Comment installer et configurer le pare-feu du serveur de configuration (CSF) sur Rocky Linux 9

Config Server Security and Firewall (CSF) est un pare-feu basé sur iptables qui offre un haut niveau de sécurité au système Linux. Il le fait en effectuant une inspection des paquets avec état (SPI).

Il est doté de nombreuses fonctionnalités, telles que le blocage IP, le blocage de port et la protection DDoS. Il prend également en charge la limitation de débit, la connexion suivi et détection de connexion SSH. Il comprend également des outils de vérification de l'intégrité du système et des fichiers. Il est livré avec un tableau de bord GUI, qui peut être utilisé pour gérer ses paramètres. Vous pouvez également intégrer CSF à des panneaux de contrôle comme DirectAdmin, cPanel, Cyberpanel, Vesta et Webmin.

Ce didacticiel vous apprend à installer et gérer CSF sur un serveur Rocky Linux 9.

Conditions préalables

- Un serveur exécutant Rocky Linux 9 avec un minimum de 1 Go de RAM.
- Un utilisateur non root avec les privilèges sudo.
- Un nom de domaine entièrement qualifié (FQDN) comme `csf.exemple.com` pointant vers votre serveur.
- Tout est mis à jour.

```
$ sudo dnf update
```

- Quelques packages essentiels sont requis pour que le didacticiel et Craft CMS fonctionnent. Certains d'entre eux seront déjà sur votre serveur.

```
$ sudo dnf install wget curl nano unzip yum-utils policycoreutils-python-utils -y
```

Étape 1 - Désactiver le pare-feu Firewalld

Rocky Linux utilise Firewalld Firewall par défaut. Nous devons d'abord le désactiver afin qu'il n'interfère pas avec le CSF.

Vérifiez d'abord l'état du pare-feu Firewalld.

```
$ sudo systemctl status firewalld
? firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
     Active: active (running) since Tue 2023-12-05 07:00:53 UTC; 40s ago
       Docs: man:firewalld(1)
   Main PID: 58756 (firewalld)
      Tasks: 2 (limit: 4424)
     Memory: 25.9M
        CPU: 496ms
     CGroup: /system.slice/firewalld.service
             ??58756 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid

Dec 05 07:00:52 csf.example.com systemd[1]: Starting firewalld - dynamic firewall daemon...
Dec 05 07:00:53 csf.example.com systemd[1]: Started firewalld - dynamic firewall daemon.
```

Arrêtez et désactivez le service Firewalld.

```
$ sudo systemctl stop firewalld
$ sudo systemctl disable firewalld
```

Étape 2 - Installer les modules Perl requis

CSF nécessite l'exécution de certains modules Perl. Mais d'abord, nous avons besoin du référentiel EPEL. Installez-le

```
$ sudo dnf install epel-release
```

Installez-les à l'aide de la commande suivante.

```
$ sudo dnf install perl-core perl-libwww-perl.noarch perl-LWP-Protocol-https.noarch perl-GDGraph -y
```

Étape 3 - Téléchargez et installez CSF

CSF n'est pas disponible dans le référentiel Rocky Linux. Par conséquent, nous devons l'installer manuellement.

Téléchargez la dernière version de l' archive CSF depuis leur site Internet.

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

Extrayez l'archive.

```
$ tar xzf csf.tgz
```

Basculez vers le répertoire extrait.

```
$ cd csf
```

Installez CSF en appelant le script d'installation.

```
$ sudo ./install.sh
```

Vous devriez obtenir le résultat suivant.

```
...............
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 → /usr/lib/systemd/system/csf.service.
Created symlink /etc/systemd/system/multi-user.target.wants/lfd.service → /usr/lib/systemd/system/lfd.service.
Unit /etc/systemd/system/firewalld.service is masked, ignoring.
The unit files have no installation config (WantedBy=, RequiredBy=, Also=,
Alias= settings in the [Install] section, and DefaultInstance= for template
units). This means they are not meant to be enabled or disabled using systemctl.

Possible reasons for having this kind of units are:
• A unit may be statically enabled by being symlinked from another unit's
  .wants/ or .requires/ directory.
• A unit's purpose may be to act as a helper for some other unit which has
  a requirement dependency on it.
• A unit may be started when needed via activation (socket, path, timer,
  D-Bus, udev, scripted systemctl call, ...).
• In case of template units, the unit is meant to be enabled with some
  instance name specified.
'/etc/csf/csfwebmin.tgz' -> '/usr/local/csf/csfwebmin.tgz'

Installation Completed
```

Vérifiez si les modules iptables requis sont disponibles.

