Asterisk ?????????? 2010-12-02

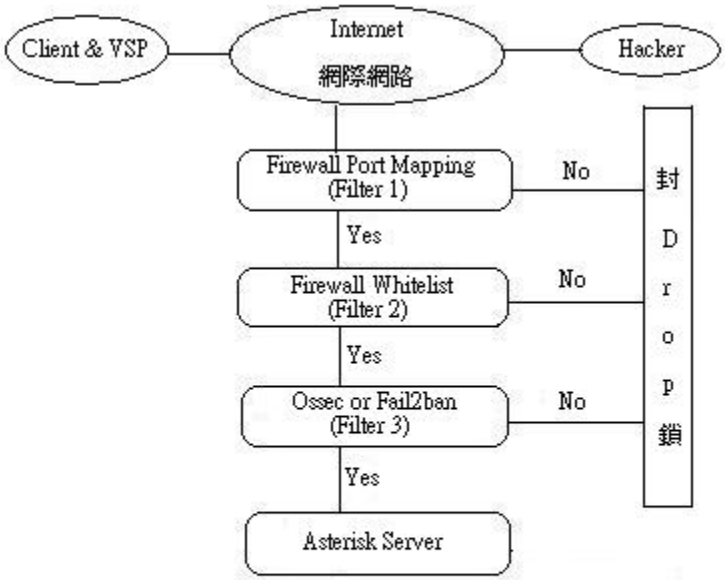
????

?? Asterisk ????????????????????????????????? Asterisk ?????????? Asterisk ??????????????????????????
????????????????????????????

?????? Asterisk ????????? Asterisk ?????????? Asterisk ????????????????????????????

????? PBX in a Flash ??

Asterisk ????????



??Asterisk ?????????

1.Firewall Port Mapping?

- ????????????????????????????
- ????????? Router ????? IP ???????????? IP ???? Firewall Whitelist????
- Asterisk ????????? IAX ??? 4569 ? SIP ??? 5060 ? SIP-RTP? 10000-20000?
- ??? Asterisk ?? bindport ???? 4569 ? 5060 ?????????????????????

2.Firewall Whitelist??? The SunshineNetworks Knock ?????

- ??
- ?????????????? IPtables ???

- ????? Client ?? Voip Service Provider ??? IP?
- ??????????????????????????????
- PIAF ??????? Firewall Blacklist ??????????????????
- ???????? IP ? Client ???? Client ????? IP ??????? The SunshineNetworks Knock?

http://www.pbxinaflash.com/forum/sho...ead.php?t=8735

3.The SunshineNetworks Knock??? Firewall Whitelist ?????

- ????????????????? The SunshineNetworks Knock ?????????????????
- ???? The SunshineNetworks Knock ??????? IPtables ???
- The SunshineNetworks Knock ?????? Voip ?? Display Name ???????????????
- ????????????? The SunshineNetworks Knock ?????????????????????
- ????????? IP ? Client ???????? Firewall Whitelist ??????????
- ?? Voip ?? Display Name ???????????????? Internet ?????????? PIAF ???

http://www.sunshinenetworks.com.au/h...rks-knock.html

4.Ossec or Fail2ban?

- ????? Firewall Whitekist ?? The SunshineNetworks Knock?????????? Asterisk ??????????????????
- Asterisk ????????????????????? IP??????
- Ossec ? Fail2ban ????????????? IP ?????????
- Ossec ? Fail2ban ? Asterisk ??????????????????

[OSSLab]OSSEC & FreePBX
[OSSLab]fail2ban for Asterisk
http://www.voip-info.org/wiki/view/F...9+And+Asterisk

5.Asterisk Server?

- Asterisk ??????????????????????????? IP ???
- ? Client ????? IP ??? FreePBX -> Extensions ? permit ??????0.0.0.0/0.0.0.0???????????????? The SunshineNetworksKnock?Ossec ? Fail2ban ???????
- ?? Asterisk ???????????[OSSLab] ?? Asterisk ?????security??

??IPTables ???

1.?? IPTables?

Code?

apt-get install iptables

IPtables ????????????????????????????

