**ENTENDENDO O IPTABLES**

**OBSERVAÇÕES PARA MELHOR ENTENDIMENTO:**

**1 - PDU:** São frames, pacotes ou datagramas.

* **O que é um FRAME ?**

Um quadro é uma unidade de transmissão digital de dados em redes de computadores e telecomunicações. Em sistemas de comutação de pacotes, um quadro é um contêiner simples para um único pacote de rede.

* **O que é um PACOTE ?**

Em uma rede de computadores ou telecomunicações, pacote ou trama é uma estrutura unitária de transmissão de dados ou uma sequência de dados transmitida por uma rede ou linha de comunicação que utilize a comutação de pacotes. A informação a transmitir geralmente é quebrada em inúmeros pacotes e então transmitida.

* **O que é um DATAGRAMA ?**

Um datagrama é uma unidade de transferência básica associada a uma rede de comutação de pacotes. Os datagramas são normalmente estruturados em seções de cabeçalho e carga útil. Os datagramas fornecem um serviço de comunicação sem conexão em uma rede comutada por pacotes.

Comando iptable 
Iptable é uma interface de linha de comando usad 
para configurar e manter tabelas para o firewall 
Netfilter para IPv4, incluído no kernel Linux. 
O firewall combina PDU com regras definidas nessas 
tabelas e, em seguida, executa a ação especificada em 
uma possível correspondência. 

**OBSERVAÇÕES PARA MELHOR ENTENDIMENTO:**

**POLICY:** Explicando esta função, então, quando um PDU passar por todas as regras (RULES) e não for de acordo com a devida regra (RULE), então será aplicado automaticamente sobre este PDU a POLICY, que nada ais é que uma regra (RULE) padrão/default.

Iptables 
Table é o nome de um conjunto de CHAINs. • 
Chain é uma coleção de RULEs. 
Rule é a condição usada para o Netfilter atuar sobre o 
PDU. 
Target é a ação realizada quando uma possível RÚLE 
corresponde. 
Policy é a ação padrão realizada em caso de não 
corresppndência com as cadeias integradas. 

**ONDE PODEMOS APLICAR O IPTABLES ?**

**OBSERVAÇÕES PARA MELHOR ENTENDIMENTO:**

**1 - ACL: É importante compreendermos bem sobre o que é uma ACL (Lista de controles de acessos), para melhor compreensão sobre a importância de um FIREWALL na rede.**

**EXPLICANDO SOBRE O QUE É O TERMO ACL EM REDES DE COMPUTADORES:** ACL em segurança de computador, uma lista de controle de acesso é uma lista de permissões associadas a um recurso do sistema. Uma ACL especifica quais usuários ou processos do sistema têm acesso aos objetos, bem como quais operações são permitidas em determinados objetos.

**2 - ALTERAÇÕES EM PDU:** Trata-se de técnicas de masquerading, com esta técnica, nos d aa possibilidade de esconder tudo "por trás" do host. Isso é válido em cenários para fornecer Internet para vários hosts quando você tiver apenas um endereço IP de uplink. Essa tecnologia é usada na maioria dos roteadores de acesso à Internet, chamados de "NAT".

**3 - NAT (NETWORK ADDRESS TRANSLATION):** É o redirecionamento de PDUs (FRAME, PACOTE ou DATAGRAMA) dentro da rede, ou seja, é pregarmos uma "carta como exemplo" e encaminhar ela se passando por nós, isto é o redirecionamento.

**4 - MASQUERADING EM SNAT:** É quando utilizamos a técnica conhecida como "guarda chuva" em nossa rede, ou seja, fazemos uma requisição para o mundo (a "carta como exemplo" sai para o mundo, sai para a internet, sai para fora), nesta etapa que a carta sai para o mundo, ela vai obter o IP de ponta do gateway **(SERÁ ALTERADA COM MASQUERADING)** e quando ela voltar, temos que saber entender este retorno e faze-la retornar ao nosso "guarda chuva", ou seja, fazer com que a nossa rede interna entenda esta "carta como exemplo" que chegou de uma rede externa totalmente distinta (MUNDO), então esta é a função do SNAT.

