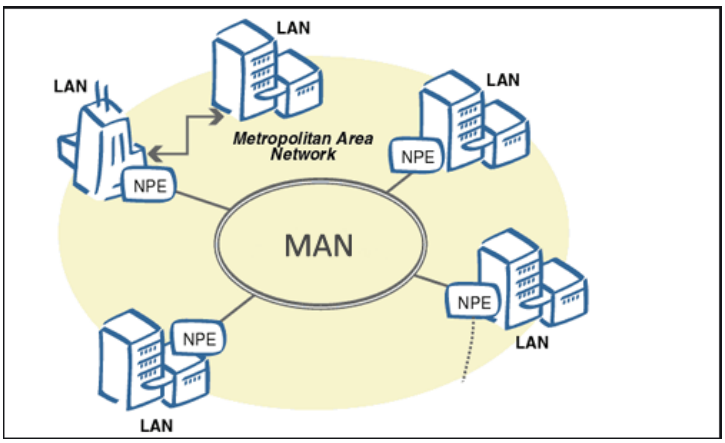


Fonte: https://informaticaeadministracao.files.wordpress.com/2014/04/redes_lan.jpg

2.1.2 MAN (Metropolitan Area Network)

É utilizada conectar redes locais dentro de distancias maiores. Pode ser utilizada para conectar escritórios que estão no mesmo município ou cidades vizinhas, e até alguns quilômetros.

Figura 4 – Rede MAN

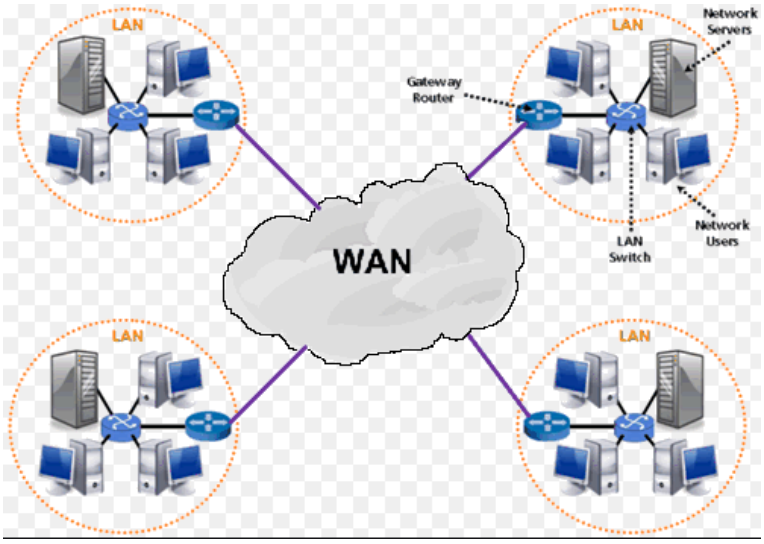


Fonte: https://informaticaeadministracao.files.wordpress.com/2014/04/man2.png

2.1.3 WAN (Wide Area Network)

Tem uma cobertura maior do que as redes Lan e Man, e possibilita a comunicação de equipamentos em diferentes localidades, alcançando a distância entre países e até continentes.

Figura 5 – Rede WAN



Fonte: https://www.criandobits.com.br/redes/img/wan.gif

2.1.4 PAN (Personal Area Network)

A rede PAN é uma rede de área pessoal, com maior alcance. Conecta aparelhos que estão bem próximos, como um bluetooth.

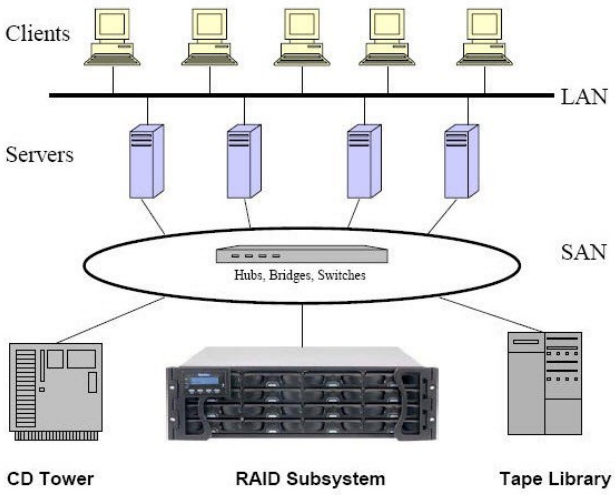
Figura 6 – Rede PAN

Fonte: https://pplware.sapo.pt/wp-content/uploads/2010/12/pan.jpg

2.1.5 SAN (Storage Area Network)

Existe para fazer a comunicação entre servidores de armazenamento, e com ela fazer o compartilhamento de dados.

Figura 7 – Rede SAN

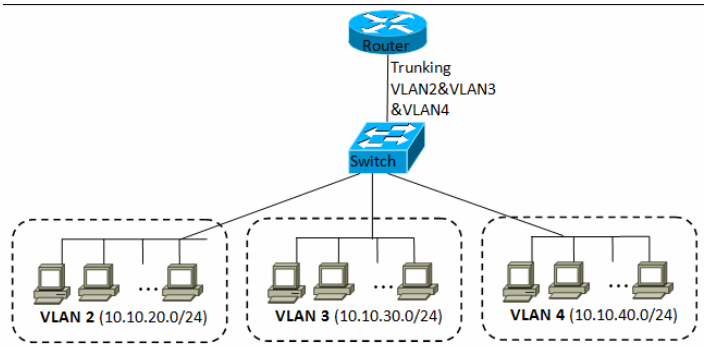


Fonte: https://pplware.sapo.pt/wp-content/uploads/2010/12/SAN_00.jpg

2.1.6 VLAN (Virtual LAN)

Reúne diversas redes de uma LAN, mas de forma lógica. Dessa forma, pode-se dividir uma Lan física em diversas Lans virtuais

Figura 8 – Rede VLAN



Fonte: https://under-linux.org/attachment.php?attachmentid=51269&d=1397496211

Como em qualquer outra área, as redes de computadores precisaram se adaptar ao uso das tecnologias sem fio. Além de todas as alternativas citadas as redes LAN, MAN e WAN também contam suas versões wireless, se tornando WLAN, WMAN ou até mesmo WWAN.

