# Segurança em redes - IDS - Firewalls - IP tables



## Segurança da Informação

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### O que é segurança de rede?

A segurança de rede é a área da cibersegurança que se concentra na proteção de redes e sistemas de computadores contra ameaças cibernéticas e ataques cibernéticos internos e externos.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### O que é segurança de rede?

A segurança da rede tem três objetivos principais: impedir o acesso não autorizado aos recursos da rede; detectar e interromper ataques cibernéticos e violações de segurança em andamento; e garantir que os usuários autorizados tenham acesso seguro aos recursos de rede de que precisam, quando precisam.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### O que é segurança de rede?

À medida que as redes crescem em tamanho e complexidade, também aumenta o risco de ataques cibernéticos. Por exemplo, de acordo com o relatório ***Cost of a Data Beach 2023*** da IBM, 82% das violações de dados (violações de segurança que resultam em acesso não autorizado a informações confidenciais ou sensíveis) ocorridas nas organizações envolveram dados armazenados na nuvem. Esses ataques saíram caro: o custo médio global de uma violação de dados é de US$ 4,45 milhões, e o custo médio de uma violação de dados nos Estados Unidos é mais do que o dobro desse valor: US$ 9,48 milhões.

A segurança da rede protege a integridade da infraestrutura, dos recursos e do tráfego da rede para provocar esses ataques e minimizar seu impacto financeiro e operacional.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de tecnologias de segurança de rede?

Os sistemas de segurança de rede funcionam em dois níveis: no perímetro e dentro da rede.

No perímetro, os controles de segurança tentam impedir que ameaças cibernéticas entrem na rede. Porém, os invasores de rede às vezes conseguem entrar, então as equipes de segurança de TI também colocam controles em torno dos recursos dentro da rede, como notebooks e dados. Mesmo que os invasores entrem, eles não terão reinado livre. Essa estratégia de colocar vários controles entre hackers e possíveis vulnerabilidades é chamada de “defesa em profundidade”.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de tecnologias de segurança de rede?

Para criar sistemas de segurança de rede, as equipes de segurança combinam as seguintes ferramentas:

### Firewalls

Um firewall é um software ou hardware que impede a entrada ou saída de tráfego suspeito de uma rede, permitindo a passagem de tráfego legítimo. Os firewalls podem ser implantados nas bordas de uma rede ou usados internamente para dividir uma rede maior em sub-redes menores. Se uma parte da rede for comprometida, os hackers ainda estarão isolados do resto.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de tecnologias de segurança de rede?

### Firewalls

Existem diferentes tipos de firewalls com recursos diferentes. Os firewalls básicos usam filtragem de pacotes para inspecionar o tráfego. Os firewalls de última geração (NGFWs) mais avançados adicionam prevenção de intrusões, IA e aprendizado de máquina, além de reconhecimento e controle de aplicações e feeds de inteligência de ameaças para proporcionar proteção extra.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de tecnologias de segurança de rede?

### Controle de acesso à rede (NAC)

As soluções de controle de acesso à rede atuam como gatekeepers, autenticando e autorizando os usuários a determinar quem é permitido na rede e o que podem fazer dentro dela. “Autenticação" significa verificar se um usuário é mesmo quem ele afirma ser. Também significa conceder permissão aos usuários autenticados para acessar os recursos da rede.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de tecnologias de segurança de rede?

### Controle de acesso à rede (NAC)

As soluções de NAC são frequentemente usadas para impor políticas de controle de acesso baseado em função (RBAC), nas quais os privilégios dos usuários são baseados em suas funções. Por exemplo, um desenvolvedor júnior pode ser capaz de visualizar e editar o código, mas não de publicá-lo. Por outro lado, desenvolvedores seniores podem ler, escrever e enviar código para a produção. O RBAC ajuda a evitar violações de dados, mantendo usuários não autorizados longe de ativos que eles não têm permissão para acessar.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de tecnologias de segurança de rede?

### Controle de acesso à rede (NAC)

As soluções de NAC são frequentemente usadas para impor políticas de controle de acesso baseado em função (RBAC), nas quais os privilégios dos usuários são baseados em suas funções. Por exemplo, um desenvolvedor júnior pode ser capaz de visualizar e editar o código, mas não de publicá-lo. Por outro lado, desenvolvedores seniores podem ler, escrever e enviar código para a produção. O RBAC ajuda a evitar violações de dados, mantendo usuários não autorizados longe de ativos que eles não têm permissão para acessar.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de tecnologias de segurança de rede?

### Controle de acesso à rede (NAC)

Além de autenticar usuários, algumas soluções de NAC podem fazer avaliações de risco nos endpoints dos usuários. O objetivo é impedir que dispositivos não protegidos ou comprometidos acessem a rede. Se um usuário tentar entrar na rede em um dispositivo com software anti-malware desatualizado ou configurações incorretas, o NAC negará o acesso. Algumas ferramentas avançadas de NAC podem corrigir automaticamente endpoints que não estejam em conformidade.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de tecnologias de segurança de rede?

### Sistemas de detecção e prevenção de intrusões (IDPSs)

Um sistema de detecção e prevenção de intrusões (às vezes chamado de sistema de prevenção de intrusões) pode ser implementado diretamente atrás de um firewall para verificar o tráfego de entrada em busca de ameaças à segurança. Essas ferramentas de segurança evoluíram a partir de sistemas de detecção de intrusões, que apenas sinalizavam atividades suspeitas para análise. Os IDPSs têm a capacidade adicionada de responder automaticamente a possíveis violações, como bloquear o tráfego ou redefinir a conexão. Os IDPSs são particularmente eficazes na detecção e bloqueio de ataques de força bruta e ataques do tipo denial of service (DoS) ou distributed denial of Service (DDoS).

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de tecnologias de segurança de rede?

### Redes privadas virtuais (VPNs)

Uma rede privada virtual (VPN) protege a identidade do usuário criptografando seus dados e mascarando seu endereço IP e localização. Quando alguém usa uma VPN, não se conecta mais diretamente à Internet, mas a um servidor seguro que se conecta à Internet em seu nome.

