UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia e Certificação Digital
Sétima Aula

Prof. Frederico Sauer, D.Sc.

Detecção de Intrusos

- Intrusos são pessoas ou programas que acessam indevidamente sistemas alheios
- Categorias:
  - *Mascarader* – faz-se passar por um usuário legítimo
  - *Misfeasor* – é usuário legítimo, mas usa seus diretos de forma indevida
  - *Clandestine* – burla segurança para ganhar acesso
- Ataques são documentados por CERTs

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Técnicas de Intrusão

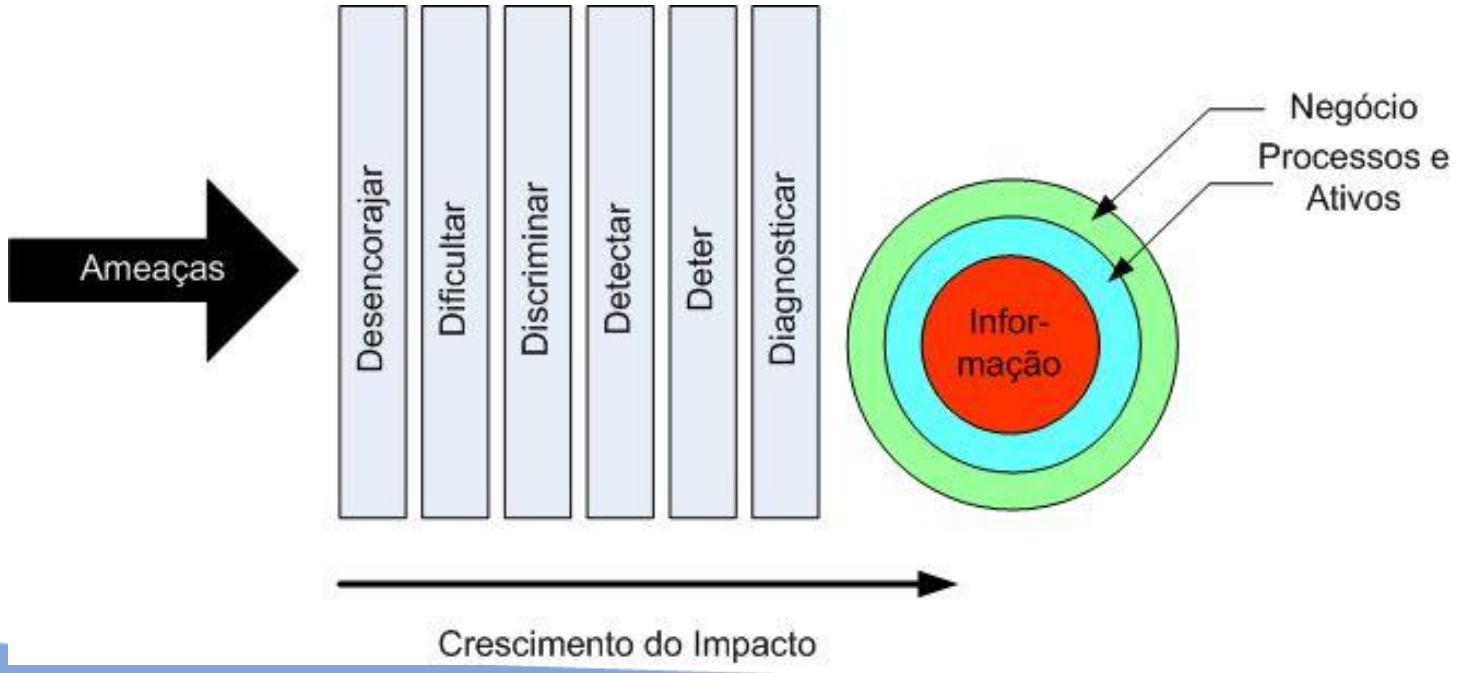
- Metodologia básica
  - Descobrir vulnerabilidades
    - Localizar, identificar, dissecar, escolher ferramenta
  - Ganhar acesso
    - Usar falhas conhecidas via rede (*exploits*), descoberta e uso de senhas (adivinhação, sniffing, engenharia social ou brute force), seqüestro de conexão
  - Aumentar privilégios (obter controle)
    - A quebra de um serviço tipicamente leva ao acesso como *root* ou administrador. Ex.: *rootkits*
    - A instalação de um *backdoor* garante retorno simplificado
  - Apagar “rastros”
- Ferramentas
  - Nmap, dsniff, nbaudit, juggernaut, nessus, trinoo, etc

Senhas

- Proteção dos arquivos de senhas
  - Função unidirecional (hash)
  - Controle de acesso
- *Guessing offline*
  - defaults, senhas simples (1234), palavras dicionarizadas
  - Informações do próprio usuário (sobrenomes, datas, interesses peculiares)
  - Busca exaustiva
- Outras técnicas
  - Observar a digitação, *keyloggers*, monitoramento de conexões inseguras

