

Faculdade de Tecnologia de Sorocaba

Tecnologia em Análise e Desenvolvimento de Sistemas

**ISG – SEGURANÇA DA INFORMAÇÃO: Segurança de Redes**

Firewall, IDS, IPS e Thread Intelligence

Prof.º Túlio Santos de Souza

Disciplina: Segurança da Informação

Evandro Rodrigues Tiburcio 0030481921018

Sorocaba

Maio/2023

**SUMÁRIO**

[1 INTRODUÇÃO 3](#__RefHeading___Toc210_2081653479)

[2 METODOLOGIA 3](#__RefHeading___Toc212_2081653479)

[3 DESENVOLVIMENTO 3](#__RefHeading___Toc214_2081653479)

[3.1 Firewall 3](#__RefHeading___Toc216_2081653479)

[3.2. IDS/IPS 6](#__RefHeading___Toc218_2081653479)

[3.3 Thread Intelligence 7](#__RefHeading___Toc220_2081653479)

[4 RESULTADOS 7](#__RefHeading___Toc222_2081653479)

[5 CONSIDERAÇOES FINAIS 8](#__RefHeading___Toc224_2081653479)

[REFERÊNCIAS 8](#__RefHeading___Toc226_2081653479)

## 1 INTRODUÇÃO

Atualmente, o mundo digital proporciona muitas facilidades e alta conectividade, porém, apresenta também, diversos desafios e muitos riscos tanto para empresas quanto para indivíduos. Neste novo cenário, são incontáveis os números de falhas de vulnerabilidades, ameaças e ataques que estamos expostos o tempo todo.

Justamente pensando na segurança dos que usuários,dispositivos e serviços que estão na rede, foram desenvolvidas soluções eficazes de prevenção e precaução, algumas delas serão abordadas neste artigo: Firewall, IPS/IDS e Threat Intelligence. Essas três tecnologias de segurança de rede são essenciais para proteger sistemas e dados contra ameaças cibernéticas, desde malwares até ataques sofisticados de hackers.

A implementação adequada e a manutenção contínua dessas tecnologias são essenciais para garantir a segurança de uma rede, e as organizações preocupadas com este tema devem investir em soluções robustas e atualizadas para proteção e prevenção de ameaças.

## 2 METODOLOGIA

A metodologia de pesquisa adotada foi a busca por informações relevantes em sites especializados no assunto de Redes e Segurança da Informação, produzindo um trabalho descritivo e teórico, porém, com foco em uma apresentação conceitual e prática, contendo os principais tópicos sobre o assunto.

## 3 DESENVOLVIMENTO

### 3.1 Firewall

O firewall é uma tecnologia (pode ser embarcada em um sistema operacional) que apresenta diversas funcionalidades, porém, a mais comum é o controle do tráfego de rede. Esse controle ocorre com base em políticas de segurança pré-definidas, permitindo ou bloqueando o acesso a recursos próprios da rede a que está inserido (nesse caso, atuando como gateway).

Atua ainda como um filtro, inspecionando cada pacote de dados que trafega por ele e aplicando as ações conforme as referidas políticas de acesso. Nesse formato, as políticas de controle (de forma sucinta) são (accept) permitir ou (drop) bloquear o fluxo de pacotes. Com Isso é possível proteger a rede/sistemas contra ameaças cibernéticas, como malware, ataques de negação de serviço (DDoS), invasões e outras formas de violação de segurança.

O firewall pode ser implementado como um hardware dedicado (único que atua na camada de enlace), um software ou uma combinação de ambos, sendo amplamente utilizado, (nem sempre bem configurado) em redes corporativas e domésticas. Ele atua com várias funções, conhecidas como áreas, onde cada área possui um tipo de cadeia (chain). As cadeias principais são:

Input: fluxo de rede com destino ao próprio dispositivo;

Output: fluxo de rede originado no próprio firewall com destino a outro dispositivo (dependendo da configuração de pacotes de dentro da rede podem ser considerados como output devido ao NAT);

Forward: fluxo de rede que passa pelo firewall, mas não é originado pelo mesmo e possui um destino externo. Isso só é possível quando o firewall é o gateway do dispositivo de destino;

Prerouting: fluxo de rede antes da tomada de decisão de rotas (antes das cadeias input, output e forward);

Posrouting: fluxo de rede após a tomada de decisão de rotas (após as cadeias input, output e forward).

Para uso das cadeias o firewall utiliza guias de cada área: veremos de forma simplificada algumas delas:

Connections;

RAW;

Mangle;

NAT;

Filter (Parte mais conhecida e descrita acima).