Por fim, as redes de computadores são um conjunto de equipamentos conectados e compartilhando recursos. A distância entre esses equipamentos é que irão nos dizer que tipo de tecnologia estão empregadas. Uma empresa pode utilizar diversos tipos de redes, até que atenda suas necessidades.

2.2 IDS (Intrusion Detection System ou Sistema de detecção de intrusão)

A detecção de intrusão é a arte de detectar algo inapropriado, incorreto ou atividade anômala. Entre outras ferramentas, um Sistema de Detecção de Intrusão

pode ser usado para determinar se uma rede de computador ou servidor apresentou uma falha ou intrusão não autorizada.

2.3 HIDS (Host-based Intrusion Detection System ou Sistema de detecção de intrusão baseado em host).

Um IDS de host precisa ser implantado em cada máquina protegida (servidor ou estação de trabalho). Ele analisa os dados locais dessa máquina, como arquivos de log do sistema, trilhas de auditoria e alterações no sistema de arquivos e, às vezes, processos e chamadas do sistema. O HIDS alerta o administrador caso ocorra uma violação das regras predefinidas. O IDS do host pode usar correspondência de padrões nas trilhas de auditoria observadas ou gerar um perfil padrão de comportamento e, em seguida, compara os eventos atuais com este perfil.

2.4 IPS (Intrusion Prevention System ou Sistema de prevenção de intrusão)

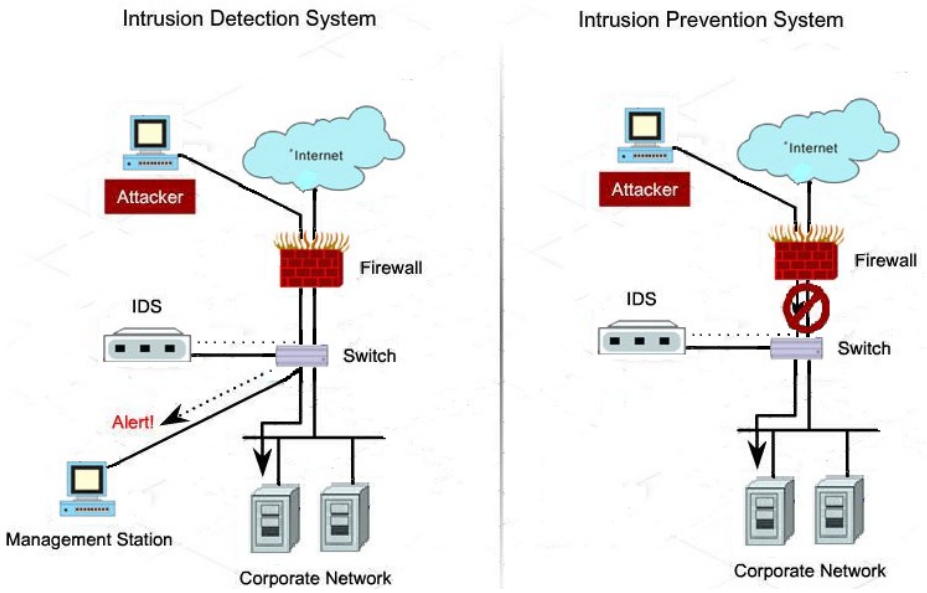
Um sistema de prevenção de intrusão é usado para descartar pacotes de dados ativamente ou desconectar conexões que contenham dados não autorizados. Prevenção de intrusão a tecnologia também é comumente a uma extensão da tecnologia de detecção de intrusão.

2.5 NIPS (Network Intrusion Prevention System ou Sistema de prevenção de intrusão baseado em rede)

Sistema baseado em um dispositivo inline, que pode ser um roteador ou um switch, pois eles repassam os pacotes entre as redes. Sempre que um ataque é identificado, são tomadas decisões baseadas em regras pré-definidas, e são essas regras que irão bloquear o ataque suspeito. O NIPS apresenta a propriedade de

efetuar drop na conexão, impedindo, dessa forma, que os pacotes cheguem ao seu destino, tal como os firewalls atuam.

Figura 9 – Funcionamento de IDS e IPS



Fonte: https://upload.wikimedia.org/wikipedia/commons/1/13/Ips-vs-ids-short.png

Figura 10 – IDS x IPS

Fonte: https://blog.starti.com.br/content/images/2019/09/Design-sem-nome--4-.jpg

3 SUGESTÕES E PREOCUPAÇÕES DE ARQUITETURA

A arquitetura do IPS e IDS se apresenta como uma solução que proporcionará um alto retorno no investimento com base na visibilidade, controle e tempo de atividade. A arquitetura também tem em mente que muitas empresas implementaram uma solução parcial ou total da solução para detecção ou prevenção de intrusão. Usando uma implantação híbrida, que é a mistura de duas tecnologias no mesmo ambiente, como Windows e Linux, a média das empresas de médio a grande porte será capaz de melhorar e desenvolver a tecnologia de ponta fornecida pelo IPS, ao mesmo tempo que aproveita as vantagens das capacidades comprovadas e desenvolvidas do IDS.

4 IDS - SITEMA DE DETECÇÃO DE INTRUSÃO

Primeiro, examinar a implementação tradicional do IDS. A maioria das empresas que possuem IDS instalados colocaram esses dispositivos no perímetro, entre o roteador de borda e firewall ou colocaram o IDS fora do roteador de borda.

O IDS coleta informações e dados e analisa seu comportamento em busca de comportamentos anormais. Nessa coleta, são armazenados os fluxos de dados e horários, e são comparados com padrões de ataques. Dessa forma é possível avaliar um possível evento malicioso.

