

Sophos XG – Guide d'Installation et de Configuration

Installation

```
FIRMWARE LOADER (press <enter> to display list of images)
```

```
Starting 17_5_1_347.
```

```
Doing Appliance Specific Setting
```

```
Loading firstboot configuration
```

```
Installing default config
```

```
Firstboot completed successfully
```

```
### System Detail ###
```

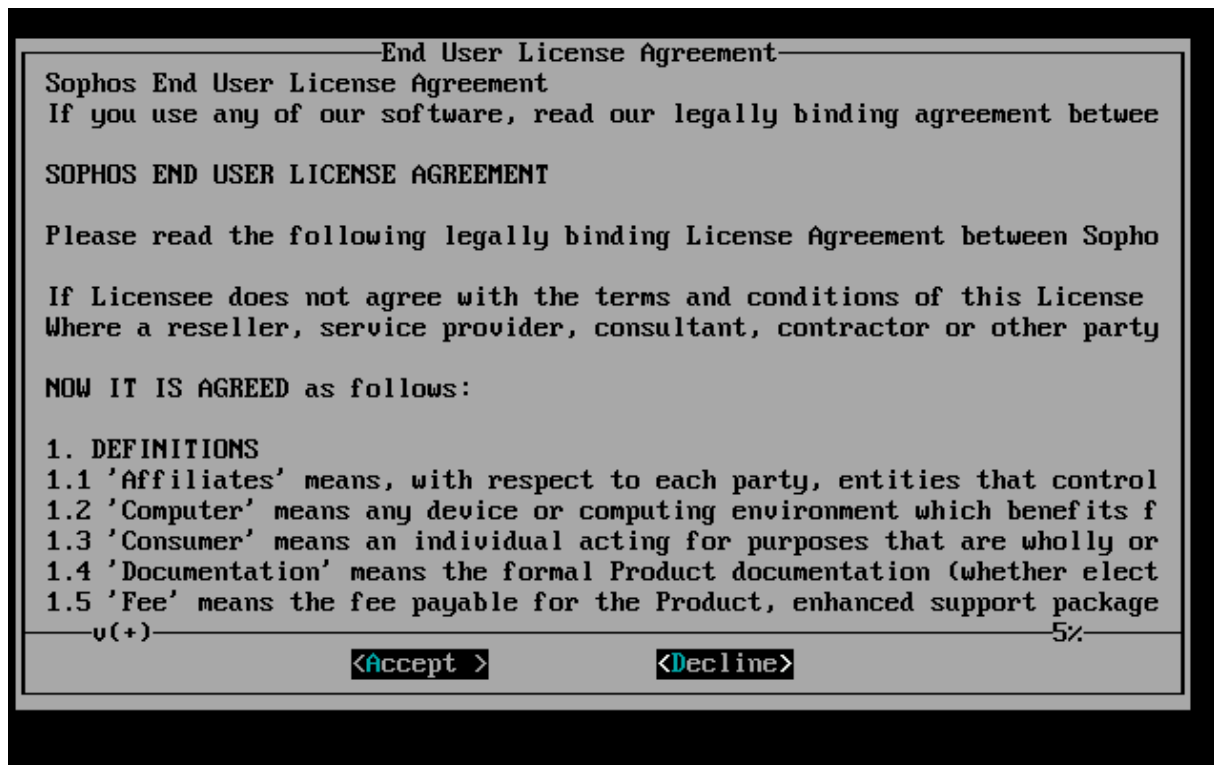
```
Number of cores:          1
Total RAM:                2016 MB
Total Number of interfaces: 2
Total Disk Size:          50 GB
```

```
#####
```

