15/12/2024

Mise en place de Stormshield Virtuel (SNS)

Proxmox

Mamadou CAMARA [NOM DE LA SOCIETE]

SOMMAIRE

1. Contexte :

Agence	ID VLAN	Adresses de sous- réseaux	Adresses IP de notre firewall Stormshield
Kayes	346	DMZ: 172.16.11.0/24	dmz : 172.16.11.254
	347	SERVEURS : 172.16.31.0/24	Seveurs: 172.16.31.254
	348	LAN 1: 192.168.11.0/24	Lan1:192.168.11.254
	349	LAN 2: 192.168.31.0/24	Lan2:192.168.31.254
	302	WAN: 192.168.229.0/26	Out: 192.168.229.36



2. Clonage du Template Modele-SNS-4.3 (Clone lié) :

Clone VM Ten	nplate 278			\otimes
Nœud cible:	siohyp2	Mode:	Clone lié	\sim
VM ID:	300 🗘	Stockage cible:	Identique à la source	
Nom:	SNS-kayes	Format:	Image au format QEMU	
Pool de ressources:	SIO2023_SISR_2_E × V			
Aide			Clon	er

3. Définir les VLAN de chaque interface

Pour définir les VLAN de chaque interface, on click sur le Taplante, on va dans Materiel. Pour l'interface net0 (Out) on met réseau wifi-cub-wan pour pouvoir accéder à l'interface graphique du Stormhield via l'adresse IP obtenue en dhcp lors de l'installation du pare-feu Virtuel.

Sur les autres interfaces, on met nos VLAN internes (LAN1, LAN2, DMZ, Serveur)

	Ajouter v Supprimer	Éditer Action disque V Revenir en arrière
	Mémoire	1.00 Gio
۲	Processeurs	2 (1 sockets, 2 cores) [x86-64-v2-AES]
	BIOS	Par défaut (SeaBIOS)
F	Affichage	Par défaut
Q,	Machine	Par défaut (i440fx)
9	Contrôleur SCSI	VirtIO SCSI single
0	Lecteur CD/DVD (ide2)	none,media=cdrom
æ	Disque dur (scsi0)	gv0:295/vm-295-disk-0.qcow2,cache=writeback,iothread=1,size=10485824K
₽	Carte réseau (net0)	virtio=BC:24:11:FA:DB:C0,bridge=vmbr302,firewall=1
₽	Carte réseau (net1)	virtio=BC:24:11:A9:9E:2F,bridge=vmbr348,firewall=1
₽	Carte réseau (net2)	virtio=BC:24:11:B5:CF:6D,bridge=vmbr349,firewall=1
₽	Carte réseau (net3)	virtio=BC:24:11:30:CC:38,bridge=vmbr346,firewall=1
₽	Carte réseau (net4)	virtio=BC:24:11:E1:B7:A3,bridge=vmbr347,firewall=1

4. Démarrer la VM et répondre aux questions de l'assistant

NS-BSD/amd64 (VMSNSX09K0639A9) (ttyv0)										
login: Passwor	admin rd:									
VMSNSX	VMSNSX09K0639A9: FW EVA1 (XL / EUROPE)									
Firewa	ll software v	ersion 4.3.	30 VM-R	ELEASE						
port	name	NS-BSD	state	addressIPv4	addressIPv6					
1	out	vtnet0	սթ	192.168.229.36/26						
2	lan1	vtnet1	սթ	192.168.11.254/24						
3	lan2	vtnet2	սթ	192.168.31.254/24						
4	dmz2	vtnet3	սթ	172.16.11.254/24						
5	Serveur	vtnet4	սթ	172.16.31.254/24						
UMSNSX	09K0639A9>									

NB : lors de l'installation du pare-feu sur proxmox, on laisse tous les interface en dhcp et on autorise l'accès de Stormshiel depuis l'interface Out.

