

SERVEUR DE LOG

KIWI SYSLOG

SERVEUR

SYSLOG SERVEUR

INSTALLATION ROUTEUR CISCO 2900

On se connecte au routeur avec notre serveur en câble console, on utilise le logiciel Putty qui est un émulateur de terminal. En effet, on se connecte via le port COM. Mise en service d'un lien SSH par la suite.

LE WAN

Le port WAN du routeur est configuré en G0/0 en DHCP.

LE LAN

Le LAN est configuré en G0/1 en 10.0.0.1 255.255.254.0 (/23)

INSTALLATION ROUTEUR CISCO 2900

Configuration du routeur

Enable

Conf t

Int g0/0 / interface WAN

Ip address dhcp

/*Ip address 172.22.101.199 255.255.0.0*/ —> en IP statique.

Ip route 0.0.0.0 0.0.0.0 172.22.100.1

No shutdown

Exit

Int g0/1 / interface LAN

Ip address 10.0.0.1 255.255.254.0

Ip dhcp pool lan

Network 10.0.0.0 255.255.254.0

Default-router 10.0.0.1

Dns-server 8.8.8.8 8.8.4.4

Ip dhcp excluded 10.10.1.1 10.10.1.100

access-list 1 permit 10.10.0.0 0.0.1.255

ip nat inside source list 1 interface **g0/0 (je sors sur l'interface 0/0 inside : lan vers → Wan)**

int g0/0

ip nat outside

int g0/1

ip nat inside

ip route 0.0.0.0 0.0.0.0 192.168.50.1

ip route 10.10.0.0 255.255.254.0 10.0.0.2

Configuration du routeur pour les messages Syslog :

Clock set 14 :23 :00 february 01 2023

Services timestamps

Logging trap 7

Logging facility local7

Logging 10.10.1.100

Ip nat log translations syslog

No ip nat log translations syslog

Show logging

No logging console informational (stop log routeur)

Sauvegarde

Copy running-config startup-config

Ou

Write memory

Voir la configuration

Show run (voir la conf)

INSTALLATION WINDOWS 10 SUR NOTRE SERVEUR

Téléchargement de l'image en .iso de Windows 10. On effectue une clef bootable avec Rufus et on boot sur la clef.

Installation du système d'exploitation.

Configuration d'une adresse IP fixe en 10.10.1.100 255.255.254.0

INSTALLATION KIWI SYSLOG SERVEUR

Téléchargement sur <https://www.solarwinds.com/fr/kiwi-syslog-server>.

Installation du logiciel KiwiSyslog version 9.8.

Le port UDP configurer est en écoute sur le port : 514

Le port TCP:1468

Le port SNMP:162

CONFIGURATION DES SOURCES D'ECOUTES

File —> setup —> input

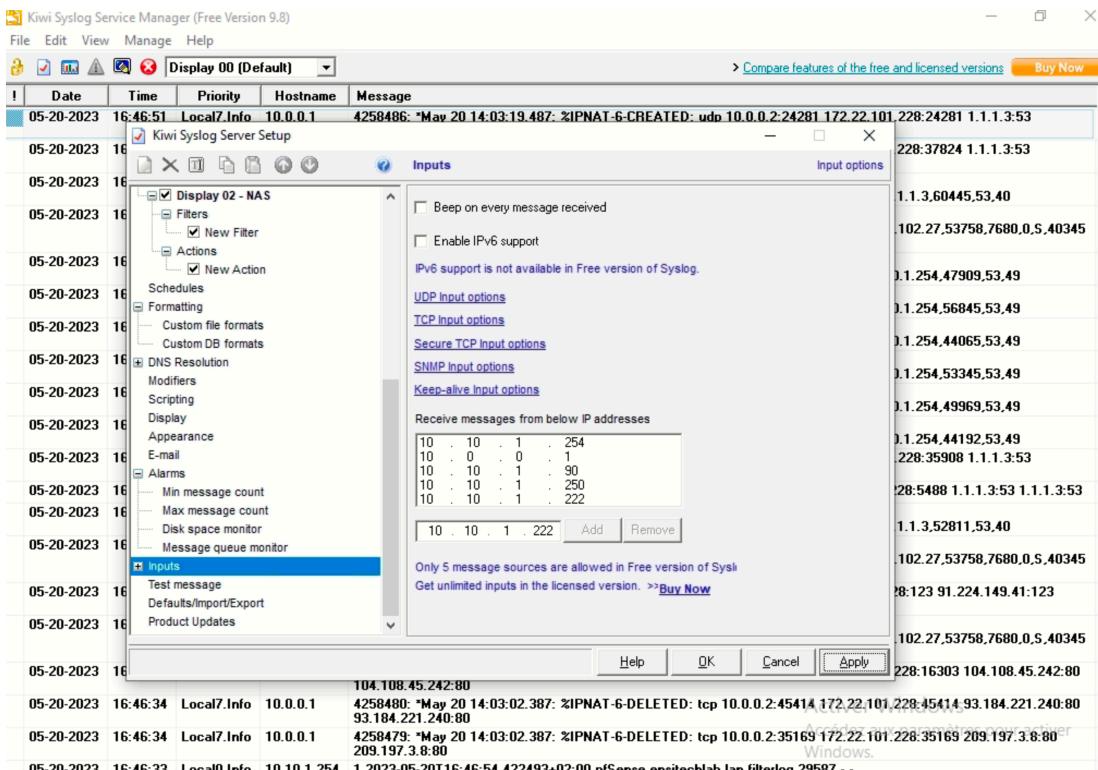
On saisit les adresses IP des machines dont on souhaite récupérer les messages systèmes.

