

Activation SNMP sur un pare-feu Fortinet

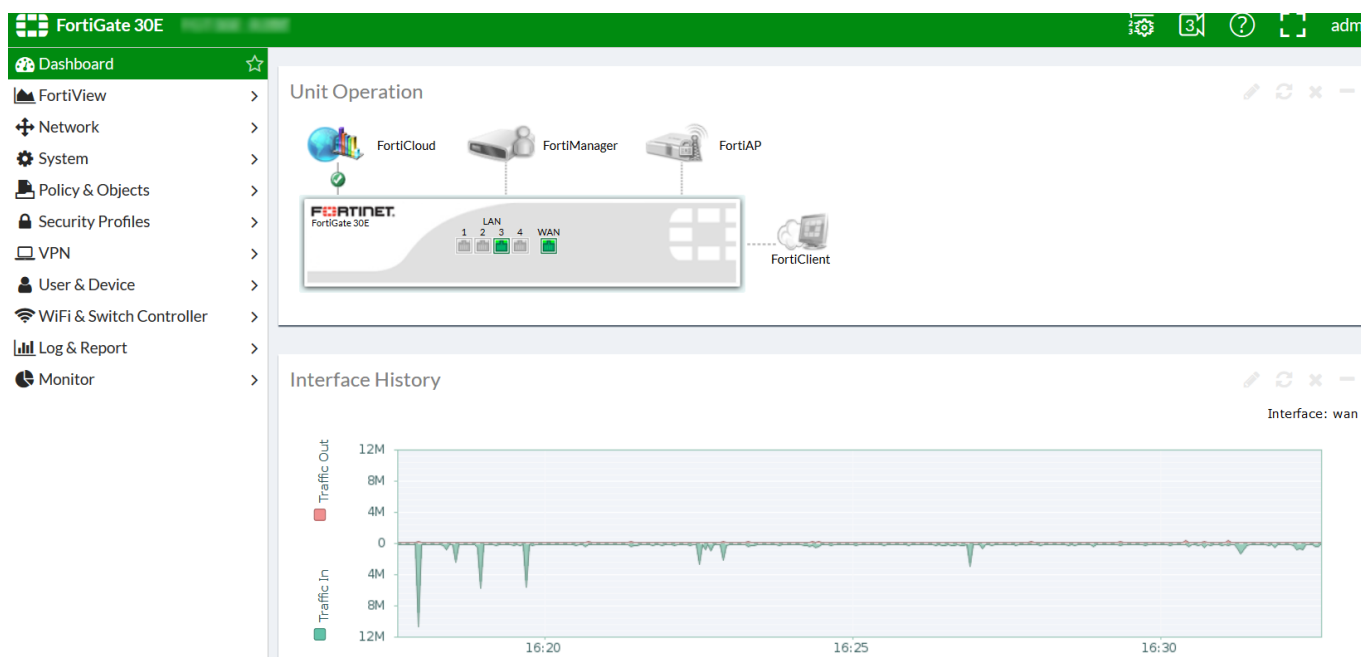


Ce tuto est rendu disponible à l'ensemble de la communauté Esia grâce à la contribution de notre partenaire Rcarre.

Leur site: <https://www.rcarre.com>

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 :

FortiGate 30E

Dashboard
FortiView
Network
System
Administrators
Admin Profiles
Settings
HA
SNMP
Replacement Messages
FortiGuard
Cooperative Security Fabric
Advanced
Feature Select
Policy & Objects
Security Profiles
VPN
User & Device
WiFi & Switch Controller
Log & Report

SNMP Agent

☐ Enable

Description
Location
Contact

Apply

SNMP v1/v2c

Create New Edit Delete

Community Name	Queries	Traps	Enable
----------------	---------	-------	--------

SNMP v3

Create New Edit Delete

User Name	Security Level	Notification Host	Queries
-----------	----------------	-------------------	---------

FortiGate SNMP MIB

[Download FortiGate MIB File](#)
[Download Fortinet Core MIB File](#)

Cochez la case « Enable » et rentrez la description, la location et le contact. Cliquez ensuite sur « Apply ». Il faut maintenant créer la communauté SNMP. Juste en dessous du bouton « Apply », cliquez sur « Create New ».