**MAIS INFORMAÇÕES SOBRE SNAT:** Também pode ser compreendido como uma forma de fazer tradução de endereços, por exemplo ao criar uma regra permite que através de um único endereço seja realizada a tradução para vários hosts em uma rede, podendo ser feita de três formas no BIG-IP, por um endereço especifico, um pool de endereços ou Automap.

**5 - REDIRECIONAMENTOS DE PORTAS COM DNAT (DESTIONATION NAT):** Muito utilizado quando queremos habilitar alguma devida porta ou jogar tal porta para "dentro" da rede, ou seja, é uma técnica que traduz o endereço IP de destino geralmente ao conectar de um endereço IP público para um endereço IP privado.

6 - **LOAD BALANCING:** Disponibiliza o balanceamento de carga entre 2 links por exemplo e etc.

Aplicações 
Filtros de PDU; 
Monitoramento de PDU; 
Conexões com serviços; 
Alterações em PDU; 
Netowork Address Translation (NAT); 
Masquerading em SNAT; 
Redirecionamento de portas com DNAT; 
Load Balancing; 

**TABELAS UTILIZADAS NO NETFILTER (IPTABLES)**

Organização das Regras 
As regras de Iptables são organizadas em tabela#, 
são estas: 
filter; 
nat; 
mangle; 
raw. 

**OBSERVAÇÕES PARA UM MELHOR ENTENDIMENTO:**

**1 - TABELA FILTER:** Resumindo, está é a tabela padrão utilizada pelo iptables. Portanto, não definirmos a nossa própria tabela, automaticamente será utilizado a tabela FILTER.

Tabela filter 
Filter é a tabela padrão para iptables. 
Portanto, se você não definir sua própria tabela, 
usará a tabela de fiter. 

Tabela filter 
A tabela de filtros de Iptables possui as seguinte 
chains embutidas. 
INPUT - Entrada para firewall. Para pacotes que chegam ao. 
servidor local. 
OUTPUT - Saída do firewall. Para pacotes gerados localmente•e • 
saindo do servidor local. 
FORWARD - Pacote para outra NIC no servidor local. Para 
pacotes roteados por meio do servidor local. 

**EXEMPLO DE FUNCIONALIDADE DAS CHAINS PADÕRES QUE JÁ VEM EMBUTIDAS NA TABELA FILTER:**

**ORIGEM:** Neste exemplo, vamos considerar que a ORIGEM é a rede mundial (externa, ou seja, na rede WAN) e esta rede WAN esta enviando PDUs (requisições HTTP sendo realizadas para a nossa VM por exemplo) para a nossa rede interna, então, segue explicações abaixo caso este PDU/REQUISIÇÃO se encaixe nas CHAINS de FORWARD, INPUT ou OUTPUT:

**FORWARD:** Imagine que o PDU/REQUISIÇÃO esta vindo da rede WAN (REDE MUNDIAL/EXTERNA QUE NO EXEMPLO ABAIXO ESTAMOS CHAMANDO DE "ORIGEM") e caso o mesmo se encaixe nas regras de FORWARD, então a regra será executada e antes de ocorrer o processamento da VM, o PDU/REQUISIÇÃO será retransmitida para a outra interface de rede passando por FORWARD.

**INPUT:** Imagine que o PDU/REQUISIÇÃO esta vindo da rede WAN (REDE MUNDIAL/EXTERNA QUE NO EXEMPLO ABAIXO ESTAMOS CHAMANDO DE "ORIGEM") e caso o mesmo se encaixe nas regras de de INPUT, então a regra será executada e o PDU/REQUISIÇÃO será processado pelos processos locais da VM passando por INPUT.