10.0.0.1 : le routeur Cisco 2900

10.10.1.254: le Pfsense

10.10.1.90: Le NAS: Network Attached Storage

10.10.1.22: Cisco 3b1 accès Wifi



CONFIGURATION DU PFSENSE POUR LES MESSAGES SYSLOGS

Remote log servers 10.10.1.100 IP[:port] IP[:port]

Remote Syslog Contents

- Everything
- System Events
- Firewall Events
- DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
- DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
- PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
- General Authentication Events
- Captive Portal Events
- VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
- Gateway Monitor Events
- Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
- Network Time Protocol Events (NTP Daemon, NTP Client)
- Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.

Save

CONFIGURATION DU NAS POUR LES MESSAGES SYSLOGS

Panneau de configuration, centre des journaux, envois des journaux.

The screenshot shows the Synology DSM interface with the URL `10.10.1.90:5000/#signin` in the address bar. On the left, there is a sidebar with navigation links: Vue d'ensemble, Journaux, Notifications, Paramètres d'archive, Envoi des journaux, Reception des journaux, and Historique des réglages. The main content area is titled "Centre des journaux". It has two tabs: "Emplacement" and "Filtres de journal". Under "Emplacement", the "Envoyer des journaux à un serveur syslog" checkbox is checked, and the "Serveur" field contains "10.10.1.100", the "Port" field contains "514", and the "Protocole de transfert" dropdown is set to "UDP". The "Format du journal" dropdown is set to "BSD (RFC 3164)". There are also checkboxes for "Activer la connexion sécurisée (SSL)" and "Importer le certificat", and a button "Envoyer un journal de test". At the bottom right, there are "Réinitialiser" and "Appliquer" buttons, and a status message "5 éléments" with a refresh icon.

IP LAN NAS : 10.10.1.90

Accès à distance : <http://QuickConnect.to/Ensitech>

CONFIGURATION DU ROUTEUR CISCO3B1 POUR LES MESSAGES SYSLOGS

On se connecte au routeur via l'URL puisqu'il ne s'utilise pas en CLI avec son adresse 10.10.1.222. On entre dans sa configuration en tant qu'administrateur et on ajoute un paramètre de journalisation.

The screenshot shows the Cisco RV130W router's web-based management interface. The left sidebar menu is visible, showing various configuration sections like 'Administration' which is currently selected. The main content area is titled 'Paramètres de journal' (Logging parameters). A success message states 'Les paramètres de configuration ont été enregistrés.' (Configuration parameters have been saved). Below this, under 'Configuration des journaux' (Logging configuration), the 'Mode journalisation' (Logging mode) is set to 'Activer' (Enable). Under 'Indiquer la gravité pour le journal local et e-mail' (Specify severity for local log and email), several checkboxes are checked: Urgence, Alerte, Critique, Erreurs, Attention, Notification, and Info. The 'Alerte e-mail' (Email alert) checkbox is also checked. In the 'Table des serveurs de journalisation distants' (Table of remote logging servers), there is one entry for a distant log server at IP address 10.10.1.100. Buttons for 'Ajouter une ligne' (Add line), 'Modif' (Modify), and 'Suppr.' (Delete) are present. At the bottom of the page, there are 'Enreg.' (Save), 'Annuler' (Cancel), and 'Afficher les journaux' (View logs) buttons. A watermark for 'Activer Windows' (Activate Windows) is visible in the bottom right corner.

