FACVLDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

ADMINISTRAÇÃO DE REDES I
LINUX

Firewall

Frederico Madeira
LPIC-1, CCNA
fred@madeira.eng.br
www.madeira.eng.br

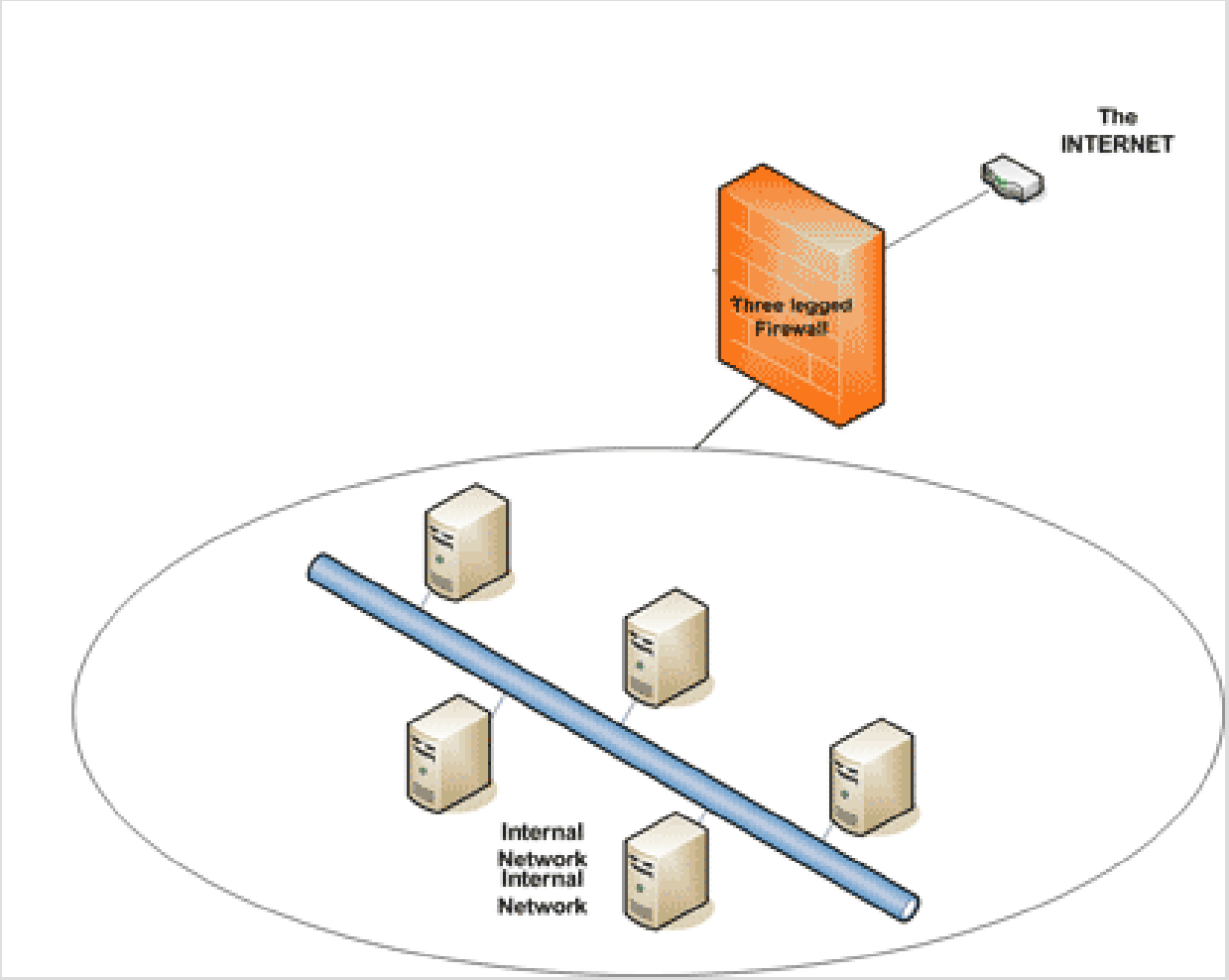
FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

- *São dispositivos que têm com função regular o tráfego entre redes distintas restringindo o fluxo de informações.*
- Começou a ser utilizado no final da década de 80 quando roteadores faziam a separação de pequenas redes
- Firewall, também chamado de Porta corta-fogo
- Regras do tipo:
  - Alguém da rede A pode acessar a rede B, ou alguém da rede C não pode acessar a rede B.
  - Filtros de pacotes e de aplicativos
  - Identificam o estado da conexão

FACVLDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall



Firewall Padrão

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

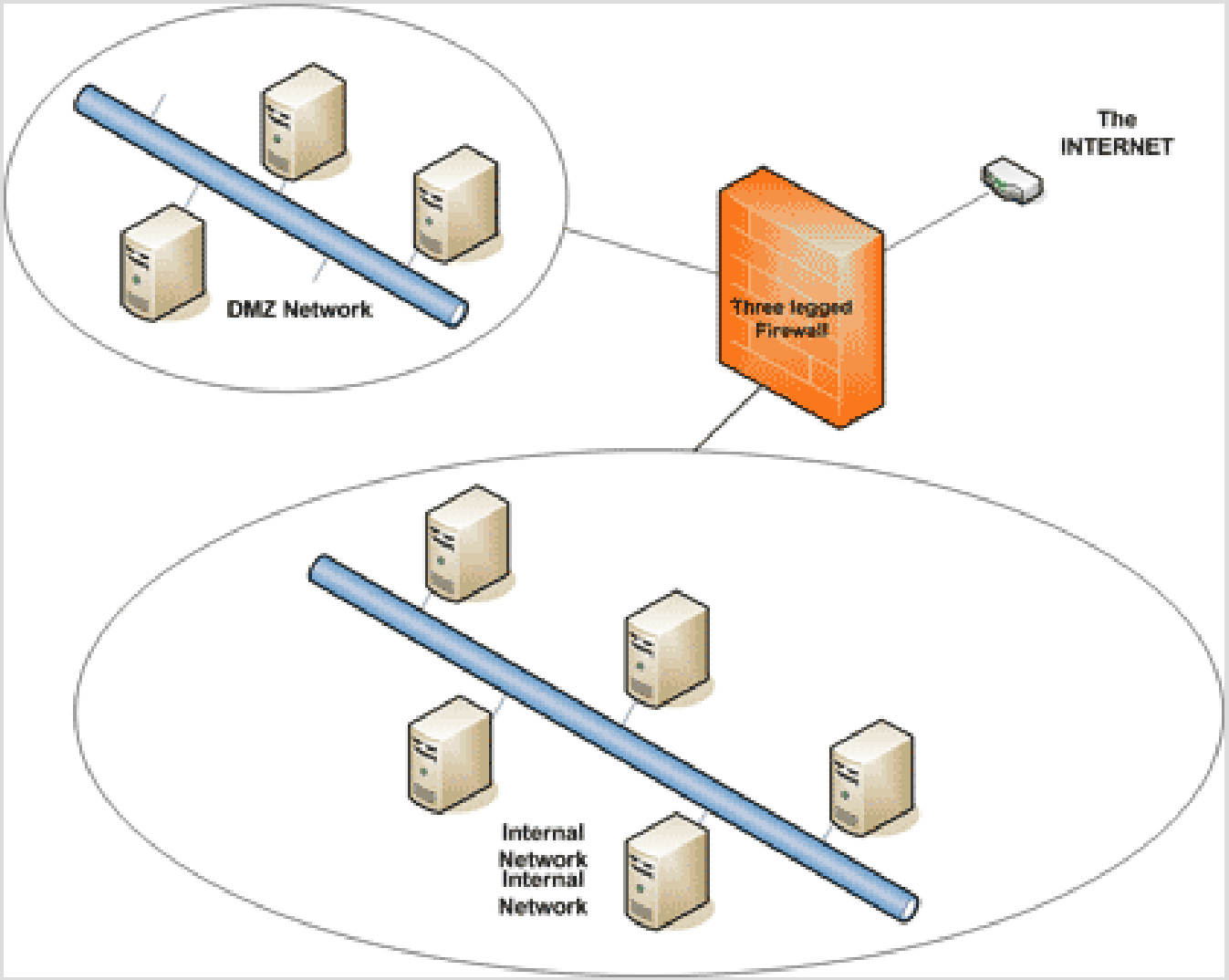
DMZ

- É a sigla para de DeMilitarized Zone ou "zona desmilitarizada" ou ainda Rede de Perímetro.
- É uma pequena rede situada entre uma rede confiável e uma não confiável, geralmente entre a rede local e a Internet.
- Sua função é manter todos os serviços que possuem acesso externo (tais como servidores HTTP, FTP, de correio eletrônico, etc) separados da rede local
- Limita o potencial dano em caso de comprometimento de algum destes serviços por um invasor

FACVLDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

DMZ



Firewall com DMZ

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Boas Práticas

- Antes da elaboração de regras, faça um levantamento da rede
- Configure seu firewall com a regra padrão de Deny ALL;
- Caso a organização possua aplicativos que necessitem atravessar o firewall, certifique-se de que a aplicação é segura, que possua mecanismo de encriptação de dados. Libere o tráfego daquela porta apenas para uma origem e destino especificados.
- Procure logar acessos a portas sensíveis, com por exemplo casos do item anterior;
- Caso precise disponibilizar serviços na Internet, configure uma DMZ, ao invés de redirecionar portas do seu firewall para servidores internos.

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Boas Práticas

- Evite mapeamento de drivers através do firewall;
- Configure o firewall para bloquear pacotes forjados, não permita que pacotes que possuam no campo de endereço de origem um endereço ip privado (10.0.0.0, 192.168.0.0, etc...) cheguem na interface externa do firewall.
- Sempre que adicionar uma regra que permita um determinado tráfego, sempre especifique endereços IP de origem e destino, protocolo e porta;
- Os serviços permitidos entre sua rede interna e sua DMZ, não devem ser permitidos entra a rede interna e a Internet e vice versa;

FACVLDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Boas Práticas

- Antes de permitir o tráfego de uma determinado protocolo, cheque se ele utiliza encriptação, de forma a evitar que as informações trafegadas possam ser snifadas.

- Sempre realizem testes em seu firewall, utilizem ferramentas do tipo Nessus ou Nmap para verificar vulnerabilidades e portas abertas em seu firewall

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Implementação em Linux

- Funções de Firewall são agregadas à própria arquitetura do kernel
- Implementações de Firewall de acordo com a versão do kernel
  - Kernel 2.0 – IPFWADM
  - Kernel 2.2 – IPCHAINS
  - **Kernel 2.4/2.6 - IPTABLES**
- Considerado um dos Firewalls mais seguros da atualidade
- Opensource
- Desenvolvido e suportado pelo Netfilter (http://www.netfilter.org/)
- Netfilter é o nome do módulo que adiciona funcionalidade de Firewall, Nat e Log de rede ao Linux
- Dividido em tabelas (Facilita o controle das regras)

FACVLDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables

- As regras são lidas de cima para baixo
- Firewalls são feitos em shell scritps
- Divido em três tabelas:
  - **Filter:** Regras aplicadas a um firewall do tipo filtro de pacotes
  - **Nat:** Regras direcionadas a um Firewall Nat (Network Address Translation)
  - **Mangle:** Funções mais avançadas e complexas de tratamento de pacotes como TOS
- Todas as tabelas possuem situações de fluxo (**Entrada**, **Saída e Redirecionamento**)

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables – Tabelas - Filter

- Divido em três Situações (Chains):
  - **INPUT:** Tudo que entra no host (O destino do pacote é o próprio firewall)
  - **FORWARD:** Tudo que chega ao host mas deve ser redirecionado
  - **OUTPUT:** Tudo o que sai do host (A origem do pacote é o próprio firewall)

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables – Aplicativos

- **Iptables**
  Aplicativo principal do pacote iptables para protocolos ipv4

- **Ip6tables**
  Aplicativo principal do pacote iptables para protocolos ipv6

- **Iptables-save**
  Aplicativo que salva todas as regras inseridas na sessão ativa e ainda em memória em um determinado arquivo
  Ex: iptables-save > iptables-save.txt

- **Iptables-restore**
  Aplicativo que restaura todas as regras salvas pelo aplicativo iptables-save
  Ex: iptables-restore < iptables-save.txt

- **Iptstate (não faz parte do iptables)**
  Mostra informações em tempo real das tabelas do iptables

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables – Sintaxe - Comandos

-t : Associa uma regra a uma tabela. (filter, nat, mangle). A tabela filter é a tabela padrão e não precisa ser especificada.
 # iptables -t nat

-A : Adiciona uma nova entrada ao final da lista de regas de uma \ determinada chain
 # iptables -A INPUT

-L : Lista as regras existentres
 # iptables -L (Lista todas as chains)
 # iptables -L FORWARD (Regras da chain FORWARD)

