
4LINUX
FREE SOFTWARE SOLUTIONS

Linux Network Servers

Servidor Firewall

Objetivos:

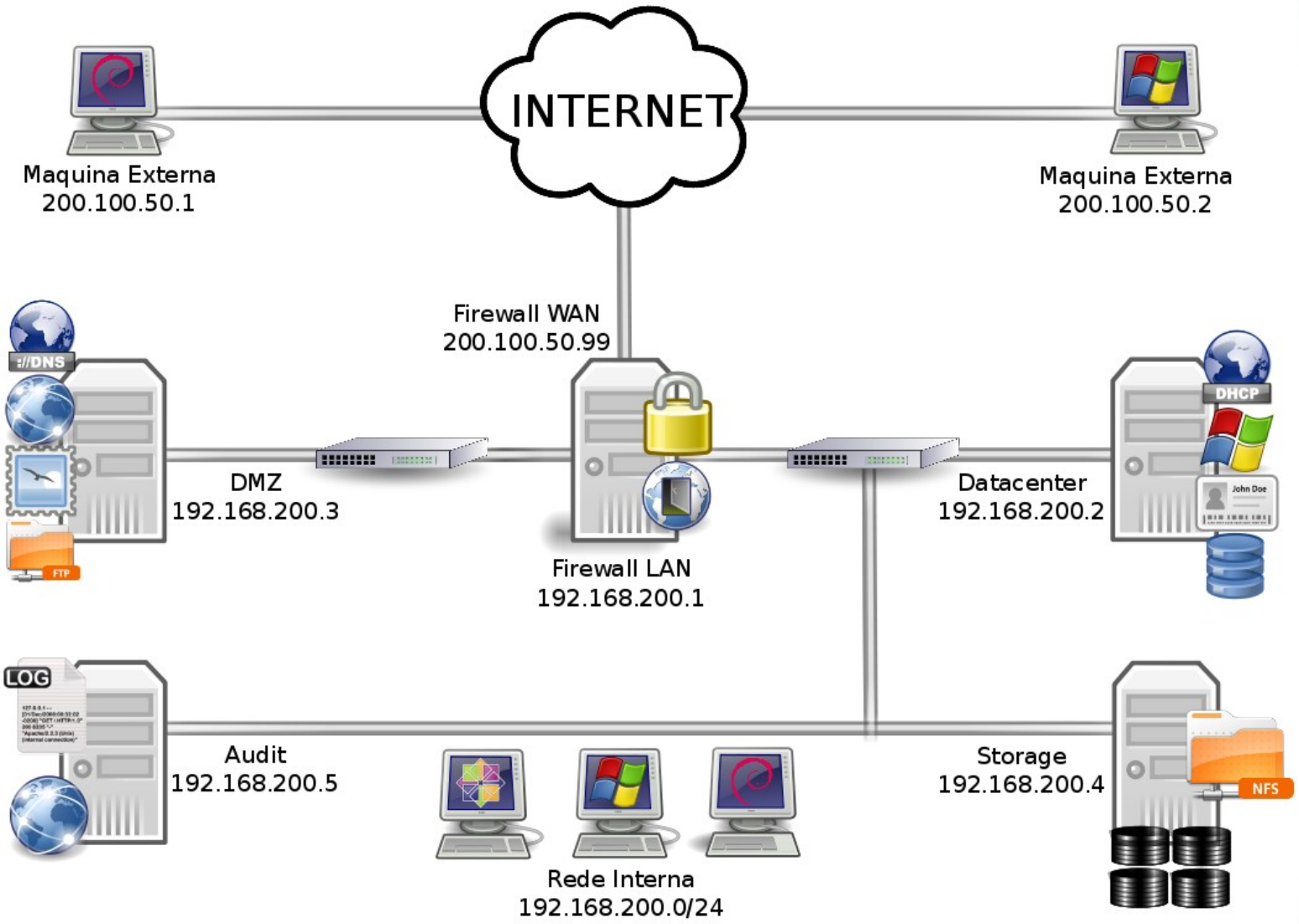
- Introdução Teórica;
- Conhecer a infraestrutura da empresa;
- Conhecer os tipos de tabelas do Iptables;
- Compreendendo as políticas e as exceções;
- Implementação prática com Script de Firewall.

