第 10 章 Proxmox VE 防火墙

Proxmox VE 防火墙为你的 IT 基础设施提供了一种简单易用的防护手段。你既可以为集群内的所有主机设置防火墙策略，也可以为单个虚拟机和容器定义策略。防火墙宏，安全组，IP 集和别名等特性将大大简化策略配置管理。

尽管所有的防火墙策略都保存在集群文件系统，但基于 iptables 的防火墙服务在每个节点都是独立运行的，从而为虚拟机提供了完全隔离的防护。这套分布式部署的防火墙较传统防火墙提供了更高的带宽。

Proxmox VE 防火墙完全支持 IPv4 和 IPv6。IPv6 的支持是完全透明的，我们默认自动对两种协议通信同时进行过滤和检测。所以没有必要为 IPv6 专门建立并维护防火墙策略。

10.1 区域

Proxmox VE 防火墙将网络划分为不同区域

Host

流出/流入集群节点的网络通信

VM

流出/流入虚拟机的网络通信

对每个区域，你都可以对流入/流出流量定义防火墙策略。

10.2 配置文件

防火墙相关的配置文件全部保存在 Proxmox VE 集群文件系统中，所以能够自动在所有节点间同步复制，而防火墙管理服务 pve-firewall 将在防火墙策略改变后自动更新底层 iptables 策略。

你可以在 WebGUI 界面完成所有的防火墙配置（例如通过，数据中心->防火墙，或者通过，节点->防火墙），或者也可以直接用你喜欢的编辑器编辑配置文件。

防火墙配置文件按小节把键-值策略对组织起来。以#字符开头的行和空行被当作注释处理。每个小节开头第一行格式都是“[小节名]”。

10.2.1 集群级别的防火墙配置

作用域为整个集群的防火墙配置保存在

/etc/pve/firewall/cluster.fw

该配置文件由以下小节构成：

[OPTIONS]

该小节用于设置整个集群的防火墙配置项。

enable: <integer> (0 -N)

启用/禁用集群范围的防火墙。

policy_in: <ACCEPT | DROP | REJECT>

流入方向的防火墙策略。

policy_out: <ACCEPT | DROP | REJECT>

流出方向的防火墙策略。

[RULES]

该小节用于设置所有节点公共的防火墙策略。

[IPSET <name>]

整个集群范围内有效的 IP 集合定义。

[GROUP <name>]

整个集群范围内有效的组定义。

[ALIASES]

整个集群范围内有效的别名定义。

启用防火墙

防火墙默认是被完全禁用的。你可以按如下方式设置启用参数项：

[OPTIONS]

enable firewall (cluster wide setting, default is disabled)

enable: 1

☒ 重要

启用防火墙后，默认所有主机的通信都将被阻断。唯一例外是集群网络内的 WebGUI（端口 8006）和 ssh（端口 22）访问可以继续使用。

如果你希望远程管理 Proxmox VE 服务器，你需要首先配置防火墙策略，允许远程 IP 访问 WebGUI（端口 8006）。根据需要，你还可以开通 ssh（端口 22）或 SPICE（端口 3128）的访问权限。

➢ 注意

请在启用防火墙前先打开到 Proxmox VE 服务器的一个 SSH 连接，这样即使策略配置有误，也还可以通过该连接访问服务器。

为简化配置，你可以创建一个名为“管理地址”的 IPSet，并把所有的远程管理终端 IP 地址添加进去。这样就可以创建策略允许所有的远程地址访问 WebGUI。

10.2.2 主机级别的防火墙配置

主机级别的防火墙配置保存在

/etc/pve/nodes/<nodename>/host.fw

该文件中的配置可以覆盖 cluster.fw 中的配置。你可以提升报警日志级别，设置 netfilter 相关参数。该配置文件由以下小节构成：

[OPTIONS]

该小节用于设置当前主机的防火墙配置项。

enable: <boolean>

启用/禁用主机防火墙策略。

log_level_in: <alert | crit | debug | emerg | err | info | nolog | notice | warning>

流入方向的防火墙日志级别。

log_level_out: <alert | crit | debug | emerg | err | info | nolog | notice | warning>

