

Kassim

SIO2

Mathieu

Mission E4 – DMZ à 3 niveaux

SOMMAIRE

- Objectif de la mission
- Détail des étapes
- Test

1. Objectif de la mission

La DMZ à 3 niveaux permet d'augmenter le niveau de sécurité du réseau qui n'avait qu'un pare feu. En effet on a donc 3 zones : la zone externe qui est la zone en dehors du pare feu externe, la zone interne qui est la zone du réseau interne et la zone de transition qui est la zone entre le pare feu interne et l'externe.

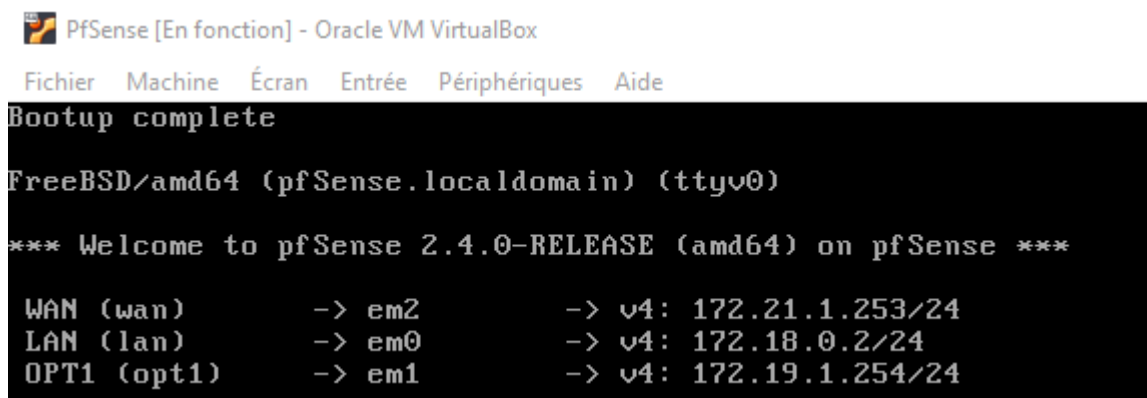
2. Détail des étapes

Tout d'abord j'ai configuré les interfaces de mon firewall externe avec l'interface WAN qui est a l'extérieur de la DMZ en DHCP et l'interface LAN qui est dans la zone de transition dans le même réseau que l'interface WAN du firewall interne.

A screenshot of a terminal window titled "FirewallExterne [En fonction] - Oracle VM VirtualBox". The terminal shows the bootup of pfSense 2.4.0-RELEASE (amd64). It displays the network configuration for WAN (wan), LAN (lan), and OPT1 (opt1) interfaces. WAN is connected to em0 and configured with DHCP (192.168.122.52/24). LAN is connected to em2 and configured with a static IP (172.21.1.254/24). OPT1 is connected to em1 and configured with a static IP (172.20.1.254/24).









```
FirewallExterne [En fonction] - Oracle VM VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
Bootup complete
FreeBSD/amd64 (pfSense.localdomain) (ttyv0)
*** Welcome to pfSense 2.4.0-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.122.52/24
LAN (lan)      -> em2      -> v4: 172.21.1.254/24
OPT1 (opt1)    -> em1      -> v4: 172.20.1.254/24
```

Rappel de la configuration du firewall interne ou j'ai modifié l'interface WAN qui était en DHCP pour pouvoir choisir le réseau de la zone de transition :

A screenshot of a terminal window titled "PfSense [En fonction] - Oracle VM VirtualBox". The terminal shows the bootup of pfSense 2.4.0-RELEASE (amd64). It displays the network configuration for WAN (wan), LAN (lan), and OPT1 (opt1) interfaces. WAN is connected to em2 and configured with a static IP (172.21.1.253/24). LAN is connected to em0 and configured with a static IP (172.18.0.2/24). OPT1 is connected to em1 and configured with a static IP (172.19.1.254/24).

```
PfSense [En fonction] - Oracle VM VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
Bootup complete
FreeBSD/amd64 (pfSense.localdomain) (ttyv0)
*** Welcome to pfSense 2.4.0-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em2      -> v4: 172.21.1.253/24
LAN (lan)      -> em0      -> v4: 172.18.0.2/24
OPT1 (opt1)    -> em1      -> v4: 172.19.1.254/24
```

