

# stormshield-int-ext

MARK RODERICK - Stormshield interne et externe

## 2.1. Conception d'une solution d'infrastructure

### ROUTAGE

	<b>user 1 bureatique</b>	<b>user 2 production</b>	<b>Srv - Authentification</b>	<b>IT</b>	<b>wi</b>
user 1 bureatique	<del>==xxxxxxxx==</del>	<i>Interdit</i>	Acces	<i>Interdit</i>	<i>Int</i>
user 2 production	<i>Interdit</i>	<del>==xxxxxxxx==</del>	Acces	<i>Interdit</i>	<i>Int</i>
Srv - Authentification	Acces- statefull	Acces - statefull	<del>==xxxxxxxx==</del>	Acces	<i>Int</i>
IT	Acces	Acces	Acces	<del>==xxxxxxxx==</del>	Ac
WIFI	<i>Interdit</i>	<i>Interdit</i>	<i>Interdit</i>	<i>Interdit</i>	<del>==</del>
Backup redondance	<i>Interdit</i>	<i>Interdit</i>	<i>Interdit</i>	Acces	<i>Int</i>

state full firewall = analyse les requetés qui sort , laisse passer les réponses

serveur de supervision = protocol snmp (simple network management Protocol)

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

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

Activités Firefox ESR 30 sept. 14:39

Restoration de session x VMSNSX09K0639A9@17 x VMSNSX00C1212A9@172 x +

https://172.16.10.253/admin/admin.html#interfaces

admin LECTURE LOGS: A

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 *interne*

RÉSEAU / INTERFACES

Entrer un filtre... Profils de modem + Ajouter x Supprimer | Superviser Accéder à la supervision

Interface	Port	Type	État	Adresse IPv4	Comm
DMZ	1	Ethernet, 1 Gb/s		172.16.10.253/28	
in	2	Ethernet, 1 Gb/s		192.168.10.254/28	
client1	3	Ethernet, 1 Gb/s		192.168.10.62/26	
client2	4	Ethernet, 1 Gb/s		192.168.10.126/26	
wifi	5	Ethernet, 1 Gb/s		192.168.10.158/27	
srv_prod	6	Ethernet, 1 Gb/s		192.168.10.174/28	
srv_it	7	Ethernet, 1 Gb/s		192.168.10.182/29	
srv_auth	8	Ethernet, 1 Gb/s		192.168.10.190/29	

creer des objets

Activités Firefox ESR 30 sept. 14:48

Restoration de session x VMSNSX09K0639A9@17 x VMSNSX00C1212A9@172 x +

https://172.16.10.254/admin/admin.html#objectdbmodule

admin

CRÉER UN OBJET *externe*

Machine

Nom DNS (FQDN)

Réseau

Plage d'adresses

Routeur

Groupe

Protocole IP

Port

Groupe de ports

Groupe de régions

Objet temps

Nom de l'objet:

Adresses IPv4

Adresse IP de réseau:

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire:

FERMER CRÉER ET DUPLIQUER **CRÉER**

sur externe dans objets >> reseau

The screenshot shows the Fortinet configuration interface for device EVA1. The main content area is titled 'OBJETS / RÉSEAU' and displays a table of network objects. A blue box highlights the following objects:

Type	Utilisation	Nom
IANA_v6_6to4	●	IANA_v6_6to4
IANA_v6_doc	●	IANA_v6_doc
IANA_v6_linklocal_unic...	●	IANA_v6_linklocal_unic...
IANA_v6_multicast	●	IANA_v6_multicast
IANA_v6_teredo	●	IANA_v6_teredo
IANA_v6_uniquelocal	●	IANA_v6_uniquelocal
Vlan_client1	●	Vlan_client1
Vlan_client2	●	Vlan_client2
Vlan_srvIT	●	Vlan_srvIT
Vlan_srvaath	●	Vlan_srvaath
Vlan_srvprod	●	Vlan_srvprod

Below the table, there are expandable sections for 'Type : Protocoles (29)' and 'Type : Plages d'adresses (1)'. The interface also includes a sidebar with navigation options like SYSTÈME, RÉSEAU, and OBJETS, and a main content area with a table of objects and a 'PROPRIÉTÉS' panel.

Routage

MONITORING CONFIGURATION EVA1 VMSNSX00C1212A9

admin ÉCRITURE LOGS : ACCÈS RESTREINT

CONFIGURATION

Rechercher...

