Firewalls

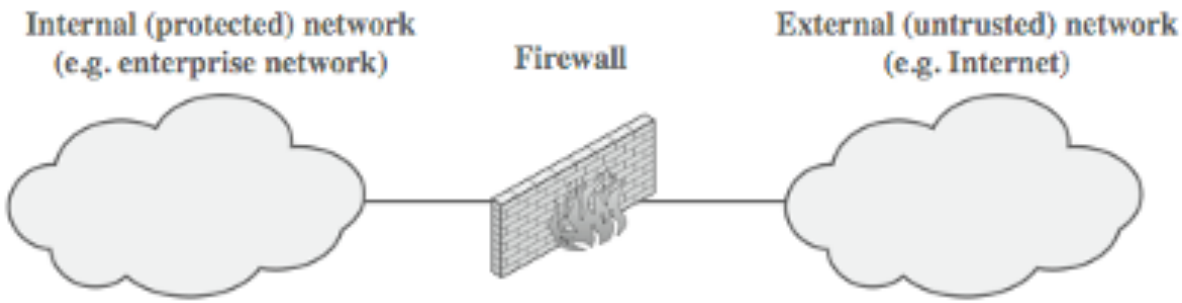
Objetivos

- Explicar o papel de firewalls como parte de uma estratégia de segurança de computadores e redes.
  - Segurança em profundidade
- Listar as características principais dos firewalls.
- Discutir as várias opções de implantação para firewalls.
- Entender os méritos relativos de várias opções de localização e configuração de firewalls.
- Discutir entre firewalls e sistemas de prevenção de intrusão.
- Discutir o conceito de sistema unificado de gerenciamento de ameaças

O Firewall

- Função: fornecer camada adicional de proteção a partes de uma rede
  - ”isolar” segmentos de rede
- Metas de projeto
  - Todo o tráfego deve passar pelo (chegar ao) firewall
  - Somente tráfego autorizado (como definido pela política de segurança) terá permissão de passar
  - O firewall em si é imune à penetração

Visualização de um firewall



Objetivos

- Controle de serviço:
  - Determina os tipos de serviços da Internet que podem ser acessados de dentro para fora e de fora para dentro da rede.
- Controle de direção:
  - Determina a direção na qual determinadas requisições de serviço podem ser iniciadas e têm permissão de transitar pelo firewall.
- Controle de usuário:
  - Controla acesso a um serviço de acordo com o usuário que está tentando acessá-lo
- Controle de comportamento:
  - Controla o modo de utilização de determinados serviços

O que é um Firewall?

- Um ponto de estrangulamento e monitoramento
- Interconecta redes com níveis de confiança distintos
- Impõe restrições a serviços de rede
  - Apenas tráfego autorizado (aderente à política de segurança) é permitido
- Auditoria e controle de acesso
  - Pode incluir alarmes por comportamento anormal
- Pode incluir serviços não-diretamente relacionados à segurança
  - NAT, Proxy de conteúdo, monitoramento,...
- Pode implementar VPNs usando IPSec
- Deve ser imune a ataques

Limitações de Firewall

- Não protege contra ataques que o bypassem
  - Dispositivos estranhos na rede interna, acessos remotos não mapeados, serviços confiáveis (eg SSL/SSH)
- Não protege contra ameaças internas
  - Sysadmins ou empregados insatisfeitos,
- Não protege contra ameaças importadas por meio de dispositivos inseridos na redes – notebooks, PDAs, pen-drives,...

Necessidade de firewalls

- Evolução evidente dos sistemas de informação
  - Virtualmente "todos estão na Internet"
  - e interconectam redes
- Preocupações constantes com segurança
  - impossível tornar seguros todos os sistemas de uma organização
- Firewall fornece uma primeira linha de defesa
  - Tipicamente, defesa de perímetro
  - Também serve para isolar segmentos de rede com diferentes características de segurança
- É parte de uma solução abrangente de segurança
  - Defesa em profundidade

Tipos de Firewall

- Filtro de pacotes
- Inspeção com estado
- Gateway de nível de aplicação
- Gateway de nível de circuito

Firewalls – Filtros de Pacotes

- modelo mais simples e rápido de firewall
- fundamento de qualquer sistema de firewall
- examina cada pacote IP (sem avaiar contexto) e permite ou nega de acordo com regras
- restringe acesso a serviços (portas)
- políticas ”default”:
  - default deny: tudo o que não é expressamente permitido é proibido
  - default accept: tudo o que não é expressamente proibido é permitido

Ataques a Filtros de Pacotes

- Spoofing de endereço IP
  - ataque: endereço de origem falso
  - mitigação: adicionar filtro para bloquear pacotes com endereço interno vindo do mundo externo
- Source routing
  - ataque: atacante define a rota do pacote
  - mitigação: bloquear pacotes source routed
- Pacoted fragmentados
  - ataque: dividir pacote em vários pequenos pacotes
  - mitigação: descartar ou reconstruir antes de verificar

