

Network

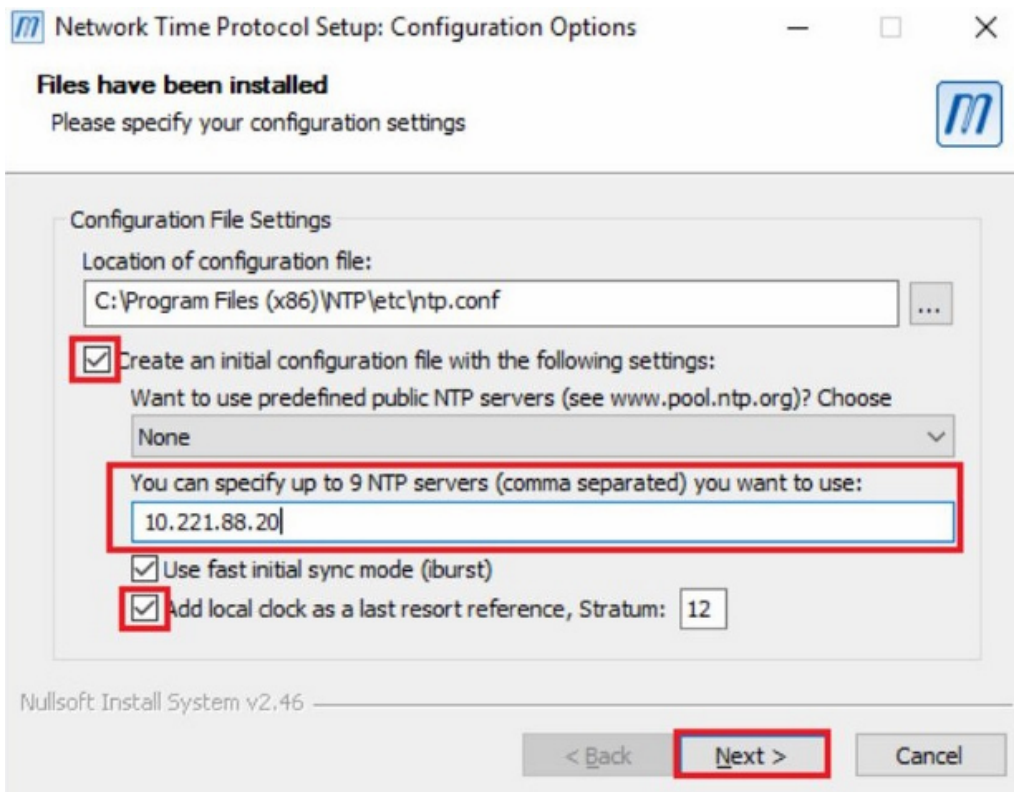
- NTP
 - Client meinberg (Windows)
 - Meinberg
- FIREWALL
 - Modification host SQUID
 - Modification Url Squid
 - Stormshield modification d'une règle
- HPE
 - Mise à jour des OS d'un switch HPE
- CISCO
 - Commandes
 - Configurer le service SNMP
- Calcul Subnet Mask

NTP

Client meinberg (Windows)

Installation du last exe stable [Meinberg NTP Software Downloads \(meinbergglobal.com\)](http://meinbergglobal.com)

1. Check the box and enable "Create an initial configuration file with the following settings:



Definir l'ip du NTP

Recupere le fichier conf

Meinberg

Cette article est divisé en 3 parties :

1. Configuration FROM SCRATCH
2. Import configuration
3. Reset Configuration

Brancher le port management au pc

Se connecter à l'adresse ip obtenu en dhcp via le navigateur web.

Utiliser les logins par défaut « root » et mdp « timeserver »

Une fois connecté aller dans [Network / Network Interfaces](#) et définir l'adresse ip, sa gateway et son mask.

The screenshot shows the 'LANTIME - Network' interface. The 'Network Interfaces' section is expanded, showing configuration for 'Interface 01 - lan0:0'. The 'IPv4' tab is selected. The configuration includes:

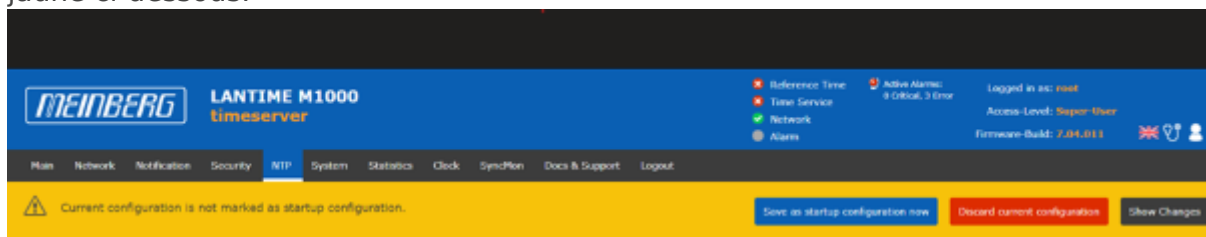
- TCP/IP address: 212.59
- Netmask: 255.255.255.224
- Gateway: 212.60
- Enable DHCP-Client

