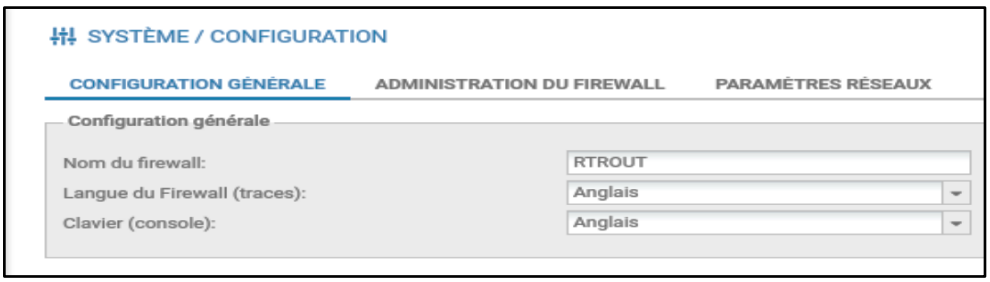
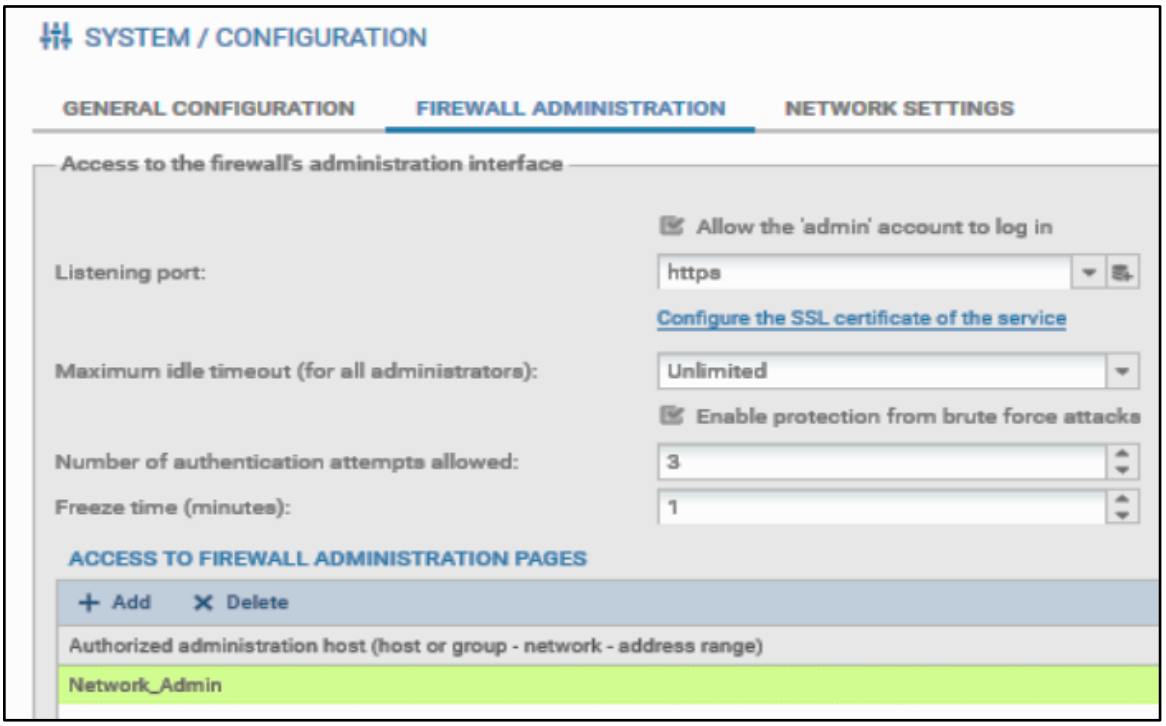
Compte rendu Mission 2