Sur le firewall interne j'ai du modifier la gateway WAN :

Gateways Static Routes Gateway Groups					
Gateways					
	Name	Interface	Gateway	Monitor IP	Description Actions
<input checked="" type="checkbox"/>	GW_LAN	LAN	172.18.0.1	172.18.0.1	Interface lan Gateway    
<input checked="" type="checkbox"/>	GW_WAN (default)	WAN	172.21.1.254	172.21.1.254	Interface wan Gateway    







J'ai configuré les règles du firewall externe pour autoriser toutes les entrées car c'est le firewall interne qui filtrera :

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	<input checked="" type="checkbox"/>	0 / 5 KiB	IPv4 *	*	*	*	*	none			    









J'ai fais les routes du pare feu externe ...

System / Routing / Static Routes		
Gateways Static Routes Gateway Groups		
Static Routes		
	Network	Gateway Interface
<input checked="" type="checkbox"/>	192.168.40.0/24	LAN - 172.21.1.253 LAN
<input checked="" type="checkbox"/>	192.168.30.0/24	LAN - 172.21.1.253 LAN
<input checked="" type="checkbox"/>	192.168.20.0/24	LAN - 172.21.1.253 LAN
<input checked="" type="checkbox"/>	192.168.10.0/24	LAN - 172.21.1.253 LAN
<input checked="" type="checkbox"/>	172.19.0.0/16	LAN - 172.21.1.253 LAN
<input checked="" type="checkbox"/>	172.18.0.0/16	LAN - 172.21.1.253 LAN
<input checked="" type="checkbox"/>	192.168.80.0/24	LAN - 172.21.1.253 LAN

... et les gateway :

Gateways					
Name	Interface	Gateway	Monitor IP	Description	Actions
<input checked="" type="checkbox"/> LAN	LAN	172.21.1.253	172.21.1.253		  
<input checked="" type="checkbox"/> WAN_DHCP (default)	WAN	192.168.122.1	192.168.122.1	Interface WAN_DHCP Gateway	  

Sur le firewall externe j'ai fait du NAT pour traduire les adresses qui rentrent et qui sortent donc sur les interfaces LAN et WAN :

Mappings										
	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input checked="" type="checkbox"/>	LAN	any	*	*	*	LAN address	*			  
<input checked="" type="checkbox"/>	WAN	any	*	*	*	WAN address	*			  

Pour pouvoir continuer à accéder aux sites interne.gsb.fr et externe.gsb.fr après le changement de disposition de la DMZ j'ai dû modifier les adresses IP dans les dossiers concernés pour que le serveur web puisse joindre la BDD.

```
Intralab-BDD [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide

Debian GNU/Linux 10 debian tty1
debian login: root
Password:
Last login: Tue Dec  1 11:11:13 CET 2020 on tty1
Linux debian 4.19.0-10-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debian:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
    link/ether 08:00:27:47:bf:0b brd ff:ff:ff:ff:ff:ff
    inet 172.21.1.100/24 brd 172.21.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe47:bf0b/64 scope link
        valid_lft forever preferred_lft forever
root@debian:~#
```

```

APP_ENV=dev
APP_SECRET=a2eb7084498f8231a6ea7343a11c6671
#TRUSTED_PROXIES=127.0.0.0/8,10.0.0.0/8,172.16.0.0/12,192.168.0.0/16
#TRUSTED_HOSTS='^(localhost|example\.com)$'
###< symfony/framework-bundle ###





###> symfony/mailer ###
# MAILER_DSN=smtp://localhost
###< symfony/mailer ###


###> doctrine/doctrine-bundle ###
# Format described at https://www.doctrine-project.org/projects/doctrine-dbal/en/latest/re
# For an SQLite database, use: "sqlite:///kernel.project_dir%/var/data.db"
# For a PostgreSQL database, use: "postgresql://db_user:db_password@127.0.0.1:5432/db_name
# IMPORTANT: You MUST configure your server version, either here or in config/packages/doc
DATABASE_URL=mysql://siteInterne:secret@172.21.1.100:3306/siteInterne?serverVersion=5.7
###< doctrine/doctrine-bundle ###