5. Accéder à l'interface Web du SNS

https:// <adresse ip 'Out' en dhcp>

On modifiera ensuite l'adresse IP Out obtenu en DHCP par notre adresse IP publique externe : **192.168.229.36**

6. Activation du SNS

5.1 Mise à jour de la licence Dans **System/licence**

뷰 SYSTEM / LICENSE

GENERAL LICENSE DETAILS								
Search for a new license Install the new license								
Local firewall date: Tuesday 15th October 2024								
A new license is available for VMSNSX09K0639A9.								
Last check for license updates performed	Last check for license updates performed on:Tuesday 15th October 2024							
License will expire in 4825 days, on Thursday 31st December 2037.								
Maintenance will expire in 320 days, on S	unday 31st August 2025.							
Stormshield Vulnerability Manager will ex	pire in 320 days, on Sunday 31st August 2025.							
Advanced antivirus will expire in 320 days	s, on Sunday 31st August 2025.							
The Extended Web Control option has no	t been subscribed.							
Sandboxing Breach Fighter option will explore the second secon	pire in 320 days, on Sunday 31st August 2025.							
Industrial option will expire in 320 days, o	n Sunday 31st August 2025.							
Install license								
License file :	C:\fakepath\VMSNSX09K0639A9.licence							
	I Install							

On choisi le Fichier : VMSNSX09K0639A9.licence puis on click sur installer.

5.2 Mise en oeuvre de la HA

Le Kit d'activation/mise à jour est à utiliser pour le déploiement initial d'une nouvelle VM.

```
Fichier: vminit-VMSNSX09K0639A9.maj
```

掉 SYSTEM / MAINTENANCE								
SYSTEM UPDATE BACKUP RESTORE CO	DNFIGURATION							
Available updates								
4.3.31 - LTSB Download this update Version rel	ease notes sha1							
Q Check for new updates								
System update								
Select the update:								
	C Update firmware							
 Advanced properties 								

5.3 Mise à jour du Firmware

L'image est en version 4.3.27 LTSB. La mise à jour en version supérieure (4.3.30) peut être réalisée une fois l'installation initiale terminée, via l'interface d'administration du firewall. Utiliser le fichier **fwupd-4.3.30-SNS-amd64-XL-VM.maj** dans le menu Systeme > Maintenance

7. Configuration des interfaces réseaux

La première interface du pare-feu est nommée « OUT », la seconde « IN » et les restes des interfaces DMZ.

NB : L'interface OUT est une interface externe que l'on utilise pour pouvoir accéder à internet et le restes des interfaces sont internes.

Nous allons procéder à la configuration des inrfaces du pare-feu

La configuration des interfaces s'effectue dans le menu Configuration / Réseau / Interfaces

	NETWORK / I	INTERFACES	S							
Q, E	inter a filter	*	2	C 4	🛃 Edit 👻	+ Add +	X Delete 🔂 Monitor	Go to monit	toring 📔 👁 Check usage	
		Interface				Port	Туре		Status	IPv4 address
	im out			-		1	Ethernet, 10 Gbit/s			192.168.229.36/26
	👘 lan1					2	Ethernet, 10 Gbit/s			192.168.11.254/24
	nt lan2					3	Ethernet, 10 Gbit/s			192.168.31.254/24
	nt dmz2					4	Ethernet, 10 Gbit/s			172.16.11.254/24
	Rerveur					5	Ethernet, 10 Gbit/s			172.16.31.254/24

8. Route par défaut

La configuration de la passerelle par défaut de notre pare-feu SNS doit pointer sur l'adresse IP du parefeu SNS du siège (enseignant) : 192.168.229.1 : Cliquez **Configuration / Réseau / Routage / onglet Routes statiques IPv4**.

L NETWORK / ROUTING

IPV4 STATIC ROU	JTES IPV4 DYI	NAMIC ROUTING	V4 RETURN ROUTES		
General					
Default gateway (r	outer):	def_gatway		▼ 2+	
STATIC ROUTES					
Searching	+	Add 🗙 Delete			
Status ≞ ▼	Destination network	(host, network or group o	Interface		Address range

On définie l'Objet def_gatway avec l'adresse IP de la passerelle : 192.168.229.1

9. Mise en œuvre de la translation d'adresse (Internet)

Ouvrez le menu Configuration / Politique de sécurité / Filtrage et NAT.

Vous allez mettre en place une nouvelle politique de sécurité, il faudra commencer par désactiver la règle de filtrage Pass all et ajouter les règles de filtrage qui respecteront le cahier des charges décrit ci-après.

Étape 1 : Copiez la politique de filtrage/NAT (1) Block all vers une autre politique vide où nous allons les copier les règles de NAT.