Remonté dans main Network information et définir le hostname

The screenshot shows the 'LANTIME - Network' interface. The 'Main Network Information' section is expanded, showing configuration for:

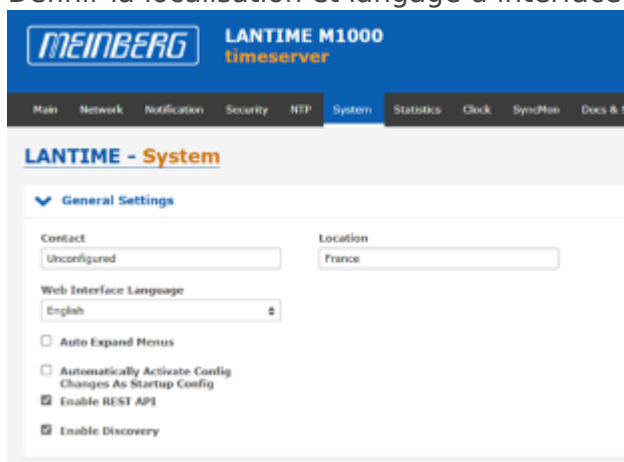
- Hostname: [Redacted]
- Domain: [Empty]
- Nameserver 1: [Empty]
- Nameserver 2: [Empty]

Sauvegarder la configuration et valider le startup configuration comme demandé dans le bandeau jaune ci-dessous.

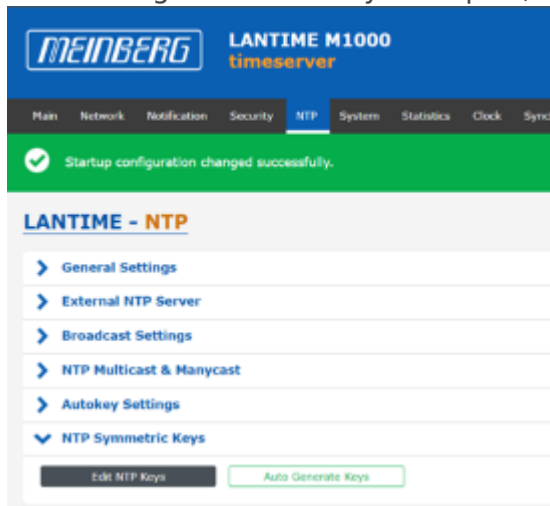


Brancher le ntp à son port switch et se connecter à la nouvelle adresse ip pour continuer les modifications.

Définir la localisation et langage d'interface préféré dans system / General Settings.



Pour Configurer les clés symétriques, aller dans [NTP / NTP Symmetric Keys / Edit NTP Keys](#)

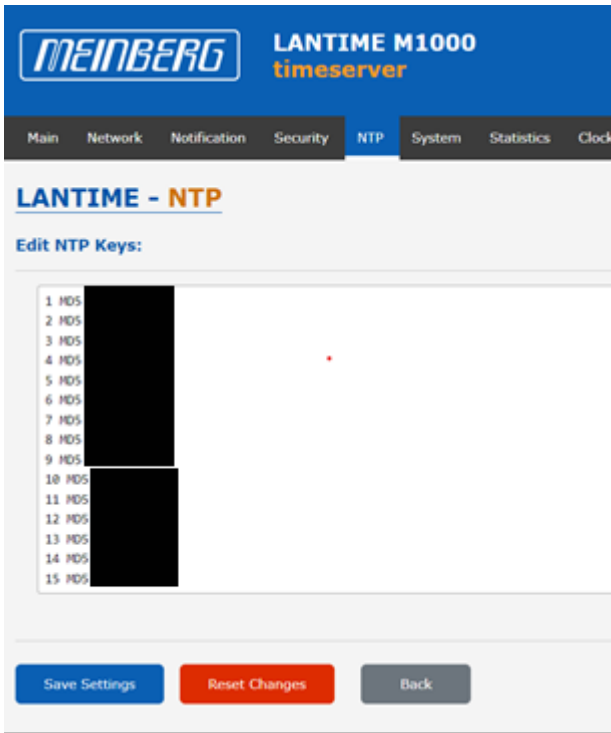


Une fois dans Edit NTP KEYS définir :