As empresas que se esforçaram para instalar um IDS fora do firewall e roteador de borda fizeram isso para que possam ver toda a amplitude de tentativas de ataque contra sua organização. Ao implantar um IDS, ambos dispositivos de perímetro externos e dentro dos dispositivos de perímetro, uma empresa pode confirmar a tempo ou não se um potencial ataque visto de fora do perímetro conseguiu passar por roteadores de borda e firewalls internos. A abordagem posterior requer mais recursos, mas fornece uma imagem mais clara em uma empresa o ponto de entrada/saída e postura de segurança. Ter um IDS em qualquer um destes locais também fornecem uma ferramenta que captura dados para uma possível análise forense conforme necessário.

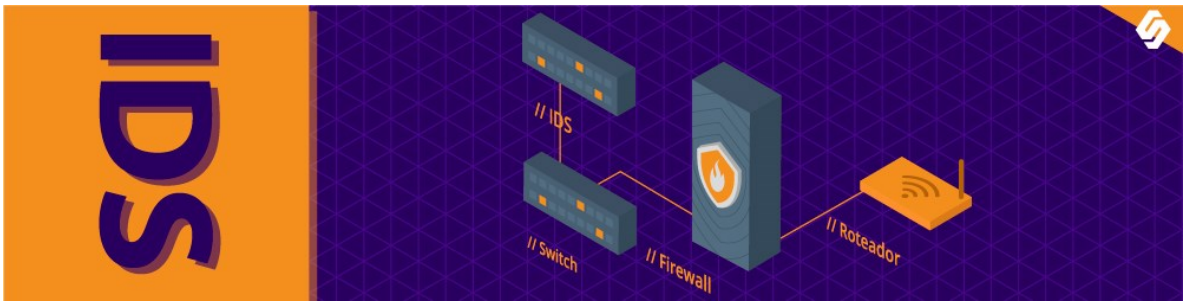
A maioria das empresas implantam dispositivos IDS fora da arquitetura de banda. Isso significa que o IDS fica em uma mídia compartilhada e captura pacotes para poder manipular em um modo promíscuo e reporta esses dados de volta para um console de gerenciamento. Outra forma de implantar um IDS no perímetro é o que é chamado de implantação em linha. Isso significa que todos os dados que entram e saem de uma empresa passam por este dispositivo. Outro exemplo de dispositivo que usa uma arquitetura em linha é um roteador ou firewall. Ter um IDS embutido significa que todos os dados serão capturados antes de continuar na rede corporativa. A desvantagem desse tipo de arquitetura é que, se o dispositivo em linha falhar, dependendo da configuração, todos os dados continuarão sem identificação ou irá parar até que o IDS seja consertado ou removido. Qualquer uma

dessas implantações de IDS em linha coloca a empresa em risco se o dispositivo falhar.

O conceito mais importante na implantação de um IDS é que é uma ferramenta usada para capturar e fornecer visibilidade em uma rede corporativa. Para empresas maiores e empresas que têm uma necessidade adicional de visibilidade total no tráfego de rede, um método de implantação comum é instalar dispositivos IDS em todos os pontos de rede para fornecer visibilidade interna e externamente. Esse tipo de implantação fornece dados necessários para rastrear ameaças internas potenciais também como ameaças externas. Ainda hoje o maior o risco vem de ameaças internas. Funcionários insatisfeitos, funcionários curiosos, serviços terceirizados e as tendências de maiores volumes de serviços contratados fornecem um nível mais alto de vulnerabilidade de dentro da rede. Como resultado,

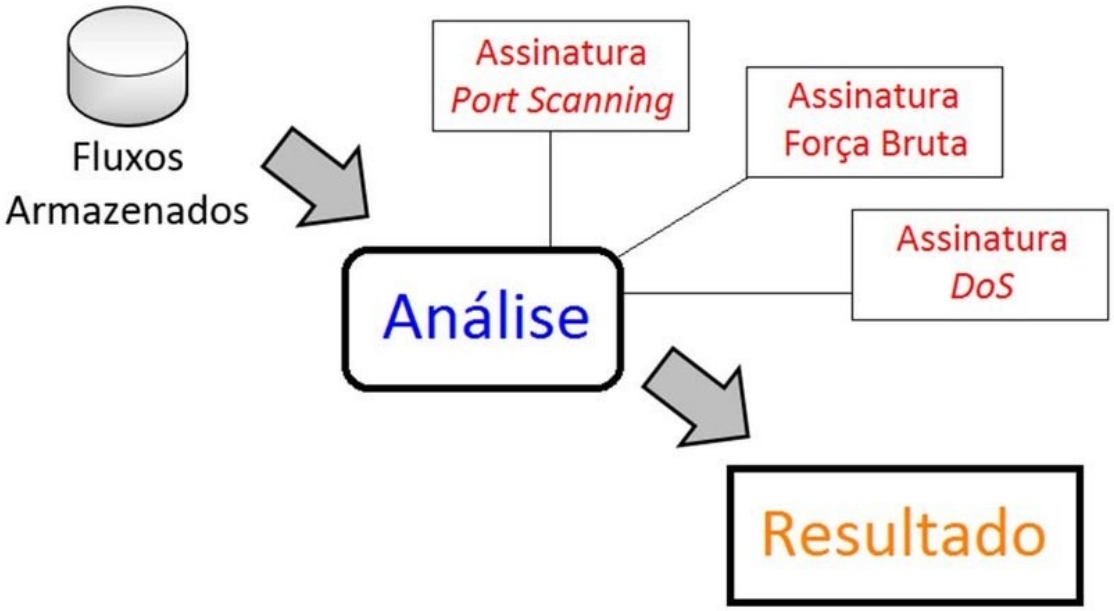
importância de implantar um mecanismo para monitorar o tráfego interno é fundamental. A chave que está sendo enfatizada neste ponto é a visibilidade.

