Comment installer CSF (Config Server Firewall) sur Debian 12

CSF ou Config Server Firewall est un pare-feu Stateful Packet Inspection (SPI) basé sur IPtables et Perl. il fournit un processus démon qui surveillera vos services pour détecter les échecs d'authentification et fournira également l'intégration de l'interface utilisateur Web pour la gestion des serveurs Web tels que Webmin, cPanel et DirectAdmin.

Dans ce tutoriel, nous vous guiderons à travers le processus d'installation de CSF (Config Server Firewall) sur le serveur Debian 12. Vous apprendrez également la configuration de base de CSF, le blocage des adresses IP à l'aide de deux méthodes différentes et la configuration Interface utilisateur Web CSF pour faciliter la gestion et la surveillance.

Conditions préalables

Pour commencer ce didacticiel, assurez-vous de disposer des éléments suivants :

- Un serveur Debian 12.
- Un utilisateur non root avec des privilèges d'administrateur.

Préparation du système

Avant d'installer CSF, vous devez vous assurer que les dépendances sont installées. Cela inclut des packages tels que Perl et iptables. De plus, lorsque vous avez un autre pare-feu en cours d'exécution tel que UFW (Uncomplicated Firewall), vous devez le désactiver.

Pour commencer, exécutez la commande suivante pour mettre à jour votre référentiel Debian.

```
sudo apt update
```

```
root@server64:~#
root@server64:~# sudo apt update
Get:1 http://deb.debian.org/debian bookworm InRelease [151 kB]
Get:2 http://security.debian.org/debian-security bookworm-security InRelease [48.0 kB]
Get:3 http://deb.debian.org/debian bookworm-updates InRelease [52.1 kB]
Get:4 http://deb.debian.org/debian bookworm/non-free-firmware Sources [6,168 B]
Get:5 http://deb.debian.org/debian bookworm/main Sources [9,488 kB]
Get:6 http://security.debian.org/debian-security bookworm-security/non-free-firmware Sources [796 B]
Get:7 http://security.debian.org/debian-security bookworm-security/main Sources [66.0 kB]
Get:8 http://security.debian.org/debian-security bookworm-security/main amd64 Packages [127 kB]
```

Une fois le référentiel mis à jour, installez les dépendances suivantes pour CSF à l'aide de la commande ci-dessous.

```
sudo apt install libio-socket-inet6-perl libsocket6-perl sendmail dnsutils unzip libio-socket-ssl-perl libcrypt-ssleay-perl git perl iptables
libnet-libidn-perl libwww-perl liblwp-protocol-https-perl libgd-graph-perl
```

Tapez Y et appuyez sur ENTRÉE pour continuer.

```
root@server64:~#
root@server64:~# sudo apt install libio-socket-inet6-perl libsocket6-perl sendmail dnsutils unzip libio-socket-ssl-per
t perl iptables libnet-libidn-perl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.39.2-1.1).
The following additional packages will be installed:
  javascript-common libbytes-random-secure-perl libc-ares2 libcrypt-random-seed-perl libidn12 libip6tc2 libjs-jquery l
  libmath-random-isaac-perl libmath-random-isaac-xs-perl libnet-ssleay-perl libnetfilter-conntrack3 libnfnetlink0 libp
  lockfile-progs m4 perl-base perl-modules-5.36 perl-openssl-defaults postfix-mta-sts-resolver procmail python3-aiodns
  python3-aioredis python3-aiosignal python3-aiosqlite python3-async-timeout python3-attr python3-cffi-backend python3
  python3-frozenlist python3-hiredis python3-multidict python3-packaging python3-pycares python3-redis python3-typing-
  python3-uvloop python3-wrapt python3-yaml python3-yarl sendmail-base sendmail-bin sendmail-cf sensible-mda
Suggested packages:
  firewalld apache2 | lighttpd | httpd m4-doc perl-doc libterm-readline-gnu-perl | libterm-readline-perl-perl libtap-ha
  debhelper python-aiosqlite-doc python-attr-doc redis-server python-pycares-doc sendmail-doc rmail logcheck sasl2-bin
The following packages will be REMOVED:
  postfix postfix-cdb
The following NEW packages will be installed:
  dnsutils iptables javascript-common libbytes-random-secure-perl libc-ares2 libcrypt-random-seed-perl libcrypt-ssleay-
  libio-socket-inet6-perl libio-socket-ssl-perl libip6tc2 libjs-jquery liblockfile1 libmath-random-isaac-perl libmath-
  libnet-libidn-perl libnet-ssleay-perl libnetfilter-conntrack3 libnfnetlink0 libsocket6-perl libyaml-0-2 lockfile-prog
  perl-openssl-defaults postfix-mta-sts-resolver procmail python3-aiodns python3-aiohttp python3-aioredis python3-aios
  python3-async-timeout python3-attr python3-cffi-backend python3-deprecated python3-frozenlist python3-hiredis python3
  python3-packaging python3-pycares python3-redis python3-typing-extensions python3-uvloop python3-wrapt python3-yaml p
  sendmail-base sendmail-bin sendmail-cf sensible-mda unzip
The following packages will be upgraded:
  libperl5.36 perl perl-base perl-modules-5.36
4 upgraded, 52 newly installed, 2 to remove and 23 not upgraded.
Need to get 14.8 MB of archives.
After this operation, 14.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

Enfin, vous devez désactiver UFW si vous l'avez sur votre serveur Debian. CSF utilise par défaut iptables comme pare-feu et filtre de paquets.