• Dans la liste déroulante des politiques de sécurité, choisissez (1) Block all.

	`							Mei	p us to improve the application Download SN Real-Lime n	Monitor
1	FILTER - NA	AT								Ū,
	(1) Block all 💙 🧸 Activate this policy Edit - 😘 Export 🗓									
F	LTERING NA	π								
:	Searched text	×	💠 New rule 🕶	🛛 Delete 🕴 🕇 👃 🔚 🛅	💣 Cut 📓 Copy	🔄 Paste 🔰 🔍 Search in I	ogs 🔍 Search in monitorin	9	=	-
		Status 🔤	Action 🔤	Source	Destination	Dest. port	Protocol	Security inspection	Comment	
	Remote Mar	nagement: Go to	o System - Configura	ation to setup the web administration appli	cation access (contains 2 rule	es, from 1 to 2)				
	1	🔵 on	🗼 pass	Any	B firewall_all	╈ firewall_srv ttps		IPS	Admin from everywhere	
	2	🕗 on	🕺 pass	💌 Any	🏭 firewall_all	🕷 Any	icmp (Echo request (Ping))	IPS	Allow Ping from everywhere	
	Default polic	cy (contains 1 rul	les, from 3 to 3)							
	3	🔵 on	block	Any	Any	Any		IPS	Block all	
l.										
1										

<u>Cliquez Éditer puis copier vers et choisir une politique vide (Filter 05).</u>

- Cliquez Sauvegarder les modifications...
- Dans la liste déroulante des politiques de sécurité, choisissez la politique copiée (05) Block all. Cliquez Éditer puis Renommer et renommez-là en Utilisateurs_Block all & NAT, puis Mettre à jour.
- Cliquez sur le bouton Appliquer puis Activer la politique "Utilisateurs_Block all & NAT".
- Dans la liste des politiques de sécurité, choisissez la politique précédente, celle où vous avez défini du NAT puis sélectionnez la règle de NAT et cliquez sur Copier.
- Dans la liste des politiques de sécurité, choisissez la politique (06)
 Utilisateurs_Block all & NAT / onglet NAT puis cliquez sur Coller. La règle de NAT/PAT est copiée.

=> Mise en place de NAT dynamique :

🦺 (5) pass_ne	twork		- Edit ·	► " <u>1</u> Export	0								
FILTERING	NAT												
Searching			+ New r	ule 👻 🗙 Del	ete 1 🖡	*	🛃 🖻 Ci	ut 🔄 Copy 🍷) Paste 🗒 Sea	rch in logs 🛛 🖓 Se	earch in monitoring		
Status =*		E۳	Original traffic (before translation)				Traffic after translation						
		1	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port	Protocol	Options	Co

10. Configuration de NAT pour publier le serveur Web interne et DNS autoritaire

FILTERING	NAT										
Searching 🔰 🕂 New rule 🗸 X Delete 🏦 🌲 🖈 🦨 🎦 Cut 🔂 Copy 🕑 Paste 🗒 Search in logs 🖾 Search in monitoring											
						Traffic a	fter translation		Deres al	0	
	Status		Destination	Dest. port		Source	Src. port	Destination Dest. port		Protocol	Options
Internet (co	ntains 1 rules, fror	n 1 to 1)									
1 🚥	on	Netwo	Internet interface: out	* Any	⇒	Firewa	🤸 🖠 ephemera	* Any			
Serveur wet	et dns publiés (c	ontains 3 rule	s, from 2 to 4)								
2 🚥	on 💽	Interne Interne Interface: o	📔 Firewall_ou	🖞 dns	⇒	* Any		🖪 serv_priv_ns0	🖞 dns		
3 🚥	on	Internet interface: o	ARP 🖥 Firewa	ቿ http	⇒	* Any		serv_priv_web	ቿ http		

Serveur	Web	interne

Original trafic			
Source	internet		
Destination	Fireware_out (192.168.229.36)		
port	http (80)		
Après translation			
Source	any		
destination	Serveur web privé (172.16.31.253)		
port	http (80)		

Serveur DNS interne			
Original trafic			
Source internet			
Destination	Fireware_out (192.168.229.36)		
port	dns (53)		
Après translation			
Source	any		
destination	Serveur dns privé (172.16.11.10)		
port	dns (53)		