**OUTPUT:** Imagine que um PDU/REQUISIÇÃO esteja sendo processado para sair da nossa VM local para a rede WAN (REDE MUNDIAL/EXTERNA QUE NO EXEMPLO ABAIXO ESTAMOS CHAMANDO DE "ORIGEM") e o mesmo se encaixe nas regras de OUTPUT, então a regra será executada e o PDU/REQUISIÇÃO será processado e RETRANSMITIDO para a INTERFACE DE REDE que for configurada.

ORIGEM 
Tabela filter 
Network 
. interface • 
• Network 
: interface 
s 
o 
FORWARD 
INPUT 
OUTPUT 
D 
s 
o 
Local 
process 
Local 
process 
ORIGEM 
Esta måquina possui 2 interfaces de rede 

**2 - TABELA NAT:** Resumindo, a tabela NAT de IPTABLES possui as cadeias integradas PREROUTING CHAIN, POSROUTING CHAN e OUTPUT - NAT.

**OBSERVAÇÕES PARA UM MELHOR ENTENDIMENTO:**

**1 - PREROUTING CHAIN:** Podemos realizar alteração de PDUs antes do roteamento por isso é chamado de PREROUTING, ou seja, podemos fazer acontecer uma tradução, uma mudança de porta como por exemplo: Imagine que recebemos um PDU no nosso gateway pela porta 80, podemos fazer com que isso mude para que seja processado internamente ()para dentro da nossa rede na nossa rede na porta 8080 e não na 80, possibilitando assim o apelido técnico que é conhecido como "GUARDA CHUVA".

Tabela nat 
A tabela NAT de Iptable possui as seguinte çadei s 
integradas. 
PREROUTING Chain - Altera os pacotes antes do roteamento. 
ou seja, a tradução do pacote acontece imediatamente após o 
pacote chegar ao sistema (e antes do roteamento). 
Isso ajuda a traduzir o endereço IP de destino dos pacotes em 
algo que corresponda ao roteamento no servidor local: 

**2 - POSROUTING CHAIN:** Como o próprio nome pode adiantar do que se trata, com este tipo de cadeia integrada conseguimos realizar alterações dos PDUs recebidos em nossa rede após o roteamento (APÓS O PROCESSAMENTO DA VM NO EXEMPLO QUE ESTAMSO UTILIZAND NOS GRÁFICOS EM QUESTÃO), ou seja, recebemos o PDU onde foi atendido na cadeia integrada PREROUTING e foi processado no processamento local, e agora precisamos realizar alguma alteração para atender uma devida particularidade, por isso se chama POSROUTING, pois conseguimos alterar o PDU para dentro da nossa rede LAN após o passo de PREROUTING, é muito útil quando precisamos fazer traduções de endereços IPs por exemplo.

Tabela nat 
o 
POSTROUTING chain - Altera os pacotesa ós 
roteamento. ou seja, a tradução de pacotes aconte 
quando os pacotes estão deixando o sistema. 
Isso ajuda a traduzir o endereço IP de origem dos 
pacotes em algo que possa corresponder ao roteamento 
no servidor de destino. 

**3 - OUTPUT - NAT:** É a saída de PDUs gerados localmente (internamente em nossa rede LAN) no firewall.

Tabela nat 
OUTPUT - NAT para pacotes gerados localmente o 
firewall. 

**EXEMPLO DAS CADEIAS INTEGRADAS (PREROUTING CHAIN, POSROUTING CHAIN E OUTPUT - NAT) EM FUNCIONAMENTO, DEMONSTRADO ATRAVÉS DO GRÁFICO ABAIXO:**

Tabela nat 
Network 
. interface 
Network 
: interface 
s 
REROUTING 
POSTROUTING 
OUTPUT 
s 
o 
Local 
process 
Local 
process 
ORIGEM 
Esta måquina possui 2 interfaces de rede 

