

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.

Règle à ajouter

Nom DNS du serveur en destination*

test.unil.ch

Le nom DNS doit être complet (FQDN), l'enregistrement doit exister.

Aucun enregistrement DNS trouvé pour test.unil.ch.

Choisissez le type de configuration :

☐ Services (TCP/UDP) ☒ Applications

Applications

web-browsing
ssl
ssh
smtp-base

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

Source*

☐ Monde ☐ Europe ☐ Suisse ☐ UNIL ☒ Subnets ☐ LDAP

Entrez vos sources personnalisées au format SUBNET/CIDR :*

130.223.0.0/16

Ex: 10.10.10.0/24,130.223.50.10/32 ...

Let's Encrypt ☐

Autoriser le challenge HTTP Let's Encrypt

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 ajoutée après validation, rendant ainsi la machine accessible sur Internet selon la demande.

Révision #20

Créé 14 mars 2023 08:29:19 par Benoit Hervieux

Mis à jour 6 mai 2024 07:24:25 par Benoit Hervieux