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

Vous devriez voir le résultat suivant.

```
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
```

Vérifiez la version CSF.

```
$ sudo csf -v
csf: v14.20 (generic)
*WARNING* TESTING mode is enabled - do not forget to disable it in the configuration
```

Etape 4 - Configuration CSF

CSF stocke sa configuration dans le fichier `/etc/csf/csf.conf` . Ouvrir le fichier pour l'éditer.

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

La première étape consiste à désactiver le mode de test. Modifiez la valeur de l'option `TESTING` variable de `1` à `0`.

```
TESTING = "0"
```

Trouver la ligne `RESTRICT_SYSLOG = "0"` et de changer sa valeur en 3. Cela signifie que seuls les membres de la `RESTRICT_SYSLOG_GROUP` peut accéder au fichiers `syslog/rsyslog`. Le `RESTRICT_SYSLOG_GROUP` contient par défaut le `root`, `mysql`, `rpc`, `daemon`, `dbus`, and plusieurs utilisateurs de cPanel et DirectAdmin. Vous pouvez ajouter d'autres utilisateurs en modifiant le fichier `/etc/csf/csf.syslogusers` .

Etape 5 - Configurer les ports

CSF garde par défaut les ports suivants ouverts.

```
# 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"
```

Les services utilisant ces ports sont :

- Port 20 : transfert de données FTP
- Port 21 : contrôle FTP
- Port 22 : Shell sécurisé (SSH)
- Port 25 : Protocole de transfert de courrier simple (SMTP)
- Port 53 : Système de noms de domaine (DNS)
- Port 80 : protocole de transfert hypertexte (HTTP)
- Port 110 : Protocole de bureau de poste v3 (POP3)
- Port 113 : Service d'authentification/protocole d'identification
- Port 123 : protocole de temps réseau (NTP)
- Port 143 : protocole d'accès aux messages Internet (IMAP)
- Port 443 : Protocole de transfert hypertexte sur SSL/TLS (HTTPS)
- Port 465 : Répertoire de rendez-vous URL pour SSM (Cisco)
- Port 587 : envoi de messages électroniques (SMTP)
- Port 993 : protocole d'accès aux messages Internet via SSL (IMAPS)
- Port 995 : protocole postal 3 sur TLS/SSL (POP3S)

Si vous n'avez pas besoin d'ouvrir tous ces ports, vous pouvez en supprimer certains pour améliorer la sécurité. Si vous utilisez IPv6 pour vos services, vous devrez configurer port(TCP6_IN , TCP6_OUT, UDP6_IN ,UDP6_OUT ports) comme indiqué.

```
# Autoriser les ports TCP IPv6 sortants
TCP6_OUT "20,21,22,25,53,853,80,110,113,443,587,993,995"

# Autoriser les ports UDP IPv6 entrants
UDP6_IN "20,21,53,853,80,443"

# Autoriser les ports UDP IPv6 sortants
# Pour autoriser le traceroute sortant, ajoutez 33434:33523 à cette liste
UDP6_OUT = "20,21,53,853,113,123"
```

Modifiez les ports selon vos besoins.

Étape 6 - Paramètres CSF supplémentaires

Il y a beaucoup de paramètres à configurer. Passons en revue quelques-uns des plus couramment utilisés.

ICMP_IN - définir cette variable sur 1 autorise les pings vers votre serveur et 0 refuse de telles requêtes. Il est recommandé d'autoriser ICMP demandes si vous hébergez des services publics afin de pouvoir déterminer si votre service est disponible.

ICMP_IN_LIMIT - définit le nombre de requêtes autorisées à partir d'une seule adresse IP dans un laps de temps spécifié. C'est Il est recommandé de conserver la valeur inchangée.

DENY_IP_LIMIT - restreint le nombre d'adresses IP bloquées par le CSF. Si le nombre d'IP bloquées dépasse ce nombre numéro, CSF débloquera l'adresse IP la plus ancienne qui sera la première entrée du fichier. Un nombre trop élevé peut ralentir le serveur. Choisissez le numéro en fonction des ressources de votre serveur.