```
sudo ufw disable
```

Téléchargement et installation de CSF

Dans la section suivante, vous allez télécharger et installer CSF (Config Server Firewall) manuellement à partir de la source. Alors, commençons.

Téléchargez le code source CSF à l'aide de la commande wget ci-dessous. Vous verrez le fichier csf.tgz.

```
wget http://download.configserver.com/csf.tgz
```

Extrayez maintenant le fichier csf.tgz à l'aide de la commande tar ci-dessous. Le code source CSF sera disponible dans le répertoire csf.

```
sudo tar -xvzf csf.tgz
```

Ensuite, accédez au répertoire csf et exécutez le script install.sh pour démarrer l'installation.

```
cd csf; sh install.sh
```

Une fois l'installation démarrée, vous devriez obtenir ce qui suit :

```
root@server64:~#
root@server64:~# ls
csf  csf.tgz
root@server64:~# cd csf; sh install.sh

Selecting installer...

Running csf generic installer

Installing generic csf and lfd

Check we're running as root

mkdir: created directory '/etc/csf'
'install.txt' -> '/etc/csf/install.txt'
Checking Perl modules...
Configuration modified to use iptables-nft
Configuration modified to use ip6tables-nft
Configuration modified for Debian/Ubuntu/Gentoo settings /etc/csf/csf.conf
...Perl modules OK

mkdir: cannot create directory ‘/etc/csf’: File exists
mkdir: created directory '/var/lib/csf'
mkdir: created directory '/var/lib/csf/backup'
mkdir: created directory '/var/lib/csf/Geo'
mkdir: created directory '/var/lib/csf/ui'
mkdir: created directory '/var/lib/csf/stats'
mkdir: created directory '/var/lib/csf/lock'
mkdir: created directory '/var/lib/csf/webmin'
mkdir: created directory '/var/lib/csf/zone'
mkdir: created directory '/usr/local/csf'
mkdir: created directory '/usr/local/csf/bin'
mkdir: created directory '/usr/local/csf/lib'
mkdir: created directory '/usr/local/csf/tpl'
'csf.generic.conf' -> '/etc/csf/csf.conf'
'csf.generic.allow' -> '/etc/csf/csf.allow'
'csf.deny' -> '/etc/csf/./csf.deny'
```

Une fois le processus terminé, vous devriez obtenir une sortie « Installation terminée ».

```
TCP ports currently listening for incoming connections:
22

UDP ports currently listening for incoming connections:
68

Note: The port details above are for information only, csf hasn't been auto-configured.

Don't forget to:
1. Configure the following options in the csf configuration to suite your server: TCP_*, UDP_*
2. Restart csf and lfd
3. Set TESTING to 0 once you're happy with the firewall, lfd will not run until you do so
'lfd.service' -> '/usr/lib/systemd/system/lfd.service'
'csf.service' -> '/usr/lib/systemd/system/csf.service'
Created symlink /etc/systemd/system/multi-user.target.wants/csf.service → /lib/systemd/system/csf.service.
Created symlink /etc/systemd/system/multi-user.target.wants/lfd.service → /lib/systemd/system/lfd.service.
Unit /etc/systemd/system/firewalld.service is masked, ignoring.
'/etc/csf/csfwebmin.tgz' -> '/usr/local/csf/csfwebmin.tgz'

Installation Completed
```

Maintenant que CSF est installé, vérifiez-le à l'aide de la commande ci-dessous.