#### 3.1.1. Connections

A fase inicial de todas as requisições, tanto externas como internas, que serão tratadas posteriormente. Essas conexões não necessitam de um firewall para ocorrer, porém, é importante ressaltar que elas sempre chegarão até um determinado dispositivo ativo e, antes das tomadas de decisões, serão criadas com um formato de ID de sessão, um protocolo e outros detalhes que não serão abordados. Existe uma configuração chamada tracking connections, caso não seja habilitada, as conexões serão gerenciadas somente no fluxo de saída do dispositivo, não podendo atuar como um gateway/firewall de rede.

#### 3.1.2. RAW

Esta é a primeira fase da entrada das conexões para o processamento, essa guia somente é utilizada por administradores de redes experientes, pois as conexões estão em um “estado bruto”, sendo assim, não existe ainda a definição de roteamento. Uma forma de aplicação é o bloqueio (muito rigoroso) de todas as respostas e recursos de um determinado IP. Suas cadeias no firewall são prerouting e output.

#### 3.1.3. Mangle

Área responsável por configurar, principalmente, as marcações de pacotes. Com essas marcações, pode-se realizar configurações como filas (liberação de tráfego de rede Download e Upload), balanceamento de cargas em links diferenciados, configurações de rotas especificas, etc. Contempla todas as cadeias padrões do firewall.

#### 3.1.4. NAT

Responsável pelo funcionamento do Network Address Translation (NAT). Entre os serviços mais comuns estão o redirecionamento de portas de redes distintas e o mascaramento de IPs. As cadeias são exclusivas dessa área, sendo a srcnat e dstnat.

#### 3.1.5. Filter

Essa área do firewall é mais conhecida, onde se encontram as políticas de acesso ao tráfego de rede. As cadeias padrões utilizadas são input, forward e output.

### 3.2. IDS/IPS

O Sistema de Detecção de Intrusão (IDS) é projetado para monitorar a rede em busca de atividades suspeitas ou mal-intencionadas. O IDS analisa os dados do tráfego de rede e compara-os com um conjunto de regras de segurança pré-definidas para identificar possíveis ameaças. Quando uma ameaça é detectada, o IDS pode emitir um alerta para um administrador de segurança para que este possa tomar medidas a fim de mitigar o problema.

Já o Sistema de Prevenção de Intrusão (IPS) é uma extensão do anterior. O IPS não apenas detecta ameaças, mas também tem a capacidade de bloqueá-las automaticamente para evitar que um ataque bem-sucedido ocorra. O IPS pode ser configurado para bloquear o tráfego malicioso ou para permitir o tráfego seguro, com base em um conjunto de políticas de segurança.

### 3.3 Thread Intelligence

A Inteligência de Ameaças é um conjunto de informações coletadas e analisadas sobre ameaças de segurança cibernética. Essas informações incluem dados sobre ameaças em potencial, bem como táticas, técnicas e procedimentos usados por hackers e outros agentes maliciosos para invadir sistemas de computadores e redes.

A Threat Intelligence é coletada de várias fontes, incluindo feeds de dados de ameaças conhecidas, análises de malware, vulnerabilidades de softwares, monitoramento de atividades em tempo real na rede, pesquisas e outros recursos. As informações coletadas são analisadas para identificar padrões e tendências, bem como para determinar o potencial de risco para sistemas e dados.

As equipes de segurança utilizam essa ferramenta para identificar, monitorar e mitigar ameaças de segurança em tempo real. Isso permite que as equipes estejam mais bem preparadas para proteger seus sistemas e dados e reduzir o tempo de resposta a possíveis ameaças.

## 4 RESULTADOS

Através da pesquisa e estudo sobre as tecnologias do Firewall e do IDS/IPS, a equipe foi capaz de construir um corpo de conhecimentos mais avançado e aprofundado sobre a área de Segurança da Informação, relacionando alguns destes conceitos com a camada de redes do modelo OSI/RM.

Desenvolveremos um projeto prático com o uso destas tecnologias e realizaremos uma demonstração em sala de aula, com o objetivo de mostrar uma aplicação real do Firewall e de suas regras de bloqueio.

Nesta abordagem prática, será utilizado um equipamento roteador Mikrotik (incluir a versão/modelo/série) em conjunto com um notebook e possíveis dispositivos móveis dos alunos. Neste contexto, focaremos na área de atuação da tabela Filter.

## 5 CONSIDERAÇOES FINAIS

O Firewall é muito legal, ...

## REFERÊNCIAS

SOFTWALL. 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/. Acesso em 03/05/2023.

STUDY-CCNA.COM. Firewalls, IDS, and IPS Explanation and Comparison. Disponível em: https://study-ccna.com/firewalls-ids-ips-explanation-comparison/ - :~:text=The%20major%20distinction%20is%20that,%2C%20destination%2C%20and%20port%20addresses. Acesso em 03/05/2023.