DENY_TEMP_IP_LIMIT - même chose que ci-dessus mais pour les blocs d'adresses IP temporaires.

PACKET_FILTER - filtre les paquets de trafic invalides, indésirables et illégaux.

CONNLIMIT - limite le nombre de connexions actives simultanées autorisées sur un seul port. Vous pouvez le définir comme suit.

```
CONNLIMITATION = "22;5;443;20"
```

La valeur ci-dessus signifie que seules 5 connexions simultanées seront autorisées sur le port 22 par adresse IP et seulement 20 connexions simultanées. les connexions seront autorisées sur le port 443 par adresse IP.

PORTFLOOD - limite le nombre de connexions par intervalle de temps pendant lequel de nouvelles connexions peuvent être établies vers des ports spécifiques. Tu peux réglez-le comme suit.

```
PORTEFEUILLE = "22;tcp;5;250"
```

La valeur ci-dessus bloquera l'adresse IP si plus de 5 connexions sont établies sur le port 22 à l'aide du protocole TCP dans un délai de 250 secondes. Le bloc sera réinitialisé après 250 secondes. Vous pouvez ajouter plus de ports en ajoutant des virgules.

```
PORTEFEUILLE = "22;tcp;5;250,80;tcp;10;300"
```

Une fois terminé, enregistrez le fichier en appuyant sur Ctrl + X et en saisissant Y à l'invite. Démarrez et

activez les services CSF et LFD.

```
$ sudo systemctl start csf lfd
$ sudo systemctl enable csf lfd
```

Vérifiez l'état du service CSF.

```
$ sudo systemctl status csf
? csf.service - ConfigServer Firewall & Security - csf
     Loaded: loaded (/usr/lib/systemd/system/csf.service; enabled; preset: disabled)
     Active: active (exited) since Tue 2023-12-05 13:57:59 UTC; 2min 7s ago
   Main PID: 11050 (code=exited, status=0/SUCCESS)
        CPU: 1.192s

Dec 05 13:57:59 csf.example.com csf[11050]: ACCEPT  all opt    in * out lo  ::/0  -> ::/0
Dec 05 13:57:59 csf.example.com csf[11050]: LOGDROPOUT  all opt    in * out !lo  ::/0  -> ::/0
Dec 05 13:57:59 csf.example.com csf[11050]: LOGDROPIN  all opt    in !lo out *  ::/0  -> ::/0
Dec 05 13:57:59 csf.example.com csf[11050]: csf: FASTSTART loading DNS (IPv4)
Dec 05 13:57:59 csf.example.com csf[11050]: csf: FASTSTART loading DNS (IPv6)
Dec 05 13:57:59 csf.example.com csf[11050]: LOCALOUTPUT  all opt -- in * out !lo  0.0.0.0/0  -> 0.0.0.0/0
Dec 05 13:57:59 csf.example.com csf[11050]: LOCALINPUT  all opt -- in !lo out *  0.0.0.0/0  -> 0.0.0.0/0
Dec 05 13:57:59 csf.example.com csf[11050]: LOCALOUTPUT  all opt    in * out !lo  ::/0  -> ::/0
Dec 05 13:57:59 csf.example.com csf[11050]: LOCALINPUT  all opt    in !lo out *  ::/0  -> ::/0
Dec 05 13:57:59 csf.example.com systemd[1]: Finished ConfigServer Firewall & Security - csf.
```

Vérifiez les ports ouverts lorsque CSF est en cours d'exécution.

```
$ sudo csf -p
Ports listening for external connections and the executables running behind them:
Port/Proto Open Conn  PID/User            Command Line                          Executable
22/tcp     4/6  2     (863/root)          sshd: /usr/sbin/sshd -D [listener] 0... /usr/sbin/sshd
111/tcp    -/-  -     (1/root)            /usr/lib/systemd/systemd --switched-... /usr/lib/systemd/systemd
111/tcp    -/-  -     (642/rpc)           /usr/bin/rpcbind -w -f                /usr/bin/rpcbind
111/udp    -/-  -     (1/root)            /usr/lib/systemd/systemd --switched-... /usr/lib/systemd/systemd
111/udp    -/-  -     (642/rpc)           /usr/bin/rpcbind -w -f                /usr/bin/rpcbind
323/udp    -/-  -     (679/chrony)        /usr/sbin/chronyd -F 2                /usr/sbin/chronyd
```

AUTO_UPDATES - La valeur désactive les mises à jour automatiques. Remplacez-le par une tâche1 si vous souhaitez des mises à jour automatiques. Cela créera un cron qui s'exécutera une fois par jour pour effectuer des mises à jour automatiques et redémarrera le csf et lfd prestations de service.