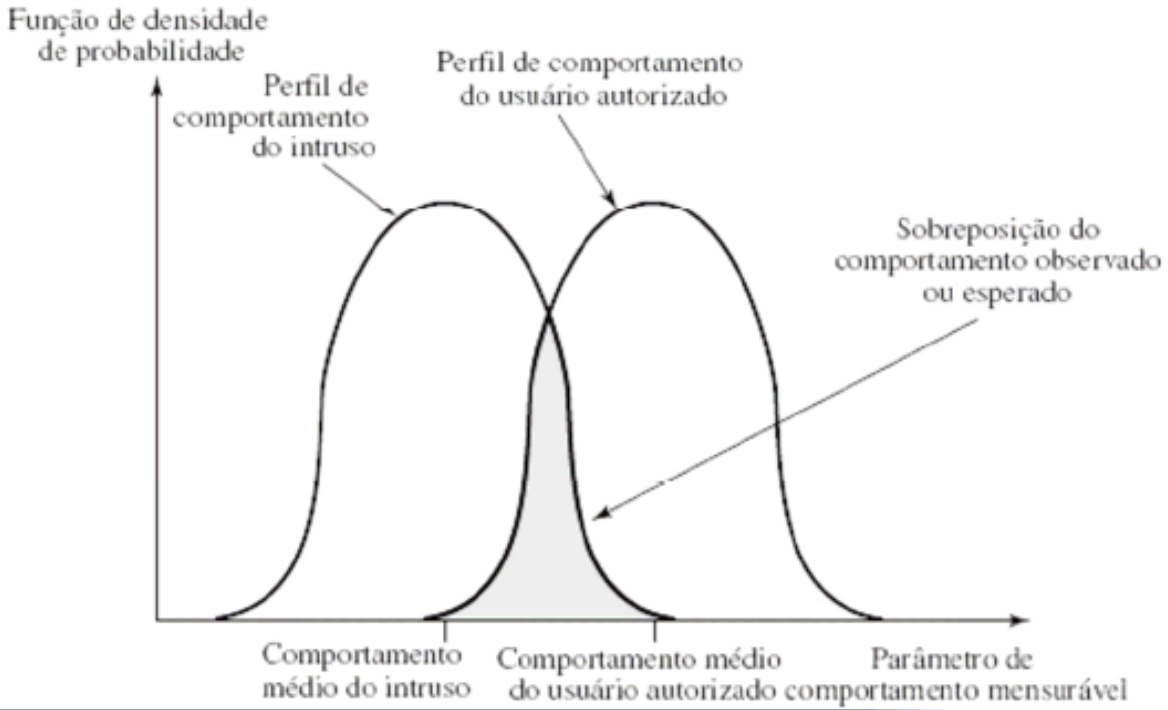
Detecção de Intrusos

- Não há garantias de inviolabilidade
- Monitoramento é essencial
  - Bloqueio rápido para redução dos impactos
  - Elemento adicional (técnica 6D)



Abordagens

- A detecção não é trivial → falsos positivos
- Detecção estatística (*thresholds* baseados no comportamento típico do usuário) ou baseada em regras (sistemas especialistas)
- Registros de auditoria da atividade do usuário
  - Nativos → problemas de formato e/ou adequação ao objetivo
  - Específicos para detecção →*overhead* adicional