As VPNs podem ajudar funcionários remotos a acessar redes corporativas com segurança, mesmo por meio de conexões Wi-Fi públicas não seguras, como as encontradas em cafeterias e aeroportos. As VPNs criptografam o tráfego de um usuário, mantendo-o protegido contra hackers que possam querer interceptar suas comunicações.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de tecnologias de segurança de rede?

### Redes privadas virtuais (VPNs)

Em vez de VPNs, algumas organizações usam acesso de rede zero trust (ZTNA). Em vez de usar um servidor proxy, o ZTNA usa políticas de controle de acesso zero trust para conectar usuários remotos com segurança. Quando os usuários remotos fazem login em uma rede por meio do ZTNA, eles não têm acesso a toda a rede. Em vez disso, eles só obtêm acesso aos ativos específicos que têm permissão para usar e devem ser verificados novamente sempre que acessarem um novo recurso.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de tecnologias de segurança de rede?

### Segurança de aplicativos

A segurança de aplicativos refere-se às etapas que as equipes de segurança adotam para proteger aplicativos e interfaces de programação de aplicativos (APIs) contra invasores de rede. Como muitas empresas atualmente usam aplicativos para realizar funções comerciais importantes ou processar dados confidenciais, os aplicativos são um alvo comum para os criminosos cibernéticos. E como muitos aplicativos de negócios são hospedados em nuvens públicas, os hackers podem explorar suas vulnerabilidades para invadir as redes privadas da empresa.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de tecnologias de segurança de rede?

### Segurança de aplicativos

As medidas de segurança de aplicações protegem as aplicações de agentes mal-intencionados. Entre as ferramentas comuns de segurança de aplicações estão: firewalls de aplicações web, autoproteção de aplicações em tempo de execução, testes estáticos de segurança de aplicações e testes dinâmicos de segurança de aplicações.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tecnologias de segurança relacionadas

Embora as ferramentas a seguir não sejam estritamente ferramentas de segurança de rede, os administradores de rede geralmente as usam para proteger áreas e recursos em uma rede.

### Data loss prevention (DLP)

Prevenção contra perda de dados (DLP) refere-se a estratégias e ferramentas de segurança da informação que garantem que dados confidenciais não sejam roubados nem vazados acidentalmente. A DLP inclui políticas de segurança de dados e tecnologias específicas que rastreiam fluxos de dados, criptografam informações confidenciais e emitem alertas quando atividades suspeitas são detectadas.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Segurança de endpoints**

As soluções de segurança de endpoint protegem todos os dispositivos que se conectam a uma rede (como notebooks, desktops, servidores, dispositivos móveis ou dispositivos IoT) contra hackers que tentam usá-los para se infiltrar na rede. O software antivírus pode detectar e destruir trojans, spywares e outros softwares mal-intencionados em um dispositivo antes que eles se espalhem para o restante da rede.

As soluções de detecção e resposta de endpoint são ferramentas mais avançadas que monitoram o comportamento do endpoint e respondem automaticamente a eventos de segurança. O software de gerenciamento unificado de endpoints permite que as empresas monitorem, gerenciem e protejam todos os dispositivos do usuário final em um único console.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Segurança na web

Soluções de segurança na web, como gateways seguros da web, bloqueiam o tráfego malicioso da internet e impedem que os usuários se conectem a sites e aplicações suspeitos.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Segmentação de rede

A segmentação de rede é uma forma de dividir grandes redes em sub-redes menores, seja fisicamente ou por meio de software. A segmentação de rede pode limitar a disseminação de ransomwares e outros malwares, isolando uma sub-rede comprometida do restante da rede. A segmentação também ajuda a manter os usuários legítimos longe dos ativos que não deveriam acessar.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Segurança na nuvem

As soluções de segurança de nuvem protegem data centers, aplicações e outros ativos de nuvem contra ataques cibernéticos. A maioria das soluções de segurança de nuvem são simplesmente medidas padrão de segurança na rede, como firewalls, NACs e VPNs, aplicadas a ambientes de nuvem. Muitos provedores de serviços de nuvem incorporam controles de segurança em seus serviços ou os oferecem como complementos.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Uma abordagem de confiança zero para segurança de rede

As redes tradicionais da empresa eram centralizadas, com os principais endpoints, dados e aplicações situados no local. Os sistemas tradicionais de segurança de rede visavam impedir que as ameaças violassem o perímetro da rede. Depois que um usuário entrou, ele foi tratado como confiável e recebeu acesso praticamente irrestrito.

No entanto, à medida que as organizações buscam a transformação digital e adotam ambientes de nuvem híbrida, as redes estão se tornando descentralizadas. Agora, existem recursos de rede em data centers na nuvem, endpoints locais e remotos e dispositivos móveis e IoT.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Uma abordagem de confiança zero para segurança de rede

Os controles de segurança baseados em perímetro são menos eficazes em redes distribuídas. Por isso, muitas equipes de segurança de TI estão migrando para frameworks de segurança de rede zero trust. Em vez de se concentrar no perímetro, a segurança de rede zero trust coloca os controles de segurança em torno de recursos individuais. Os usuários nunca são implicitamente confiáveis. Toda vez que um usuário tenta acessar um recurso, ele deve ser autenticado e autorizado, independentemente de já estar na rede da empresa. Os usuários autenticados recebem apenas acesso com privilégios mínimos e suas permissões são revogadas assim que a tarefa é concluída.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Uma abordagem de confiança zero para segurança de rede

A segurança de rede zero trust se baseia em políticas de acesso granular, validação contínua e dados coletados do maior número possível de fontes (incluindo muitas das ferramentas mencionadas acima) para garantir que só os usuários certos possam acessar os recursos certos pelos motivos certos no momento certo.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Soluções de segurança de rede corporativa

Embora uma abordagem de defesa profunda possa proteger a rede de uma empresa, isso também significa que a equipe de segurança de TI precisa gerenciar vários controles de segurança separados. As plataformas de segurança de rede corporativa podem ajudar a simplificar o gerenciamento de segurança de rede, integrando ferramentas de segurança diferentes e permitindo que as equipes de segurança monitorem toda a rede a partir de um único console. Plataformas comuns de segurança de rede incluem:

1. Gerenciamento de informações e eventos de segurança (SIEM)
2. Orquestração, automação e resposta de segurança (SOAR)
3. Detecção e resposta de rede (NDR)
4. Detecção e resposta estendidas (XDR)

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Soluções de segurança de rede corporativa

- O gerenciamento de eventos e informações de segurança coleta informações de ferramentas de segurança internas, agrega-as em um log central e identifica anomalias.

