Firewall as a Service

Service de demande de création de règle Firewall pour ouvrir une machine sur internet. (Ex liste verte)

- Documentation publique
  - Ajouter une règle d'ouverture FWaaS
  - Modifier une règle d'ouverture FWaaS
  - Supprimer une règle d'ouverture FWaaS
  - Demande de liste des règles FWaaS en production
  - Demande de Blacklist

Documentation publique

Documentation publique

Ajouter une règle d'ouverture FWaaS

Firewall as a Service est un système de gestion des demandes d'ouverture de règles Firewall. Il remplace l'ancien système de demande de liste verte sur formulaire papier : https://www.unil.ch/ci/home/menuinst/catalogue-de-services/reseau-et-telephonie/firewall-as-a-service.html

Ce service permet la création, la modification et la suppression de règles rendant accessible une machine sur les ports TCP et UDP ou services désirés.

Pour ajouter une règle :

1. Remplissez le formulaire en indiquant le nom FQDN de la machine concernée : Lien vers le service

2. Pour le service en destination, vous avez deux choix possibles :

   - Service TCP/UDP : Indiquez les ports TCP ou UDP à ouvrir en respectant le format suivant : séparateur virgule "," , plage séparée par "-". Il n'est plus possible d'utiliser ANY.

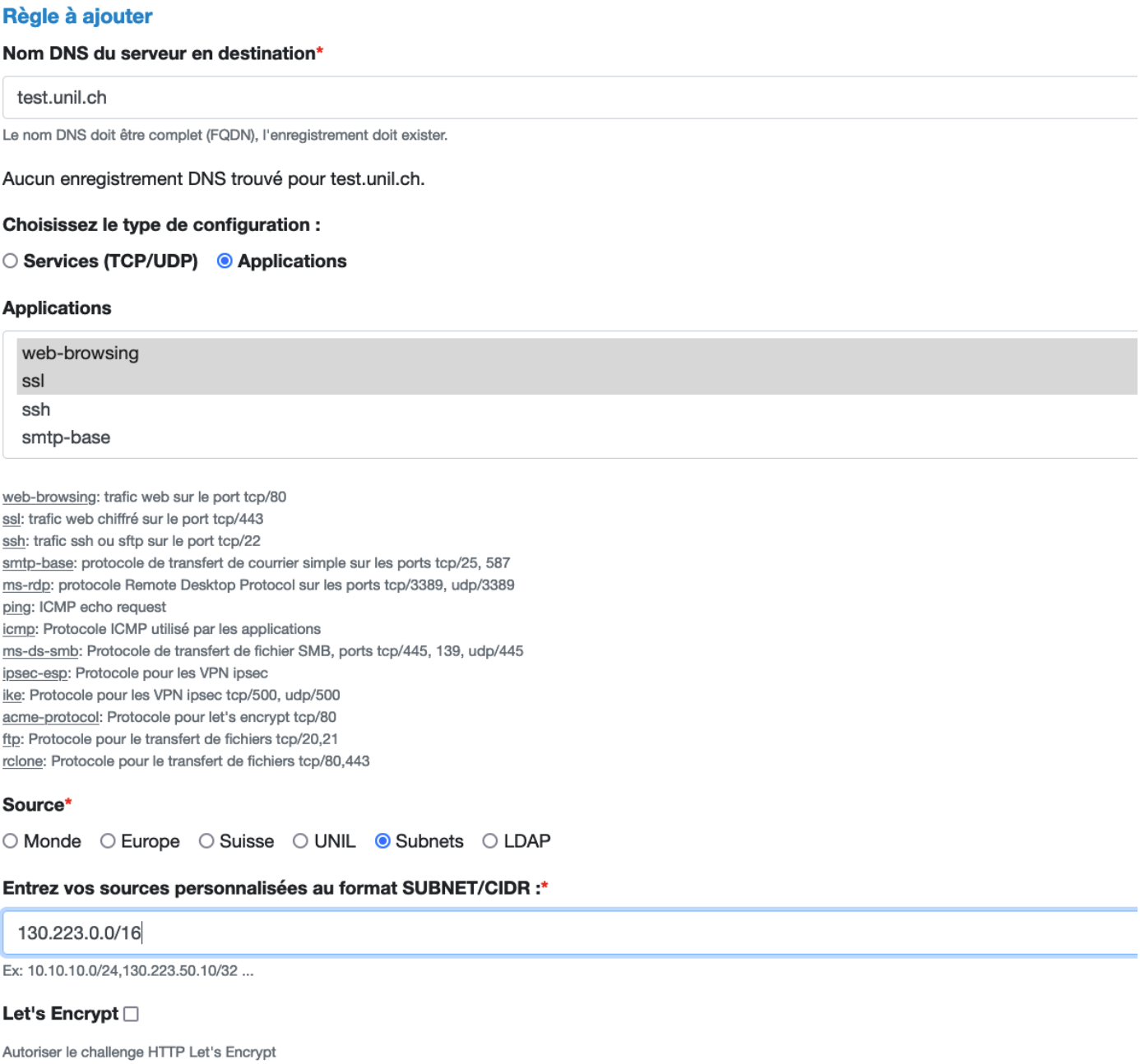
   - Applications : Sélectionnez l'application dans la liste suivante. CTRL+CLIC pour multi sélections.

