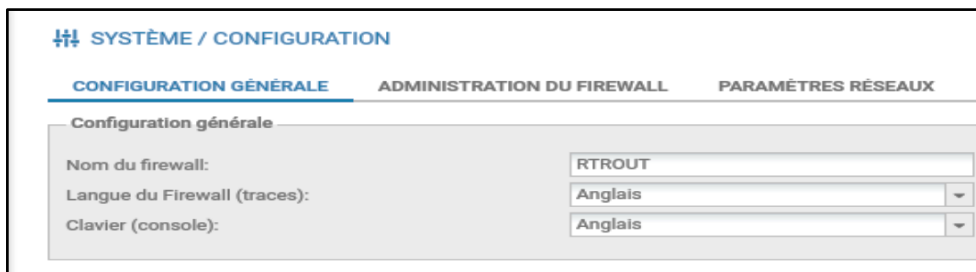


Compte rendu Mission 2

1) Configurations basiques Stormshield sur “Network security” :

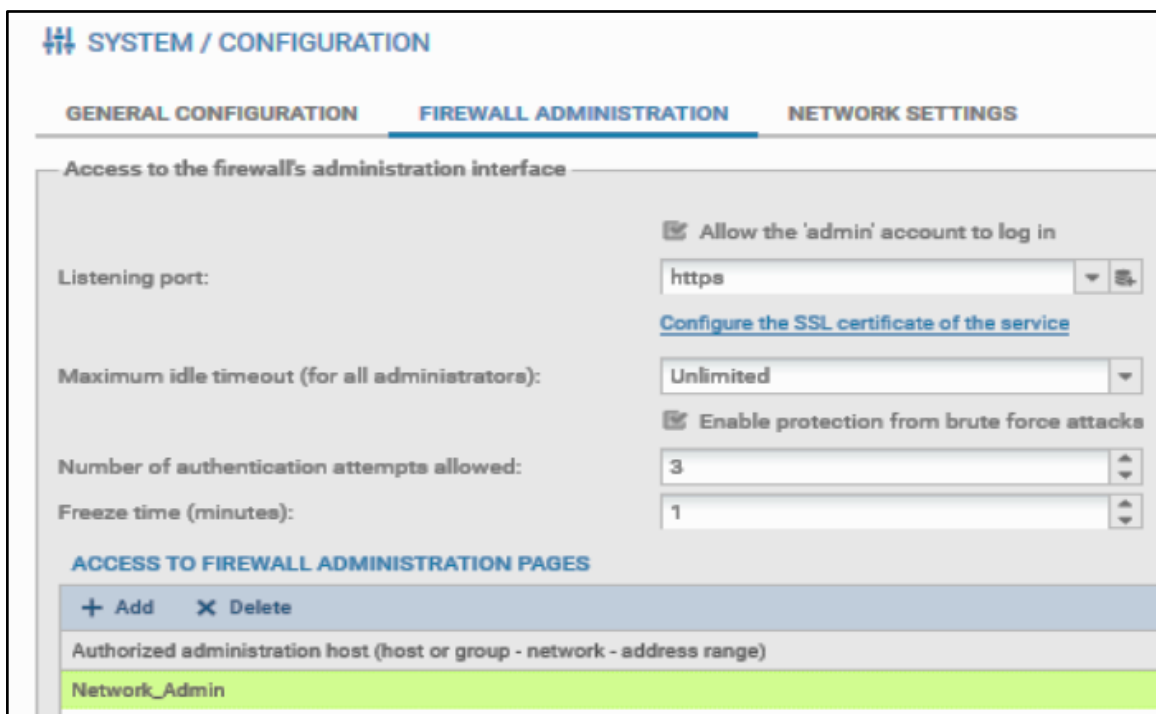
- Mot de passe Routeur : DAsisr1*
- Sur SW4 :
 - *#inter g0/2*
 - *#switchport mode trunk*
- Configuration du nom du routeur
⇒ *SYSTEM → Configuration*



The screenshot shows the 'SYSTEM / CONFIGURATION' page with three tabs: 'CONFIGURATION GÉNÉRALE', 'ADMINISTRATION DU FIREWALL', and 'PARAMÈTRES RÉSEAUX'. The 'CONFIGURATION GÉNÉRALE' tab is active. It contains a 'Configuration générale' section with the following fields:

Nom du firewall:	RTROUT
Langue du Firewall (traces):	Anglais
Clavier (console):	Anglais

- Configuration accès au Routeur (seulement VLAN “admin”) :
⇒ *Revenir le faire après avoir créé et configuré les VLANs*
Permet l'accès à la passerelle du routeur seulement aux postes du VLAN Admin.