Servidor Firewall

Introdução ao Firewall

Um firewall faz o filtro de pacotes que passam na rede. Para configurar um firewall é necessário o conhecimento sobre a estrutura da rede em questão e dos diferentes protocolos envolvidos na comunicação, isto é, dos serviços que a rede usa para que eles não percam a comunicação. O objetivo em ter uma máquina fazendo o papel de Firewall Gateway em nossa é rede é minimizar as tentativas de ataques que elas recebem, tentando impedir possíveis invasões e levantamento de informações.

Servidor Firewall



Servidor Firewall

Tipos de Tabelas

- **Filter**
- **Nat**
- **Mangle**
- **Raw**

Para listar as “chains” que cada tabela possui use a sinxtaxe:

 # iptables -L -t <tabela>

Servidor Firewall

Tipos de Chain

Uma chain é local onde vão ser definidas as regras para o nosso firewall. Cada Tabela possui suas CHAINS.

Chais da tabela Filter:

INPUT – Regras de entrada de pacotes;

OUTPUT – Regras de saída de pacotes;

FORWARD – Regras de passagem de pacotes pelo firewall.

Servidor Firewall

Tipos de Chain

Chais da tabela NAT:

PREROUTING – Regras que serão processadas antes do roteamento dos pacotes nas interfaces do firewall;

POSTROUTING – Regras que serão processadas pós roteamento dos pacotes nas interfaces do firewall;

OUTPUT – Regras de saída de pacotes.

Servidor Firewall

Compreendendo as políticas e as exceções

- **Políticas básicas:**
  - Negar todo o tráfego para as "chains"de "INPUT", "OUTPUT" e "FORWARD".
- **Exceções:**
  - Definir a relação dos serviços que devem ser liberados no "Firewall".
- **Controles**:
  - O que não for oficialmente permitido já está expressa e previamente negado.

Servidor Firewall

SIntaxe do Iptables

A sintaxe do comando iptables:

iptables [-t tabela] [opção] [chain] [dados] -j [alvo]

Exemplo para compartilhar a internet:

Iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

Servidor Firewall

Parâmetros e alvos do Iptables

	Parâmetros	Descrição
-P	--policy	Estabelece a politica de acesso de uma chain.
-t	--table	Seleciona uma tabela
-A	--append	Adiciona como ultima regra da sequencia de uma chain
-I	--insert	Insere como primeira regra da sequencia de uma chain
-N	--new-chain	Cria uma nova chain
-D	--delete	Remove uma regra
-X	--delete-chain	Elimina todas as regras presentes em chains de usuário
-F	--flush	Elimina todas as regras presentes em uma chain padrão
-s	-source	Determina a origem do pacote
-d	--destination	Determina o destino do pacote

Servidor Firewall

Parâmetros e alvos do Iptables

--sport	--source-port	Define a porta de origem
-i	--in-interface	Define a interface de entrada
-o	--out-interface	Define a interface de saida
-p	--protocol	Seleciona o protocolo (tcp, udp, icmp)
Alvo (target)		**Descrição**
ACCEPT		O pacote é aceito
REJECT		O pacote é rejeitado imediatamento
DROP		O pacote é negado silenciosamente

Servidor Firewall

Implementação prática com script de Firewall

1 – Antes de começar o script, ative de forma permanente o repasse de pacotes entre as interfaces de rede:

 # vim +28 /etc/sysctl.conf

net.ipv4.ip_forward=1

 # sysctl -p

2 – Adicione um cabeçalho para inicialização durante o boot, e permissão de execução ao script de Firewall:

 # head /etc/init.d/ssh > /etc/init.d/firewall

 # chmod u+x /etc/init.d/firewall ; vim /etc/init.d/firewall

Servidor Firewall

Implementação prática com script de Firewall

3 – Abra o script e após o cabeçalho, declare as variáveis

```
ALL="0:65535"
PA="1024:65535"
LAN="192.168.200.0/24"
LANVPN="10.0.0.0/24"
WAN1="200.100.50.99"
WAN2=$(ifconfig eth1 | grep "inet end.:" | awk -F" " '{print $3 }')
FW="192.168.200.1"
DC="192.168.200.2"
DMZ="192.168.200.3"
STORAGE="192.168.200.4"
AUDIT="192.168.200.5"
```

Servidor Firewall

Implementação prática com script de Firewall

4 – Após as variáveis continue a construção do script:

```
case $1 in
stop)
# politicas que aceitam qualquer tipo de conexão
iptables -P OUTPUT ACCEPT
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT

# limpar as regras das tabelas nat e filter
iptables -t nat -F
```