KEY ID = XXX

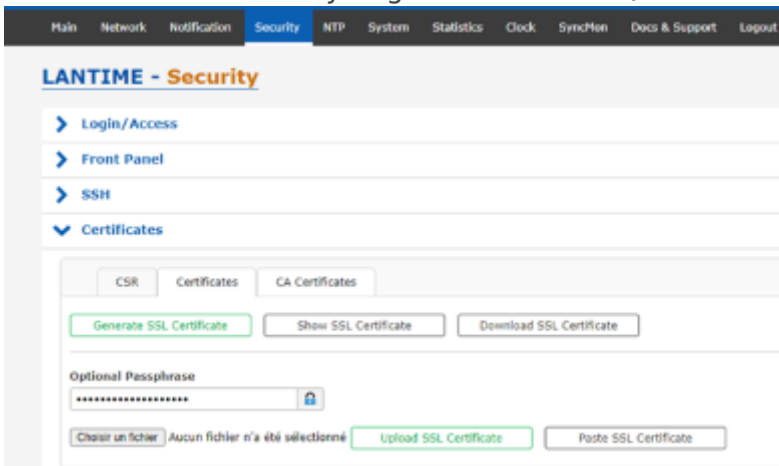
TYPE = MD5 / SHA1

KEY = MOT DE PASSE SOUHAITE

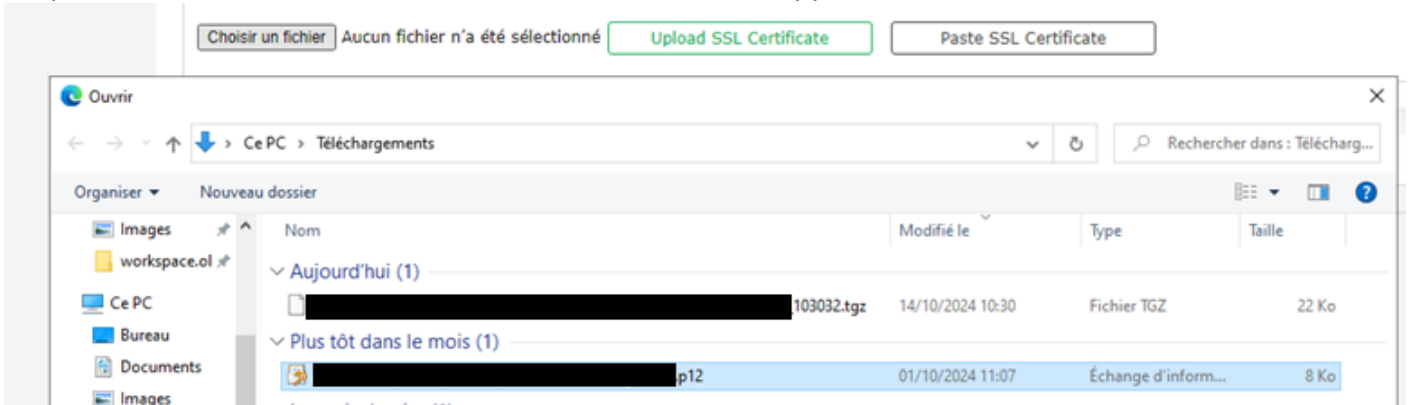


Sauvegarder les changements

Se rendre Dans security onglets Certificates / Certificates




Cliquer sur choisir un fichier, et choisir le certificat en rapport

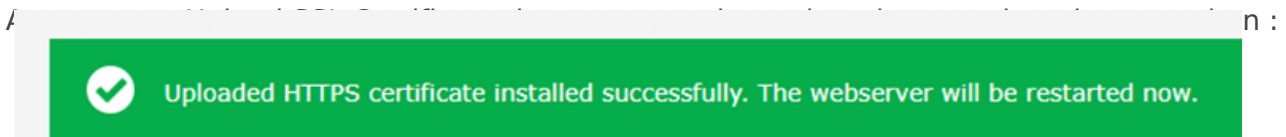


Puis définir le mot de passe du certificats

Optional Passphrase

..... 

