

Projet CCNA Cisco

Groupe formé de Ethan Ménoury, Kephas Assogba, Yanick Mbaihingabe, Raphaël Jolivel-Savage, Edouard Vallet

Organisation interne

Ethan Chef d'équipe / Coordinateur projet (obligatoire)

Ethan Yanick Raphaël Responsable Réseau (Routeur, routage, interconnexions)

Yanick Raphaël Responsable Virtualisation / ESXi

Yanick Raphaël Responsable Sécurité / OPNsense

Ethan Edouard Responsable Recette & Qualité (tests, preuves, documentation)

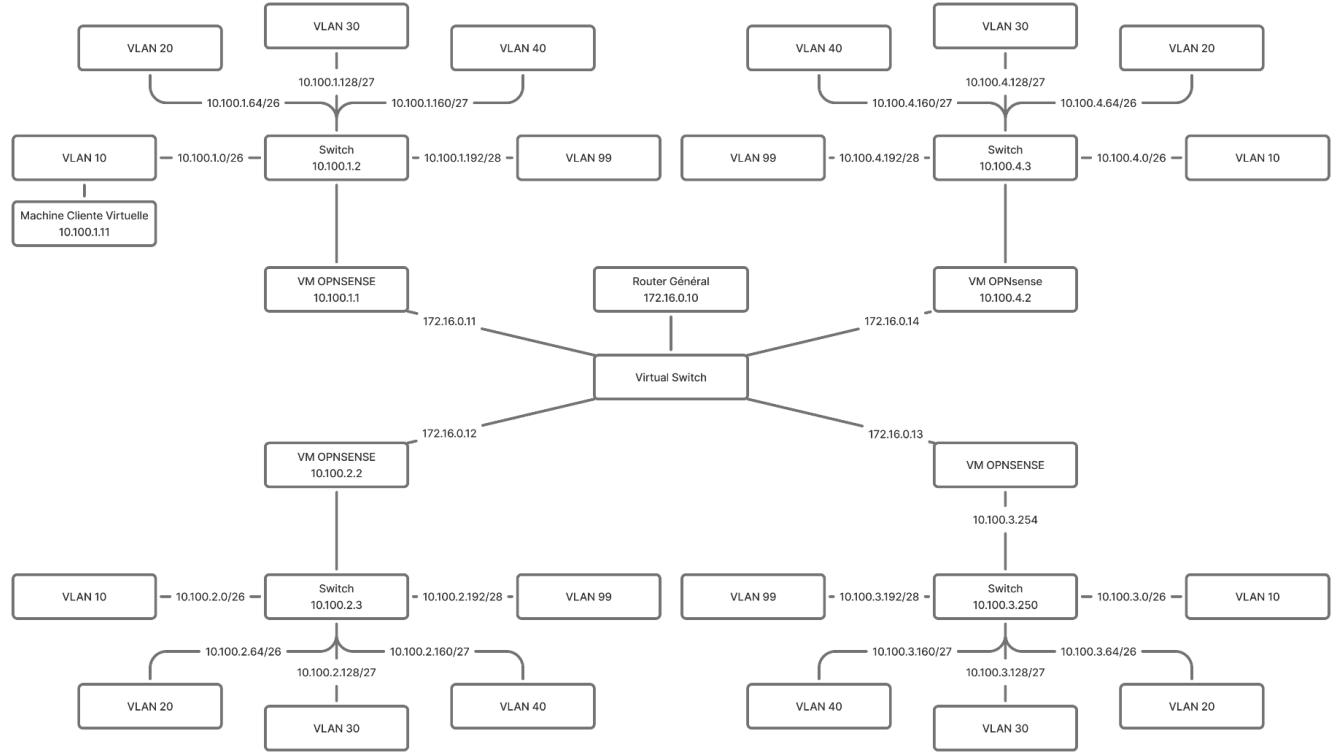
Ethan Edouard Kephas Responsable Documentation / Runbook (peut être fusionné avec Qualité)

Maquette fonctionnelle (MEP)

- Maquette opérationnelle (routeur + ESXi + OPNsense + VLANs + services) conforme au cahier des charges.
- Preuves minimales : inter-divisions IPv4, IPv6 minimal, DHCP/DNS, politique firewall, logs.
- Réseau WAN : 172.16.0.0/24
- Adresses WAN :
 - **G1 Commercial : 172.16.0.11/24**
 - G2 Développement : 172.16.0.12/24
 - G3 R&D : 172.16.0.13/24
 - G4 Marketing : 172.16.0.14/24

Dossier de conception

- Schéma logique (WAN + transit + OPNsense + VLANs + VMs)



- Plan d'adressage IPv4/IPv6 complet (tableaux)

VLAN	Nom	Réseau	Masque	Plage d'adresses utiles	Passerelle	Diffusion
10	ADMIN	10.100.1.0	/26 255.255.255. 192	10.100.1.2 - 10.100.1.62	10.100.1.1	10.100.1.63
20	USERS	10.100.1.64	/26 255.255.255. 192	10.100.1.66 - 10.100.1.126	10.100.1.65	10.100.1.127
30	SRV	10.100.1.128	/27 255.255.255. 224	10.100.1.130 - 10.100.1.158	10.100.1.129	10.100.1.159

40	GUEST	10.100.1.160	/27 255.255.255. 224	10.100.1.162 - 10.100.1.190	10.100.1.161	10.100.1.191
99	MGMT	10.100.1.192	/28 255.255.255. 240	10.100.1.194 - 10.100.1.206	10.100.1.193	10.100.1.207

- Stratégie de routage (routes statiques) + fiches d'interconnexion
- Architecture L3 Routeur↔OPNsense (transit /30 + /64, routes) appliquée

Interconnexion WAN

Équipement source	Interface	IP source	Équipement destination	Interface	IP destination	Réseau
Routeur G1	WAN	172.16.0.11/24	Réseau WAN	-	-	172.16.0.0/24
Routeur G2	WAN	172.16.0.12/24	Réseau WAN	-	-	172.16.0.0/24
Routeur G3	WAN	172.16.0.13/24	Réseau WAN	-	-	172.16.0.0/24
Routeur G4	WAN	172.16.0.14/24	Réseau WAN	-	-	172.16.0.0/24

Interconnexion Routeur ↔ OPNsense

Routeur G1	G0/0 (Transit)	10.255.4.2/ 30	OPNsense	WAN	10.255.4.1/ 30	10.255.4.0/ 30	Transit L3
Routeur G1	G0/0 (IPv6)	2001:db8: 4::2/64	OPNsense	WAN	2001:db8: 4::1/64	2001:db8: 4::/64	Transit IPv6

Interconnexion OPNsense ↔ Switch (Trunk VLAN)

OPNsense	LAN (Trunk)	802.1Q Trunk	10,20,30,40, 99	Switch G1	Port Trunk	Distribution des VLANs
Switch G1	Port Trunk	802.1Q Trunk	10,20,30,40, 99	OPNsense	LAN	Accès firewall

Interconnexion Switch ↔ ESXi

Switch G1	Port Access	20 (USERS)	ESXi	vmnic0	Accès VM USERS
Switch G1	Port Access	10 (ADMIN)	ESXi	vmnic1	Administration
Switch G1	Port Trunk	10,20,30,40,99	ESXi	vmnic2	Trunk VMs

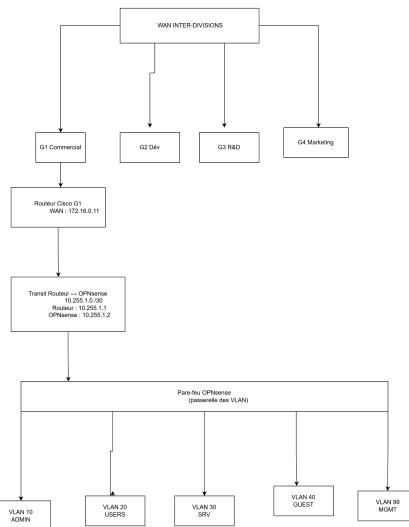
Synthèse des flux autorisés / bloqués

VM	Port Group (VLAN)	IP	Passerelle	Rôle
OPNsense FW	VLAN10 (ADMIN)	10.100.1.1	-	Firewall
Routeur virtuel	WAN	172.16.0.11	-	Routage WAN
Client Debian	VLAN20 (USERS)	DHCP	10.100.1.65	Poste utilisateur
Serveur Intranet	VLAN30 (SRV)	10.100.1.130	10.100.1.129	Services internes

Source	Destination	Service	Action	Justification
VLAN20	Internet	HTTP/HTTPS	ALLOW	Accès web utilisateurs
VLAN10	OPNsense	HTTPS	ALLOW	Administration
VLAN40	Internet	HTTP/HTTPS	ALLOW	Accès invités
VLAN20	VLAN10	Any	DENY	Séparation Admin / Users
VLAN40	Interne	Any	DENY	Sécurité invités
G1/G4	Intranet	HTTPS	ALLOW	Flux imposé
G3	Intranet	HTTPS	DENY	Flux imposé

Schéma logique

[WAN 172.16.0.0/24] → [Routeur G1] → (Transit /30) → [OPNsense] → (Trunk VLANs) → [Switch] → [ESXi] - VMs (Users, Admin, Serveurs, Guest)



- Politique de sécurité (principes + exceptions)

Services: ISC DHCPv4: [SERVERS]



You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.

[full help](#)

<input type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable DHCP server on the SERVERS interface		
<input type="checkbox"/> Deny unknown clients	<input type="checkbox"/>		
<input type="checkbox"/> Ignore Client UIDs	<input type="checkbox"/>		
<input type="checkbox"/> Subnet	10.100.1.128		
<input type="checkbox"/> Subnet mask	255.255.255.192		
<input type="checkbox"/> Available range	10.100.1.129 - 10.100.1.190		
<input type="checkbox"/> Range	from 10.100.1.135	to 10.100.1.180	
<input type="checkbox"/> Additional Pools	Pool Start	Pool End	Description +
<input type="checkbox"/> WINS servers			
<input type="checkbox"/> DNS servers	8.8.8.8		
<input type="checkbox"/> Gateway	10.100.1.129		

Services: ISC DHCPv4: [GUESTS]



You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.

[full help](#)

<input type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable DHCP server on the GUESTS interface		
<input type="checkbox"/> Deny unknown clients	<input type="checkbox"/>		
<input type="checkbox"/> Ignore Client UIDs	<input type="checkbox"/>		
<input type="checkbox"/> Subnet	10.100.1.192		
<input type="checkbox"/> Subnet mask	255.255.255.192		
<input type="checkbox"/> Available range	10.100.1.193 - 10.100.1.254		
<input type="checkbox"/> Range	from	to	
	10.100.1.200	10.100.1.250	
<input type="checkbox"/> Additional Pools	Pool Start	Pool End	Description <input type="button" value="+"/>
<input type="checkbox"/> WINS servers	<input type="text"/> <input type="text"/>		
<input type="checkbox"/> DNS servers	8.8.8.8 <input type="text"/>		
<input type="checkbox"/> Gateway	10.100.1.193		

On ajoute un règle Firewall sur chaque Vlans en suivant le modèle suivant, on change juste la source par "nom de vlan" net

Edit Firewall rule

<input type="checkbox"/> Action	<input type="button" value="Pass"/>
<input type="checkbox"/> Disabled	<input type="checkbox"/> Disable this rule
<input type="checkbox"/> Quick	<input checked="" type="checkbox"/> Apply the action immediately on match.
<input type="checkbox"/> Interface	GUEST
<input type="checkbox"/> Direction	in
<input type="checkbox"/> TCP/IP Version	IPv4
<input type="checkbox"/> Protocol	any
<input type="checkbox"/> Source / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
<input type="checkbox"/> Source	GUEST net

On ajoute une règle supplémentaire sur l'interface GUEST pour respecter la politique 0 confiance

Firewall: Rules: SERVERS

Inspect

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.

	Protocol	Source	Description	?	+						
			Automatically generated rules								
	IPv4 *	SERVERS net	Autoriser accès internet et inter-vlan								

Firewall: Rules: LAN

Inspect

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.

The changes have been applied successfully.