Servidor Firewall

Implementação prática com script de Firewall

```
iptables -t filter -F

;;


start)
# politicas que bloqueiam qualquer tipo de conexão
iptables -P OUTPUT DROP
iptables -P INPUT DROP
iptables -P FORWARD DROP
;;
```

Servidor Firewall

Implementação prática com script de Firewall

```
restart)
$0 stop
sleep 0.5
$0 start
;;


*)
echo 'POR FAVOR USE "stop|start|restart"'
;;
esac
```

Servidor Firewall

Testando a primeira parte do script de Firewall

Liste as regras da tabela Filter:

 # iptables -nL

Execute o script para aplicar as regras de bloqueio:

 # service firewall start

Liste novamente as regras:

 # iptables -nL

Execute o script para aplicar as regras de acesso:

 # service firewall stop

Servidor Firewall

Criando a segunda parte do script de Firewall

1 – Abra o script e adicione novas regras no final da seção “start”

 # permite que a maquina FIREWALL ping a loopback

iptables -A OUTPUT -p icmp -d 0/0 -j ACCEPT

iptables -A INPUT -p icmp -d 127.0.0.1 -j ACCEPT

 # permite que a maquina FIREWALL ping para o resto do mundo

iptables -A INPUT -p icmp -d $WAN1 -j ACCEPT

iptables -A INPUT -p icmp -d $WAN2 -j ACCEPT

iptables -A INPUT -p icmp -d $FW -j ACCEPT

Servidor Firewall

Criando a segunda parte do script de Firewall

 # permite que a maquina ping para o resto do mundo por nomes

iptables -A INPUT -p udp --sport 53 -s 0/0 -d $WAN2 --dport $PA -j ACCEPT

iptables -A OUTPUT -p udp --sport $PA -s $WAN2 -d 0/0 --dport 53 -j ACCEPT

 # permite a passagem de pacotes pela porta http

iptables -A INPUT -p tcp --sport 80 -s 0/0 -d $WAN2 --dport $PA -j ACCEPT

iptables -A OUTPUT -p tcp --sport $PA -s $WAN2 -d 0/0 --dport 80 -j ACCEPT

Servidor Firewall

Criando a segunda parte do script de Firewall

 # permite que a maquina FIREWALL receba conexões remotas por SSH

iptables -A INPUT -p tcp -s 0/0 --sport $PA -d $WAN1 --dport 51000 -j ACCEPT

iptables -A OUTPUT -p tcp -s $WAN1 --sport 51000 -d 0/0 --dport $PA -j ACCEPT

2 – Salve e teste o script

 # service firewall restart ; iptables -nL

Servidor Firewall

Criando a terceira parte do script de Firewall

1 – Abra o script e adicione novas regras no final da seção “start”

 # habilita a passagem de pacotes da REDE local em direção ao mundo.

iptables -t nat -I POSTROUTING -o eth1 -s $LAN -j MASQUERADE

 # habilita a passagem de pings da REDE para o mundo.

iptables -A FORWARD -p icmp -d $LAN -j ACCEPT

iptables -A FORWARD -p icmp -s $LAN -j ACCEPT

Servidor Firewall

Criando a terceira parte do script de Firewall

 # habilita a resolução de nomes do mundo para a REDE.

```
iptables -A FORWARD -p udp --sport 53 -s 0/0 -d $LAN --dport $PA -j ACCEPT

iptables -A FORWARD -p udp --sport $PA -s $LAN -d 0/0 --dport 53 -j ACCEPT
```

 # habilita a passagem e o uso dos protocolos comuns para as maquinas internas.

```
for serv_ext in  80 443 25 110 143 993 995 21 20

do
```

Servidor Firewall

Criando a terceira parte do script de Firewall

iptables -A FORWARD -p tcp --sport $serv_ext -s 0/0 -d $LAN --dport $PA -j ACCEPT

iptables -A FORWARD -p tcp --sport $PA -s $LAN -d 0/0 --dport $serv_ext -j ACCEPT

done

2 – Salve e teste o script

 # service firewall restart

 # iptables -nL ; iptables -t nat -nL

Servidor Firewall

Criando a quarta parte do script de Firewall

1 – Abra o script e adicione novas regras no final da seção “start”

