

SNMP activation on a Stormshield firewall



This tutorial has been made available to the entire Esia community thanks to the contribution of our partner Ab Network. Many thanks to them.

Their website: <https://www.abnetwork.be/>

Via the WEB interface

Once you have logged in, you will be taken to the firewall dashboard as shown in the image below.

Date	Action	Priority	Source	Destination	Message
09:41:28 AM	Block	Info	Wlan	192.168.1.102	Blocker site user
09:41:28 AM	Pass	Info	Wlan	192.168.1.102	Blocker site user
09:41:28 AM	Pass	Info	Wlan	192.168.1.102	Blocker site user
09:41:24 AM	Block	Info	Wlan	192.168.1.102	Blocker site user
09:41:24 AM	Block	Info	Wlan	192.168.1.102	Blocker site user
09:41:21 AM	Block	Info	Wlan	192.168.1.102	Blocker site user

Click on "Notification" and then on "SNMP Agent" to go to the SNMP configuration page. As shown below:

STORMSHIELD SN300

SN300A admin Read/Write...

SNMP AGENT

GENERAL SNMP V3 (INACTIVE) SNMPV1 - SNMPV2C

Enable the agent

SNMP V3 (recommended)
 SNMP V1 and V2c
 SNMPv1/v2c and SNMPv3

Configuration of MIB-II information

Location (sysLocation) : SN300A
Contact (sysContact) : who@where

Send SNMP alerts (traps)

Intrusion prevention alarms
 do not send
 send only major alarms
 send major and minor alarms

System events
 do not send
 send only major alarms
 send major and minor alarms

Buttons: Apply, Cancel

Tick the “Enable the agent” box and enter the location and contact. Then click on “Apply”.

Now you need to create the SNMP community. Go to the SNMPV1-SNMPV2 tab

STORMSHIELD SN300

SN300A admin Read/Write...

SNMP AGENT

GENERAL SNMP V3 (INACTIVE) **SNMPV1 - SNMPV2C**

Enable the agent

SNMP V3 (recommended)
 SNMP V1 and V2c
 SNMPv1/v2c and SNMPv3

Configuration of MIB-II information

Location (sysLocation) : SN300A
Contact (sysContact) : who@where

Send SNMP alerts (traps)

Intrusion prevention alarms
 do not send
 send only major alarms
 send major and minor alarms

System events
 do not send
 send only major alarms
 send major and minor alarms

Buttons: Apply, Cancel

On the page that appears, specify the SNMP community and add the destination object. Then click on “Apply”.

SN300A 2.7.0 admin Read/Write...

SNMP AGENT

GENERAL SNMP V3 (INACTIVE) SNMPV1 - SNMPV2C

Connection to the SNMP agent

Community : public

Send SNMPv2c alerts (traps)

LIST OF SNMP SERVERS

Destination server (object)	Port	Community
ABBOX	snmp	public

Send SNMPv1 alerts (traps)

Apply

Now you need to add a rule for the SNMP protocol to your firewall. Click on Objects and then on “New Rules”.

SN300A1 2.7.0 admin Read/Write...

FILTER - NAT

(5) prophac prog jour Activate this policy | Edit |

FILTERING NAT

Searched text + New rule Up Down Reset rules statistics

	Status	Action	Source	Src. port	Destination	Dest. port
66	on	pass	ABBOX	Any	Firewall_In	snmp

Page 1 of 2 Couper Ctrl+X Copier Ctrl+C Coller Ctrl+V Save and apply Cancel

https://prophac.dyndns.org:10443/admin/admin.html?nc=1614257579127#

Click on “Save and apply”, SNMP is now configured on your Stormshield firewall.

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

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

Last update: 2025/03/06 14:11