```
perl /usr/local/csf/bin/csftest.pl
```

Assurez-vous que le résultat de chaque test de fonctionnalité est correct .

```
root@server64:~#
root@server64:~# perl /usr/local/csf/bin/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
root@server64:~#
```

Enfin, exécutez la commande suivante pour vérifier l'emplacement et la version du binaire CSF.

```
which csf
csf -v
```

Dans la sortie suivante, vous pouvez voir CSF v14.20 est installé dans /usr/sbin/csf .

```
root@server64:~#
root@server64:~# which csf
/usr/sbin/csf
root@server64:~# csf -v
csf: v14.20 (generic)
*WARNING* TESTING mode is enabled - do not forget to disable it in the configuration
root@server64:~#
root@server64:~#
```

Configuration de CSF

Après avoir installé CSF, vous apprendrez quelques configurations de base de CSF (Config Server Firewall). Le principal
Le répertoire de configuration de CSF est le répertoire /etc/csf , vous y trouverez le fichier de configuration principal de CSF, csf.conf.

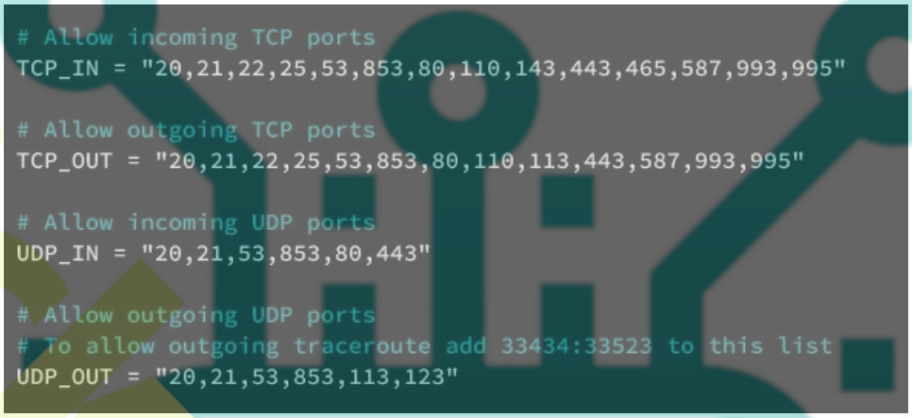
Utilisez la commande suivante de l'éditeur nano pour ouvrir le fichier de configuration CSF /etc/csf/csf.conf .

```
sudo nano /etc/csf/csf.conf
```

Autoriser le trafic via CSF

Recherchez les options TCP_* et UDP_* et ajoutez vos ports.

```
# Allow incoming TCP ports
TCP_IN = "20,21,22,25,53,853,80,110,143,443,465,587,993,995"

# Allow outgoing TCP ports
TCP_OUT = "20,21,22,25,53,853,80,110,113,443,587,993,995"

# Allow incoming UDP ports
UDP_IN = "20,21,53,853,80,443"

# Allow outgoing UDP ports
# To allow outgoing traceroute add 33434:33523 to this list
UDP_OUT = "20,21,53,853,113,123"
```



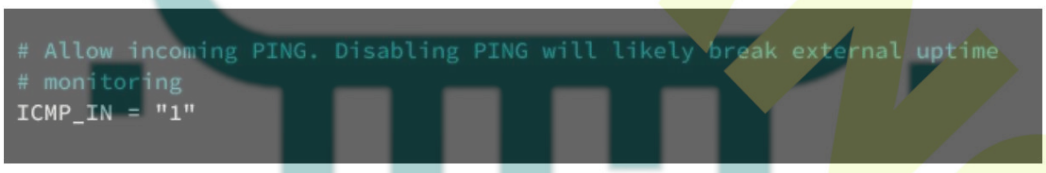
Options détaillées :

- TCP_IN : autorise le trafic entrant vers les ports TCP.
- TCP_OUT : autorise le trafic sortant vers des ports TCP spécifiques.
- UDP_IN : autorise le trafic entrant vers les ports UDP.
- UDP_OUT : autorise le trafic sortant vers des ports UDP spécifiques.

Autoriser/Refuser les requêtes Ping ou ICMP

Si vous avez vraiment besoin de désactiver Ping ou ICMP 'IN et OUT', utilisez les options suivantes. Le 'ICMP_IN = 1' signifie que le ping sera autorisé et le 'ICMP_OUT = 1' signifie que le serveur peut cingler vers un autre réseau.