	Protocol	Source	Description	?	+						
			Automatically generated rules								
	IPv4 *	LAN net	Default allow LAN to any rule								
	IPv6 *	LAN net	Default allow LAN IPv6 to any rule								
	IPv4 *	LAN net	Autoriser tout le trafic ADMIN								

Firewall: Rules: USERS

Inspect

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.

The changes have been applied successfully.

	Protocol	Source	Description	?	+						
			Automatically generated rules								
	IPv4 *	USERS net	Autoriser accès Internet et inter-vlan								

Firewall: Rules: GUESTS

[Inspect](#)

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.

The changes have been applied successfully.

<input type="checkbox"/>	Protocol	Source	Description	+	←	Delete	Check	Edit
<input type="checkbox"/>			Automatically generated rules	↓	13			
<input type="checkbox"/>	   	IPv4 *	GUESTS net	Autoriser accès internet et inter-vlan	←	Edit	Copy	Delete

Mise en place du DHCP sur les VLANS USERS, GUESTS et SERVERS

Services: ISC DHCPv4: [USERS]

[Play](#) [Stop](#) [Reset](#)

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.

[full help](#)

 Enable	<input checked="" type="checkbox"/> Enable DHCP server on the USERS interface								
 Deny unknown clients	<input type="checkbox"/>								
 Ignore Client UIDs	<input type="checkbox"/>								
 Subnet	10.100.1.64								
 Subnet mask	255.255.255.192								
 Available range	10.100.1.65 - 10.100.1.126								
 Range	<table border="1"> <tr> <td>from</td> <td>to</td> </tr> <tr> <td>10.100.1.70</td> <td>10.100.1.120</td> </tr> </table>	from	to	10.100.1.70	10.100.1.120				
from	to								
10.100.1.70	10.100.1.120								
 Additional Pools	<table border="1"> <thead> <tr> <th>Pool Start</th> <th>Pool End</th> <th>Description</th> <th>+</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td>+</td> </tr> </tbody> </table>	Pool Start	Pool End	Description	+				+
Pool Start	Pool End	Description	+						
			+						
 WINS servers	<table border="1"> <tr><td></td></tr> <tr><td></td></tr> </table>								
 DNS servers	<table border="1"> <tr><td>8.8.8.8</td></tr> <tr><td></td></tr> </table>	8.8.8.8							
8.8.8.8									
 Gateway	10.100.1.65								

On ajoute Intranet en allant dans Services > Unbound DNS > Overrides pour pouvoir Communiquer avec SRV du G2

<input checked="" type="checkbox"/>	Enabled	Host	Domain	Type	TTL (secondes)	IP address	Description	Command:
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	intranet	ttb.local	A (IPv4 add...)		10.100.2.128		Edit Copy Delete

Ensuite dans nos règles de Firewall on ajoute ces règles à l'interface LAN (VLAN 10 admin)

<input type="checkbox"/>		IPv4 TCP	LAN net	*	This Firewall	443 (HTTPS)	*	*	Autoriser WebGUIT HTTPS			
<input type="checkbox"/>		IPv4 TCP	LAN net	*	This Firewall	22 (SSH)	*	*	Accès SSH			
<input type="checkbox"/>		IPv4 *	LAN net	*	*	*	*	*	Accès total			

Maintenant avec tous les paramètres qu'on a mis quand on va sur notre VLAN 20 on ne peut plus accéder aux paramètres du FW



La connexion a échoué

Firefox ne peut établir de connexion avec le serveur à l'adresse 10.100.1.1.

- Le site est peut-être temporairement indisponible ou surchargé. Réessayez plus tard ;
- Si vous n'arrivez à naviguer sur aucun site, vérifiez la connexion au réseau de votre ordinateur ;
- Si votre ordinateur ou votre réseau est protégé par un pare-feu ou un proxy, assurez-vous que Firefox est autorisé à accéder au Web.

[Réessayer](#)

Et on le voit dans les logs

Interface	Time	Source	Destination	Proto	Label
🚫 LAN	→ 2026-01-16T13:00:51	192.168.1.125:57621	192.168.1.255:57621	udp	Default deny / state violation rule
🚫 WAN	→ 2026-01-16T13:00:51	192.168.1.125:57621	192.168.1.255:57621	udp	Default deny / state violation rule

Analyse de flux (obligatoire)

- Tableau des flux (source/destination/ports/justification/règle/test) conforme à la section 10.7.
- Les flux refusés doivent être explicités (DENY) avec leur justification.

Source	Destination	Protocole /Ports	Action	Sens / Initiateur	Justificati on métier	Règle associée	Test de validation
VLAN10(A dmin)	Infrastructure (Firewall, Routeur, ESXI)	TCP : 443, 22	ALLOW	Administrat ion / Interne	Gestion des équipemen ts critiques	G1_ADMIN_INFRA	Pouvoir envoyer une requête SSH vers le Routeur
VLAN10 (Admin)	Wan / Internet	TCP/UD P : 53, 80, 443	ALLOW	Administrat ion / Sortant	Mises à jour du système et téléchargement de paquets	G1_ADMIN_NET	Pouvoir mettre à jour les paquets avec pkg update
VLAN20 (Users)	Le Pare-feu (Interface Users 10.100.1.65)	UDP : 53	ALLOW	Utilisateur / Interne	Résolution de DNS interne et externe	G1_DNS_SVC	Pouvoir nslookup google.com
VLAN20 (Users)	Wan / Internet	TCP : 80, 443, 443 (UDP/Q UIC)	ALLOW	Utilisateur / Sortant	Accès aux CRMs, Mails, Visio, etc... (SaaS)	G1_USERS_WEB	Pouvoir naviguer sur le web
VLAN20 (Users)	VLAN30 (Serveur 10.100.1.13)	TCP : 445 (SMB)	ALLOW	Utilisateur / Inter-VLAN	Accès aux contrats et fichiers sur le serveur local	G1_USERS_TO_SRV	Pouvoir avoir accès aux fichiers et en partager sur 10.100.1.130

VLAN20 (Users)	Serveur G2 10.100.2.130	TCP : 443	ALLOW	Utilisateur / Inter-Site	Accès obligatoire au portail Intranet	G1_TO_G 2_INTRA	Pouvoir avoir accès à l'intranet local (https://intr anet.ttb.loc al)
VLAN20 (Users)	VLAN10 (admin)	Tous	DENY	Utilisateur / Intern-VLA N	Les commercia ux ne doivent pas accéder au réseau d'admin	G1_BLOC K_SENS	Ne pas pouvoir ping 10.100.1.1
VLAN40 (Guest)	Wan / Internet	TCP/UD P : 53, 80, 443	ALLOW	Invité / Sortant	Accès internet uniquemen t pour les visiteurs	G1_GUES T_NET	Pouvoir naviguer sur le web en tant que guest
VLAN40 (Guest)	Tous réseaux privés	Tous	DENY	Invité / Interne	Les guests sont isolés et ne voient rien du réseau interne	G1_GUES T_ISO	Ne pas pouvoir ping 10.100.1.65
Tout	Tout	Tous	DENY	Tout / Tout	"Zero Trust", Si ce n'est pas autorisé c'est interdit	DEFAULT _DENY	Tout flux hors tableau est bloqué

PV de recette

- Plan de tests + résultats (captures) + commentaires.
- Synthèse de conformité : exigences respectées / non respectées + actions correctives.

1. Client VLAN20 : DHCP OK + ping GW OK

Procédure

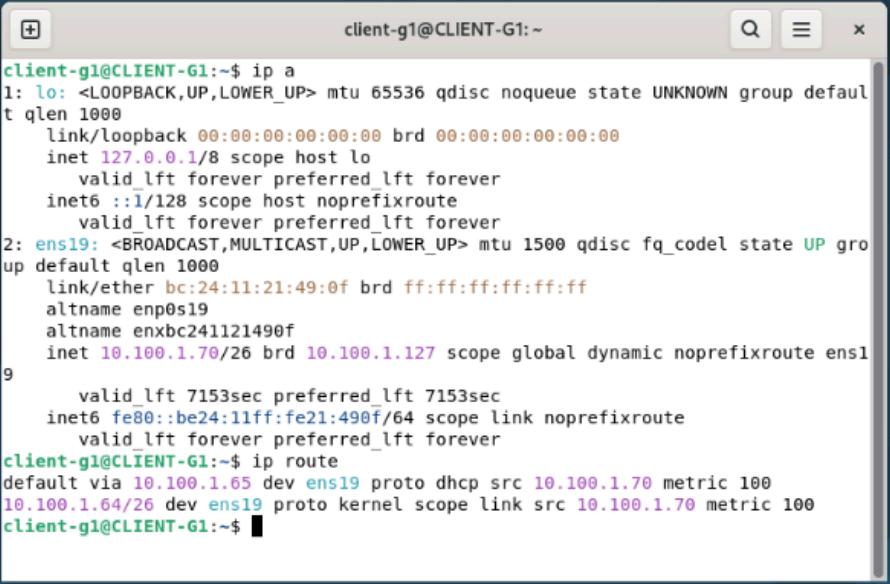
- Brancher un poste client sur le VLAN20
- Contrôler les paramètres réseau du poste (commande ipconfig /all ou équivalent)
- Vérifier la connectivité en envoyant un ping vers la passerelle

Résultat attendu

- Le poste client reçoit une adresse IP appartenant au réseau du VLAN20
- La passerelle par défaut correspond à l'adresse IP de l'interface OPNsense associée au VLAN20
- La passerelle répond aux requêtes ping

Résultat observé

- Le poste client obtient correctement une adresse IP dans la plage définie par le DHCP
- La passerelle est joignable et répond au ping



```
client-g1@CLIENT-G1:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    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 noprefixroute
        valid_lft forever preferred_lft forever
2: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether bc:24:11:21:49:0f brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    altname enx0c241121490f
    inet 10.100.1.70/26 brd 10.100.1.127 scope global dynamic noprefixroute ens19
        valid_lft 7153sec preferred_lft 7153sec
    inet6 fe80::be24:11ff:fe21:490f/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
client-g1@CLIENT-G1:~$ ip route
default via 10.100.1.65 dev ens19 proto dhcp src 10.100.1.70 metric 100
10.100.1.64/26 dev ens19 proto kernel scope link src 10.100.1.70 metric 100
client-g1@CLIENT-G1:~$
```

2. Client VLAN20 : DNS OK (résolution)

Procédure

- Depuis un poste appartenant au VLAN20, effectuer une requête de résolution DNS (nslookup ou ping vers un nom de domaine)

- Tester la résolution d'un nom de domaine interne et/ou externe

Résultat attendu

- Le nom de domaine est correctement traduit en adresse IP
- Aucune erreur liée au service DNS n'est rencontrée

Résultat observé

- Le nom de domaine testé est résolu correctement en adresse IP
- Aucune erreur DNS n'est retournée lors des tests

```

client-g1@CLIENT-G1:~$ nslookup google.com
Server:      10.100.1.1
Address:     10.100.1.1#53

Non-authoritative answer:
Name:   google.com
Address: 142.251.39.206
Name:   google.com
Address: 2a00:1450:4007:80f::200e

client-g1@CLIENT-G1:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=10.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=11.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=11.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=10.6 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=116 time=11.2 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=116 time=10.6 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=116 time=10.6 ms