流出方向的防火墙日志级别。

ndp: <boolean>

启用 NDP。

nf_conntrack_max: <integer> (32768 -N)

最大的跟踪连接数量。

nf_conntrack_tcp_timeout_established: <integer> (7875 -N)

反向连接建立超时时间。

nosmurfs: <boolean>

启用 SMURFS 过滤器。

smurf_log_level: <alert | crit | debug | emerg | err | info | nolog | notice | warning>

SMURFS 过滤器日志级别。

tcp_flags_log_level: <alert | crit | debug | emerg | err | info | nolog | notice | warning>

非法 TCP 标志过滤器日志级别。

tcpflags: <boolean>

启用非法 TCP 标志组合过滤器。

[RULES]

该小节用于设置当前主机的防火墙策略。

10.2.3 虚拟机和容器级别的防火墙配置

虚拟机和容器级别的防火墙配置保存在

/etc/pve/firewall/<VMID>.fw

其内容由以下数据构成：

[OPTIONS]

该小节用于设置当前虚拟机或容器的防火墙配置项。

dhcp: <boolean>

启用 DHCP。

enable: <boolean>

启用/禁用防火墙策略。

ipfilter: <boolean>

启用默认 IP 地址过滤器。相当于为每个网卡接口增加一个空白的 ipfilter-net<id>地址集合。该 IP 地址集合隐式包含了一些默认控制，例如限制 IPv6 链路本地地址为网卡 MAC 生成的地址。对于容器，配置的 IP 地址将被隐式添加进去。

log_level_in: <alert | crit | debug | emerg | err | info | nolog | notice | warning>

流入方向的防火墙日志级别。

log_level_out: <alert | crit | debug | emerg | err | info | nolog | notice | warning>

流出方向的防火墙日志级别。

macfilter: <boolean>

启用/禁用 MAC 地址过滤器。

ndp: <boolean>

启用 NDP。

policy_in: <ACCEPT | DROP | REJECT>

流入方向的防火墙策略。

policy_out: <ACCEPT | DROP | REJECT>

流出方向的防火墙策略。

radv: <boolean>

允许发出路由通知。

[RULES]

该小节用于设置当前虚拟机或容器的防火墙策略。

[IPSET <name>]

IP 集合定义。

[ALIASES]

IP 地址别名定义。

启用虚拟机或容器上的防火墙

每个虚拟网卡设备都有一个防火墙启用标识。你可以控制每个网卡的防火墙启用状态。在设置启用虚拟机防火墙后，你必须设置网卡上的防火墙启用标识才可以真正启用防火墙。

防火墙需要网络设备标识配置的配合，在启用网卡的防火墙标识后你必须重启虚拟机或容器才可以。

10.3 防火墙策略

防火墙策略定义了网络通信方向（IN 或 OUT）和处理动作（ACCEPT，DENY，REJECT）。你也可以定义一个宏来预定义的策略和配置项，还可以在策略前插入字符“|”来禁用策略。

防火墙策略语法

[RULES]

DIRECTION ACTION [OPTIONS]

|DIRECTION ACTION [OPTIONS] # disabled rule

DIRECTION MACRO(ACTION) [OPTIONS] # use predefined macro

如下参数可用于完善策略匹配规则。

-dest <string>

设置数据包目的地址。可以设置为一个 IP 地址，一个 IP 集合（IP 集合名称）或 IP 别名。也可以设置为一个 IP 地址范围如 20.34.101.207-201.3.9.99，或一组 IP 地址和网络地址列表（使用逗号分隔开）。注意不要在列表中同时混合配置 IPv4 地址和 IPv6 地址。

-dport <string>

设置 TCP/UDP 目的端口。可像/etc/services 一样设置为服务名称或端口号（0-65535），也可按照“\d+:\d+”格式设置为端口范围，如 80:85，也可以设置为由逗号分隔开的端口和端口范围列表。