Choisir un fichier [redacted]ntp01... [redacted]p12 **Upload SSL Certificate**



Pour vérifier que celui-ci est bien envoyé allez dans Show SSL Certificate

Main Network Notification **Security** NTP System Statistics Clock SyncMon Docs & Support Logout


LANTIME - Security

- > Login/Access
- > Front Panel
- > SSH
- ▼ Certificates

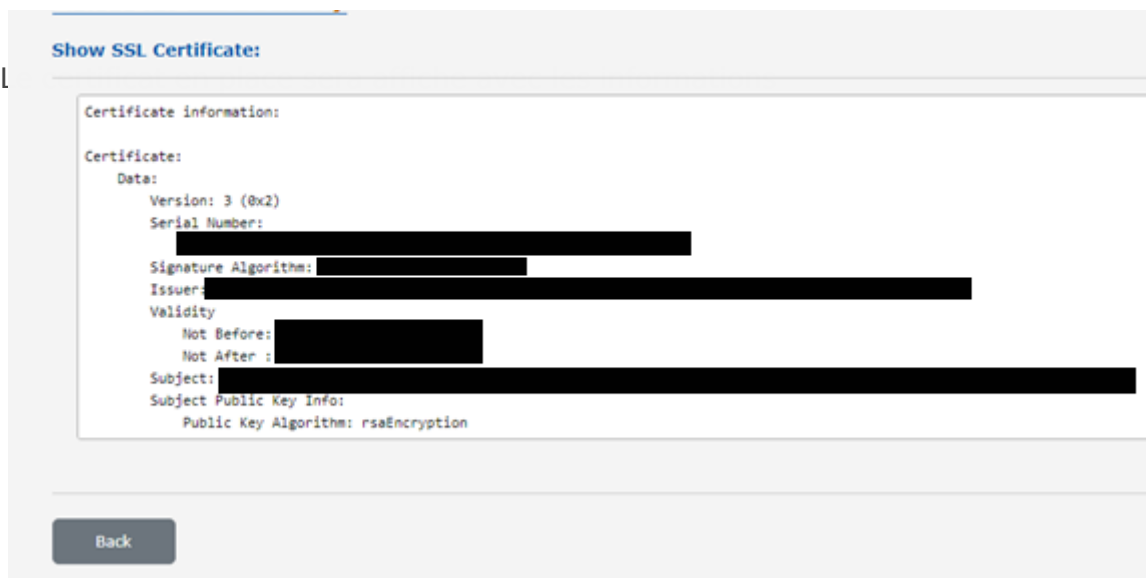
CSR Certificates CA Certificates

Generate SSL Certificate Show SSL Certificate Download SSL Certificate

Optional Passphrase

..... 

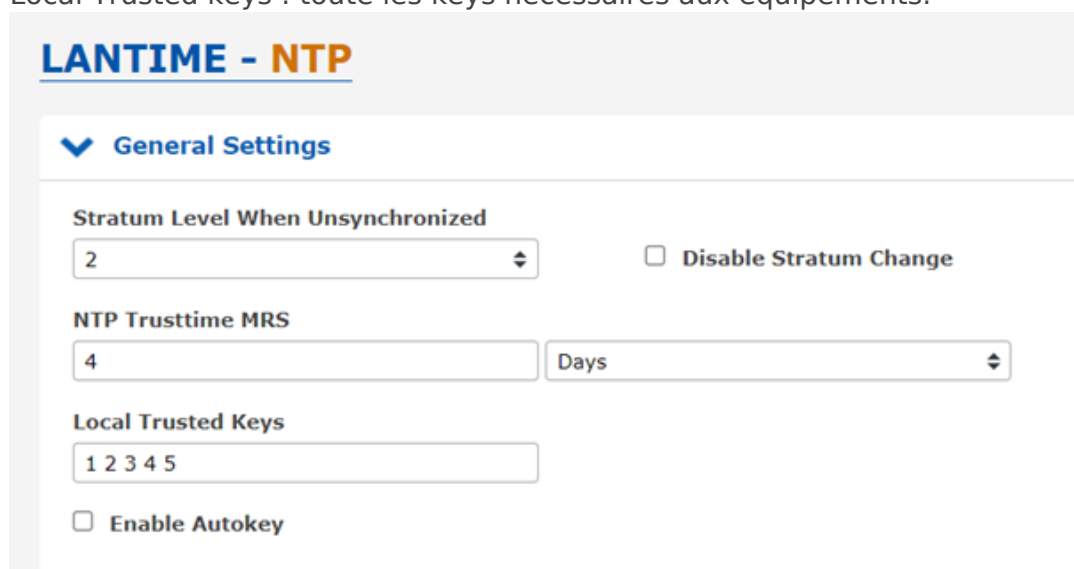
Choisir un fichier Aucun fichier n'a été sélectionné **Upload SSL Certificate** Paste SSL Certificate



Aller dans NTP / General Settings puis définir les paramètres suivant :