Figura 11 – Trânsito do IDS



Fonte: https://www.softwall.com.br/wp-content/uploads/ilustra-blog-cada-um-atua-ids.jpg

Figura 12 – Funcionamento do IDS



Fonte:https://www.researchgate.net/figure/Figura-1-Funcionamento-do-IDS_fig1_320482247

Uma preocupação das implantações de IDS é o fator de desempenho. As soluções IDS oferecidas hoje percorreram um longo caminho no design e no uso de

componentes de alto desempenho que ajudam a garantir a maior captura de dados. Mesmo com componentes de alto desempenho e software atualizado, um fato conhecido é que as implementações atuais de IDS tendem a descartar pacotes devido a alto taxa de transferência dos dispositivos de rede de alta largura de banda de hoje. Desempenho é um problema em uma implementação de IDS e IPS. Outra preocupação com implantações de IDS é criptografia. Atualmente, a maioria das soluções IDS não tem a capacidade de descriptografar pacotes de entrada ou saída e isso cega os administradores de segurança quanto ao que está entrando e saindo de redes corporativas. Com o crescimento explosivo de VPN e outros fluxos de dados criptografados, a necessidade de ter uma solução como IPS em o perímetro está se tornando cada vez mais necessário.

5 IPS – SISTEMA DE PREVENÇÃO DE INTRUSÃO

O IPS é uma tecnologia que atua na prevenção de ameaças. É uma solução ativa, diferente do IDS, que atua mais passivamente.

Tecnologias IPS em software ou hardware são relativamente novos. Pode-se dizer que a ideia existe há um muito tempo e pode sugerir que listas de controle de acesso de roteador ou regras de firewall podem ser considerados um IPS básico. Quando você combina os recursos de bloqueio de um firewall com a inspeção profunda de pacotes de um IDS, você obtém os sistemas de prevenção de intrusão ou IPS. A verdade é que o mercado de IPS está apenas começando a amadurecer o suficiente para realmente identificar o que realmente é um IPS. Ainda hoje existem muitas definições para IPS e muitos pontos de vista quanto aos requisitos para implementações IPS. Alguns grupos sugerem que o IPS é uma evolução do IDS e que eventualmente o IDS irá desaparecer e todos os produtos relacionados à intrusão se concentrarão na prevenção. Uma empresa pelo nome da Sourcefire está trabalhando em um termo e linha de produtos que combina várias tecnologias no que é chamado de “Conscientização de Rede em Tempo Real (Real-time Network Awareness - RNA)”. RNA permite que as organizações protejam suas redes com mais segurança por meio de uma combinação única de patente pendente de descoberta de rede passiva, comportamental criação de perfis e análise de vulnerabilidade integrada para oferecer os benefícios de tempo real perfil de rede e gerenciamento de mudanças sem as desvantagens das tradicionais abordagens para identificar ativos de rede e vulnerabilidades.

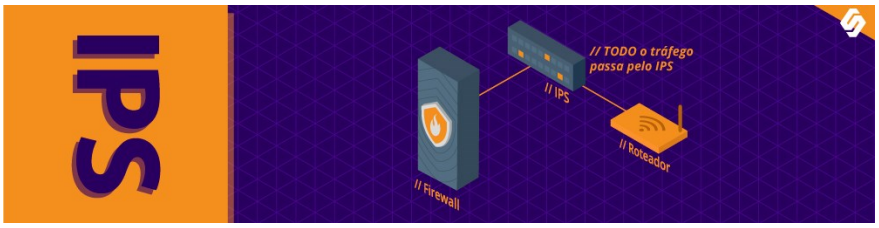
A realidade é que o tempo dirá ou não se IDS será colocado em museu, a necessidade de captura e rastrear dados que cruzam nossas redes será de suma importância. Além de as tecnologias de RNA da Sourcefire que estão tentando preencher a lacuna entre IPS e IDS, outras empresas estão construindo tecnologias IPS em torno da premissa de identificar e parar as intrusões, monitoramento e captura de dados para análise forense.

A ideia de um IPS negando tráfego é o aspecto mais importante a respeito deste papel. Muitas empresas implantaram a tecnologia IDS ou IPS por um motivo principal. Esse motivo é que tempo é dinheiro e a disponibilidade da rede é fundamental para todas as organizações. O argumento pode ser feito que uma implantação de IPS ou IDS é na verdade uma tecnologia que ajuda a garantir que a rede continue em atividade e disponibilidade, identificando e possivelmente evitando invasões de rede e ataques que normalmente seriam a causa do tempo de inatividade da rede. Os custos associados a uma implantação IPS ou IDS não são

normalmente associados como uma despesa geradora de receita. Em muitos casos, pode-se argumentar que a decisão de implantar a tecnologia IPS ou IDS é como a analogia do ovo e da galinha. Como as implantações de IPS e IDS não geram receita diretamente, é difícil justifique a despesa. No entanto, o oposto deste argumento é que sem visibilidade na rede e a capacidade de evitar invasões e ataques um aumento potencial dos custos associados ao tratamento de tais atividades. Um argumento poderia ser que com uma implantação IPS configurada corretamente, uma empresa poderia economizar dinheiro através da identificação e prevenção de ataques de worm ou vírus.

Como empresas desenvolvem matrizes para quantificar a quantidade de dinheiro e/ou tempo perdido devido ao vírus ou ataques de worm, eles terão as informações de suporte para justificar os custos associado a implantações de IPS e/ou IDS. À medida que as empresas começam a perceber a economia potencial associada à prevenção o tempo de inatividade associado a um dos ataques quase semanais de worm ou vírus eles estarão mais inclinados a alavancar medidas preventivas como IPS tecnologias. Da mesma forma, o uso de tecnologias IDS pode ser usado para confirmar a economia de tempo e fornecer os dados necessários para lidar com ameaças internas. Sobre os últimos anos, vimos um aumento no nível de responsabilidade associado com o uso de tecnologia. Os múltiplos requisitos de conformidade cobrados sobre empresas de organizações federais também colocam os departamentos de TI em alerta de o ponto de vista de ter que fornecer políticas, procedimentos e recursos para garantir boas práticas e implantações de tecnologia. Usando uma combinação de IPS e as tecnologias IDS aumentarão claramente o nível de visibilidade e controle para redes corporativas.

