

Activation SNMP sur un pare-feu WatchGuard

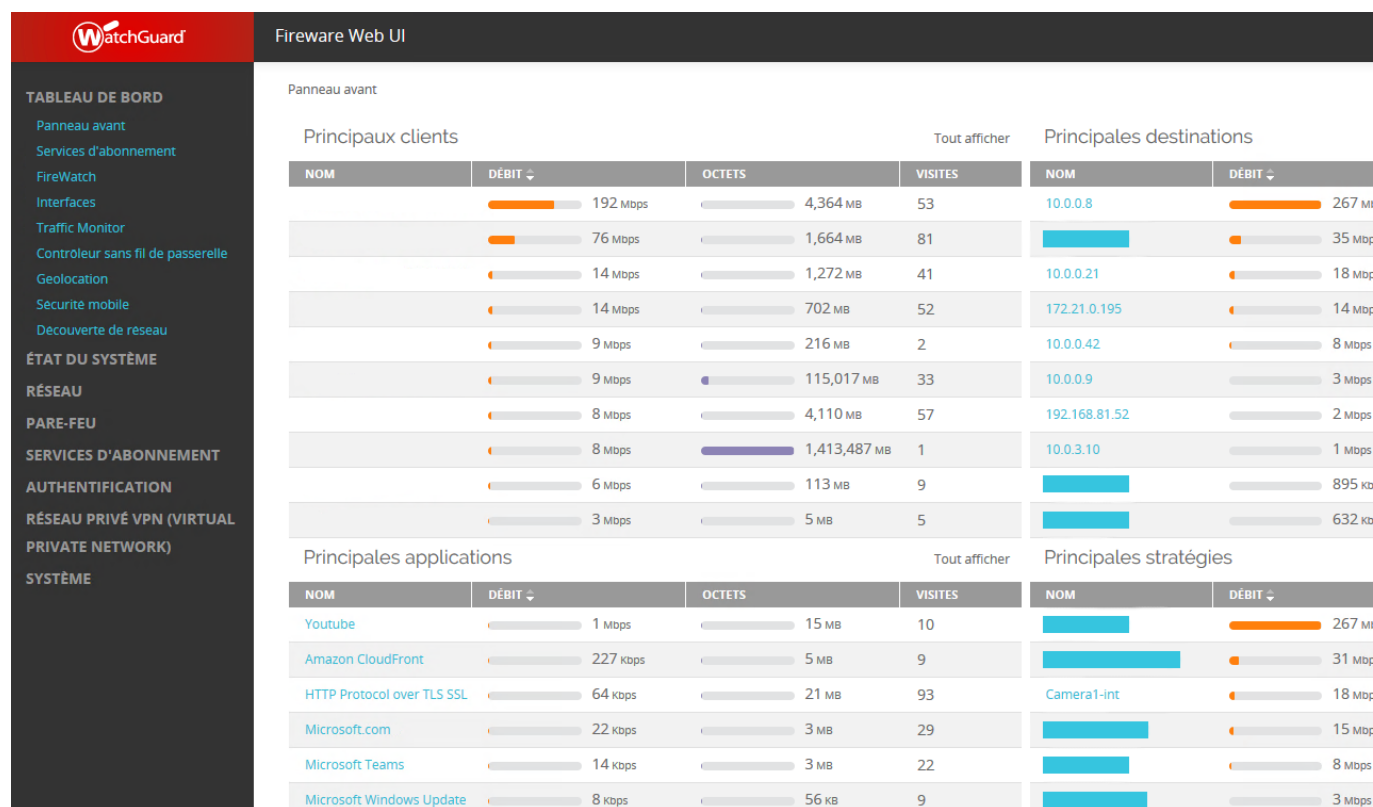
Ce tuto est rendu disponible à l'ensemble de la communauté Esia grâce à la contribution de notre partenaire Premium Computer. Merci à eux.



Leur site: <https://www.premium-computer.fr/>

Via l'interface WEB

Une fois connecté, vous arrivez sur le tableau de bord du pare-feu comme sur l'image ci-dessous.