**EXEMPLO DE CHAINS ENTRE AS TABELAS FILTER E NAT SENDO EXECUTADAS EM CONJUNTO E EM SEQUENCIA (POR VIA DE REGRA, AS CHAINS SÃO EXECUTADAS DE FORMA SEQUENCIAL):**

**OBSERVAÇÃO IMPORTANTE PARA ENTENDIMENTO: As ACLs são executadas dentro das CHAINs de cada tabela no IPTABLES.**

Tabela nat 
Network 
. interface 
Network 
: interface 
s 
REROUTING 
POSTROUTING 
OUTPUT 
s 
o 
Local 
process 
Local 
process 
ORIGEM 
Esta måquina possui 2 interfaces de rede 

**3 - TABELA MANGLE:** Resumindo, a tabela MANGLE do IPTABLES é dedicada para alterações especializada de PDUs, e isso altera os bits de QOS no cabeçalho, ou seja, faz a alteração sobre "envelopes dos pacotes" que chegam na nossa rede LAN (rede interna).

Tabela mangle 
A tabela Mangle do Iptables é para alterÀçã 
especializada de PDU. Isso altera os bits de QOS ncy 
cabeçalho TCP. 

**OBSERVAÇÕES PARA UM MELHOR ENTENDIMENTO: A tabela MANGLE utiliza as seguintes cadeias integradas (CHAINs) PREROUTING, OUTPUT, FORWARD, INPUT e POSROUTING.**

A tabela Mangle tem as seguintes cadeias integradas. 
PREROUTING 
OUTPUT 
FORWARD 
INPUT 
POSTROUTING 

**EXEMPLO DAS CADEIAS INTEGRADAS (CHAINs) EM EXECUÇÃO DEMOSNTRADAS ATRAVÉS DO GRÁFICO ABAIXO:**

Tabela mangle 
ORIGEM 
DESTINO 
Network 
interface 
Network 
interface 
REROUTING 
FORWARD 
POSTROUTING 
INPUT 
OUTPUT 
s 
o 
Local 
process 
Local 
process 
ORIGEM 

**4 - TABELA RAW:** Resumindo, a tabela RAW é uma tabela bruta e utilizamos a mesma antes de qualquer coisa, ou seja, colocamos em RAW aquilo que é utilizado antes de qualquer coisa, como por exemplo e boa prática algum PDU que não queiramos rastrear, pois nem todos os PDUs faz-se necessários monitoramento e/ou rastreamento.

O Tabela raw 
E usado apenas para configurar pacotes.de orma e 
fiquem isentos de rastreamento de conexão. 

**5 - OPÇÕES DE REGRAS:** Resumida em "SE O PDU EM QUESTÃO NÃO SE APLICA A NENHUMA DAS REGRAS DE INPUT OU FORWARD OU OUTPUT, ENTÃO DEVE SER APLICADO A REGRA DA POLICY PADRÃO, QUE POR PADRÃO DO PRÓRPRIO FABRICANTE É ACCEPT, OU SEJA, É MUITO PERMISSIVA E RETORNAMOS A DIZER, ISTO É UMA FALHA DE SEGURANÇA E ESTA REGRA PADRÃO PRECISA SER ALTERADA PELO ADMINISTRADOR EM AMBIENTES DE PRODUÇÃO, PODE SER MANTIDA ASSIM APENAS EM AMBIENTE DE LABORATÓRIO".

Opções de Regras 
INPUT 
Executado se 
nenhuma regra de 
entrada foi 
executada. 
FORWARD 
Executada quando 
nenhuma regra de 
redirecionamento foi 
executada. 
OUTPUT 
Executada se 
nenhuma regrá de 
saída foi executada. 