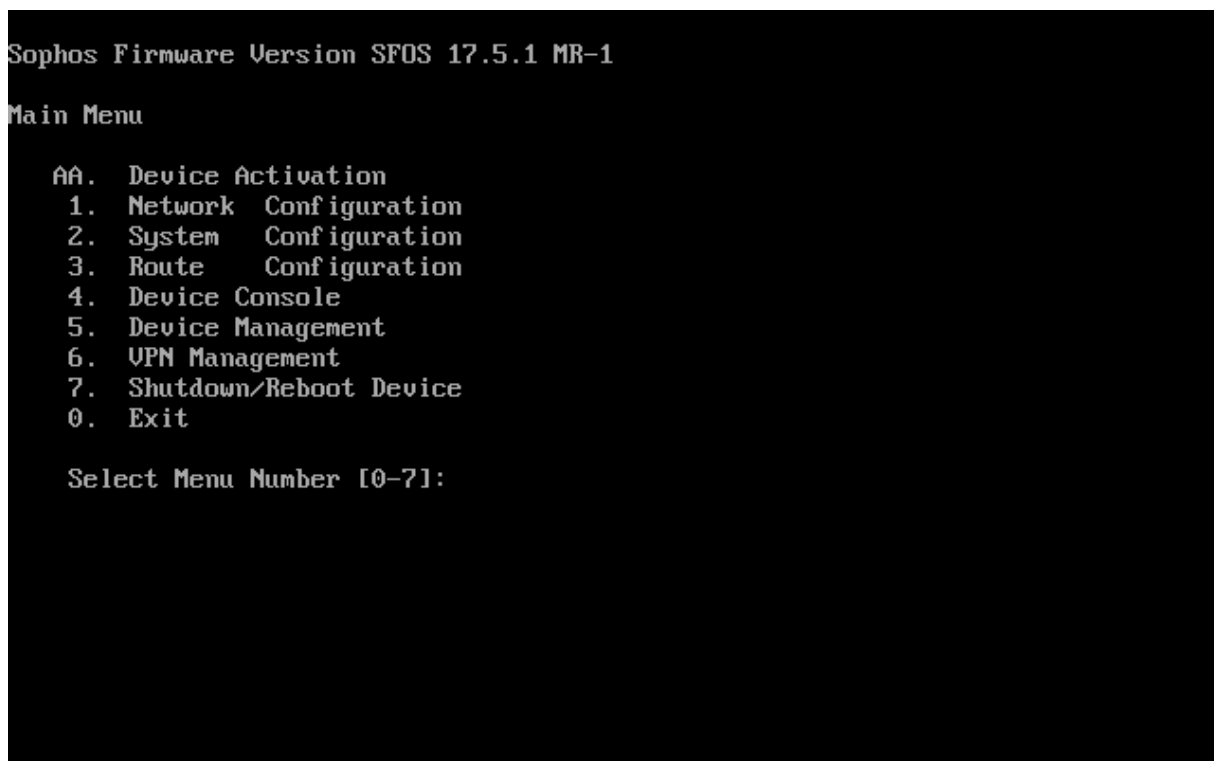
```
Password: _
```

Lors de la première connexion en console sur un Sophos XG, il faut utiliser le mot de passe par défaut : **admin**

Remarque : Sophos est configuré en QWERTY par défaut, il faut donc taper « **qd,in** » pour écrire « **admin** ».




Accepter les conditions générales pour atteindre la console d'administration :



Il est possible de laisser les paramètres par défaut, car le lien LAN est configuré pour être un serveur DHCP joignable à l'adresse **172.16.16.16/24**. L'installation est terminée, nous pouvons passer à la configuration de l'appareil.

Configuration

Si les paramètres IP n'ont pas été modifiés depuis la console, on peut passer à la configuration en ouvrant un navigateur web sur <http://172.16.16.16:4444>. Une alerte de sécurité apparaîtra, ce qui est normal étant donné que le certificat SSL du site a été auto-généré par le Sophos, et n'est donc pas reconnu par une autorité de certification :



Attention : risque probable de sécurité

Firefox a détecté un problème et a interrompu le chargement de 10.69.1.44. Soit le site est mal configuré, soit l'horloge de votre ordinateur est réglée à la mauvaise heure.