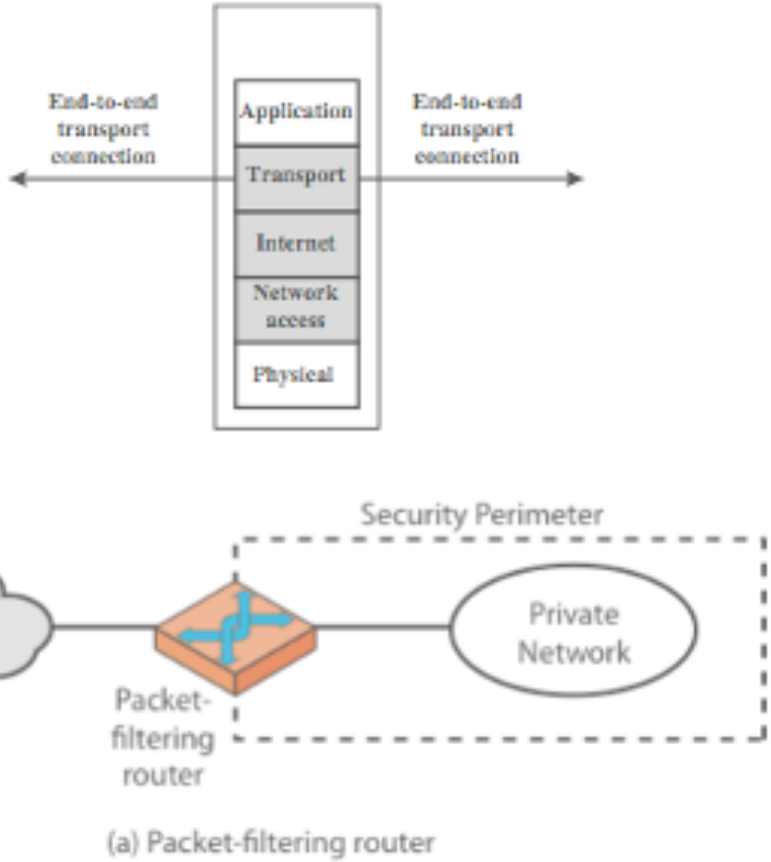
Filtro de pacotes

- aplica um conjunto de regras a cada pacote IP que chega e que sai, e então transmite ou descarta o pacote
- tipicamente configurado para filtrar pacotes que transitam em ambas as direções
- Regras de filtragem baseadas em informações contidas em um pacote de rede
  - Endereço IP de origem
  - Endereço IP de destino
  - Endereços de origem e de destino no nível de transporte
  - Campo IP de protocolo
  - Interface

Filtro de pacotes – políticas

- O filtro de pacotes é normalmente composto por uma lista de regras baseadas em correspondências com campos no cabeçalho IP ou TCP.
  - Se houver correspondência com uma das regras, essa regra é invocada para determinar se o pacote deve ser transmitido ou descartado.
  - Se não houver correspondência com qualquer regra, uma ação padrão é executada.
- Duas políticas padrão são possíveis
  - Padrão = descartar: Aquilo que não é expressamente permitido é proibido
  - Padrão = transmitir: Aquilo que não é expressamente proibido é permitido.
- A política padrão de descartar é mais conservadora.

Firewalls – Filtros de Pacotes



(a) Packet-filtering router

Firewalls – Filtros de Pacotes

Table 20.1 Packet-Filtering Examples

A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Filtro de pac. – vantagens e desvantagens

- Vantagens
  - Simplicidade
  - Velocidade
- Desvantagens
  - Não protegem contra ataques em camada de aplicação
  - Não suporta esquemas avançados de autenticação de usuários
  - vulneráveis a problemas estruturais do TCP/IP (e.g. falsificação de endereço IP)
  - Impossibilidade de usar regras mais complexas/sofisticadas

Filtro de pacotes – exemplos de ataques

- Falsificação de endereço IP
  - O intruso transmite pacotes que vêm de fora da rede com um campo de endereço IP de origem
- Ataques de roteamento baseado na origem
  - A estação de origem especifica a rota que um pacote deve seguir ao atravessar a Internet, na esperança de que isso o desviará de medidas de segurança que não analisam informações de roteamento baseado na origem.
- Ataques de fragmentos minúsculos
  - O intruso usa a opção de fragmentação do IP para criar fragmentos extremamente pequenos e forçar que a informação do cabeçalho TCP fique em um fragmento de pacote separado.

Firewalls com inspeção de estado

- Filtros de pacotes tradicionais não examinam contexto em camadas superiores
- filtros com inspeção de estado abordam tal necessidade
- examinam cada pacote IP dentro de um contexto
  - mantêm registro de sessões
  - avaliam se cada pacote pretence a uma sessão
- são capazes, portanto, de detectar pacotes fora de contexto.
- Podem inspecionar dados de aplicação

Inspeção com estado

- Leva em consideração o ”contexto” de uma comunicação
  - Em oposição ao filtro de pacotes, que analisa pacotes individualmente
- Na prática: mapeia as conexões TCP em andamento, implementando política restritiva para conexões de entrada para ”portas com números elevados”
  - Em firewall sem estado, essas portas altas precisam ficar liberadas por defaul

Exemplo de tabela de estados de conexão

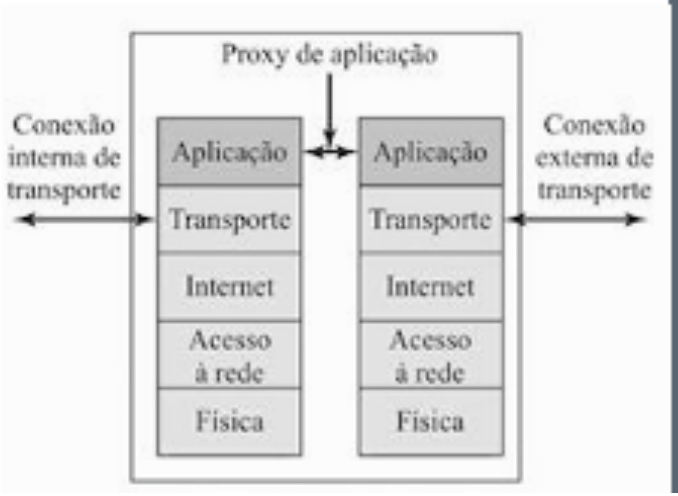
Endereço de origem	Porta de origem	Endereço de destino	Porta de destino	Estado da conexão
192.168.1.100	1030	210.9.88.29	80	Estabelecida
192.168.1.102	1031	216.32.42.123	80	Estabelecida
192.168.1.101	1033	173.66.32.122	25	Estabelecida
192.168.1.106	1035	177.231.32.12	79	Estabelecida
223.43.21.231	1990	192.168.1.6	80	Estabelecida
219.22.123.32	2112	192.168.1.6	80	Estabelecida
210.99.212.18	3321	192.168.1.6	80	Estabelecida
24.102.32.23	1025	192.168.1.6	80	Estabelecida
223.21.22.12	1046	192.168.1.6	80	Estabelecida

Gateway de nível de aplicação

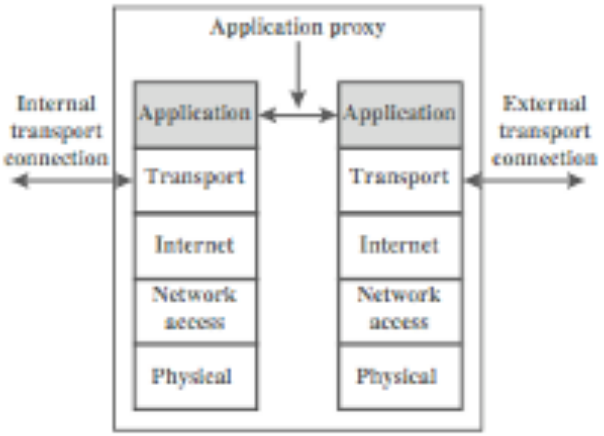
- possui gateway/proxy específico de aplicação
- possui acesso total ao protocolo
  - usuário solicita serviço do proxy
  - proxy valida solicitação
  - todas as ações e comunicações passam pelo proxy
  - pode-se gerar logs e registros de eventos em nível de aplicação
- necessário um proxy para cada serviço
  - dificuldade varia de acordo com o serviço