Figura 13 – Trânsito de um IPS



Fonte: https://www.softwall.com.br/wp-content/uploads/ilustra-blog-cada-um-atua-ips.jpg

É aí que surge a sugestão de tecnologias IPS e IDS existindo em harmonia vem para suportar. A recomendação é colocar estrategicamente a tecnologia IPS no perímetro da rede corporativa para ajudar na prevenção de zero ataques diários, como worms ou vírus, por meio de regras baseadas em anomalias, bem como inspeção de pacotes baseada em assinatura. O uso de um sistema devidamente ajustado e gerenciando a solução IPS em todos os pontos de entrada/saída corporativos ajudará a garantir que o ameaças mais recentes e identificadas anteriormente são descartadas. Como novas tecnologias e aplicativos são desenvolvidos, é fundamental que a equipe que gerencia o IPS seja envolvida durante o desenvolvimento para garantir que o tráfego legítimo tenha permissão para passar. Normalmente, há maior latitude para o tráfego sendo interrompido ou interrompido no perímetro da rede do que dentro da rede.

Este tempo de atividade da rede interna é onde a implantação da tecnologia IDS ainda é crítica. A maioria das arquiteturas IDS fornecem um meio passivo de coletar e identificar mal-intencionado ou desconhecido atividade e alertando uma equipe para iniciar a investigação de tal atividade. O trânsito continua a passar e os negócios continuam normalmente, mas neste caso qualquer atividade suspeita é sinalizada para investigação. Usando este tipo de arquitetura promove o tempo de atividade ao mesmo tempo em que enfatiza a necessidade de monitorar alguma ameaça. Ter uma implantação de IPS nas partes externas da rede irá fornecer as medidas preventivas e de controle necessárias para combater ameaças novas e existentes

Enquanto inclui um IDS dentro do firewall e em nó de rede interna crítica fornecerá visibilidade e confirmação quanto à atividade interna. Os custos associados com este tipo de implantação são muito menores do que aqueles necessários para implantar ambas as tecnologias em paralelo. Um aspecto fundamental que precisamos cobrir é a equipe e treinamento porque as pessoas são um recurso essencial necessário em qualquer um desses implantações para ter sucesso.

Temos também o NIPS (Network Intrusion Prevention System), uma tecnologia que utiliza o software instalado em dispositivos online de rede computador. Exemplos de dispositivos online: os roteadores e switches que são responsáveis por repassar pacotes IP’s entre redes. Seu principal objetivo é verificar

pacotes de dados que passam por ele no segmento de rede que ele monitora. Ele inspeciona cada pacote que passa e verifica por qualquer indicação de exploração de vulnerabilidade. Quando identificado um ataque, ele toma as devidas decisões baseadas em suas regras existentes, sendo assim ele pode bloquear o tráfego suspeito.

6 USO NA PRÁTICA

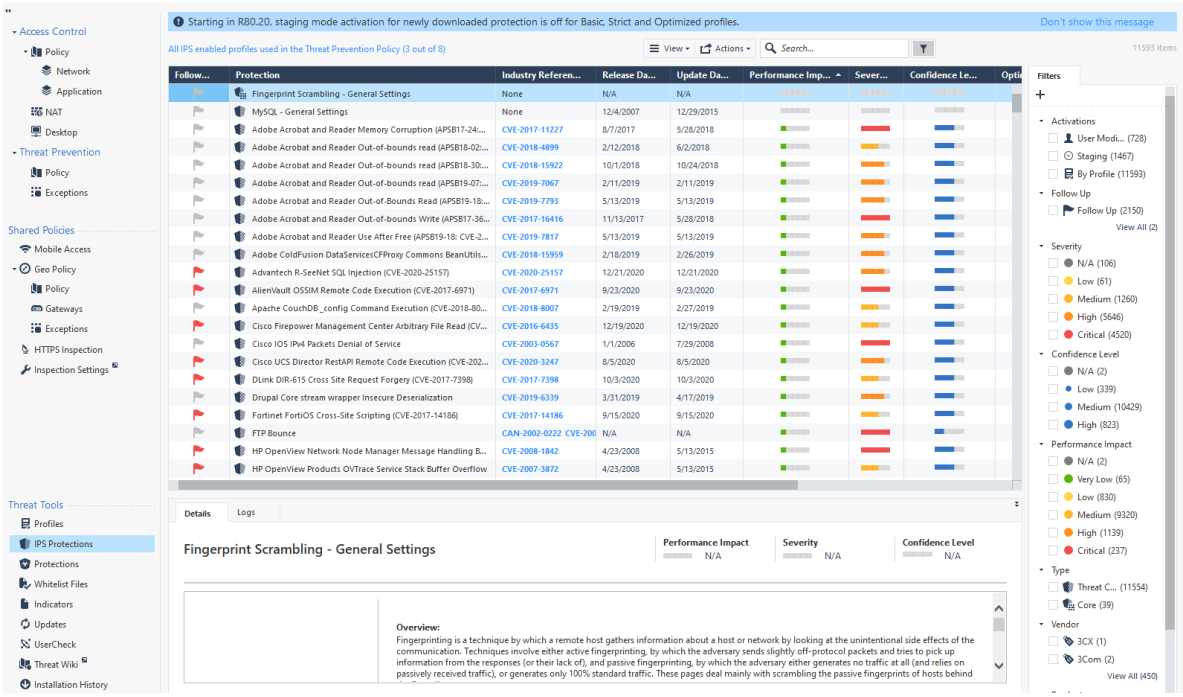
Na prática, onde tudo acontece, o IPS e IDS atuam de forma semelhantes, mas sua postura e decisão são diferentes. IPS protege e IDS detecta.