```

3. Client VLAN20 : accès web/service externe OK (si service disponible)

Procédure

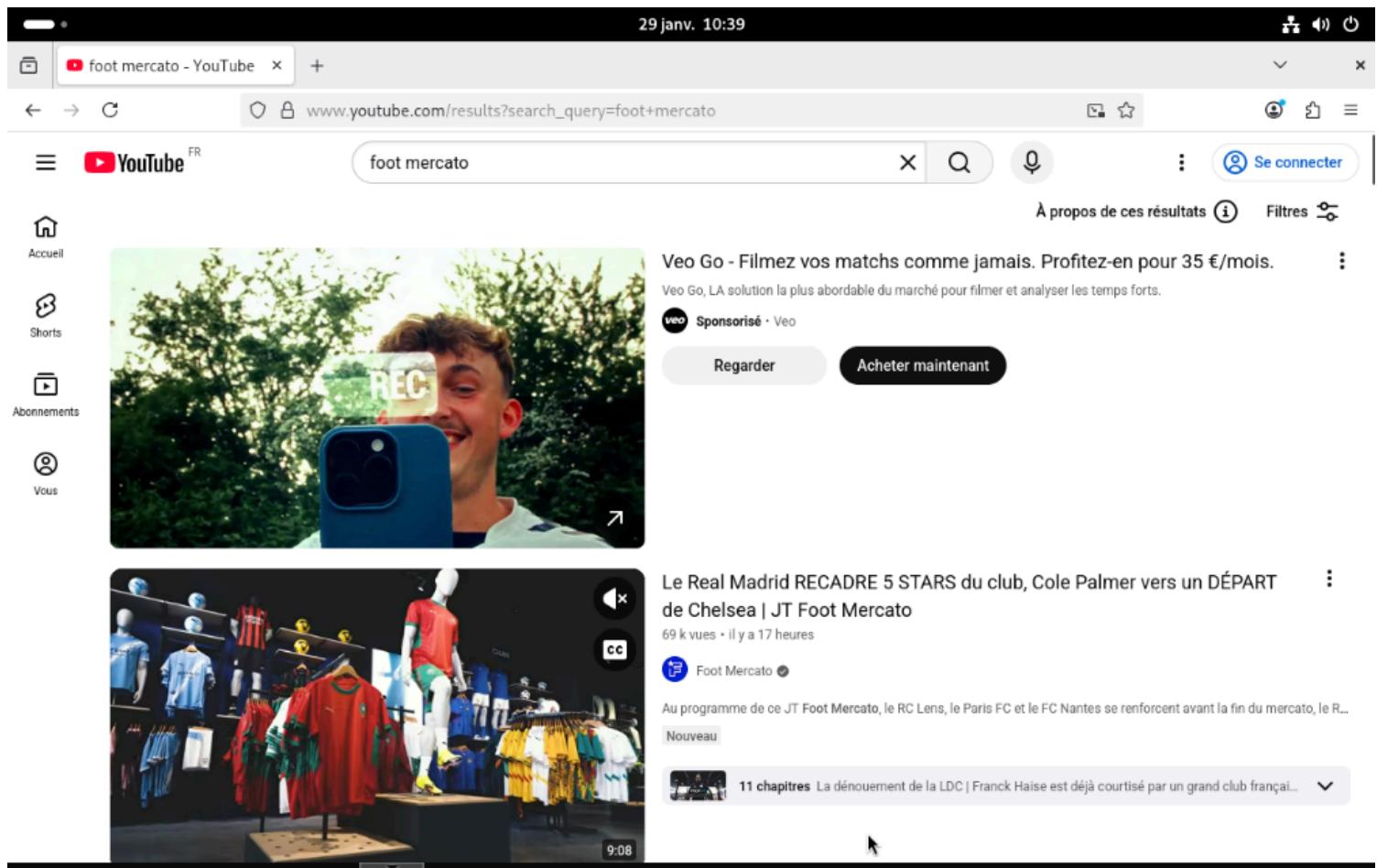
- Depuis un poste connecté au VLAN20, accéder à un site web externe via un navigateur en HTTP et/ou HTTPS

Résultat attendu

- Le site web est accessible depuis le navigateur
- La connexion HTTP/HTTPS s'établit sans erreur

Résultat observé

- Le poste client parvient à joindre le site web externe sans erreur
- La connectivité vers le service externe est fonctionnelle



4. Client VLAN20 : accès VLAN10 interdit (preuve)

Procédure

- Depuis un poste appartenant au VLAN20, tenter d'établir une communication (ping ou connexion réseau) vers une machine située dans le VLAN10

Résultat attendu

- Toute tentative de communication vers le VLAN10 est bloquée
- Aucune réponse n'est reçue depuis les équipements du VLAN10

Résultat observé

- Le poste client du VLAN20 ne parvient pas à joindre les machines du VLAN10
- Les requêtes de type ping échouent

The screenshot shows the OPNsense administration interface. The top bar displays the date and time (29 janv. 10:50) and the URL (10.100.1.1/firewall_rules.php?if=opt2). The left sidebar menu includes options like Pare-feu, Alias, Automatisation, Catégories, Groupes, NAT, Règles, Flottant, ADMIN, and GUEST. The main content area is titled "Pare-feu: Règles: USERS" and shows a table of rules. A message at the top of the table says "Les modifications ont été appliquées avec succès." (The changes have been applied successfully). The table has columns for Protocole, Source, Port, Destination, Port, Passerelle, Planifier, and Description. There are two visible rules:

- IPv4 * USERS net * * * * * Règles générées automatiquement
- IPv4 ICMP USERS net * ADMIN net * * * Interdiction acces VLAN20 a VLAN 10

A terminal window titled "client-g1@CLIENT-G1:~" is open, showing the command "ping 10.100.1.20" and its output:

```

client-g1@CLIENT-G1:~$ ping 10.100.1.20
PING 10.100.1.20 (10.100.1.20) 56(84) bytes of data.
^C
--- 10.100.1.20 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9222ms

client-g1@CLIENT-G1:~$

```

5. Client VLAN10 : accès admin OPNsense (HTTPS) OK

Procédure

- Depuis un poste connecté au VLAN10, accéder à l'interface web d'administration d'OPNsense via HTTPS

Résultat attendu

- L'interface d'administration OPNsense est accessible depuis le VLAN10
- La connexion HTTPS est autorisée et fonctionnelle

Résultat observé

- L'interface d'administration OPNsense est accessible depuis un poste du VLAN10
- La connexion HTTPS s'établit correctement sans erreur

The screenshot shows the OPNsense web interface at the URL 10.100.1.1/interfaces.php?if=opt1. The left sidebar is a navigation menu with various icons and labels. The main content area is titled "Interfaces: [ADMIN]" and contains two sections: "Configuration de base" and "Configuration générale".

Configuration de base:

- Activer: Checked (Activer l'interface)
- Verrouiller: Unchecked (Empêcher la suppression de l'interface)
- Identifiant: opt1
- Dispositif: wlan01
- Description: ADMIN

Configuration générale:

- Bloquer les réseaux privés: Unchecked
- Bloquer les adresses bogon (non attribuées par l'IANA): Unchecked
- Type de configuration IPv4: Address IPv4 statique
- Type de configuration IPv6: Aucun

At the bottom of the page, there is a footer with the text "OPNsense (c) 2014-2025 Deciso B.V."

6. Client VLAN40 : Internet OK ; accès interne interdit

Procédure

- Depuis un poste connecté au VLAN40, accéder à un site Internet
- Tenter d'établir une communication (ping ou connexion réseau) vers les autres VLANs ou le réseau interne

Résultat attendu

- L'accès à Internet est opérationnel
- Toute tentative d'accès aux VLANs internes est bloquée

Résultat observé

- Le poste client parvient à joindre un site Internet sans erreur
- Les communications vers les VLANs internes échouent

The screenshot shows the OPNsense firewall rules configuration interface. The left sidebar lists categories: Pare-feu, Alias, Automatisation, Catégories, Groupes, NAT, Règles, Flottant, ADMIN, GUEST, SERVER, USERS, and WAN. The 'GUEST' category is selected. The main pane displays the 'Pare-feu: Règles: GUEST' section with a message: 'Les modifications ont été appliquées avec succès.' Below is a table of rules:

	Protocole	Source	Port	Destination	Port	Passerelle	Planifier	Description	Actions
<input type="checkbox"/>	x → IPv4 *	GUEST net	*	ADMIN net	*	*	*	Règles générées automatiquement	Edit Delete
<input type="checkbox"/>	x → IPv4 *	GUEST net	*	SERVER net	*	*	*		Edit Delete
<input type="checkbox"/>	x → IPv4 *	GUEST net	*	USERS net	*	*	*		Edit Delete
<input type="checkbox"/>	→ IPv4 *	GUEST net	*	*	*	*	*	Accès à internet Vlan 40	Edit Delete

The terminal window below shows the following command output:

```

client-g1@CLIENT-G1:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=10.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=11.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=10.2 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 10.238/10.578/11.041/0.338 ms
client-g1@CLIENT-G1:~$ ping 10.100.1.1
PING 10.100.1.1 (10.100.1.1) 56(84) bytes of data.
^C
--- 10.100.1.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2050ms

client-g1@CLIENT-G1:~$

```

7. Inter-divisions IPv4 : ping + traceroute vers 2 divisions

Procédure

- Depuis une machine locale, effectuer un ping vers deux adresses IPv4 appartenant à deux divisions différentes
- Réaliser un traceroute vers ces mêmes destinations afin d'observer le chemin emprunté par les paquets

Résultat attendu

- Les requêtes ping n'aboutissent pas en raison des règles de filtrage inter-divisions
- Le traceroute affiche le chemin correct en passant par les routeurs intermédiaires configurés

Résultat observé

- Les requêtes ping entre un poste du VLAN10 et un poste du VLAN20 n'aboutissent pas
- Les requêtes ping entre un poste du VLAN20 et un poste du VLAN30 n'aboutissent pas non plus
- Le filtrage inter-divisions est bien appliqué

8. IPv6 : ping ICMPv6 local + ping ICMPv6 inter-division (1 minimum)

Procédure

- Vérifier l'attribution automatique d'une adresse IPv6 sur un poste client
- Tester la connectivité ICMPv6 locale (adresse link-local)
- Tester la possibilité de communication ICMPv6 entre différentes divisions (inter-VLAN)

Résultat attendu

- Une adresse IPv6 de type link-local (fe80::/10) est automatiquement attribuée en l'absence de configuration DHCPv6
- Le ping ICMPv6 local est fonctionnel
- Le ping ICMPv6 inter-divisions n'est pas possible en l'absence de routage IPv6 configuré

Résultat observé

- Une adresse IPv6 link-local est bien attribuée au poste client
- Le ping ICMPv6 local est fonctionnel
- Le ping ICMPv6 inter-divisions échoue, notamment lors d'un test vers un poste situé sur un autre VLAN

9. Logs : 1 preuve ALLOW + 1 preuve BLOCK associées à vos règles

Procédure

- Générer volontairement un trafic autorisé conformément aux règles firewall en place
- Générer volontairement un trafic bloqué par une règle de filtrage
- Consulter les journaux du pare-feu sur OPNsense

Résultat attendu

- Une entrée de log de type ALLOW correspondant à un flux autorisé
- Une entrée de log de type BLOCK correspondant à un flux interdit

Résultat observé

- Une entrée de journal ALLOW est générée pour le trafic autorisé
- Une entrée de journal BLOCK est générée pour le trafic bloqué

10. Preuve L2 : ARP/MAC observé et expliqué (court)

Procédure

- Envoyer un ping vers la passerelle du VLAN afin de déclencher une requête ARP
- Afficher la table ARP depuis le poste client

Résultat attendu

- Une correspondance entre une adresse IP et une adresse MAC apparaît dans la table ARP

Résultat observé

- Une entrée ARP correspondant à l'adresse IP de la passerelle est bien présente dans la table ARP

11. Preuve routage : show ip route expliqué (au moins 5 lignes)

Procédure

- Afficher la table de routage avec la commande show ip route (ou équivalent)
- Analyser au moins cinq routes correspondant aux VLANs et réseaux distants

Résultat attendu

- Les routes des VLANs locaux et des réseaux distants sont correctement présentes
- Le routage vers les différentes destinations est possible selon la configuration

Résultat observé

- La table de routage contient bien des entrées pour les VLAN10, VLAN20, VLAN30, VLAN40 et le réseau externe
- Les adresses réseau sont associées à leurs interfaces correspondantes
- Les routes statiques et dynamiques sont identifiables et conformes à la configuration prévue

10.100.1.0/26	link#7	U	vlan01
10.100.1.1	link#3	UHS	lo0
10.100.1.64/26	link#8	U	vlan02
10.100.1.65	link#3	UHS	lo0
10.100.1.128/27	link#9	U	vlan03
10.100.1.129	link#3	UHS	lo0
10.100.1.160/27	link#10	U	vlan04
10.100.1.161	link#3	UHS	lo0
127.0.0.1	link#3	UH	lo0