```

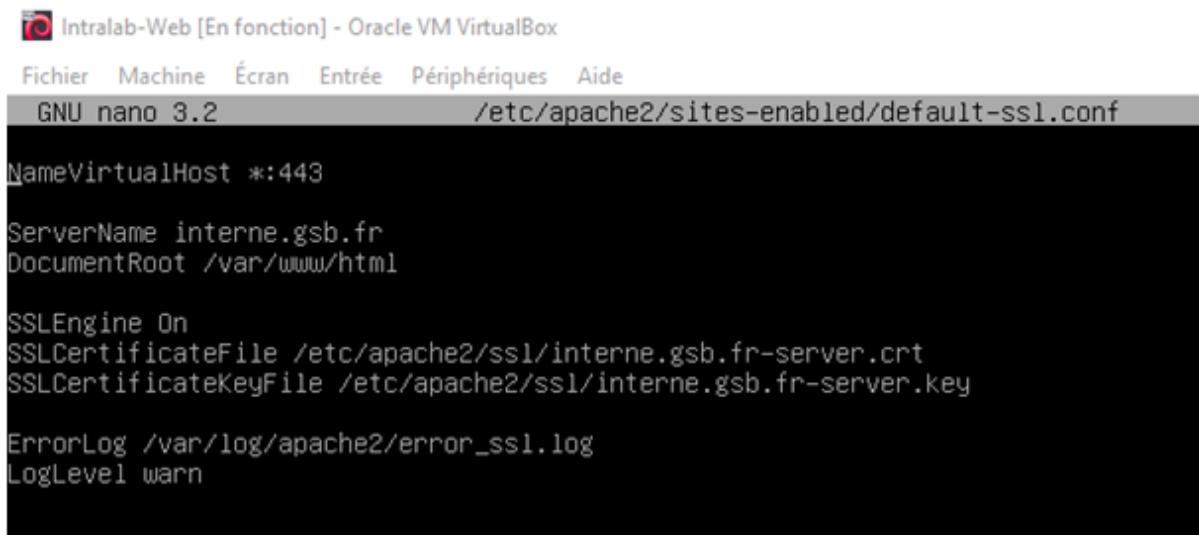
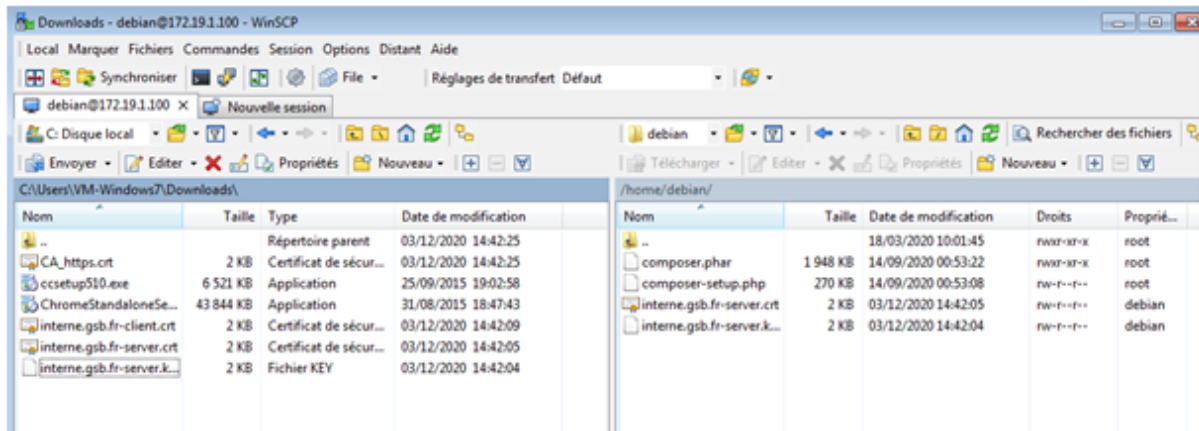
HTTPS

J'ai créé un certificat d'autorité sur le PfSense pour interne.gsb.fr puis un certificat server et un certificat client.