 # habilita o redirecionamento de portas do SSH da maquina Firewall para as maquinas internas.

```
for ip in 2 3 4 5
do
iptables -A OUTPUT -p tcp -s 0/0  --sport $PA -d 192.168.200.$ip  --dport 5$ip'000' -j ACCEPT
iptables  -A  INPUT  -p  tcp   --sport  5$ip'000'  -s  192.168.200.$ip   -d  0/0 --dport $PA -j  ACCEPT
```

Servidor Firewall

Criando a quarta parte do script de Firewall

iptables -A FORWARD -p tcp --sport 5$ip'000' -s 192.168.200.$ip -d 0/0 --dport $PA -j ACCEPT

iptables -A FORWARD -p tcp --sport $PA -s 0/0 -d 192.168.200.$ip --dport 5$ip'000' -j ACCEPT

iptables -t nat -A PREROUTING -p tcp --sport $PA -s 0/0 -d $WAN1 --dport 5$ip'000' -j DNAT --to-destination 192.168.200.$ip':'5$ip'000'

done

2 – Salve e teste o script

 # service firewall restart ; iptables -nL

Servidor Firewall

Carregando o script no boot

Para que ele seja iniciado junto com sistema quando a máquina for ligada, podemos colocar o "script" nos níveis de execução:

 # insserv -d firewall

 # ls -l /etc/rc2.d

Utilização dos comandos "iptables-save" e "iptables-restore".

 # iptables-save > /root/firewall ; service firewall stop

 # iptables-restore /root/firewall

 # iptables -nL ; iptables -t nat -nL

Servidor DHCP

Objetivos:

- Introdução Teórica;
- Entender o funcionamento do serviço;
- Implementar na prática o Servidor DHCP;
- Configurar Servidor DHCP;
- Configurar clientes DHCP;
- Fixar IP via DHCP.

Servidor DHCP

Introdução ao DHCP

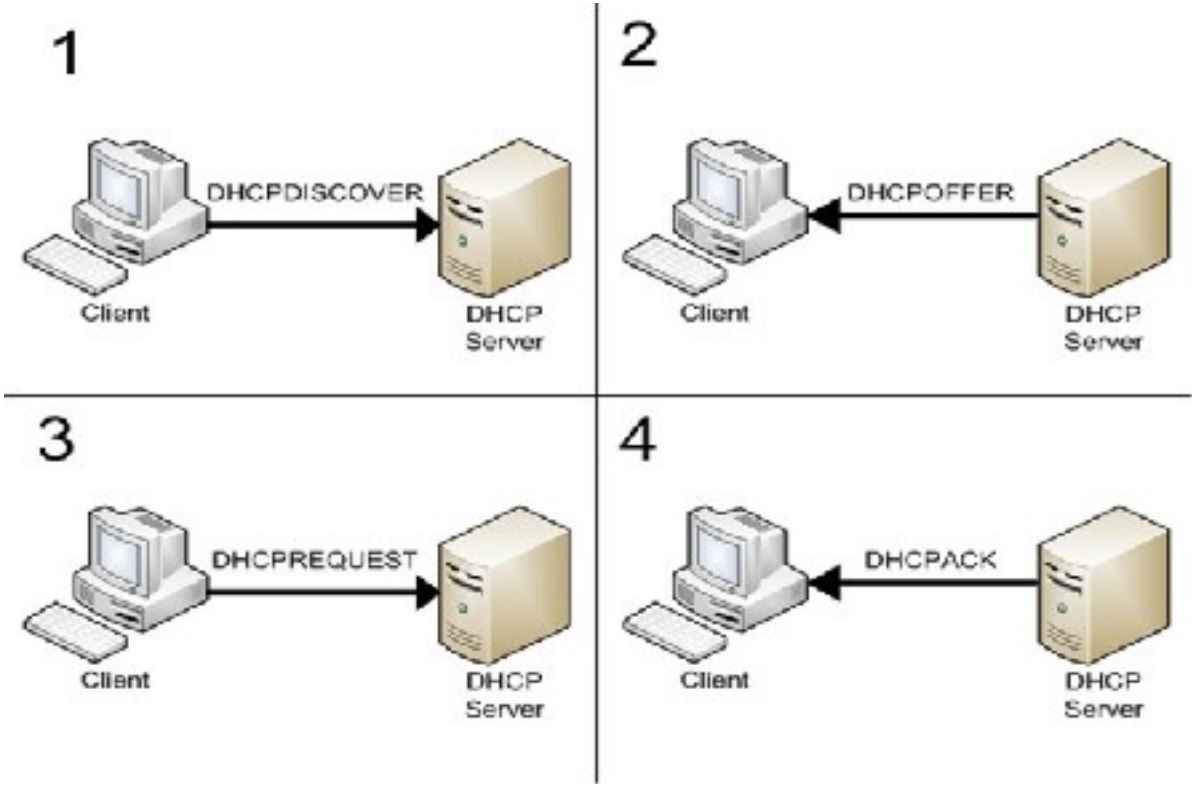
O protocolo **DHCP** (Dynamic Host Configuration Protocol)} funciona nas camadas 2 e 3 do modelo OSI e é amplamente utilizado para oferecer endereço IP a um "host" que ainda não está configurado, o que oferece uma flexibilidade ao Administrador de Redes.

