Segurança de Redes

Curso Superior de Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Aula 04
Técnicas de Defesa - Firewall de Rede

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

"O sentimento de inferioridade é o grande dificultador dos relacionamentos seguros e sadios. Esse sentimento produz uma necessidade de estarmos sempre certos e sendo aplaudidos pelos outros." (Hammed)

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

O que Aprenderemos?

- Entender o que são mecanismos de segurança;
- Conhecer quais são os principais mecanismos de segurança;
- Aprenderemos o que é um firewall? sua finalidade?
- Conhecer o funcionamento dos principais tipos de firewall;
- Entender o que é um DMZ e *honeypot*.
- Conhecer exemplos de *softwares* de firewall com licença software livre.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Introdução

Não existe nenhuma rede 100% segura, mas podemos empregar diversos mecanismos para minimizar a ocorrência de problemas relacionados à segurança. E quando ocorrerem, poderem ser detectados e tratados de forma satisfatória.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução

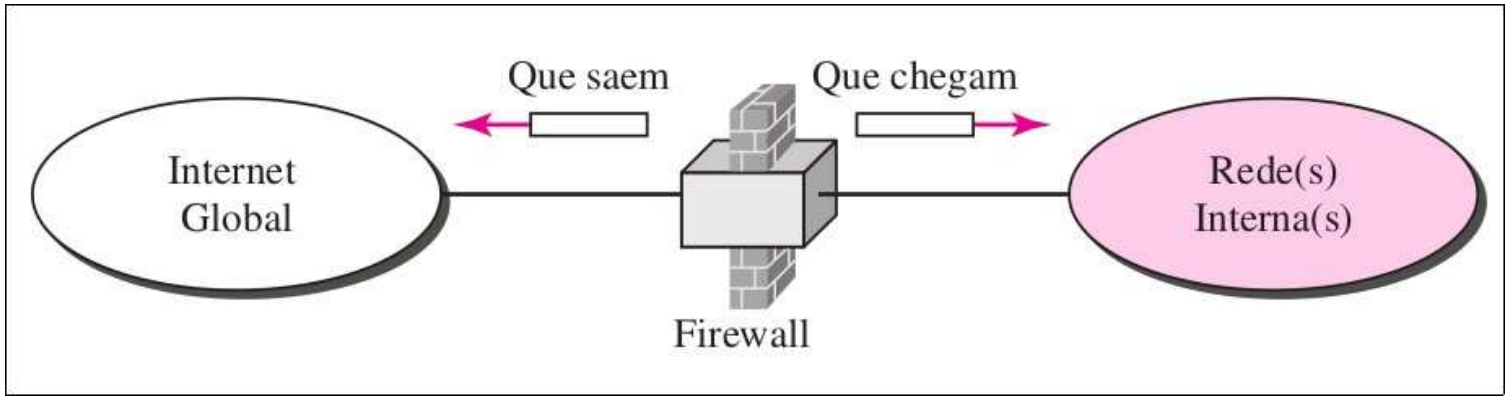
Estes mecanismo de segurança são: processos (ou dispositivos) projetados para detectar, impedir ou recuperar-se de um ataque à segurança. Os principais mecanismos são:

- Antivírus;
- Criptografia;
- Firewall;
- Rede Virtual Privada (VPN);
- Autenticação;
- Assinatura Digital;
- Sistema de Detecção de Intruso;
- Política de Segurança.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