Stratum : 2

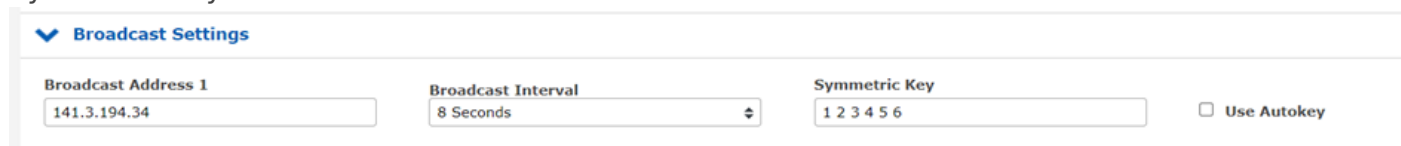
Local Trusted keys : toute les keys nécessaires aux équipements.



Aller dans NTP / Broadcast Settings puis définir les paramètres suivant :

Broadcast Address 1: IP du NTP

Symmetric Key: Les clefs utilisés



Sauvegarder et Valider la sauvegarde au démarrage.

Aller dans Clock / State & Configuration / Timezone
Définir le paramètre sur UTC 0 / UTC

Main Network Notification Security NTP System Statistics **Clock** SyncMon Docs & Support Logout

LANTIME - Clock

▼ State & Configuration

GPS Clock [CLK1 - Sync to OSC]:

MRS State MRS-Settings IRI

Time Zone Enable Outputs M

Time Zone for External Outputs

(UTC+1) - CET/CEST

Edit the time zone table in the display section of the system page. [\(Link\)](#)

Pour modifier l'utilisateur

Main Network Notification Security NTP **System**

LANTIME - System

➤ General Settings

➤ Services and Functions

▼ User Management

User Administration

gement puis cliquer

sur User Administration



Changer le mot de passe par défaut du root et/ou créé un utilisateur

Main Network Notification Security NTP **System** Statistics Clock SyncMon Docs & S

LANTIME - System



User Administration

▼ Change Current User Password

New Password  Confirm Password 

▼ Create User

User Name Group Membership

Password  Confirm Password 

IMPORT CONFIG

Allez dans système onglets Configuration & Firmware Management

▼ Configuration & Firmware Management

Configuration Management

Save Current Configuration As:

Upload Configuration: Aucun fichier n'a été sélectionné

Available Configurations	Options	
startup	<input type="button" value="Activate"/>	<input type="button" value="Delete"/> <input type="button" value="Download"/>

Firmware Management

Running Firmware
OSV

Scheduled Firmware
OSV

Available Firmware Files	Version	Type	Options
OSV (Original Shipped Version)	7.04.011		<input type="button" value="Activate"/> <input type="button" value="Delete"/>

Cliquer sur Choisir un fichier et sélectionner le tgz pour importer la config

Niveau dossier				Modifié le	Type	Taille
Aujourd'hui (1)						
It_backup_config_startup_████████████████████20241014_103032.tgz				14/10/2024 10:30	Fichier TGZ	22 Ko

Une fois sélectionné appuyer sur Upload, le fichier devrait apparaître dans les configurations available puis appuyer sur activate pour charger la configuration

Available Configurations	Options		
startup	Activate	Delete	Download
It_backup_config_startup_████████████████████20241014_103032	Activate	Delete	Download

LANTIME - System

✓ Configuration uploaded successfully

[➤ General Settings](#)

Réinitialisation du NTP

Allez dans System / Services and Functions puis cliquer sur Reset Factory Defaults

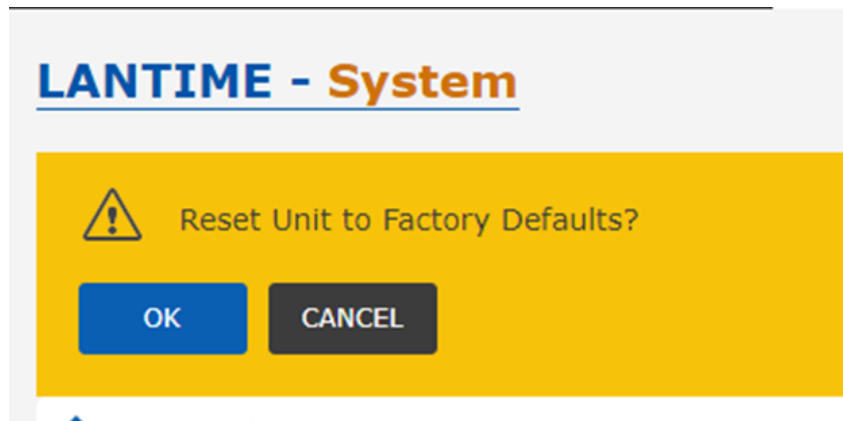
LANTIME - System

[➤ General Settings](#)

