MONSTA

MONITORAMENTO DE REDES IP

UTILIZANDO O FIREWALLD

Índice

Este manual tem como objetivo demonstrar um funcionamento básico para liberar e bloquear portas no firewall do CentOS.

O FIREWALL DO CENTOS

O CentOS utiliza o Firewalld para gerenciar o filtro de pacotes baseado em iptables. Esse firewall possui algumas regras padrão e trabalha com o conceito de zonas onde a liberação de serviços é feito dentro delas.

A tabela abaixo demonstra como está configurado o firewall da rede após a instalação do sistema operacional:

Regra	Comportamento
INPUT	Liberado apenas o acesso a porta 22(TCP) e conexões do tipo RELATED,ESTABLISHED.
FORWARD	Aceita apenas conexões do tipo RELATED,ESTABLISHED.
OUTPUT	Não possui restrições.

Zonas

O firewalld gerencia um grupo de regras conhecido como zonas. As zonas definem o tipo de tráfego que será permitido baseado no nível de confiança da rede onde o seu servidor está conectado. Cada zona está atrelada a uma interface de rede existente no servidor.

O comando abaixo lista as zonas existentes:

```
firewall-cmd --get-zones
```

Abaixo são mostradas as zonas existentes no firewalld em ordem de nível de confiança:

Zona	Descrição
drop	Todos os pacotes são descartados.
block	Todos os pacotes são rejeitados.
public	Rede que você não conhece, pública.
external	Rede externa onde o servidor com o firewalld funciona como um gateway para a rede interna. É configurada com mascaramento para manter a privacidade da rede interna.
internal	É a parte interna da rede. Equipamentos nessa rede possuem um nível maior de confiança e serviços adicionais estão disponíveis.
dmz	São equipamentos isolados, ou seja, que não devem possuir acesso

	a sua rede. Apenas algumas conexões de entrada para esses equipamentos são permitidas.
work	Equipamentos de trabalho com liberação de serviços adicionais.
home	Equipamentos de casa. São dispositivos mais conhecidos e confiáveis e que possuem liberação para um pouco mais de serviços que a zona work.
trusted	Equipamentos de confiança. Praticamente todos os serviços estão disponíveis para os equipamentos nesta zona.

Listando as regras existentes

O comando abaixo lista todas as regras existentes no serviço firewalld:

```
firewall-cmd --list-all
```

Se desejar listar apenas as regras de uma determinada zona utilize a opção –zone:

```
firewall-cmd –zone=public --list-all
```

Liberando portas de entrada

Para modificar as regras de entrada do firewall do CentOS, utilizamos o comando firewall-cmd.

No exemplo abaixo é demonstrado como liberar as portas 80(TCP) e 443(TCP) para acesso da rede pública, de forma permanente, para um servidor HTTP através da linha de comando:

```
firewall-cmd --permanent --zone=public --add-port=80/tcp
firewall-cmd --permanent --zone=public –add-port=443/tcp
firewall-cmd --reload
```

onde:

--permanent	Adiciona a regra de forma permanente, ou seja, após reiniciar o filtro as regras permanecerão. Se for omitida esta opção as regras são válidas até o firewalld ser reiniciado.
--zone=public	É a zona pública não confiável. São endereços que você não conhece mas podem ser autorizados caso a caso.
--add-port=80/tcp	Informação da porta e protocolo que serão adicionados na zona public.
--reload	Recarrega as regras mantendo o estado das conexões.

Liberando um host ou uma rede

Abaixo é demonstrado como liberar o acesso total ao servidor para a rede cuja origem é 192.168.1.0/24:

```
firewall-cmd --permanent --zone=public –add-source=192.168.1.0/24
firewall-cmd --reload
```

--permanent	Adiciona a regra de forma permanente, ou seja, após reiniciar o filtro as regras permanecerão. Se for omitida esta opção as regras são válidas até o firewalld ser reiniciado.
--zone=public	É a zona pública não confiável. São endereços que você não conhece mas podem ser autorizados caso a caso.
--add-source=192.168.1.0/24	Informação da rede ou host que serão adicionados na zona public.
--reload	Recarrega as regras mantendo o estado das conexões.

Configurando o firewalld para agir como NAT

Para essa função faz-se necessário ter pelo menos 2 interfaces de rede no servidor, uma que faça a conexão com a rede pública e outra a rede interna.

No exemplo abaixo, a interface eth0 está conectada na rede pública e a eth1 na rede interna.

```
firewall-cmd --permanent –zone=internal –add-interface=eth1
firewall-cmd –permanent –zone=public -add-masquerade
firewall-cmd --reload
```

onde

--permanent	Adiciona a regra de forma permanente, ou seja, após reiniciar o filtro as regras permanecerão. Se for omitida esta opção as regras são válidas até o firewalld ser reiniciado.
--zone=public --zone=internal	Selecionamos a zona public para fazer o mascaramento e a internal para informar a rede interna.
--add-masquerado	Adiciona o mascaramento na zona selecionada.
--reload	Recarrega as regras mantendo o estado das conexões.

Configurando o firewalld para Port Forward

Para redirecionar portas da rede externa para um endereço da rede interna, utilize os comandos abaixo:

```
firewall-cmd --permanent --zone=public –add-forward-port=port=443:proto=tcp:toport=443:toaddr=192.168.1.11

firewall-cmd --reload
```

onde:

--permanent	**Adiciona a regra de forma permanente, ou seja, após reiniciar o filtro as regras permanecerão. Se for omitida esta opção as regras são válidas até o firewalld ser reiniciado.**
--zone=public	**É a zona pública não confiável. São endereços que você não conhece mas podem ser autorizados caso a caso.**
--add-forward-port=	**Ativa a regra para o port forward.**
port=443	**Porta de origem.**
proto=tcp	**Protocolo de origem.**
toport=443	**Porta de destino.**
toaddr=192.168.1.11	**IP de destino na rede interna.**
--reload	**Recarrega as regras mantendo o estado das conexões.**

APÊNDICE A | Contato

Monsta Tecnologia Ltda

Site: **http://www.monsta.com.br**
Downloads: **http://www.monsta.com.br/download.html**
E-mail: **suporte@monsta.com.br**


MONSTA
MONITORAMENTO DE REDES IP