Que pouvez-vous faire ?

L'horloge de votre ordinateur est réglée sur . Assurez-vous que la date, l'heure et le fuseau horaire soient corrects dans les paramètres système de votre ordinateur, puis actualisez 10.69.1.44.

Si votre horloge est déjà bien réglée, le site web est probablement mal configuré et il n'y a rien que vous puissiez faire pour résoudre le problème. Essayez éventuellement de le signaler à l'administrateur du site.

[En savoir plus...](#)

[Retour \(recommandé\)](#)[Avancé...](#)

Les sites web justifient leur identité par des certificats. Firefox ne fait pas confiance à ce site, car il utilise un certificat qui n'est pas valide pour 10.69.1.44:4444. Le certificat n'est valide que pour .

Code d'erreur : `MOZILLA_PKIX_ERROR_NOT_YET_VALID_ISSUER_CERTIFICATE`

[Afficher le certificat](#)

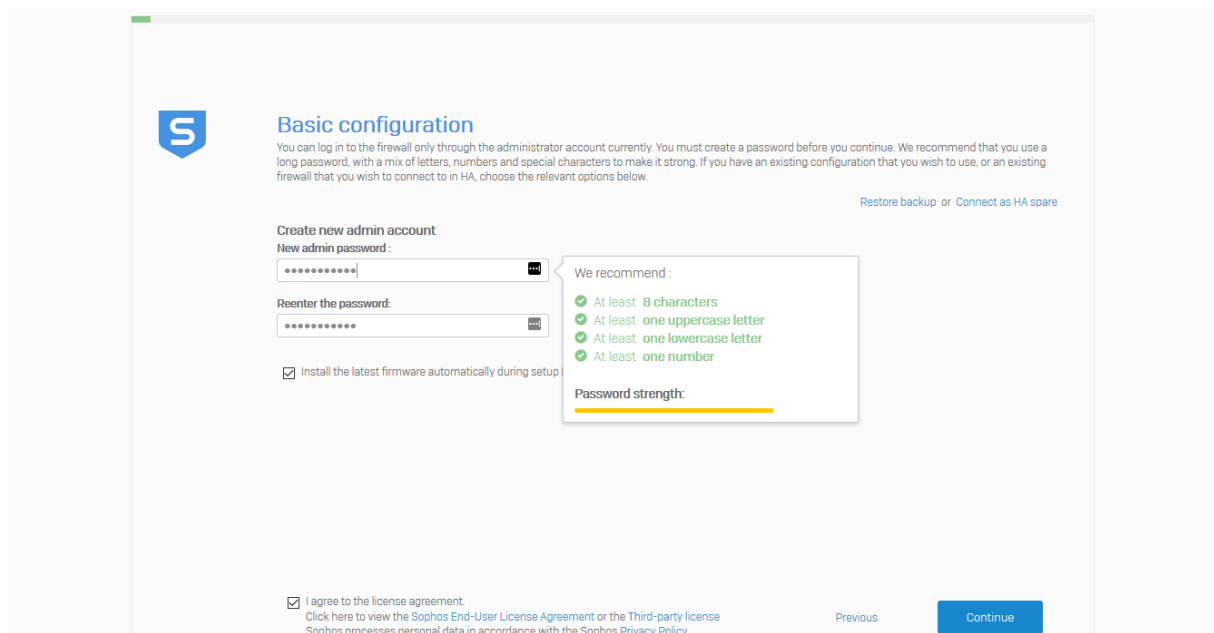
[Retour \(recommandé\)](#)[Accepter le risque et poursuivre](#)

☐ Signaler les erreurs similaires pour aider Mozilla à identifier et bloquer les sites malveillants

Il faut donc poursuivre en ignorant l'alerte.