12. Flux imposé : depuis G1 et G4, accès au portail intranet.ttb.local (HTTPS) OK (preuve)

Procédure

- Depuis une machine du groupe G1, tenter d'accéder au portail intranet via HTTPS
- Répéter la même opération depuis une machine du groupe G4

Résultat attendu

- Le portail intranet est accessible depuis les postes des divisions G1 et G4

Résultat observé

- Le nom de domaine intranet.ttb.local n'est pas résolu par le DNS pour G1 et G4
- Après communication avec la division G2, le portail est accessible uniquement depuis G2, en raison des règles de pare-feu actuellement appliquées

- L'accès depuis G1 et G4 ne sera possible qu'après la configuration correcte du routeur principal et de son service DNS

```
29 janv. 11:32
client-g1@CLIENT-G1:~$ nslookup intranet.ttb.local
;; communications error to 10.100.1.1#53: timed out
^C
client-g1@CLIENT-G1:~$
```

13. Flux imposé : depuis G3, accès au portail intranet.ttb.local KO (preuve)

Recette CCNA1 — preuves supplémentaires (obligatoires)

14. Encapsulation/OSI (flux intranet) : explication 8 lignes max + capture associée.

Procédure

- Préparer une capture réseau sur un poste client (Wireshark ou équivalent)
- Accéder à <https://intranet.ttb.local> depuis un VLAN autorisé (ex : VLAN20 du G4)
- Identifier et associer chaque protocole aux couches OSI :

Couche 7 (Application) : HTTPS

Couche 6 (Présentation) : Chiffrement TLS

Couche 5 (Session) : Session TLS

Couche 4 (Transport) : TCP/443

Couche 3 (Réseau) : IPv4

Couche 2 (Liaison) : Ethernet (MAC)

Couche 1 (Physique) : Transmission sur le lien Ethernet

Résultat attendu

- Le flux HTTPS vers le portail intranet est observable
- Les différentes couches OSI sont clairement identifiables dans la capture

Résultat observé

- Test non réalisé pour l'instant
- Le DNS inter-division n'est pas encore configuré
- L'accès à intranet.ttb.local est actuellement limité au G2

15. Transport : capture DNS (UDP/53) + capture début HTTPS (TCP/443 SYN/SYN-ACK/ACK).

Procédure

- Réaliser une capture réseau lors d'une résolution DNS depuis un poste client
- Réaliser une capture réseau lors de l'établissement d'une connexion HTTPS vers un serveur autorisé

Résultat attendu

- Le trafic DNS utilise le protocole UDP sur le port 53
- La connexion HTTPS utilise le protocole TCP sur le port 443, avec l'établissement classique SYN → SYN-ACK → ACK

Résultat observé

- Le DNS tente de résoudre le nom de domaine, mais la résolution échoue (problème lié au DNS inter-division non configuré)
- L'établissement HTTPS échoue, probablement en raison du firewall ou de l'absence de configuration DNS inter-division

16. Switching : preuve show mac address-table (si switch Cisco) ou preuve ARP/broadcast + explication broadcast domain vs collision domain.

Procédure

- Afficher la table MAC du switch ou observer le trafic réseau (ARP, broadcasts)
- Identifier les domaines de broadcast et de collision

Résultat attendu

- Le switch apprend correctement les adresses MAC des appareils connectés
- Les broadcasts et requêtes ARP sont visibles dans le réseau

Résultat observé

- Les adresses MAC sont correctement enregistrées par le switch sur les ports correspondants
- Les requêtes ARP sont transmises en broadcast, visibles par tous les appareils du VLAN

17. Subnetting : 1 calcul détaillé (réseau/broadcast/plage/nb hôtes) prouvant que le VLAN choisi couvre le besoin.

Procédure

- Calcul détaillé du sous-réseau VLAN20 : adresse réseau, adresse broadcast, plage d'adresses et nombre d'hôtes
- Considérations sur le nombre d'utilisateurs : le service marketing d'une PME/ETI représente environ 2 à 10 % des effectifs (estimation : 50 employés maximum)
- Vérification que le plan d'adressage permet de couvrir ces besoins

Résultat attendu

- Les adresses disponibles suffisent pour le nombre d'utilisateurs du service marketing
- La plage DHCP est correctement définie et incluse dans le sous-réseau

Résultat observé / Calcul

Adresse réseau : 10.100.1.0/26

Masque réseau : /26 \rightarrow 32 - 26 = 6 bits hôtes $\rightarrow 2^6 = 64$ adresses totales

Adresse broadcast : 10.100.1.63

Plage d'adresses disponibles : 10.100.1.1 - 10.100.1.62

Passerelle : 10.100.1.1

Nombre d'hôtes utilisables : 64 - 2 = 62 hôtes

→ Suffisant pour l'équipe administrative (effectif réduit).

Exploitation (runbook)

Le runbook doit contenir :

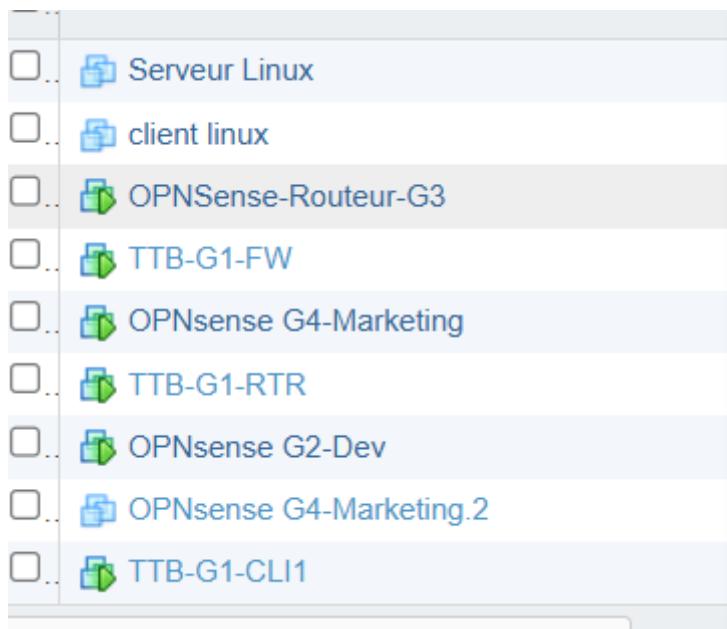
- Inventaire (équipements, VMs, réseaux, VLANs)

Équipements

Username : root

Password : SDVNantes!

Le routeur est branché sur le groupe PG-WAN-G1 pour simuler le lien vers le réseau commun .
Un lien a été établi entre le Routeur et le Pare-feu pour faire passer les paquets.



Physique

Équipement	Hostname	Adresses IPs	Marque
Routeur WAN	TTB-G1-RTR	10.255.4.2/30	Routeur Cisco
Switch Commercial	TTB-G1-SW1	10.100.1.2	Switch HP

Hyperviseur

Équipement	Hostname	Adresses IPs	OS

Hyperviseur	ESXi-Local	10.30.0.21	VMware
--------------------	------------	------------	--------

Machines virtuelles

Équipement	Hostname	Adresses IPs	OS
Firewall Virtuel	TTB-G1-FW	10.100.1.1 (HTTPS)	OPNsense
Routeur Virtuel	TTB-G1-RTR	172.16.0.11 (SSH)	OPNsense
Machine Cliente Virtuelle	TTB-G1-CLI1	10.100.1.11	Debian

VLANs

Plage : 10.100.1.0/24 - Groupe 1

VLANs	Nom	Adresse	Passerelle	DHCP	Usage
VLAN 10	ADMIN	10.100.1.0/26	.1	NON	Administration OPNsense et Switch
VLAN 20	USERS	10.100.1.64/26	.65	OUI	Postes Commerciaux (CRM, Web)
VLAN 30	SRV	10.100.1.128/27	.129	NON	Serveurs

VLAN 40	GUEST	10.100.1.160/27	.161	OUI	Invités
VLAN 99	MGMT	10.100.1.192/28	.193	NON	Management technique

- Procédure : ajouter une VM sur VLAN20 (ESXi + IP/DHCP)

Côté ESXi :

- Sélectionner la VM > *Modifier les paramètres*.
- Au niveau de l'adaptateur réseau, choisir le Port Group PG-USERS-G1 (VLAN 20).

Côté Client (VM) :

- Configurer la carte réseau en mode Automatique.
- **Sur Linux** : exécuter `sudo dhclient -v`
- **Sur Windows** : exécuter `ipconfig /renew`

Vérification :

- L'IP doit être comprise entre 10.100.1.70 et 10.100.1.126.
- Tester le ping vers la passerelle : ping 10.100.1.65.

- Procédure : ajouter un VLAN (ESXi + OPNsense + DHCP + règle de base)

OPNsense (Interfaces) :

- Aller dans *Interfaces* > *Other Types* > *VLAN*.
- Ajouter un VLAN sur l'interface parent (Trunk) avec le tag correspondant.
- Aller dans *Assignments* pour activer la nouvelle interface.

OPNsense (Services) :

- Assigner une IP statique à l'interface (ex: 10.100.1.x/27).
- Activer le serveur DHCP pour ce VLAN dans Services > DHCPv4.

OPNsense (Firewall) :

- Ajouter une règle "Pass" de base dans Firewall > Rules > [NouveauVLAN] pour autoriser le flux vers Internet.

- Procédure : sauvegarde/restauration OPNsense

Sauvegarde :

- Aller dans System > Configuration > Backups.
- Cliquer sur Download Configuration.
- Stocker le fichier .xml de manière sécurisée et en suivant les conditions de nommage.

Restauration :

- Sur un nouvel OPNsense, aller dans System > Configuration > Restore

- Sélectionner le fichier de sauvegarde et cliquer sur *Restore Configuration*.
- Le système redémarre avec tous les VLANs et règles récupérés

- Procédure : sauvegarde routeur

Commande de copie interne :

- *copy running-config startup-config* (pour sauvegarder en cas de redémarrage).

Extraction de la config :

- Exécuter *show running-config*
- Copier l'intégralité du texte affiché dans la console PuTTY
- Le coller dans un fichier texte nommé *TTB-G1-RTR_config_date.txt* sur votre PC d'administration.

- Checklists diagnostic : "DHCP KO", "DNS KO", "Pas d'accès inter-division", "Internet KO", "VM sur mauvais réseau ESXi"

Incident	Actions à mener pour tester
DHCP KO	<ul style="list-style-type: none"> - Vérifier si le service est "Running" dans <i>Services > ISC DHCPv4 > Interface</i>. - Vérifier si la VM est sur le bon Port Group ESXi. - Vérifier que la plage d'IP n'est pas pleine.
DNS KO	<ul style="list-style-type: none"> - Tenter un ping 8.8.8.8 - Vérifier si Unbound DNS est activé sur OPNsense. - Vérifier que le client a bien l'IP du Firewall (10.100.1.65 ou 10.100.1.161) comme DNS.
Pas d'accès Inter-Division	<ul style="list-style-type: none"> - Vérifier la route statique sur le Routeur G1 (<i>show ip route</i>). - Vérifier les règles Firewall sur l'interface d'entrée. - Consulter <i>Firewall > Log Files > Live View</i> pour voir si le flux est bloqué → BLOCK.
Internet KO	<ul style="list-style-type: none"> - Vérifier si la Gateway WAN (10.255.1.1) est "Online" dans <i>System > Gateways</i>. - Vérifier que le NAT Outbound est en mode "Automatic" ou "Hybrid". - Pinger l'IP du routeur voisin pour tester le lien de transit.

VM sur mauvais réseau ESXi	<ul style="list-style-type: none"> - Comparer l'IP de la VM avec le plan d'adressage - Vérifier le tag VLAN du Port Group dans ESXI.
----------------------------	--

- Points de contrôle (interfaces up, DHCP, DNS, NAT, logs)

- Interfaces UP : Sur le dashboard OPNsense, toutes les flèches des interfaces (WAN, USERS, GUEST, ADMIN) doivent être vertes.
- Services : Unbound DNS et DHCPv4 doivent être marqués comme démarrés.
- NAT : Présence des règles automatiques pour chaque sous-réseau vers l'interface WAN.
- Logs : Vérifier que le flux DNS/HTTP des USERS génère bien des lignes "Pass".