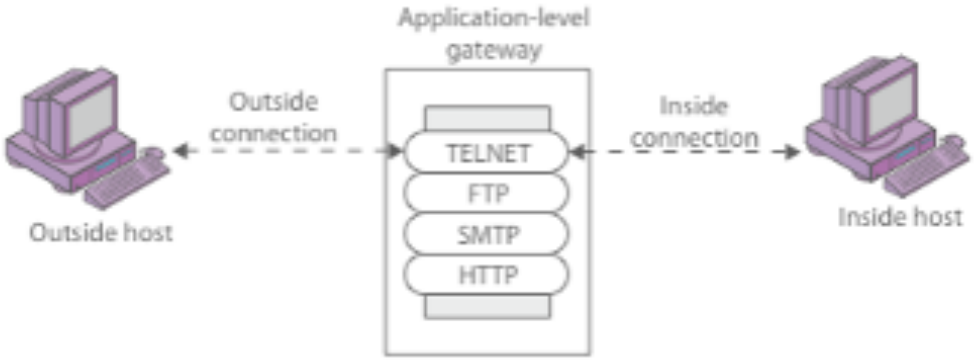
Gateway de nível de aplicação

- Retransmissor de tráfego no nível de aplicação
- Etapas:
  - Usuário contata o gateway, informando credenciais de acesso, aplicação (e.g. FTP) e estação remota
  - Gateway conecta estação remota
  - Gateway passa a retransmitir segmentos TCP
- Se o serviço não for suportado, o gateway não transmite
- Mais seguro porque o gateway analisa muito menos dados
- Desvantagem: custo de cada conexão



Gateway de nível de aplicação





(b) Application-level gateway

Gateway em nível de circuito

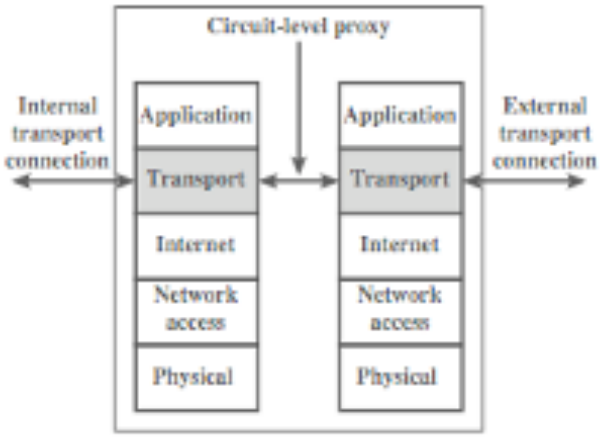
- conecta (retransmite) dois ”circuitos” (conexões) TCP
- impõe segurança a o limitar as conexões permitidas
- uma vez estabelecida a conexão, simplesmente retransmite, sem examinar conteúdo
- tipicamente, confia em usuários internos, permitindo conexões com o mundo exterior
- SOCKS é um padrão de facto
  - RFC 1928

Gateway de nível de circuito

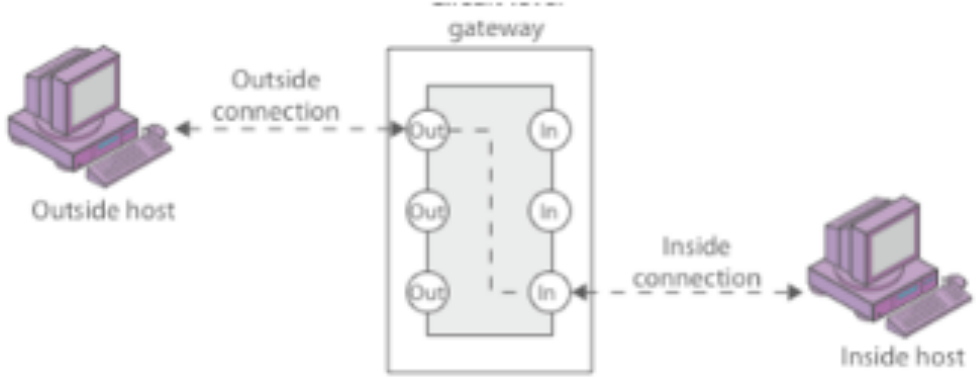
- Também é uma espécie de retransmissor
- Gateway estabelece duas conexões TCP

- Conexão TCP não é examinada
  - Segurança está em determinar quais conexões serão permitidas
- Pode ser um sistema autônomo ou uma função especializada executada por um gateway de nível de aplicação

Gateway em nível de circuito



(e) Circuit-level proxy firewall



(c) Circuit-level gateway

Bastion Host (Bastião)

- host altamente seguro para segurança de redes
  - executa gateways de nível de circuito ou aplicação
- provê serviços acessíveis externamente
- potencialmente exposto a elementos hostis
- portanto, deve ser seguro para defender-se
  - sistema operacional fortalecido, autenticação extra, apenas serviços essenciaismay support 2 or more net connections
- confiável o suficiente para promover separação entre as redes

Firewalls baseados em Host

- módulo de software usado para proteger host individual
  - disponível em muitos sistemas operacionais
  - pode ser disponibilizado como um pacote add-on
- fequentemente usado em servidores
- vantegens:
  - pode ajustar as regras de fltragem de acordo com o ambiente do host
  - proteção independente de topologia
  - mais uma camada de proteção