**EXEMPLO**: POLICY padrão é ACCEPT para as CHAINs INPUT, FORWARD e OUTPUT:

Isso quer dizer que quando recebermos quaisquer PDUs da rede WAN (REDE MUNDIAL/EXTERNA), automaticamente os pacotes irão para o PROCESSAMENTO LOCAL DA VM, conforme é o cenário dos gráficos que estamos utilizando como exemplo, isso é perigoso e pode ser uma falha de segurança, pois é MUITO PERMISSIVO, por isso é recomendado que esta regra na POLICY PADRÃO seja alterada em ambiente de produção, para não ser PERMISSIVA neste nível que é como padrão.

root@debian i tables —t 
filter 
-L 
Chain INPUT (policu RCCEPT 
target 
pro op source 
Chain FORLAIRRD (policu ACCEPT) 
target 
prot opt 
Chain OUTPUT ( 01 ic 
target 
prot opt 
root@debian : ft$ 
source 
source 
dest inat ion 
destination 
dest i nation 

**PRINCIPAIS TARGETS (OPÇÕES) DE POLICY PADRÃO**

0 Principais opções 
ACCEPT 
o Firewall aceitará o PDU; 
QUEIJE 
O Firewall passará o PDU 
para o espaço do usuário; 
DROP 
O Firewall descartará U• 
RETURN 
O Firewall irá parar de 
executar o próximo conjunto 
de regras na corrente atual 
para este pacote. 

**SINTAXE DE COMANDOS IPTABLES NO LINUX**

Sintaxe do comando iptables no Linux 
iptabtes 
iptables 
iptab les 
iptables 
iptab les 
iptabtes 
tab le] 
tab te] 
tab te] 
tab te] 
tab te] 
tab le] 
{ -Al -Cl -D} chain 
-I chain [rulenum] rule-specificatio 
-R chain rulenum rule-specification 
-D chain rulenum 
-S [chain [rulenum]] 
{-FI-LI -Z} [chain [rulenum]] [options. 

Sintaxe do comando iptables no Linux 
iptabtes [ -t table] 
iptables [ -t table] 
iptabtes [ -t table] 
iptables [ -t table] 
rule-specification = 
-N chain 
-X [chain] 
-P chain target 
-E old-chain-name new-chain-name 
[matches . 
• • ] [target] 
match = -m matchname [per-match-options] 
target = -j targetname [per-target-options] 

iptabtes 
iptab les 
iptables 
iptables 
iptab les 
iptab les 
Sintaxe do comando iptables no Linux 
-t 
tab le] 
tab le] 
tab te] 
tab te] 
tab te] 
tab te] 
{ -Al -Cl -D} chain 
-I chain [rulenum] rule-specificatio 
-R chain rulenum rule-specification 
-D chain rulenum 
-S [chain [rulenum]] 
{-FI-LI -Z) [chain [rutenum]] [options. 

**OBSERVAÇÕES PARA UM MELHOR ENTENDIMENTO:**

1 - Quando não colocamos o parâmetro -t NOME\_TABELA, então o comando em questão será aplicado para todas as tabelas (FILTER, NAT, MANGLE e RAW), pois não houve definição de nome da tabela.

**PARAMETROS PARA USO COM OS COMANDOS IPTABLES**

Regras do comando Iptables 
-A anexa a regra ao fim da lista (CHAIN) já existe te. 
-D apaga a regra especificada. 
-L lista as regras existentes na lista. 
-P altera a Policy padrão das chains. 
-F remove todas as regras, ou remove todas as regras referentes a 
um determinado chain. 
A inserir uma nova regra, mas no início da lista (CHAIN) de regras. 
-R'substitui uma regra já adicionada por outra. 
-Nt permite inserir uma nova Chain na tabela especificada. 
E Renorneia uma nova Chain criada. 
-X apaga uma Chain criada pelo administrador do firewall, 

**PARAMETROS DE AÇÕES NOS COMANDO IPTABLES**

Ações 
-p: especifica o protocolo aplicado a reg ast.p, udp 
icmp, etc) 
-i : especifica a interface de entrada a ser utilizada 
-o: especifica a interface de saída a ser utilizada 
-s: origem do pacote ao qual a regra deve ser aplicada 
-d: especifica o destino do pacote ao qual a regra deve 
ser aplicada 

Ações 
-j: define o alvo do pacote caso se encaixe e uma 
regra (ACCEPT, DROP, etc) 
—sport: define porta de origem (usado com tcpe dp) 
—dport: porta de destino Ex: -p tcp —dport 25 
! Usado quando se deseja aplicar exclusão a uma 
regra. 