ETH_DEVICE - Par défaut, CSF filtre le trafic sur toutes les cartes réseau, à l'exception de la carte de bouclage. Si vous souhaitez que les règles s'appliquent seulement au eth0 carte, puis définissez sa valeur sur eth0 .

LF_DAEMON - définissez sa valeur sur 1 pour activer la fonctionnalité de détection d'échec de connexion de CSF.

LF_CSF - définissez sa valeur sur 1 pour activer la fonction de redémarrage automatique de CSF. Il attendra toutes les 300 secondes pour effectuer la vérification.

LF_SELECT - définir sa valeur sur 1 signifie que lorsque l'adresse IP enfreint les règles LFD, elle bloquera uniquement le trafic vers le service que cette connexion IP échoue au lieu de bloquer tout le trafic.

LF_SSHD - définit le nombre de fois après lequel la mauvaise connexion SSH est bloquée.

CT_LIMIT - limite le nombre de connexions d'une seule adresse IP au serveur. Si le nombre de connexions dépasse le valeur définie, l'IP est alors temporairement bloquée.

Étape 7 - Autoriser et bloquer les adresses IP

Bloquer et autoriser les adresses IP est l'une des capacités les plus fondamentales d'un pare-feu. CSF vous permet de refuser (liste noire), d'autoriser (liste blanche) ou ignorez les adresses IP à l'aide des fichiers de configuration csf.deny, csf.allow et csf.ignore.

Ouvrez le fichier à éditer. csf.deny

```
$ sudo nano /etc/csf/csf.deny
```

Les adresses ou plages d'adresses IP bloquées doivent être ajoutées sur une seule ligne. Par exemple, si vous souhaitez bloquer l'adresse IP 1.2.3.4 ainsi que la plage 2.3.*.*, ajoutez-les comme suit.

```
1.2.3.4          2.3.0.0/16
```

Une fois terminé, enregistrez le fichier en appuyant sur Ctrl + X et en saisissant Y à l'invite.
Les adresses IP autorisées doivent être configurées à l'aide du fichier csf.allow. Les adresses IP autorisées sont autorisées même si elles sont bloquées dans le fichier csf.deny.
Ouvrez le fichier csf.allow pour l'éditer.
Ouvrez le csf.autoriser fichier à éditer.

```
$  sudo nano /etc/csf/csf.allow
```

Les adresses IP doivent être ajoutées de la même manière que dans le fichier de blocage.

Les adresses IP ignorées sont exclues des filtres du pare-feu. Elles ne peuvent être bloquées que si elles sont

répertoriées dans le fichier csf.deny. Ouvrir

```
$ sudo nano /etc/csf/csf.ignore
```

Une fois que vous avez effectué toutes les modifications nécessaires, vous devez redémarrer le pare-feu. Utilisez la commande suivante pour le faire.

```
$ sudo csf -r
```

Étape 8 - Protection contre les attaques DDoS

Voyons comment CSF peut aider à se protéger contre les attaques par déni de service distribué (DDoS) en mettant en œuvre les éléments suivants configurations.

Protection contre les inondations SYN

Il s'agit d'un type d'attaque DDoS dans lequel un attaquant envoie un grand nombre de paquets SYN à un serveur. Pour permettre une protection contre de telles attaques, activez les paramètres suivants dans le fichier /etc/csf/csf.conf

```
SYNFLOOD = "1"
SYNFLOOD_RATE = "100/s"
SYNFLOOD_BURST = "150"
```

Cela permettra la protection contre les inondations SYN et configurera les limites de débit et de rafale pour les attaques entrantes. Ces options devraient être activé uniquement si vous êtes soumis à une attaque SYN, car cela ralentira toutes les nouvelles connexions à partir de n'importe quelle adresse IP.