▼ Services and Functions

Reboot Device	Reset Factory Defaults
Download SNMP MIB	Send Test Notifications
Resend Current Error Conditions	Save NTP Drift File
Reset Error Relay	Manual Configuration
Activate Physical Identification	Rescan Refclocks
NIC Manager	

Le message suivant apparait appuyer sur OK le ntp execute sa réinitialisation



FIREWALL

Modification host SQUID

Se connecter au serveur squid :

Une fois connecté modifier le fichier contenant les host server

```
sudo su  
nano /etc/squid/host_list/GRP_Linux_Servers
```

```
[root@ ~]# nano /etc/squid/host_list/GRP_Linux_Servers
```

Ajouter ensuite l'@IP comme ci-dessous dans le fichier

```
GNU nano 2.9.8 /etc/squid/host_list/GRP_Linux_Servers  
10.  
10.  
10.
```

une fois le fichier quitter et enregistrer , exécuter la commande suivante :

```
squid -k reconfigure
```

```
[root@ ~]# squid -k reconfigure
```

Vous verrez la liste des ip apparaître comme suivant

```
2025/07/04 15:45:19| WARNING: because of this '10.' is ignored to keep splay tree searching predictable  
2025/07/04 15:45:19| WARNING: You should probably remove '10.' from the ACL named 'Servers'
```

Tester si le serveur peut maintenant passer à travers le proxy.

Modification Url Squid

Se connecter au serveur squid :

Une fois connecté modifier le fichier contenant les host server

```
sudo su
nano /etc/squid/White_liste/Update_Redhat_Centos
```

```
[root@ ~]# nano /etc/squid/host_list/GRP_Linux_Servers
```

Ajouter ensuite l'url comme ci-dessous dans le fichier

```
GNU nano 2.9.8 /etc/squid/white_liste/Update_Redhat_Centos
openseuse.org
.istio.io
.github.io
.quay.io
.fedorainfracloud.org
.gcr.io
.googleapis.com
.rancher.com
.k8s.io
```

une fois le fichier quitter et enregistrer , exécuter la commande suivante :

```
squid -k reconfigure
```

```
[root@ ~]# squid -k reconfigure
```

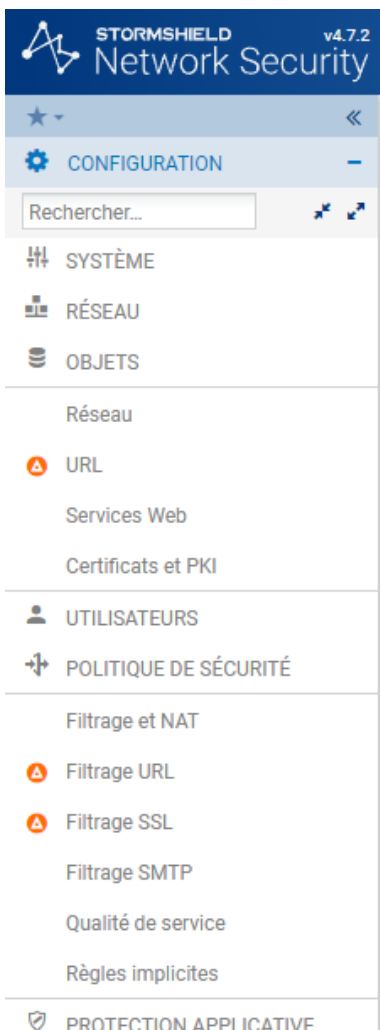
Vous verrez la liste des IP apparaître comme suivant

```
2025/07/04 15:45:19| WARNING: because of this '10.' is ignored to keep splay tree searching predictable
2025/07/04 15:45:19| WARNING: You should probably remove '10.' from the ACL named 'Servers'
```

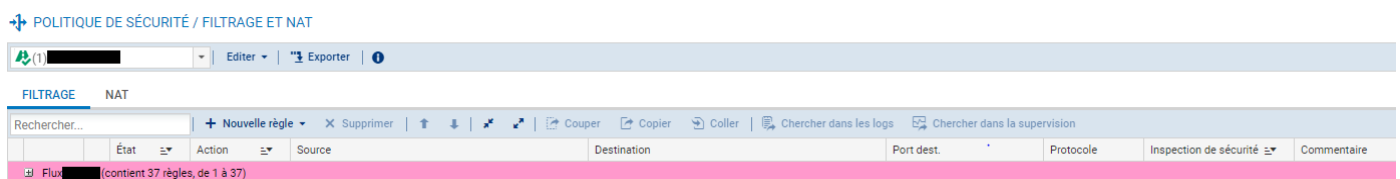
Tester si le serveur peut maintenant accéder à l'url.