Code?

iptables -nL

???????

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

2.????? IPTables?

?????? iptables_script ???**?**

Code?

cd /root
nano -w iptables_script

??????????????

```
#!/bin/bash
# ??????????????????????????????????????

# ???? IP ????? TCP/UDP ?????
LANA="127.0.0.0/8"
LANB="10.0.0.0/8"
LANC="172.16.0.0/12"
LAND="192.168.0.0/16"
TCPPORTS="22,80,139,443,445,4445,5038,9001,9022,9080,10000"
UPDPORTS="53,69,123,137:138,1514,4520,4569,5060,10000:20000"

# ??????? (filter) ??????? INPUT ???? DROP ??????????????????
iptables -F
iptables -X
iptables -Z

# ????????? (policy)????????????????????????????? Policy ?????
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT

# ????????????????? Asterisk ?????
```

```
iptables -A INPUT ! -i eth0 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --tcp-flags ACK ACK -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -m state --state RELATED -j ACCEPT
iptables -A INPUT -p udp -m udp --dport 1024:65535 --sport 53 -j ACCEPT
iptables -A INPUT -p icmp -m icmp --icmp-type echo-reply -j ACCEPT
iptables -A INPUT -p icmp -m icmp --icmp-type destination-unreachable -j ACCEPT
iptables -A INPUT -p icmp -m icmp --icmp-type source-quench -j ACCEPT
iptables -A INPUT -p icmp -m icmp --icmp-type time-exceeded -j ACCEPT
iptables -A INPUT -p icmp -m icmp --icmp-type parameter-problem -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dports $TCPPORTS -s $LANA -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dports $TCPPORTS -s $LANB -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dports $TCPPORTS -s $LANC -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dports $TCPPORTS -s $LAND -j ACCEPT
iptables -A INPUT -p udp -m multiport --dports $UPDPORTS -s $LANA -j ACCEPT
iptables -A INPUT -p udp -m multiport --dports $UPDPORTS -s $LANB -j ACCEPT
iptables -A INPUT -p udp -m multiport --dports $UPDPORTS -s $LANC -j ACCEPT
iptables -A INPUT -p udp -m multiport --dports $UPDPORTS -s $LAND -j ACCEPT

# ????????
iptables-save > /etc/iptables.up.rules
```

?????????????? IPTables?

Code?

```
chmod +x iptables_script
./iptables_script
```

3.??? IPTables ??? Firewall Whitelist ????????

- ?? whitelist ??? whitelist ??????????? IP ?? 4569 ? 5060 ??????? Google Voice?????????????????????
- ???????????????

Code?

```
iptables -A INPUT -p udp -m udp --dport 10000:20000 -j ACCEPT
iptables -N whitelist
iptables -A INPUT -p udp -m multiport --dports 4569,5060 -j whitelist
iptables -A whitelist -s 66.54.140.46 -j ACCEPT
iptables -A whitelist -s 66.54.140.47 -j ACCEPT
iptables -A whitelist -s 210.202.244.130 -j ACCEPT
iptables -A whitelist -s 210.244.221.240 -j ACCEPT
iptables-save > /etc/iptables.up.rules
```

???? /etc/iptables.up.rules ???????????????? IPTables ?????

```
# Generated by iptables-save v1.4.8 on Wed Dec 15 18:12:29 2010
*nat
:PREROUTING ACCEPT [101:50660]
:POSTROUTING ACCEPT [104:17692]
:OUTPUT ACCEPT [104:17692]
COMMIT
# Completed on Wed Dec 15 18:12:29 2010
# Generated by iptables-save v1.4.8 on Wed Dec 15 18:12:29 2010
*mangle
:PREROUTING ACCEPT [1294:303173]
:INPUT ACCEPT [1294:303173]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [1194:333833]
:POSTROUTING ACCEPT [1236:339950]
COMMIT
# Completed on Wed Dec 15 18:12:29 2010
# Generated by iptables-save v1.4.8 on Wed Dec 15 18:12:29 2010
*filter
:INPUT DROP [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [185:88716]
:whitelist - [0:0]
-A INPUT ! -i eth0 -j ACCEPT
-A INPUT -p tcp -m tcp --tcp-flags ACK ACK -j ACCEPT
-A INPUT -m state --state ESTABLISHED -j ACCEPT
-A INPUT -m state --state RELATED -j ACCEPT
-A INPUT -p udp -m udp --sport 53 --dport 1024:65535 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 4 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 12 -j ACCEPT
-A INPUT -s 127.0.0.0/8 -p tcp -m multiport --dports 22,80,139,443,445,4445,5038,9001,9022,9080,10000 -j
ACCEPT
-A INPUT -s 10.0.0.0/8 -p tcp -m multiport --dports 22,80,139,443,445,4445,5038,9001,9022,9080,10000 -j
ACCEPT
-A INPUT -s 172.16.0.0/12 -p tcp -m multiport --dports 22,80,139,443,445,4445,5038,9001,9022,9080,10000 -j
ACCEPT
-A INPUT -s 192.168.0.0/16 -p tcp -m multiport --dports 22,80,139,443,445,4445,5038,9001,9022,9080,10000
-j ACCEPT
-A INPUT -s 127.0.0.0/8 -p udp -m multiport --dports 53,69,123,137:138,1514,4520,4569,5060,10000:20000 -j
ACCEPT
-A INPUT -s 10.0.0.0/8 -p udp -m multiport --dports 53,69,123,137:138,1514,4520,4569,5060,10000:20000 -j
ACCEPT
-A INPUT -s 172.16.0.0/12 -p udp -m multiport --dports 53,69,123,137:138,1514,4520,4569,5060,10000:20000
-j ACCEPT
-A INPUT -s 192.168.0.0/16 -p udp -m multiport --dports
53,69,123,137:138,1514,4520,4569,5060,10000:20000 -j ACCEPT
-A INPUT -p udp -m udp --dport 10000:20000 -j ACCEPT
-A INPUT -p udp -m multiport --dports 4569,5060 -j whitelist
```

-A whitelist -s 66.54.140.46/32 -j ACCEPT
-A whitelist -s 66.54.140.47/32 -j ACCEPT
-A whitelist -s 210.202.244.130/32 -j ACCEPT
-A whitelist -s 210.244.221.240/32 -j ACCEPT
COMMIT
Completed on Wed Dec 15 18:12:29 2010

4.??? IPTables ??? The SunshineNetworks Knock ????????

- ?????????? "mysecretpass" ???????????????? SIP message ?? "SIP-Header-Request" ? "Info-SIP-Message"????????????? Voip ??? Display Name ????????
- ??????? "mysecretpass" ????????????? "mysecretpass" ????????? "mysecretpass" ????? Google Voice?????????????????????
- ????????????????

Code?

iptables -A INPUT -p udp -m udp -s 66.54.140.46/32 --dport 4569 -j ACCEPT
iptables -A INPUT -p udp -m udp -s 66.54.140.47/32 --dport 4569 -j ACCEPT
iptables -A INPUT -p udp -m udp --dport 10000:20000 -j ACCEPT
iptables -N door
iptables -I door 1 -p udp --dport 5060 -m string --string "mysecretpass" --algo bm -m recent --set --name portisnowopen
iptables -A INPUT -p udp --dport 5060 --source 210.202.244.130/32 -j ACCEPT
iptables -A INPUT -p udp --dport 5060 --source 210.244.221.240/32 -j ACCEPT
iptables -A INPUT -p udp --dport 5060 -m recent --rcheck --seconds 4000 --name portisnowopen -j ACCEPT
iptables -A INPUT -p udp --dport 5060 -j door
iptables -A INPUT -p udp --dport 5060 -j DROP
iptables-save > /etc/iptables.up.rules

???? /etc/iptables.up.rules ???????????????? IPTables ?????