11. Filtrage pour le contexte

FILTE	RING	NAT						
Searching 🔰 🕂 New rule 👻 X Delete 🕇 🌲 💉 🖉 🗁 Cut 🕑 Copy 🕑 Paste 🗒 Search in logs 🚱 Search in monitoring						g		
		Status 🚉	Action =•	Source	Destination	Dest. port	Protocol	Security ins
E R	emote Ma	magement: Go to S	System - Configuratio	n to setup the web administration	application access (contains 2 rules, from 1 to 2)			
1		C on	pass	* Any	₽ firewall_all	<pre> firewall_srv fittps </pre>		IPS
2	E	💽 on	ᅌ pass	* Any	🖶 firewall_all	* Any	icmp (Echo reques	IPS
🗏 in	ternet (co	ontains 3 rules, from	m 3 to 5)					
3		💽 on	pass	Network_internals	* Any	* Any	icmp (Echo reques	IPS
4		💽 on	pass	P Network_internals	⊕ Internet interface: out	* Any		IPS
5		💽 on	pass	Internet interface: out	Firewall_out	¥ http ¥ dns		IPS
🗉 S	E Serveurs internes (contains 6 rules, from 6 to 11)							
6		💽 on	pass	Network_internals	serv_priv_recursif	🖞 dns		IPS
7		💽 on	pass	Network_internals	📔 serv_priv_relai	🖞 bootps		IPS
8	E	💽 on	pass	serv_priv_relai	🔋 serv_priv_dhcp	* Any		IPS
9		💽 on	pass	serv_priv_recursif	<pre>serv_priv_ns0</pre>	* Any		IPS
10		💽 on	pass	Network_internals	serv_priv_web	🖞 http		IPS
11		💽 on	🕤 pass	Network_internals	🛙 serv_priv_ns0	🖞 dns		IPS
E D	Default policy (contains 1 rules from 12 to 12)							

Default policy (contains 1 rules, from 12 to 12)

12. Test

GNU nano 7.2					db.kayes.cub.fr
; ; BIND ;	data fil	e for lo	cal loop)	back inte	erface
ŞTTL	604800				
kayes.c	ub.fr.		IN	SOA	ns0.kayes.cub.fr. hostmaster.kayes.cub.fr. (
			2		; Serial
			604800		; Refresh
			86400		; Retry
			2419200		; Expire
			604800)	; Negative Cache TTL
kayaa a	uh fr	TN	Ng	ng() karr	rea cub fr
Aayes.c	TN	110	100 100	1130. Kay	ves.cub.ll.
G	IN	A	192.168	.229.36	
ns0	IN	A	172.16.	11.10	
www	IN	A	192.168	.229.36	
glpi	IN	A	172.16.	31.253	

Dans le fichier de configuration de notre serveur dns, on ajoute les informations suivantes :

www IN A 192.168.229.36

pour permettre au réseau externe CUB WAN d'accéder au serveur Web avec le nom **www.kayes.cub.fr**

glpi IN A 172.16.31.253

pour rendre accessible le serveur web depuis interne

NB: 172.16.31.253 est notre serveur web privée

192.168.229.36 est l'adresse IP publique du serveur après translation

```
root@ns0:/etc/bind# dig glpi.kayes.cub.fr
; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> glpi.kayes.cub.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36969
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;glpi.kayes.cub.fr.
                              IN
                                      Α
;; ANSWER SECTION:
                      79203 IN A
                                           172.16.31.253
glpi.kayes.cub.fr.
;; Query time: 8 msec
;; SERVER: 192.168.31.20#53(192.168.31.20) (UDP)
;; WHEN: Tue Oct 15 08:46:37 UTC 2024
;; MSG SIZE rcvd: 62
;; WHEN: Tue Oct 15 08:46:37 UTC 2024
;; MSG SIZE rcvd: 62
root@ns0:/etc/bind# dig www.kayes.cub.fr
; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> www.kayes.cub.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51232
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.kayes.cub.fr.
                                IN
                                       A
;; ANSWER SECTION:
www.kayes.cub.fr.
                       79128 IN A
                                               192.168.229.36
;; Query time: 0 msec
;; SERVER: 192.168.31.20#53(192.168.31.20) (UDP)
;; WHEN: Tue Oct 15 08:47:07 UTC 2024
;; MSG SIZE rcvd: 61
```