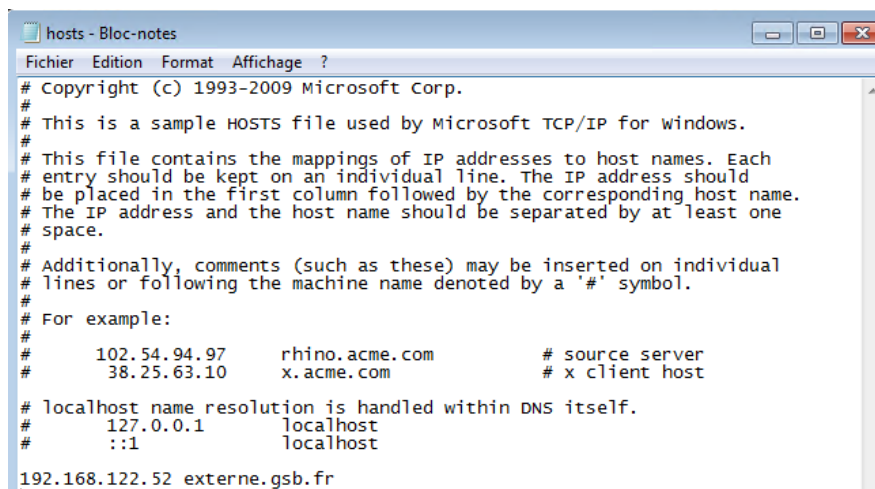
Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA_https	✓	self-signed	2	emailAddress=jhghu@uitg.fr, ST=DOUBS, OU=BTSINFO, O=LLB, L=Besancon, CN=https_interne.gsb.fr, C=FR Valid From: Thu, 03 Dec 2020 10:22:15 +0000 Valid Until: Sun, 01 Dec 2030 10:22:15 +0000		   

Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
interne.gsb.fr-server Server Certificate CA: No Server: Yes	CA_https	emailAddress=jhghu@uitg.fr, ST=DOUBS, OU=BTSINFO, O=LLB, L=Besancon, CN=interne.gsb.fr, C=FR  Valid From: Thu, 03 Dec 2020 13:04:54 +0000 Valid Until: Sun, 01 Dec 2030 13:04:54 +0000	webConfigurator	  
interne.gsb.fr-client User Certificate CA: No Server: No	CA_https	emailAddress=jhghu@uitg.fr, ST=DOUBS, OU=BTSINFO, O=LLB, L=Besancon, CN=interne.gsb.fr, C=FR  Valid From: Thu, 03 Dec 2020 13:05:48 +0000 Valid Until: Sun, 01 Dec 2030 13:05:48 +0000		  

J'ai transféré le certificat et la clé du certificat serveur sur IntralabWeb et j'ai modifié le default-ssl.conf.