**COMANDOS PARA LIMPAR TABLES NO IPTABLES**

**OBSERVAÇÃO IMPORTANTE:** Por padrão, as tables do iptables ficam alocadas na memória RAM, ou seja, caso o servidor seja reiniciado, essas informações são perdidas.

**COMO PREVENIR ESTA PERCA DE DADOS ALOCADOS NA MEMÓRIA RAM (VOLÁTIL):** Podemos reconstruir estes dados perdidos via scripts e adiciona-lo depois das TARGET NETWORK ou utilizarmos o pacote IPTABLES PERSISTENT

Limpando tabelas 
iptables 
iptables 
iptables 
iptables 
-t filter 
-t filter 
-t nat -F 
-t nat -X 
-F 
-x 

**COMANDOS PARA ALTERAR REGRAS DEFAULT DE POLICY**

**OBSERVAÇÃO IMPORTANTE:**

**1** - Por padrão, a regra da POLICY é que caso nenhuma regra se encaixe em nenhuma, então será entendido pelo FW (NETFILTER IPTABLES) automaticamente o ACCEPT para as CHAINs INPUT, FORWARD e OUTPUT. Isso quer dizer que quando recebermos quaisquer PDUs da rede WAN (REDE MUNDIAL/EXTERNA), automaticamente os pacotes irão para o PROCESSAMENTO LOCAL DA VM, conforme é o cenário dos gráficos que estamos utilizando como exemplo, isso é perigoso e pode ser uma falha de segurança, pois é MUITO PERMISSIVO, por isso é recomendado que esta regra na POLICY PADRÃO seja alterada em ambiente de produção, para não ser PERMISSIVA neste nível que é como padrão.

**2 -** Nunca executar este comando acessando a máquina via SSH (pelo PUTTY por exemplo), estes comando podem ser executados via ACESSO PELA CONSOLE DO HYPERVISOR, pois ao executar o primeiro comando como exemplo iptables -P INPUT DROP, isso significa que todas as entradas que não se encaixarem em nenhuma regra (CHAINs INPUT, FORWARD ou OUTPUT) passarão a serem encaminhadas para a serem consideradas como DROP e não mais ACCEPT como padrão, e isso vale não apenas para a CHAIN INPUT, mas também vale para as outras FORWARD e OUTPUT, e se o servidor que estamos acessando via SSH não tiver nenhuma regra de liberação criada, então a sua conexão SSH será DROPADA conforme a aplicação da regra default e não será mais permissiva igual quando estava configurado com o padrão ACCEPT, basta seus comandos serem executados, segue exemplo abaixo:

EXEMPLO:

Alterando as regras padrões de Policu 
No Linux para alterar estes valores para olicy. 
iptables -P INPUT DROP 
iptables -P FORWARD DROP 
iptables -P OUTPUT DROP 
Tomar cuidado ao executar este tipo de regra em 
m Servidor Virtual; 

**COMANDOS PARA PERMITIR/LIBERAR PROCESSOS GERADOS PELO PRÓPRIO SERVIDOR ATRAVÉS DE SUA INTERFACE DE REDE LOOPBACK**

**MOTIVO**: Geralmente este tipo de permissão é aplicado para permitirmos que processos gerados/executados dentro do devido servidor será permitido, ou seja, seja aceito (resultado do comando ACCEPT) pela interface de loopback da própria máquina.

