stormshield-int-ext

```
    MARK RODERICK - Stormshield interne et externe
```

2.1. Conception d’une solution d’infrastructure

ROUTAGE

	user 1 bureatique	**user 2 production**	**Srv - Authentififcation**	**IT**	**wi**
user 1 bureatique	~~==xxxxxxx~~x==	*Interdit*	Acces	*Interdit*	*Int*
user 2 production	*Interdit*	~~==xxxxxxx~~x==	Acces	*Interdit*	*Int*
Srv - Authentififcation	Acces- statefull	Acces - statefull	~~==xxxxxxx~~x==	Acces	*Int*
IT	Acces	Acces	Acces	~~==xxxxxxx~~x==	Ac
WIFI	*Interdit*	*Interdit*	*Interdit*	*Interdit*	~~==
Backup redondance	*Interdit*	*Interdit*	*Interdit*	Acces	*Int*

state full firewall = analyse les requetés qui sort , laisse passer les réponses
serveur de supervision = protocol snmp (simple network management Protocol)

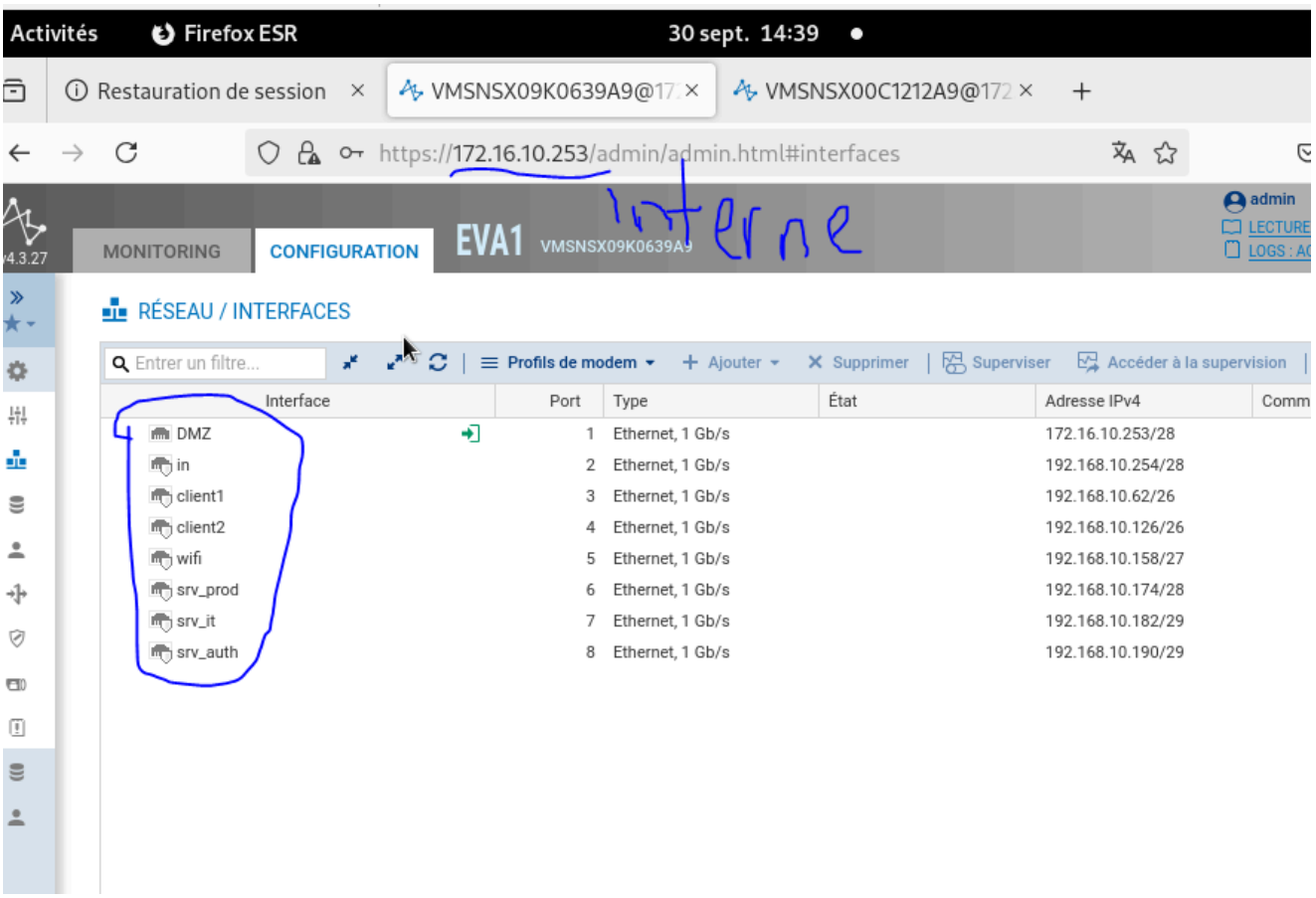
Source	**Destination**	**Service(Port destination)**	**Action**	**Description**	**Précision**
user 1 bureatique	Srv - Authentififcation	LDAP	Autoriser		Acces efficace aux outils de travaille
user 2 production	Srv - Authentififcation	LDAP	Autoriser		Acces efficace aux outils de travaille
Srv - Authentififcation	Backup redondance	SSH	Autoriser		Authentifier les utilisateurs
	Internet		Autoriser		
IT	Srv - Authentififcation	ANY	Autoriser		Facilite l'acces