Stormshield modification d'une règle

Se connecter au STORMSHIELD et aller dans POLITIQUE DE SECURITE



Créer / chercher la règle à modifier dans la barre



Sélectionner la règle à modifier et faire éditer

Nous allons laisser passer le flux dans celle-ci, donc nous allons choisir **PASSER** dans actions

EDITION DE LA RÈGLE N° 101

Général	ACTION
Action	
Source	GÉNÉRAL QUALITÉ DE SERVICE CONFIGURATION AVANCÉE
Destination	
Port / Protocole	
Inspection	

Général

Action:

Niveau de trace:

Programmation horaire:

Routage

Passerelle - routeur:

Ajoutons les machines/groupes sources

EDITION DE LA RÈGLE N° 101

Général	SOURCE
Action	
Source	GÉNÉRAL GÉOLOCALISATION / RÉPUTATION CONFIGURATION AVANCÉE
Destination	
Port / Protocole	
Inspection	

Général

Utilisateur:

Machines sources:

+ Ajouter X Supprimer

Interface d'entrée:

Services Web et réputations IP

Sélectionnez un service Web ou une catégorie de réputation IP:

Nous devons maintenant ajouter les machines de destination, faire **AJOUTER** et rentrer **I@IP** ou le **NOM** déjà créé dans les **OBJETS** du Stormshield

EDITION DE LA RÈGLE N° 101

Général
Action
Source
Destination
Port / Protocole
Inspection

DESTINATION

GÉNÉRAL GÉOLOCALISATION / RÉPUTATION CONFIGURATION AVANCÉE

Général

Machines destinations:

Services Web et réputations IP

Sélectionnez un service Web ou une catégorie de réputation IP:

Maintenant ajoutons le port que nous souhaitons laisser passer

EDITION DE LA RÈGLE N° 101

Général
Action
Source
Destination
Port / Protocole
Inspection

PORT ET PROTOCOLE

Port

Port destination:

30007
30008

Protocole

Type de protocole:

Protocole applicatif: Basé sur les ports par défaut ou le contenu

Protocole IP: Tous

SI VOTRE OBJET N'EST PAS EXISTANT CREER LE DEPUIS LES 2 PETITES BARRES DANS AJOUTER ET REMPLIR LA FENÊTRE CI DESSOUS

CRÉER UN OBJET

- Machine
- Nom DNS (FQDN)
- Réseau
- Plage d'adresses
- Routeur
- Groupe
- Protocole IP
- Port**
- Groupe de ports
- Groupe de régions
- Objet temps

Nom de l'objet:

Port

Port:

Plage de ports

Depuis:

Jusqu'à:

Protocole:

Commentaire:

une fois cela fait, vérifier que la règle est bien **ON**

EDITION DE LA RÈGLE N° 101

- Général**
- Action
- Source
- Destination
- Port / Protocole
- Inspection

ÉTAT - COMMENTAIRE - NOM

Général


État: On

Commentaire: Créée le 2025-07-04 14:32:09, par [REDACTÉ]

▼ Configuration avancée

En faisant OK la fenêtre suivante apparaîtra il ne vous reste plus qu'à activer celle-ci.

ACTIVER LA POLITIQUE

 Cette politique est la politique active.
Pour appliquer immédiatement les modifications vous devez réactiver la politique.
Voulez-vous activer la nouvelle politique [REDACTÉ] maintenant ?

HPE

HPE

Mise à jour des OS d'un switch HPE

1 - Connecter un PC portable sur le port console de l'équipement

2 - Remettre l'équipement en mode de configuration « usine » :

```
undo startup saved-configuration
```

```
delete startup.cfg
```

```
Y
```

```
delete lauth.dat
```

```
Y
```

```
reboot
```

```
N
```

```
Y
```

3 - Vérifier la version logicielle active sur l'équipement

```
display version
```

4 - Vérifier les versions logicielles autorisées sur l'équipement

```
display boot-loader
```

5 - Si la version logicielle active est autorisée uniquement au seul emplacement « main » ou « backup » alors l'autoriser sur le 2ème emplacement

```
boot-loader file boot flash:/5140ei-cmw710-boot-xxx.bin system flash:/5140ei-cmw710-system-xxx.bin slot 1 main
```

```
Y
```

ou

```
boot-loader file boot flash:/5140ei-cmw710-boot-xxx.bin system flash:/5140ei-cmw710-system-xxx.bin slot 1 backup
```

```
Y
```