- As soluções de orquestração, automação e resposta de segurança coletam e analisam dados de segurança e permitem que as equipes de segurança definam e executem respostas automatizadas a ameaças cibernéticas.

- As ferramentas de detecção e resposta de rede usam IA e aprendizado de máquina para monitorar o tráfego de rede e detectar atividades suspeitas.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Soluções de segurança de rede corporativa

- Detecção e resposta estendidas é uma arquitetura aberta de segurança cibernética que integra ferramentas de segurança e unifica as operações de segurança em todas as camadas de segurança: usuários, endpoints, e-mail, aplicações, redes, cargas de trabalho na nuvem e dados. Com o XDR, as soluções de segurança que não são necessariamente projetadas para trabalhar juntas podem interoperar sem dificuldades na prevenção, detecção, investigação e resposta a ameaças. O XDR também pode automatizar fluxos de trabalho de detecção de ameaças, triagem de incidentes e caça a ameaças.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### O que é um IDS?

Um sistema de detecção de intrusões (IDS) é uma ferramenta de segurança de rede que monitora o tráfego da rede e dispositivos em busca de atividades maliciosas conhecidas, atividades suspeitas ou violações de políticas de segurança.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### O que é um IDS?

Um IDS pode ajudar a acelerar e automatizar a detecção de ameaças na rede, alertando os administradores de segurança sobre ameaças conhecidas ou potenciais, ou enviando alertas para uma ferramenta centralizada de segurança. Uma ferramenta centralizada de segurança, como um sistema de gerenciamento de informações e eventos de segurança (SIEM), pode combinar dados de outras fontes para ajudar as equipes de segurança a identificar e responder a ameaças cibernéticas que possam passar despercebidas por outras medidas de segurança.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### O que é um IDS?

Os IDSs também podem apoiar os esforços de conformidade. Certas regulamentações, como o padrão de segurança de dados do setor de cartões de pagamento (PCI-DSS), exigem que as organizações implementem medidas de detecção de intrusões.

Um IDS não pode parar ameaças de segurança por conta própria. Atualmente, os recursos do IDS são normalmente integrados ou incorporados a sistemas de prevenção de intrusões (IPSs), que podem detectar ameaças à segurança e agir automaticamente para evitá-las.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Como funcionam os sistemas de detecção de intrusão?**

Os IDSs podem ser aplicações de software instaladas em endpoints ou dispositivos de hardware dedicados conectados à rede. Algumas soluções IDS estão disponíveis como serviços em nuvem. Independentemente da forma que assuma, um IDS utiliza um ou ambos os dois métodos principais de detecção de ameaças: detecção baseada em assinatura ou detecção baseada em anomalia.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Como funcionam os sistemas de detecção de intrusão?

### Detecção baseada em assinatura

A detecção baseada em assinatura analisa pacotes de rede em busca de assinaturas de ataque, características ou comportamentos exclusivos associados a uma ameaça específica. Um trecho de código que aparece em uma variante específica de malware é um exemplo de assinatura de ataque.

Um IDS baseado em assinatura mantém um banco de dados de assinaturas de ataques contra o qual compara os pacotes de rede. Se um pacote corresponder a uma das assinaturas, o IDS o sinaliza. Para ser eficaz, os bancos de dados de assinaturas devem ser atualizados regularmente com nova **inteligência de ameaças** à medida que novos ataques cibernéticos surgem e ataques existentes evoluem. Ataques completamente novos, que ainda não foram analisados para assinaturas, podem escapar de um IDS baseado em assinatura.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Como funcionam os sistemas de detecção de intrusão?**

**Detecção baseada em anomalias**

Os métodos de detecção baseada em anomalia usam aprendizado de máquina para criar — e continuamente refinar — um modelo de referência da atividade normal da rede. Em seguida, comparam a atividade da rede com o modelo e sinalizam desvios — como um processo que usa mais largura de banda do que o normal ou um dispositivo abrindo uma porta.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Como funcionam os sistemas de detecção de intrusão?**

**Detecção baseada em anomalias**

Como relatam qualquer comportamento anômalo, os IDS baseados em anomalias podem frequentemente detectar novos ataques cibernéticos que poderiam escapar da detecção baseada em assinatura. Por exemplo, IDSs baseados em anomalias podem detectar vulnerabilidades de dia zero — ataques que aproveitam vulnerabilidades de software antes que o desenvolvedor de software saiba sobre elas ou tenha tempo de corrigi-las.

No entanto, IDSs baseados em anomalias podem ser mais propensos a falsos positivos. Mesmo atividades benignas, como um usuário autorizado acessando um recurso de rede sensível pela primeira vez, podem desencadear um IDS baseado em anomalias

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Como funcionam os sistemas de detecção de intrusão?**

**Métodos de detecção menos comuns**

A detecção baseada em reputação bloqueia o tráfego de endereços IP e domínios associados a atividades maliciosas ou suspeitas. A análise de protocolo com estado foca no comportamento do protocolo — por exemplo, pode identificar um ataque de negação de serviço (DoS) detectando um único endereço IP fazendo muitas solicitações de conexão TCP simultâneas em um curto período.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Como funcionam os sistemas de detecção de intrusão?**

**Métodos de detecção menos comuns**

Seja qual for o(s) método(s) usado(s), quando um IDS detecta uma ameaça potencial ou violação de política, ele alerta a **equipe de resposta a incidentes** para investigar. IDSs também mantêm registros de incidentes de segurança, seja em seus próprios logs ou registrando-os com uma **ferramenta de gerenciamento de informações e eventos de segurança (SIEM)**. Esses registros de incidentes podem ser usados para refinar os critérios do IDS, como adicionando novas assinaturas de ataque ou atualizando o modelo de comportamento da rede.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de sistemas de prevenção de intrusão

Os IDSs são categorizados com base em onde são colocados em um sistema e em que tipo de atividade eles monitoram.