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Métricas

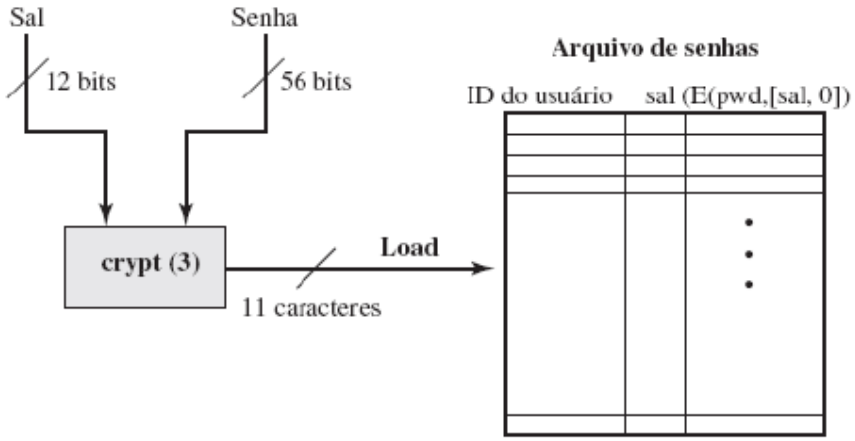
Medida	Modelo	Tipo de intrusão detectada
Atividade de login e sessão		
Freqüência de login por dia e hora	Média e desvio padrão	Intrusos provavelmente poderão efetuar login durante horas livres.
Freqüência de login em diferentes locais	Média e desvio padrão	Intrusos podem efetuar login a partir de um local que um usuário em particular nunca ou quase nunca usa.
Tempo desde o último login	Operacional	Invasão em uma conta 'morta'.
Tempo decorrido por sessão	Média e desvio padrão	Desvios significativos podem indicar um mascarado.
Quantidade de saída para um local	Média e desvio padrão	Quantidades excessivas de dados transmitidos para locais remotos podem significar vazamento de dados sensíveis.
Utilização de recursos da sessão	Média e desvio padrão	Níveis incomuns de processador ou E/S podem sinalizar um intruso.
Falhas de senha no login	Operacional	Tentativa de entrada por adivinhação de senha.
Falhas de login a partir de terminais especificados	Operacional	Tentativa de invasão
Comando ou atividade de execução de programa		
Freqüência de execução	Média e desvio padrão	Pode detectar intrusos, que provavelmente usam comandos diferentes, ou uma penetração bem-sucedida por um usuário legítimo, que obteve acesso a comandos privilegiados.
Utilização de recursos do programa	Média e desvio padrão	Um valor anormal pode sugerir injeção de um vírus ou cavalo-de-tróia, que acarreta efeitos colaterais que aumentam a utilização de E/S ou processador.
Negações de execução	Modelo operacional	Pode detectar tentativa de penetração por usuário individual que busca privilégios mais altos.
Atividade de acesso a arquivo		
Freqüência de leitura, escrita, criação, exclusão	Média e desvio padrão	Anormalidades de acesso de leitura e escrita para usuários individuais pode significar mascaramento ou navegação.
Registros lidos, escritos	Média e desvio padrão	Anormalidade pode significa uma tentativa de obter dados importantes por inferência e agregação.
Contador de falhas de leitura, escrita, criação, exclusão	Operacional	Pode detectar usuários que tentam persistentemente acessar arquivos não autorizados.

Honeypots

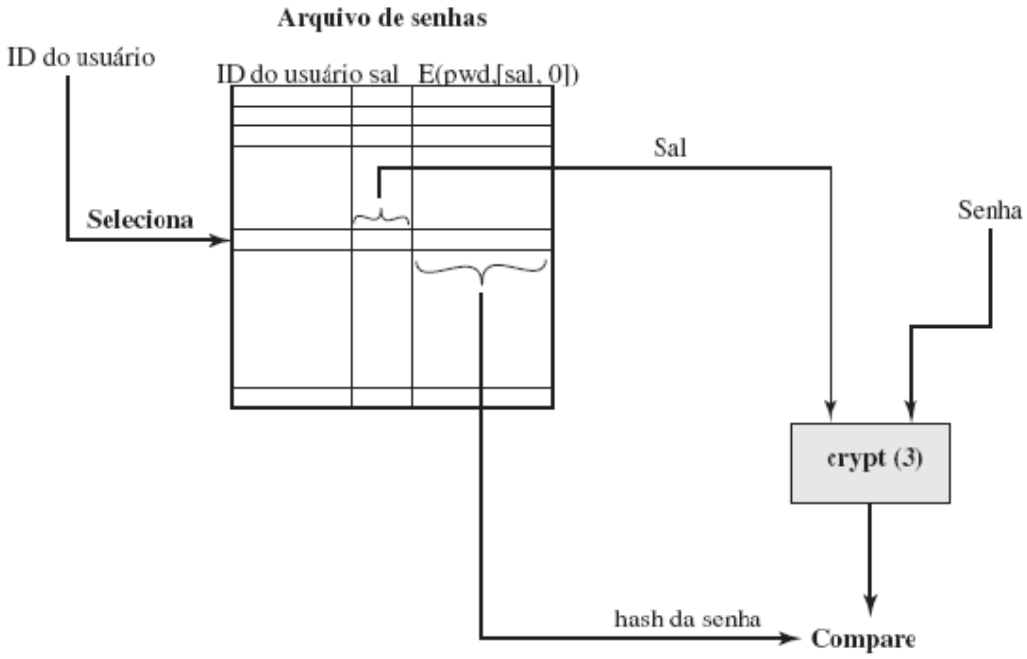
- Alvo artificial, criado para:
  - Desviar a ameaça de sistemas críticos
  - Coletar informações sobre a ameaça
  - Ganhar tempo para reação
- Deve ser usado “com moderação”

Gerenciamento de Senhas

- A senha é a primeira barreira de segurança
  - Adicionalmente, define os direitos de acesso
- Exemplo - Unix



(a) Gravando uma nova senha



(b) Verificando uma senha

Gerenciamento de Senhas

- Estudos indicam que a robustez é negligenciada pelos usuários
  - Regras rígidas conduzem a procedimentos inadequados (*sticky label syndrome*)
  - Melhor abordagem de senhas é a do uso de mnemônicos
  - O ideal é avançar um step
    - O que sabe
    - O que possui
    - Quem é