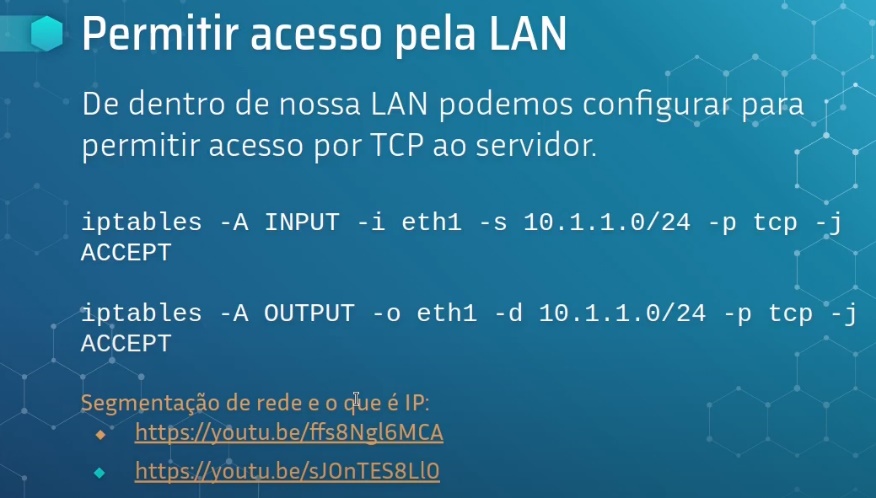
**EXEMPLO:** Segue comando abaixo para realizarmos estas liberações dos PDUs que utilizarão as CHAINs INPUT e OUTPUT.

Permitindo loopback 
Permitir que a comunicação provenient deloopba 
seja executado. 
iptables 
iptables 
-A INPUT -i 10 -j ACCEPT 
-A OUTPUT -0 10 -j ACCEPT 

**COMANDOS PARA PERMITIRMOS/LIBERARMOS ACESSOS DE TODA A NOSSA LAN PARA UM DETERMINADO SERVIDOR**

**MOTIVO:** Estes comandos geralmente são aplicados quando queremos que um determinador servidor seja liberado o acesso ao mesmo para todos que estiverem dentro de uma determinada rede LAN.

**EXEMPLO:** Neste exemplo abaixo, podemos perceber que estamos liberando acessos a um determinado servidor através da sua interface de gerencia com apontamento de nome "ETH01" e todo tipo de PDUs que chegarem utilizando o protocolo TCP (Como solicitações de coneões SSH por exemplo) será permitida a entrada (INPUT) e saída (OUTPUT) neste determinado servidor possuindo a interface de gerencia "ETH01"



**COMANDOS PARA PERMITIR ACESSO A UM DETERMINADO SERVIDOR ATRAVÉS DA PORTA 22 (SSH)**

**EXEMPLO:** INPUT para permitirmos entradas dos PDUs nesta devida interface de rede que esta gerenciando o IP de LAN do servidor, ou seja, a interface de gerencia (No exemplo estamos utilizando o ponteiro chamado de "ETH1"), e OUTPUT para permitirmos as saídas através desta mesma interface e também para termos retornos através da mesma.

**OBSERVAÇÃO IMPORTANTE: Se aplicarmos este comando somente na interface de rede que esta gerenciando o IP de LAN, então poderemos acessar o devido servidor via SSH somente dentro da rede LAN (OU SEJA, SOMENTE COM CONEXÃO QUE ESTEJA ALCANÇANDO DENTRO DA EMPRESA), para conseguirmos acessa-lo de qualquer rede de qualquer lugar, então deve ser executado estes mesmos comando, porém, alterando o apontamento que esta com o nome da interface de rede que gerencia o IP da rede LAN e devemos colocar o apontamento que esta com o nome da interface de rede que gerencia o IP da rede WAN.**

Permitir SSH no servidor 
Fazemos manutenção no servidor por ( ais. 
seguro), então vamos habilitar. 
iptables 
ACCEPT 
iptables 
CCEPT 
-A 
-A 
INPUT 
OUTPUT 
-i ethl 
-o ethl 
-p tcp 
-p tcp 
--dport 22 -j 
- -sport 22 -j 