Generated by iptables-save v1.4.8 on Fri Dec 17 14:15:15 2010
*nat
:PREROUTING ACCEPT [67:8613]
:POSTROUTING ACCEPT [3076:226290]
:OUTPUT ACCEPT [3076:226290]
COMMIT
Completed on Fri Dec 17 14:15:15 2010
Generated by iptables-save v1.4.8 on Fri Dec 17 14:15:15 2010
*mangle
:PREROUTING ACCEPT [41440:9679999]
:INPUT ACCEPT [41440:9679999]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [38953:11437844]
:POSTROUTING ACCEPT [39131:11476397]
COMMIT

```
# Completed on Fri Dec 17 14:15:15 2010
# Generated by iptables-save v1.4.8 on Fri Dec 17 14:15:15 2010
*filter
:INPUT DROP [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [58:52600]
:door - [0:0]
-A INPUT ! -i eth0 -j ACCEPT
-A INPUT -p tcp -m tcp --tcp-flags ACK ACK -j ACCEPT
-A INPUT -m state --state ESTABLISHED -j ACCEPT
-A INPUT -m state --state RELATED -j ACCEPT
-A INPUT -p udp -m udp --sport 53 --dport 1024:65535 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 4 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 12 -j ACCEPT
-A INPUT -s 127.0.0.0/8 -p tcp -m multiport --dports 22,80,139,443,445,4445,5038,9001,9022,9080,10000 -j
ACCEPT
-A INPUT -s 10.0.0.0/8 -p tcp -m multiport --dports 22,80,139,443,445,4445,5038,9001,9022,9080,10000 -j
ACCEPT
-A INPUT -s 172.16.0.0/12 -p tcp -m multiport --dports 22,80,139,443,445,4445,5038,9001,9022,9080,10000 -j
ACCEPT
-A INPUT -s 192.168.0.0/16 -p tcp -m multiport --dports 22,80,139,443,445,4445,5038,9001,9022,9080,10000
-j ACCEPT
-A INPUT -s 127.0.0.0/8 -p udp -m multiport --dports 53,69,123,137:138,1514,4520,4569,5060,10000:20000 -j
ACCEPT
-A INPUT -s 10.0.0.0/8 -p udp -m multiport --dports 53,69,123,137:138,1514,4520,4569,5060,10000:20000 -j
ACCEPT
-A INPUT -s 172.16.0.0/12 -p udp -m multiport --dports 53,69,123,137:138,1514,4520,4569,5060,10000:20000
-j ACCEPT
-A INPUT -s 192.168.0.0/16 -p udp -m multiport --dports
53,69,123,137:138,1514,4520,4569,5060,10000:20000 -j ACCEPT
-A INPUT -s 66.54.140.46/32 -p udp -m udp --dport 4569 -j ACCEPT
-A INPUT -s 66.54.140.47/32 -p udp -m udp --dport 4569 -j ACCEPT
-A INPUT -p udp -m udp --dport 10000:20000 -j ACCEPT
-A INPUT -s 210.202.244.130/32 -p udp -m udp --dport 5060 -j ACCEPT
-A INPUT -s 210.244.221.240/32 -p udp -m udp --dport 5060 -j ACCEPT
-A INPUT -p udp -m udp --dport 5060 -m recent --rcheck --seconds 4000 --name portisnowopen --rsource -j
ACCEPT
-A INPUT -p udp -m udp --dport 5060 -j door
-A INPUT -p udp -m udp --dport 5060 -j DROP
-A door -p udp -m udp --dport 5060 -m string --string "mysecretpass" --algo bm --to 65535 -m recent --set
--name portisnowopen --rsource
COMMIT
# Completed on Fri Dec 17 14:15:15 2010
```

??Ossec or Fail2ban ???

???

[OSSLab]OSSEC & FreePBX

[OSSLab]fail2ban for Asterisk

http://www.voip-info.org/wiki/view/F...9+And+Asterisk

???????

http://linux.vbird.org/linux_server/...e_firewall.php

http://www.pbxinaflash.com/forum/sho...?t=7560&page=2

http://www.pbxinaflash.com/forum/sho...ead.php?t=8735

http://www.sunshinenetworks.com.au/h...rks-knock.html

http://nerdvittles.com/?p=709

http://www.voip-info.org/wiki/view/F...9+And+Asterisk