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*



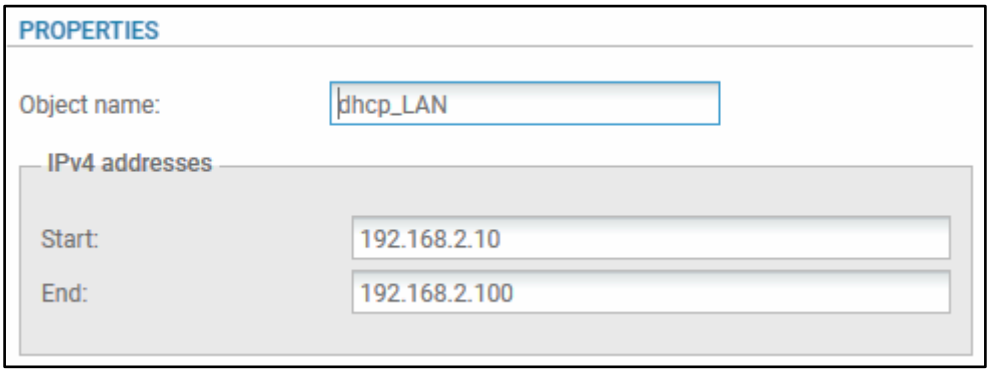
- Configuration accès au Routeur (seulement VLAN “admin”) :
  ⇒ *Revenir le faire après avoir créé et configuré les VLANs*
  Permet l’accès à la passerelle du routeur seulement aux postes du VLAN Admin.



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

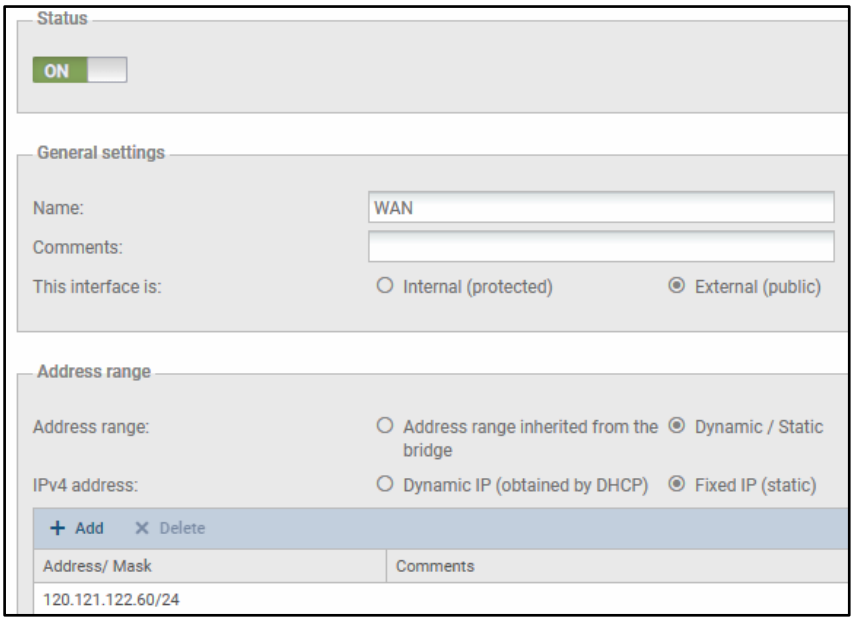
- Configuration de la passerelle interne (in : LAN) :

  ⇒ *OBJECTS → Network*

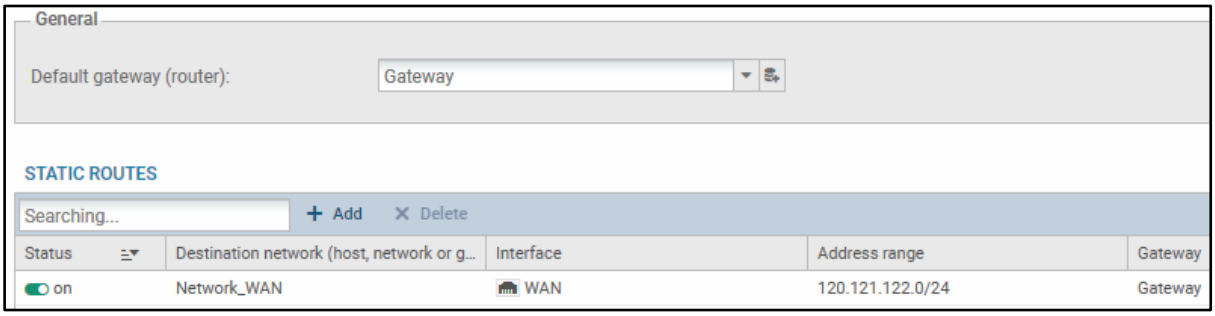


- Configuration de la passerelle externe (out : WAN) :

