配置 IPS 防止 SSH 暴力破解

版本	1.0
时间	2015 年 9 月
支持的版本	FortiOS v5.2 及更高版本
审核	已通过 hcxie
反馈	support_cn@fortinet.com

目录

功能简介.....3
步骤一：配置 IPS 防止 SSH 暴力破解.....3
步骤二：在策略中启用 IPS 功能.....4
步骤三：验证.....4

功能简介

FortiGate 防火墙可以通过 IPS 功能（Rate Based Signatures）防止 SSH 暴力破解，它通过限制源 IP 每秒内连接的次数实现该功能。IPS 协议解码器可以识别 SSH 协议，因此不管 SSH 是否使用标准 TCP 22 端口或其他 TCP 端口 IPS 都可以识别。

SSH 应用只是 IPS 防止暴力破解的一个应用，其他应用列表可以在 IPS 部分查看。

步骤一：配置 IPS 防止 SSH 暴力破解

在安全配置文件---->入侵防御菜单中编辑 default 条目，

在 Rate Based Signatures 下找到 SSH.Connection.Brute.Force 条目，其中

阈值表示符合条件的次数

Duration(每秒)表示规定的时间

本例的触发条件是 1 秒内 ssh 连接数大于 1 次，该条件需要根据用户实际情况具体配置，

对应的 CLI 是

```
config ips sensor
    edit "default"
        config entries
            edit 2
                set rule 35662
                set status enable
                set action block
                set quarantine attacker
                set quarantine-expiry 2
                set rate-count 1
                set rate-duration 1
```

```
                set rate-track src-ip
            next
        next
end
```

步骤二：在策略中启用 IPS 功能

在相应的策略中启用 IPS 功能，对应的 CLI 是

```
config firewall policy
    edit 5
        set srcintf "wan1"
        set dstintf "lan"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ips-sensor "default"
        set profile-protocol-options "default"
        set ssl-ssh-profile "certificate-inspection"
        set nat enable
    next
end
```

步骤三：验证

在日志与报告---->安全日志---->入侵检测菜单中查看相应日志

2	10:46:23		172.168.1.168	tcp		dropped		SSH.Connection.Brute.Force

1 / 1 [合计: 4]

#	2	Log ID	16384
严重性		事件序列号	2053796063
事件类型	signature	动作	dropped
协议	tcp	协议数	6
参考	http://www.fortinet.com/ids/VID35662	威胁分数	30
威胁等级	high	子类型	ips
序号	467947	攻击ID	35662
攻击名称	SSH.Connection.Brute.Force	方向	outgoing
日期/时间	2015/9/7 上午10:46:23	日期/时间	10:46:23
服务	SSH	消息	remote_access: SSH.Connection.Brute.Force,
源	172.168.1.168	源接口	wan1
源端口	61751	目标接口	lan
目的	192.168.118.2	目的端口	22
级别		虚拟域	root
配置名称	default		

注，下面的日志为使用非标准 SSH 端口产生的记录

#	@	日期/时间	严重性	源	协议	用户	动作	计数	攻击名称
1		10:59:57		172.168.1.168	tcp		dropped		SSH.Connection.Brute.Force

1 / 1 [合计: 4]

#	1	Log ID	16384
严重性		事件序列号	2053796064
事件类型	signature	动作	dropped
协议	tcp	协议数	6
参考	http://www.fortinet.com/ids/VID35662	威胁分数	30
威胁等级	high	子类型	ips
序号	469143	攻击ID	35662
攻击名称	SSH.Connection.Brute.Force	方向	outgoing
日期/时间	2015/9/7 上午10:59:57	日期/时间	10:59:57
服务	tcp/2222	消息	remote_access: SSH.Connection.Brute.Force,
源	172.168.1.168	源接口	wan1
源端口	61882	目标接口	lan
目的	192.168.118.162	目的端口	2222
级别		虚拟域	root
配置名称	default		