

Ajout d'une startup réseau dans l'infrastructure

- **Attribuer une plage d'adresse pour la startup**

Plage d'adresse de la nouvelle startup :

VLAN StartupITservices = 172.17.4.224 → 172.17.4.254 (SVI)

Vérifier si l'interface du vlan existe déjà avec **show ip interface brief**.

- **Ajout de la startup dans switch coeur 1**

Se connecter sur un port MANA, et mettre une ip du même réseau en static.

Se connecter en SSH (SVI MANA) sur le Switch

Commande pour ajouter une startup :

vlan140

name VLAN startup itservices

interface vlan 140

ip address 172.17.4.224 255.255.255.224

interface vlan 140

ip helper-address 192.168.20.1 (adresse du serveur DHCP)

- **Voir le switch access**

Pinger la passerelle (SVI) du nouveau VLAN.

Le VLAN est directement descendu du Switch Coeur grâce au VTP.

- **Attribuer des ports au nouveau VLAN**

Sur le Switch Access :

Attribution port n°15 et 16 sur le switch Access 1.

Commande pour l'attribution des port au nouveau vlan :

int fa0/15

int fa0/16

switchport access vlan 140

switchport mode access

- **Test ping inter-vlan (d'un vlan à un autre)**

1. Brancher son PC sur le port 15, changer son ip pour la mettre sur le même réseau que VLAN140. (172.17.5.10)
2. Pinguer sa SVI, puis une autre (SERVER), afin de voir si le routage fonctionne
3. Pinguer la SVI_EXIT du Switch Coeur 192.168.92.6
4. Pinguer le VLAN EXIT (IN du stormshield) 192.168.92.1

- **Test ping intra-vlan (Ping entre les hôtes du même VLAN (PC1 vers PC2))**

Mettre les pc dans le même réseau (VLAN140)

- **Faire une nouvelle étendue DHCP**

Se connecter sur MANA, changer son ip, aller sur le lien Proxmox, et sur la machine ADDS.

Aller dans le serveur ADDS, se connecter avec l'admin du domaine (ex : Adrien, S101..)

Faire : Outil, DHCP, IPV4, Étendue, Clic droit, Créer une étendu.

Notre etendue : 172.17.4.230 → 172.17.4.240 mask : 255.255.255.224 / bail : 4 heures / routeur (passerelle par défaut) : 172.17.4.254

Aller dans "option d'étendue" afin de voir si tout est bien configuré

Tester une ip en étant en DHCP

Faire les commande "ipconfig / renew" et "ipconfig /all" dans le CMD

- **Firewall - 192.168.21.251**

Créer une route pour le vlan qui veut avoir accès à internet

Dans l'onglet route du stormshield, créer une route statique

172.17.4.254 - interface in du stormshield – range 172.17.0.0/27 – interface exit du switch coeur

- **Règle NAT (translation ip privé vers ip public pour accéder à internet)**

➦ SECURITY POLICY / FILTER - NAT

<div> (1) Block all <div> Edit Export ⓘ </div> </div>									
<div> <div>FILTERING NAT</div> <div> Searching... + New rule X Delete ↑ ↓ ↺ ↻ Cut Copy Paste Search in logs Search in monitoring ⋮ </div> </div>									
	Status	Original traffic (before translation)			Traffic after translation				
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port	
	on	Network_in:in	Internet interface: out	Any	Firewall_out	ephemera	Any		

- **Exemple règles de filtrage (dns, https et icmp)**

➦ SECURITY POLICY / FILTER - NAT

(1) Block all

Edit

Export

FILTERING

NAT

Searching...

+ New rule

X Delete

↑

↓

↶

↷

Cut

Copy

Paste

Search in logs

Search in monitoring

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
1	<div><div></div>on</div>	<div><div></div>pass</div>	<div><div></div>Network_in</div>	<div><div></div>Internet</div>	<div><div></div>Any</div>	icmp	<div><div></div>IPS</div>	Created on 2025-01-...
2	<div><div></div>on</div>	<div><div></div>pass</div>	<div><div></div>Network_in</div>	<div><div></div>Internet</div>	<div><div></div>https</div>		<div><div></div>IPS</div>	Created on 2025-01-...
<div>Remote Management: Go to System - Configuration to setup the web administration application access (contains 3 rules, from 3 to 5)</div>								
3	<div><div></div>on</div>	<div><div></div>pass</div>	<div><div></div>Any</div>	<div><div></div>Firewall_all</div>	<div><div></div>firewall_srv https</div>		<div><div></div>IPS</div>	Admin from everywh...
4	<div><div></div>on</div>	<div><div></div>pass</div>	<div><div></div>Any</div>	<div><div></div>Internet</div>	<div><div></div>dns</div>		<div><div></div>IPS</div>	Created on 2025-01-...
5	<div><div></div>on</div>	<div><div></div>pass</div>	<div><div></div>Any</div>	<div><div></div>Firewall_all</div>	<div><div></div>Any</div>	icmp	<div><div></div>IPS</div>	Allow Ping from ever...
<div>Separator - rule grouping (contains 2 rules, from 6 to 7)</div>								
6	<div><div></div>on</div>	<div><div></div>pass</div>	<div><div></div>TCP_VPN via SSL VPN tunnel</div>	<div><div></div>Network_in</div>	<div><div></div>Any</div>		<div><div></div>IPS</div>	Created on 2025-02-...
7	<div><div></div>on</div>	<div><div></div>pass</div>	<div><div></div>UDP_VPN via SSL VPN tunnel</div>	<div><div></div>Network_in</div>	<div><div></div>Any</div>		<div><div></div>IPS</div>	Created on 2025-02-...
<div>Default policy (contains 1 rules, from 8 to 8)</div>								
8	<div><div></div>on</div>	<div><div></div>block</div>	<div><div></div>Any</div>	<div><div></div>Network_in</div>	<div><div></div>Any</div>		<div><div></div>IPS</div>	Block all - Updated o...

<<

<

Page 1 of 1

>

>>

↺

Displaying 1 - 11 of 11

1er règle de filtrage : Network_in vers internet - protocole icmp

2ème règle de filtrage : Network_in vers internet - dest port https

3ème règle de filtrage : any vers internet - dest port dns

- **Test ping internet**

Pinguer le DNS 8.8.8.8 (Google)