SYSTÈME

RÉSEAU

Interfaces

Interfaces virtuelles

Routeur

Routeur multicast

DNS dynamique

DHCP

Proxy cache DNS

OBJETS

Réseau

URL

OBJETS

RÉSEAU / ROUTAGE

ROUTES STATIQUES IPV4 ROUTAGE DYNAMIQUE ROUTES DE RETOUR IPV4

Configuration générale

Passerelle par défaut (routeur): Firewall\_out\_router

ROUTES STATIQUES

Rechercher... Ajouter Supprimer

État	Réseau de destination...	Interface	Plan d'adressage	Passerelle	Commentaire
on	Vlan_client1	in	192.168.10.0/26	sts_interne	
on	Vlan_client2	in	192.168.10.64/26	sts_interne	
on	Vlan_srvIT	in	192.168.10.176/29	sts_interne	
on	Vlan_srvauth	in	192.168.10.184/29	sts_interne	
on	Vlan_srvprod	in	192.168.10.160/28	sts_interne	

ANNULER APPLIQUER

sts intern

```

sts_interne_mark sur 9-RA-P2 - Connexion à un ordinateur virtuel
Fichier Action Média Presse-papiers Affichage Aide
3 - es
4 - fr
5 - it
6 - pl
7 - us
Select your keyboard mapping number: 4
New keyboard mapping is fr
#####
## Change SRP/SSH password for admin ##
#####
setting password for admin
enter password:
verify:
Modify SRP/SSH password of user 'admin' successful
#####
## Configure initial network connection ##
#####
Current network settings:
1st interface (out): DHCP
Change 1st network interface (out) settings ? [y|N]:

```

configuration srv

The screenshot shows the Mikrotik WinBox interface for configuring a DMZ4 interface. The browser address bar displays `https://172.16.10.253/admin/admin.html#interfaces`. The page title is "EVA1 VMSNSX09K0639A9". The user is logged in as "admin" with "ÉCRITURE" (write) permissions and "LOGS : ACCÈS RESTREINT" (restricted log access). The "CONFIGURATION" tab is active, and the "RÉSEAU / INTERFACES" menu is highlighted. The "CONFIGURATION DE DMZ4" window is open, showing the "CONFIGURATION GÉNÉRALE" tab. The "Nom:" field is set to "srv\_prod". The "Cette interface est:" radio buttons are set to "Interne (protégée)". The "Plan d'adressage" section shows "Adresse:" set to "Plan d'adressage hérité du bridge" and "Adresse IPv4:" set to "IP fixe (statique)".

### srv production

The screenshot shows the Mikrotik WinBox interface for configuring the IP address for the DMZ4 interface. The "CONFIGURATION DE DMZ4" window is open, showing the "CONFIGURATION GÉNÉRALE" tab. The "Adresse IPv4:" radio buttons are set to "IP fixe (statique)". The "Adresse / Masque" table is populated with the following entry:

Adresse / Masque	Commentaire
192.168.10.174/28	

The "APPLIQUER" button is highlighted, indicating the configuration is being applied.

### authentification

Browser address: https://172.16.10.253/admin/admin.html#interfaces

Page title: **EVA1** VMSNSX09K0639A9

Navigation: MONITORING | CONFIGURATION

Section: RÉSEAU / INTERFACES

Interface	Port	Type	État	Adresse IPv4	Adresse MAC physi...	Commentaire
out	1	Ethernet, 1 Gb/s		172.16.10.253/28	00:15:5d:03:36:7b	
in	2	Ethernet, 1 Gb/s		DHCP	00:15:5d:03:36:7c	
client1	3	Ethernet, 1 Gb/s		192.168.10.62/26	00:15:5d:03:36:7d	
client2	4	Ethernet, 1 Gb/s		192.168.10.126/26	00:15:5d:03:36:7e	
wifi	5	Ethernet, 1 Gb/s		192.168.10.158/27	00:15:5d:03:36:7f	
srv_prod	6	Ethernet, 1 Gb/s		192.168.10.174/28	00:15:5d:03:36:80	
srv_it	7	Ethernet, 1 Gb/s		192.168.10.182/29	00:15:5d:03:36:81	
srv_auth	8	Ethernet, 1 Gb/s		192.168.10.190/29	00:15:5d:03:36:82	

### STS EXTERNE

Terminal window: sts\_externe\_mark sur 9-RA-P2 - Connexion à un ordinateur virtuel

```

ASQ Initialization...Done
Pattern checking...Done
Starting daemons... logd hardwared monitord asqd userreqd sso openvpn_proxymod
em service dns ldap voucher certreq filter network routerd dialup ha snmp bird i
psec sl openvpn antivirus dhcp ntp smcrouting event cad thind alived telemetryd.
Setting boot partition to Main
No BACKUP partition found

VMSNSX00C1212A9: FW EVA1 (XL / EUROPE)
Firewall software version 4.3.27
VM-RELEASE
System Name: STS-ext

port      name      NS-BSD   state   address IPv4      address IPv6
  1        out      hm0     up     10.30.5.141/16
  2        in       hm1     up     172.16.10.254/28

System is now ready.

NS-BSD/amd64 (VMSNSX00C1212A9) (ttyv0)
login:
  
```

### 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  address IPv4  address IPv6
1         DMZ       hm0     up     172.16.10.250/28
2         in        hm1     up     192.168.10.254/28
3         client1   hm2     up     192.168.10.62/26
4         client2   hm3     up     192.168.10.126/26
5         wifi      hm4     up     192.168.10.158/27
6         srv_prod  hm5     up     192.168.10.174/28
7         srv_it    hm6     up     192.168.10.182/29
8         srv_auth  hm7     up     192.168.10.190/29

System is now ready.

NS-BSD/amd64 (VMSNSX09K0639A9) (ttyu0)
login: 
```

172.16.10.254 Administr x 172.16.10.250 Administr x