Source	Destination	Service(Port destination)	Action	Description	Précision
					pour les utilisateurs, user 1 & 2
WIFI	IT		Autoriser		
Backup redondance	IT				Garde les donner accessible en cas d'une perte
Tous	Backup redondance				

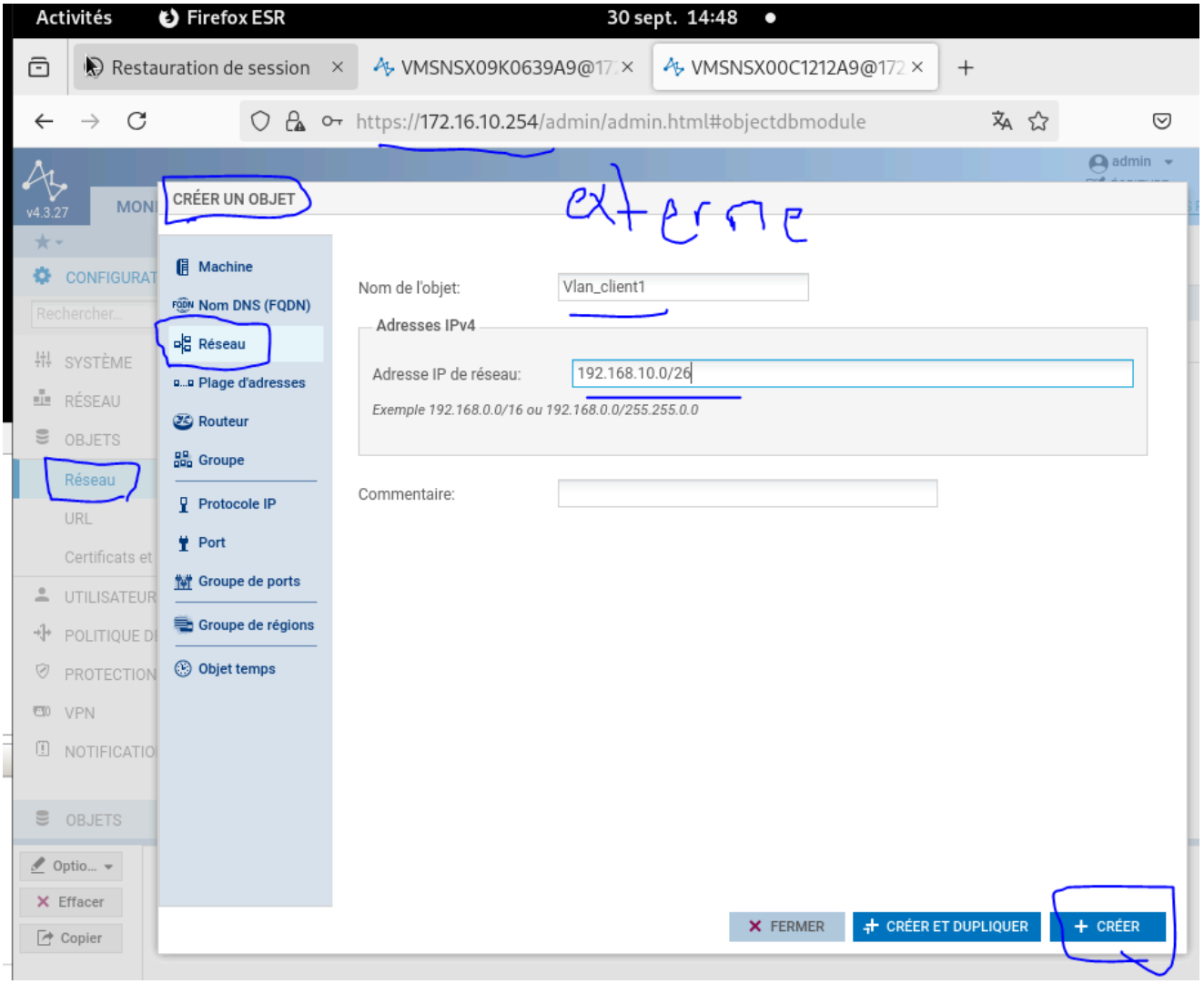
cve =
SMB = Partage réseau - attaque ransomeware

Les interfaces *internes* Stormshield servent à protéger et organiser le réseau local (LAN), tandis que les interfaces *externes* sont dédiées à la connexion vers Internet (WAN). La distinction est cruciale car elle permet de filtrer, contrôler et sécuriser les flux entrants et sortants, évitant ainsi les intrusions et les attaques

