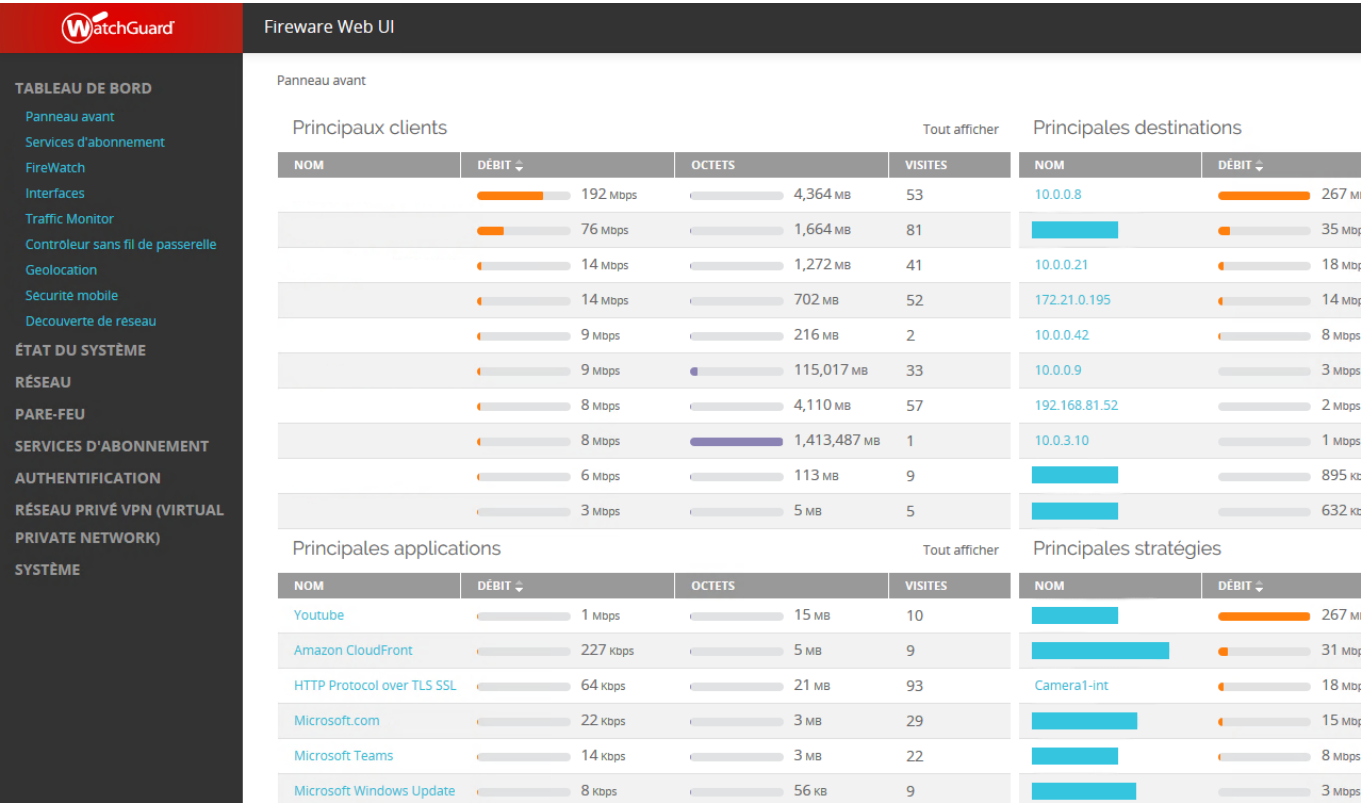


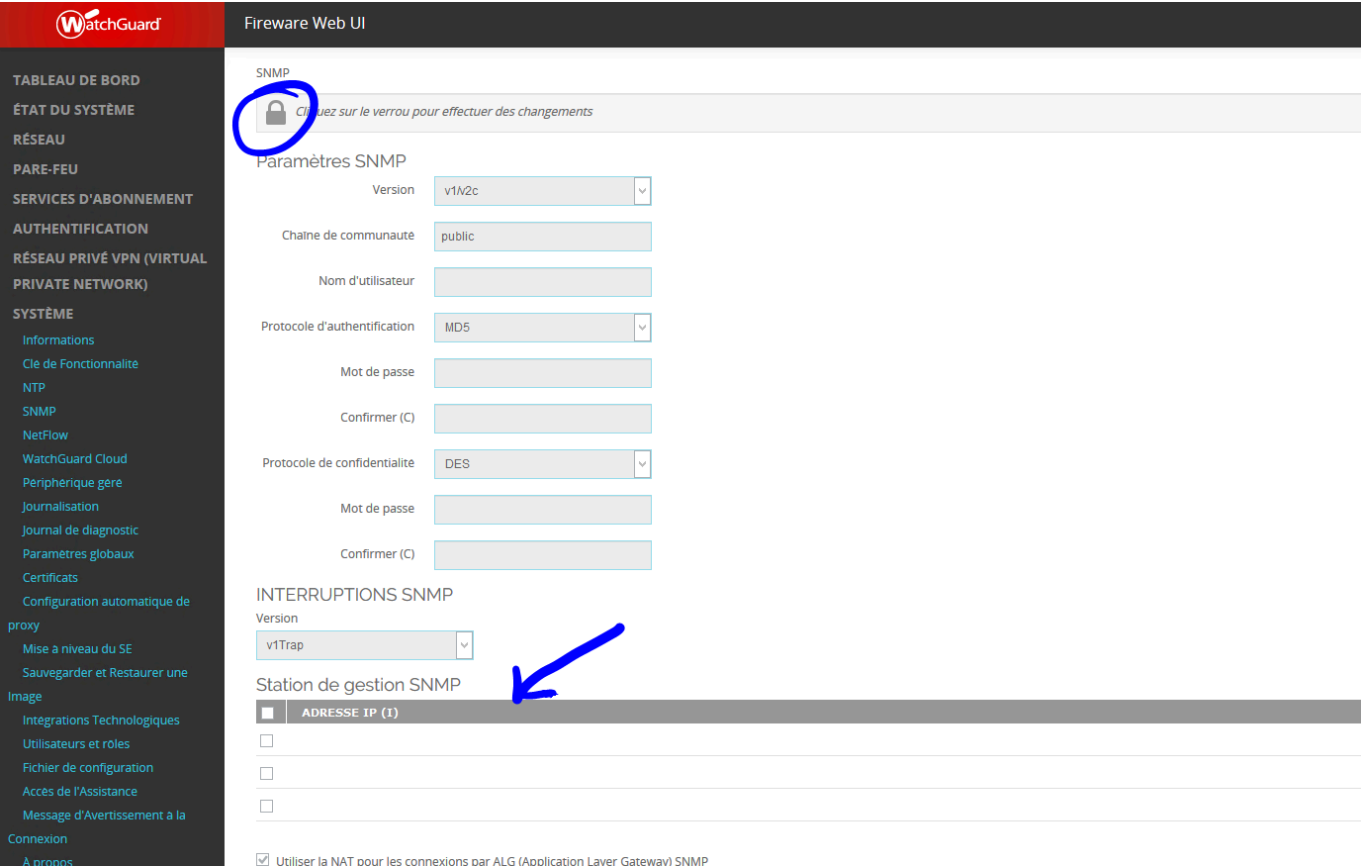
Activation SNMP sur un pare-feu WatchGuard