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Software Malicioso

- Pesadelo de grandes empresas a usuários caseiros

Nome	Descrição
Vírus	Anexa-se a um programa e propaga cópias de si mesmo a outros programas
Verme	Programa que propaga cópias de si mesmo a outros computadores
Bomba lógica	Dispara uma ação quando ocorre uma determinada condição
Cavalo-de-tróia	Programa que contém funcionalidade adicional inesperada
Backdoor (trapdoor)	Modificação de programa que permite o acesso não autorizado à funcionalidade
Exploit	Código específico para uma única vulnerabilidade ou conjunto de vulnerabilidades
Downloaders	Programa que instala outros itens em uma máquina sob ataque. Normalmente, um downloader é enviado em um e-mail
Auto-rooter	Ferramentas maliciosas de hacker usadas para invasão de novas máquinas remotamente
Kit (gerador de vírus)	Conjunto de ferramentas para gerar novos vírus automaticamente
Programas de spam	Usados para enviar grandes volumes de e-mail indesejado
Flooders	Usados para atacar sistemas de computador em rede com um grande volume de tráfego para executar um ataque de negação de serviço (DoS)
Keyloggers	Capta teclas digitadas em um sistema comprometido
Rootkit	Conjunto de ferramentas de hacker usadas após um atacante ter invadido um sistema de computador e obtido acesso em nível de root
Zumbi	Programa ativado em uma máquina infectada, que é preparado para desferir ataques a outras máquinas

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Alguns exemplos

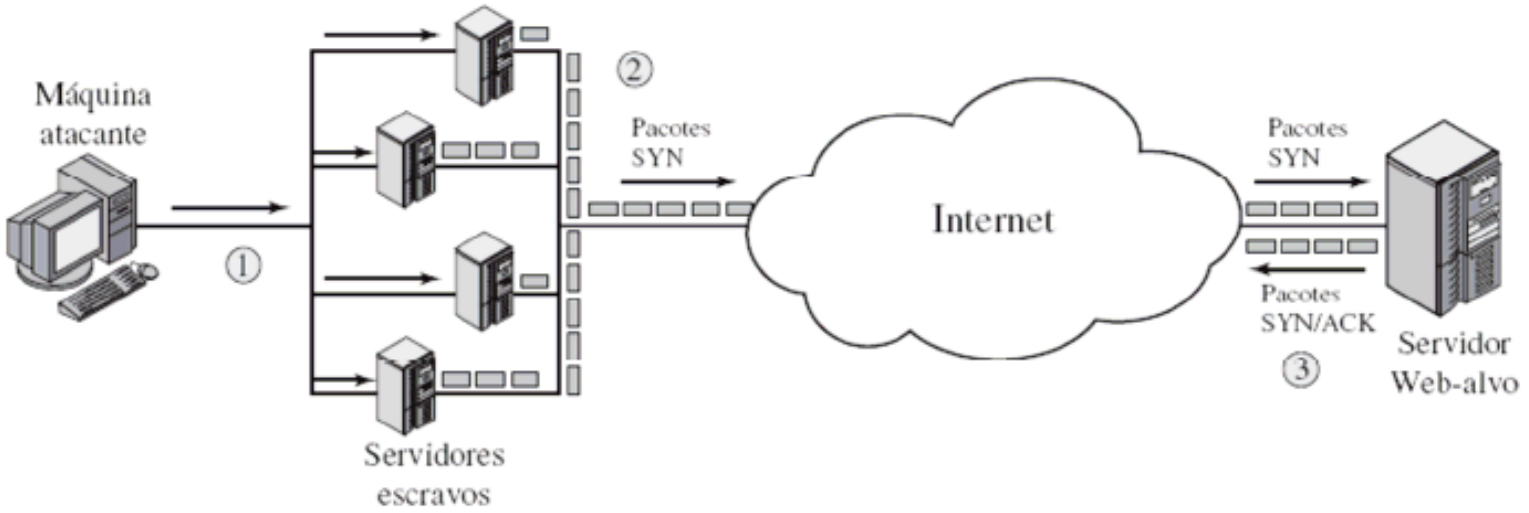
- Code Red – explora uma falha do MS IIS
  - Testa IPs buscando servidores IIS
  - Disparador de ataque DoS
  - 2ª fase infectou 360000 servidores em 14 horas
- Code Red 2 – instala um backdoor
- Nimda - multiple infection mechanisms
- SQL Slammer (2003) – ataques em MS SQL server
- Sobig.f (2003) – atacou servidores proxy para emitir spam contaminado
- Blaster (2003) – um dos primeiros a usar o RPC do Windows. DDoS no site do Windows Update, travamentos na máquina contaminada
- Mydoom (2004) – worm propagado por SMTP + backdoor que permitia acesso remoto
- Sasser (2004) – degrada desempenho
- Conficker (2008) – estima-se que mais de 15 mi de máquinas estejam contaminadas