  ⇒ *NETWORK → Interfaces*

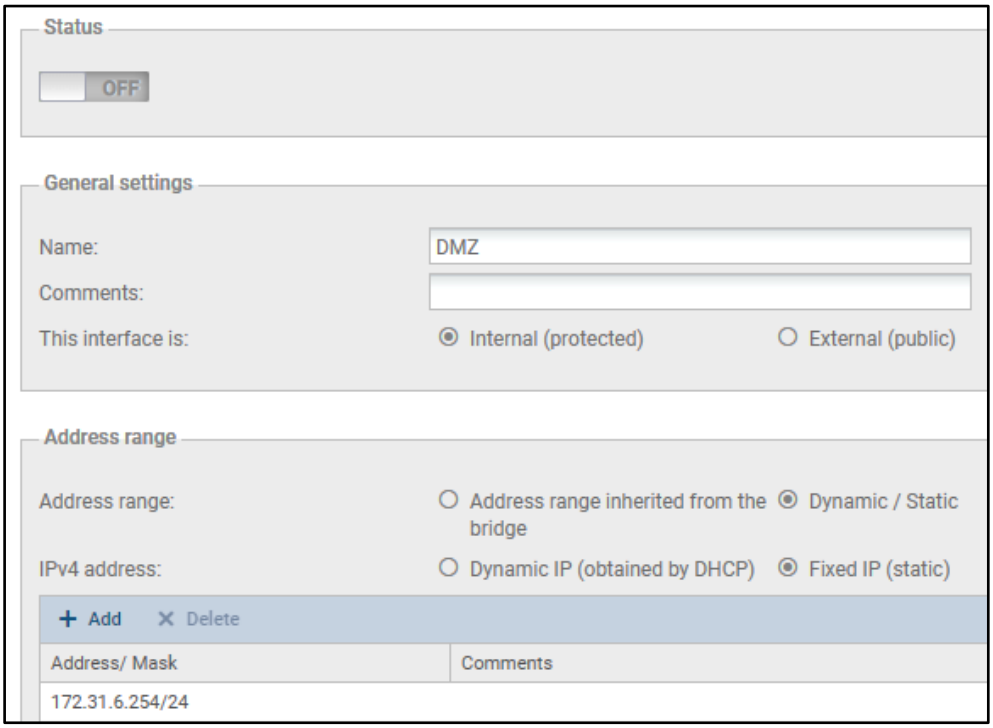


⇒ *NETWORK → Routing*

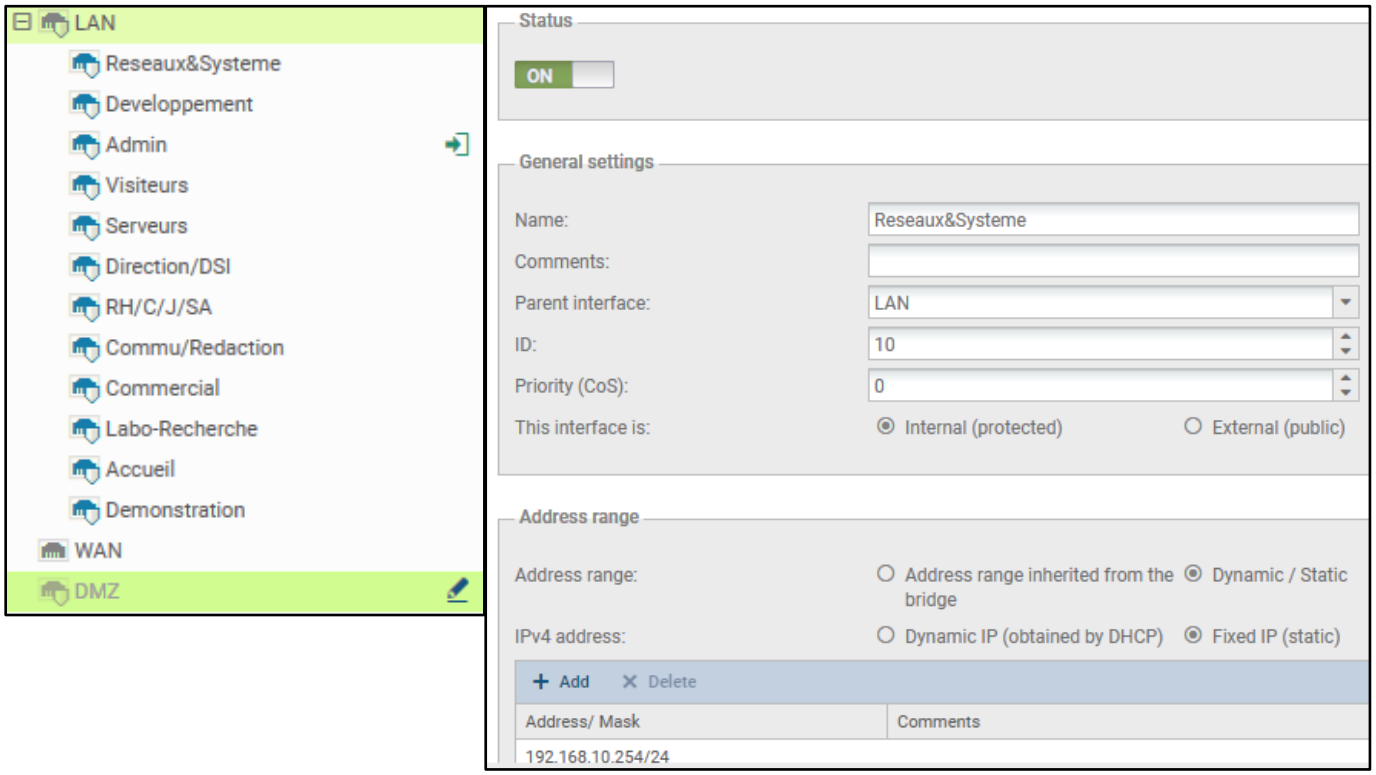