-iface <string>

设置网卡名称。可以设置为网络配置中的虚拟机和容器网卡名称（net\d+）。主机级别的防火墙策略可使用任意字符串。

-proto <string>

设置 IP 协议。你可以设置为协议名称（tcp/udp）或/etc/protocols 中定义的协议编号。

-source <string>

设置数据包源地址。可以设置为一个 IP 地址，一个 IP 集合（IP 集合名称）或 IP 别名。也可以设置为一个 IP 地址范围如 20.34.101.207-201.3.9.99，或一组 IP 地址和网络地址列表（使用逗号分隔开）。注意不要在列表中同时混合配置 IPv4 地址和 IPv6 地址。

-sport <string>

设置 TCP/UDP 目的端口。可像/etc/services 一样设置为服务名称或端口号（0-65535），也可按照“\d+:\d+”格式设置为端口范围，如 80:85，也可以设置为由逗号分隔开的端口和端口范围列表。

以下是一些防火墙策略示例

[RULES]

IN SSH(ACCEPT) -i net0

IN SSH(ACCEPT) -i net0 # a comment

IN SSH(ACCEPT) -i net0 -source 192.168.2.192 # only allow SSH from 192.168.2.192

IN SSH(ACCEPT) -i net0 -source 10.0.0.1-10.0.0.10 # accept SSH for ip range

IN SSH(ACCEPT) -i net0 -source 10.0.0.1,10.0.0.2,10.0.0.3 #accept ssh for ip list

IN SSH(ACCEPT) -i net0 -source +mynetgroup # accept ssh for ipset mynetgroup

IN SSH(ACCEPT) -i net0 -source myserveralias #accept ssh for alias myserveralias

|IN SSH(ACCEPT) -i net0 # disabled rule

IN DROP # drop all incoming packages

OUT ACCEPT # accept all outgoing packages

10.4 安全组

安全组是一个防火墙策略的集合。安全组属于集群级别的防火墙对象，可用于所有的虚拟机防火墙策略。例如，你可以定义一个名为“webserver”的安全组，以开放 http 和 https 服务端口。

/etc/pve/firewall/cluster.fw

[group webserver]

IN ACCEPT -p tcp -dport 80

IN ACCEPT -p tcp -dport 443

之后，就可以将该安全组添加到虚拟机防火墙策略中

/etc/pve/firewall/<VMID>.fw

[RULES]

GROUP webserver

10.5 IP 地址别名

IP 地址别名能够让你为 IP 地址定义一个名称。之后可以通过名称来引用 IP 地址：

- 在 IP 集合内部
- 在防火墙的 source 和 dest 属性中

10.5.1 标准 IP 地址别名 local_network

该别名是系统自动定义的。可以使用如下命令查看分配的地址别名：

pve-firewall localnet

local hostname: example

local IP address: 192.168.2.100

network auto detect: 192.168.0.0/20

using detected local_network: 192.168.0.0/

防火墙将利用该别名自动生成策略，开放 Proxmox VE 集群对网络的访问权限（corosync，API，SSH）。

用户可以修改 cluster.fw 中定义的别名。如果你在公共网络上有一台独立的 Proxmox VE 主机，最好明确指定本地 IP 地址的别名

/etc/pve/firewall/cluster.fw

[ALIASES]

local_network 1.2.3.4 # use the single ip address

10.6 IP 地址集合

IP 地址集合可用来定义一组网络和主机。你可以在防火墙策略的 source 和 dest 属性中用“+名称”的格式引用 IP 地址集合。

如下策略将允许来自名为 management 的 IP 地址集合的 HTTP 访问

IN HTTP(ACCEPT) -source +management

10.6.1 标准 IP 地址集合 management

标准 IP 地址集合 management 仅限主机级别防火墙使用（不支持在虚拟机级别防火墙使用）。系统对该 IP 地址集合开放日常管理所需的网络访问权限（PVE GUI，VNC，SPICE，SSH）。

本地集群网络地址将被自动添加到该 IP 地址集合（别名 cluster_network），以便于集群内的主机相互通讯（multicast，ssh 等）。

/etc/pve/firewall/cluster.fw

[IPSET management]

192.168.2.10

192.168.2.10/24

10.6.2 标准 IP 地址集合 blacklist

标准 IP 地址集合 blacklist 中的地址对任何主机或虚拟机发起的访问请求都将被丢弃。

/etc/pve/firewall/cluster.fw

[IPSET blacklist]