The screenshot shows the 'SYSTEM / CONFIGURATION' page with three tabs: 'GENERAL CONFIGURATION', 'FIREWALL ADMINISTRATION', and 'NETWORK SETTINGS'. The 'FIREWALL ADMINISTRATION' tab is active. It contains a section titled 'Access to the firewall's administration interface' with the following settings:

- ☒ Allow the 'admin' account to log in
- Listening port: https
- [Configure the SSL certificate of the service](#)
- Maximum idle timeout (for all administrators): Unlimited
- ☒ Enable protection from brute force attacks
- Number of authentication attempts allowed: 3
- Freeze time (minutes): 1

Below this section is a table titled 'ACCESS TO FIREWALL ADMINISTRATION PAGES' with a header row containing '+ Add' and 'X Delete' buttons. The table has one row with the following data:

Authorized administration host (host or group - network - address range)
Network_Admin

2) Configurations des passerelles (interne, externe, DMZ) du routeur :

- Configuration de la passerelle interne (in : LAN) :
⇒ *OBJECTS* → *Network*

PROPERTIES

Object name:

IPv4 addresses

Start:

End:

- Configuration de la passerelle externe (out : WAN) :
⇒ *NETWORK* → *Interfaces*

Status

☒ ON

General settings

Name:

Comments:

This interface is: ☐ Internal (protected) ☒ External (public)

Address range

Address range: ☐ Address range inherited from the bridge ☒ Dynamic / Static

IPv4 address: ☐ Dynamic IP (obtained by DHCP) ☒ Fixed IP (static)

[+ Add](#) [X Delete](#)

Address/ Mask	Comments
120.121.122.60/24	

⇒ *NETWORK* → *Routing*

General

Default gateway (router):

STATIC ROUTES

[+ Add](#) [X Delete](#)

Status	Destination network (host, network or g...)	Interface	Address range	Gateway
☒ on	Network_WAN	WAN	120.121.122.0/24	Gateway

- Configuration DMZ :
⇒ *NETWORK* → *Interfaces*

Status
☐ OFF

General settings
Name:
Comments:
This interface is: ☒ Internal (protected) ☐ External (public)

Address range
Address range: ☐ Address range inherited from the ☒ Dynamic / Static bridge
IPv4 address: ☐ Dynamic IP (obtained by DHCP) ☒ Fixed IP (static)

+ Add **× Delete**

Address/ Mask	Comments
172.31.6.254/24	

3) Création et configuration des VLANs :

LAN

Reseaux&Systeme

Developpement

Admin

Visiteurs

Serveurs

Direction/DSI

RH/C/J/SA

Commu/Redaction

Commercial

Labo-Recherche

Accueil

Demonstration

WAN

DMZ

Status

ON

General settings

Name:

Reseaux&Systeme

Comments:

Parent interface:

LAN

ID:

10

Priority (CoS):

0

This interface is:

☒ Internal (protected)
☐ External (public)

Address range

Address range:

☐ Address range inherited from the ☒ Dynamic / Static bridge

IPv4 address:

☐ Dynamic IP (obtained by DHCP) ☒ Fixed IP (static)