- Configuration DMZ :

  ⇒ *NETWORK → Interfaces*



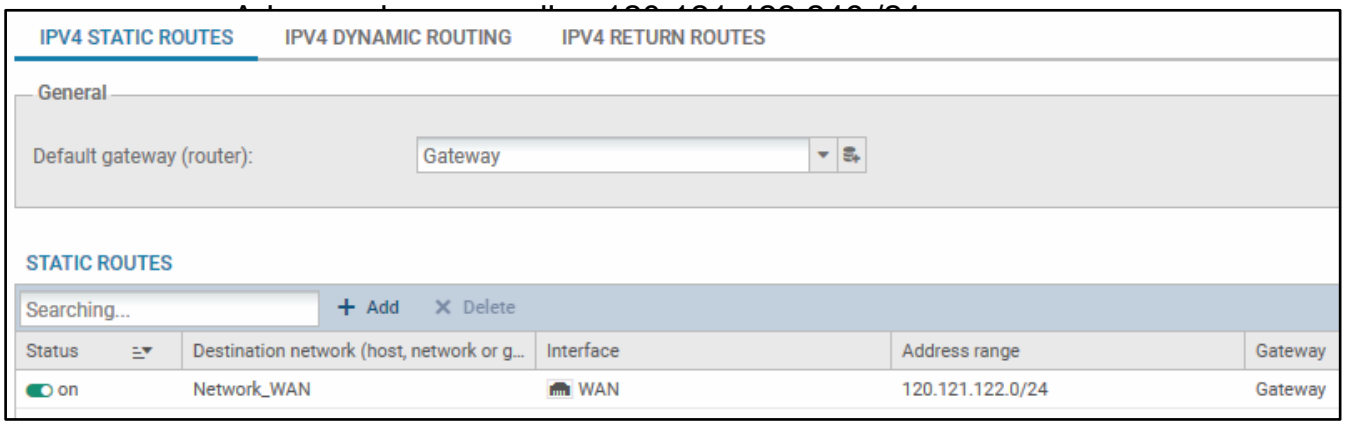
3) Création et configuration des VLANs :