-P : Altera a política padrão de uma chain. (Por padrão elas estão em ACCEPT – Aceitam todo tipo de tráfego)
 # iptables -P FORWARD DROP

FACVLDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables – Sintaxe - Comandos

-F : Remove todas as regras adicionadas a uma chain, sem alterar a política padrão.
 # iptables -F (Remove todas as regras)
 # iptables -F INPUT (Remove todas as regras da chain INPT)

-N : Nos permite criar uma nova chain a tabela especificada. Recurso usado para organizar as regras de firewall.
 # iptables -t filter -N pacotes_maliciosos

-X : Apaga uma chain criada com a opção -N
 # iptables -X pacotes_maliciosos

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables – Sintaxe - Ação

-p : Especifica o protocolo aplicado a regra. Pode ser qualquer valor numérico especificado em /etc/protocol ou o próprio nome do protocolo (tcp, udp, icmp)

 # iptables -p icmp

-i : Especifica a interface de entrada (muito importante, pois firewalls possuem múltiplas interfaces)

 # iptables -i eth0

-o : Especifica a interface de saída

 # iptables -o eth1

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables – Sintaxe - Ação

-s : Especifica a origem (source) do pacote ao qual a regra deve ser aplicada. Deve ser um host ou uma rede. Normalmente é utilizado o IP seguido da sub-rede

 # iptables -s 189.1.100.0/255.255.255.0

 # iptables -s 189.1.100.0/24

 # iptables -s www.terra.com.br (Resol. de nomes deve estar ativa)

-d : Especifica o destino (destination) do pacote ao qual a regra deve ser aplicada. Deve ser um host ou uma rede. Normalmente é utilizado o IP seguido da sub-rede

 # iptables -d 189.1.100.0/255.255.255.0

 # iptables -d 189.1.100.0/24

 # iptables -d www.terra.com.br (Resol. de nomes deve estar ativa)

! : Significa exclusão. Exceção a uma regra.

 # iptables -p ! icmp (todos os protocolos com exceção do icmp)

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables – Sintaxe - Ação

--sport : porta de origem (source port), filtros aplicados com base na porta de origem. Só é aplicada aos protocolos TCP e UDP.

 # iptables -p tcp –-sport 80

--dport : porta de destino (destination port), filtros aplicados com base na porta de destino. Só é aplicada aos protocolos TCP e UDP.

 # iptables -p tcp –-dport 80

FACVLDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables – Sintaxe – Alvo (target)

Quando um pacote se adequa a uma regra, ele deve ser direcionado a um alvo especificado na própria regra. O alvo é definido pela opção **-j**

ACCEPT : Corresponde a aceitar o pacote. Permite a entrada/passagem do pacote

DROP : Corresponde a descartar. O pacote é descartado imediatamente. Não informa ao dispositivo emissor o que houve.

REJECT: Corresponde a rejeitar. O pacote é descartado imediatamente. Sua diferença em relação ao anterior é que nesse alvo, o host emissor é notificado.

LOG : Cria uma entrada no arquivo de log /var/log/messages. Deve ser usada antes da regra em questão.

FACVLDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables – Sintaxe – Alvo (target)

SNAT : Altera o endereço de origem das máquinas clientes antes dos pacotes serem roteados. (NAT padrão)

DNAT : Altera o endereço de destino das máquinas clientes. Recebe um pacote na porta 80 do host A e redireciona para a porta 3128 do host B. (proxy transparente).

REDIRECT: Redirecionamento de portas juntamente com a opção --to-port.

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables - Atividades

1. Listando as regras que estão aplicadas ao firewall local.

 # Iptables -L

```
[root@localhost Aula 24 - Firewall]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

* Façam testes de ping uns contra os outros.

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables - Atividades

2. Configure a política padrão das chains da tabela filter para DROP.

```
# Iptables -P INPUT DROP
# Iptables -P OUTPUT DROP
# Iptables -P FORWARD DROP
```

* Re-façam os testes de ping uns contra os outros.

3. Libere totalmente o tráfego para a interface loopback. Essa regra é obrigatória para todo script de firewall, pois garante a comunicação entre processos.