Cliquez sur « System » et ensuite sur « SNMP », vous arriverez sur la page de configuration SNMP. Comme ci-dessous :

SNMP

Cliquez sur le verrou pour effectuer des changements

Paramètres SNMP

Version: v1/v2c

Chaine de communauté: public

Nom d'utilisateur:

Protocole d'authentification: MD5

Mot de passe:

Confirmer (C):

Protocole de confidentialité: DES

Mot de passe:

Confirmer (C):

INTERRUPTIONS SNMP

Version: v1Trap

Station de gestion SNMP

ADRESSE IP (1)

☒ Utiliser la NAT pour les connexions par ALG (Application Layer Gateway) SNMP

Cliquez sur « Cadenas » en haut à gauche pour déverrouiller la page de configuration et ensuite saisissez les informations dont vous avez besoin (communauté, version SNMP (si v3 l'authentification))

Si vous utilisez les TRAP, vous devez également renseigner les adresses des serveurs autorisés. Suite à la validation de cette fonction, une règle NAT va se créer :

Stratégies de pare-feu / Modifier (E)

Cliquez sur le verrou pour effectuer des changements

Nom: SNMP-Lan-Firebox ☒ Activer

Paramètres SD-WAN Application Control Geolocation Gestion du Trafic Planification Avancées **SNMP**

Les connexions sont: Autorisé

DE

Type de stratégie: SNMP

PORT	PROTOCOLE
161	UDP

A: Firebox

☒ Activer Intrusion Prevention Service
☐ Activer des quotas de bande passante et de durée
☐ Bloquer automatiquement les sites qui tentent de se connecter
☐ Définir un délai d'inactivité personnalisé: 180 secondes

Journalisation

☒ Envoyer un message de journal
☐ Envoyer un message du journal pour les rapports
☐ Envoyer une interruption SNMP
☐ Envoyer une notification
 ☒ E-mail
 ☐ Fenêtre contextuelle
Intervalle de lancement: 15 minutes

Dans le champ DE : rentrer les adresses IP du ou des serveur(s) de supervision

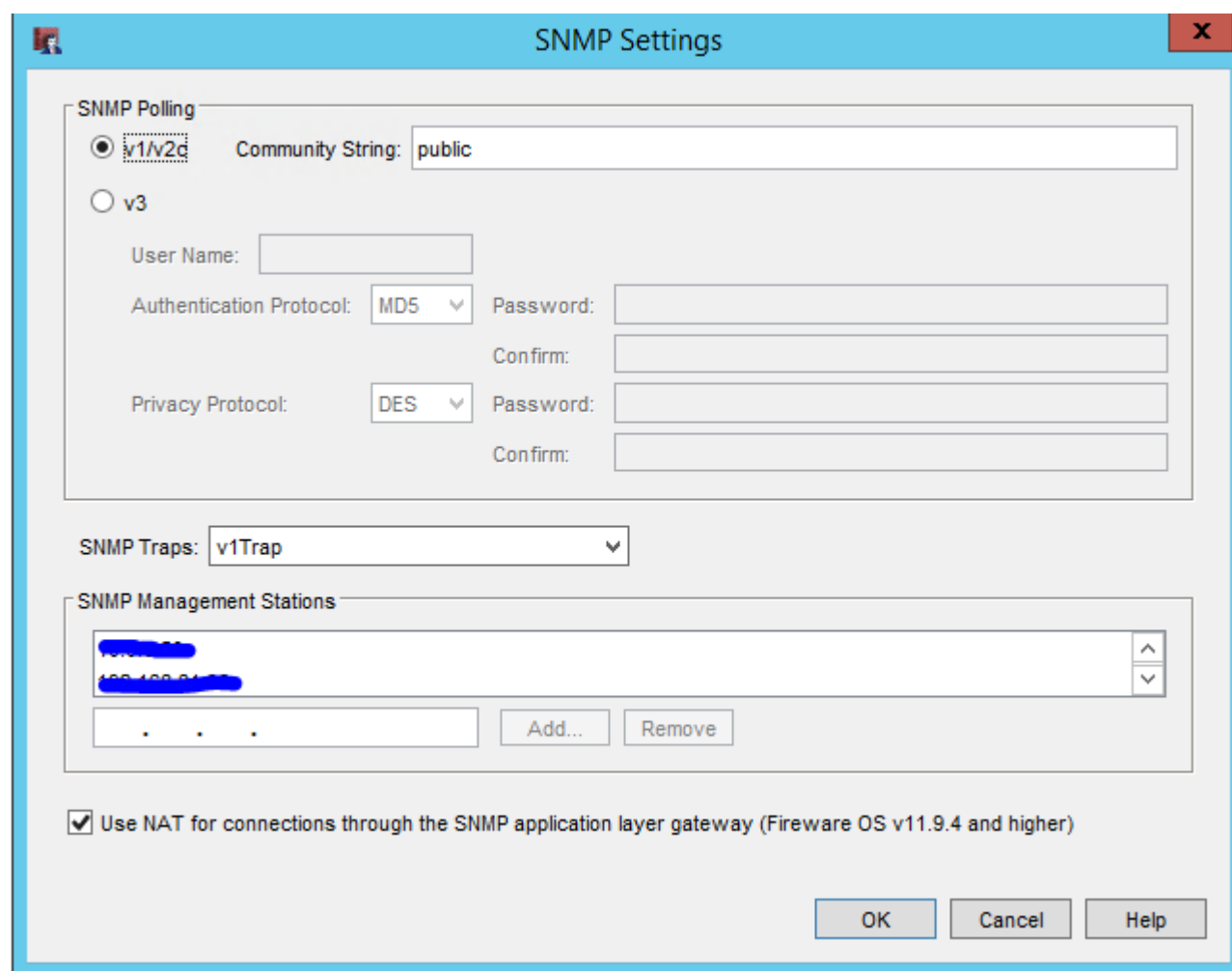
Enregistrez la configuration.