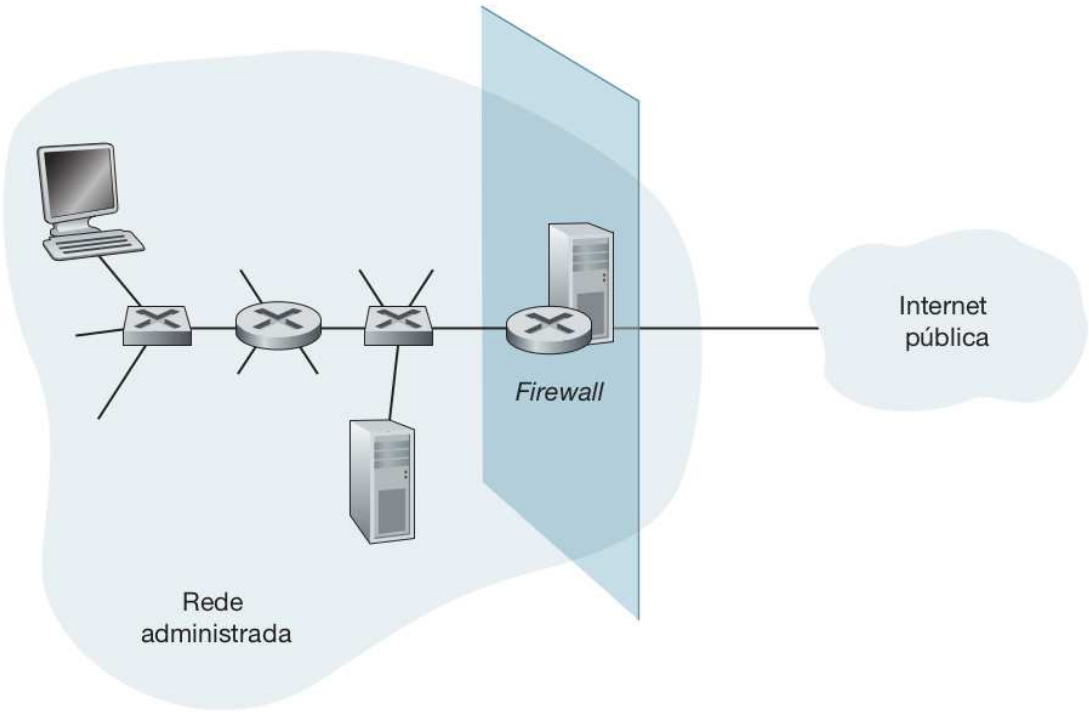
Firewall

Um firewall é uma combinação de hardware e software que isola a rede interna de uma organização da Internet em geral (fincando na borda de rede), interceptar todo o tráfego e permite que alguns pacotes passem e bloqueando outros (somente o tráfego autorizado poderá passar). O objetivo é proteger a rede interna contra ataques provenientes da Internet.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

- Com o firewall poderemos ainda:
  - Proteger uma rede privada contra “intrusos” externos;
  - Impedir envio de informações não autorizadas;
  - Bloquear acesso a sites particulares;
  - Prevenir que certos usuários/máquinas acessem certos serviços;
  - Permite implementação de serviços como NAT e VPN;
  - Facilita a geração de estatísticas e auditorias do uso da rede;



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Tecnologias de Firewall

As principais tecnologias de firewall são:

- Filtro de pacotes (*Packet Filter*);
- Filtro de pacotes dinâmicos (*StatefulPacket*);
- Proxy.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Filtro de Pacote

Um filtro de pacotes examina cada datagrama, determinando se deve passar ou ficar baseado nas regras específicas definidas pelo administrador. As decisões de filtragem costumam ser baseadas em:

- Endereço IP de origem e de destino
- Tipo de protocolo no campo do datagrama IP: TCP, UDP, ICMP, OSPF etc.
- Porta TCP ou UDP de origem e de destino
- Bits de flag do TCP: SYN, ACK etc.
- Tipo de mensagem ICMP
- Regras diferentes para datagramas que entram e saem da rede.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Filtro de Pacote

Os filtros de pacotes também são chamados de *stateless* firewall. Cada pacote é tratado de forma isolada, ou seja, não guarda o estado da conexão e não sabe se o pacote faz parte de uma conexão feita anteriormente.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Filtro de Pacote

As regras são colocadas em tabelas de acordo com a política da organização. As regras são aplicadas a cada datagrama que atravessa a interface sequencialmente, da parte de cima da tabela para baixo. Por exemplo,