- Rollback simple : comment revenir à la dernière config stable (routeur + OPNsense)

- Aller dans *System > Configuration > History*.
- Comparer les versions de configuration par date et heure.
- Cliquez sur le bouton "Restore" à côté de la dernière version fonctionnelle connue.
- Le firewall recharge immédiatement les anciens paramètres sans redémarrage nécessaire.

Supervision

* La partie Wazuh n'a pas pu être réalisé à cause d'un retard pris : manque d'équipement → pas assez de ports sur le routeur WAN pour tous les groupes → nous avons dû changer de routeur pour le routeur 27 et avons donc perdu beaucoup du temps de TP supervision pour devoir refaire notre configuration cisco - VMs ESXI sur le routeur 27.

Ainsi ce TP à été réalisé sur Proxmox et sur un serveur hébergé chez un des membres du groupe en parallèle du rattrapage de la configuration ESXI afin d'avancer sur ce TP puis d'appliquer cela sur la configuration physique EXSI.

Lien vers fichier d'export du dashboard JSON.

https://drive.google.com/file/d/1S0g0leDlcilXkuFGs0Tc66ohXpa34WQN/view?usp=drive_link

Résumé & périmètre

5.1 Inclus

- Supervision (disponibilité, performance, capacité)
- Centralisation logs OPNsense (preuve ALLOW/BLOCK)
- Alerting Grafana actionnable

Alerte active sur l'instance OPNsense

Règle lorsque CPU > 1%

Une alerte de supervision a été configurée dans Grafana afin de surveiller la charge CPU du pare-feu OPNsense.

Pour les besoins du test, le seuil a été volontairement abaissé à 1 %, ce qui permet de déclencher rapidement l'alerte.

Lors du dépassement de ce seuil, l'alerte passe à l'état FIRING, confirmant le bon fonctionnement de la chaîne de supervision Prometheus / Grafana.

29 janv. 19:22

Non sécurisé http://10.100.1.140:3000/alerting/list

Grafana

Alert rules - Alertin x Dashboards - Graf x Prometheus Time x GUEST | Règles | P x Vue en direct | Fich x Document sans tit x

Home Alerting Alert rules

Alert rules

Rules that determine whether an alert will fire

Search by data sources Dashboard

All data sources Select dashboard

State Rule type Health

Firing Normal Pending Recovering Alert Recording Ok No Data Error

Contact point Choose a contact point

Search View as

Q Search Grouped List State

1 rule 1 firing

Grafana-managed

Export rules + New recording rule

Supervision > CRITIQUE

1 firing | 30s |

State	Name	Health	Summary	Next evaluation	Actions
Firing for 5m	OPNSENSE CPU	ok	CPU OPnse	within 30s	View Edit More

1 rule 1 firing

Grafana-managed

Export rules + New recording rule

Supervision > CRITIQUE

1 firing | 30s |

State	Name	Health	Summary	Next evaluation	Actions
Firing for 6m	OPNSENSE CPU	ok	CPU OPnse	in a few seconds	View Edit More

● ITSM GLPI (inventaire, SLA, incidents, journal CHG)

Installation GLPI

30 janv. 11:23

Document sans titre - Glpi x [SERVER] | ISC DHCPv4 x Nouvel onglet x Apache2 Debian Default Page x Setup GLPI x

Non sécurisé http://10.100.1.142/glpi/install/install.php

GLPI SETUP

Sélectionnez votre langue

French

OK >

GLPI a été déployé sur une VM dédiée en VLAN SERVER.

Les dépendances applicatives ont été ajustées pour assurer la compatibilité PHP, et l'installation a été sécurisée selon les recommandations de l'éditeur.

The screenshot shows the GLPI dashboard with a prominent orange warning box at the top. The box contains several bullet points regarding security, including changing default passwords, removing install files, securing the root directory, and defining session.cookie_httponly. Below the warning, there are several status cards: Logiciel (0), Ordinateur (0), Matériel réseau (0), Téléphone (0), Licence (0), Moniteur (0), Table (0), and Imprimante (0). A large central area displays a chart titled "Statuts des tickets par mois" with a single bar labeled "Aucune donnée trouvée".

Configuration de GLPI

This screenshot shows the "Ordinateurs" (Computers) section of the GLPI configuration interface. It includes a search bar, filter options, and a table listing two computer assets. The table columns include Nom, Statut, Fabricant, Numéro de Série, Type, Modèle, Système d'exploitation - Nom, Lieu, Dernière Modification, and Composants - Processeur. The assets listed are "PC-CLIENT-G1" (En production, Bureau) and "SRV-ITSM-01" (En production, Virtuel).

This screenshot shows the "Parc" (Inventory) section of the GLPI configuration interface. It features a summary card with counts for various asset types: 2 Ordinateurs, 0 Logiciel, 1 Matériel réseau, 0 Boîte, and 0 Châssis. Below this, there is a table with columns: Nom, Statut, Fabricant, Numéro de Série, Type, Modèle, Système d'exploitation - Nom, Lieu, Dernière Modification, and Composants - Processeur. The table lists the same two computer assets as the previous screenshot.

Non sécurisé http://10.100.1.142/glpi/front/ticket.form.php

GLPI

Accueil / Assistance / Tickets

Rechercher

Super-Admin Entité racine (Arborescence) GL

glpi

Ticket sera ajouté à l'entité Entité racine

Titre
DNS intranet Indisponible

Description *

Paragraphe B I A ...

Fichier(s) (2 Mio maximum) i
Glissez et déposez votre fichier ici, ou

Ticket

Date d'ouverture

Type Incident

Catégorie Réseau > DNS

Statut Nouveau

Source de la demande Helpdesk

Urgence

+ Ajouter

Incident GLPI créés et attribués.

Non sécurisé http://10.100.1.142/glpi/front/ticket.php

GLPI

Accueil / Assistance / Tickets

Rechercher

Super-Admin Entité racine (Arborescence) US

Tickets	Tickets entrants	Tickets en attente	Tickets assignés	Tickets planifiés	Tickets résolus	Tickets fermés
2	0	0	1	0	0	0

Caractéristiques - Statut est Non résolu

Actions

ID	TITRE	STATUT	DERNIÈRE MODIFICATION	DATE D'OUVERTURE	PRIORITÉ	DEMANDEUR - DEMANDEUR	ATTRIBUÉ À - TECHNICIEN	CATÉGORIE TTR
1	DNS intranet Indisponible	En cours (Attribué)	2026-01-30 13:22	2026-01-30 13:12	Haute	USER103 i	tech i	Réseau > DNS
2	Perte de connectivité VLAN 30 -	En cours (Attribué)	2026-01-30 13:21	2026-01-30 13:16	Très haute	USER103 i	tech i	Réseau - Pare feu

Création SLA

[SERVER] | ISC DHCPv4 | + G Niveau de services - SLA - +

Non sécurisé http://10.100.1.142/glpi/front/slm.form.php?id=3

GLPI

Accueil / Configuration / Niveaux de services

Rechercher

Super-Admin Entité racine (Arborescence) US

Niveau de services

SLAs 2

OLA

Historique 3

Tous

Ajouter un nouvel élément

Niveau de services - SLA - Incident Critique Intranet

Actions

Nom	Type	Durée maximale	Calendrier
SLA - Incident Critique Intranet	TTO	4 heures	24 heures sur 24, 7 jours sur 7
SLA - incident standar reseau	TTO	4 heures	24 heures sur 24, 7 jours sur 7

SLA ATTRIBUER

The screenshot shows the GLPI software interface. The left sidebar is titled 'GLPI' and contains a navigation menu with items like 'Parc', 'Assistance' (selected), 'Tickets' (selected), 'Problèmes', 'Changements', 'Planning', and 'Statistiques'. A purple box highlights the 'Assistance' and 'Tickets' items. The main content area shows a ticket titled 'Perte de connectivité VLAN 30 - intranet (2)'. The ticket details include:

- Ticket**: Created 1 hour ago by USER103, last updated at the instant by USER103.
- Description**: Perte de connectivité VLAN 30 - intranet.
- Notes**: Les Utilisateurs du Vlan 30 n'ont plus accès à internet.
- Associated Entities**: 2 Acteurs, 0 Éléments.
- SLA**: SLA - Incident standard réseau.

- SOC-lite Wazuh (agents, 2 scénarios, triage)

5.2 Hors périmètre (sauf bonus)

- Haute disponibilité / PRA complet
- SIEM avancé multi-sources
- IDS complet (Snort = bonus)

Architecture cible (topologie, flux)

6.1 Topologie

- OPNsense (VM) : routeur central (routage inter-VLAN + interconnexion WAN inter-divisions), NAT, DHCP/DNS, règles.
- Routeur Cisco : accès WAN / point de raccordement inter-groupes (liaison de transit vers OPNsense).
- ESXi : hébergement OPNsense + VMs.

Targets Prometheus

The screenshot shows the Prometheus Targets page with two sections:

- opnSense_node_exporter (1/1 up)**: A table with one row. The endpoint is `http://10.100.1.1:9100/metrics`, state is `UP`, labels include `instance="10.100.1.1:9100"` and `job="opnSense node exporter"`. Last scrape was 2.783s ago, scrape duration was 3.36ms, and there were no errors.
- prometheus (1/1 up)**: A table with one row. The endpoint is `http://localhost:9090/metrics`, state is `UP`, labels include `instance="localhost:9090"` and `job="prometheus"`. Last scrape was 10.592s ago, scrape duration was 3.86ms, and there were no errors.

Configuration (détails par brique)

Exigences — LOT 1 : Grafana (NOC)