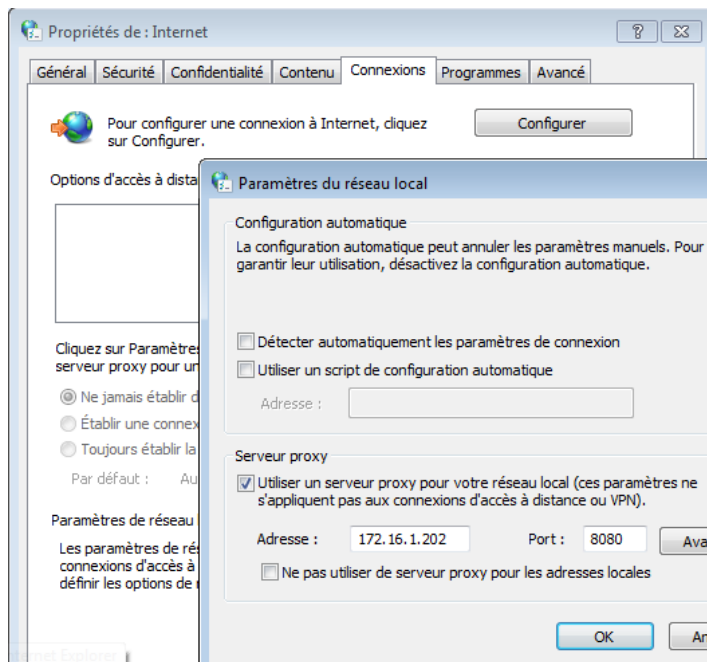


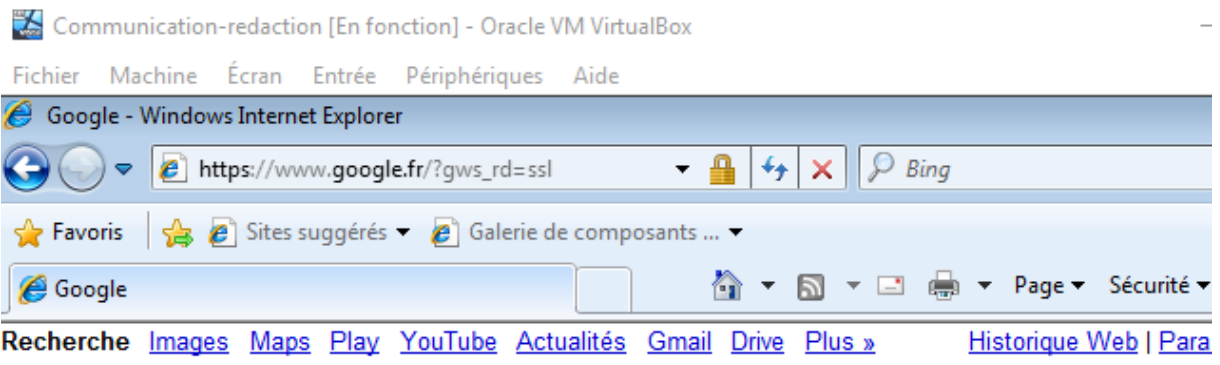
Résolution DNS sur la VM extérieure au réseau :



3. Test

Je peux accéder à internet en rentrant le proxy :



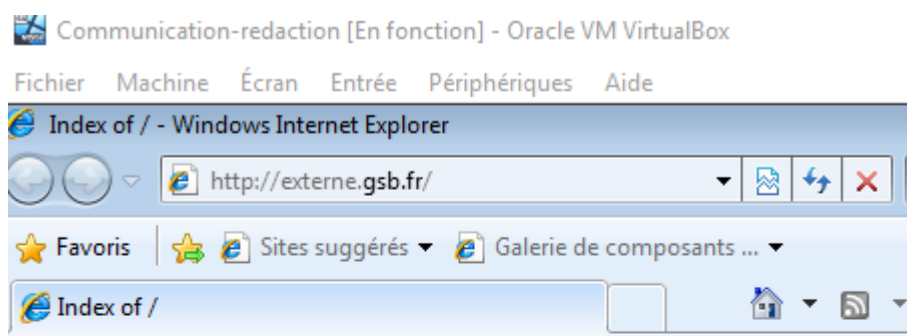


Recherche Google

J'ai de la chance

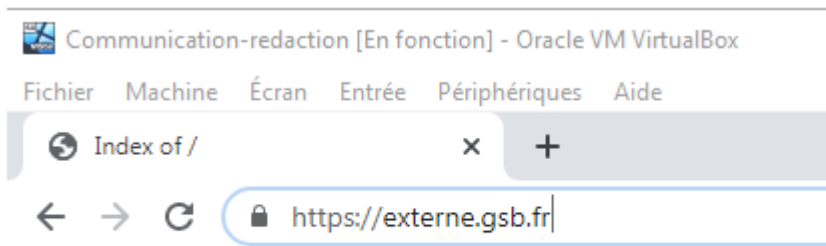
Si on désactive le proxy je peux aussi accéder à interne.gsb.fr et a externe.gsb.fr :

DNS	Nom	Type	Données	Horodateur
WIN-MHRFDV79422	(identique au dossier parent)	Source de nom (SOA)	[6], win-mhrfdv79422.gala...	statique
Zones de recherche direc	(identique au dossier parent)	Serveur de noms (NS)	redondance.galaxy-swiss....	statique
_msdcg.galaxy-swiss.	(identique au dossier parent)	Serveur de noms (NS)	win-mhrfdv79422.galaxy-s...	statique
galaxy-swiss.com	externe	Hôte (A)	172.20.1.100	statique
gsb.fr	interne	Hôte (A)	172.19.1.100	statique
Zones de recherche invei				
Points d'approbation				
Redirecteurs conditionne				