Listes de blocage

CSF s'intègre à diverses listes de blocage basées sur IP pour empêcher les adresses IP malveillantes de se connecter au serveur. CSF déjà stocke la configuration des listes de blocage populaires telles que Spamhaus, Project Honey Pot, BruteForceBlocker, Blocklist.de, Stop Forum Spam, etc. ouvrez le fichier pour le modifiez ici : /etc/csf/csf.blocklists

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

Décommentez les sections suivantes pour activer les listes de blocage 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
```

Une fois terminé, enregistrez le fichier en appuyant sur Ctrl + X et en entrant Y lorsque vous y êtes invité. Vous pouvez également ajouter votre liste de blocage. Le format pour inclure une nouvelle liste est la suivante.

```
NAME|INTERVAL|MAX|URL
```

NOM - est le nom de la liste avec tous les caractères majuscules sans espaces et un maximum de 25 caractères.

INTERVALLE - intervalle d'actualisation pour télécharger la liste. Cela devrait durer au moins 3 600 secondes.

MAX - nombre maximum d'adresses IP à utiliser dans la liste. Une valeur de 0 signifie toutes les adresses IP.

URL - l'URL à partir de laquelle télécharger la liste.

Blocage au niveau du pays

CSF vous permet de bloquer l'accès depuis des pays spécifiques. Cela peut être utile lorsque vous souhaitez restreindre l'accès depuis des pays connus pour lancer des attaques DDoS. Il existe deux méthodes permettant à CSF de faire correspondre les adresses IP aux pays. La méthode par défaut utilise DB-IP, ipdeny.com et iptoasn.com comme sources. Ils sont gratuits et ne nécessitent pas de clé de licence mais peuvent ne pas être fiables. Si tu veux blocage précis, vous avez besoin d'une clé de licence MaxMind. MaxMind fournit également une licence gratuite. Vous pouvez les utiliser. Une fois que vous disposez de la clé de licence, configurez les deux paramètres suivants dans le fichier /etc/csf/csf.conf

```
MM_LICENSE_KEY = "XXXXXXXXXX"
CC_SRC = "1"
```

Une fois que vous avez configuré cela, utilisez la configuration suivante pour bloquer les adresses IP de Russie.

```
CC_DENY = "RU"
```

Vous pouvez utiliser le paramètre suivant pour autoriser les connexions uniquement à partir de pays spécifiques.

```
CC_ALLOW_FILTER = "EN, GB"
```

Ce paramètre configure les connexions uniquement depuis l'Inde et le Royaume-Uni (UK). Enregistrez et fermez le fichier lorsque vous avez terminé.

Redémarrez le pare-feu une fois la configuration terminée.

```
$ sudo csf -r
```

Il existe d'autres moyens de prévenir les attaques DDoS, comme l'inondation de ports et la limite de connexion, dont nous avons déjà parlé à l'étape 6.

Étape 9 - Commandes CSF couramment utilisées

Active et démarre CSF.

```
$ sudo csf -e
```

Désactive le CSF.

```
$ sudo csf -x
```

Démarrez les règles de pare-feu.

```
$ sudo csf -s
```

Vider/arrêter les règles du pare-feu.

```
$ sudo csf -f
```

Redémarrez le pare-feu.

```
$ sudo csf -r
```

Ajoute l'adresse IP à la liste d'interdiction temporaire. (/var/lib/csf/csf.tempban)

```
$ sudo csf -td 1.2.3.4
```

Supprime l'adresse IP de la liste d'interdiction temporaire.

```
$ sudo csf -tr 1.2.3.4
```

Supprime toutes les adresses IP des entrées temporaires.

```
$ sudo csf -tf
```

Ajoute l'adresse IP à la liste de refus.

```
$ sudo csf -d 1.2.3.4
```

Supprimez l'adresse IP de la liste de refus.

```
$ sudo csf -dr 1.2.3.4
```

Supprime toutes les adresses IP de la liste de refus.

```
$ sudo csf -dr
```

Permet une adresse IP.

```
$ sudo csf -a 1.2.3.4
```

Supprime une adresse IP de la liste verte.

```
$ sudo csf -ar 1.2.3.4
```

Recherche dans les règles iptables et ip6tables une adresse IP, un CIDR et un numéro de port.