— P0

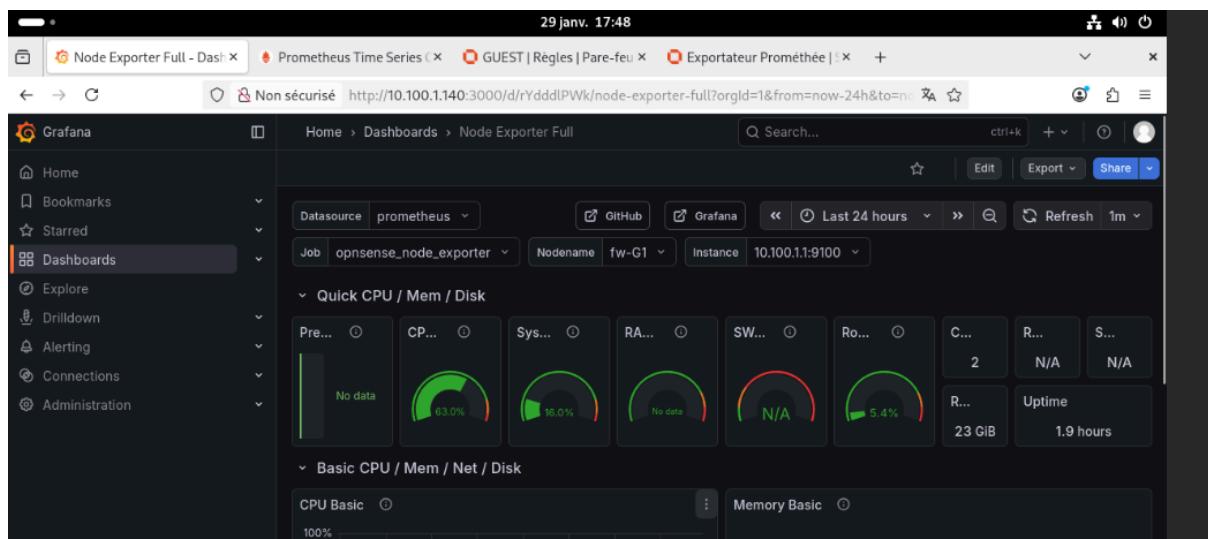
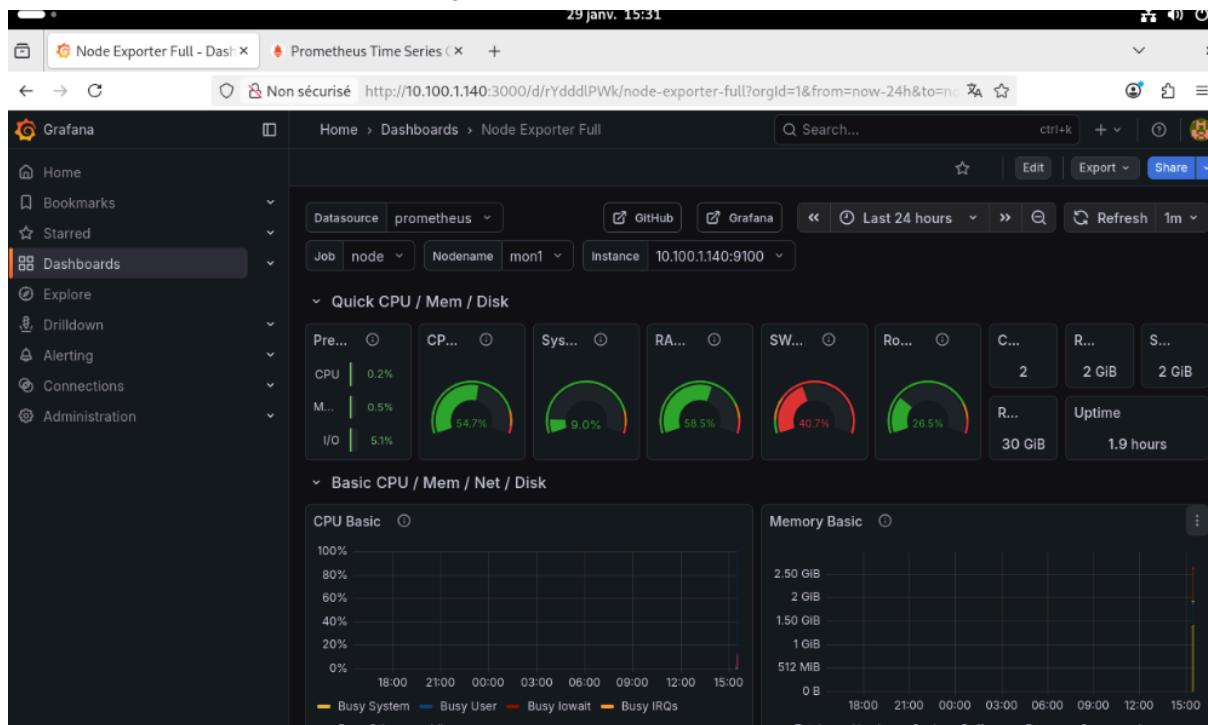
Stack : Grafana, Prometheus, Node Exporter

Périmètre LAN (obligatoire) :

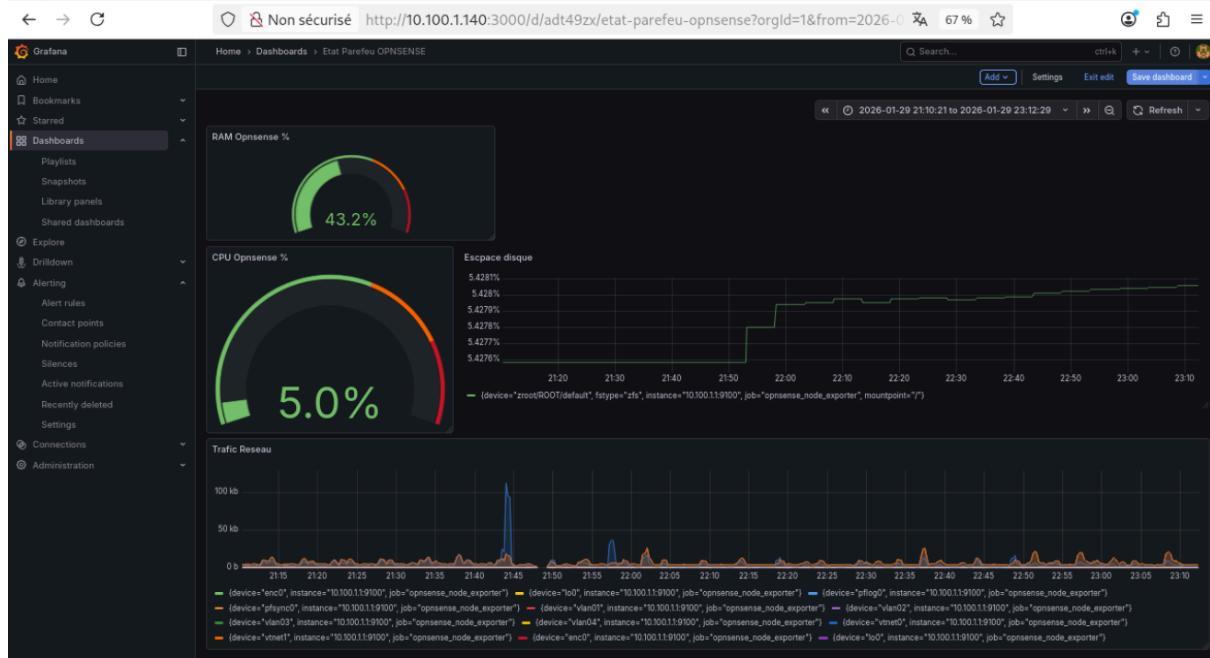
- supervision des équipements du groupe (RTR1/FW1/ESX1 + VMs + services),

Le pare-feu OPNsense est supervisé via Prometheus et Grafana.

Les métriques CPU, mémoire, uptime et ressources système sont collectées en temps réel grâce à l'exportateur Node Exporter intégré à OPNsense.



Supervision OPNsense (système)



Interface finale :



- supervision SLA "vue client" depuis le LAN (Blackbox),
- logs firewall OPNsense (preuve ALLOW/BLOCK).

Analyse (post-mortem de 2 incidents)

Incident 1 — Alerte CPU anormale sur OPNsense

Une alerte Grafana s'est déclenchée indiquant une utilisation CPU supérieure au seuil configuré sur l'instance OPNsense.

Le seuil ayant été volontairement fixé à 1% pour les tests, l'alerte est passée rapidement à l'état FIRING.

Détection

Source : Prometheus + Node Exporter

Outil d'alerte : Grafana

Règle : CPU usage > 1%

État : FIRING

Chronologie

- départ : Activation règle de test CPU
- après quelques secondes : déclenchement alerte FIRING
- puis vérification métriques dans Grafana
- identification seuil trop bas
- après quelques minutes : correction du seuil

Augmentation du seuil à une valeur réaliste :

Warning : 60 %

Critical : 85 %

Incident 2 — Absence de remontée des métriques / logs OPNsense vers Grafana

Les métriques Prometheus et les logs firewall (ALLOW/BLOCK) n'étaient plus visibles dans Grafana.

L'origine provenait d'un blocage firewall inter-VLAN, empêchant la communication entre OPNsense et le serveur de supervision.

Détection

Dashboards Grafana vides

Targets Prometheus marquées DOWN

Absence de nouveaux logs firewall

Chronologie

- Déploiement nouvelles règles VLAN (segmentation Users/Guests)
- après quelques minutes perte des métriques
- Grafana affiche targets DOWN
- vérification connectivité (ping KO)
- identification règle bloquante

- ajout alias + règle d'autorisation supervision
- retour métriques (targets UP)

Mise en service (procédure d'installation)

Règles Firewall pour Supervision dans OPNSense

Ajout d'un alias pour mettre des ports précis pour permettre le flux de supervision vers les autres VLANs

Edit Alias

The screenshot shows the 'Edit Alias' configuration page. The 'Enabled' field is checked. The 'Name' field contains 'Supervision_Ports'. The 'Type' field is set to 'Port(s)'. The 'Content' field lists ports 9100 and 9115, with buttons for Clear All, Copy, Paste, and Text.

Enabled	<input checked="" type="checkbox"/>
Name	Supervision_Ports
Type	Port(s)
Categories	
Content	9100 <input type="button" value="x"/> 9115 <input type="button" value="x"/> ✖ Clear All
Description	

Ajout de la règle

The screenshot shows the 'Edit Firewall rule' configuration page for the 'SERVERS' interface. The 'Action' is set to 'Pass'. The 'Disabled' checkbox is unchecked. The 'Quick' checkbox is checked. The 'Interface' is 'SERVERS', 'Direction' is 'in', 'TCP/IP Version' is 'IPv4', and 'Protocol' is 'TCP'. The 'Source' is 'SERVERS net' and the 'Destination' is 'any'. The 'Destination port range' is 'from: Supervision_Ports to: Supervision_Ports'. There are also sections for 'Source / Invert' and 'Destination / Invert'.

Firewall: Rules: SERVERS

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the password "root".

Action	Pass
Disabled	<input type="checkbox"/> Disable this rule
Quick	<input checked="" type="checkbox"/> Apply the action immediately on match.
Interface	SERVERS
Direction	in
TCP/IP Version	IPv4
Protocol	TCP
Source / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Source	SERVERS net
Source / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Destination / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Destination	any
Destination port range	from: Supervision_Ports to: Supervision_Ports

Règles SERVERS

Firewall: Rules: SERVERS

Select category

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.

The changes have been applied successfully.

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	Actions
IPv4 *	SERVERS net	*	*	*	*	*	Automatically generated rules	
IPv4 TCP	SERVERS net	*	*	Supervision_Ports	*	*	Autoriser accès internet et inter-vlan	
IPv4 ICMP	SERVERS net	*	*	*	*	*	Flux de supervision vers les autres VLANs	
pass	block				reject		Ping	
pass (disabled)	block (disabled)				reject (disabled)			
					log		first match	
					log (disabled)		last match	
Active/Inactive Schedule (click to view/edit)								

Création d'un alias pour l'administration OPNsense

Edit Alias

Enabled

Name Admin_OPNSense

Type Port(s)

Categories

Content 22 443

Description

Création d'un alias pour l'interface Grafana

Edit Alias

Enabled

Name Grafana

Type Port(s)

Categories

Content 3000

Description Port Grafana

Puis création de la règle pour autoriser la supervision

Firewall: Rules: LAN

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using

Edit Firewall rule

Action	Pass	
Disabled	<input type="checkbox"/> Disable this rule	
Quick	<input checked="" type="checkbox"/> Apply the action immediately on match.	
Interface	LAN	
Direction	in	
TCP/IP Version	IPv4	
Protocol	TCP	
Source / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.	
Source	LAN net	
Source	Advanced	
Destination / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.	
Destination	SERVERS net	
Destination port range	from: Grafana	to: Grafana
Log	<input type="checkbox"/> Log packets that are handled by this rule	
Category		
Description	Accès Supervision	

Récap règles LAN (admin)

Firewall: Rules: LAN

Select category

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.

The changes have been applied successfully.

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Actions	Description	Buttons	
Automatically generated rules										
IPv4 *	LAN net	*	*	*	*	*		Default allow LAN to any rule		
IPv6 *	LAN net	*	*	*	*	*		Default allow LAN IPv6 to any rule		
IPv4 *	LAN net	*	*	*	*	*		Autoriser tout le trafic ADMIN		
IPv4 TCP	LAN net	*	LAN address	Admin_OPNSense	*	*		Administration OPNsense		
IPv4 TCP	LAN net	*	SERVERS net	Grafana	*	*		Accès Supervision		
IPv4 *	LAN net	*	*	*	*	*		Accès général		
pass	block	reject	log	in	first match					
pass (disabled)	block (disabled)	reject (disabled)	log (disabled)	out	last match					

Création d'un alias pour le réseau (que l'on bloquera)

Edit Alias

Enabled	<input checked="" type="checkbox"/>
Name	RFC1918
Type	Network(s)
Categories	
Content	<input type="text" value="10.0.0.0/8"/> <input type="text" value="172.16.0.0/12"/> <input type="text" value="192.168.0.0/16"/> <input type="button" value="Clear All"/> <input type="button" value="Copy"/> <input type="button" value="Paste"/> <input type="button" value="Text"/>
Statistics	<input type="checkbox"/>
Description	

Création de la règle pour bloquer l'accès Inter Vlan pour la VLAN Users et autoriser uniquement internet

Firewall: Rules: USERS

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the password "openwrt".