```
# Allow incoming PING. Disabling PING will likely break external uptime
# monitoring
ICMP_IN = "1"
...
# Allow outgoing PING

 Unless there is a specific reason, this option should NOT be disabled as it
# could break OS functionality
ICMP_OUT = "1"
```



Synflood Protection

N'ACTIVEZ cette option qu'en cas de nécessité, par exemple contre les attaques DOS sur votre serveur.

```
######################################################################
# SECTION:Port Flood Settings
######################################################################
# Enable SYN Flood Protection. This option configures iptables to offer some
# protection from tcp SYN packet DOS attempts.
...
SYNFLOOD = "0"
SYNFLOOD_RATE = "100/s"
SYNFLOOD_BURST = "150"
```

```
###############################################################################
# SECTION:Port Flood Settings
###############################################################################
# Enable SYN Flood Protection. This option configures iptables to offer some
# protection from tcp SYN packet DOS attempts. You should set the RATE so that
# false-positives are kept to a minimum otherwise visitors may see connection
# issues (check /var/log/messages for *SYNFLOOD Blocked*). See the iptables
# man page for the correct --limit rate syntax
#
# Note: This option should ONLY be enabled if you know you are under a SYN
# flood attack as it will slow down all new connections from any IP address to
# the server if triggered
SYNFLOOD = "1"
SYNFLOOD_RATE = "100/s"
SYNFLOOD_BURST = "150"
```

Limiter les connexions simultanées

Ensuite, utilisez l'option « CONNLIMIT » pour limiter les connexions simultanées pour des ports spécifiques. Le format est « PORT;LIMIT », donc, par exemple, la configuration « 22;5 » limitera le port SSH à seulement 5 connexions simultanées.

```
# Connection Limit Protection. This option configures iptables to offer more
# protection from DOS attacks against specific ports. It can also be used as a
# way to simply limit resource usage by IP address to specific server services.
# Note: Run /etc/csf/csftest.pl to check whether this option will function on
# this server
CONNLIMIT = "22;5,21;10"
```

```
# Connection Limit Protection. This option configures iptables to offer more
# protection from DOS attacks against specific ports. It can also be used as a
# way to simply limit resource usage by IP address to specific server services.
# This option limits the number of concurrent new connections per IP address
# that can be made to specific ports
#
# This feature does not work on servers that do not have the iptables module
# xt_connlimit loaded. Typically, this will be with MONOLITHIC kernels. VPS
# server admins should check with their VPS host provider that the iptables
# module is included
#
# For further information and syntax refer to the Connection Limit Protection
# section of the csf readme.txt
#
# Note: Run /etc/csf/csftest.pl to check whether this option will function on
# this server
CONNLIMIT = "22;5,21;10"
```

Désactiver le mode TEST et restreindre l'accès au Syslog

Maintenant, si vous avez tout configuré et ajouté vos ports, remplacez le 'TESTING' par '1' et restreignez l'accès aux sockets rsyslog avec 'RESTRICT_SYSLOG= "3"'.

```
# lfd will not start while this is enabled
TESTING = "0"
...
# 0 = Allow those options listed above to be used and configured
# 1 = Disable all the options listed above and prevent them from being used
# 2 = Disable only alerts about this feature and do nothing else
# 3 = Restrict syslog/rsyslog access to RESTRICT_SYSLOG_GROUP ** RECOMMENDED **
RESTRICT_SYSLOG = "3"
```

Lorsque tout est terminé, enregistrez le fichier et quittez l'éditeur.

```
#
# lfd will not start while this is enabled
TESTING = "0"
```

Test et démarrage du service CSF

Exécutez maintenant la commande csf ci-dessous pour vérifier votre configuration. Si la configuration de CSF est correcte, vous verrez apparaître le message suivant

Sortie CSF. En revanche, vous verrez l'erreur détaillée lorsque votre configuration est incorrecte.