     > Veuillez noter que seul le port par défaut est autorisé

     - web-browsing : trafic web sur le port tcp/80
     - ssl : trafic web chiffré sur le port tcp/443
     - ssh : trafic ssh ou sftp sur le port tcp/22
     - smtp-base : protocole de transfert de courrier simple sur les ports tcp/25,587
     - ms-rdp : protocole Remote Desktop Protocol sur les ports tcp/3389, udp/3389
     - ping : ICMP echo request
     - icmp : Protocole ICMP utilisé par les applications
     - ms-ds-smb : Protocole de transfert de fichier SMB, ports tcp/445,139, udp/445
     - ipsec-esp: Protocole pour les VPN ipsec
     - ike : Protocole pour les VPN ipsec tcp/500, udp/500
     - acme-protocol : Protocole pour let's encrypt tcp/80
     - ftp : Protocole pour le transfert de fichiers tcp/20,21

    - rclone : Protocole pour le transfert de fichiers tcp/80,443
3. Indiquez la source qui accède à la machine :

    - WORLD : Tout Internet
    - EUROPE : Union Européenne + Royaume-Uni + Suisse
    - SUISSE : Seulement la Suisse
    - UNIL : Les réseaux de l'UNIL
    - OTHER : Vous pouvez mettre une liste de sous-réseaux au format IP/CIDR. Exemple : 192.168.1.1/24 pour un sous-réseau, 192.168.1.1/32 pour une adresse IP unique.
    - LDAP : Ouvre seulement à un groupe LDAP en interne de l'UNIL, le groupe doit figurer dans la liste. Pour toute demande d'ajout veuillez contacter le groupe CI-Réseau.



> Avant de soumettre la demande, assurez-vous de lire et de valider les conditionsd'utilisation.

La demande générera un ticket, et le suivi ainsi que l'historique seront accessibles sur https://tickets.unil.ch. La règle associée sera ajoutée après validation, rendant ainsi la machine accessible sur Internet selon la demande.

Documentation publique

Modifier une règle d'ouverture FWaaS

Firewall as a Service est un système de gestion des demandes d'ouverture de règles Firewall. Il remplace l'ancien système de demande de liste verte sur formulaire papier.

Ce service permet la création, la modification et la suppression de règles rendant accessible une machine depuis Internet sur les ports TCP et UDP désirés.

Pour modifier une règle : Lien vers le service

1. Indiquez dans le formulaire le nom FQDN de la machine concernée.
2. Précisez les ports TCP/UDP ou les applications à modifier (voir la documentation pour l'ajout de règles). **Les nouveaux ports ou applications écraseront les anciennes configurations.**
3. Indiquez la source qui accède à la machine. **La nouvelle source remplacera l'ancienne.**

Avant de soumettre la demande, assurez-vous de lire et de valider les conditions d'utilisation. La demande générera un ticket, et le suivi ainsi que l'historique seront accessibles sur https://tickets.unil.ch. La règle associée sera modifiée après validation. Après cette opération, la machine sera accessible sur Internet selon la demande de modification.

Documentation publique

Supprimer une règle d'ouverture FWaaS

Firewall as a Service est un système de gestion des demandes d'ouverture de règles Firewall. Il remplace l'ancien système de demande de liste verte sur formulaire papier.

Ce service permet la création, la modification et la suppression de règles permettant à une machine d'être accessible sur les ports TCP/UDP ou applications désirés.