Política	Configuração de *firewall*
Não há acesso exterior à Web	Descartar todos os pacotes de saída para qualquer endereço IP, porta 80
Não há conexões TCP de entrada, exceto aquelas apenas para o servidor Web público da organização	Descartar todos os pacotes TCP SYN para qualquer IP exceto 130.207.244.203, porta 80
Impedir que rádios Web devorem a largura de banda disponível	Descartar todos os pacotes UDP de entrada — exceto pacotes DNS
Impedir que sua rede seja usada por um ataque DoS *smurf*	Descartar todos os pacotes *ping* que estão indo para um endereço de difusão (por exemplo, 130.207.255.255)
Impedir que a rota de sua rede seja rastreada	Descartar todo o tráfego de saída ICMP com TTL expirado

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Filtro de Pacote

Uma política de filtragem também pode ser baseada na combinação de endereços, números de porta e flags TCP. Por exemplo, o que a tabela a seguir permite e bloqueia?

Ação	Endereço de origem	Endereço de destino	Protocolo	Porta de origem	Porta de destino	Bit de flag
Permitir	222.22/16	Fora de 222.22/16	TCP	> 1023	80	Qualquer um
Permitir	Fora de 222.22/16	222.22/16	TCP	80	> 1023	ACK
Permitir	222.22/16	Fora de 222.22/16	UDP	> 1023	53	—
Permitir	Fora de 222.22/16	222.22/16	UDP	53	> 1023	—
Negar	Todos	Todos	Todos	Todos	Todos	Todos

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Filtro de Pacote de Pacotes Dinâmicos

Em um filtro de pacotes tradicional, as decisões de filtragem são feitas em cada pacote isolado. Os filtros de pacotes dinâmicos (também chamado de filtros de pacote com controle de estado) rastreiam conexões TCP e usam esse conhecimento para tomar decisões sobre filtragem. Desta forma, as decisões de filtragem usam informações dos cabeçalhos dos pacotes e uma tabela de estados, que guarda os estados de todas as conexões TCP.

O firewall mantém informações sobre o estado das conexões TCP e permite automaticamente todos os pacotes relacionados, de modo que o administrador necessita apenas especificar a regra do primeiro pacote e indicar que os pacotes relacionados serão automaticamente aceitos.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Por exemplo, temos três conexões TCP em andamento. Ademais, o filtro do firewall inclui uma nova coluna, "verificar conexão". Quando o pacote chega ao firewall, este verifica a lista de controle de acesso da, que poderá indicar que a tabela de conexão deve também ser verificada antes de permitir que esse pacote entre na rede da organização.

Endereço de origem	Endereço de destino	Porta de origem	Porta de destino
222.22.1.7	37.96.87.123	12699	80
222.22.93.2	199.1.205.23	37654	80
222.22.65.143	203.77.240.43	48712	80

Ação	Endereço de origem	Endereço de destino	Protocolo	Porta de origem	Porta de destino	Bit de flag	Verificar conexão
Permitir	222.22/16	Fora de 222.22/16	TCP	>1023	80	Qualquer um	
Permitir	Fora de 222.22/16	222.22/16	TCP	80	>1023	ACK	X
Permitir	222.22/16	Fora de 222.22/16	UDP	>1023	53	—	
Permitir	Fora de 222.22/16	222.22/16	UDP	53	>1023	—	X
Negar	Todos	Todos	Todos	Todos	Todos	Todos	

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Suponha que um atacante tente enviar um pacote para a rede da organização (222.22/16) por meio de um datagrama com porta de origem TCP 80 e com o flag ACK marcado. Suponha ainda que ele possua um número de porta de origem 12543 e endereço IP remetente 150.23.23.155. O que ocorrerá no Firewall?