6.1 IPS

Abaixo mostra a prática de como funciona uma ferramenta conhecida por médias e grandes empresas. A empresa que desenvolve essa solução chama-se Checkpoint. A ferramenta é um SMA (Security Management Appliances ou Dispositivos de gerenciamento de segurança). Por motivos de segurança, não será citado o modelo nem versão em uso para evitar exploração e falhas de versões. A solução mostrará como obter eficiência, alta visibilidade e recursos de gerenciamento de segurança simultâneos.

O software que gerencia seu uso é o Checkpoint SmartConsole R80 (há versões que partem de 80 a 83). A SmartConsole será a blade de IPS e seu banco de dados que é atualizado constantemente através de uma comunicação direta com os servidores da Checkpoint. Cada vulnerabilidade publicada é automaticamente enviada ao appliance para que esteja sempre atualizado.

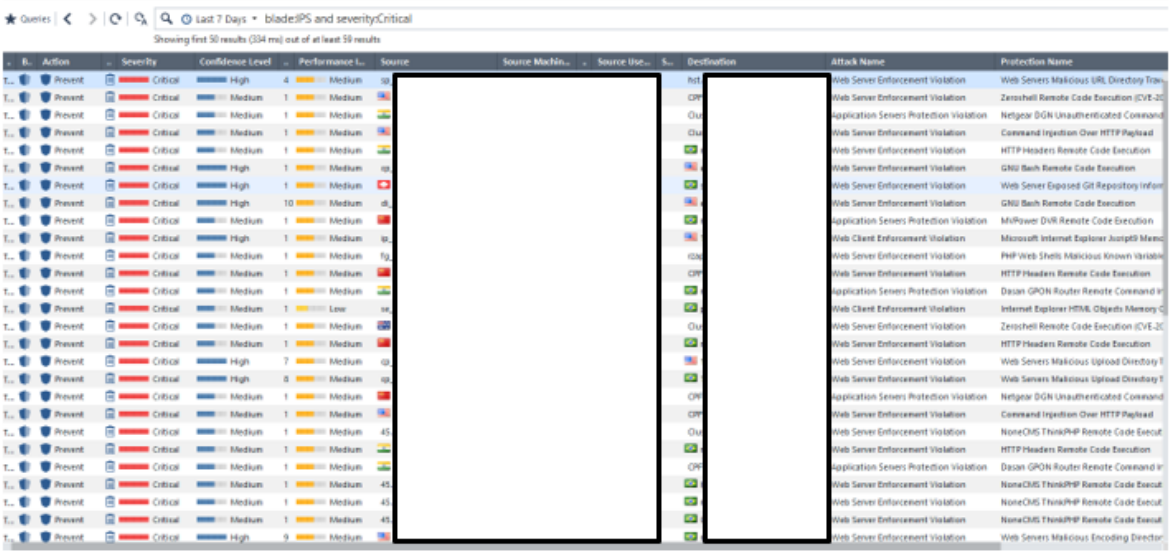
Figura 14 – Checkpoint SmarConsole



Fonte: Imagem retirada do ambiente de trabalho

Os logs permitem acompanhar todo tipo de ataque que acontece contra a empresa e nosso IPS entra em ação. Abaixo, nota-se que houve diversas tentativas de intrusão de diversos locais.

Figura 15– Logs Checkpoint SmarConsole - Blade IPS



Fonte: Imagem retirada do ambiente de trabalho

Explica-se abaixo os campos *Action (ação), Severity (severidade), Confidence Level (nível de confidencialidade) e performance impact (performance de impacto).*

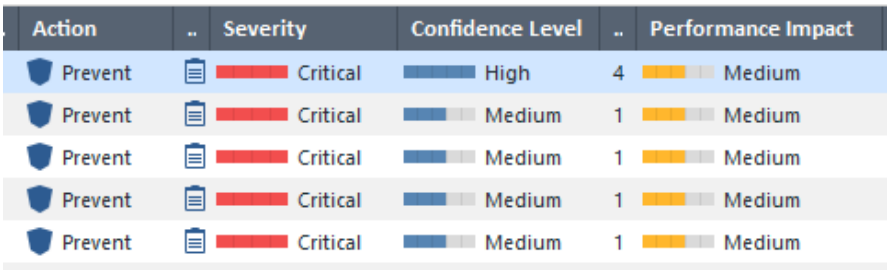
Action informa qual foi a ação tomada para esse ataque. Neste exemplo, o IPS fez sua função corretamente, que é prevenir. Se fosse IDS, seria *Detection*.

Severity mostra o nível de criticidade, ou o quão poderoso pode ser o ataque.

Confidence level leva até o nível de confidencialidade aquele alvo foi classificado. Esse nível pode ser obtido através da IA ou por polices/rules (políticas e regras) dentro do appliance.

O *Performance Impact* será o nível de impacto no negócio. O tamanho do estrago que ele causaria no ambiente. Também pode ser configurado através da IA ou por polices/rules (políticas e regras) dentro do appliance.

Figura 16 – Logs Checkpoint SmarConsole - Blade IPS - Detalhes



Action	..	Severity	Confidence Level	..	Performance Impact
Prevent		Critical	High	4	Medium
Prevent		Critical	Medium	1	Medium
Prevent		Critical	Medium	1	Medium
Prevent		Critical	Medium	1	Medium
Prevent		Critical	Medium	1	Medium

Fonte: Imagem retirada do ambiente de trabalho

Na próxima imagem será demonstrado o *Source (Origem), Source User (Usuário de origem), Destination (Destino), Attack Name (Nome do ataque) e Protection Name (Nome da proteção).*

O *Source* mostra a origem de onde partiu o ataque. A imagem mostra o país de origem apenas por entender o IP.