**COMANDOS PARA DESSABILITAR O PROTOCOLO ICMP**

**MOTIVO:** Muito utilizado esta desabilitação nos roteadores de borda que estão gerenciando o GATEWAY da rede, ou seja, nestes devices que gerenciam a borda da rede, geralmente são aplicadas regras muito BRUTAS (NÃO PERMISIVAS), para melhora e garantia na camada de segurança da rede, evitando ataques simples de ICMP (UTILIZANDO PING) por exemplo que podem sobrecarregar o device e "derruba-lo".

**OBSERVAÇÃO IMPORTANTE: Não devemos utilizar estes comando em devices que gerenciam o roteamento interno da rede, geralmente chamamos ROTEADORES INTERNOS, pois estes gerenciam o "seguimento" da nossa determinada rede.**

**EXEMPLO:**

Desabilitar ICMP 
Uma operação importante é desabilitar [CMP para it 
ataques simples de ICMP. 
iptables 
iptab les 
-A INPUT 
-A OUTPUT 
-p icmp 
-p icmp 
--icmp-type any 
--icmp-type any 
-j DROP 
-j DROP 

**COMANDOS PARA REDIRECIONAMENTO DE PORTAS NO IPTABLES**

**MOTIVO:** Este tipo de liberação é geralmente utilizado quando temos uma determinada aplicação e precisamos permitir que a mesma seja acessada através da rede WAN (rede mundial) pelos usuários, porém, passando pelo roteador de borda e somente será acessível através do gateway que possuir as devidas regras nas CHAINs PREROUTING e FORWARD.

**EXEMPLO:**

Redirecionando uma porta 
Em um servidor de ponta que atua como firewal d 
rede, talvez seja importante redirecionar requisiçN 
na interface externa para uma máquina interna. 
iptables -A PREROUTING 
--dport -j DNAT 
iptables -A FORWARD -p 
-j ACCEPT 
-t nat 
tcp -d 
-i eth@ 
-p tcp 
--dport 

**COMANDOS PARA "NEGAR" PDUs QUE CHEGUEM UTILIZANDO PROTOCOLO UDP**

EXEMPLO:

Negando o protocolo UDP 
Se você possui certeza que o servidor não provê 
nenhum serviço por protocolo UDP, você pode neg r. 
iptables -t fi Iter -A INPUT -p udp -j DROP 

**GRÁFICO DEMONSTRANDO A SEQUENCIA DE EXECUÇÃO DAS CHAIN'S EM TABELAS DIFERENTES SENDO EXECUTADAS EM PARALELO**

**EXEMPLO:**

Fluxo final 
As cadeias organizadas no 
fluxo final pode ser visto 
ao lado. 
Incoming Packet 
Conneclton 
mangle 
PREROI_JTING 
iptables 
Processing 
Flowchart 
Locally. 
nerated 
packet 
ROW ng 
(state) 
OUTPUT 
OUTPUT 
PREROIJTING 
this 
INPUT 
security 
INPUT 
Local 
by Phil Hag«m 2019-04-30) 
SANS FOR572; Advanced Network Forensics 
32019 Lewes Consulting. LLC 
Derived i 
FORWARD 
FOHWARO 
FORWARD 
mangle 
POSTROI_JTING 
host 
Outgoing packet 

**OUTRA FORMA DE VISUALIZAÇÃO DE EXECUÇÃO DAS SEQUENCIAS**

1 
Other NF parts 
c. Other Networking 
basic set ot filtering 
opportunities at the 
neuork level 
bndge level 
Fluxo final 
Packet flow in Netfilter and General Networking 
Appllcat]on Layer 
Protocol Layer 
Network Layer 
unk Layer 
p r m tng 
out tot 6revity 
• •nar table only consulnd 
hr •NEW connections 
no cone to 
AC_ ET 
output 
o uzput 
—Ppmmutmq 
decson 