MISE EN PLACE D'UNE AUTOMATISATION DE SAUVEGARDE DU FICHIER LOG

J'ai utiliser un script bash :

```
«xcopy C:\\"Program Files (x86)"\Syslogd\Logs\ \\NAS-BACKUP\KiwiSyslog /D /E /C /R /H /K /Y»
```

Il copie le fichier source : C:\\"Program Files (x86)"\Syslogd\Logs vers NAS-BACKUP\KiwiSyslog avec des paramètres.

Les paramètres concernés:

/D : Copie tous les fichiers sources qui sont plus récents que les fichiers de destination existants.

/E: Copie les répertoires et sous-répertoires, y compris les vides.

/C: Continue la copie même si des erreurs se produisent.

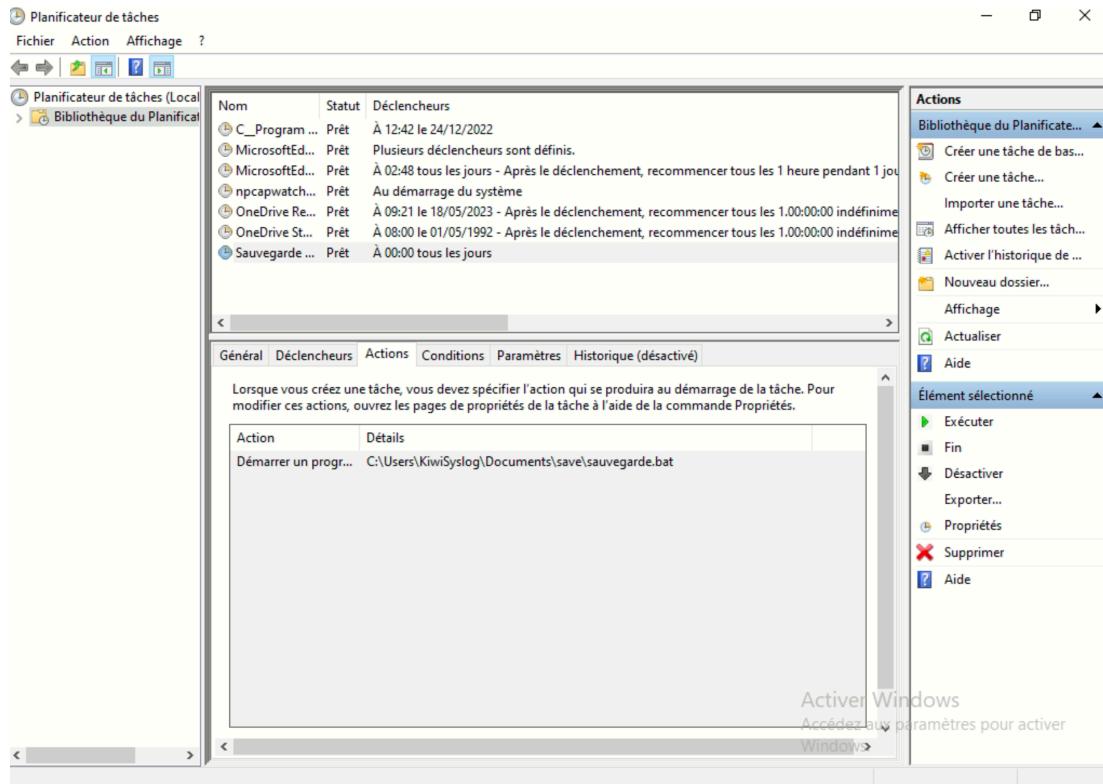
/R: Remplace les fichiers en lecture seule.

/H: Copie les fichiers avec des attributs de fichier système et masqués.

/K: Copie les attributs de fichiers.