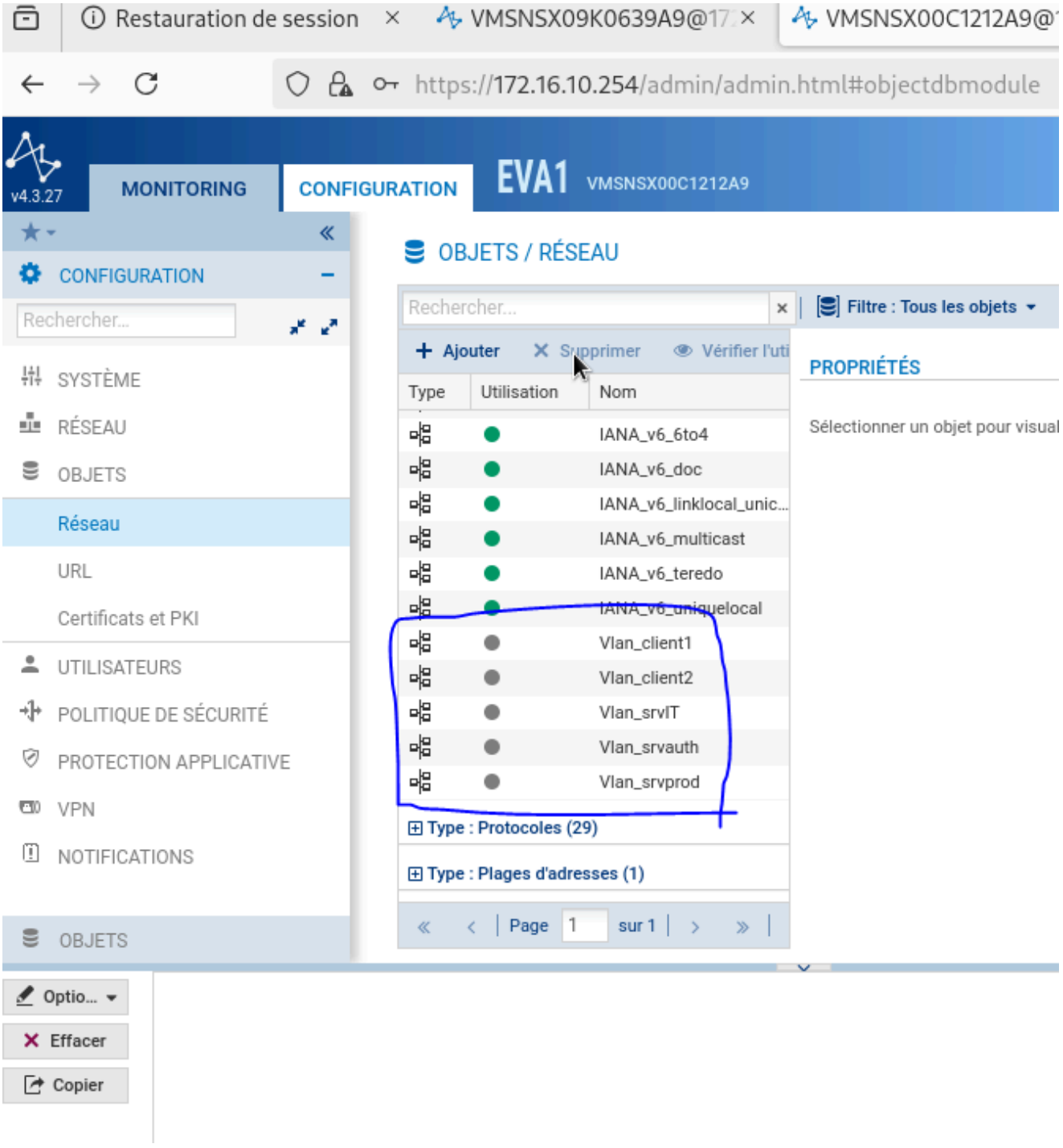
- **Interface externe (OUT/WAN)**
  - Reliée directement à Internet ou à un réseau public.
  - Sert de point d’entrée et de sortie pour tout le trafic externe.
  - Exposée aux menaces (attaques, intrusions, usurpations IP).
  - Nécessite des règles de sécurité strictes (filtrage, IPS/IDS, antivirus, antispam).
- **Interface interne (IN/LAN)**
  - Connectée au réseau local de l’entreprise (ordinateurs, serveurs, imprimantes).
  - Protège les ressources internes contre les accès non autorisés.
  - Permet de segmenter le réseau (ex. : utilisateurs, serveurs sensibles, DMZ).
  - Généralement considérée comme « zone de confiance », mais toujours filtrée pour éviter les menaces internes.
- **Interfaces DMZ (zone démilitarisée)**
  - Option intermédiaire entre interne et externe.
  - Héberge des services accessibles depuis Internet (sites web, serveurs mail).
  - Séparée du LAN pour éviter qu’une attaque sur ces services compromette tout le réseau