+ Add

× Delete

Address/ Mask	Comments
192.168.10.254/24	

Nom	Réseau	Masque CIDR	Passerelle
LAN	192.168.2.0	/24	192.168.2.254
WAN	120.121.122.0	/24	120.121.122.60
DMZ	172.31.6.0	/24	172.31.6.254
Vlan 1	192.168.1.0	/24	192.168.1.254
Vlan 10	192.168.10.0	/24	192.168.10.254
Vlan 50	192.168.50.0	/24	192.168.50.254
Vlan 99	192.168.99.0	/24	192.168.99.254
Vlan 150	192.168.150.0	/24	192.168.150.254
Vlan 250	192.168.250.0	/24	192.168.250.254
Vlan 200	192.168.200.0	/24	192.168.200.254
Vlan 201	192.168.201.0	/24	192.168.201.254
Vlan 202	192.168.202.0	/24	192.168.202.254
Vlan 203	192.168.203.0	/24	192.168.203.254
Vlan 204	192.168.204.0	/24	192.168.204.254
Vlan 205	192.168.205.0	/24	192.168.205.254
Vlan 206	192.168.206.0	/24	192.168.206.254

4) Création et configuration passerelle :

⇒ *NETWORK* → *Routing*

IPv4 STATIC ROUTES IPv4 DYNAMIC ROUTING IPv4 RETURN ROUTES

General

Default gateway (router):

STATIC ROUTES

Searching... [+ Add](#) [X Delete](#)

Status	Destination network (host, network or g...	Interface	Address range	Gateway
☒ on	Network_WAN	WAN	120.121.122.0/24	Gateway

5) Création et configuration des ACL :

- *Création des objets :*

DNS

Nom de l'objet DNS

Objets inclus dans ce groupe :

- ServeurDNS1 (192.168.250.1)
- ServeurDNS2 (192.168.250.2)

Contient les 2
DNS LABANNU

Network-Entreprise

Nom de l'objet Network-Entreprise

Commentaire tous vlan sauf visiteurs

Objets inclus dans ce groupe :

- Network_Accueil (192.168.205.0/255.255.255.0)
- Network_Admin (192.168.99.0/255.255.255.0)
- Network_Commercial (192.168.203.0/255.255.255.0)
- Network_Commu/Redaction (192.168.202.0/255.255.255.0)
- Network_Demonstration (192.168.206.0/255.255.255.0)
- Network_Developpement (192.168.50.0/255.255.255.0)
- Network_Direction/DSI (192.168.200.0/255.255.255.0)
- Network_Labo-Recherche (192.168.204.0/255.255.255.0)
- Network_Reseaux&Systeme (192.168.10.0/255.255.255.0)
- Network_RH/C/J/SA (192.168.201.0/255.255.255.0)
- et 1 de plus.

Contient tous les
vlan sauf le vlan
visiteurs

Serveur-OUTLAB

172.31.6.10 / static

Nom de l'objet Serveur-OUTLAB

Adresse IP 172.31.6.10

Machine OUTLAB

- Règle de filtrage (ACL):

The screenshot shows two firewall rules in a configuration interface. The first rule, 'Vlan serveurs' (containing 2 rules, 5 to 6), is highlighted in pink. It has a priority of 6, is enabled (on), and its action is 'bloquer' (block). The source is 'Network_Serveurs' and the destination is 'Internet'. The second rule, 'Accès Internet' (containing 1 rule, 7 to 7), is highlighted in teal. It has a priority of 7, is enabled (on), and its action is 'passer' (allow). The source is 'Network_internals' and the destination is 'Internet'. Below the second rule, there is a handwritten note in red: 'Accès bloqué pour le vlan serveurs vers internet'.

➤ Accès autorisé pour tous les vlans vers internet

The screenshot shows a firewall rule named 'Vlan visiteurs' (containing 2 rules, 1 to 2), highlighted in purple. It has a priority of 2, is enabled (on), and its action is 'passer' (allow). The source is 'Network-Entreprise' and the destination is 'Network_Serveurs'.

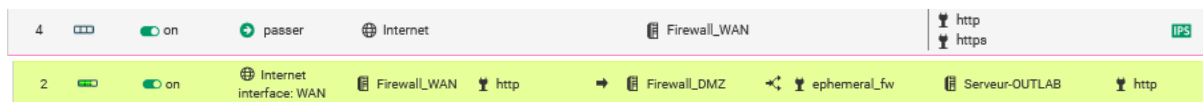
➤ Accès autorisé pour Network-Entreprise (tous les vlans sauf visiteurs) vers le vlan serveurs
L'accès à internet est déjà fait à l'aide de la règle "Accès Internet"

⇒ Le VLAN "visiteurs" peut uniquement interroger les serveurs DNS et DHCP et sortir sur internet :

The screenshot shows the same 'Vlan visiteurs' rule, but with the destination set to 'DNS' instead of 'Network_Serveurs'. The action remains 'passer' (allow).