Os **sistemas de detecção de intrusões de rede (NIDSs)** monitoram o tráfego de entrada e saída para dispositivos em toda a rede. Os NIDS são colocados em pontos estratégicos na rede, frequentemente imediatamente atrás de firewalls no perímetro da rede para que possam sinalizar qualquer tráfego malicioso que penetre.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de sistemas de prevenção de intrusão

Os NIDS também podem ser colocados dentro da rede para detectar ameaças internas ou hackers que sequestraram contas de usuários. Por exemplo, NIDS podem ser colocados atrás de cada firewall interno em uma rede segmentada para monitorar o tráfego entre sub-redes.

Para evitar impedir o fluxo de tráfego legítimo, um NIDS é frequentemente colocado "fora de banda", o que significa que o tráfego não passa diretamente por ele. Um NIDS analisa cópias de pacotes de rede em vez dos próprios pacotes. Dessa forma, o tráfego legítimo não precisa esperar pela análise, mas o NIDS ainda pode capturar e sinalizar tráfego malicioso.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de sistemas de prevenção de intrusão

Os **sistemas de detecção de intrusão de host (HIDSs)** são instalados em um endpoint específico, como um laptop, roteador ou servidor. O HIDS monitora apenas a atividade nesse dispositivo, incluindo o tráfego de e para ele. Um HIDS normalmente funciona tirando instantâneos periódicos de arquivos críticos do sistema operacional e comparando esses instantâneos ao longo do tempo. Se o HIDS perceber uma alteração, como edição de arquivos de log ou alteração de configurações, ele alertará a equipe de segurança.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tipos de sistemas de prevenção de intrusão

As equipes de segurança frequentemente combinam sistemas de detecção de intrusões baseados em rede e baseados em host. O NIDS analisa o tráfego de forma geral, enquanto o HIDS pode adicionar proteção extra em torno de ativos de alto valor. Um HIDS também pode ajudar a capturar atividades maliciosas de um nó de rede comprometido, como **ransomware** se espalhando de um dispositivo infectado.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Táticas de evasão de SMI

Embora as soluções IDS possam detectar muitas ameaças, os hackers podem contorná-las. Os fornecedores de IDS respondem atualizando suas soluções para levar em conta essas táticas. No entanto, essas atualizações de solução criam algo como uma corrida armamentista, com hackers e IDSs tentando ficar um passo à frente um do outro.

Algumas táticas comuns de evasão de IDS incluem:

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Táticas de evasão de SMI

- **Ataques distribuídos de negação de serviço (DDoS)** —colocando os IDSs off-line, inundando-os com tráfego obviamente malicioso de diversas fontes. Quando os recursos do IDS são sobrecarregados pelas ameaças falsas, os hackers entram sorrateiramente.

- **Spoofing**– falsificação de registros IP lidar com e DNS para fazer parecer que o tráfego vem de uma fonte confiável.

- **Fragmentação**: divisão do malware ou de outras cargas maliciosas em pequenos pacotes, obscurecendo a assinatura e evitando a detecção. Ao atrasar estrategicamente os pacotes ou enviá-los fora de ordem, os hackers podem impedir que o IDS reembale-os e observe o ataque.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Táticas de evasão de SMI

- **Criptografia** - uso de protocolos criptografados para contornar um IDS se o IDS não tiver a chave de descriptografia correspondente.
- **Fadiga do operador** - gerarum grande número de alertas de IDS propositalmente para distrair a equipe de resposta a incidentes de sua atividade real.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### IDS e outras soluções de segurança

Os IDSs não são ferramentas independentes. Eles foram projetados para fazer parte de um sistema holístico de segurança cibernética e geralmente são totalmente integrados a uma ou mais das seguintes soluções de segurança.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### IDS e outras soluções de segurança

### IDS e SIEM (gerenciamento de informações e eventos de segurança)

Os alertas de IDSs geralmente são canalizados para o SIEM de uma organização, onde podem ser combinados com alertas e informações de outras ferramentas de segurança em um único painel centralizado. A integração do IDS com o SIEMs permite que as equipes de segurança enriqueçam os alertas do IDS com inteligência de ameaças e dados de outras ferramentas, filtrem alarmes falsos e priorizem incidentes para correção.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### IDS e outras soluções de segurança

### IDS e firewalls

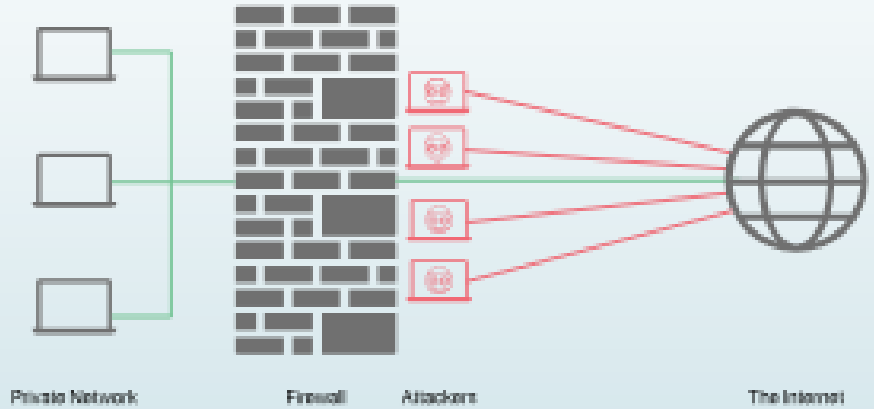
IDSs e firewalls são complementares. Os firewalls enfrentam o exterior da rede e atuam como barreiras usando conjuntos de regras predefinidas para permitir ou bloquear o tráfego. Os IDSs geralmente ficam perto dos firewalls e ajudam a capturar qualquer coisa que passe por eles. Alguns firewalls, especialmente os firewalls de próxima geração, têm funções integradas de IDS e IPS.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### O que é um firewall?

