H??ng d?n cài ??t và c?u hình csf trên centos 7(B?o v? VPS)

admin Sun, Apr 14, 2019 Cài Đặt Cơ Bản & Hướng Dẫn 0 1921

CSF LÀ GÌ ?

CSF (ConfigServer & Firewall) là 1 gói ?ng d?ng ho?t ??ng trên Linux nh? 1 Firewall ???c phát hành mi?n phí ?? t?ng tính b?o m?t cho server (VPS và Dedicated). CSF ho?t ??ng d?a trên iptables và ti?n trình ldf ?? quyét các file log ?? phát hi?n các d?u hi?u t?n công b?t th??ng.

CSF s? giúp server c?a b?n:
- Ch?ng DoS các lo?i
- Ch?ng Scan Port
- ??a ra các l?i khuyên v? vi?c c?u hình server (VD: Nên nâng c?p MySQL lên b?n m?i h?n)
- Ch?ng BruteForce Attack vào ftp server, web server, mail server,directadmin,cPanel...
- Ch?ng Syn Flood
- Ch?ng Ping Flood
- Cho phép ng?n ch?n truy c?p t? 1 qu?c gia nào ?ó b?ng cách ch? ??nh Country Code chu?n ISO
- H? tr? IPv6 và IPv4
- CHo phép khóa IP t?m th?i và v?nh vi?n ? t?ng m?ng (An toàn h?n ? t?ng ?ng d?ng) nên webserver ko ph?i m?t nh?c x? lý yêu c?u t? các IP b? c?m n?a
- Cho phép b?n chuy?n h??ng yêu c?u t? các IP b? khóa sang 1 file html ?? thông báo cho ng??i dùng bi?t IP c?a h? b? khóa
-Và r?t nhi?u tính n?ng khác, các b?n t? tìm hi?u thêm

B??c 1: Cài ??t các gói c?n thi?t ?? ch?y csf

```
# yum install wget vim perl-libwww-perl.noarch perl-Time-HiRes -y
```

B??c 2: T?i v? và cài ??t csf

T?o 1 th? m?c ?? ch?a file cài ??t

```
# mkdir /download
# cd /download/
```

Download file cài ??t c?a csf

```
# wget https://download.configserver.com/csf.tgz
```

Doawload xong ta gi?i nén file v?a t?i v?

```
# tar -xvf csf.tgz
```

Ta dùng l?nh sh ?? cài ??t

```
# cd csf
# sh install.sh
```

N?u xu?t hi?n các dòng sau là b?n ?ã cài ??t thành công

Adding current SSH session IP address to the csf whitelist in csf.allow:
Adding 14.160.38.66 to csf.allow only while in TESTING mode (not iptables ACCEPT)
WARNING TESTING mode is enabled - do not forget to disable it in the configuration
‘lfd.service’ -> ‘/usr/lib/systemd/system/lfd.service’
‘csf.service’ -> ‘/usr/lib/systemd/system/csf.service’
Created symlink from /etc/systemd/system/multi-user.target.wants/csf.service to /usr/lib/systemd/system/csf.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/lfd.service to /usr/lib/systemd/system/lfd.service.
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
Removed symlink /etc/systemd/system/basic.target.wants/firewalld.service.
‘/etc/csf/csfwebmin.tgz’ -> ‘/usr/local/csf/csfwebmin.tgz’

Installation Completed

??n ?ây các b?n truy c?p vào th? m?c /usr/local/csf/bin và ch?y file csftest.pl ?? ki?m tra xem ho?t ??ng c?a cfs

```
# cd /usr/local/csf/bin

# perl csftest.pl
```

[root@maxserver bin]# perl csftest.pl

Testing ip_tables/iptable_filter...OK
Testing ipt_LOG...OK
Testing ipt_multiport/xt_multiport...OK
Testing ipt_REJECT...OK
Testing ipt_state/xt_state...OK
Testing ipt_limit/xt_limit...OK
Testing ipt_recent...OK
Testing xt_connlimit...OK
Testing ipt_owner/xt_owner...OK
Testing iptable_nat/ipt_REDIRECT...OK
Testing iptable_nat/ipt_DNAT...OK

RESULT: csf should function on this server

B??c 3: C?u hình CSF

Tr??c khi b??c vào quá trình c?u hình CSF, ?i?u ??u tiên b?n ph?i bi?t là "CentOS 7" có m?t ?ng d?ng t??ng l?a m?c ??nh g?i là "firewalld". B?n ph?i ng?ng firewalld và lo?i b? nó t? khi kh?i ??ng.

```
# systemctl stop firewalld
# systemctl disable firewalld
```

Sau ?ó vào th? m?c c?u hình CSF "/ etc / CSF /" và ch?nh s?a các t?p tin

"csf.conf" :

```
# nano /etc/csf/csf.conf
```

Thay ??i dòng 11 "TESTING" thành "0" ?? áp d?ng các c?u hình t??ng l?a.

Sau khi thay ??i xong gõ l?nh sau ?? kh?i ??ng csf

```
# systemctl start csf
# systemctl start lfd
```

Cho ch?y cùng h? th?ng

```
# systemctl enable csf
# systemctl enable lfd
```

Các t?p tin c?u hình chính

- csf.conf - các t?p tin c?u hình chính, nó có ý ki?n h?u ích ?? gi?i thích nh?ng gì m?i tùy ch?n nào
- csf.allow - m?t danh sách các ??a ch? CIDR c?a IP và ph?i luôn luôn ???c phép thông qua các b?c t??ng l?a
- csf.deny - m?t danh sách các ??a ch? CIDR c?a IP và không bao gi? ???c phép thông qua các b?c t??ng l?a
- csf.ignore - m?t danh sách các IP và ??a ch? CIDR r?ng LFD nên b? qua và không ng?n ch?n n?u phát hi?n

C?u hình trong t?p tin csf.conf

```
# nano /etc/csf/csf.conf
```

M? port

Cho phép các c?ng TCP ??n

```
# Allow incoming TCP ports
TCP_IN = "20,21,22,25,53,80,110,143,443,465,587,993,995"
```

Cho phép các c?ng TCP g?i ?i

```
# Allow outgoing TCP ports
TCP_OUT = "20,21,22,25,53,80,110,113,443,587,993,995"
```

Cho phép các c?ng UDP ??n

```
# Allow incoming UDP ports
UDP_IN = "20,21,53"
```

Cho phép các c?ng UDP g?i ?i

```
# Allow outgoing UDP ports
# To allow outgoing traceroute add 33434:33523 to this list
UDP_OUT = "20,21,53,113,123"
```

Ch?n ping

Cho phép PING ??n, thay ??i giá tr? 1 ho?c 0 ?? ch?n

```
# Allow incoming PING
ICMP_IN = "1"
```

??t t?c ?? ping ??n

?? vô hi?u hóa gi?i h?n t?c ?? thi?t l?p ?? "0"

```
# Set the per IP address incoming ICMP packet rate
# To disable rate limiting set to "0"
ICMP_IN_RATE = "1/s"
```

Cho phép PING ?i, thay ??i giá tr? 1 ho?c 0 ?? ch?n

```
# Allow outgoing PING
ICMP_OUT = "1"
```

??t t?c ?? ping ?i

```
# Set the per IP address outgoing ICMP packet rate (hits per second allowed),
# e.g. "1/s"
# To disable rate limiting set to "0"
ICMP_OUT_RATE = "0"
```

Thi?t l?p v?o v? ch?ng DOS

B?n có th? ch? ??nh s? l??ng cho phép k?t n?i trên m?i c?ng trong kho?ng th?i gian c?a ý thích c?a b?n

PORTFLOOD = "port;protocol;hit count*;interval seconds"

VD:

PORTFLOOD = "22;tcp;5;300,80;tcp;20;5"

1. N?u có nhi?u h?n 5 k?t n?i ??n tcp port 22 trong vòng 300 giây, thì sau ?ó ch?n ??a ch? IP t? port 22 cho ít nh?t 300 giây sau khi các gói tin cu?i cùng ???c nhìn th?y, t?c là không có m?t k?t n?i nào ??n trong th?i gian 300 giây thì ch?n s? ?c d? b?

2. N?u có nhi?u h?n 20 k?t n?i ??n tcp port 80 trong vòng 5 giây, thì sau ?ó ch?n ??a ch? IP t? port 80 cho ít nh?t 5 giây sau khi các gói tin cu?i cùng ???c nhìn th?y, t?c là không có m?t k?t n?i nào ??n trong th?i gian 5 giây thì ch?n s? ?c d? b?

Online URL: https://huongdan.maxserver.com/article-131.html