Test pour l'HTTPS :

externe.gsb.fr

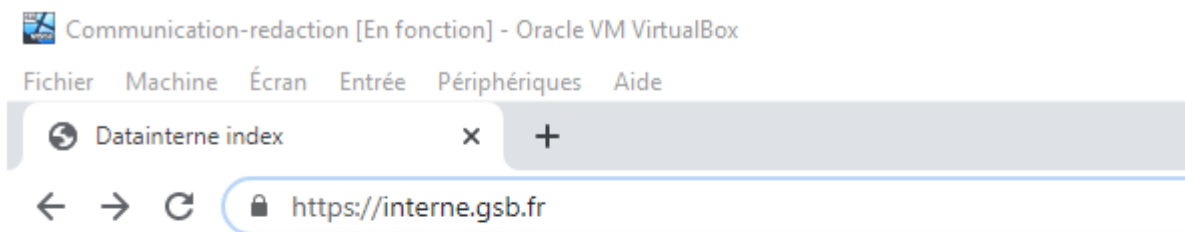


Index of /

Name	Last modified	Size	Description
 frontSite/	2020-10-05 09:46	-	
 interneSite/	2020-12-03 10:19	-	

Apache/2.4.38 (Debian) Server at externe.gsb.fr Port 443

interne.gsb.fr



Datainterne index

Cle	primaire	Champinterne1	Champinterne2	Champinterne3	actions
1	test	test	test		show edit
Create new					

GPO :

LABANNU [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Éditeur de gestion des stratégies de groupe

Fichier Action Affichage ?

Stratégie Default Domain Policy [WIN-MHRFDV79422.GALAXY ^

- Configuration ordinateur
 - Stratégies
 - Paramètres du logiciel
 - Paramètres Windows
 - Stratégie de résolution de noms
 - Scripts (démarrage/arrêt)
 - Imprimantes déployées
 - Paramètres de sécurité
 - Stratégies de comptes
 - Stratégies locales
 - Journal des événements
 - Groupes restreints
 - Services système
 - Registre
 - Système de fichiers
 - Stratégies de réseau filaire (IEEE 802.3)
 - Pare-feu Windows Defender avec fonctions
 - Stratégies du gestionnaire de listes de réseau
 - Stratégies de réseau sans fil (IEEE 802.11)
 - Stratégies de clé publique
 - Système de fichiers EFS (Encrypting File S...
 - Protection des données
 - Chiffrement de lecteur BitLocker
 - Certificat de déverrouillage réseau pour l...
 - Paramètres de demande automatique de...
 - Autorités de certification racines de conf...

Délivré à	Délivré par	Date d'expirati...	Rôles prévus	Nom convivial
https_interne.gsb.fr	https_interne.gsb.fr	01/12/2030	<Tout>	<Aucun>

LABANNU [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Éditeur de gestion des stratégies de groupe

Fichier Action Affichage ?

Stratégie Default Domain Policy [WIN-MHRFDV79422.GALAXY ^

- Configuration ordinateur
 - Stratégies
 - Paramètres du logiciel
 - Paramètres Windows
 - Stratégie de résolution de noms
 - Scripts (démarrage/arrêt)
 - Imprimantes déployées
 - Paramètres de sécurité
 - Stratégies de comptes
 - Stratégies locales
 - Journal des événements
 - Groupes restreints
 - Services système
 - Registre
 - Système de fichiers
 - Stratégies de réseau filaire (IEEE 802.3)
 - Pare-feu Windows Defender avec fonctions
 - Stratégies du gestionnaire de listes de réseau
 - Stratégies de réseau sans fil (IEEE 802.11)
 - Stratégies de clé publique
 - Système de fichiers EFS (Encrypting File S...
 - Protection des données
 - Chiffrement de lecteur BitLocker
 - Certificat de déverrouillage réseau pour l...
 - Paramètres de demande automatique de...
 - Autorités de certification racines de conf...
 - Confiance de l'entreprise
 - Autorités de certification intermédiaires
 - Éditeurs approuvés
 - Certificats non autorisés
 - Personnes autorisées

Délivré à	Délivré par	Date d'expirati...	Rôles prévus	Nom convivial	St
interne.gsb.fr	https_interne.gsb.fr	01/12/2030	Authentification du...	<Aucun>	