On commence par modifier le mot de passe de l'administrateur, et on accepte le règlement :



The screenshot shows the 'Basic configuration' screen of a Sophos firewall. It features the Sophos logo and a blue header. The main text explains that a password must be created to log in. There are two input fields for the 'New admin password' and 'Reenter the password'. A checkbox is present for 'Install the latest firmware automatically during setup'. A 'We recommend' box lists password requirements: at least 8 characters, one uppercase letter, one lowercase letter, and one number. A 'Password strength' bar is shown below these requirements. At the bottom, there is a checkbox for 'I agree to the license agreement' with a link to view the license and privacy policy. 'Previous' and 'Continue' buttons are at the bottom right.

Basic configuration

You can log in to the firewall only through the administrator account currently. You must create a password before you continue. We recommend that you use a long password, with a mix of letters, numbers and special characters to make it strong. If you have an existing configuration that you wish to use, or an existing firewall that you wish to connect to in HA, choose the relevant options below.

[Restore backup](#) or [Connect as HA spare](#)

Create new admin account

New admin password:

Reenter the password:

☒ Install the latest firmware automatically during setup

We recommend :

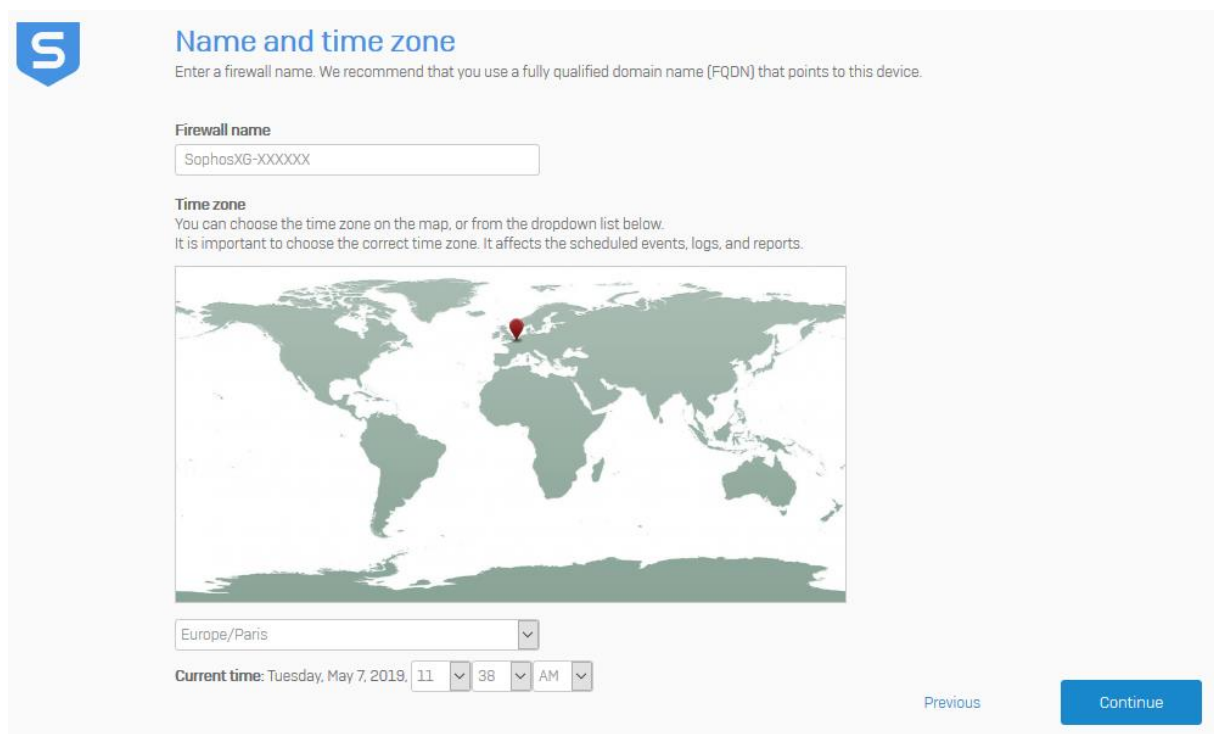
- At least 8 characters
- At least one uppercase letter
- At least one lowercase letter
- At least one number

Password strength:

☒ I agree to the license agreement.
[Click here to view the Sophos End-User License Agreement or the Third-party license](#)
Sophos processes personal data in accordance with the Sophos Privacy Policy.