Um firewall é um sistema de segurança que monitora e controla o tráfego da rede com base em um conjunto de regras de segurança. Os firewalls geralmente ficam entre uma rede confiável e uma rede não confiável; muitas vezes, a rede não confiável é a internet. Por exemplo, redes de escritórios frequentemente usam um firewall para proteger sua rede contra ameaças on-line.

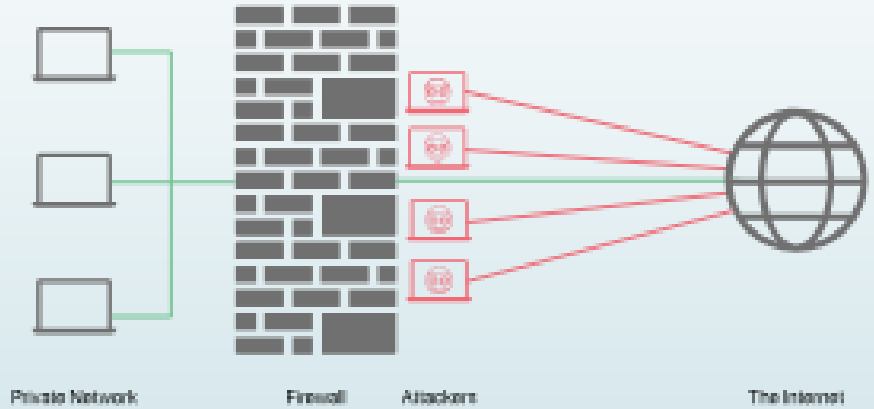


# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### O que é um firewall?

Os firewalls decidem se permitem a passagem do tráfego de entrada e de saída. Eles podem ser integrados ao hardware, ao software ou a uma combinação de ambos. Na verdade, o termo "firewall" é emprestado de uma prática de construção de paredes entre edifícios ou no meio deles e projetadas para conter um incêndio. De forma semelhante, os firewalls de rede atuam para conter ameaças on-line.



# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Por que usar um firewall?

A principal justificativa para utilizar um firewall é a segurança. Os firewalls podem interceptar o tráfego malicioso recebido antes que ele chegue à rede, além de evitar que informações confidenciais saiam da rede.

Os firewalls também podem ser usados para filtragem de conteúdo. Por exemplo, uma escola pode configurar um firewall para evitar que os usuários da sua rede acessem conteúdo adulto. Da mesma forma, em alguns países, o governo usa um firewall que pode evitar que as pessoas dentro daquele país acessem determinadas partes da internet.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Quais são os diferentes tipos de firewall?**

**Firewalls baseados em proxy:**

São proxies* que ficam entre clientes e servidores. Os clientes se conectam ao firewall e o firewall inspeciona os pacotes de saída. Em seguida ele criará uma conexão com o destinatário desejado (o servidor web ). Da mesma forma, quando o servidor web tenta enviar uma resposta ao cliente, o firewall interceptará essa solicitação, inspecionará os pacotes e então enviará essa resposta em uma conexão separada entre o firewall e o cliente. Um firewall baseado em proxy evita uma conexão direta entre o cliente e o servidor de forma eficaz.

- *Um proxy é um computador que atua como um gateway entre uma rede local e uma rede maior, como a internet.*

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Quais são os diferentes tipos de firewall?**

**Firewalls baseados em proxy:**

Um firewall baseado em proxy é um tipo de segurança de bar. Esse segurança intercepta os convidados antes que eles entrem no bar para se assegurar que eles não são menores de idade, não estão armados ou não constituem uma ameaça para o bar e seus clientes. O segurança também para os clientes na saída para garantir que eles tenham uma maneira segura de chegar em casa e não estejam planejando beber e dirigir.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Quais são os diferentes tipos de firewall?**

**Firewalls baseados em proxy:**

A desvantagem de ter um segurança no bar é que quando muitas pessoas estão tentando entrar ou sair do bar simultaneamente, haverá uma longa fila e várias pessoas terão que esperar. O mesmo acontece com o firewall: uma grande desvantagem de um firewall baseado em proxy é que ele pode causar latência, especialmente em momentos de tráfego intenso.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Quais são os diferentes tipos de firewall?**

**Stateful firewalls**

Em ciências da computação, um aplicativo "stateful" é um aplicativo que salva dados de eventos e interações anteriores. Um stateful firewall salva informações sobre conexões abertas e usa essas informações para analisar o tráfego de entrada e saída, em vez de inspecionar cada pacote. Como eles não inspecionam todos os pacotes, os stateful firewalls são mais rápidos do que os firewalls baseados em proxy.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Quais são os diferentes tipos de firewall?**

**Stateful firewalls**

Stateful firewalls dependem de muito contexto na tomada de decisões. Por exemplo, se o firewall registrar pacotes de saída em uma conexão solicitando determinado tipo de resposta, ele só permitirá a entrada de pacotes nessa conexão se eles fornecerem o tipo de resposta solicitada.

Stateful firewalls também podem proteger as portas*, mantendo-as todas fechadas, a menos que os pacotes de entrada solicitem acesso a uma porta específica. Isso pode mitigar um ataque conhecido como varredura de porta.