```
csf -v
```

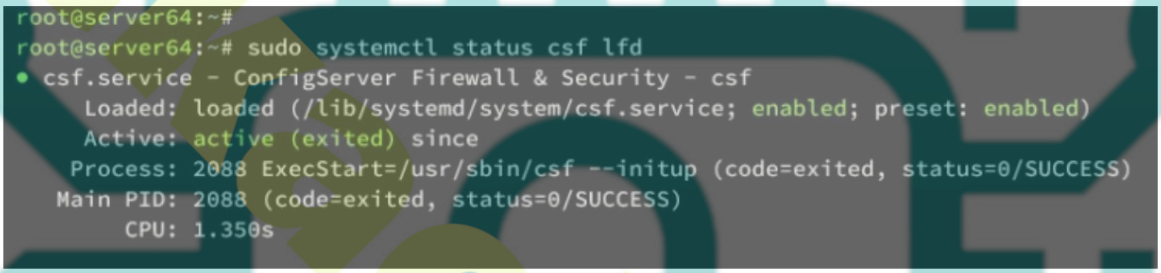
Ensuite, exécutez la commande systemctl ci-dessous pour démarrer les services csf et lfd.

```
sudo systemctl start csf lfd
```

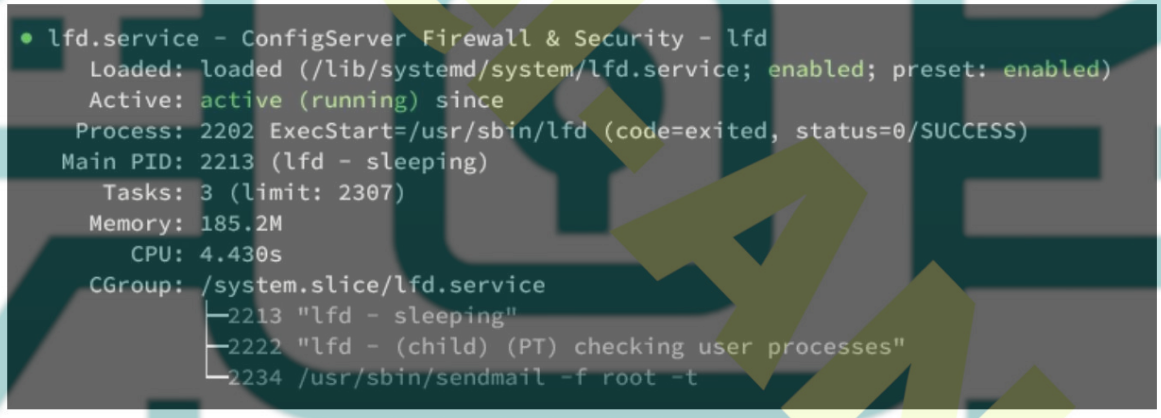
Une fois le service csf exécuté, vous serez automatiquement déconnecté du serveur. Vous pouvez vous reconnecter au serveur, puis vérifier les services csf et lfd à l'aide de la commande ci-dessous.

```
sudo systemctl status csf lfd
```

Vous pouvez voir que le service csf est en cours d'exécution.



Vous pouvez également voir que le service lfd est en cours d'exécution.



Blocage via CSF

À ce stade, vous avez appris la configuration de base de CSF (Config Server Firewall). Voyons maintenant le blocage des adresses IP via CSF.

Blocage des adresses IP via les listes IP BLOCK

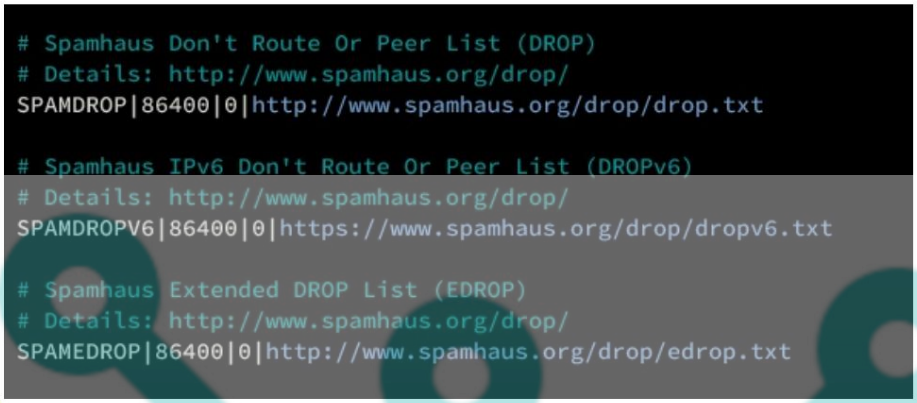
Ouvrir la configuration des listes IP BLOCk par défaut /etc/csf/csf.blocklists en utilisant la commande nano editor ci-dessous.