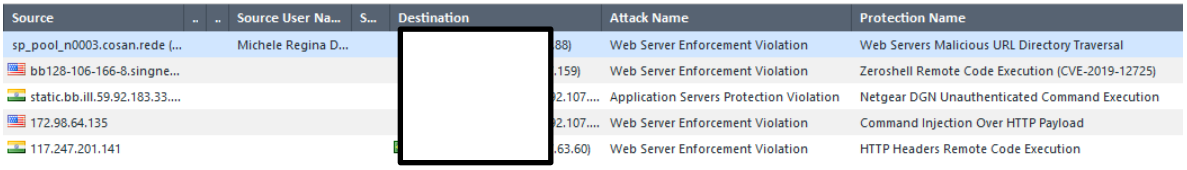
Já *Source user* aparece apenas quando é um ataque interno ou identificado. O atacante pode utilizar um recurso dentro da empresa para efetuar o ataque, este é muito comum em casos que o usuário esteja infectado com algum malware e o atacante tem poder sobre aquele computador.

Destination será o destino do ataque, e na imagem foi ofuscado por questões de segurança, mas sempre é um endereço interno, sendo um servidor ou o próprio equipamento de rede.

O *Attack name* informa o método utilizado pelo atacante. Neste exemplo foi um Web Server Enforcement Violation, ou ataque de força.

No *Protection Name* é a proteção entrando em ação e salvando a infraestrutura. No caso, foi utilizado a vacina para *Web Servers Malicious URL Directory Traversal.*

Figura 17 – Logs Checkpoint SmarConsole - Blade IPS – Detalhes ataque



Source	..	..	Source User Na...	S...	Destination	Attack Name	Protection Name
sp_pool_n0003.cosan.rede (...			Michele Regina D...		[redacted]	Web Server Enforcement Violation	Web Servers Malicious URL Directory Traversal
bb128-106-166-8.singne...						Web Server Enforcement Violation	Zeroshell Remote Code Execution (CVE-2019-12725)
static.bb.ill.59.92.183.33....						Application Servers Protection Violation	Netgear DGN Unauthenticated Command Execution
172.98.64.135						Web Server Enforcement Violation	Command Injection Over HTTP Payload
117.247.201.141						Web Server Enforcement Violation	HTTP Headers Remote Code Execution

Fonte: Imagem retirada do ambiente de trabalho

6.2 IDS

O IDS utilizado no Checkpoint é utilizado em modo medium, já que a blade mais ativa é o IPS. Por conta do consumo de recurso das caixas (servidores em Cluster), ele precisa ser bem otimizado, pois a proporção de detecções é quase três vezes maior do que a proteção. Isso se dá por conta dos falsos positivos, que são detectados, analisados e descartados como possíveis ameaças.

Abaixo as colunas mais importantes, como *Destination, HTTPS Validation, Service e Description*. Normalmente indentifica os ofensores nessas 3 colunas. Infelizmente por conta de informações da empresa não serão mostrados os resultados, apenas que foi detectado algo com comportamento atípico na porta *TCP/443* (HTTPS) acessando o endereço *herah.com.br*

Figura 18 – Logs Checkpoint SmarConsole - Blade IDS – Detalhes ataque

Action	HTTPS Inspec...	Source	Destination	HTTPS Validation	Service	Source User...	Source Machine...	Description
Detect		ra_medi_e09.cos...	ec2-3-215-87...	Invalid CRL Retrieved	https (TCP/443)	Analice da Silva...	ra_medi_e09@cos...	herah.com.br Detected
Detect	Inspect	ra_medi_e09.cos...	ec2-3-215-87...	Invalid CRL Retrieved	https (TCP/443)	Analice da Silva...	ra_medi_e09@cos...	herah.com.br Detected
Detect		ra_medi_e09.cos...	ec2-3-215-87...	Invalid CRL Retrieved	https (TCP/443)	Analice da Silva...	ra_medi_e09@cos...	herah.com.br Detected
Detect		ra_medi_e09.cos...	ec2-3-215-87...	Invalid CRL Retrieved	https (TCP/443)	Analice da Silva...	ra_medi_e09@cos...	herah.com.br Detected
Detect		ra_medi_e09.cos...	ec2-3-215-87...	Invalid CRL Retrieved	https (TCP/443)	Analice da Silva...	ra_medi_e09@cos...	herah.com.br Detected
Detect		ra_medi_e09.cos...	ec2-3-215-87...	Invalid CRL Retrieved	https (TCP/443)	Analice da Silva...	ra_medi_e09@cos...	herah.com.br Detected
Detect		ra_medi_e09.cos...	ec2-3-215-87...	Invalid CRL Retrieved	https (TCP/443)	Analice da Silva...	ra_medi_e09@cos...	herah.com.br Detected
Detect		ra_medi_e09.cos...	ec2-3-215-87...	Invalid CRL Retrieved	https (TCP/443)	Analice da Silva...	ra_medi_e09@cos...	herah.com.br Detected
Detect		ba_medi_e28.co...	ec2-3-215-87...	Invalid CRL Retrieved	https (TCP/443)	Elza de Lourdes...	ba_medi_e28@co...	herah.com.br Detected
Detect		sf_spat_e10.cos...	ec2-3-215-87...	Invalid CRL Retrieved	https (TCP/443)	Yan Gonçalves d...	sf_smed_e13@cos...	herah.com.br Detected
Detect		sf_spat_e10.cos...	ec2-3-215-87...	Invalid CRL Retrieved	https (TCP/443)	Yan Gonçalves d...	sf_smed_e13@cos...	herah.com.br Detected

Fonte: Imagem retirada do ambiente de trabalho

7 RECURSOS E TREINAMENTOS

Um dos maiores desafios hoje é encontrar e manter pessoas qualificadas em ferramentas de segurança. A implantação de tecnologia IPS ou IDS requer habilidades especializadas que administradores de rede e sistemas típicos não têm. Normalmente um especialista de segurança vem de uma formação que inclui experiência de trabalho em rede ou administração de sistemas e, às vezes, em ambos. No entanto, as habilidades adicionais e especializadas associadas à análise e relatórios de segurança não são habilidades que um funcionário desenvolve, a menos que receba este treinamento especializado por meio de cursos ou integrando equipe de segurança.