- *Uma porta de rede é um local para onde as informações são enviadas; não é um lugar físico, mas sim o ponto final de uma comunicação.*

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Quais são os diferentes tipos de firewall?**

**Stateful firewalls**

Uma conhecida vulnerabilidade associada aos stateful firewalls é que eles podem ser manipulados e levar um cliente a solicitar um determinado tipo de informação. Assim que o cliente solicitar essa resposta, o invasor pode então enviar pacotes maliciosos que correspondam a esses critérios por meio do firewall. Por exemplo, sites não seguros podem usar código JavaScript para criar esses tipos de solicitação forjadas a partir de um navegador web.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Quais são os diferentes tipos de firewall?**

**Firewalls de próxima geração (NGFW):**

NGFWs são firewalls que têm os recursos dos firewalls tradicionais, mas também empregam uma série de recursos adicionais para lidar com as ameaças em outras camadas do modelo OSI. Alguns recursos específicos do NGFW incluem:

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Quais são os diferentes tipos de firewall?**

**Firewalls de próxima geração (NGFW):**

- **Inspeção profunda de pacotes (DPI)** - Os NGFWs realizam uma inspeção muito mais profunda de pacotes do que os firewalls tradicionais. Essa inspeção profunda pode procurar coisas como payloads de pacotes e qual aplicativo está sendo acessado pelos pacotes. Isso permite que o firewall aplique regras de filtragem mais minuciosas.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Quais são os diferentes tipos de firewall?**

**Firewalls de próxima geração (NGFW):**

- **Application awareness -** Habilitar esse recurso torna o firewall ciente de quais aplicativos estão sendo executados e quais portas esses aplicativos estão usando. Isso pode proteger contra determinados tipos de malware que têm como objetivo encerrar um processo em execução e depois assumir o controle de sua porta.

- **Identity awareness -** Esse recurso permite que um firewall aplique regras baseadas na identidade, tais como qual computador está sendo usado, qual usuário está conectado, etc.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Quais são os diferentes tipos de firewall?**

**Firewalls de próxima geração (NGFW):**

- **Sandboxing -** Firewalls podem isolar pedaços de código associados aos pacotes recebidos e executá-los em um ambiente "sandbox" para garantir que não estejam se comportando de forma maliciosa. Os resultados desse teste em sandbox podem então ser usados como critério ao decidir se os pacotes devem ou não entrar na rede.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Quais são os diferentes tipos de firewall?**

**Firewalls de aplicativos web (WAF)**

Enquanto os firewalls tradicionais ajudam a proteger as redes privadas contra aplicativos web maliciosos, os WAFs ajudam a proteger os aplicativos web contra usuários maliciosos. Um WAF ajuda a proteger aplicativos web filtrando e monitorando o tráfego HTTP entre um aplicativo web e a internet. Normalmente eles protegem os aplicativos web contra ataques como **cross-site forgery**, **cross-site-scripting**, inclusão de arquivos, e injeção de SQL, entre outros.

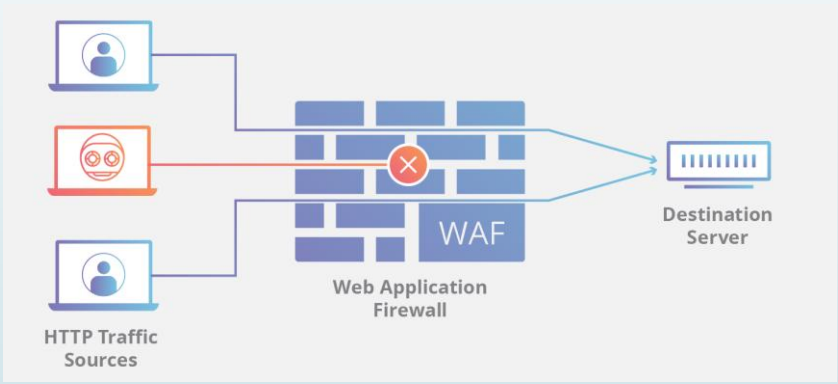
# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Quais são os diferentes tipos de firewall?**

**Firewalls de aplicativos web (WAF)**

Ao implantar um WAF na frente de um aplicativo web, coloca-se um escudo entre o aplicativo web e a internet. Enquanto um firewall de proxy protege a identidade da máquina cliente com o uso de um intermediário, o WAF é um tipo de proxy reverso que protege o servidor contra a exposição, já que seus clientes passam pelo WAF antes de chegar ao servidor.



# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Quais são os diferentes tipos de firewall?**

**Firewalls de aplicativos web (WAF)**

Um WAF opera por meio de um conjunto de regras frequentemente chamadas de políticas. Essas políticas visam proteger contra vulnerabilidades do aplicativo por meio de filtragem do tráfego malicioso. O valor de um WAF decorre em parte da velocidade e da facilidade com que a modificação de políticas pode ser implementada, permitindo uma resposta mais rápida a diversos vetores de ataque; durante um ataque DDoS, o rate limiting pode ser implementado rapidamente modificando as políticas de WAF. Produtos comerciais WAF como o Web Application Firewall da Cloudflare protegem milhões de aplicativos web contra ataques todos os dias.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### O que é um "firewall de rede"?

Um "firewall de rede" é qualquer firewall que defende uma rede. Por definição, quase todos os firewalls de segurança são firewalls de rede, embora os firewalls também possam proteger máquinas individuais.

Embora os firewalls sejam um componente importante da segurança de rede, essa área também tem muitos outros aspectos, incluindo controle de acesso, autenticação de usuários e mitigação de DDoS. Saiba mais sobre soluções de segurança de rede.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Os firewalls são baseados em software ou em hardware?**

Originalmente, os firewalls eram dispositivos de hardware. Embora alguns firewalls de hardware ainda estejam em uso, muitos firewalls modernos são baseados em software, o que significa que podem ser executados em vários tipos diferentes de hardware. O FWaaS, por sua vez, está hospedado na nuvem.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Qual é a história dos firewalls?

Os firewalls datam do final dos anos 1980. Os primeiros firewalls permitiam ou bloqueavam pacotes de dados individuais. Eles decidiam quais pacotes seriam permitidos e quais seriam bloqueados inspecionando sua camada de rede e seus cabeçalhos da camada de transporte para ver o endereço de IP de origem e de destino deles e a porta (como ver as seções "Para" e "De" de um e-mail). Isso evitou o tráfego ilegítimo e impediu muitos ataques de malware.

A última geração de firewalls acrescentou recursos stateful. E as gerações mais novas (como as NGFWs) acrescentaram a capacidade de inspecionar o tráfego na camada de aplicação.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Qual é a história dos firewalls?