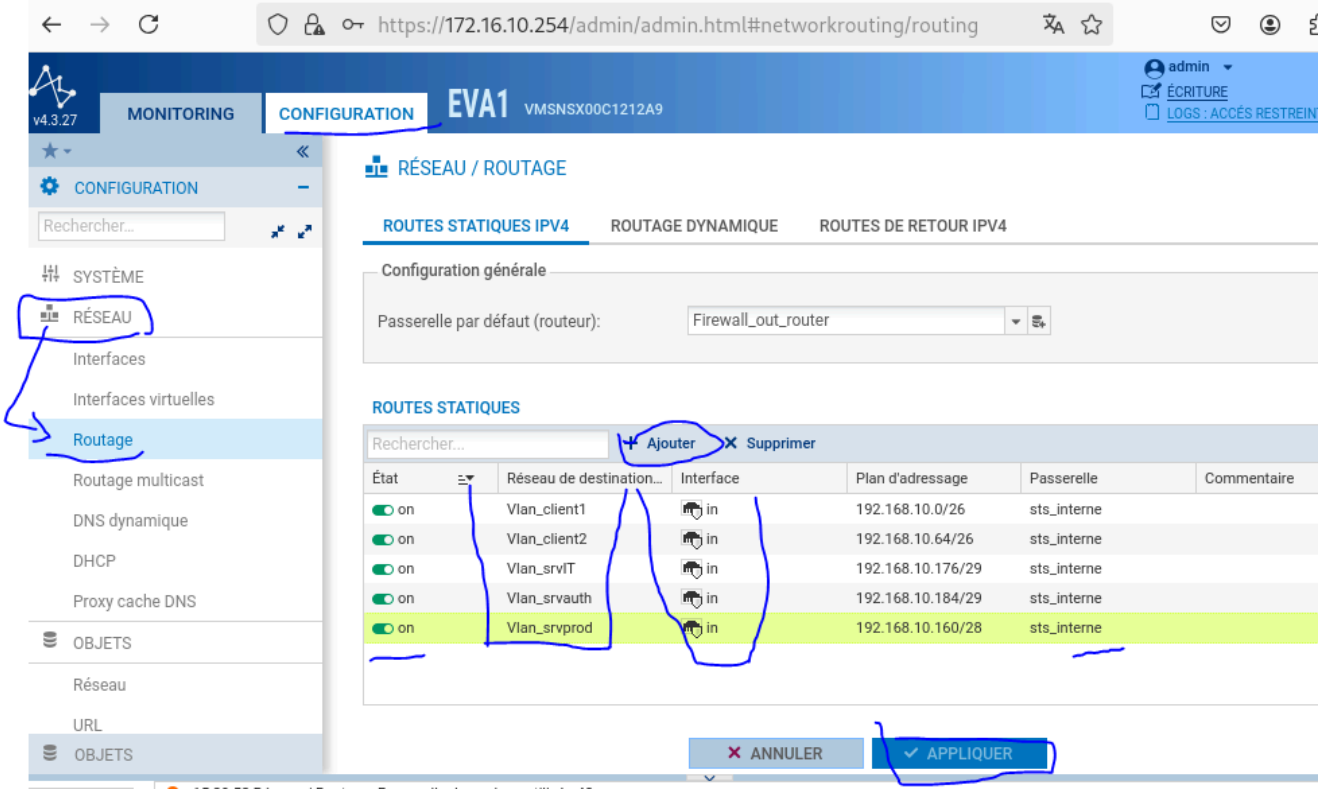
creer des objets



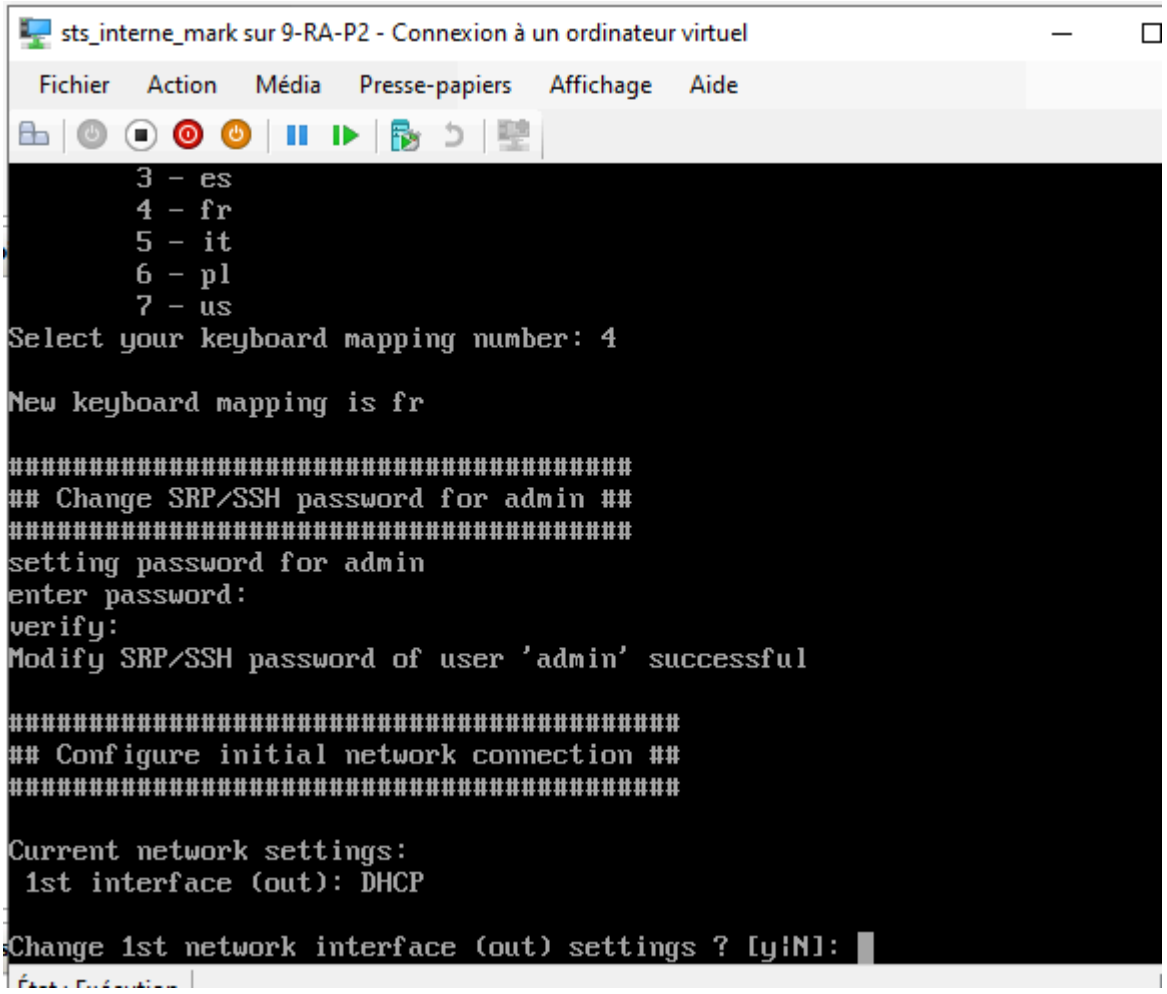
sur externe dans objets >> reseau



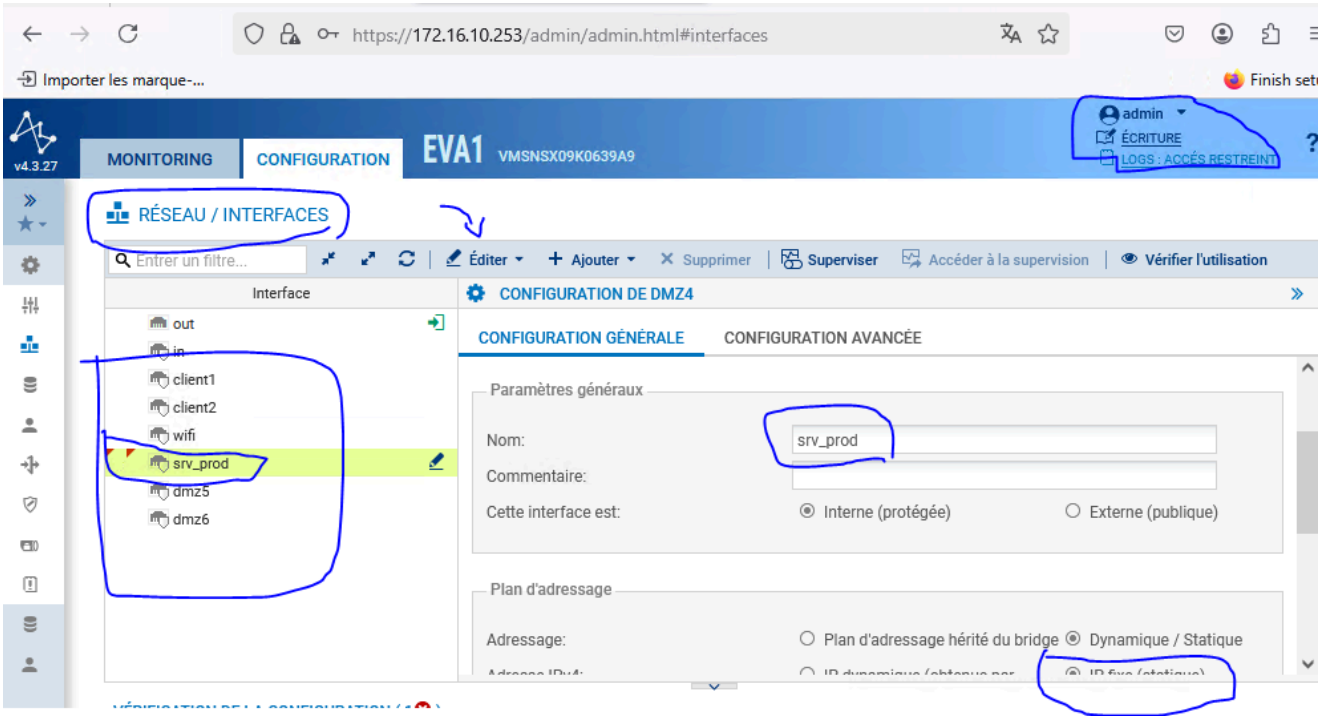
Routage



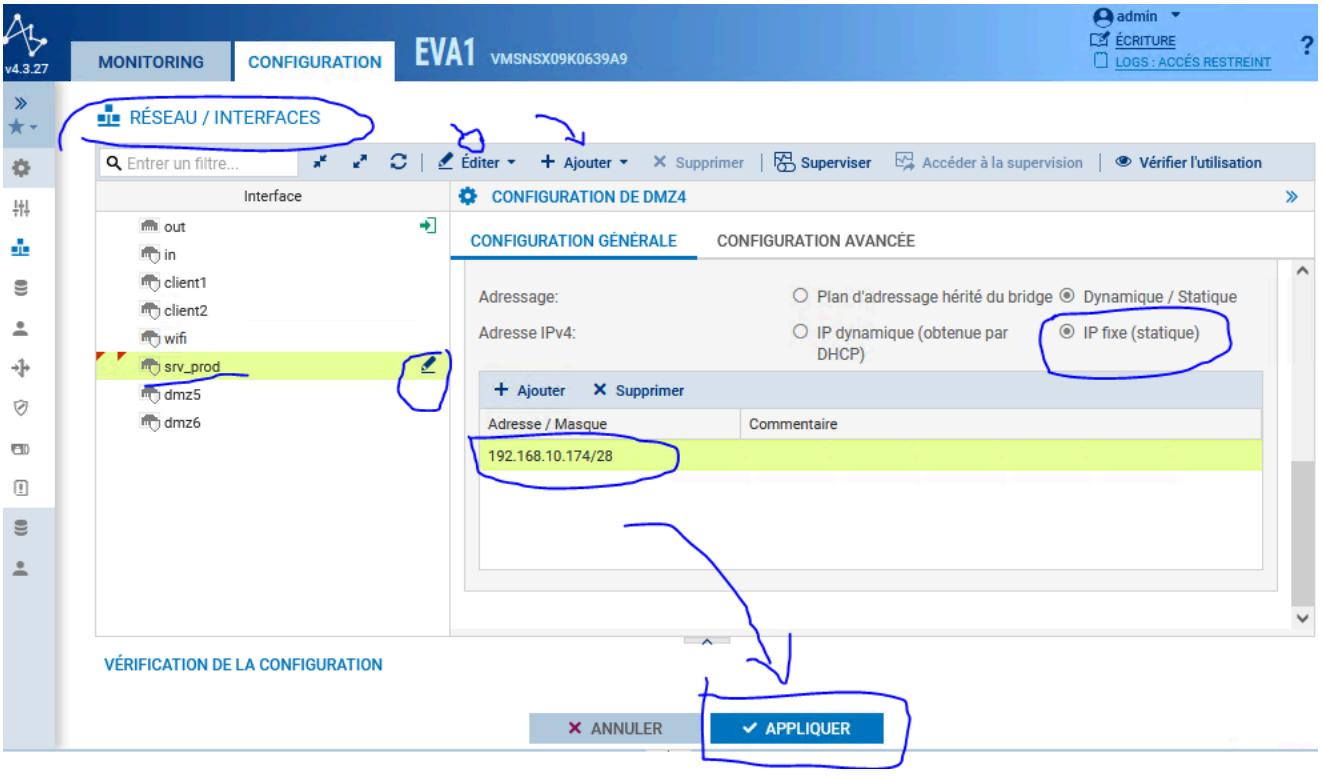
sts intern