Contramedidas para Vírus

- Ferramentas não são sempre eficazes
- A educação do usuário é essencial
- Manutenção de atualizações mitiga, mas não resolve
- Gerações de Antivírus
  - 1G → scanner simples
  - 2G → scanner heurístico
  - 3G → interceptação de atividade
  - 4G → proteção completa
- Defesa proativa

DDoS

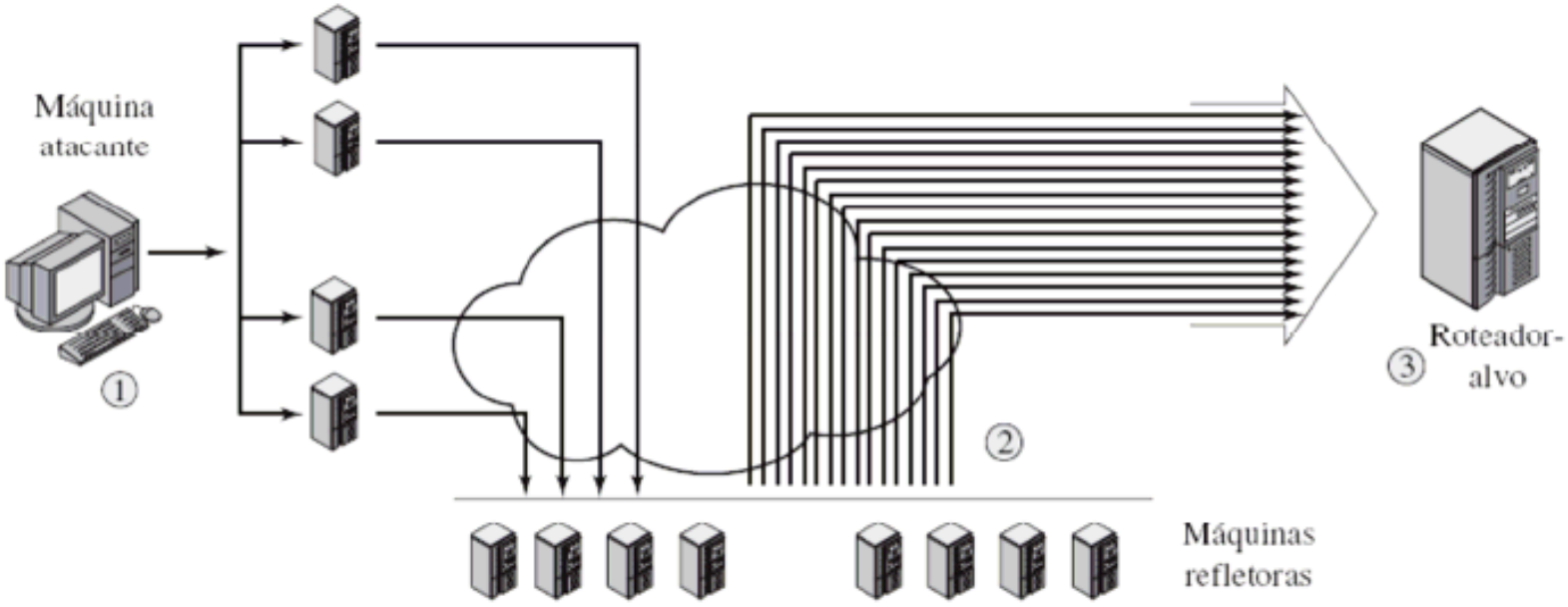
- DoS – consumo de recursos para atacar disponibilidade. Ex.: SYN Flooding



(a) Ataque distribuído de inundação de SYN

DDoS

- Outro ataque: exaustão dos recursos de comunicação, e não diretamente do alvo



(a) Ataque distribuído de ICMP

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

DDoS - Contramedidas

- Prevenção de Ataque e Ação antecipada
  - Políticas de consumo, recursos reserva, hardening focado em DoS
- Detecção e Filtragem do Ataque
  - Ação proativa de acordo com padrões de comportamento
- Rastreamento e Identificação da origem do Ataque
  - Visando evitar ataques futuros

Firewalls

- É uma solução complexa e customizada de acordo com os ambientes interno e externo
- Requisitos Fundamentais de Projeto:
  - Todo o tráfego de um ambiente para outro deve passar pelo firewall
  - Apenas o tráfego em conformidade com a PolSeg deve passar
  - O Firewall deve ser imune à penetração
- Capacidades previstas
  - Recurso para monitoramento e auditoria
  - Possibilidade de uso de NAT, VPNs, antivírus

Limitações

- Não pode controlar tráfego que contraria os requisitos. Ex.: modens em estações, PDPL/PDPC
- Não tem como combater ameaças internas com as credenciais necessárias
- Não tem como analisar todo o tráfego entrante e “saínte”