Via l'interface WEB

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

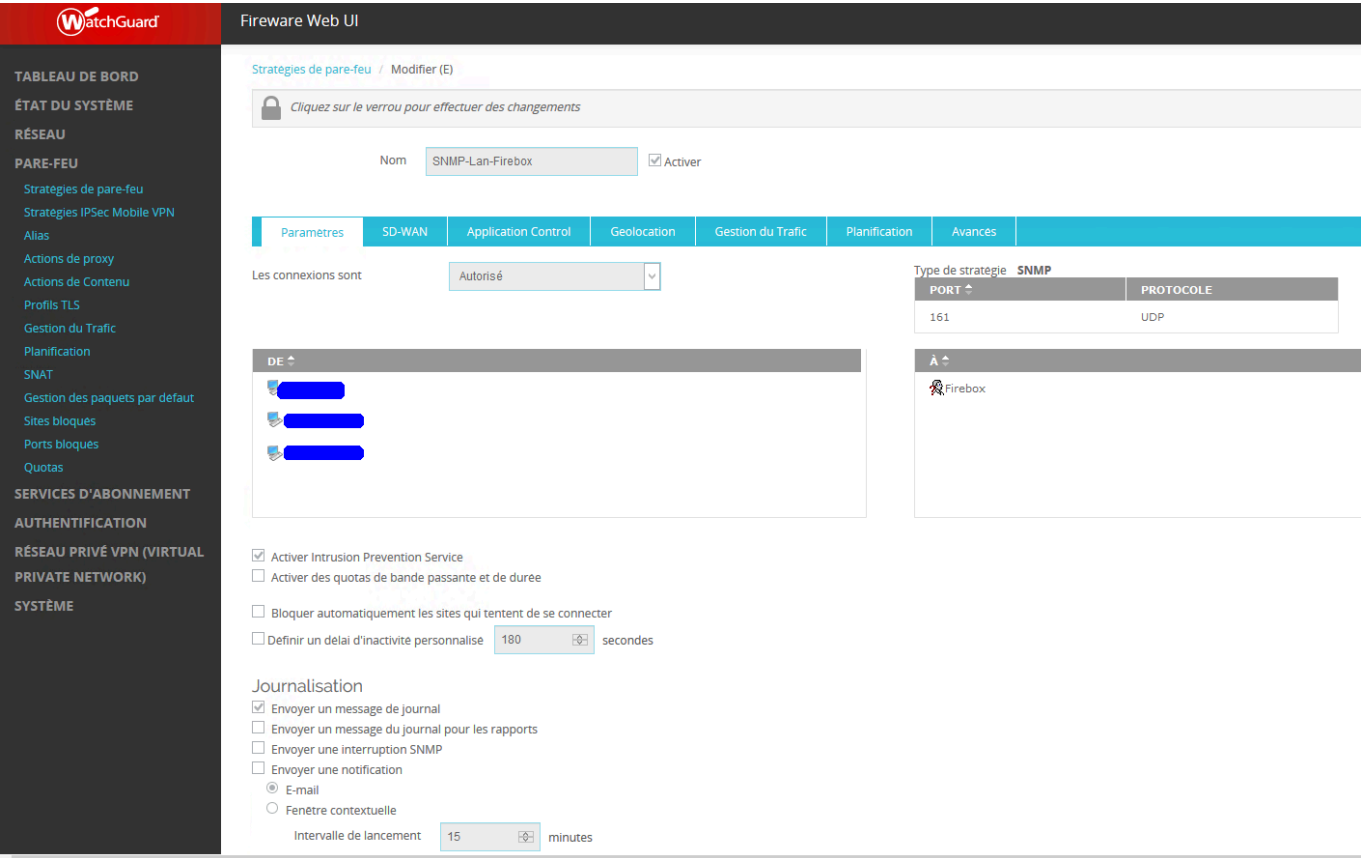


Cliquez sur « System » et ensuite sur « SNMP », vous arriverez sur la page de configuration SNMP. Comme ci-dessous :



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 :