Edit Firewall rule		
Action	Pass	
Disabled	<input type="checkbox"/> Disable this rule	
Quick	<input checked="" type="checkbox"/> Apply the action immediately on match.	
Interface	USERS	
Direction	in	
TCP/IP Version	IPv4	
Protocol	any	
Source / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.	
Source	USERS net	
Source	Advanced	
Destination / Invert	<input checked="" type="checkbox"/> Use this option to invert the sense of the match.	
Destination	RFC1918	
Destination port range	from: any	to: any
Log	<input type="checkbox"/> Log packets that are handled by this rule	
Category		
Description	Autoriser Internet uniquement (Bloquer inter-VLAN)	

Firewall: Rules: USERS

Select category @ Inspect

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.

The changes have been applied successfully.

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description		
IPv4 *	USERS net	*	! RFC1918	*	*	*	Autoriser Internet uniquement (Bloquer inter-VLAN)		
pass			block		reject				
pass (disabled)			block (disabled)		reject (disabled)				
Active/Inactive Schedule (click to view/edit)									
Alias (click to view/edit)									

Et on répète la même chose pour la VLAN Guests

Firewall: Rules: GUESTS

Select category @ Inspect

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.

The changes have been applied successfully.

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description		
IPv4 *	GUESTS net	*	! RFC1918	*	*	*	Autoriser Internet uniquement (Bloquer inter-VLAN)		
pass			block		reject				
pass (disabled)			block (disabled)		reject (disabled)				
Active/Inactive Schedule (click to view/edit)									
Alias (click to view/edit)									

Afin d'autoriser l'accès à notre PC, on crée un Port Forward sur notre Opnsense.

Firewall: NAT: Port Forward

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.

Edit Redirect entry [full help](#)

<input type="checkbox"/> Disabled	<input type="checkbox"/> Disable this rule	
<input type="checkbox"/> No RDR (NOT)	<input type="checkbox"/>	
<input type="checkbox"/> Interface	WAN	
<input type="checkbox"/> TCP/IP Version	IPv4	
<input type="checkbox"/> Protocol	TCP	
Source	Advanced	
<input type="checkbox"/> Destination / Invert	<input type="checkbox"/>	
<input type="checkbox"/> Destination	WAN address	
<input type="checkbox"/> Destination port range	from: Grafana	to: Grafana
<input type="checkbox"/> Redirect target IP	Ip_grafana	
<input type="checkbox"/> Redirect target port	Grafana	
<input type="checkbox"/> Pool Options:	Default	
<input type="checkbox"/> Log	<input type="checkbox"/> Log packets that are handled by this rule	
<input type="checkbox"/> Category		
<input type="checkbox"/> Description		
<input type="checkbox"/> Set local tag		

Et une règle

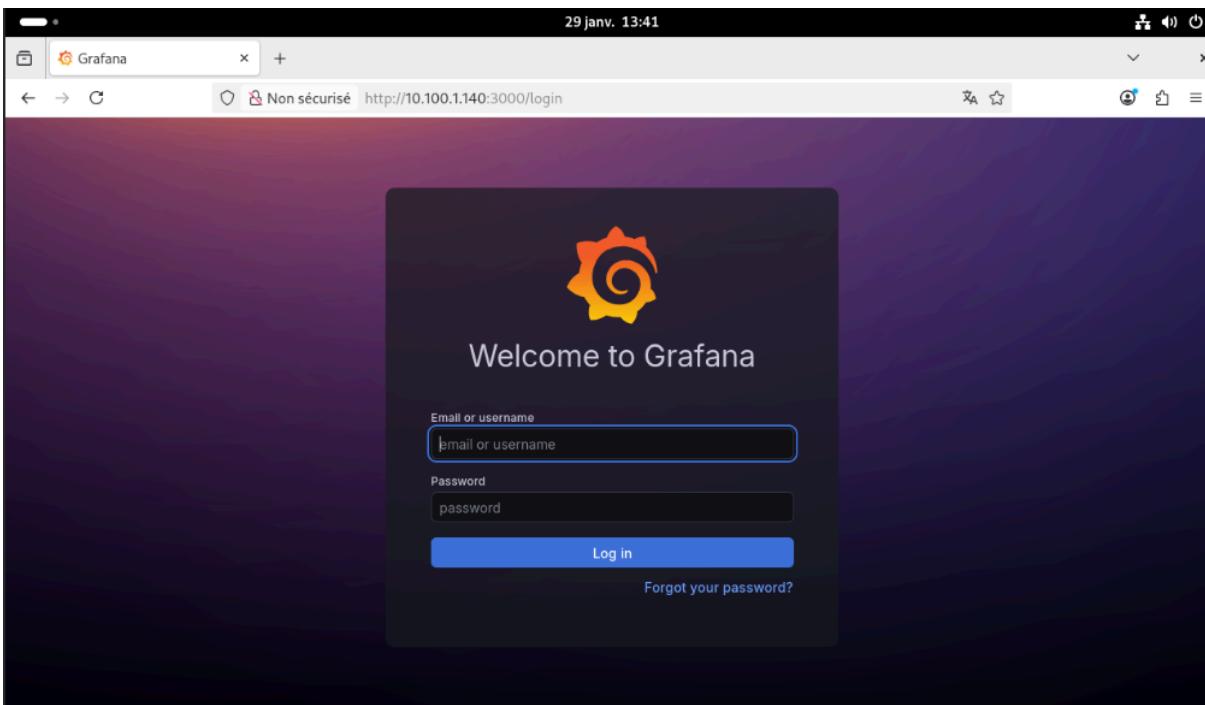
Firewall: Rules: WAN

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.

Edit Firewall rule		full help 
 Action	Pass	
 Disabled	<input type="checkbox"/> Disable this rule	
 Quick	<input checked="" type="checkbox"/> Apply the action immediately on match.	
 Interface	WAN	
 Direction	in	
 TCP/IP Version	IPv4	
 Protocol	TCP	
 Source / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.	
 Source	any	
Source	Advanced	
 Destination / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.	
 Destination	ip_grafana	
 Destination port range	from: Grafana	to: Grafana
 Log	<input type="checkbox"/> Log packets that are handled by this rule	
 Category		
 Description	Accès PC	
 No XMI RPC Sync	<input type="checkbox"/>	

Il faut également ajouter une route dans le CMD en admin

```
C:\Windows\System32>route add 10.100.1.0 mask 255.255.255.192 10.30.0.238
OK!
```



Username : admin

Password : admin

A screenshot of the Grafana dashboard home page. The left sidebar is titled "Grafana" and includes links for Home, Bookmarks, Starred, Dashboards, Explore, Drilldown, Alerting, Connections, and Administration. The main content area has a "Welcome to Grafana" header and a "Need help?" section with links to Documentation, Tutorials, Community, and Public Slack. It also features a "Basic" panel with instructions for setting up Grafana, a "TUTORIAL DATA SOURCE AND DASHBOARDS" panel, a "Grafana fundamentals" panel, and a "DATA SOURCES" panel with a "Add your first data source" button. At the bottom, there are links for Dashboards, Latest from the blog, and a blue banner for "CAN data analysis with Grafana Assistant". The address bar shows "Non sécurisé http://10.100.1.140:3000/?orgId=1&from=now-6h&to=now&timezone=browser".

Service Prometheus

```

29 janv. 13:50
Dashboards - Grafana
Non sécurisé http://10.100.1.140:3000/dashboards
Grafana
Home Bookmarks Starred Dashboards Explore Drilldown Alerting Connections Administration
client-g1@mon1: ~
prometheus.service - Monitoring system and time series database
  Loaded: loaded (/usr/lib/systemd/system/prometheus.service; enabled; preser...
  Active: active (running) since Thu 2026-01-29 13:35:14 CET; 15min ago
    Invocation: c5ec40cc5dbc430e9bf91ce9e3f9c845
  Docs: https://prometheus.io/docs/introduction/overview/
        man:prometheus(1)
  Main PID: 639 (prometheus)
    Tasks: 8 (limit: 2280)
   Memory: 47.8M (peak: 97.2M, swap: 1.8M, swap peak: 1.9M)
      CPU: 1.603s
     CGrou...
janv. 29 13:35:34 mon1 prometheus[639]: ts=2026-01-29T12:35:34.509Z caller=head>
janv. 29 13:35:34 mon1 prometheus[639]: ts=2026-01-29T12:35:34.509Z caller=head>
janv. 29 13:35:34 mon1 prometheus[639]: ts=2026-01-29T12:35:34.509Z caller=head>
janv. 29 13:35:34 mon1 prometheus[639]: ts=2026-01-29T12:35:34.511Z caller=main>
janv. 29 13:35:34 mon1 prometheus[639]: ts=2026-01-29T12:35:34.511Z caller=main>
janv. 29 13:35:34 mon1 prometheus[639]: ts=2026-01-29T12:35:34.511Z caller=main>
janv. 29 13:35:34 mon1 prometheus[639]: ts=2026-01-29T12:35:34.544Z caller=main>
janv. 29 13:35:34 mon1 prometheus[639]: ts=2026-01-29T12:35:34.544Z caller=main>
janv. 29 13:35:34 mon1 prometheus[639]: ts=2026-01-29T12:35:34.545Z caller=main>
janv. 29 13:35:34 mon1 prometheus[639]: ts=2026-01-29T12:35:34.545Z caller=main>
lines 1-23

```

Connection API au service de Prometheus

The screenshot shows the Grafana interface for managing connections. A new connection for 'prometheus' has been created and is being configured.

Connection Details:

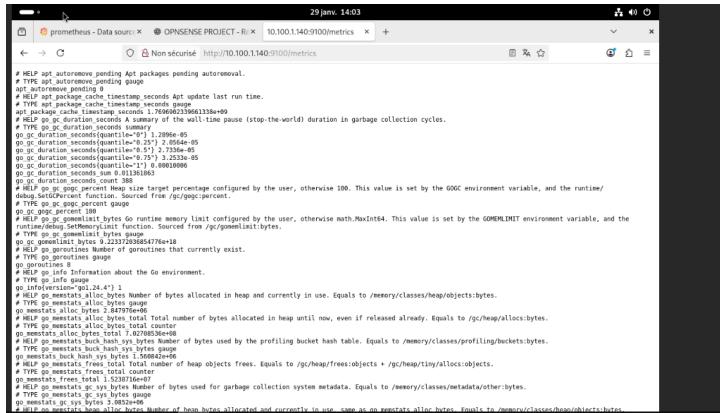
- Type:** Prometheus
- Name:** prometheus
- Prometheus server URL:** http://localhost:9090
- Authentication:** No Authentication

Configuration Notes:

Configure your Prometheus data source below
Or skip the effort and get Prometheus (and Loki) as fully-managed, scalable, and hosted data sources from Grafana Labs with the [free-forever Grafana Cloud plan](#).

Documentation: view the documentation

Installation des metrics sur la machine serveur



Ensuite on met bien prometheus en source et on peut changer le temps d'actualisation/time range

Ensuite on va permettre à Prometheus de voir les autres Vlans en modifiant ce fichier

```
utilisateur@admin:~$ sudo nano /etc/prometheus/prometheus.yml
```

On y modifie/ajoute ces lignes, bien faire attention aux espaces

```
scrape_configs:
  - job_name: 'prometheus'
    static_configs:
      - targets: ['localhost:9090']

  - job_name: 'node_exporter'
    static_configs:
      - targets: ['localhost:9100', '10.100.1.1:9100']
```

Pour relancer

```
utilisateur@admin:~$ sudo systemctl status prometheus
```

Et pour vérifier que c'est bon

```
utilisateur@admin:~$ sudo systemctl status prometheus
● prometheus.service - Monitoring system and time series database
  Loaded: loaded (/usr/lib/systemd/system/prometheus.service; enabled; preset: enabled)
  Active: active (running) since Fri 2026-01-30 14:17:50 UTC; 1min 16s ago
    Docs: https://prometheus.io/docs/introduction/overview/
          man:prometheus(1)
  Main PID: 19869 (prometheus)
    Tasks: 8 (limit: 4606)
   Memory: 56.8M (peak: 57.4M)
      CPU: 813ms
     CGroup: /system.slice/prometheus.service
             └─19869 /usr/bin/prometheus
```

Ensute on peut se rendre sur Prometheus

Il faut possiblement recréer un Port Forward

Firewall: NAT: Port Forward

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.