```
# iptables -A INPUT -i lo -j ACCEPT
```

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables - Atividades

4. Permita pings apenas do IP da pessoa que está ao seu lado

```
# Iptables -A OUTPUT -j ACCEPT
# Iptables -A INPUT -i eth0 -s ip/32 -p icmp -j ACCEPT
```

5. Permita pings de todos os computadores da rede local e proíba a pessoa ao seu lado. Use o DROP e REJECT e veja a diferença

```
# Iptables -A INPUT -i eth0 -s ip/32 -p icmp -j DROP
# Iptables -A INPUT -i eth0 -s ip_rede/24 -p icmp -j ACCEPT
```

```
# Iptables -A INPUT -i eth0 -s ip/32 -p icmp -j REJECT
# Iptables -A INPUT -i eth0 -s ip_rede/24 -p icmp -j ACCEPT
```

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables - Atividades

6. Habilite o encaminhamento de pacotes entre redes.

```
# echo "1" > /proc/sys/net/ipv4/ip_forward
ou
# sysctl -w net.ipv4.ip_forward=1
```

7. Bloqueie o seu acesso ao servidor proxy.

```
# Iptables -A OUTPUT -o eth0 -d ip_do_proxy/32 -p tcp –-dport 3128 -j
    DROP
```

Firewall

Iptables - Atividades

9. Limpe todas as regras criadas

```
# iptables -F
```

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables – Tabelas - Nat

- Dividida em três Situações (Chains):
  - **PREROUTING:** Alteração em pacotes antes que os mesmos sejam roteados.
  - **OUTPUT:** Trata de pacotes emitidos pelo host firewall.
  - **POSTROUTING:** Alteração em pacotes após o roteamento.
- Qualquer regra que use SNAT (nat tradicional), a chain utilizada será POSTROUTING.
- Para que o NAT funcione, é necessário ativar no kernel o redirecionamento de pacotes (vide atividade 6).

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables - Nat

- **Ativando o NAT**

 # iptables -t nat -A POSTROUTING -s 10.0.3.1/32 -o eth1 -j SNAT --to 192.111.22.33

Dessa forma, todo pacote que vier do host 10.0.3.1 terá seu endereço de origem alterado.

 # iptables -t nat -A POSTROUTING -s source_net/24 -o eth1 -j MASQUERADE

Ativo o NAT para todos os hosts da rede source_net para o endereço IP da interface eth1.

FACVLDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables - Atividades

10. Adicione um novo endereço IP de uma rede diferente da rede atual em sua interface eth0. Ative nat do novo endereço para o antigo endereço Na máquina do vizinho, remova o endereço atual, e adicione um da nova rede. Configure como rota padrão dessa máquina o endereço novo de sua máquina e tente acessar a internet.

No Firewall

```
# ifconfig eth0:1 192.168.100.X up
# sysctl -w net.ipv4.ip_forward=1
# iptables -F
# iptables -t nat -A POSTROUTING -s rede_nova/24 -o eth0 -j SNAT
    --to ip_antigo
```

No cliente

```
# ifconfig eth0 down
# ifconfig eth0 192.168.100.X up
# route add default gw ip_firewall
```

FACULDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables - Atividades

11. Teste o acesso a Internet e ping a partir do cliente
12. Bloqueie no firewall o acesso a internet de apenas um cliente

```
# Iptables -A FORWARD -i eth0 -s ip_cliente/32 -p tcp –-dport 80 -j
    DROP
```

13. Bloqueie no firewall o encaminhamento de icmp de toda a rede

```
# Iptables -A FORWARD -i eth0 -s ip_nova_rede/24 -p icmp  -j DROP
```

FACVLDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

Firewall

Iptables - Atividades

14. Configure um firewall que possua uma interface eth0(Lan 192.168.120.0/24) e uma interface eth1(wan) com as seguintes características (coloque as configurações em um script):

- Define a política padrão para DROP

- Permita acesso a Internet da LAN via NAT

- Permita que apenas a máquina do administrador (192.168.120.10) tenha acesso a todas as portas/hosts da Internet, os demais poderão acessar apenas as portas 80, 20, 21, 25, 110 do protocolo tcp.

- Permita todo o tráfego de saída gerado pelo servidor

- Permita acesso aos seguintes serviços do firewall:
  - SSH apenas para o administrador
  - DNS para toda a rede
  - PING para toda a rede

FACVLDADE MAURÍCIO DE NASSAU
FAZENDO PARTE DA SUA HISTÓRIA
RECIFE • JOAO PESSOA • CAMPINA GRANDE

ADMINISTRAÇÃO DE REDES I
LINUX

Firewall

Frederico Madeira
LPIC-1, CCNA
fred@madeira.eng.br
www.madeira.eng.br