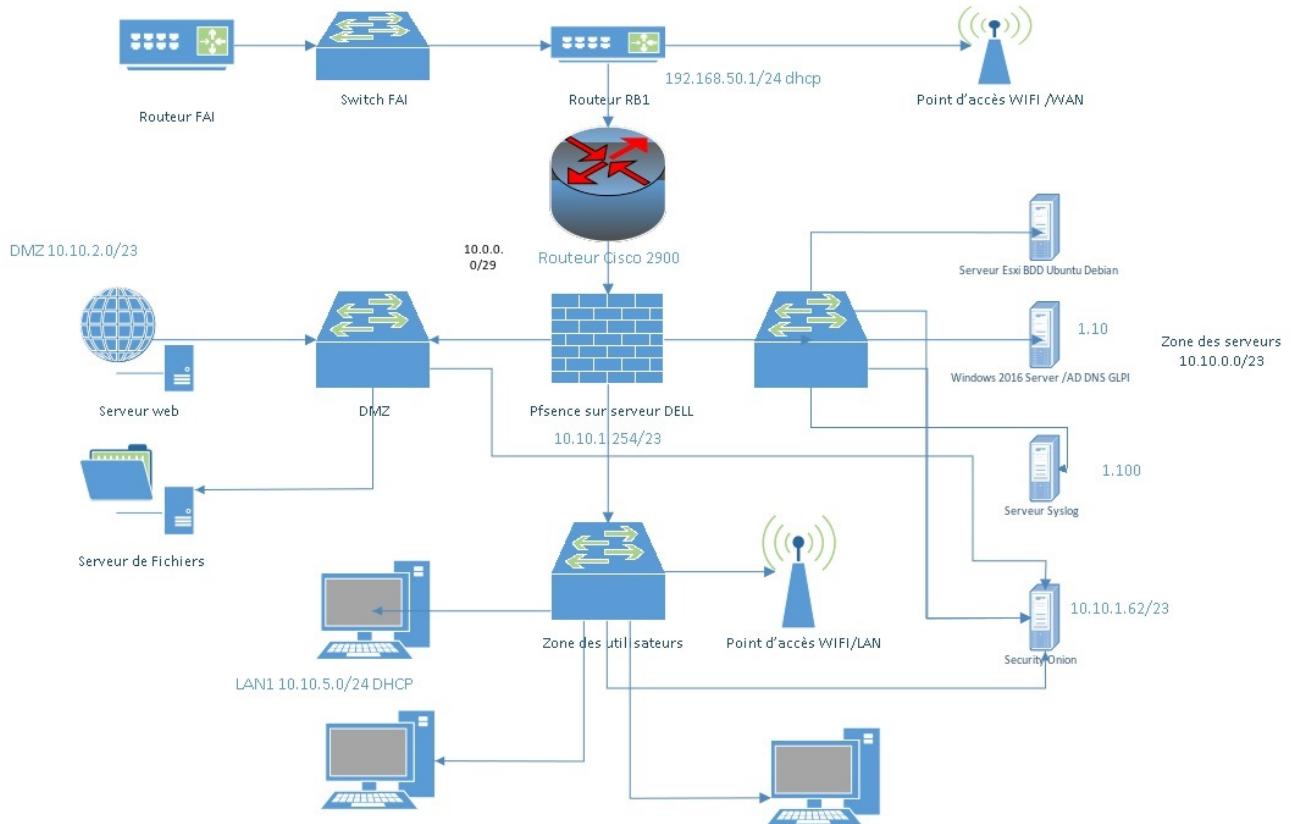
/Y: Supprime l'invite à confirmer que vous souhaitez remplacer un fichier de destination existant.

Dans le planificateur de tâche Windows, on crée une tâche que l'on nomme sauvegardes des journaux. On y ajoute un déclencheur, ici tous les jours à minuit. Puis une action, le fichier script.