Inventaire

Routeur							
nature : routeur							
Port	e0/0	e0/1	e0/1.10	e0/1.20	e0/1.30	e0/1.40	e0/1.80
ip	172.18.0.3	no ip	192.168.10.254	192.168.20.254	192.168.30.254	192.168.40.254	192.168.80.254
masque CIDR	24		24	24	24	24	24
VLAN			10	20	30	40	80
Ip Helper			172.17.0.10	172.17.0.10	172.17.0.10	172.17.0.10	172.17.0.10
Ip Helper2			172.17.0.20	172.17.0.20	172.17.0.20	172.17.0.20	172.17.0.20
Service	Néant						
Table de routage							
Route par défaut	192.168.1.2						

Routeurbis							
nature : routeur							
Port	e0/0	e0/1	e0/1.10	e0/1.20	e0/1.30	e0/1.40	e0/1.80
ip	172.18.0.4	no ip	192.168.10.2	192.168.20.2	192.168.30.2	192.168.40.2	192.168.80.254
masque CIDR	24		24	24	24	24	24
VLAN			10	20	30	40	80
Ip Helper			172.17.0.10	172.17.0.10	172.17.0.10	172.17.0.10	172.17.0.10
Ip Helper2			172.17.0.20	172.17.0.20	172.17.0.20	172.17.0.20	172.17.0.20
Service	Néant						
Table de routage							
Route par défaut	192.168.1.2						

Labannu			
Serveur			
Interface	ethernet 0		
mode	IP		
IP	172.17.0.30/16		
Services	DNS	étendue	galaxy-swiss.com
	AD DS	domaine	galaxy-swiss.com
Pare feu logiciel : activé			
Mise à jour : activé			
Bureau à distance : désactivé			

Rezolab							
Serveur							
Interface	ethernet 0						
mode	IP						
IP	172.17.0.10/16						
Services	DHCP	Etendues	Vlan10	vlan20	vlan30	vlan40	Vlan80
	/24	Première Adresse	192.168.10.10	192.168.20.10	192.168.30.10	192.168.40.10	192.168.80.10
	/24	Dernière Adresse	192.168.10.100	192.168.20.100	192.168.30.100	192.168.40.100	192.168.80.100
Pare feu logiciel : activé							
Mise à jour : activé							
Bureau à distance : désactivé							

SwArchi				
nature :	switch			
Port	e0/0	e0/1	e0/2	e0/3
mode	trunk	trunk	trunk	trunk
vlan	300	300	10,20,30,40,300,400	10,20,30,40,300,400
Service	Spanningtree	Désactivé		

SwEtag1			
nature :	switch		
Port	e0/0	e0/1	e0/2
mode	trunk	access	access
vlan		30, 40	30, 40
Service	Spanningtree	Désactivé	

SwEtag4				
nature :	switch			
Port	e0/0	e1/0-3	e2/0-3	e3/0-3
mode	trunk	access	access	access
vlan		30	10	80
Service	Spanningtree	Désactivé		

SwEtag6					
nature :	switch				
Port	e0/0	e0/1	e0/2	e0/3	e0/4
mode	trunk	access	access	access	access
vlan		300	300	300	300
Interface	vlan 300				
ip	172.17.0.6/16				
gateway	172.17.0.254				
Service	Spanningtree	Désactivé			

IOV1		
nature :	switch	
Port	e0/0	e0/1
mode	trunk	trunk
vlan		

IOV2				
nature :	switch			
Port	e0/0	e0/1	e0/2	e0/3
mode	trunk	trunk	trunk	trunk
vlan				

IOV3		
nature :	switch	
Port	e0/0	e0/1
mode	trunk	trunk
vlan		

IOV4			
nature :	switch		
Port	e0/0	e0/1	e0/2
mode	trunk	trunk	trunk
vlan			

IOV5			
nature :	switch		
Port	e0/0	e0/1	e0/2
mode	trunk	trunk	trunk
vlan			

PfSense [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

*** Welcome to pfSense 2.4.0-RELEASE (amd64) on pfSense ***

```

WAN (wan)      -> em2      -> v4: 172.21.1.253/24
LAN (lan)      -> em0      -> v4: 172.18.0.2/24
OPT1 (opt1)    -> em1      -> v4: 172.19.1.254/24
  