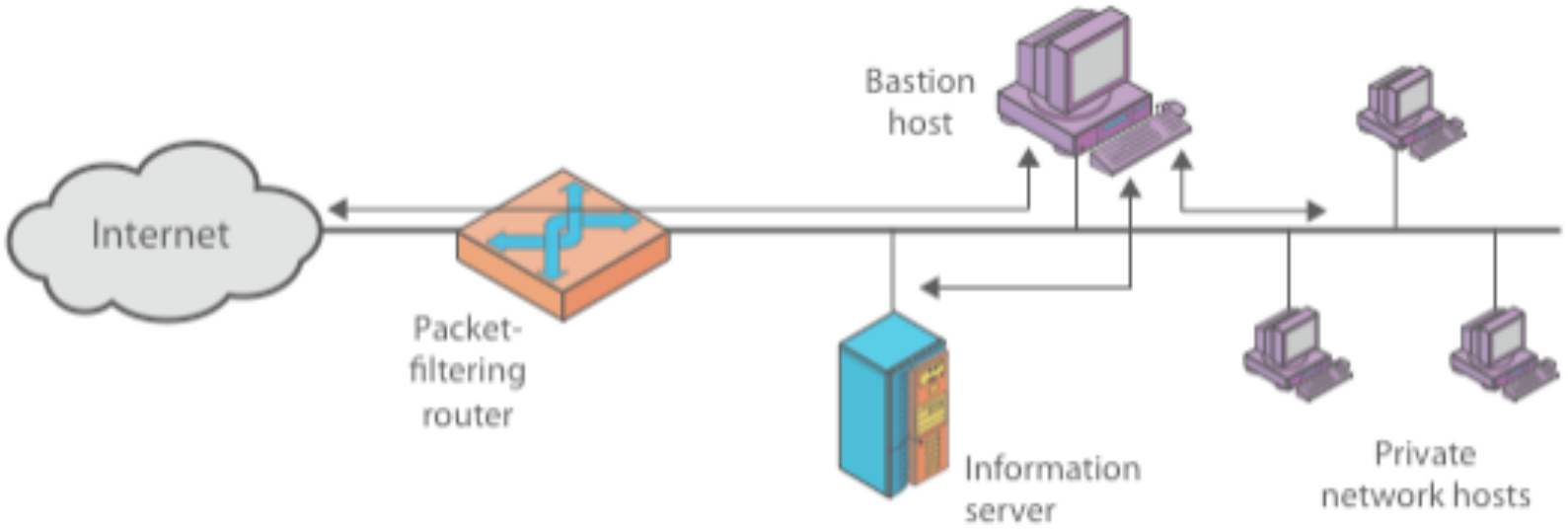
Firewalls Pessoais

- controla o tráfego entre computador pessoal e a rede em que ele está conectado
- geralmente, um módulo de software num computador pessoal
  - ou em roteador DSL/cabo/ISP em casa ou escritório
- tipicamente, muito menos complexo que outros tipos de firewall
- Pode monitorar atividades de malware

Localização e Topologias de Firewall

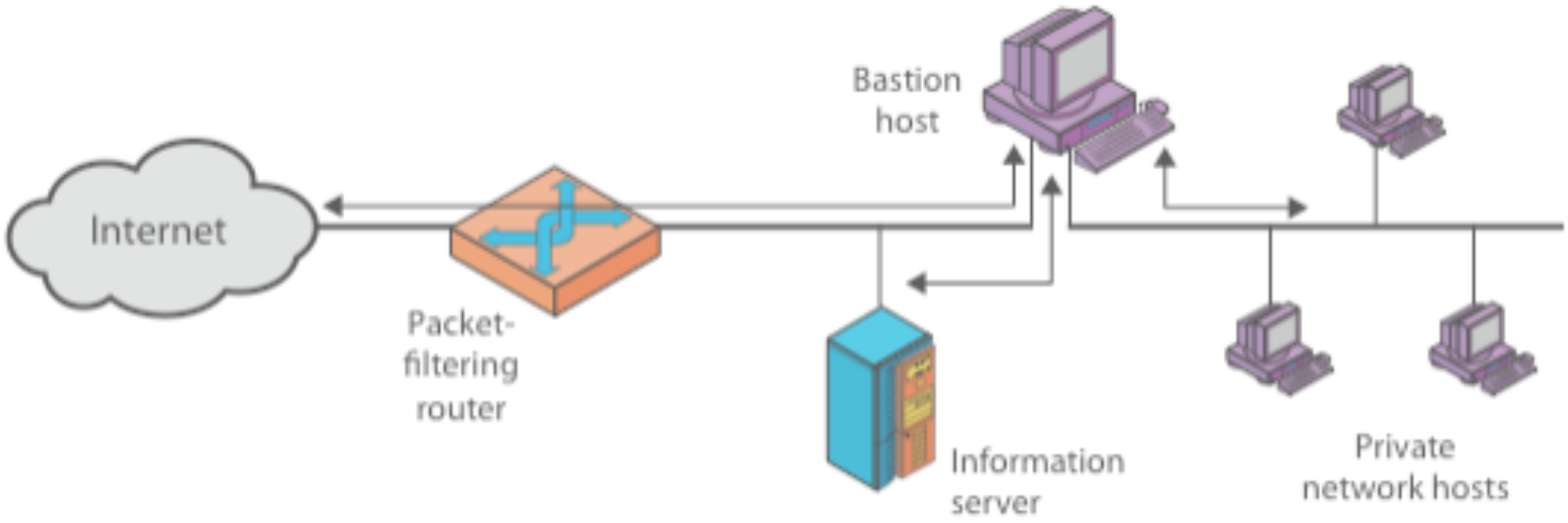
- host-resident firewall
- screening router
- single bastion inline
- single bastion T
- double bastion inline
- double bastion T
- distributed firewall configuration

Configurações de Firewall



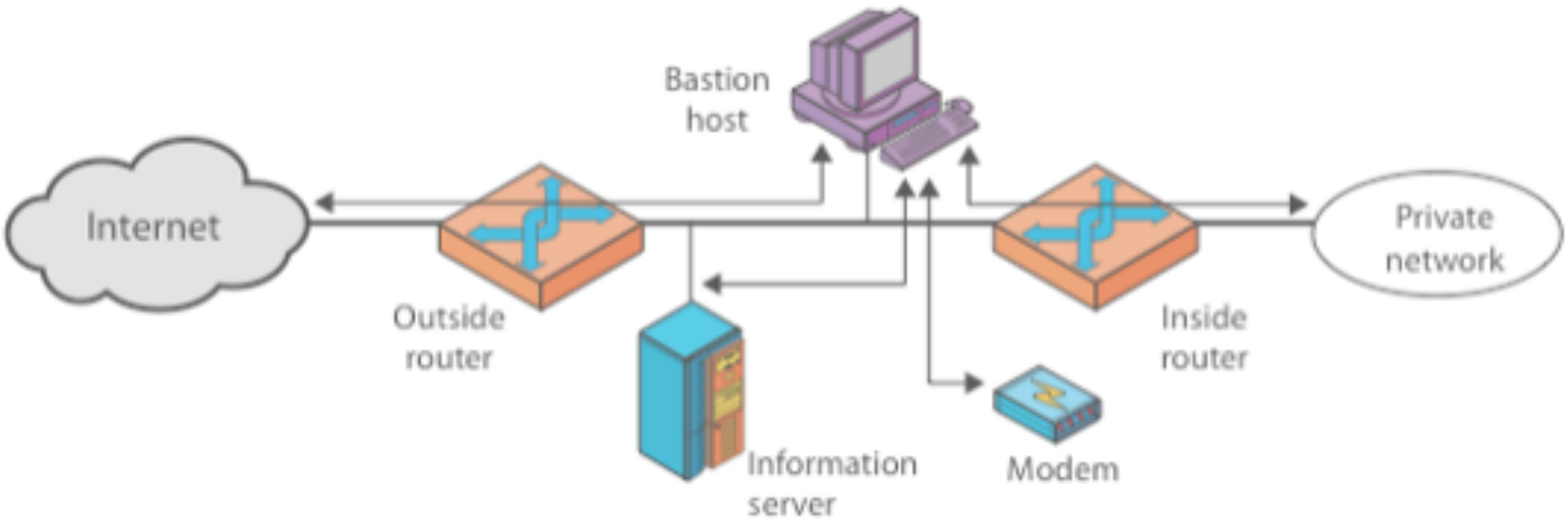
(a) Screened host firewall system (single-homed bastion host)