```
$ sudo csf -g 1.2.3.4
$ sudo csf -g 80
```

Étape 10 - Activer l'interface graphique CSF

CSF est livré avec une interface Web pour gérer le pare-feu. Il est désactivé par défaut. Avant d'activer l'interface graphique, nous devons installez quelques modules Perl supplémentaires.

```
$ sudo dnf install perl-IO-Socket-SSL.noarch perl-Net-SSLeay perl-IO-Socket-INET6 perl-Socket6 -y
```

Open the CSF configuration file.

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

Find the line `UI = "0"` and change its value as below.

```
UI = "1"
```

Modifiez le port sur lequel le panneau Web est accessible. CSF utilise le port 6666 par défaut mais il est bloqué par le navigateur Chrome comme il le qualifie de port dangereux. Par conséquent, nous devons changer sa valeur en autre chose. Choisissez n'importe quel port supérieur à 1024. Pour notre tutoriel, nous utiliserons le port 1037.

```
UI_PORT = "1037"
```

Utilisez la variable suivante pour autoriser uniquement certaines adresses IP à lier au panneau Web. Laissez-le vide pour vous lier à toutes les adresses IP adresses sur le serveur.

```
UI_IP = "1.2.3.4"
```

Configurez les informations d'identification pour le panneau Web.

```
UI_USER = "username"
UI_PASS = "password"
```

Par défaut, CSF n'autorise l'accès au panneau web qu'à partir des adresses IP répertoriées dans le fichier /etc/csf/ui/ui.allow. Si vous souhaitez qu'il soit accessible à partir de toutes les adresses IP, définissez la variable UI_ALLOW à 0.

```
UI_ALLOW = "0"
```

Une fois terminé, enregistrez le fichier en appuyant sur Ctrl + X et en saisissant Y à l'invite.De même, les adresses IP interdites doivent être ajoutées au

fichier /etc/csf/ui/ui.ban.Le panneau web de CSF utilise des certificats auto-signés. Vous pouvez également utiliser les certificats SSL de Let's Encrypt.

Étape 11 - Installer et configurer Let's Encrypt SSL

Nous devons installer Certbot pour générer le certificat SSL. Nous utiliserons le programme d'installation du package Snapd pour cela. Depuis Rocky Linux n'est pas livré avec, installez le programme d'installation Snapd. Il nécessite le référentiel EPEL (Extra Packages for Enterprise Linux) pour fonctionner. Mais comme nous l'avons déjà installé à l'étape 2, nous pouvons directement avancer.

Installez Snapd.

```
$ sudo dnf installer snapd -y
```

Activez et démarrez le service Snap.

```
$ sudo systemctl activer snapd --now
```

Installez le package principal Snap et assurez-vous que votre version de Snapd est à jour.

```
$ sudo snap install core sudo snap actualiser le noyau
```

Créez les liens nécessaires au fonctionnement de Snapd.

```
$ sudo ln -s /var/lib/snapd/snap /snap
$ echo 'export PATH=$PATH:/var/lib/snapd/snap/bin' | sudo tee -a /etc/profile.d/snapd.sh
```

Installez Certbot.

```
$ sudo snap install --classic certbot
```

Utilisez la commande suivante pour vous assurer que la commande Certbot peut être exécutée en créant un lien symbolique vers le répertoire /usr/bin.

```
$ sudo ln  -s /snap/bin/certbot /usr/bin/certbot
```

Vérifiez si Certbot fonctionne correctement.

```
$ certbot --version
certbot 2.7.4
```

Exécutez la commande suivante pour générer un certificat SSL.

```
$ sudo certbot certonly --standalone --agree-tos --no-eff-email --staple-ocsp --preferred-challenges http -m name@example.com -d csf.example.com
```

La commande ci-dessus téléchargera un certificat dans le répertoire /etc/letsencrypt/live/csf.example.com de votre serveur.
Renommez les anciens certificats auto-signés.

```
$ sudo    mv  /etc/csf/ui/server.crt /etc/csf/ui/server.crt.old
$ sudo    mv  /etc/csf/ui/server.key /etc/csf/ui/server.key.old
```

Copiez les certificats SSL générés dans l' annuaire. /etc/csf/ui

```
$ sudo cp /etc/letsencrypt/live/csf.example.com/fullchain.pem /etc/csf/ui/server.crt
$ sudo cp /etc/letsencrypt/live/csf.example.com/privkey.pem /etc/csf/ui/server.key
```

Redémarrez les services CSF et LFD.