6 - Si la version logicielle active ne correspond pas à la version « cible » alors configurer le serveur SFTP sur l'équipement

```
system-view
public-key local create dsa
y
2048
public-key local create rsa
y
2048
```

```
interface vlan-interface 1
ip address (adresse ip) (mask)
undo shutdown
```

```
local-user LOGIN class manage
authorization-attribute user-role network-admin
undo authorization-attribute user-role network-operator
password simple PASSWORD
service-type ssh
state active
```

```
domain system
accounting default none
authentication default local
authorization default local
undo authorization-attribute user-profile
state active
```

```
user-group system
ssh server enable
ssh server authentication-retries 3
ssh server authentication-timeout 60
Undo ssh server compatible-ssh1x
undo ssh server port
```

```
undo scp server enable
sftp server enable
sftp server idle-timeout 5
ssh user LOGIN service-type all authentication-type password
```

```
line vty 0 63
authentication-mode scheme
idle-timeout 5 0
protocol inbound ssh
```

```
return
```

7 - Connecter le PC portable sur un port de l'équipement

8 - Initialiser une session SFTP entre le PC portable (Client) et l'équipement (Serveur)

Remarque : Si le client SFTP utilisé est WinSCP alors sélectionner Options/Préférences/Solidité et désactiver « Autoriser la reprise/transférer vers un fichier temporaire pour » puis cliquer sur OK

9 - Transférer, via le client SFTP, la version logicielle dans la flash de l'équipement au niveau de la « racine »

10 - Vérifier les versions logicielles contenues dans la flash de l'équipement

```
dir flash:/
```

11 - Autoriser la version logicielle téléchargée à l'emplacement « main »

```
boot-loader file flash:/5140ei-CMW710-xxx.ipe slot 1 main
```

```
Y
```

```
Y
```

12 - Redémarrer l'équipement sur la version logicielle téléchargée

```
reboot
```

```
N
```

```
Y
```

13 - Vérifier la version logicielle active

```
display version
```

14 - Autoriser la version logicielle téléchargée à l'emplacement « backup »

```
boot-loader file boot flash:/5140ei-cmw710-boot-xxx.bin system flash:/5140ei-cmw710-system-xxx.bin slot 1 backup
```

```
Y
```

15 - Supprimer les versions logicielles non utilisées contenues dans la flash de l'équipement

```
delete flash:/5140ei-cmw710-boot-xxx.bin
```

```
Y
```

```
delete flash:/5140ei-cmw710-system-xxx.bin
```

```
Y
```

CISCO

CISCO

Commandes

Enregistrer la configuration active

```
write
```

Afficher la configuration active

```
show running-config
```

Informations matériels du switch

```
show version
```

Découvrir les équipements connectés

```
show cdp neighbors
```

Afficher les informations des PoE

```
show power inline
```

Afficher les différents TRUNK

```
show interfaces trunk
```

Afficher le détail des VLANs

```
show vlan
```

Créer un VLAN

```
enable  
conf t  
vlan 2  
vlan 2
```

Supprimer un VLAN

```
enable  
conf t  
vlan 2  
no vlan 2
```

Réinitialiser par défaut une interface

```
enable  
conf t  
default interface range GigabitEthernet1/0/1 - 48
```

Création d'un teaming LACP

```
enable
conf t
interface range GigabitEthernet1/0/1 - 2
channel-group 1 mode active
channel-protocol lacp
exit
```

```
enable
configure terminal
interface port-channel 1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan add 1
exit
```

Statut de toutes les interfaces

```
enable
show interfaces status
```

statut d'une interface spécifique

```
enable
show interfaces Gi1/0/1 status
```

Désactiver une interface

```
enable
configure terminal
interface gi1/0/1
shutdown
end
```

Modifier l'IP d'une interface

```
enable
configure terminal
interface Vlan3
ip address 192.168.1.2 255.255.255.0
exit
```

Ajouter une passerelle par défaut

```
enable
configure terminal
ip default-gateway 10.0.0.60
```

Modifier un range de port

```
enable
configure terminal
interface range GigabitEthernet1/0/1 - 48
```

Activer une interface

enable

configure terminal

interface gi1/0/1

no shutdown

end

CISCO

Configurer le service SNMP

```
enable
configure terminal
snmp-server community "nom"
snmp-server location "localisation"
snmp-server contact "mail@mail.com"
end
```

```
write
```

Calcul Subnet Mask

Calcul s'effectuant en puissance de 2

Va jusqu'à /32 max

Pour exemple /27

$32 - 27 = 5 > 2$ puissance 5 > 32

Je retire 32 a 256

Mon subnet est en 224