```
sudo nano /etc/csf/csf.blocklists
```

Décommentez les lignes suivantes pour bloquer les adresses IP de la base de données Spamhaus .

```
# Spamhaus Don't Route Or Peer List (DROP)
# Details: http://www.spamhaus.org/drop/
SPAMDROP|86400|0|http://www.spamhaus.org/drop/drop.txt

# Spamhaus IPv6 Don't Route Or Peer List (DROPv6)
# Details: http://www.spamhaus.org/drop/
SPAMDROPV6|86400|0|https://www.spamhaus.org/drop/dropv6.txt

# Spamhaus Extended DROP List (EDROP)
# Details: http://www.spamhaus.org/drop/
SPAMEDROP|86400|0|http://www.spamhaus.org/drop/edrop.txt
```

Enregistrez le fichier et quittez l'éditeur lorsque vous avez terminé.



Vous trouverez ci-dessous quelques options détaillées :

- **SPAMDROP** : nom du bloc qui sera utilisé comme nom de canal iptables. Utilisez uniquement des MAJUSCULES avec un maximum de 25 caractères.
- **86400** : intervalle d'actualisation pour télécharger et renouveler les adresses IP des listes de blocage.
- **MAX** : adresses IP maximales qui seront utilisées dans la liste. Une valeur de 0 signifie que toutes les adresses IP seront incluses. URL :
- **l'URL** de téléchargement des adresses IP des listes de blocage.

Blocage des adresses IP via GeoIP

Une autre méthode pour bloquer une adresse IP consiste à utiliser GeoIP, qui vous permet de bloquer le trafic entrant en provenance d'un pays spécifique.

Utilisez la commande suivante de l'éditeur nano pour ouvrir la configuration CSF ' /etc/csf/csf.conf '.

```
sudo nano /etc/csf/csf.conf
```

Retrouvez les paramètres CC_DENY et CC_ALLOW pour mettre en place le blocage par pays via GeoIP.

# Each option is a comma-separated list of CC's, e.g. "US,GB,DE"
CC_DENY = "RU,CN"
CC_ALLOW = "US,GB,DE,NL,SG"

Par défaut, CSF utilise la base de données GeoIP de db-ip, ipdeny et iptoasn. Mais vous pouvez également le modifier via la base de données MaxMind GeoIP. Pour utiliser la base de données MaxMind , remplacez « CC_SRC » par « 1 », puis saisissez votre clé de licence MaxMind dans l'option « MM_LICENSE_KEY » .

# MaxMind License Key:
MM_LICENSE_KEY = ""

...
Set the following to your preferred source:
"1" - MaxMind
"2" - db-ip, ipdeny, iptoasn

#The default is "2" on new installations of csf, or set to "1" to use the
# MaxMind databases after obtaining a license key
CC_SRC = "1"

Enregistrez le fichier et quittez l'éditeur lorsque vous avez terminé.

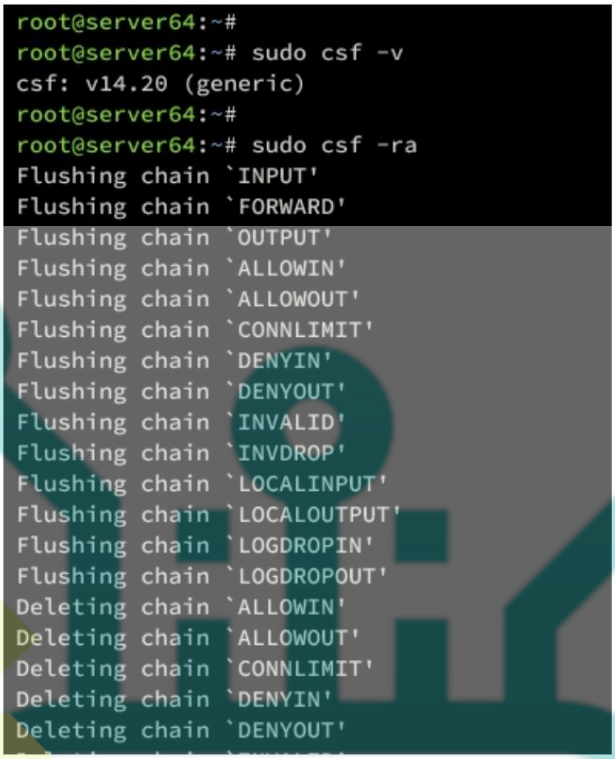
Maintenant, exécutez la commande suivante pour vérifier la configuration CSF. S'il n'y a pas d'erreur, vous devriez obtenir la version CSF.