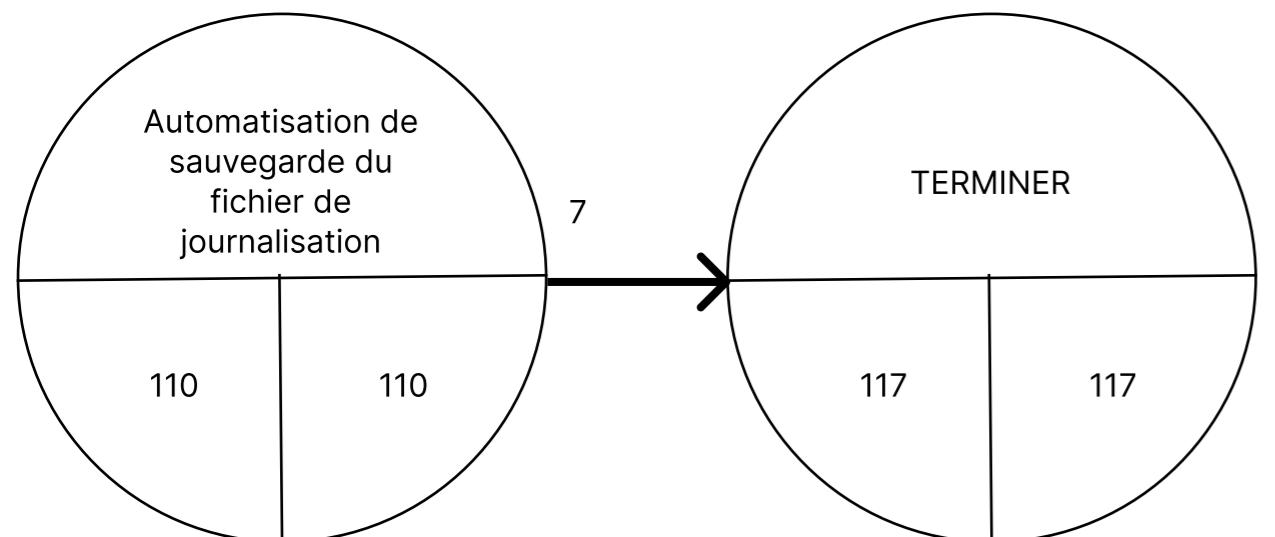
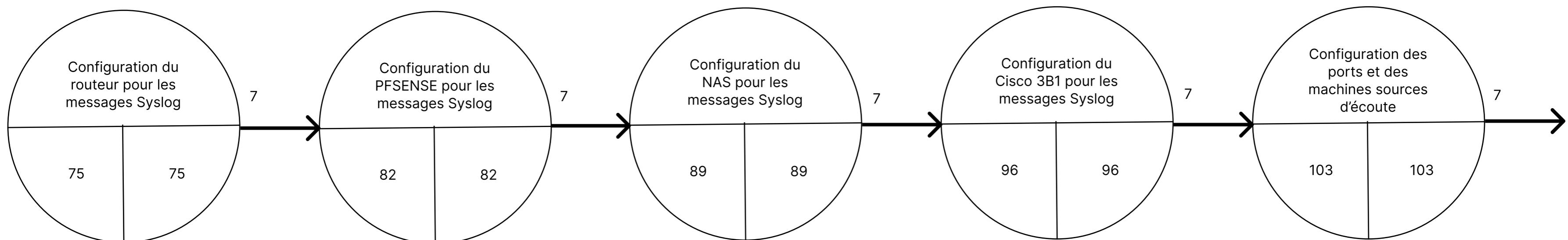
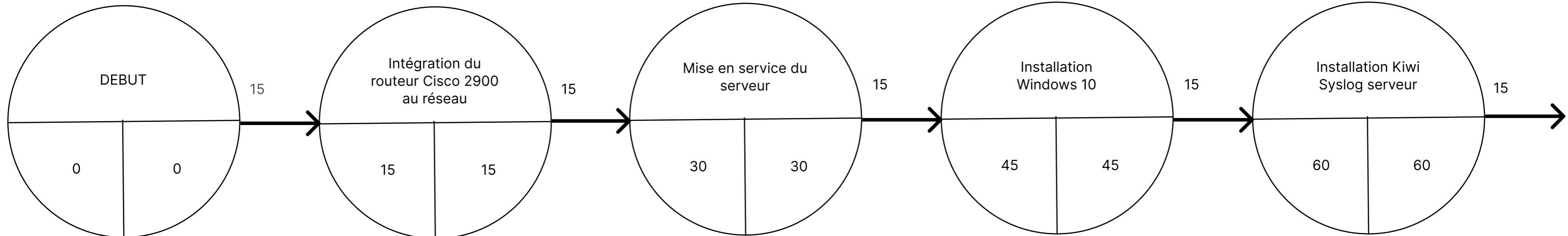
Le serveur Kiwi en service :