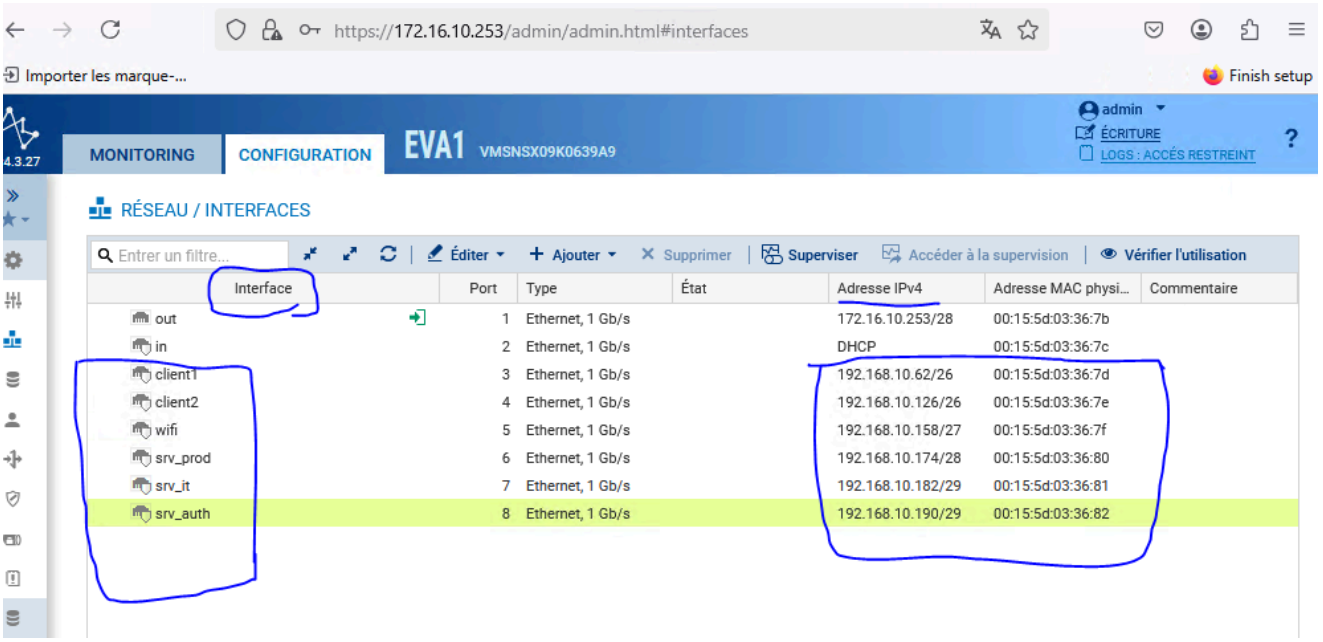
configuration srv



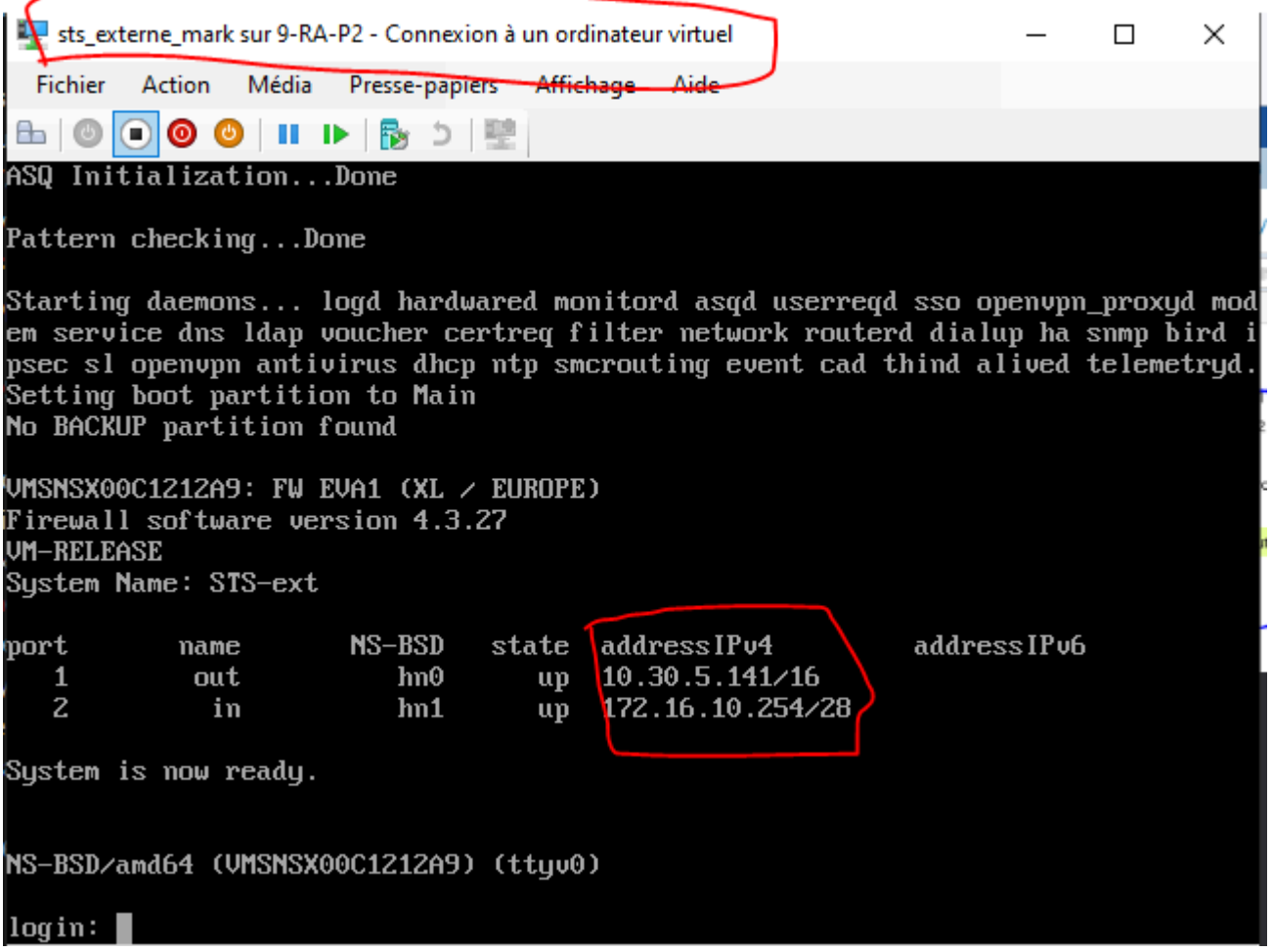
srv production



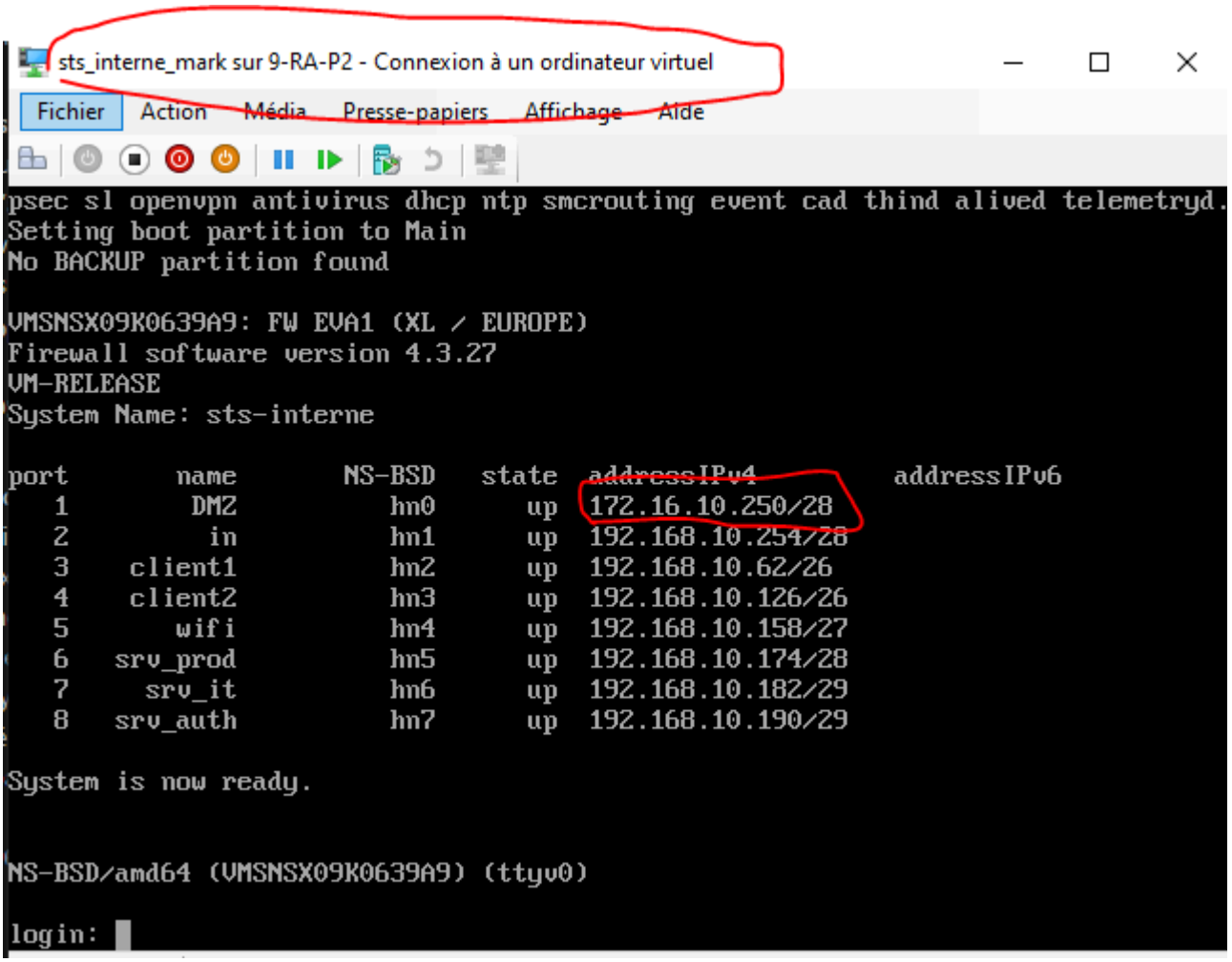
authentification

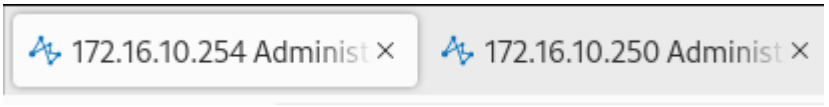


STS EXTERNE



STS INTERNE


sts_interne_mark sur 9-RA-P2 - Connexion à un ordinateur virtuel
Fichier
Action
Média
Presse-papiers
Affichage
Aide
psec sl openvpn antivirus dhcp ntp smcrouting event cad thind alived telemetryd.
Setting boot partition to Main
No BACKUP partition found
VMSNSX09K0639A9: FW EVA1 (XL / EUROPE)
Firewall software version 4.3.27
VM-RELEASE
System Name: sts-interne
port name NS-BSD state addressIPv4 addressIPv6
1 DMZ hn0 up 172.16.10.250/28
2 in hn1 up 192.168.10.254/28
3 client1 hn2 up 192.168.10.62/26
4 client2 hn3 up 192.168.10.126/26
5 wifi hn4 up 192.168.10.158/27
6 srv_prod hn5 up 192.168.10.174/28
7 srv_it hn6 up 192.168.10.182/29
8 srv_auth hn7 up 192.168.10.190/29
System is now ready.
NS-BSD/amd64 (VMSNSX09K0639A9) (ttyv0)
login:


172.16.10.254 Administ
172.16.10.250 Administ