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

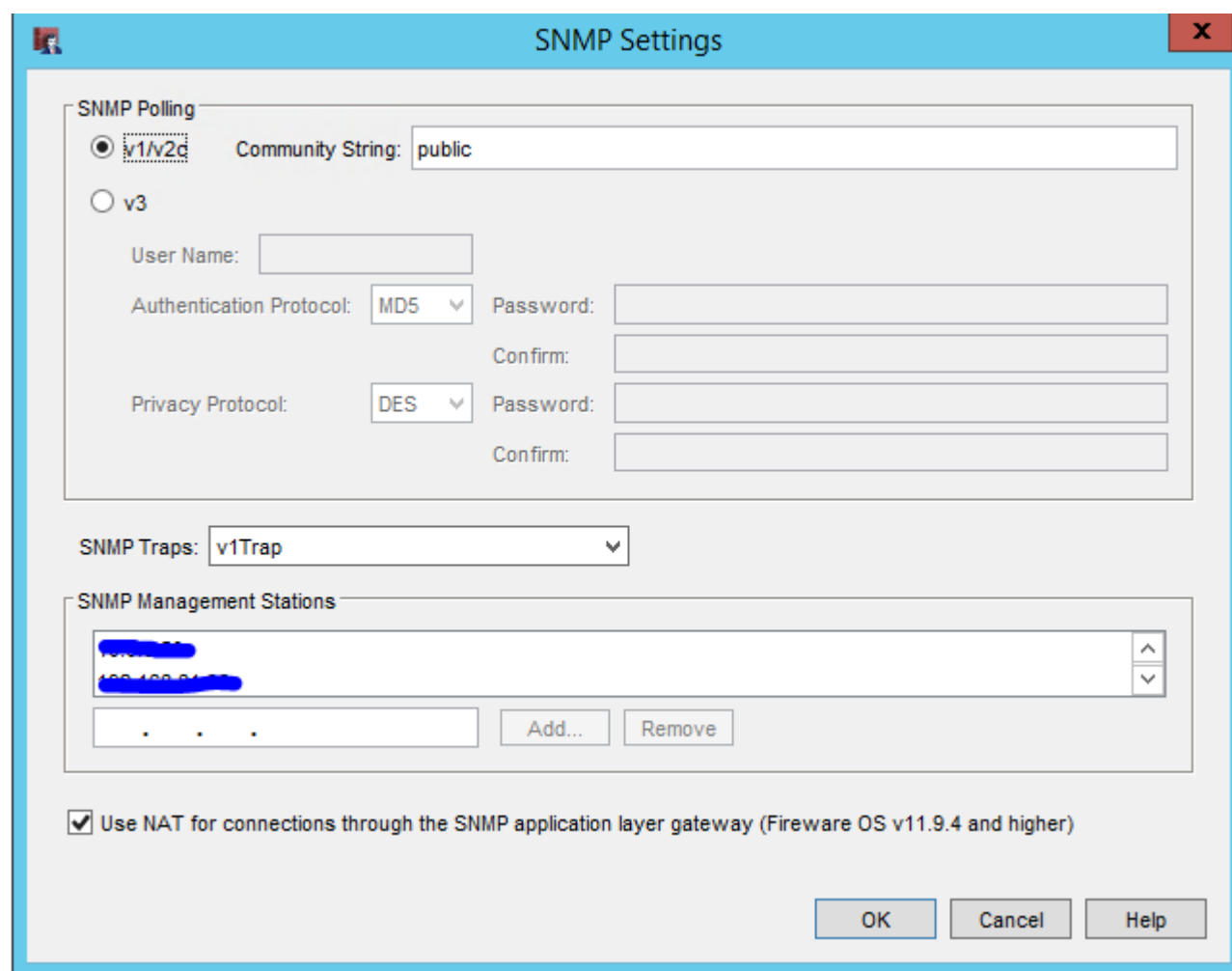
Enregistrez la configuration.

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 'v1/v2c' section includes a 'Community String' field with the value 'public'. The 'v3' section includes fields for 'User Name', 'Authentication Protocol' (set to 'MD5'), 'Password', 'Confirm', 'Privacy Protocol' (set to 'DES'), and another 'Password' and 'Confirm' pair. Below this is the 'SNMP Traps' section with a dropdown menu set to 'v1Trap'. The 'SNMP Management Stations' section features a list box containing two IP addresses: '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 dialog box ends with '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...
Allowed Send TCP RST

From

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

Add... Edit... Remove

To

- Firebox

Add... Edit... Remove

☐ Route outbound traffic using SD-WAN Based Routing (Fireware OS v12.3 or higher)

SD-WAN Action

☐ Enable Application Control: Global

☒ Enable Geolocation: Global

☒ 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:
<https://wiki.esia-sa.com/> - **Esia Wiki**

Permanent link:
https://wiki.esia-sa.com/snmp/snmp_watchguard

Last update: **2025/04/18 13:59**