FortiGate 30E

Dashboard
FortiView
Network
System
Administrators
Admin Profiles
Settings
HA
SNMP
Replacement Messages
FortiGuard
Cooperative Security Fabric

SNMP Agent

☒ Enable

Description: Test
Location: test
Contact: test@test.com

Apply

SNMP v1/v2c

Create New Edit Delete

Community Name	Queries
----------------	---------

SNMP v3

Create New Edit Delete

User Name	Security Level
-----------	----------------

FortiGate SNMP MIB

[Download FortiGate MIB File](#)

Sur la page qui apparaît, indiquez la communauté SNMP, l'adresse IP de votre serveur Esia ou de votre unity dans le champ HOST et cochez les cases comme ci-dessous. Cliquez ensuite sur « Apply ».

FortiGate 30E admin

New SNMP Community

Community Name

Hosts:

IP Address/Netmask	Host Type	Delete
<input type="text"/>	Accept queries and send traps	

Add

Queries:

Protocol	Port	Enable
v1	161	<input checked="" type="checkbox"/>
v2c	161	<input checked="" type="checkbox"/>

Traps:

Protocol	Local	Remote	Enable
v1	162	162	<input checked="" type="checkbox"/>
v2c	162	162	<input checked="" type="checkbox"/>

SNMP Events

<input checked="" type="checkbox"/> CPU usage is high	<input checked="" type="checkbox"/> Memory is low
<input checked="" type="checkbox"/> Log disk space is low	<input checked="" type="checkbox"/> Interface IP is changed
<input checked="" type="checkbox"/> VPN tunnel up	<input checked="" type="checkbox"/> VPN tunnel down
<input checked="" type="checkbox"/> WiFi Controller AP up	<input checked="" type="checkbox"/> WiFi Controller AP down
<input checked="" type="checkbox"/> FortiSwitch Controller Session up	<input checked="" type="checkbox"/> FortiSwitch Controller Session down

Maintenant, il faut autoriser le protocole SNMP sur l'interface LAN de votre pare-feu. Pour ce faire rendez-vous dans le menu « Network » et ensuite « Interface». Il faut ensuite cocher la case SNMP dans « Restrict Access ».

FortiGate 30E admin

Edit Interface

Interface Name: lan

Type: Hardware Switch

Physical Interface Members: lan1, lan2, lan3, lan4

Role: LAN

Address

Addressing mode: Manual | DHCP | PPPoE | Dedicated to FortiSwitch

IP/Network Mask: /255.255.255.0

Restrict Access

Administrative Access: ☒ HTTPS, ☒ SSH, ☒ PING, ☒ SNMP, ☒ HTTP, ☒ FMG-Access, ☒ CAPWAP, ☐ RADIUS Accounting, ☐ FortiTelemetry

DHCP Server

Address Range: Starting IP, End IP

Create New **Edit** **Delete**

Cliquez sur « Apply » pour sauvegarder la configuration.

SNMP est maintenant activé sur votre pare-feu Fortigate.

Via le CLI/SSH

Une fois connecté en SSH, vous pouvez taper les commandes suivantes pour activer SNMP. Vous devez évidemment adapter les champs de description/contact/location.

```
config system snmp sysinfo
set status enable
set description "ce que je veux"
```

```
set contact-info "absent"
set location "Liège"
end
```

SNMP est maintenant activé, il nous faut configurer la communauté SNMP via les commandes suivantes:

```
config system snmp community
  edit 1
    set name "public"
    config hosts
      edit 1
        next
      end
      set events cpu-high mem-low log-full intf-ip vpn-tun-up vpn-tun-down
      ha-switch ha-hb-failure ips-signature ips-anomaly av-virus av-oversize av-
      pattern av-fragmented fm-if-change bgp-established bgp-backward-transition
      ha-member-up ha-member-down ent-conf-change av-conserve av-bypass av-
      oversize-passed av-oversize-blocked ips-pkg-update ips-fail-open faz-
      disconnect wc-ap-up wc-ap-down
    next
  end
```

N'oubliez pas de changer la communauté "public".

From:

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

Permanent link:

https://wiki.esia-sa.com/snmp/snmp_fortinet

Last update: **2025/03/06 14:07**