Endereço de origem	Endereço de destino	Porta de origem	Porta de destino
222.22.1.7	37.96.87.123	12699	80
222.22.93.2	199.1.205.23	37654	80
222.22.65.143	203.77.240.43	48712	80

Ação	Endereço de origem	Endereço de destino	Protocolo	Porta de origem	Porta de destino	Bit de flag	Verificar conexão
Permitir	222.22/16	Fora de 222.22/16	TCP	>1023	80	Qualquer um	
Permitir	Fora de 222.22/16	222.22/16	TCP	80	>1023	ACK	X
Permitir	222.22/16	Fora de 222.22/16	UDP	>1023	53	—	
Permitir	Fora de 222.22/16	222.22/16	UDP	53	>1023	—	X
Negar	Todos	Todos	Todos	Todos	Todos	Todos	

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Suponha que um usuário interno (222.22/16) queira navegar em um site externo (porta de origem $>$ 1023 e de destino $=$ 80) do IFRN (200.137.1.195). O que ocorrerá no Firewall?

Endereço de origem	Endereço de destino	Porta de origem	Porta de destino
222.22.1.7	37.96.87.123	12699	80
222.22.93.2	199.1.205.23	37654	80
222.22.65.143	203.77.240.43	48712	80

Ação	Endereço de origem	Endereço de destino	Protocolo	Porta de origem	Porta de destino	Bit de flag	Verificar conexão
Permitir	222.22/16	Fora de 222.22/16	TCP	>1023	80	Qualquer um	
Permitir	Fora de 222.22/16	222.22/16	TCP	80	>1023	ACK	X
Permitir	222.22/16	Fora de 222.22/16	UDP	>1023	53	—	
Permitir	Fora de 222.22/16	222.22/16	UDP	53	>1023	—	X
Negar	Todos	Todos	Todos	Todos	Todos	Todos	

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Proxy Firewall

O Firewall de filtragem de pacotes se baseia nas informações disponíveis nos cabeçalhos da camada de rede e de transporte (IP e TCP/UDP). Entretanto, algumas vezes precisamos filtrar uma mensagem baseada nas informações da camada de aplicação. Neste caso devemos utilizar o proxy firewall, também conhecido como firewall de aplicação ou gateway firewall.

Suponha, por exemplo, que uma organização queira implementar as seguintes políticas somente aqueles usuários Internet que tiverem estabelecido relações comerciais anteriores com a empresa poderão ter acesso; o acesso para outros tipos de usuários deve ser bloqueado. Nesse caso, um firewall para filtragem de pacotes não é viável. Devem ser realizados testes no nível de aplicação.