Pour supprimer une règle, il vous suffit d'indiquer dans le formulaire de suppression le nom FQDN de la machine concernée. La règle associée sera retirée après validation, rendant ainsi la machine non accessible sur Internet : Lien vers le service

Après avoir soumis la demande, un ticket sera généré, et le suivi ainsi que l'historique seront accessibles sur https://tickets.unil.ch.

Documentation publique

Demande de liste des règles FWaaS en production

Firewall as a Service est un système de gestion des demandes d'ouverture de règles Firewall. Il remplace l'ancien système de demande de liste blanche sur formulaire papier : Lien vers le service

La demande de liste des règles permet aux utilisateurs d'obtenir la liste de leurs règles en production.

Le processus est simple : il vous suffit d'envoyer le formulaire de demande, et un courrier électronique automatique contenant la liste au format HTML vous sera envoyé en retour.

Pour les demandes de listes appartenant à une équipe : lors de l'ajout ou de la modification d'une règle FWaaS, vous pouvez ajouter l'appartenance à un email de groupe. Ceci permettra de notifier lors de la demande toutes les règles appartenant à une équipe. Lors de la demande, vous devez renseigner l'email de l'équipe mentionnée.

Pour consulter cette liste, il vous suffit d'ouvrir le fichier HTML à l'aide d'un navigateur (Firefox, Chrome, Safari, Edge, ...).

Veuillez noter que seule la personne propriétaire des règles recevra la demande. Il n'y a pas de notion d'équipe dans ce système. Veillez donc à bien vous organiser pour transférer les règles d'un propriétaire à un autre, afin de conserver une visibilité sur l'ensemble des règles

Documentation publique

Demande de Blacklist

Bienvenue sur le service de Blacklist FWaaS :

Ce service vous permet de prendre le contrôle de la sécurité de notre réseau en blacklistant des adresses IP spécifiques. Mais qu'est-ce que cela signifie et pourquoi devriez-vous utiliser ce service ?

Qu'est-ce que le blacklisting IP ?

Blacklister une adresse IP signifie bloquer toute communication entrante ou sortante depuis ou vers cette adresse. Imaginez cela comme la création d'une liste noire des adresses IP indésirables. Cela peut être nécessaire pour diverses raisons :

1. **Sécurité du réseau :** Si nous identifions une adresse IP associée à des activités malveillantes, nous pouvons la blacklister pour empêcher tout accès non autorisé à notre réseau.
2. **Protection contre les attaques :** En bloquant les adresses IP qui tentent des intrusions, des attaques par déni de service (DDoS) ou des tentatives de piratage, nous renforçons la sécurité de notre réseau.
3. **Prévention des abus :** Nous pouvons également blacklister des adresses IP pour éviter des abus, tels que l'utilisation excessive de la bande passante, le téléchargement excessif de données ou l'accès non autorisé à des ressources sensibles.

Comment utiliser ce service ?

Le formulaire en lien est conçu pour faciliter le processus de blacklisting. Voici comment vous pouvez l'utiliser :

1. **Informations personnelles :** Remplissez d'abord vos informations personnelles, notamment votre nom, prénom, adresse e-mail UNIL, fonction ou titre, institut, faculté ou service auquel vous êtes affilié.
2. **Blacklist à ajouter :** Indiquez l'adresse IP que vous souhaitez blacklister. Vous devez fournir une adresse IP ou un sous-réseau au format "X.X.X.X/XX". Si vous avez besoin d'aide pour trouver cette adresse, n'hésitez pas à nous contacter.
3. **Action :** Sélectionnez l'action que vous souhaitez effectuer, soit "Ajouter" pour blacklister l'adresse IP, soit "Supprimer" pour retirer une adresse de la liste noire existante.
4. **Remarques :** Vous pouvez ajouter des remarques supplémentaires si nécessaire.
5. **Conditions d'utilisation :** Cochez la case pour confirmer que vous avez pris connaissance des conditions d'utilisation de notre service FWaaS.
6. **Envoyer la demande :** Une fois le formulaire rempli, cliquez sur le bouton "Envoyer la demande" pour soumettre votre demande de blacklisting.

Une fois le formulaire reçu, une validation sera effectués par les ingénieurs réseau pour vérifier les informations.

Une fois la confirmation de validation, le blacklist sera effectué automatiquement sous 5 minutes.

En cas de doute ou si vous avez des questions, n'hésitez pas à nous contacter pour obtenir de l'aide. Merci de contribuer à la sécurité de notre réseau en utilisant ce service de blacklisting FWaaS.