[Previous](#) [Continue](#)

On nomme la machine, et on sélectionne le fuseau horaire adéquat :



The screenshot shows the 'Name and time zone' screen of a Sophos firewall. It features the Sophos logo and a blue header. The main text asks for a firewall name and recommends using a fully qualified domain name (FQDN). There is an input field for the 'Firewall name' with the placeholder 'SophosXG-XXXXXX'. Below this, the 'Time zone' section explains that the time zone can be chosen on a map or from a dropdown list. A world map is shown with a red pin over Europe. Below the map is a dropdown menu showing 'Europe/Paris'. At the bottom, there is a 'Current time' field showing 'Tuesday, May 7, 2019, 11:38 AM'. 'Previous' and 'Continue' buttons are at the bottom right.

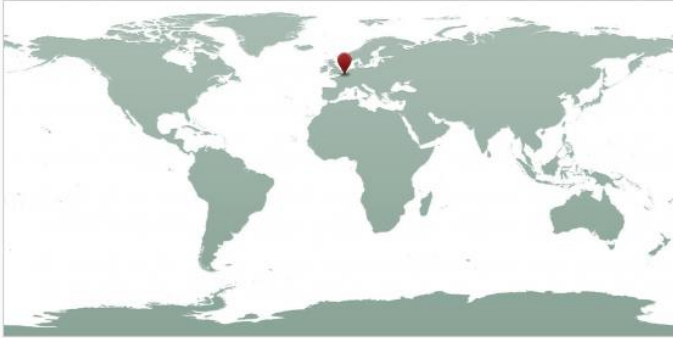
Name and time zone

Enter a firewall name. We recommend that you use a fully qualified domain name (FQDN) that points to this device.

Firewall name

Time zone


You can choose the time zone on the map, or from the dropdown list below.
It is important to choose the correct time zone. It affects the scheduled events, logs, and reports.



Current time: Tuesday, May 7, 2019,

[Previous](#) [Continue](#)

Si l'on possède une clé de licence Sophos XG ou Sophos UTM 9, il est possible de la renseigner à l'étape suivante. Sinon, il est possible de démarrer un essai de 30 jours, ou de passer cette étape :



Register your firewall

Every firewall must have a serial number. We can get one for you automatically. Alternatively, if you have an unused serial number, you can specify it here.

☒ **I have an existing serial number**

Once you register the firewall, you cannot change the serial number. If you have more than one serial number, make sure that you choose the correct one. Home users must use an XG Home. Use serial number obtained from [here](#)

☐ **I don't have a serial number (start a trial).**

You will automatically receive a serial number and a 30-day trial period. During this period, you can test the full functionality of Sophos XG Firewall. **Do not use this option for home use.**

☐ **I would like to migrate my UTM 9 license now**

You will receive a serial number automatically. Your equivalent UTM 9 license will be converted and applied to the XG Firewall.

This is not reversible. If you are not sure about migrating now, click "Start a trial". You can migrate the license after you test XG Firewall.

☒ **I do not want to register now**

You can skip registration for now. A reminder to register will appear during your next login. You can continue without registration for another 30 days.

SOPHOS

License Schedule

License Schedule

Activated On: 11 May 12

Expiry Date: 11 May 12


License Key: C160703HBRQMRCE

Serial Number

Previous

Continue

Nous avons alors un résumé de la configuration initiale :



Basic setup is complete

You have completed the basic setup and have chosen to register the firewall later. We have activated all capabilities, you can configure and try them. The wizard will help you set up the basic networking and security features. To configure these manually, click "Skip to finish".