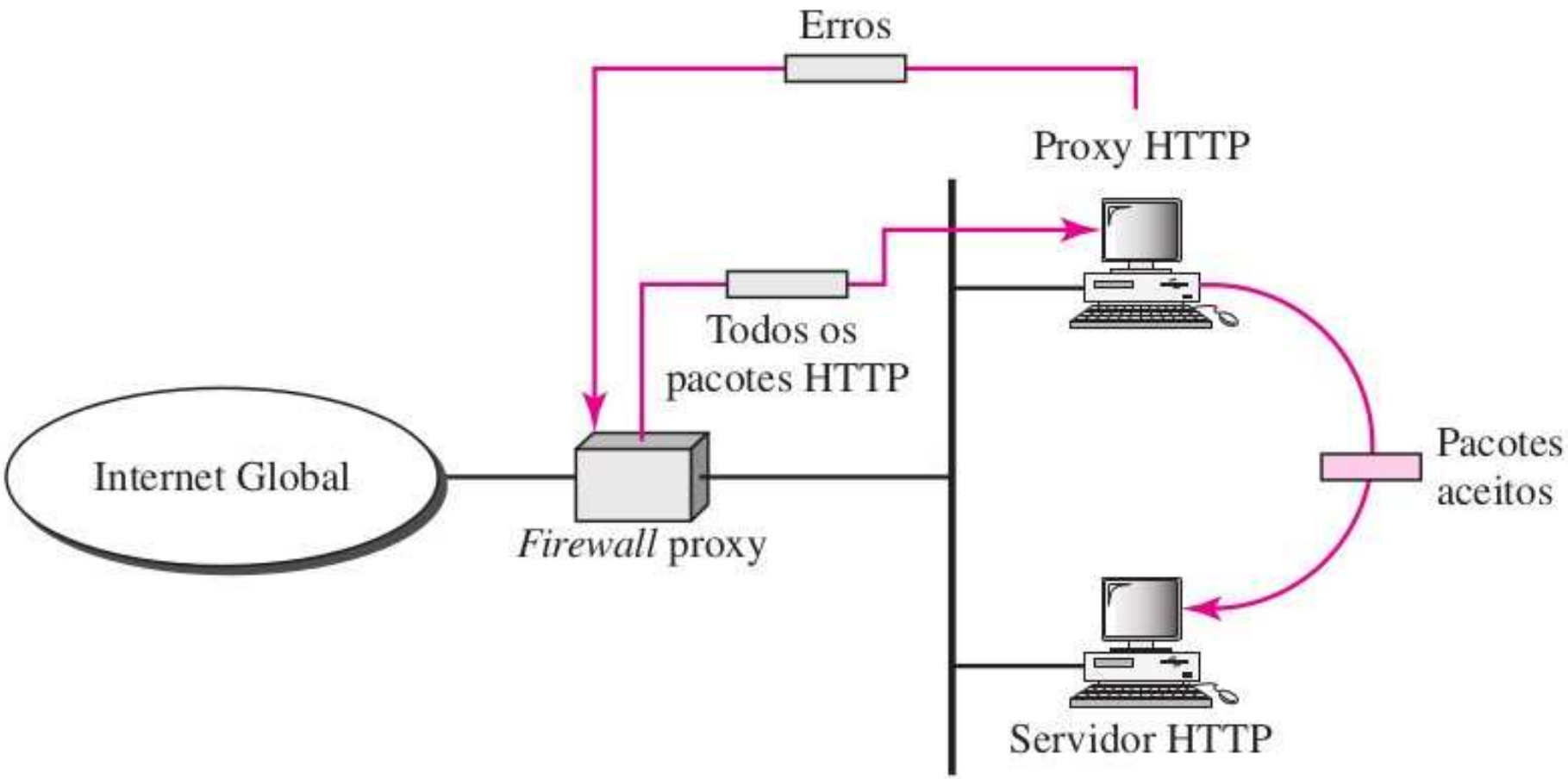
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Proxy Firewall

Devido ao custo computacional, algumas vezes o firewall e o proxy de aplicação ficam em equipamentos diferentes. Quando o cliente envia uma mensagem, o firewall recebe a solicitação e envia para o proxy. O mesmo abre o pacote no nível de aplicação e determina se a solicitação é legítima. Se for, o proxy envia a mensagem para o verdadeiro servidor. Se não for legítima, a mensagem é eliminada e é enviada uma mensagem de erro. Dessa maneira, as solicitações dos usuários são filtradas tomando-se como base o conteúdo na camada de aplicação.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Proxy Firewall



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Proxy Firewall

Os proxy firewall tem um desempenho computacional inferior ao de filtro de pacote. Entretanto, eles são considerados um dos tipos mais seguros de firewall, pois eles são capazes de prover registros detalhados sobre os acessos realizados, além de permitir o controle de acesso através de parâmetros de aplicação, como bloquear o acesso a arquivos executáveis em conexões HTTP, controle impossível de ser realizado apenas com filtros de pacotes.