O "DHCP" oferece três tipos de alocação de endereços IP:

- Atribuição manual
- Atribuição automática
- Atribuição dinâmica

Servidor DHCP

Funcionamento do DHCP



Servidor DHCP

Implementação prática: Configuração do Servidor

1 – Primeiro iremos instalar o pacote do servidor dhcp na maquina Datacenter:

 # aptitude install isc-dhcp-server

2 – Vamos renomear o arquivo original do DHCP para uma possível consulta:

 # cd /etc/dhcp

 # mv dhcpd.conf dhcpd.conf.dist

Servidor DHCP

Implementação prática: Configuração do Servidor

3 - Agora vamos iniciar nossa configuração num arquivo zerado

 # vim /etc/dhcp/dhcpd.conf

```
ddns-update-style none;
#deny unknown-clients;
log-facility local7;

subnet 192.168.200.0 netmask 255.255.255.0 {
    range 192.168.200.10 192.168.200.100;
    authoritative;
```

Servidor DHCP

Implementação prática: Configuração do Servidor

```
    option domain-name "dexter.com.br";
    option domain-name-servers 192.168.200.3,192.168.200.2;
    option netbios-name-servers 192.168.200.2;
    option routers 192.168.200.1;
    default-lease-time 600;
    max-lease-time 7200;
    min-lease-time 120;
}
```

Para habilitar o suporte ao servidor dinâmico, utilize **dynamic-bootp**

Servidor DHCP

Implementação prática: Configuração do Servidor

4 – Ative os Logs para o servidor DHCP

 # vim /etc/rsyslog.conf

local7.* /var/log/dhcpd.log

 # service rsyslog restart

5 – Reinicie o serviço e verifique os Logs

 # service isc-dhcp-server restart

 # tail -f /var/log/dhcpd.log

Servidor DHCP

Implementação prática: Configuração do Cliente

1 – Na maquina **interna**, abra o arquivo de rede e configure a interface eth0 para pegar IP via DHCP :

 # vim /etc/network/interfaces

```
auto eth0
   iface eth0 inet dhcp
```

2 – Reinicie o serviço de rede para obter as configurações do servidor

 # service networking restart

 # dhclient eth0 -v

Servidor DHCP

Fixar IP via DHCP

1 – Na maquina **Datacenter**, ping o cliente para testar a conectividade:

 # ping -c4 192.168.200.10

2 – Envie para o final do arquivo de configuração o **"MAC Address"** do cliente:

 # arp -n | awk -F" " '{print $3}' >> /etc/dhcp/dhcpd.conf

Servidor DHCP

Fixar IP via DHCP

3 – Adicione no final do arquivo de configuração o bloco abaixo, para "fixar" um IP ao **"MAC Address"** do cliente:

```
host maq-interna {
        hardware ethernet 00:00:00:00:00:00;
        fixed-address 192.168.200.10;
}
```

4 – Reinicie o serviço par aplicar as mudanças

 # service isc-dhcp-server restart

Próximos passos

Para que você tenha um melhor aproveitamento do curso, participe das seguintes atividades disponíveis no Netclass:

- Executar as tarefas do "**Laboratório**" dexterlab-2 para treinar a configuração de um servidor Firewall e DHCP;
- Resolver o "**Desafio**" para bloquear a duplicação de IPs, no servidor de DHCP, e postar o resultado no Fórum Temático;
- Responder as questões do "**Teste de Conhecimento**" sobre o conteúdo visto em aula.

Mãos a obra!