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

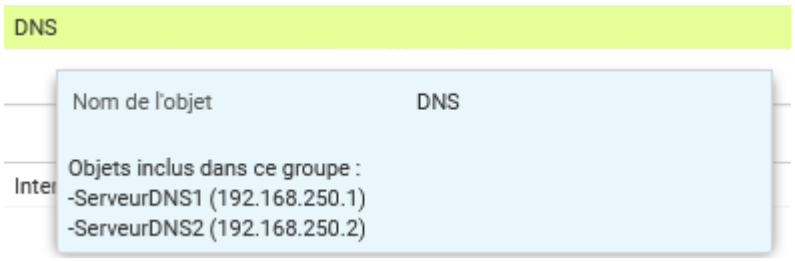
4) Création et configuration passerelle :

⇒ *NETWORK → Routing*



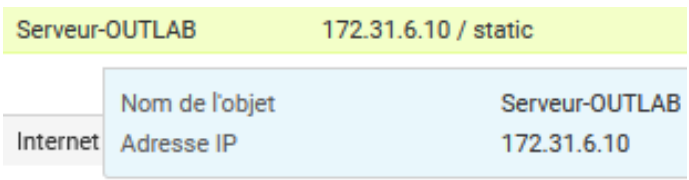
5) Création et configuration des ACL :

- *Création des objets :*



Contient les 2 DNS LABANNU

Contient tous les vlan sauf le vlan visiteurs



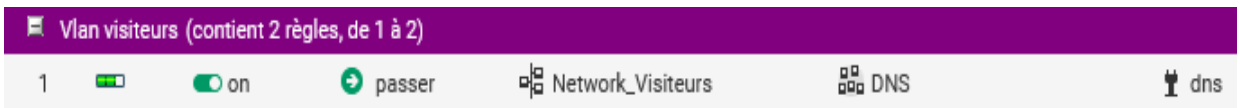
- Règle de filtrage (ACL):

➢ *Accès bloqué pour le vlan serveurs vers internet*

➢ *Accès autorisé pour tous les vlans vers internet*

➢ 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 :