Assim como as capacidades de firewall evoluíram com o tempo, também evoluiu a forma como os firewalls são implantados. Originalmente, os firewalls eram dispositivos físicos de hardware que se conectavam à infraestrutura de rede de uma empresa. Mas à medida que os processos de negócios se deslocaram para a nuvem, a canalização de todo o tráfego de rede por uma caixa física se tornou ineficiente. Atualmente, os firewalls também podem ser executados em softwares ou virtualmente na nuvem.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### O que é iptables?

**Iptables é uma ferramenta de firewall** para sistemas Linux que atua como uma espécie de "guarda de fronteira" entre o seu computador e a internet. Ela **permite controlar o tráfego de rede**, decidindo quais conexões são permitidas e quais são bloqueadas.

Imagine o iptables como um segurança que verifica cada pacote de dados que chega ou sai do seu dispositivo, verificando se eles têm permissão para passar ou se devem ser barrados de acordo com as regras definidas.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### O que é iptables?

Essas regras podem ser configuradas para permitir que certos tipos de tráfego, como navegação na web, passem livremente, enquanto bloqueiam outras atividades maliciosas, como tentativas de invasão ou acesso não autorizado ao seu sistema.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tabelas e cadeias (Tables and chains)?

No iptables, existem **quatro tabelas principais**, cada uma com suas cadeias (chains) e propósitos específicos:

- **Tabela "filter":** Essa é a tabela padrão do iptables e é usada para filtrar o tráfego de pacotes com base em regras definidas. As três cadeias padrão nesta tabela são:
  - **INPUT**: Essa cadeia lida com pacotes destinados à própria máquina (tráfego de entrada).
  - **OUTPUT**: Essa cadeia lida com pacotes originados na própria máquina e enviados a outros destinos (tráfego de saída).
  - **FORWARD**: Essa cadeia lida com pacotes que estão apenas passando pelo sistema, atuando como um roteador.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

**Tabelas e cadeias (Tables and chains)?**

- **Tabela "nat" (Network Address Translation):** Essa tabela é usada para realizar a tradução de endereços de rede, geralmente usada para redirecionamento de portas (port forwarding) ou para mascaramento de endereços IP (SNAT – Source Network Address Translation). As cadeias padrão nesta tabela são:
  - **PREROUTING:** Essa cadeia é utilizada para modificar pacotes antes de serem roteados, permitindo o redirecionamento de portas.
  - **OUTPUT:** Esta cadeia é usada para modificar pacotes gerados localmente antes de saírem do sistema.
  - **POSTROUTING:** Esta cadeia é utilizada para modificar pacotes após o roteamento, geralmente usada para mascaramento de IP (SNAT).

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tabelas e cadeias (Tables and chains)?

- **Tabela "mangle":** A tabela mangle é usada para modificar os cabeçalhos dos pacotes. É usada principalmente para marcação de pacotes para posterior manipulação por outras regras ou ferramentas. As cadeias padrão nesta tabela são:
  - **PREROUTING:** Usada para modificar pacotes antes de serem roteados.
  - **INPUT:** Usada para modificar pacotes de entrada antes de serem entregues localmente.
  - **FORWARD:** Usada para modificar pacotes que estão apenas passando pelo sistema.
  - **OUTPUT:** Usada para modificar pacotes de saída antes de deixarem o sistema.
  - **POSTROUTING:** Usada para modificar pacotes após o roteamento.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Tabelas e cadeias (Tables and chains)?

- **Tabela "raw":** Essa tabela é usada principalmente para controlar o rastreamento de conexões, permitindo que os pacotes escapem do rastreamento feito pela tabela "conntrack". As cadeias padrão nesta tabela são:
  - **PREROUTING:** Usada para modificar pacotes antes de serem roteados.
  - **OUTPUT:** Usada para modificar pacotes gerados localmente antes de saírem do sistema.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Políticas padrão (Default Policies)

As “políticas padrão (default policies)" do iptables podem ser comparadas às regras iniciais de boas-vindas que você estabelece para todos os convidados da sua festa antes de fazer ajustes específicos para atender às suas necessidades de segurança e preferências. É como se você definisse previamente o comportamento padrão para o tráfego de entrada, saída e encaminhado, caso nenhuma regra específica seja aplicada a eles.

A política de uma cadeia pode ser configurada com três valores possíveis:

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Políticas padrão (Default Policies)

- **ACCEPT**: O tráfego correspondente é permitido.
- **DROP**: O tráfego correspondente é silenciosamente descartado, sem enviar nenhuma resposta.
- **REJECT**: O tráfego correspondente é descartado, mas é enviado uma resposta ICMP ao remetente informando que a conexão foi rejeitada.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Políticas padrão (Default Policies)

Veja um exemplo de regra do iptables:

```
iptables -P INPUT ACCEPT
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
```

Como não foi especificado a tabela dessa regra, por padrão a tabela selecionada é a filter (Tabela 1). A flag -P configura uma política padrão na cadeia.

Linha 1: A cadeia é INPUT e a política padrão definida é ACCEPT.

Linha 2: A cadeia é FORWARD e a política padrão definida é DROP.

Linha 3: A cadeia é OUTPUT e a política padrão definida é ACCEPT.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Comandos básicos do iptables

***Atenção! Antes de começarmos, é importante observar que para utilizar o iptables, é necessário ter permissões de superusuário (root).***

Existem comandos básicos para gerenciar o iptables através da linha de comando, confira a seguir alguns comandos básicos:

- **Exibindo as regras atuais**: Para verificar as regras já existentes no iptables, utilize o comando

```
sudo iptables -L
```