Licensed features

Feature	Status	Expiry
Network protection	✓ Evaluating	-
Web protection	✓ Evaluating	-
Email protection	✓ Evaluating	-
Web server protection	✓ Evaluating	-
Sandstorm	✓ Evaluating	-
Enhanced support	✗ Not evaluating	-
Enhanced plus support	✗ Not evaluating	-


☐ **Opt in to the customer experience improvement program.**
[View Sophos privacy policy](#)

Skip to finish

Previous

Continue

L'étape suivant permet de modifier les paramètres IP des interfaces, ainsi que d'activer ou non le serveur DHCP sur l'interface :



Network configuration (LAN)

Let us set up a protected network. Select the ports to which you will connect the devices you wish to protect. The selected ports will be bridged together, and traffic will be permitted among them. You are connected to "Port1" right now.

Port1

Choose gateway

This firewall (route mode)

Do you want this firewall to act as the gateway for the protected network (commonly used)? Alternatively, you can use your existing internet gateway, and bridge the protected network with it. The firewall delivers the same level of security in both cases. Additionally, it can act as a router between the protected network and other local networks if configured as a gateway.

LAN address and internal client network size


172.16.16.16
/24 (up to 254 client devices)

[Edit internet connection](#)

☐ **Enable DHCP**
Let the firewall assign IP addresses to your internal devices.


[Enable TAP/discover mode](#)
[Previous](#)
[Continue](#)


On peut ensuite activer ou non des fonctionnalités avancées de protection (on peut le faire également après la configuration initiale) :





Network protection

You can configure permissions for users on wired and wireless networks to protect them when they access the internet.


☐ **Protect users from network threats**
Protects users from network intrusion attempts, protects against advanced threats that could be within your network, and blocks network traffic from high-risk applications.



☐ **Protect users from the suspicious and malicious websites**
Protects users from clicking malicious links, and from visiting harmful sites. It does not scan the SSL traffic.
[Click here](#) to learn how to scan HTTPS traffic.


☒ **Scan files that were downloaded from the web for malware**
Even reputed sites may contain malicious files. Scan files with Sophos malware detection engine to catch known malware and their variants.


☐ **Send suspicious files to Sophos Sandstorm**
Protects users from undiscovered malware through advanced detection techniques that involve running applications, and viewing documents in a safe sandbox in the cloud, before letting users download files to their computers.

[Previous](#)
[Continue](#)

Enfin, on peut spécifier un email de contact où envoyer les sauvegardes de configuration :



Notifications and backups

It is important to have quick access to backups. Enter the details to receive the latest backups and notifications by email.


Email recipient

Email sender

☒ Send weekly configuration backup

☐ Specify an external mail server

[Previous](#) [Continue](#)



Configuration summary

Please review your choices in the window. Click Finish. This will apply the settings that you have specified, install the latest firmware, and reboot the firewall. It will take approximately five minutes to complete.

Basic settings

Hostname: SophosXG-XXXXXX
Time zone: Europe/Paris

Network settings

Internet connection: DHCP on Port2
Local network: Port1
IP: 10.69.1.44/255.255.255.0
DHCP disabled

#Default_Network_Policy has been created with:

Scan HTTP: Disable
Decrypt & scan HTTPS: Disable
Detect zero-day threats with Sandstorm: Disable
Web policy: Default Policy
Intrusion prevention: -

Notifications and backups:

Send weekly configuration backup: Enable
[Built-in email server](#)
Email recipient: test@test.test
Email sender: test@test.test

[Copy to clipboard](#) [Send as email](#) [Previous](#) [Finish](#)

Après un redémarrage, le Sophos XG est prêt à l'emploi.



FINISHING



Downloading latest firmware: 100 %



Applying configuration changes

Please wait a few moments for the changes to be applied.



Updating firmware

Once the firewall is configured, the firmware will be installed.



Reboot

Once the process is complete, the firewall will reboot automatically. This will take five minutes to complete.