77.240.159.182

213.87.123.0/24

10.6.3 标准 IP 地址集合 ipfilter-net*

该类过滤器专门为虚拟机的虚拟网卡定义，主要用于防止 IP 地址欺骗。为虚拟网卡定义该 IP 地址集合后，从网卡发出的任何与 ipfilter 集合中 IP 地址不符的数据包都将被丢弃。

对于配置指定 IP 地址的容器，如果定义了该 IP 地址集合（或通过在虚拟机防火墙 options 选项卡勾选通用 IP Filter 激活），容器 IP 地址会被自动加入该 IP 地址集合。

/etc/pve/firewall/<VMID>.fw

[IPSET ipfilter-net0] # only allow specified IPs on net0

192.168.2.10

10.7 服务及管理命令

防火墙在每个节点都运行了两个服务进程：

- pvefw-logger: NFLOG 服务进程（替换 ulogd）。
- pve-firewall: 更新 iptables 策略。

还提供了一个管理命令 pve-firewall，可用于启停防火墙服务：

pve-firewall start

pve-firewall stop

或查看防火墙服务状态：

pve-firewall status

如上命令将读取并编译所有的防火墙策略，如果发现配置错误，将会自动发出告警。

如果你需要查看生成的 iptables 策略，可以运行如下命令：

iptables-save

10.8 提示和窍门

10.8.1 如何开放 FTP

FTP 是一个古老的协议，使用固定端口 21 和其他一些动态端口。所以，你需要配置一条开放端口 21 的策略，并加载 ip_contrack_ftp 内核模块。加载命令如下：

modprobe ip_conntrack_ftp

进一步还需要在/etc/modules 中添加 ip_contrack_ftp（以便系统重启后自动加载）。

10.8.2 集成 Suricata IPS

你也可以集成使用 Suricata IPS（入侵防御系统）。

只有通过防火墙策略校验的数据包才会发送给 IPS。

被防火墙拒绝/丢弃的数据包不会发送给 IPS。

首先需要在 Proxmox VE 主机安装 suricata：

apt-get install suricata

modprobe nfnetlink_queue

不要忘记在/etc/modules 中添加 nfnetlink_queue，以便系统下次重启后自动加载。

然后可以在指定虚拟机的防火墙上激活 IPS：

/etc/pve/firewall/<VMID>.fw

[OPTIONS]

ips: 1

ips_queues: 0

ips_queues 配置项将为虚拟机绑定一个指定的 cpu 队列。

可用队列定义在如下配置文件中

/etc/default/suricata

NFQUEUE=0

10.9 IPv6 注意事项

防火墙中有一些专用于 IPv6 的配置项。首先，IPv6 不再使用 ARP 协议，取而代之的是 NDP（Neighbor Discovery Protocol），而 NDP 工作在 IP 层，需要配置 IP 地址后才可以使用。为此，系统用虚拟网卡 MAC 地址生成了一个 IPv6 链路本地地址。在主机级别防火墙和虚拟机级别的防火墙上，NDP 配置项默认都是启用的，以便邻居发现（NDP）数据包的收发。

除了邻居发现以外，NDP 也被用于完成其他任务，比如自动配置和路由通知。

虚拟机默认可以发送路由查询消息（以获取路由）和接收路由通知数据包。这允许虚拟机使用无状态的自动配置。但是，虚拟机默认不能向外发送宣称自己是路由器的路由通知数据包，除非设置“允许路由通知”（radv:1）配置项。

为便于 NDP 使用链路本地地址通信，防火墙提供了一个“IP 过滤器”（ipfilter:1）配置项。启用该配置的效果类似于在虚拟机网卡上启用 IP 地址集合 ipfilter-net*，然后把链路本地地址添加进去一样（详情可查看标准 IP 地址集合 ipfilter-net*一节）。

10.10 Proxmox VE 端口列表

- Web 界面：8006

- VNC 控制台：5900-5999
- SPICE proxy：3128
- sshd（用于集群管理）：22
- rpcbind：111
- corosync 多播（集群通信使用）：5404, 5405 UDP