Pelo fato da tecnologia IPS ser relativamente nova, existem poucos cursos disponíveis, tanto treinamentos genéricos como específico do fornecedor. É certo que muitas das habilidades associadas com o suporte IDS é diretamente mapeado para suportar tecnologias IPS; entretanto, existem alguns aspectos que são desconhecidos e só serão desenvolvidos com o tempo. Empresas com orçamentos apertados ou que atualmente não possuem um título a arquitetura em vigor considerará a equipe e o treinamento os mais desafiadores. Estas empresas provavelmente canibalizarão seus sistemas e equipes de rede para construir o grupo necessário para apoiar as tecnologias IPS e IDS.

Dependendo da iniciativa da equipe e apoio da gestão para este tipo de organização irão determinar o sucesso de uma implantação de IPS e/ou IDS. Empresas com equipe completa de segurança também encontrarão o desafio de encontrar, treinar e manter engenheiros altamente qualificados são desanimadores ao adicionar IPS a uma arquitetura IDS existente. Uma área chave que certamente receberá cobertura adicional em breve será a remodelação das equipes de TI para atender aos requisitos de segurança emergentes.

Existem empresas que estão percebendo a necessidade de desenvolver pessoal para atender as diversas questões de conformidade sendo cobradas de suas organizações por agências federais. Há também uma área que não foi discutida e que exigirá a atenção de TI gerentes e é assim que os requisitos de pessoal mudarão conforme as tecnologias mudança. Atualmente, a defesa contra vírus e worms geralmente recai sobre os ombros dos administradores de sistemas

para corrigir e manter as definições de vírus em todos servidores e sistemas de desktop.

A maioria das empresas também empregam analistas e instrutores que fornecem comunicação e treinamento aos usuários sobre a conscientização para ajudar a evitar a propagação de vírus e worms. Alguns analistas podem argumentar que com a implementação de uma configuração e mantida a arquitetura IPS, uma empresa colherá os benefícios de precisar de menos administradores de desktop e administradores de sistema atualmente necessários para que se mantenha atualizado com as definições de patches e antivírus em resposta a worm e vírus lançamentos. Essa mudança pode, facilmente, resultar na reformulação da rede e dos sistemas administradores, bem como outras equipes importantes de TI para adquirir as habilidades necessárias para gerenciar e oferecer suporte a um novo ambiente de segurança.

8 CONSIDERAÇÕES FINAIS

Este conteúdo teve como objetivo principal entender como funciona um IDS e IPS e compararmos suas funcionalidades. A introdução a redes de computadores e segurança da informação demonstra como interceptar um dado e tratá-lo de forma que fosse disseminado e analisado profundamente.

A análise de dados deste estudo permitiu concluir que à medida que mais e mais tráfego de rede tornam-se criptografado, IDSs tornam-se inúteis porque não podem analisar pacotes criptografados. Conforme o tráfego de redes aumenta, eles normalmente veem apenas uma pequena quantidade de tráfego em sua rede. Em uma rede comutada, você precisa aumentar muito o número de sensores de detecção de intrusão para monitorar tráfego em todos os segmentos da rede. Em grandes redes, isso significa que o total do custo de propriedade de IDSs pode ser muito alto. Pode-se reparar que os IDSs geram muitos falsos positivos, informando que a rede está sendo atacada, quando não está.

A partir dessas conclusões entende-se o que estão levando muitas empresas a mudar para IPSs.

9 REFERÊNCIAS

O que são e quais os tipos de redes de computadores – Disponível em https://netsupport.com.br/blog/redes-de-computadores/. Acesso em 27 de mar 2021

História das Redes. Disponível em https://www.hardware.com.br/tutoriais/historia-redes/. Acessado em 20/03/2021

MIRANDA, Anibal D. A. Introducao a redes de computadores, 1º ed. 2008 - ESAB - Escola Suporior Aberta do Brasil – Download PDF em 20/03/2021

CANTÚ, Evandro. Redes de computadores e Internet, CEFET/SC - Download PDF em 20/03/2021

Como Funciona um IDS? Disponível em: https://www.gta.ufrj.br/grad/16_2/2016IDS/conceituacao.html. Acessado em 11, jan. 2021.

O que é um sistema IPS? Disponível em: https://www.portalgsti.com.br/sistema-prevencao-intrusos/sobre/. Acessado em 11 de jan. de 2021.

Firewall, IPS, IDS e WAF: como cada um atua? Disponível em: https://www.softwall.com.br/blog/firewall-ips-ids-e-waf-como-cada-um-atua/. Acessado em 25 jan. 2021.

Security Management Appliances. Disponível em: https://www.checkpoint.com/products/security-management-appliances/. Acessado em 19, jan. 2021.

NIPS – Disponível em: https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08B/Maristela%20Cheron%20-%20Artigo.pdf. Acessado em 26 de jan. 2021

Rede WAN – Disponível em: https://www.criandobits.com.br/redes/wan. Acessado em 20 de abr. 2021

Rede LAN, MAN e WAN – Disponível em: https://informaticaeadministracao.wordpress.com/2014/04/22/lan-man-e-wan. Acessado em 21 de abr. 2021

Principais redes de computadores – Disponível em: https://ead.catolica.edu.br/blog/principais-tipos-de-redes-de-computadores. Acessado em 18 de abr. 2021

Sistemas distribuídos e redes de computadores para controle e automação industrial – Disponível em: http://alvarestech.com/temp/simprebal/Relatorios_Tecnicos-Publicacoes-Dissertacoes/docs/cursos/Aula6-Apostila-

Sistemas_Distribuidos_E_Redes_De_Computadores_Para_Controle.pdf. Acessado em: 16 jan. 2021.