```
$ sudo systemctl restart csf lfd
```

Il y a encore une chose que nous devons configurer. Le certificat SSL sera renouvelé automatiquement tous les 90 jours, ce qui signifie que vous devrez copier les certificats manuellement. Nous pouvons cependant automatiser cela.
Créez le fichier /etc/csf/certcopy.sh pour copier les certificats après chaque renouvellement et ouvrez-le pour l'éditer.

```
$ sudo nano /etc/csf/certcopy.sh
```

Collez-y le code suivant.

```
#!/bin/sh
cp -f /etc/letsencrypt/live/csf.example.com/fullchain.pem /etc/csf/ui/server.crt
cp -f /etc/letsencrypt/live/csf.example.com/privkey.pem /etc/csf/ui/server.key
```

Une fois terminé, enregistrez le fichier en appuyant sur Ctrl + X et en entrant Y lorsque vous y êtes invité. Rendre le fichier exécutable.

```
 $ sudo chmod +x /etc/csf/certcopy.sh
```

Ouvrir le fichier /etc/letsencrypt/renewal/csf.example.com.conf pour l'édition.

```
$ sudo nano /etc/letsencrypt/renewal/csf.example.com.conf
```

Ajoutez la ligne suivante en bas.

```
post_hook = /etc/csf/certcopy.sh
```

Une fois terminé, enregistrez le fichier en appuyant sur Ctrl + X et en entrant Y lorsque vous y êtes invité. Cela post_hook l'option exécute le certcopy.sh scénario après chaque renouvellement, éliminant ainsi le besoin de copier les certificats manuellement.

Vérifiez le service de planification de renouvellement Certbot.

```
$ sudo systemctl list-timers
```

Tu trouveras snap.certbot.renew.service comme l'un des services dont l'exécution est planifiée.

```
NEXT                        LEFT        LAST                        PASSED     UNIT                         ACTIVATES
-------------------------------------------------------------------------------------------------------------------------
Wed 2023-12-06 07:23:57 UTC 18min left Wed 2023-12-06 06:04:46 UTC 1h 0min ago dnf-makecache.timer          dnf-makecache.service
Wed 2023-12-06 07:24:15 UTC 40min left Wed 2023-12-06 00:00:01 UTC 6h ago      logrotate.timer              logrotate.service
Wed 2023-12-06 18:39:00 UTC 10h left   Wed 2023-12-06 03:25:07 UTC 2h 4min ago snap.certbot.renew.timer     snap.certbot.renew.service
```

Effectuez un essai à sec du processus pour vérifier si le renouvellement SSL fonctionne correctement.

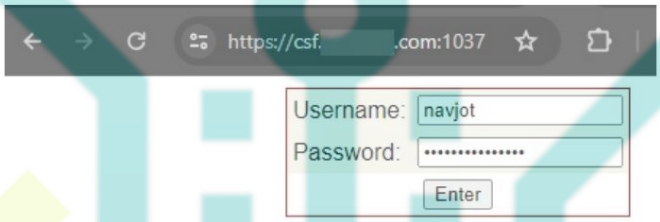
```
$ sudo certbot renew --dry-run
```

Si vous ne voyez aucune erreur, vous êtes prêt. Votre certificat sera renouvelé automatiquement. Les certificats seront copiés et vous pourrez les contrôler en vérifiant la liste du répertoire /etc/csf/ui.