Controles

- Controle de serviço
  - Que podem ser acessados interna e externamente
- Controle de Direção
  - Maior detalhe no controle
- Controle de Usuário
  - Depende de autenticação
- Controle de Comportamento
  - A forma de usar um recurso. ex.: SPAM

Tipos de Firewalls

- Filtros de Pacotes
  - Mais simples e rápidos, fundamentados em ACLs implementando regras para políticas do tipo:
    - O que não for permitido é proibido
    - O que não é proibido é permitido

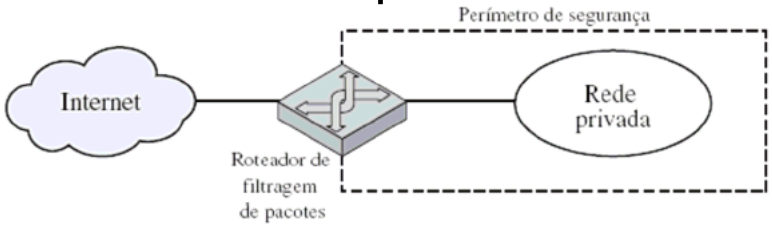


Tabela 20.1 Exemplos de filtragem de pacotes

A

ação	nossohost	porta	hostdeles	porta	comentário
bloquear	*	*	SPIGOT	*	não confiamos nessas pessoas
permitir	OUR-GW	25	*	*	conexão com nossa porta SMTP

B

ação	nossohost	porta	hostdeles	porta	comentário
bloquear	*	*	*	*	padrão

C

ação	nossohost	porta	hostdeles	porta	comentário
permitir	*	*	*	25	conexão com a porta SMTP deles

D

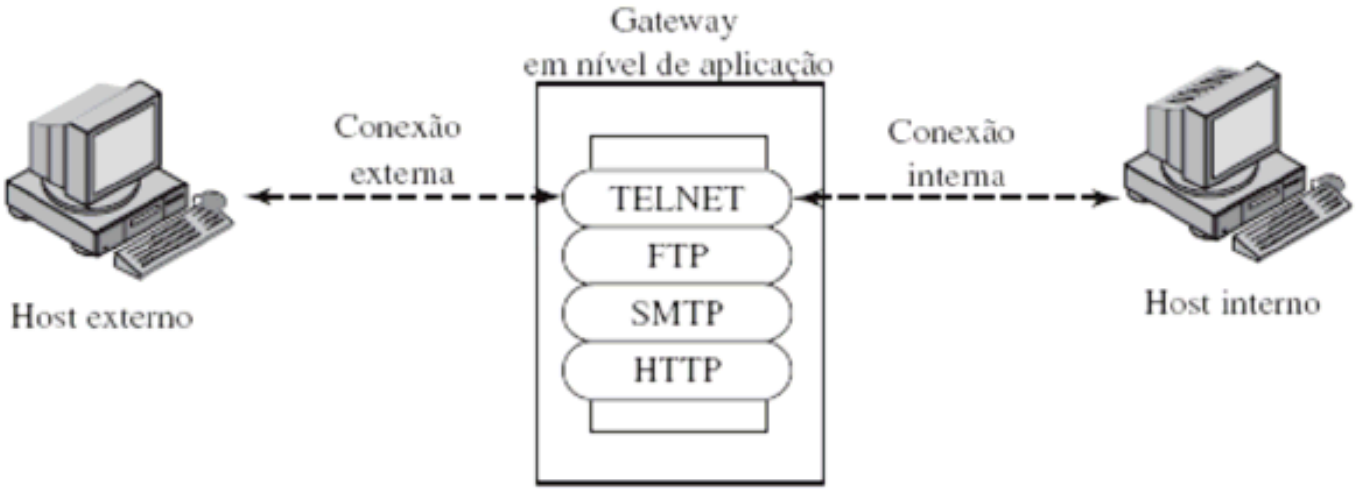
ação	src	porta	dest	porta	flags	comentário
permitir	{our hosts}	*	*	25		nossos pacotes para a porta SMTP deles
permitir	*	25	*	*	ACK	respostas deles

E

ação	src	porta	dest	porta	flags	comentário
permitir	{our hosts}	*	*	*		nossas chamadas para fora
permitir	*	*	*	*	ACK	respostas às nossas chamadas
permitir	*	*	*	>1024		tráfego para não-servidores