Configuration

L'un des paramètres les plus importants à configurer sur un routeur/pare-feu est la redirection NAT, afin de rendre accessibles des services sur les serveurs protégés.

Dans Sophos XG, on peut créer, modifier ou supprimer des règles NAT dans **Protection > Pare-feu**.

ID	Nom	Source	Destination	Laquelle ?	Action
5	Traffic to Interna...	entrant 195.25 GB, sortant 1...			
1	Traffic to WAN	entrant 0 B, sortant 0 B			
1	Traffic to DMZ	entrant 0 B, sortant 0 B			
1	Auto added firewall...	entrant 0 B, sortant 4.09 KB	Toute zone, Tout hôte	Toute zone, Tout hôte	SMTP, SMTPS
5	#Default Network P...	entrant 9764 MB, sortant 2...	LAN, Tout hôte	WAN, Tout hôte	Tout service

Si l'on veut créer une redirection NAT, il faut alors cliquer sur « **Ajouter une règle de pare-feu** », puis « **Règles d'application métier** ». On obtient alors la fenêtre suivante :

Ajouter Règle d'application métier

Modèle d'application: Sélectionner

Description: Description

Position de la règle: Haut

Nom de la règle *: Nom de la règle

Dans le menu déroulant du champ « **Modèles d'application** », on sélectionne alors « **DNAT/Full NAT/Load Balancing** », ce qui active alors une série de champs appropriés à la configuration du service :

The screenshot shows the 'Ajouter Règle d'application métier' (Add Business Application Rule) configuration page in the Sophos XG Firewall web interface. The left sidebar contains navigation menus for 'SURVEILLANCE & ANALYSE', 'PROTECTION', 'CONFIGURER', and 'SYSTÈME'. The main content area is divided into several sections:

- Modèle d'application:** A dropdown menu set to 'DNAT/Full NAT/Load Balancing'.
- Description:** A text field containing 'Lorem ipsum'.
- Position de la règle:** A dropdown menu set to 'Haut'.
- Groupe de règles:** A dropdown menu set to 'Automatique'.
- Nom de la règle *:** A text field containing 'Test NAT'.
- Source:** Three columns for 'Zones émettrices *', 'Autorisés les réseaux client *', and 'Bloqués les réseaux client', each with a 'Tous' selection and an 'Ajouter un nouvel élément' button.
- Destination & Service:** A section with 'Hôte/Réseau de destination *' set to '#Port1' and 'Services *' set to 'IMAP', both with 'Ajouter un nouvel élément' buttons.
- Redirection:** A text field for specifying the target port or IP.
- Résumé:** A sidebar on the right providing a summary of the rule configuration, including 'Source', 'Destination', 'Redirection', and 'Avancés' settings.

At the bottom, there are 'Enregistrer' (Save) and 'Annuler' (Cancel) buttons.

Après avoir donné un nom et une description (facultative) à la règle, on règle les paramètres propres à la source du trafic : quels sont les zones de provenance, le ou les pays/régions autorisés, et s'il y a des adresses ou des réseaux à bannir d'office.

On configure ensuite les paramètres de destination : quel est le port du Sophos qui recevra le trafic (dans un DNAT, il s'agit du port WAN), et quel est le service. On peut alors choisir un service « de base » dans le menu déroulant, ou créer notre service sur mesure pour répondre à un besoin plus spécifique (par exemple, si l'on veut rediriger le port externe 55000 vers le port SSH d'une machine protégée par le Sophos, il faudra créer une règle sur mesure, car le port 55000 ne correspond pas au port SSH par défaut).

Enfin, dans la section « **Redirection** », on paramètre la machine sur laquelle sera redirigé le trafic répondant aux critères spécifiés plus haut, le port (ou la plage de ports) de destination, ainsi que la zone à laquelle appartient l'équipement.