```
sudo csf -v
```

Ensuite, redémarrez les services csf et lfd à l'aide de la commande suivante.

```
sudo csf -ra
```

Vous devriez voir un résultat semblable à celui-ci :



Pour vous assurer que csf et lfs sont en cours d'exécution, utilisez la commande suivante pour vérifier les deux services.

```
sudo systemctl status csf lfd
```

Activer l'interface utilisateur Web CSF

Dans la section suivante, vous apprendrez comment activer l'interface utilisateur Web CSF pour la surveillance via un navigateur Web.

Ouvrez la configuration CSF à l'aide de l'éditeur nano suivant.

```
sudo nano /etc/csf/csf.conf
```

Remplacez l' option « UI » par « 1 » et activez l'interface utilisateur Web CSF. Ensuite, ajustez UI_PORT, UI_IP, UI_USER , et le UI_PASS le avec vos coordonnées.

Changez l'option 'UI' sur '1' et activez CSF Web UI. Ajustez ensuite les paramètres UI_PORT, UI_IP, UI_USER et UI_PASS avec vos coordonnées.

```
# 1 to enable, 0 to disable
UI = "1"

...

# Do NOT enable access to this port in TCP_IN, instead only allow trusted IPs
# to the port using Advanced Allow Filters (see readme.txt)
UI_PORT = "1048"

...

# If the server is configured for IPv6 but the IP to bind to is IPv4, then the
# IP address MUST use the IPv6 representation. For example, 1.2.3.4 must use
# ::ffff:1.2.3.4

 #Leave blank to bind to all IP addresses on the server
UI_IP = "127.0.0.1"

...

# This should be a secure, hard to guess username

 #This must be changed from the default
UI_USER = "alice"
...
# numbers and non-alphanumeric characters

 #This must be changed from the default
UI_PASS = "passw0rd"
```

Enregistrez le fichier et quittez l'éditeur lorsque vous avez terminé.
Trouvez maintenant votre adresse IP publique à l'aide de la commande ci-dessous.

```
curl https://ipinfo.io/
```

Ajoutez votre adresse IP aux configurations '/etc/csf/csf.allow' et '/etc/csf/ui/ui.allow'. Cela mettra votre adresse IP publique sur liste blanche et vous permettra d'accéder à l'interface Web de CSF et au serveur.

single ip
192.168.5.1

subnet
192.168.5.0/24

Après cela, exécutez la commande ci-dessous pour vérifier la configuration CSF et redémarrez les services csf et lfd.

```
sudo csf -v
sudo csf -ra
```

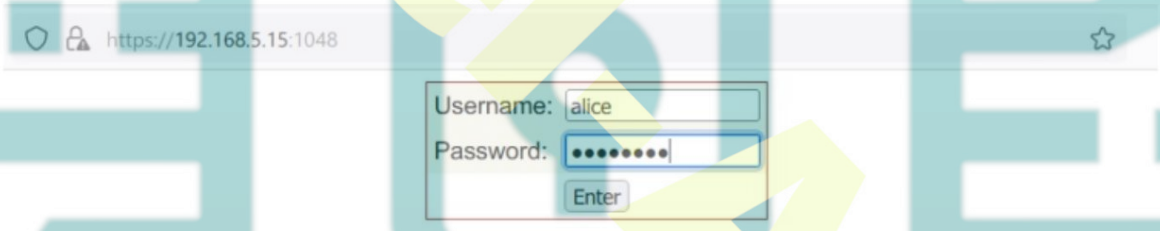
Ensuite, vérifiez la liste des adresses IP sur liste blanche sur CSF à l'aide de la commande ci-dessous. Trouver la chaîne iptables ALLOWIN et AUTORISER, et vous devriez voir vos adresses IP sur liste blanche.