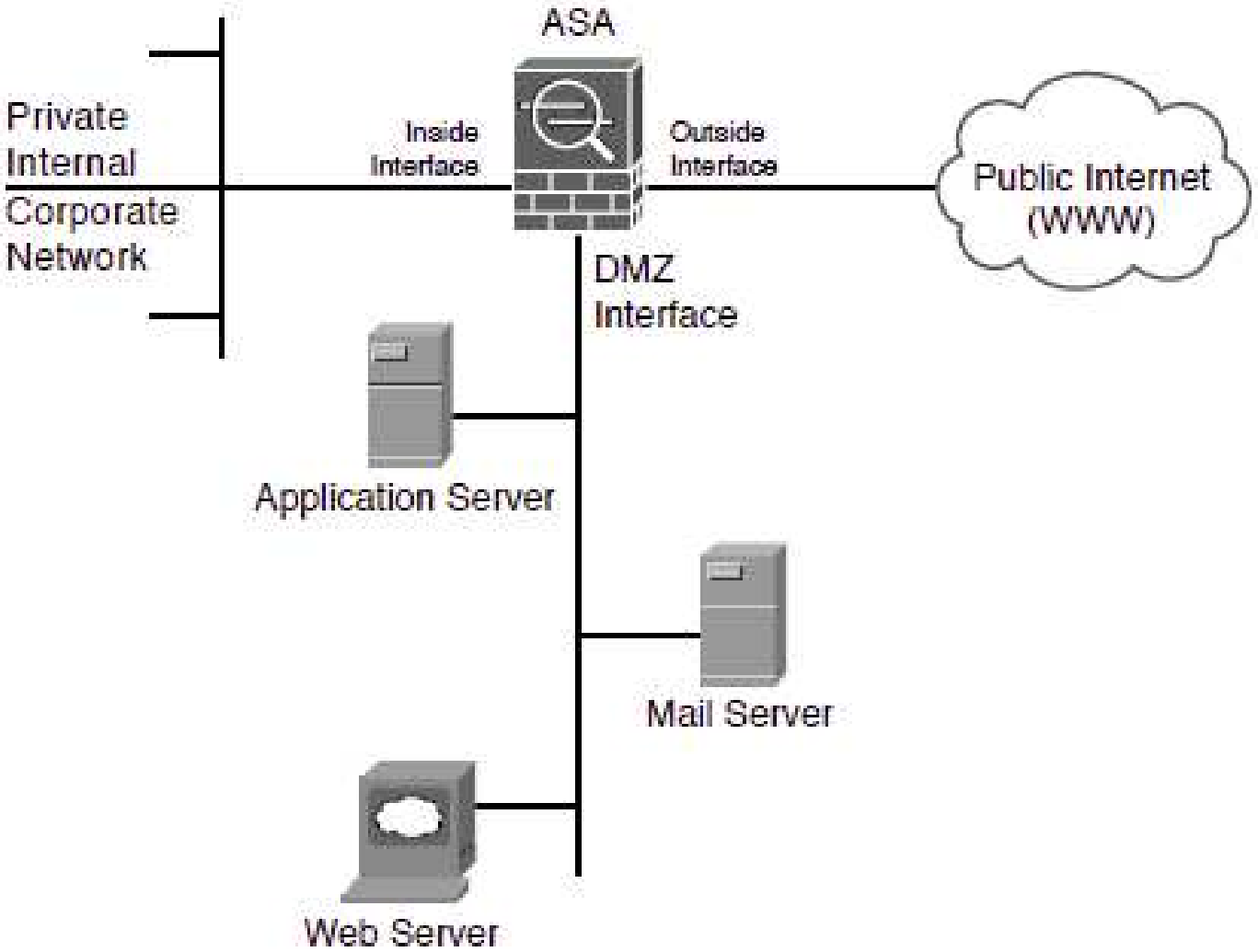
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

DMZ

DMZ é uma sigla para *Demilitarized Zone* (Zona Desmilitarizada), é uma rede que se situa entre uma rede confiável (LAN) e uma rede não confiável (Internet). O objetivo é realizar um isolamento entre as três redes através de diferentes níveis de permissões no firewall. Desta forma, usuários na Internet acessam com regras específicas os servidores isolados no DMZ (normalmente mais permissiosas que a rede LAN). Os servidores mais comumente encontrados no DMZ são os de email, FTP, e HTML.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