Edit Redirect entry [full help](#)

<input type="checkbox"/> Disabled	<input type="checkbox"/> Disable this rule	
<input type="checkbox"/> No RDR (NOT)	<input type="checkbox"/>	
<input type="checkbox"/> Interface	WAN	
<input type="checkbox"/> TCP/IP Version	IPv4	
<input type="checkbox"/> Protocol	TCP	
Source	Advanced	
<input type="checkbox"/> Destination / Invert	<input type="checkbox"/>	
<input type="checkbox"/> Destination	WAN address	
<input type="checkbox"/> Destination port range	from: Prometheus	to: Prometheus
<input type="checkbox"/> Redirect target IP	Ip_grafana	
<input type="checkbox"/> Redirect target port	Prometheus	
<input type="checkbox"/> Pool Options:	Default	
<input type="checkbox"/> Log	<input type="checkbox"/> Log packets that are handled by this rule	
<input type="checkbox"/> Category		
<input type="checkbox"/> Description		
<input type="checkbox"/> Set local tag		
<input type="checkbox"/> Match local tag		

← → ⌂ Non sécurisé 10.30.0.238:9090/classic/graph

Prometheus Alerts Graph Status Help

Enable query history

Expression (press Shift+Enter for newlines)

Execute - insert metric at cursor - [Remove Graph](#)

[Graph](#) [Console](#)

◀ Moment ▶

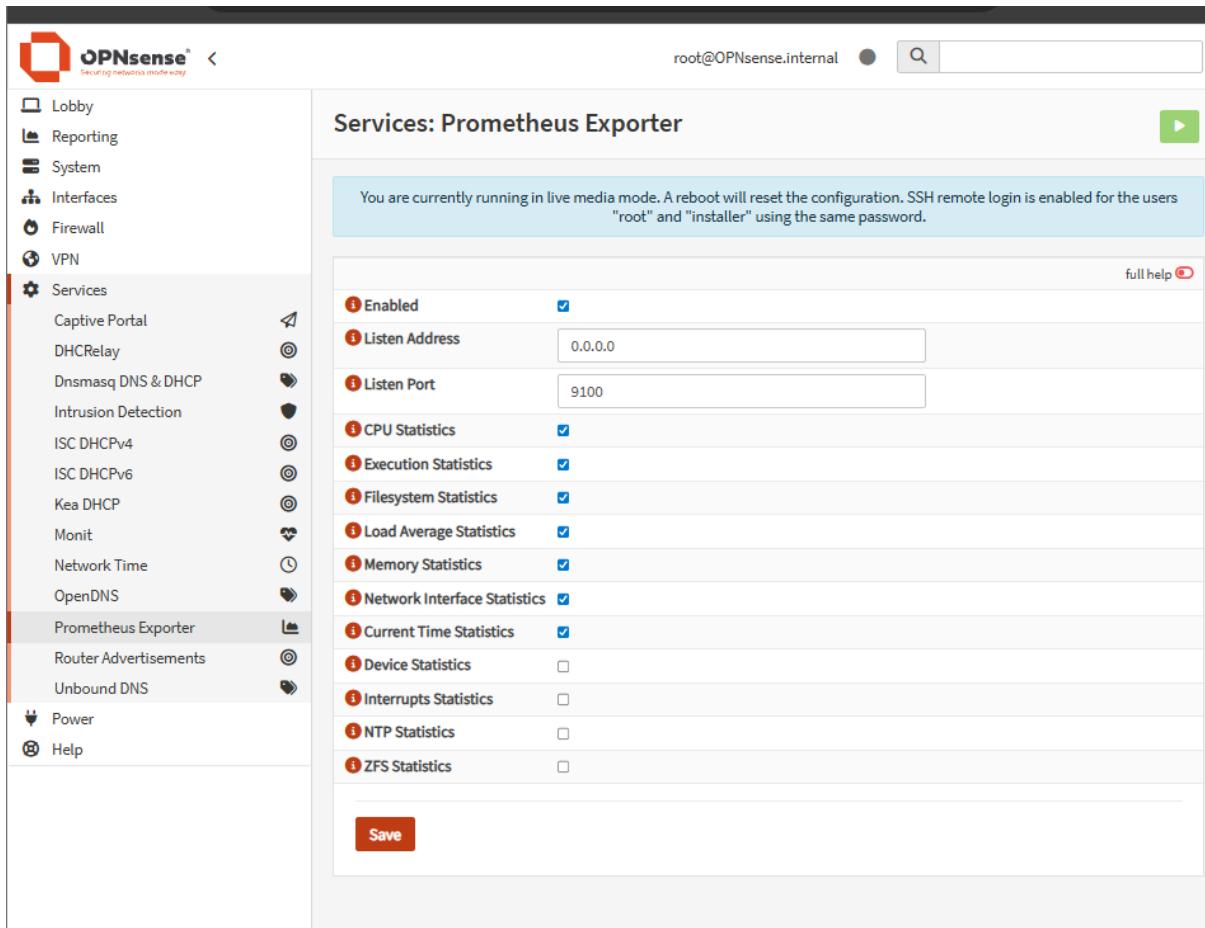
Element	Value
no data	

[Add Graph](#)

On doit rajouter le plugin os-node-exporter sur Opnsense

Name	Version	Size	Tier	Repository	Comment	<input type="checkbox"/> Show community plugins
os-node_exporter (misconfigured)	1.2	18.7KiB	3	OPNsense	Prometheus exporter for machine metrics	 

Puis on l'active et mets les paramètres suivants



The screenshot shows the OPNsense web interface under the 'Services' section. The left sidebar lists various services like 'Lobby', 'Reporting', 'System', 'Interfaces', 'Firewall', 'VPN', 'Services' (selected), 'Captive Portal', 'DHCRelay', 'Dnsmasq DNS & DHCP', 'Intrusion Detection', 'ISC DHCPv4', 'ISC DHCPv6', 'Kea DHCP', 'Monit', 'Network Time', 'OpenDNS', 'Prometheus Exporter' (selected), 'Router Advertisements', 'Unbound DNS', 'Power', and 'Help'. The right panel is titled 'Services: Prometheus Exporter' and contains a configuration form. A message at the top states: 'You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.' The configuration form includes fields for 'Enabled' (checked), 'Listen Address' (0.0.0.0), 'Listen Port' (9100), and several statistics checkboxes: CPU Statistics (checked), Execution Statistics (checked), Filesystem Statistics (checked), Load Average Statistics (checked), Memory Statistics (checked), Network Interface Statistics (checked), Current Time Statistics (checked), Device Statistics (unchecked), Interrupts Statistics (unchecked), NTP Statistics (unchecked), and ZFS Statistics (unchecked). A 'Save' button is at the bottom.

Ensuite sur Prometheus dans Status Targets tout sera Up

Nom de l'instance : 10.30.0.238:9090/classic/targets

Prometheus Alerts Graph Status Help

Targets

All Unhealthy Collapse All

node_exporter (2/2 up) [show less](#)

Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
http://10.100.1.1:9100/metrics	UP	instance="10.100.1.1:9100" job="node_exporter"	7s ago	7.394ms	
http://localhost:9100/metrics	UP	instance="localhost:9100" job="node_exporter"	539ms ago	255.1ms	

prometheus (1/1 up) [show less](#)

Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
http://localhost:9090/metrics	UP	instance="localhost:9090" job="prometheus"	8.818s ago	10.46ms	

Pour aller avec notre dashboard il faut installer Blackbox

```
utilisateur@admin:~$ sudo apt install prometheus-blackbox-exporter
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  prometheus-blackbox-exporter
0 mis à jour, 1 nouvellement installés, 0 à enlever et 134 non mis à jour.
Il est nécessaire de prendre 4 758 ko dans les archives.
Après cette opération, 14,9 Mo d'espace disque supplémentaires seront utilisés.
Réception de :1 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 prometheus-blackbox-exporter amd64
2ubuntu0.3 [4 758 kB]
4 758 ko réceptionnés en 1s (4 186 ko/s)
Préconfiguration des paquets...
Sélection du paquet prometheus-blackbox-exporter précédemment désélectionné.
(Lecture de la base de données... 152408 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../prometheus-blackbox-exporter_0.24.0-2ubuntu0.3_amd64.deb ...
Dépaquetage de prometheus-blackbox-exporter (0.24.0-2ubuntu0.3) ...
Paramétrage de prometheus-blackbox-exporter (0.24.0-2ubuntu0.3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/prometheus-blackbox-exporter.service → /usr/lib/system/prometheus-blackbox-exporter.service.
Traitement des actions différées (« triggers ») pour man-db (2.12.0-4build2) ...
```

Puis on entre le code suivant dans le fichier prometheus.yml :

```

- job_name: 'blackbox-https-intranet'
metrics_path: /probe
params:
  module: [http_2xx]
static_configs:
  - targets:
    - https://10.100.1.1 # URL de ton OPNsense ou Portail
relabel_configs:
  - source_labels: [__address__]
    target_label: __param_target
  - source_labels: [__param_target]
    target_label: instance
  - target_label: __address__
    replacement: 127.0.0.1:9115

job_name: 'blackbox-dns-intranet'
metrics_path: /probe
params:
  module: [dns_udp]
static_configs:
  - targets:
    - 10.100.1.1 # Ton serveur DNS
relabel_configs:
  - source_labels: [__address__]
    target_label: __param_target
  - target_label: __address__

```

```

  - target_label: __address__
    replacement: 127.0.0.1:9115

```

Loki également et le enable

```

utilisateur@admin:~$ sudo apt update && sudo apt install -y loki
Atteint :1 http://archive.ubuntu.com/ubuntu noble InRelease
Atteint :2 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Atteint :3 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Atteint :4 https://packages.grafana.com/oss/deb stable InRelease
Atteint :5 http://security.ubuntu.com/ubuntu noble-security InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
134 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
W: https://packages.grafana.com/oss/deb/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  loki

```

Et le connecter sur Grafana

The screenshot shows the configuration interface for a Loki data source in Grafana. At the top, there's a navigation bar with tabs for Settings (selected), Permissions, Insights, Cache, and a button to Build a dashboard. Below the navigation, a message box prompts the user to configure the Loki data source or skip to the Grafana Cloud plan. The main configuration area includes fields for Name (set to 'loki'), URL (set to 'http://localhost:3100'), and a Default toggle switch (which is off). A note below the URL field states: 'Before you can use the Loki data source, you must configure it below or in the config file. For detailed instructions, [view the documentation](#)'.

Type: Loki

Type: Loki

Settings Permissions Insights Cache Build a dashboard

Configure your Loki data source below

Or skip the effort and get Loki (and Prometheus) as fully-managed, scalable, and hosted data sources from Grafana Labs with the [free-forever Grafana Cloud plan](#).

Name: loki

URL: http://localhost:3100

Default:

Before you can use the Loki data source, you must configure it below or in the config file. For detailed instructions, [view the documentation](#).

Connection

Authentication

Authentication methods

Choose an authentication method to access the data source

Authentication method: No Authentication

Et puis on doit faire la connexion entre les logs et Loki

Edit destination

Enabled	<input checked="" type="checkbox"/>
Transport	UDP(4)
Applications	Nothing selected
	<input type="button" value="Clear All"/> <input checked="" type="button" value="Select All"/>
Levels	Nothing selected
	<input type="button" value="Clear All"/> <input checked="" type="button" value="Select All"/>
Facilities	Nothing selected
	<input type="button" value="Clear All"/> <input checked="" type="button" value="Select All"/>
Hostname	10.100.1.135
Port	1514
rfc5424	<input type="checkbox"/>
Description	Vers Loki Monitoring