➢ 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		on	passer	Network_internals		Network_internals		Any	icmp (requête Echo	IPS	Créée le 2024-03-13 08:37:04, par admin (192.168.99.21)
2		on	passer	Network_internals		Any		Any	icmp (requête Echo	IPS	Créée le 2024-03-13 08:37:04, par admin (192.168.99.21) - Mise...
Nutanix (contient 1 règles, de 3 à 3)										
3		on	passer	Network_Admin		Server_NUTANIX		Any		IPS	Créée le 2024-04-03 08:56:39, par admin (192.168.99.21)
Vlan visiteurs (contient 4 règles, de 4 à 7)										
4		on	passer	Network_Visiteurs		DNS_INTERNE		dns		IPS	Créée le 2023-12-13 09:19:11, par admin (192.168.99.23)
5		on	bloquer	Network_Visiteurs		Network_Serveurs		Any		IPS	Créée le 2023-12-13 09:05:49, par admin (192.168.99.23)
6		on	passer	Network_Visiteurs		Internet		http https		IPS	Créée le 2023-12-06 08:58:01, par admin (192.168.99.21) - Mise...
7		on	bloquer	Network_Visiteurs		Network-Entreprise		Any		IPS	Créée le 2023-12-06 08:58:01, par admin (192.168.99.21) - Mise...
DNS (contient 6 règles, de 8 à 13)										
8		on	passer	Network_Serveurs		Network_Serveurs		snmp		IPS	Créée le 2024-04-17 10:39:03, par admin (192.168.99.23)
9		on	passer	ServeurDNS_DMZ		ServeurDNS_Internet		dns		IPS	Créée le 2023-12-13 09:35:09, par admin (192.168.99.23)
10		on	passer	ServeurDNS_DMZ		Internet		dns		IPS	Créée le 2023-12-13 09:35:09, par admin (192.168.99.23) - Mise...
11		on	passer	ServeurDNS_LABANNU1		ServeurDNS_DMZ		dns		IPS	Créée le 2024-03-13 11:34:21, par admin (192.168.99.21)
12		on	passer	ServeurDNS_LABANNU2		ServeurDNS_DMZ		dns		IPS	Créée le 2024-03-13 11:34:21, par admin (192.168.99.21) - Mise...
13		on	passer	Network-Entreprise		LABANNU_DNS		dns		IPS	Créée le 2023-12-06 08:58:01, par admin (192.168.99.21) - Mise...
Network Entreprise accès (contient 2 règles, de 14 à 15)										
14		on	passer	Network-Entreprise		Network_Serveurs		Any		IPS	Créée le 2024-04-02 15:34:05, par admin (192.168.99.21)
15		on	passer	Network-Entreprise		Network_DMZ		Any		IPS	Créée le 2024-04-02 15:34:05, par admin (192.168.99.21) - Mise...
Accès DMZ (contient 4 règles, de 16 à 19)										
16		on	passer	Internet		Firewall_WAN		dns		IPS	Créée le 2024-03-13 10:52:54, par admin (192.168.99.21)
17		on	passer	Internet		Firewall_WAN		http https		IPS	Créée le 2023-12-13 10:31:11, par admin (192.168.99.23)
18		on	passer	Network_internals		swiss-galaxyC2.com		http https		IPS	Créée le 2023-12-13 11:03:40, par admin (192.168.99.23)
DNS (contient 6 règles, de 8 à 13)										
8		on	passer	Network_Serveurs		Network_Serveurs		snmp		IPS	Créée le 2024-04-17 10:39:03, par admin (192.168.99.23)
9		on	passer	ServeurDNS_DMZ		ServeurDNS_Internet		dns		IPS	Créée le 2023-12-13 09:35:09, par admin (192.168.99.23)
10		on	passer	ServeurDNS_DMZ		Internet		dns		IPS	Créée le 2023-12-13 09:35:09, par admin (192.168.99.23) - Mise...
11		on	passer	ServeurDNS_LABANNU1		ServeurDNS_DMZ		dns		IPS	Créée le 2024-03-13 11:34:21, par admin (192.168.99.21)
12		on	passer	ServeurDNS_LABANNU2		ServeurDNS_DMZ		dns		IPS	Créée le 2024-03-13 11:34:21, par admin (192.168.99.21) - Mise...
13		on	passer	Network-Entreprise		LABANNU_DNS		dns		IPS	Créée le 2023-12-06 08:58:01, par admin (192.168.99.21) - Mise...
Network Entreprise accès (contient 2 règles, de 14 à 15)										
14		on	passer	Network-Entreprise		Network_Serveurs		Any		IPS	Créée le 2024-04-02 15:34:05, par admin (192.168.99.21)
15		on	passer	Network-Entreprise		Network_DMZ		Any		IPS	Créée le 2024-04-02 15:34:05, par admin (192.168.99.21) - Mise...
Accès DMZ (contient 4 règles, de 16 à 19)										
16		on	passer	Internet		Firewall_WAN		dns		IPS	Créée le 2024-03-13 10:52:54, par admin (192.168.99.21)
17		on	passer	Internet		Firewall_WAN		http https		IPS	Créée le 2023-12-13 10:31:11, par admin (192.168.99.23)
18		on	passer	Network_internals		swiss-galaxyC2.com		http https		IPS	Créée le 2023-12-13 11:03:40, par admin (192.168.99.23)
19		on	passer	Network_internals		zabbix.swiss-galaxyC2.com		http https		IPS	Créée le 2023-12-13 11:03:40, par admin (192.168.99.23) - Mise...
Accès Internet (contient 2 règles, de 20 à 21)										
20		on	bloquer	Network_Serveurs		Internet		Any		IPS	Créée le 2023-12-06 09:00:50, par admin (192.168.99.21)
21		on	passer	Network-Entreprise		Internet		http https		IPS	Créée le 2023-12-06 08:58:01, par admin (192.168.99.21)
Accès routeur (contient 2 règles, de 22 à 23)										
22		on	passer	Any		Firewall_Admin		firewall_srv https		IPS	Admin from everywhere
23		on	passer	Any		firewall_all		Any	icmp (requête Echo	IPS	Allow Ping from everywhere
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		on	bloquer	Any		Any		Any		IPS	Block all - Mise à jour le 2023-12-06 10:36:03 par admin (192.16...