```

Name	Interface	Gateway	Monitor IP	Description	Actions
GW_LAN	LAN	172.18.0.1	172.18.0.1	Interface lan Gateway	
GW_WAN (default)	WAN	172.21.1.254	172.21.1.254	Interface wan Gateway	

Gateways Static Routes Gateway Groups

Network	Gateway	Interface	Description	Actions
192.168.10.0/24	GW_LAN - 172.18.0.1	LAN		
192.168.20.0/24	GW_LAN - 172.18.0.1	LAN		
192.168.30.0/24	GW_LAN - 172.18.0.1	LAN		
192.168.40.0/24	GW_LAN - 172.18.0.1	LAN		
192.168.80.0/24	GW_LAN - 172.18.0.1	LAN		
172.17.0.0/24	GW_LAN - 172.18.0.1	LAN		

Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
WAN	any	*	*	*	WAN address	*			

Floating WAN LAN OPT1

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	172.16.1.202	*	*	*	*	none			
0/0 B	IPv4 *	*	*	172.19.1.0/24	*	*	none			
0/0 B	IPv4 *	*	*	172.17.0.0/16	*	*	none			
0/0 B	IPv4 *	*	*	172.18.0.0/16	*	*	none			
4/51 K B	IPv4 *	*	*	192.168.0.0/16	*	*	none			

Floating WAN LAN OPT1

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
1/1.82 MB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
0/1.50 MB	IPv4 TCP	*	*	*	*	*	none			
25/54 K B	IPv4 *	*	*	*	*	*	none			
0/0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Floating WAN LAN OPT1

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 TCP	*	*	*	*	*	none			

FirewallExterne [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

*** Welcome to pfSense 2.4.0-RELEASE (amd64) on pfSense ***

```

WAN (wan)      -> em0      -> v4/BHCP4: 192.168.122.52/24
LAN (lan)      -> em2      -> v4: 172.21.1.254/24
OPT1 (opt1)    -> em1      -> v4: 172.20.1.254/24
  
```

Name	Interface	Gateway	Monitor IP	Description	Actions
LAN	LAN	172.21.1.253	172.21.1.253		
WAN_DHCP (default)	WAN	192.168.122.1	192.168.122.1	Interface WAN_DHCP Gateway	

Gateways Static Routes Gateway Groups

Network	Gateway	Interface	Description	Actions
192.168.40.0/24	LAN - 172.21.1.253	LAN		
192.168.30.0/24	LAN - 172.21.1.253	LAN		
192.168.20.0/24	LAN - 172.21.1.253	LAN		
192.168.10.0/24	LAN - 172.21.1.253	LAN		
172.19.0.0/16	LAN - 172.21.1.253	LAN		
172.18.0.0/16	LAN - 172.21.1.253	LAN		
192.168.80.0/24	LAN - 172.21.1.253	LAN		

Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
WAN	any	*	*	*	WAN address	*			

Floating WAN LAN OPT1

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/8 K B	IPv4 *	*	*	*	*	*	none			

Floating WAN LAN OPT1

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
1/1.79 MB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
0/0 B	IPv4 *	LAN address	*	172.21.1.253	*	*	none			
43/235 K B	IPv4 *	*	*	*	*	*	none			
0/0 B	IPv4 *	172.21.1.100	*	172.21.1.254	*	*	none		Easy Rule: Passed from Firewall Log View	

Floating WAN LAN OPT1

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
4/80 K B	IPv4 *	*	*	*	*	*	none			
0/0 B	IPv4 UDP	172.20.1.100	*	192.168.1.254 (DNS)	53	*	none		Easy Rule: Passed from Firewall Log View	

INTRALAB WEB	
Nature : Debian	
Adresse IP	172.19.1.100
Masque	255.255.255.0
Passerelle	172.19.1.254

INTRALAB BDD	
Nature : Debian	
Adresse IP	172.21.1.100
Masque	255.255.255.0
Passerelle	172.21.1.254

EXTERNE.GSB	
Nature : Debian	
Adresse IP	172.20.1.100
Masque	255.255.255.0
Passerelle	172.20.1.254