Isso listará as regras para todas as tabelas padrão (filter, nat e mangle).

```
root@vps-5524087.tutoriaishg.com [~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
cphulk     all  --  anywhere             anywhere
ACCEPT     all  --  179-108-123-250.static.ctbctelecom.com.br  anywhere
ACCEPT     all  --  216-172-160-201.unifiedlayer.com  anywhere
ACCEPT     all  --  anywhere             anywhere            /* Inbound Allow lo */
ACCEPT     tcp  --  anywhere             anywhere            tcp dpts:ndmps:65534
tcpchk     tcp  --  anywhere             anywhere
udpchk     udp  --  anywhere             anywhere
ipdrop_global  all  --  anywhere            anywhere
input_custom  all  --  anywhere            anywhere
ACCEPT     all  --  anywhere             anywhere
ssh        tcp  --  anywhere             anywhere            state NEW tcp dpt:ssh
ssh        tcp  --  anywhere             anywhere            state NEW tcp dpt:22022
ACCEPT     icmp --  anywhere             anywhere            icmp echo-request limit: up
10 mode srcip
```

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Comandos básicos do iptables

- **Limpando as regras**: Caso você tenha regras existentes que não deseja mais, pode limpá-las utilizando:

```
sudo iptables -F
```

***Atenção! Essa opção remove todas as regras de todas as cadeias (chains) nas tabelas. Para especificar uma tabela use o padrão abaixo:***

```
sudo iptables -F FORWARD
```

Este comando limpa todas as regras da cadeia FORWARD.

- **-F**: Indica que queremos limpar todas as regras da cadeia especificada.
- **FORWARD**: Especifica a cadeia a ser limpa.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Comandos básicos do iptables

```
sudo iptables -A OUTPUT -o eth0 -p udp --dport 53 -j DROP
```

Neste exemplo, estamos adicionando uma regra à cadeia de saída (OUTPUT) que bloqueia tráfego UDP na porta 53 (porta padrão do DNS) na interface de rede “eth0” (interface de rede de saída) e direcionando-o para a ação “DROP”, que descarta o pacote.

- -A: Adiciona a regra à cadeia especificada.
- -o: Especifica a interface de rede de saída para onde o tráfego está sendo enviado.
- -p: Especifica o protocolo do pacote (neste caso, UDP).
- --dport: Especifica a porta de destino do pacote.
- -j: Indica a ação a ser tomada se a regra for correspondida (neste caso, DROP).

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Comandos básicos do iptables

- **Remover uma regra específica:**

```
sudo iptables -D INPUT 3
```

Este comando remove a terceira regra da cadeia de entrada (INPUT).

- **-D:** Indica que estamos excluindo uma regra.
- **INPUT**: Especifica a cadeia da qual a regra será removida.
- **3:** É o número da regra que será excluída. Você pode ver os números das regras usando o comando iptables -L numerado.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Comandos básicos do iptables

Essas são apenas algumas das muitas possibilidades do iptables. Lembre-se de que, ao alterar as regras do firewall, é importante ter cuidado para não bloquear o acesso ao seu sistema inadvertidamente. Sempre teste suas regras antes de aplicá-las permanentemente, especialmente se estiver trabalhando remotamente em um servidor.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Salvando e restaurando regras

Uma parte essencial da administração do iptables é a capacidade de salvar e restaurar as regras criadas no firewall. Isso é particularmente importante porque, ao reiniciar o sistema ou após uma falha, todas as regras definidas serão perdidas se não forem salvas adequadamente.

Aqui estão as etapas para salvar e restaurar as regras do iptables de forma fácil e segura:

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Salvando e restaurando regras

- **Salvando as regras**: Para salvar as regras do iptables, você precisa usar o comando iptables-save. Este comando exibe as regras do iptables em um formato legível por máquina, permitindo que você redirecione a saída para um arquivo.

  Passo a passo:

  1. Abra o terminal ou a linha de comando no seu sistema.
  2. Use o comando iptables-save para exibir as regras atuais do iptables no seu terminal.
  3. Redirecione a saída para um arquivo de texto. Por exemplo, para salvar as regras em um arquivo chamado regras-iptables.txt, você pode usar o seguinte comando:

```
iptables-save > regras-iptables.txt
```

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Salvando e restaurando regras

- **Restaurando as regras:** Após salvar as regras em um arquivo, você pode restaurá-las a qualquer momento usando o utilitário iptables-restore. Esse comando lerá o arquivo de texto contendo as regras salvas e as aplicará no iptables.

**Passo a passo:**

1. Verifique se você tem um arquivo contendo as regras salvas. No nosso exemplo, o arquivo é **regras-iptables.txt**.
2. Abra o terminal ou a linha de comando no seu sistema.
3. Use o comando **iptables-restore** e especifique o arquivo contendo as regras para restaurá-las:

```
iptables-restore < regras-iptables.txt
```

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Salvando e restaurando regras

**Dicas importantes:**

- Certifique-se de que está executando os comandos acima com privilégios de superusuário (root) para que as alterações sejam aplicadas corretamente.
- Sempre salve as regras em um local seguro, preferencialmente fora do diretório /tmp, para evitar perdas acidentais ou exclusão durante a limpeza do sistema.
- Ao restaurar regras, verifique se você está restaurando para o mesmo ambiente ou sistema semelhante, pois regras incompatíveis podem causar problemas na rede.

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Salvando e restaurando regras

**Dica Pro:** Para evitar a perda de regras toda vez que o sistema é reiniciado, você pode automatizar o processo de restauração durante o processo de inicialização utilizando uma **cronjob**. Para isso, você pode criar um script que contém o comando **iptables-restore** com o arquivo de regras adequado e, em seguida, configurar esse script para ser executado na inicialização do sistema (usando: "@reboot comando_a_ser_executado").

# Segurança da Informação

## Segurança em redes - IDS - Firewalls - IP tables

### Considerações Finais

Este texto abordou diversas características do iptables, mas há muito mais para aprender sobre suas funcionalidades avançadas e opções adicionais. Certifique-se de consultar a documentação oficial e tutoriais para aprofundar seus conhecimentos e utilização do iptables.

# Referências


- **IBM**

  https://www.ibm.com/br-pt/topics/network-security

  https://www.ibm.com/br-pt/topics/intrusion-detection-system

- **CloudFlare**

  https://www.cloudflare.com/pt-br/learning/security/what-is-a-firewall/

- **Hostgator**

  https://www.hostgator.com.br/blog/guia-iptables/