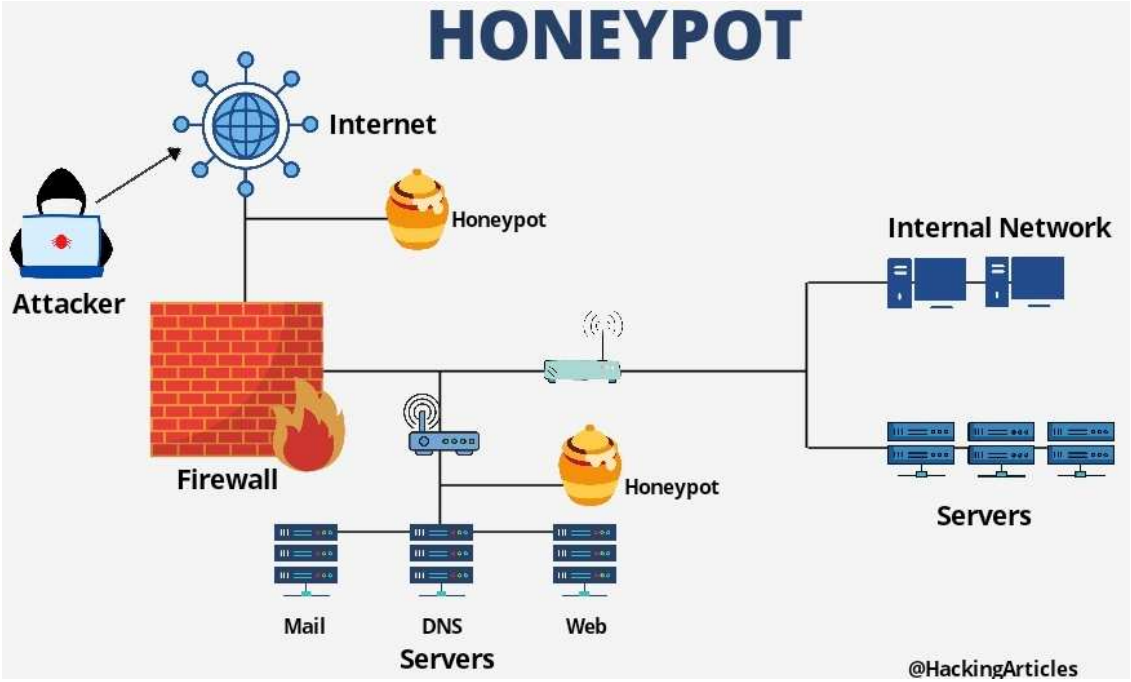
DMZ



ISTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Honeypot

Um honeypot é um sistema de computador sacrificial (com baixo controle de segurança) que pretende atrair ciberataques pensando ser um alvo legítimo, mas é uma emboscada. Ele emula um alvo para os hackers e usa suas tentativas de intrusão para obter informações sobre cibercriminosos e a maneira como eles estão operando ou para distraí-los de outros alvos.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Honeypot

Um honeypot não é configurado para resolver um problema específico, como um firewall ou um antivírus. Em vez disso, é uma ferramenta de informação que pode ajudá-lo a compreender as ameaças existentes ao seu negócio e detectar o surgimento de novas ameaças. Com a inteligência obtida de um honeypot, os esforços de segurança podem ser priorizados e focados.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Implementações de Firewall

Existem diversas soluções de firewall com licença software livre, as soluções mais comuns são: Netfilter (Iptables) para Linux; Ipfilter (IPF) e IP Firewall (IPFW) para FreeBSD;e Packet Filter (PF) para OpenBSD e FreeBSD.

Quando uma empresa de grande porte faz a opção por uma solução de firewall baseada em software livre, não o faz pelo custo. Eles, colocamos em primeiro lugar a funcionalidade e maturidade da tecnologia. Dessa forma, soluções de firewall baseadas em Linux ou mesmo baseadas em Unix BSD são usadas por serem funcionais e confiáveis.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Iptables

O Netfilter é a parte do Kernel do Linux que vai compor as capacidades de firewall e que será configurado e gerenciado pela ferramenta chamada Iptables. Todavia, quando se menciona o firewall do Linux, é comum simplesmente denominá-lo Iptables.

O Iptables é um framework capaz de realizar filtros de pacotes baseado em estados com suporte a diversos protocolos, tradução de endereços de rede e tradução de número de portas TCP e UDP, redirecionamento de pacotes, suporte a NAT, além de outros tipos de manipulação de pacotes TCP/IP.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Dúvidas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE