

Hướng dẫn cài đặt và cấu hình csf trên centos 7 (Báo và VPS)

admin Sun, Apr 14, 2019 [Cài Đặt Cơ Bản & Hướng Dẫn](#) 0 2000

CSF LÀ GÌ ?

CSF (ConfigServer & Firewall) là 1 gói ứng dụng hoạt động trên Linux như 1 Firewall được phát hành miễn phí và tính bảo mật cho server (VPS và Dedicated). CSF hoạt động dựa trên iptables và tiến trình lfd để quyết các file log để phát hiện các dấu hiệu tấn công bất thường.

CSF sẽ giúp server của bạn:

- Chống DoS các loại
- Chống Scan Port
- Đề ra các lời khuyên về việc cấu hình server (VD: Nên nâng cấp MySQL lên bản mới hơn)
- Chống BruteForce Attack vào ftp server, web server, mail server, directadmin, cPanel...
- Chống Syn Flood
- Chống Ping Flood
- Cho phép ngăn chặn truy cập từ 1 quốc gia nào đó bằng cách chọn Country Code chuẩn ISO
- Hỗ trợ IPv6 và IPv4
- Cho phép khóa IP tạm thời và vĩnh viễn nếu tấn công (An toàn hơn và ứng dụng) nên webserver không phải nhấc x lý yêu cầu từ các IP bị cấm nữa
- Cho phép bạn chuyển hướng yêu cầu từ các IP bị khóa sang 1 file html để thông báo cho người dùng biết IP của họ bị khóa
- Và rất nhiều tính năng khác, các bạn có thể tìm hiểu thêm

Bước 1: Cài đặt các gói cần thiết để chạy csf

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

Bước 2: Tải về và cài đặt 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
```

Download 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/iptables_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/iptables_REDIRECT...OK
```

```
Testing iptable_nat/iptables_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 dòng 11 "TESTING" thành "0" và áp dụng các cấu hình tương tự.

Sau khi thay xong gõ lệnh sau khi khởi động csf

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

Cho chạy cùng hệ thống

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

Các tệp tin cấu hình chính

- csf.conf - các tệp tin cấu hình chính, nó có ý kiến hữu ích về gì thích nhưng gì tùy chọn nào
- csf.allow - một danh sách các địa chỉ CIDR của IP và phải luôn luôn được phép thông qua các bộ lọc
- csf.deny - một danh sách các địa chỉ CIDR của IP và không bao giờ được phép thông qua các bộ lọc
- csf.ignore - một danh sách các IP và địa chỉ CIDR riêng LFD nên bỏ qua và không nên chọn nếu phát hiện

Cấu hình trong tệp tin csf.conf

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

Mở port

Cho phép các cổng TCP

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

Cho phép các cổng TCP gửi đi

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

Cho phép các cổng UDP nhận

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

Cho phép các cổng UDP gửi đi

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

Chặn ping

Cho phép PING nhận, thay đổi giá trị 1 hoặc 0 để chặn

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

Thiết lập tốc độ ping nhận

Thiết lập vô hiệu hóa giới hạn tốc độ gửi đi thì đặt là "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>