Configurações de Firewall



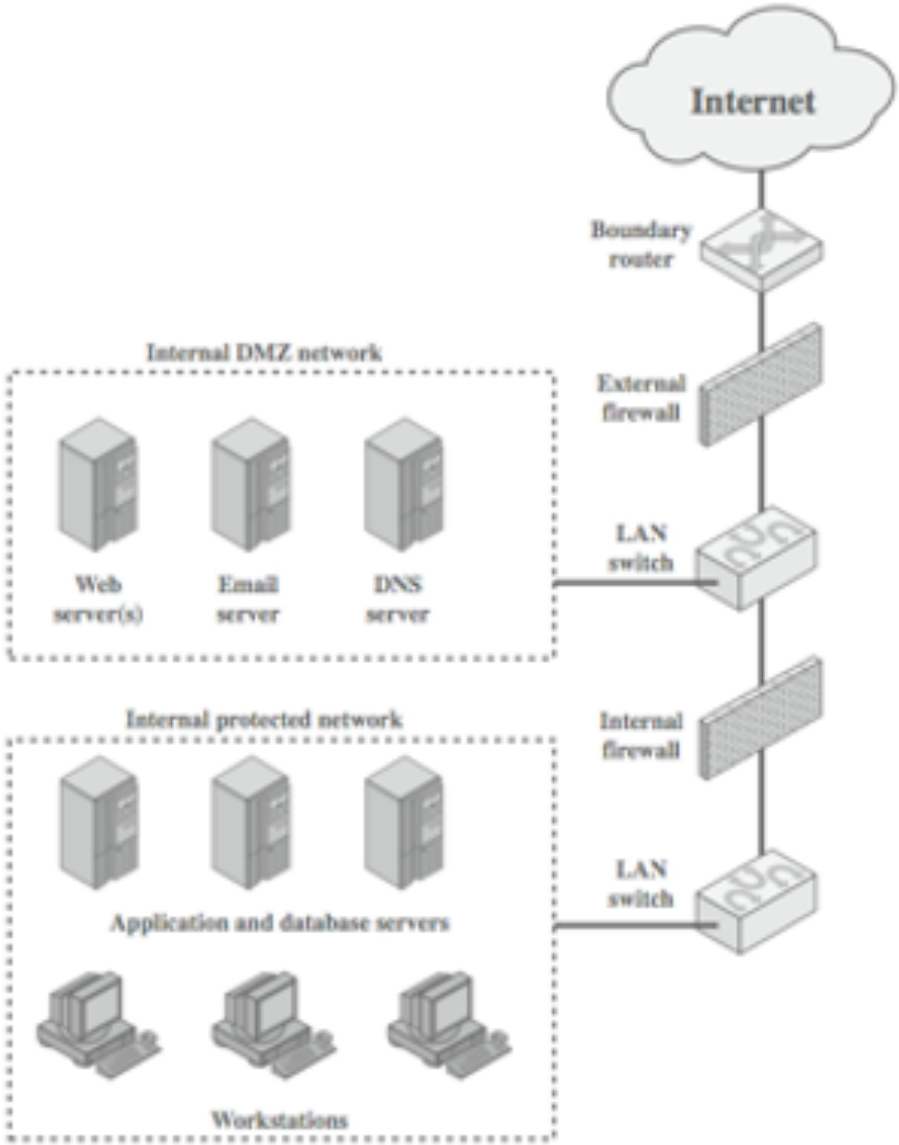
(b) Screened host firewall system (dual-homed bastion host)