```
$ sudo ls /etc/csf/ui -al
drw-------. 3 root root  130 Dec  6 05:57 .
drw-------. 4 root root 4096 Dec  6 06:09 ..
drw-------. 3 root root 4096 Dec  6 00:06 images
-rw-r--r--. 1 root root 5242 Dec  6 06:09 server.crt
-rw-------. 1 root root 1220 Jun 17  2020 server.crt.old
-rw-------. 1 root root  241 Dec  6 06:09 server.key
-rw-------. 1 root root 1704 Jun 17  2020 server.key.old
-rw-------. 1 root root   15 Dec  5 23:34 ui.allow
-rw-------. 1 root root    0 Feb  1  2013 ui.ban
```

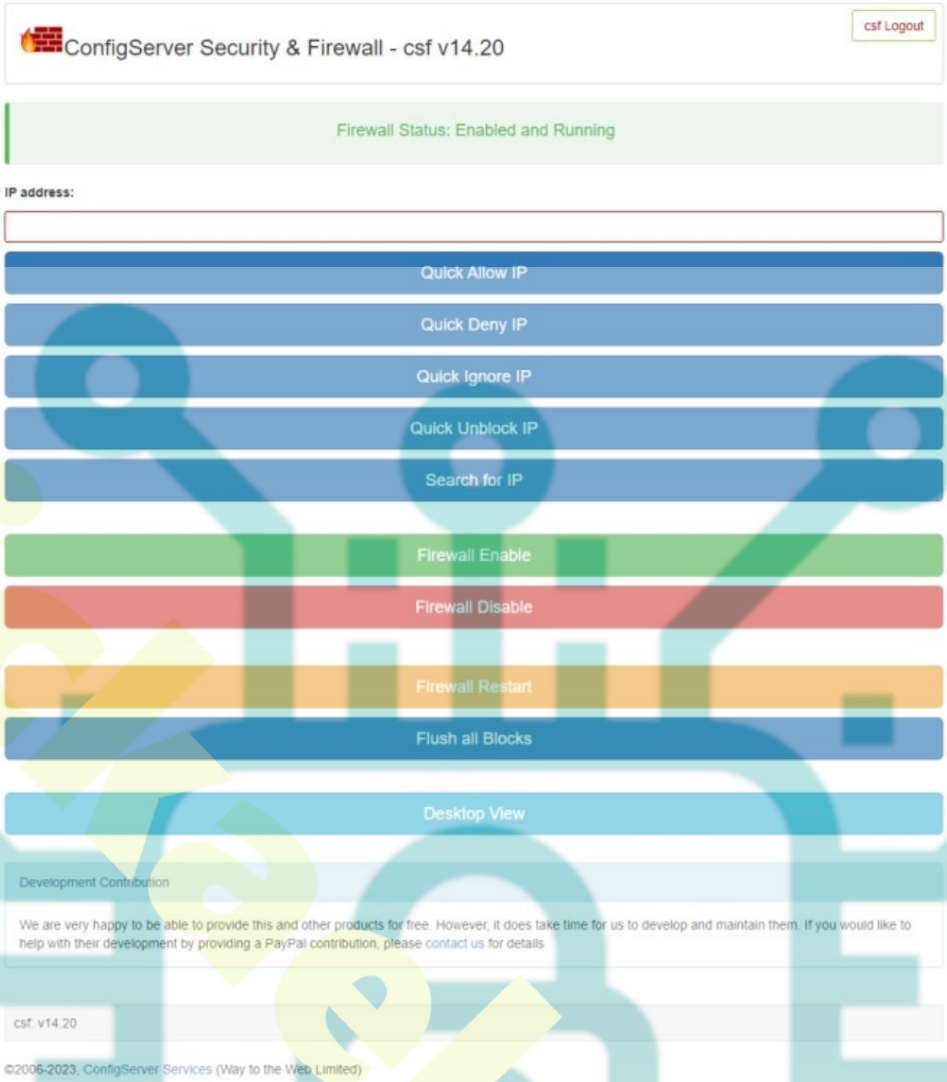
Étape 12 - Accéder au panneau Web CSF

Visitez l'URL https://csf.example.com:1037 et vous serez accueilli par la page de connexion suivante.



Entrez vos informations d'identification et cliquez sur la touche Entrée pour vous connecter et vous obtiendrez la page suivante.

Il est même livré avec une vue mobile vers laquelle vous pouvez basculer à l'aide du bouton Vue mobile .



Le panneau Web vous permet de configurer tous les paramètres du pare-feu. Ce panneau Web s'intègre bien avec d'autres panneaux de contrôle.

Étape 13 - Désinstaller CSF

Si, pour une raison quelconque, vous souhaitez supprimer CSF, vous pouvez exécuter la commande suivante pour exécuter le script de désinstallation.

```
$ sudo sh /etc/csf/uninstall.sh
```

Activez et démarrez le pare-feu Firewalld.

```
$ sudo systemctl enable firewalld --now
```