Kiwi Syslog Service Manager (Free Version 9.8)					
	Date	Time	Priority	Hostname	Message
05-20-2023	15:27:14	Local7.info	10.0.0.1		4252218: *May 20 12:43:43.239: %IPNAT-6-DELETED: udp 10.0.0.2:17589 172.22.101.228:17589 1.1.1.3:53
05-20-2023	15:27:14	Local7.info	10.0.0.1		4252217: *May 20 12:43:43.239: %IPNAT-6-DELETED: tcp 10.0.0.2:62141 172.22.101.228:62141 20.166.126.56:443
05-20-2023	15:27:14	Local7.info	10.0.0.1		4252216: *May 20 12:43:42.727: %IPNAT-6-DELETED: udp 10.0.0.2:61183 172.22.101.228:61183 1.1.1.3:53
05-20-2023	15:27:14	Local7.info	10.0.0.1		4252215: *May 20 12:43:42.727: %IPNAT-6-DELETED: tcp 10.0.0.2:59511 172.22.101.228:59511 87.248.222.128:80
05-20-2023	15:27:14	Local7.info	10.0.0.1		4252214: *May 20 12:43:42.727: %IPNAT-6-DELETED: tcp 10.0.0.2:5198 172.22.101.228:5198 95.140.239.0:80
05-20-2023	15:27:14	Local0.info	10.10.1.254		05-20-2023-05-20T15:27:34.612514+02:00 pfSense.ensitechlab.lan filterlog 29587 -- 4..10000000103.em1.match.block.in 4.0x0..64.11650.0.DF.17 udp.229.10.10.1.90.10.10.1.255.138.138.209
05-20-2023	15:27:14	Local0.info	10.10.1.254		05-20-2023-05-20T15:27:34.612532+02:00 pfSense.ensitechlab.lan filterlog 29587 -- 105...1682002193.em1.match.pass.in.4.0x0..64.52333.0.none.17.udp.60.10.10.1.250.1.1.1.3.51277.53.40
05-20-2023	15:27:13	Local7.info	10.0.0.1		4252213: *May 20 12:43:42.147: %IPNAT-6-CREATED: udp 10.0.0.2:42434 172.22.101.228:42434 1.1.1.3:53
05-20-2023	15:27:13	Local7.info	10.0.0.1		4252212: *May 20 12:43:41.703: %IPNAT-6-DELETED: udp 10.0.0.2:43249 172.22.101.228:43249 1.1.1.3:53
05-20-2023	15:27:13	Local7.info	10.0.0.1		4252211: *May 20 12:43:41.191: %IPNAT-6-DELETED: udp 10.0.0.2:41395 172.22.101.228:41395 1.1.1.3:53
05-20-2023	15:27:13	Local7.info	10.0.0.1		4252210: *May 20 12:43:41.191: %IPNAT-6-DELETED: tcp 10.0.0.2:9473 172.22.101.228:9473 95.140.239.0:80
05-20-2023	15:27:13	Local7.info	10.0.0.1		4252209: *May 20 12:43:41.191: %IPNAT-6-DELETED: tcp 10.0.0.2:39817 172.22.101.228:39817 87.248.222.128:80
05-20-2023	15:27:12	Local7.info	10.0.0.1		4252208: *May 20 12:43:40.167: %IPNAT-6-DELETED: tcp 10.0.0.2:15273 172.22.101.228:15273 95.140.239.0:80
05-20-2023	15:27:12	Local7.info	10.0.0.1		4252207: *May 20 12:43:40.167: %IPNAT-6-DELETED: tcp 10.0.0.2:30548 172.22.101.228:30548 87.248.222.128:80
05-20-2023	15:27:10	Local7.info	10.0.0.1		4252206: *May 20 12:43:39.143: %IPNAT-6-DELETED: tcp 10.0.0.2:28048 172.22.101.228:28048 95.140.239.0:80
05-20-2023	15:27:10	Local7.info	10.0.0.1		4252205: *May 20 12:43:39.143: %IPNAT-6-DELETED: tcp 10.0.0.2:28028 172.22.101.228:28028 87.248.222.128:80
05-20-2023	15:27:10	Local7.info	10.0.0.1		4252204: *May 20 12:43:38.631: %IPNAT-6-DELETED: udp 10.0.0.2:3190 172.22.101.228:3190 1.1.1.3:53 1.1.1.3:53
05-20-2023	15:27:10	Local7.info	10.0.0.1		4252203: *May 20 12:43:38.631: %IPNAT-6-DELETED: udp 10.0.0.2:55902 172.22.101.228:55902 1.1.1.3:53
05-20-2023	15:27:10	Local7.info	10.0.0.1		4252202: *May 20 12:43:38.631: %IPNAT-6-DELETED: udp 10.0.0.2:36758 172.22.101.228:36758 1.1.1.3:53
05-20-2023	15:27:10	Local7.info	10.0.0.1		4252201: *May 20 12:43:38.631: %IPNAT-6-DELETED: udp 10.0.0.2:61737 172.22.101.228:61737 1.1.1.3:53
05-20-2023	15:27:09	Local7.info	10.0.0.1		4252200: *May 20 12:43:38.631: %IPNAT-6-DELETED: udp 10.0.0.2:17500 172.22.101.228:17500 1.1.1.3:53



Vous retrouverez ce projets menée en autonomie ci-dessous :

<https://astro-portfolio-serres-nicolas.vercel.app/projet>



SERVEUR KIWI SYSLOG

Installation et prise en main