Configurações de Firewall

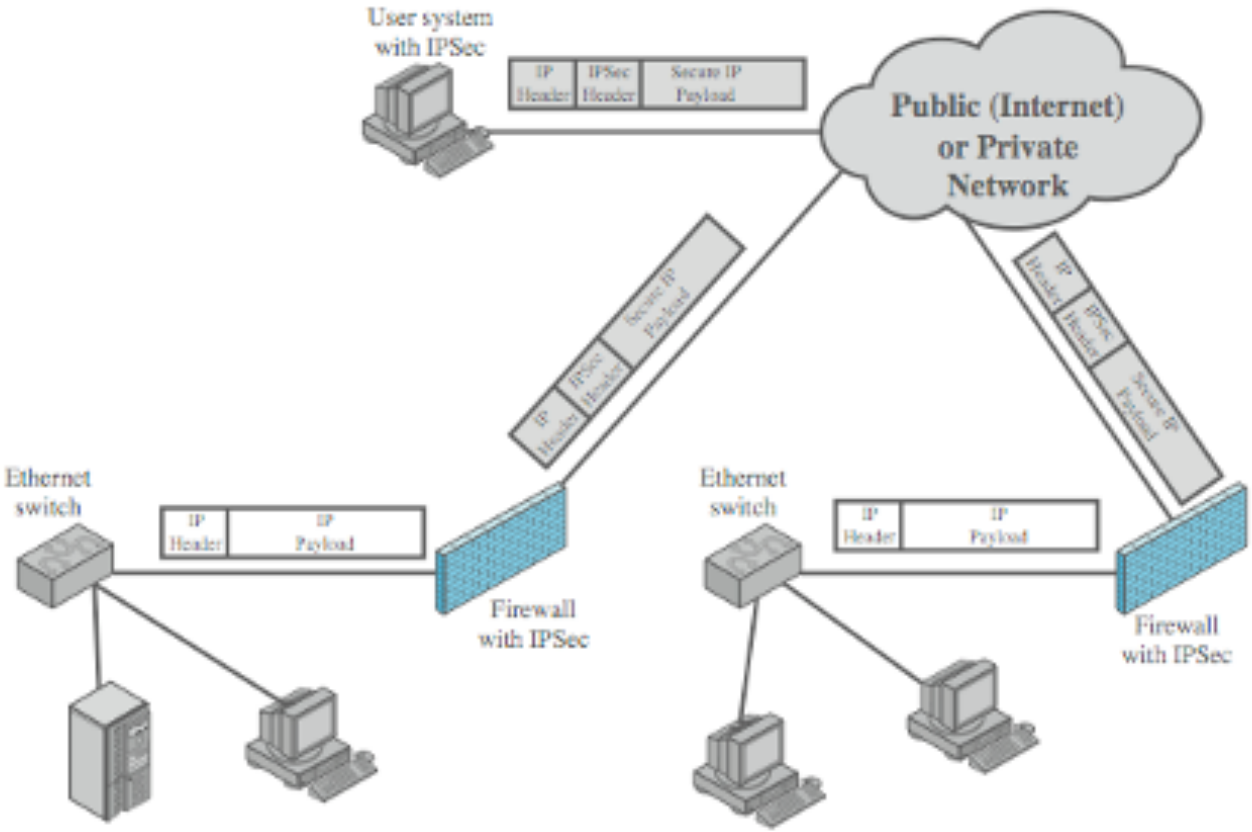


(c) Screened-subnet firewall system

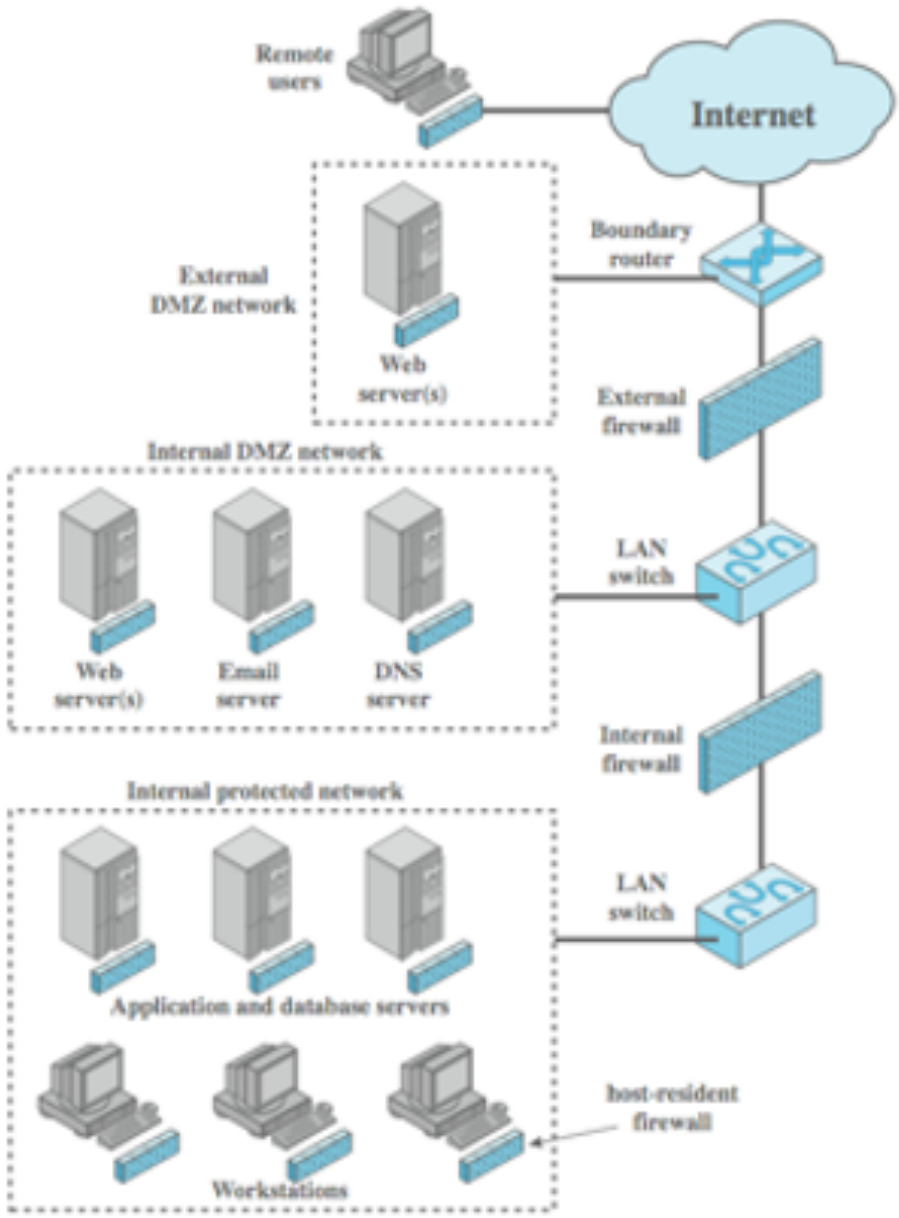
Redes DMZ


Internet
Boundary router
External firewall
LAN switch
Internal DMZ network
Web server(s)
Email server
DNS server
Internal firewall
LAN switch
Internal protected network
Application and database servers
Workstations

VPNs (Virtual Private Networks)



Distributed Firewalls



Resumo

- Estudamos
  - firewalls
  - Tipos de Firewall
    - filtro de pacotes, inspeção de estado, proxy de aplicação, nível de circuito
  - ambiente de instalação do firewall
    - bastião, host, pessoal
  - localização, arquitetura e configurações
    - DMZ, VPN, distribuído, topologias

Conclusões – segurança de firewall

- Firewall podem proteger um ambiente apenas se são capazes de controlar todo o perímetro
- Firewall não protegem recursos fora do perímetro
- Firewall são o componente de rede mais visível no mundo externo – portanto, mais suscetíveis a ataques
- Configurações do firewall devem ser frequentemente revistas

Network Address Translation (NAT)