Ajouter Règle d'application métier

Redirection

Serveur(s) protégé(s) * : [IP] | Port mappé * : 143 | Zone protégée * : LAN

Avancés

Stratégie pour les applications métiers : Prévention des intrusions (Aucune), Régulation de flux (Aucune)

Sécurité synchronisée : Source HD minimale autorisée (No Restriction), Destination HD minimale autorisée (No Restriction)

Routage : Réécrire l'adresse source (déguise) (OFF), Créer une règle réflexive (OFF)

Enregistrement du trafic

☒ Enregistrer le trafic du pare-feu

Résumé

Test NAT

Règle

Source : Zones émettrices : Any, Autorisés les réseaux client : Any, Bloqués les réseaux client : -

Destination : Hôte/Réseau de destination : [IP]

Redirection : Serveur(s) protégé(s) : [IP], Zone protégée : LAN

Avancés

Sécurité synchronisée

Source : La sécurité Heartbeat minimale est Aucune restriction, Clients sans signal Heartbeat autorisés

Destination : La sécurité Heartbeat minimale est Aucune restriction, Requête de destination sans signal Heartbeat autorisée

Déguise (Masquage) : OFF

Règle réflexive

Activer pour créer automatiquement une règle de pare-feu réflexive pour l'hôte protégé.

Une règle réflexive a les mêmes stratégies que les règles configurées sur le serveur hébergé. Néanmoins, la règle est applicable depuis la zone de destination vers la zone source plutôt que l'inverse.

Les options de la section « **Avancés** » sont facultatives, et contrôlent notamment les stratégies de prévention des intrusions, le contrôle de régulation de flux, les paramètres de sécurité synchronisée HeartBeat, ou encore s'il faut activer la réécriture d'adresse source ou rendre la règle réflexive (c'est-à-dire que les stratégies qui lui sont appliquées seront automatiquement ajoutées au trafic sortant issu de cette machine).

Pare-feu

IPv4 | IPv6 | Activer le filtre

[Ajouter une règle de pare-feu](#)

ID	Nom	Source	Destination	Laquelle ?	Action	Fonctions
6	Traffic to Interna... entrant 195.25 GB, sortant 1...					To LAN, WIFI, VPN, DMZ, Z. Firewal...
10	Test NAT entrant 0 B, sortant 0 B	Toute zone, 82.231.127.88	LAN, 10.69.1.4	IMAP	Transférer	[AV] [WEB] [APP] [QoS] [Tb] [Lb] [NAT] [100] [IPS]
9					Transférer	[AV] [WEB] [APP] [QoS] [Tb] [Lb] [NAT] [100] [IPS]
8					Transférer	[AV] [WEB] [APP] [QoS] [Tb] [Lb] [NAT] [100] [IPS]
7					Transférer	[AV] [WEB] [APP] [QoS] [Tb] [Lb] [NAT] [100] [IPS]
6					Transférer	[AV] [WEB] [APP] [QoS] [Tb] [Lb] [NAT] [100] [IPS]
4	[exemple] Traffic... entrant 0 B, sortant 0 B	Toute zone, Tout hôte, Tout uti...	LAN, DMZ, WIFI, VPN, T out hôte...	Tout service	Annuler	[AV] [WEB] [APP] [QoS] [Tb] [Lb] [NAT] [100] [IPS]
1	Traffic to WAN entrant 0 B, sortant 0 B					Outbound traffic to WAN, Firewa...
1	Traffic to DMZ entrant 0 B, sortant 0 B					Inbound traffic to DMZ, Firewal...
1	Auto added firewall... entrant 0 B, sortant 4.09 KB	Toute zone, Tout hôte	Toute zone, Tout hôte	SMTP, SMTPS	Transfé...	[AV] [WEB] [APP] [QoS] [Tb] [Lb] [NAT] [100] [IPS]
5	#Default_Network_P... entrant 97.70 MB, sortant 22...	LAN, Tout hôte	WAN, Tout hôte	Tout service	Accept...	[AV] [WEB] [APP] [QoS] [Tb] [Lb] [NAT] [100] [IPS]