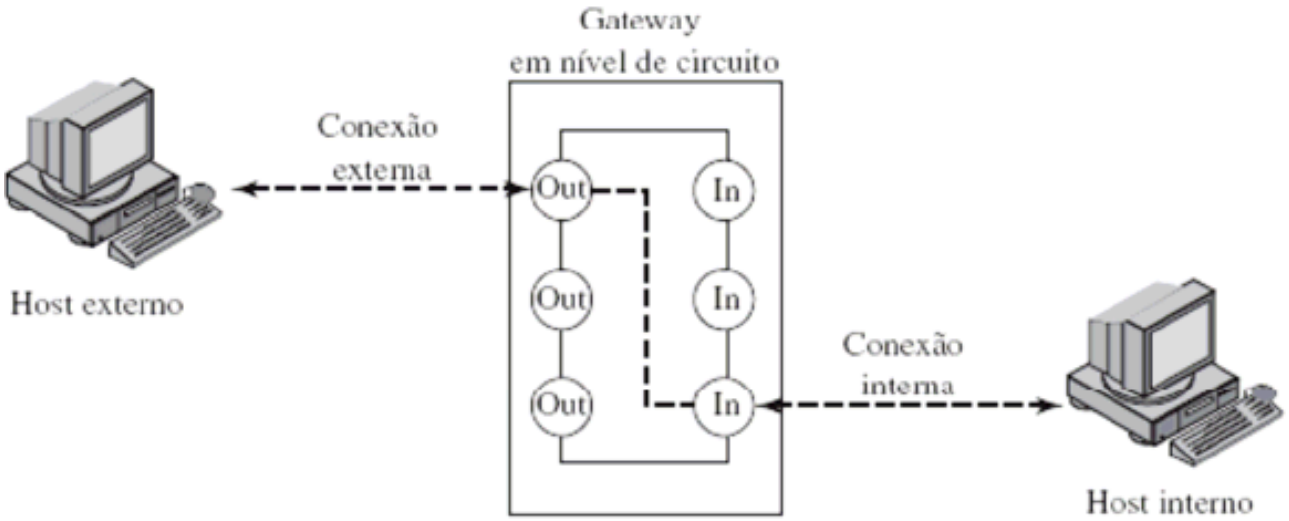
Tipos de Firewall

- Gateway de Aplicação (Proxy)
  - Vantajoso por endereçar uma deficiência dos filtros de pacotes → poder inspecionar conteúdo
  - Desvantajoso pelo grande overhead e especialização da ferramenta



Tipos de Firewall

- Gateway de Circuito
  - Conexões são realizadas apenas se confiáveis
  - Menor overhead por não inspecionar (a priori) o conteúdo das conexões
  - Ex.: SOCKS (TCP 1080)

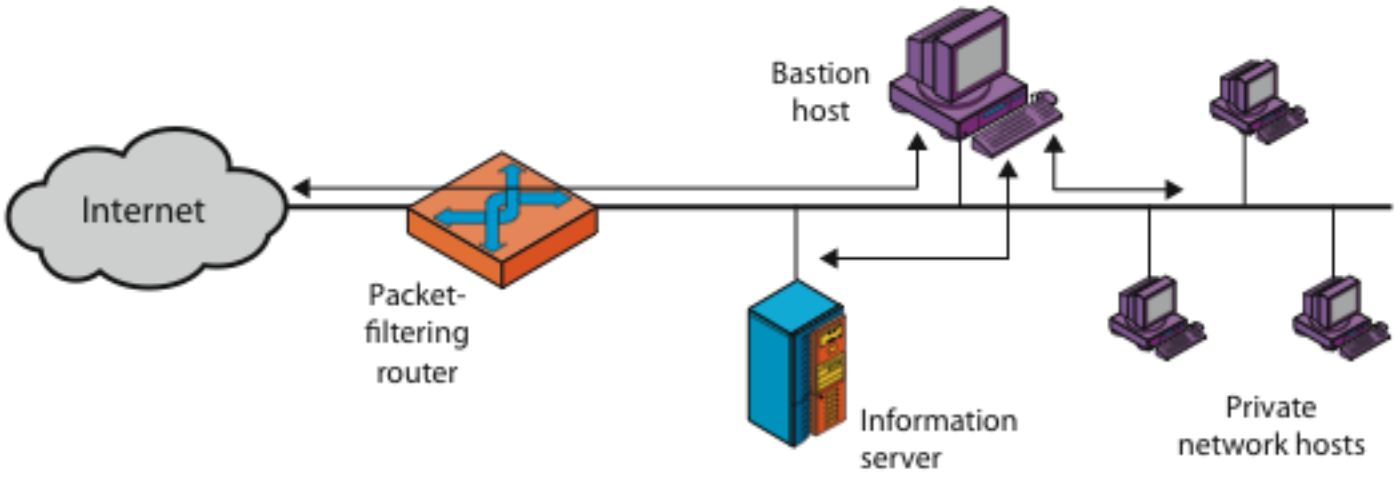


Configurações de Firewall

- Bastion Host → Concentração dos recursos de firewall
  - SO robustecido e essencial ao seu funcionamento
  - Autenticação robusta e limitada
  - Monitorado mais intensivamente. Ex.: MAC de todos os arquivos do SO