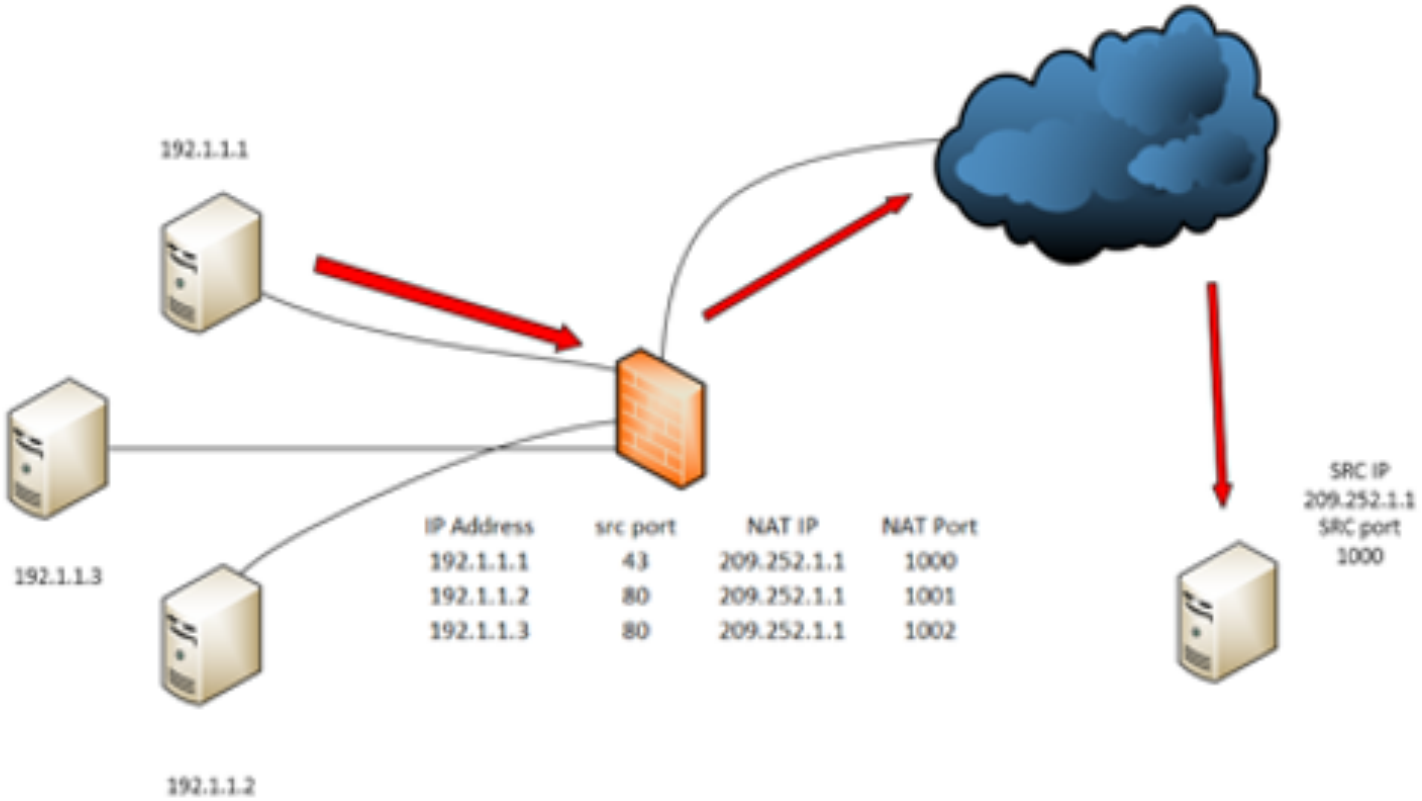
Network Address Translation (NAT)

- NAT é, na verdade, uma solução temporária para o "esgotamento de endereços IP" no IPv4
  - Descrito na RFC 1631
  - No modelo IPv6, esse problema desaparece
- NAT é um gateway "mapeia" endereços globais válidos da Internet para endereços de hosts internos de uma rede
- Desta forma, o uso NAT reduz a visibilidade externa sobre detalhes da topologia interna
  - Esconde vários hosts atrás de um único endereço IP
  - Muitos acreditam que existem benefícios de segurança no uso de NAT

Implementação do NAT

- NAT é um recurso de roteamento, mas frequentemente implementado no firewall
  - **Não** é um recurso de segurança – mas pode ajudar...
- Diversos tipos de mapeamento possíveis
  - Estático: endereço IP interno é mapeado para um endereço IP globalmente válido
  - Dinâmico: vários endereços IP internos são mapeados para um único endereço IP globalmente válido
    - Uma estratégia para isso é usar "portas" para ajudar neste mapeamento (estratégia denominada PAT)

Implementação do NAT



Guia para firewalls e políticas de firewall

Visão do padrão NIST SP 800-41

Tecnologias de Firewall

- Definição
  - *Firewalls* are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures
- Várias tecnologias disponíveis
  - One way of comparing their capabilities is to look at the Transmission Control Protocol/Internet Protocol (TCP/IP) layers that each is able to examine
  - Basic firewalls operate on one or a few layers—typically the lower layers—while more advanced firewalls examine all of the layers

Tecnologias de Firewall

- Firewalls e roteamento
  - Firewalling is often combined with other technologies—most notably routing—and many technologies often associated with firewalls are more accurately part of these other technologies
  - For example, network address translation (NAT) is sometimes thought of as a firewall technology, but it is actually a routing technology.
- Firewalls e filtros de conteúdo
  - Many firewalls include content filtering features to enforce organization policies not directly related to security.
- Firewalls e IDPS
  - Some firewalls include intrusion prevention system (IPS) technologies

Firewalls na prática

Opções de firewall

› Dispositivos comerciais (Cisco, Fortinet, PaloAlto,...)

Figure 1. Magic Quadrant for Enterprise Network Firewalls

Source: Gartner (October 2018)


FORTINET


AKER
FIREWALL UTM


paloalto

Opções de firewall

- Appliances comerciais (Cisco, Fortinet, PaloAlto,...) e roteadores (ACLs)
- Pacotes de software (Kaspersky, McAfee, Norton, Avast,...)