SNMP est maintenant activé sur votre pare-feu WatchGuard.

Via l'interface du client lourd

Une fois que vous avez ouvert le Policy Manager, cliquez sur Setup et SNMP

Configurez ensuite le composant avec vos informations :



The screenshot shows the 'SNMP Settings' dialog box. It has a title bar with a blue background and a red close button. The main area is divided into sections. The 'SNMP Polling' section has two radio buttons: 'v1/v2c' (selected) and 'v3'. The 'Community String' field is set to 'public'. The 'v3' section has fields for 'User Name', 'Authentication Protocol' (MD5), 'Password', 'Confirm', 'Privacy Protocol' (DES), and another 'Password' and 'Confirm' pair. The 'SNMP Traps' section has a dropdown menu set to 'v1Trap'. The 'SNMP Management Stations' section has a list box with two entries: '10.10.10.1' and '10.10.10.2'. Below the list box are 'Add...' and 'Remove' buttons. At the bottom, there is a checkbox labeled 'Use NAT for connections through the SNMP application layer gateway (Fireware OS v11.9.4 and higher)' which is checked. The bottom right corner has 'OK', 'Cancel', and 'Help' buttons.

Une fois validé, modifiez la règle SNMP créer par le firewall en spécifiant les adresses du ou des serveur(s) de supervision

Edit Policy Properties

Name: ☒ Enable

Policy Properties Advanced

SNMP connections are...

From

- [Redacted]
- [Redacted]
- [Redacted]

Add... Edit... Remove

To

- Firebox

Add... Edit... Remove

☐ Route outbound traffic using (Fireware OS v12.3 or higher)

SD-WAN Action

☐ Enable Application Control:

☒ Enable Geolocation:

☒ Enable IPS for this policy

☐ Enable bandwidth and time quotas (Fireware OS v11.10 and higher)

Proxy action:

OK Cancel Help

Cliquez sur OK.

SNMP est maintenant activé

From:
<http://10.8.0.12/> - **Esia Wiki**

Permanent link:
http://10.8.0.12/snmp/snmp_watchguard

Last update: **2023/02/10 10:22**