Bastion Host Single-homed

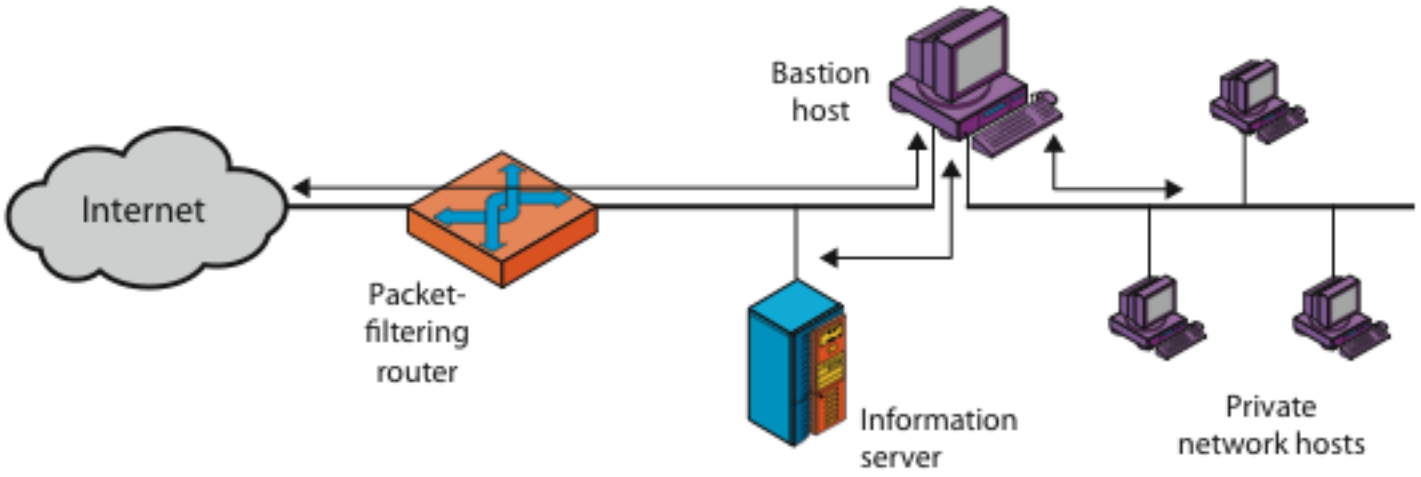
- Todo o tráfego passa pelo Bastion host, se aprovado pelo roteador filtro de pacotes
- Se comprometido (o roteador), é possível o acesso direto aos hosts da rede



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

Bastion Host Dual-homed

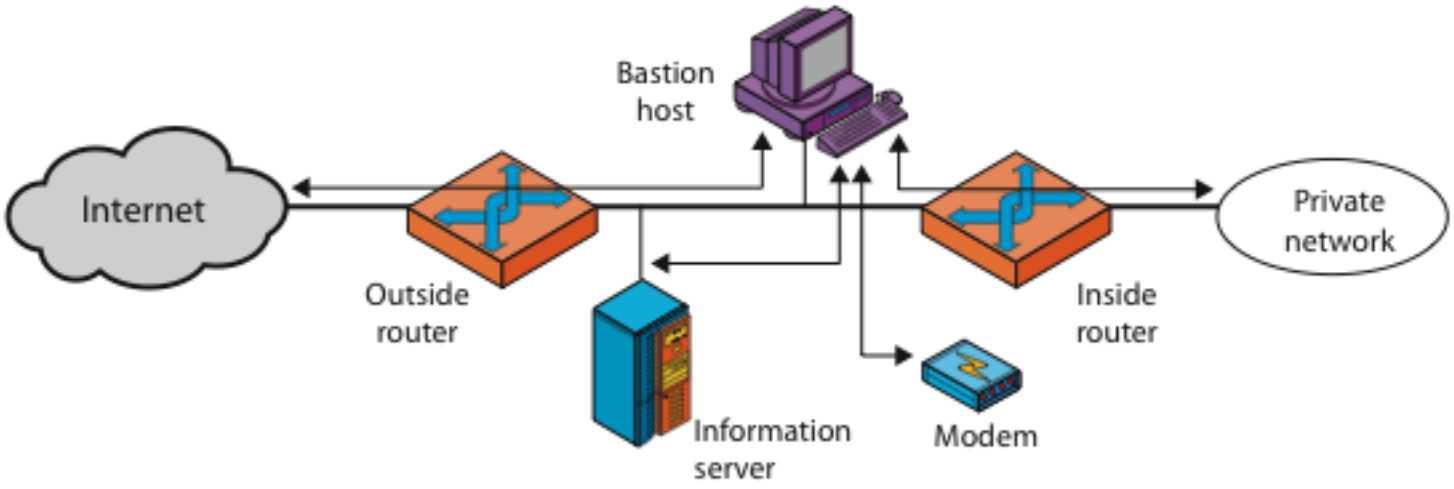
- Endereça a brecha de segurança do single-homed



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

Screened subnet

- Mais robusta que as anteriores, possibilita a criação de uma DMZ, além de três filtros de regras entre o intruso e a rede interna



(c) Screened-subnet firewall system