Norton Personal Firewall
Block Traffic
LiveUpdate
Options
Help & Support
Norton Protection Center
Norton Personal Firewall
Status & Settings
Statistics
Subscription Status
Norton Personal Firewall
Security On
Personal Firewall On
Intrusion Prevention On
On
On
Privacy Control
Privacy Control helps protect your personal information.
More Info
Turn Off
Configure
symantec.
Norton
2004
Personal Firewall
Keeps hackers out and personal data in


Avast Premier
Application Rules
Filter:
Flatten view
Application
Allowed connections
Microsoft Corporation
App UX Handlers Registration V...
Internet out (otherwise auto-decide)
Background Task Host
Internet out (otherwise auto-decide)
Download/Upload Host
Internet out (otherwise auto-decide)
Host Process for Windows Servi...
All connections
FILE DETAILS
Check paths
New Group
New application rule
Close


Kaspersky Internet Security
KASPERSKY
Settings
General
Protection
Performance
Scan
Additional
1
2
File Anti-Virus
Web Anti-Virus
Application Control
Firewall
Private Browsing
Webcam Protection
Software Updater
Anti-Banner
Other products
My Kaspersky


KASPERSKY
Kaspersky
INTERNET SECURITY
2018


Segurança e Privacidade
Buscar
Bloquear todas as conexões de entrada
Bloqueia todas as conexões de entrada, exceto aquelas necessárias para serviços básicos de Internet, como DHCP, Bonjour e IPSec.
com.apple.WebKit.Networking.xpc
Permitir conexões de entrada
Dropbox.app
Permitir conexões de entrada
GarageBand.app
Permitir conexões de entrada
IRPF2019.app
Permitir conexões de entrada
Skype.app
Permitir conexões de entrada
Spotify.app
Permitir conexões de entrada
Permitir que o software integrado receba conexões de entrada automaticamente
Permitir que o software transferido receba conexões de entrada automaticamente
Permite que aplicativos assinados por uma autoridade de certificação válida forneçam serviços acessados por meio da rede.
Ativar modo discreto
Não responde ou não reconhece tentativas de acesso a este computador realizadas via rede por aplicativos de teste que usem o protocolo ICMP, como Ping.
Cancelar
OK
Clique no cadeado para evitar alterações.
Avançado...

Opções de firewall

- Appliances comerciais (Cisco, Fortinet, PaloAlto,...) e roteadores (ACLs)
- Pacotes de software (Kaspersky, McAfee, Norton, Avast,...)
- Open source – Linux IPTables

```
root@cbz01:~#
root@cbz01:~# iptables -S INPUT
-P INPUT DROP
-A INPUT -i lxdbr0 -p tcp -m tcp --dport 53 -m comment --comment "generated for LXD network lxdbr0" -j ACCEPT
-A INPUT -i lxdbr0 -p udp -m udp --dport 53 -m comment --comment "generated for LXD network lxdbr0" -j ACCEPT
-A INPUT -i lxdbr0 -p udp -m udp --dport 67 -m comment --comment "generated for LXD network lxdbr0" -j ACCEPT
-A INPUT -j ufw-before-logging-input
-A INPUT -j ufw-before-input
-A INPUT -j ufw-after-input
-A INPUT -j ufw-after-logging-input
-A INPUT -j ufw-reject-input
-A INPUT -j ufw-track-input
root@cbz01:~#
root@cbz01:~#
root@cbz01:~# iptables -S OUTPUT
-P OUTPUT ACCEPT
-A OUTPUT -o lxdbr0 -p tcp -m tcp --sport 53 -m comment --comment "generated for LXD network lxdbr0" -j ACCEPT
-A OUTPUT -o lxdbr0 -p udp -m udp --sport 53 -m comment --comment "generated for LXD network lxdbr0" -j ACCEPT
-A OUTPUT -o lxdbr0 -p udp -m udp --sport 67 -m comment --comment "generated for LXD network lxdbr0" -j ACCEPT
-A OUTPUT -j ufw-before-logging-output
-A OUTPUT -j ufw-before-output
-A OUTPUT -j ufw-after-output
-A OUTPUT -j ufw-after-logging-output
-A OUTPUT -j ufw-reject-output
-A OUTPUT -j ufw-track-output
root@cbz01:~#
```

Exemplos de comandos IPTables

- Bloquear um endereço específico
  - Caso seja identificada atividade não-usual ou abusiba originada de um endereço de IP específico é possível bloquear:
    - `# iptables -A INPUT -s xxx.xxx.xxx.xxx -j DROP`
  - Caso deseje bloquear apenas tráfego TCP, é possível usar o –p, que especifica o protocolo:
    - `# iptables -A INPUT -p tcp -s xxx.xxx.xxx.xxx -j DROP`
- Desbloquear endereço IP
  - Caso queira remover o IP, usa-se o seguinte comando:
    - `# iptables -D INPUT -s xxx.xxx.xxx.xxx -j DROP`

Exemplos de comandos IPTables

- Bloquear uma porta específica
  - Bloquear conexões de entrada numa porta específica:
    - `# iptables -A OUTPUT -p tcp --dport xxx -j DROP`
  - Para permitir conexões de saída usar:
    - `# iptables -A INPUT -p tcp --dport xxx -j ACCEPT`
- Permitir múltiplas portas (com multiport)
  - Regras para conexões de entrada e de asída:
    - `# iptables -A INPUT -p tcp -m multiport --dports 22,80,443 -j ACCEPT`
    - `# iptables -A OUTPUT -p tcp -m multiport --sports 22,80,443 -j ACCEPT`

Exemplos de comandos IPTables

- Bloquear Flood no webserver
  - Mitigação de cenários de sobrecarga com a seguinte regra:
    - `# iptables -A INPUT -p tcp --dport 80 -m limit --limit 100/minute --limit-burst 200 -j ACCEPT`
- Bloquear pacotes PING de entrada
  - Uma boa prática de segurança é bloquear ping (protocolo ICMP), o que pode ser feito com a seguinte regra:
    - `# iptables -A INPUT -p icmp -i eth0 -j DROP`

Exemplos de comandos IPTables

- Manter log de pacotes descartados
  - É possível manter o registro dos pacotes decartados. Por exemplo, para pacotes descartados pela interface de rede eth0, é possível usar o seguinte comando:
    - `# iptables -A INPUT -i eth0 -j LOG --log-prefix "IPtables dropped packets:"`
- Bloquear acesso a um endereço MAC específico
  - É possível bloquear acesso a um endereço MAC específico:
    - `# iptables -A INPUT -m mac --mac-source 00:00:00:00:00:00 -j DROP`
- Limitar o número de conexões por endereço IP
  - Impede o estabelecimento de muitas conexões concorrentes para o mesmo endereço IP:
    - `# iptables -A INPUT -p tcp --syn --dport 22 -m connlimit --connlimit-above 3 -j REJECT`