➤ Accès autorisé pour les requêtes DNS du vlan visiteurs vers le groupe DNS (contient les serveurs DNS LABANNU1 et LABANNU2)

⇒ Le serveur web OUTLAB dans la DMZ devra être accessible depuis le LAN et le WAN :



6) Fiche de recette :

- **Rappel du contexte :** *Mise en place de l'infrastructure configuration du routeur*

Etape : *connexion au routeur*

Description du test : *connexion au routeur via Vm ou sur machine physique*

Résultats attendus : *connexion OK*

Résultats obtenus : *connexion OK*

Etape : *configuration NAT et connexion à internet*

Description du test : *connexion à internet grâce au NAT routeur*

Résultats attendus : *connexion OK*

Résultats obtenus : *pas de connexion*

Résolution des problèmes : *il manquait la configuration de la passerelle du côté public (WAN) du routeur afin de pouvoir sortir du réseau*

ICMP (contient 2 règles, de 1 à 2)						
1				Network_internals	Network_internals	Any icmp (requête Echo)
2				Network_internals	Any	Any icmp (requête Echo)
Nulantez (contient 1 règles, de 3 à 3)						
3				Network_Admin	Server_MJTANIX	Any
Vlan visiteurs (contient 4 règles, de 4 à 7)						
4				Network_Visiteurs	DNS_INTERNE	dns
5				Network_Visiteurs	Network_Serveurs	Any
6				Network_Visiteurs	Internet	http https
7				Network_Visiteurs	Network-Entreprise	Any
DNS (contient 6 règles, de 8 à 13)						
8				Network_Serveurs	Network_Serveurs	snmp
9				ServeurDNS_DMZ	ServeurDNS_Internet	dns
10				ServeurDNS_DMZ	Internet	dns
11				ServeurDNS_LABANNJ1	ServeurDNS_DMZ	dns
12				ServeurDNS_LABANNJ2	ServeurDNS_DMZ	dns
13				Network-Entreprise	LABANNJ1_DNS	dns
Network Entreprise accès (contient 2 règles, de 14 à 15)						
14				Network-Entreprise	Network_Serveurs	Any
15				Network-Entreprise	Network_DMZ	Any
Accès DMZ (contient 4 règles, de 16 à 19)						
16				Internet	Firewall_WAN	dns
17				Internet	Firewall_WAN	http https
18				Network_internals	swiss-galaxyC2.com	http https
DNS (contient 6 règles, de 8 à 13)						
8				Network_Serveurs	Network_Serveurs	snmp
9				ServeurDNS_DMZ	ServeurDNS_Internet	dns
10				ServeurDNS_DMZ	Internet	dns
11				ServeurDNS_LABANNJ1	ServeurDNS_DMZ	dns
12				ServeurDNS_LABANNJ2	ServeurDNS_DMZ	dns
13				Network-Entreprise	LABANNJ1_DNS	dns
Network Entreprise accès (contient 2 règles, de 14 à 15)						
14				Network-Entreprise	Network_Serveurs	Any
15				Network-Entreprise	Network_DMZ	Any
Accès DMZ (contient 4 règles, de 16 à 19)						
16				Internet	Firewall_WAN	dns
17				Internet	Firewall_WAN	http https
18				Network_internals	swiss-galaxyC2.com	http https
19				Network_internals	zabbix.swiss-galaxyC2.com	http https
Accès Internet (contient 2 règles, de 20 à 21)						
20				Network_Serveurs	Internet	Any
21				Network-Entreprise	Internet	http https
Accès routeur (contient 2 règles, de 22 à 23)						
22				Any	Firewall_Admin	firewall_srv
23				Any	firewall_all	Any icmp (requête Echo)
Default policy - Mise à jour le 2023-12-06 10:35:38 par admin (192.168.99.21) (contient 1 règles, de 24 à 24)						
24				Any	Any	Any