```
sudo csf -l
```

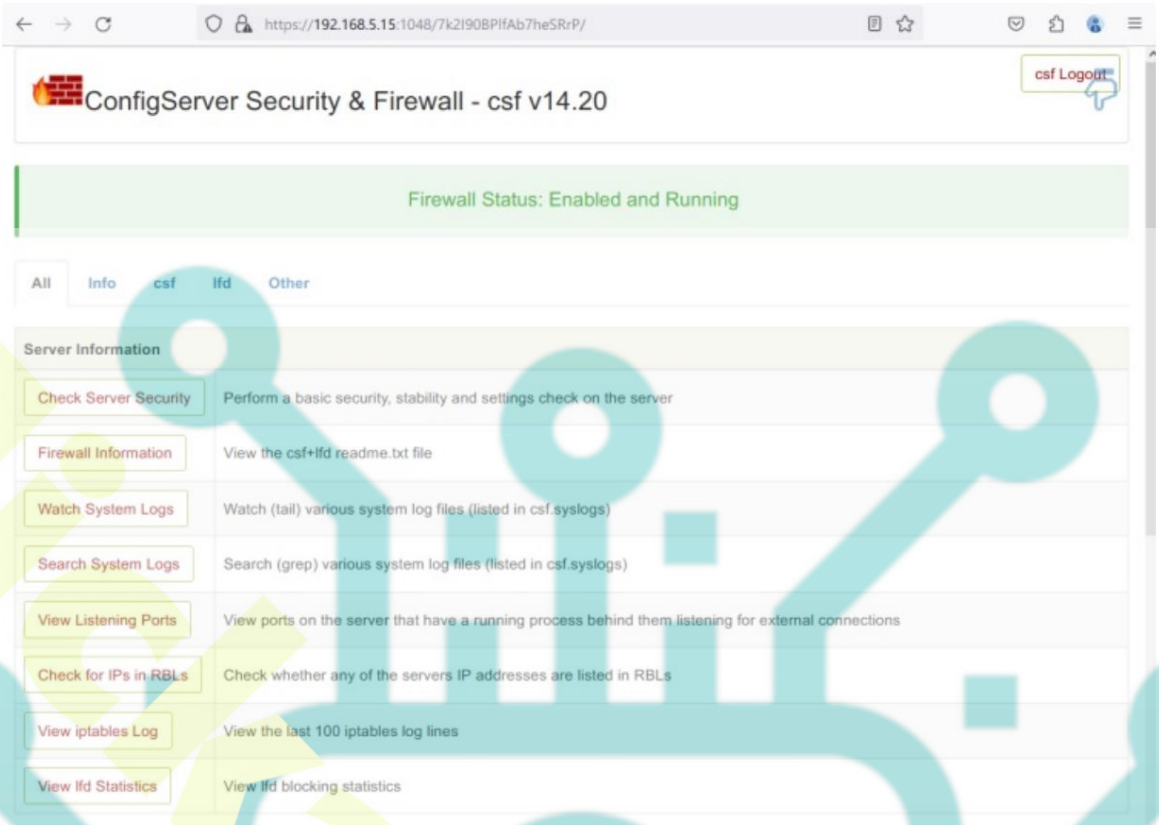
```
Chain ALLOWIN (1 references)
num   pkts bytes target     prot opt in     out     source               destination
1      952 95372 ACCEPT     0    --  !lo    *       192.168.5.1          0.0.0.0/0

Chain ALLOWOUT (1 references)
num   pkts bytes target     prot opt in     out     source               destination
1      765 1638K ACCEPT     0    --  *      !lo     0.0.0.0/0            192.168.5.1
```

Ouvrez maintenant votre navigateur Web et visitez l'adresse IP du serveur suivie du port de l'interface utilisateur Web CSF (c'est-à-dire : https://192.168.5.15:1048). Si votre configuration réussit, vous devriez voir la page de connexion CSF.

Saisissez votre utilisateur administrateur et votre mot de passe, puis cliquez sur ENTRÉE.



Vous devriez voir le tableau de bord CSF comme suit :



Conclusion

Toutes nos félicitations! Vous avez maintenant installé avec succès CSF (Config Server Firewall) sur le serveur Debian 12. vous avez également appris l'utilisation de base de CSF pour autoriser le trafic vers un port spécifique, désactiver le ping ou ICMP et configurer la limite de connexion pour les ports.

En plus de cela, vous avez également appris à bloquer les adresses IP avec CSF en utilisant les listes IP BLOCK et GeoIP. En outre, vous avez activé l'interface utilisateur Web CSF pour faciliter la gestion et la surveillance de votre serveur CSF.
