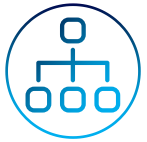
GS21 Cyber-enquête en entreprise

Mise en place d'un système de surveillance

A. NICOLAS, A. PINON - A20

PLAN



Partie I - Architecture du SI

> *L'Architecture idéale*

> *L'infrastructure simplifié pour la simulation*

Partie II – Mise en œuvre

> *Serveur **Syslog-NG***

> *SIEM **Splunk®***

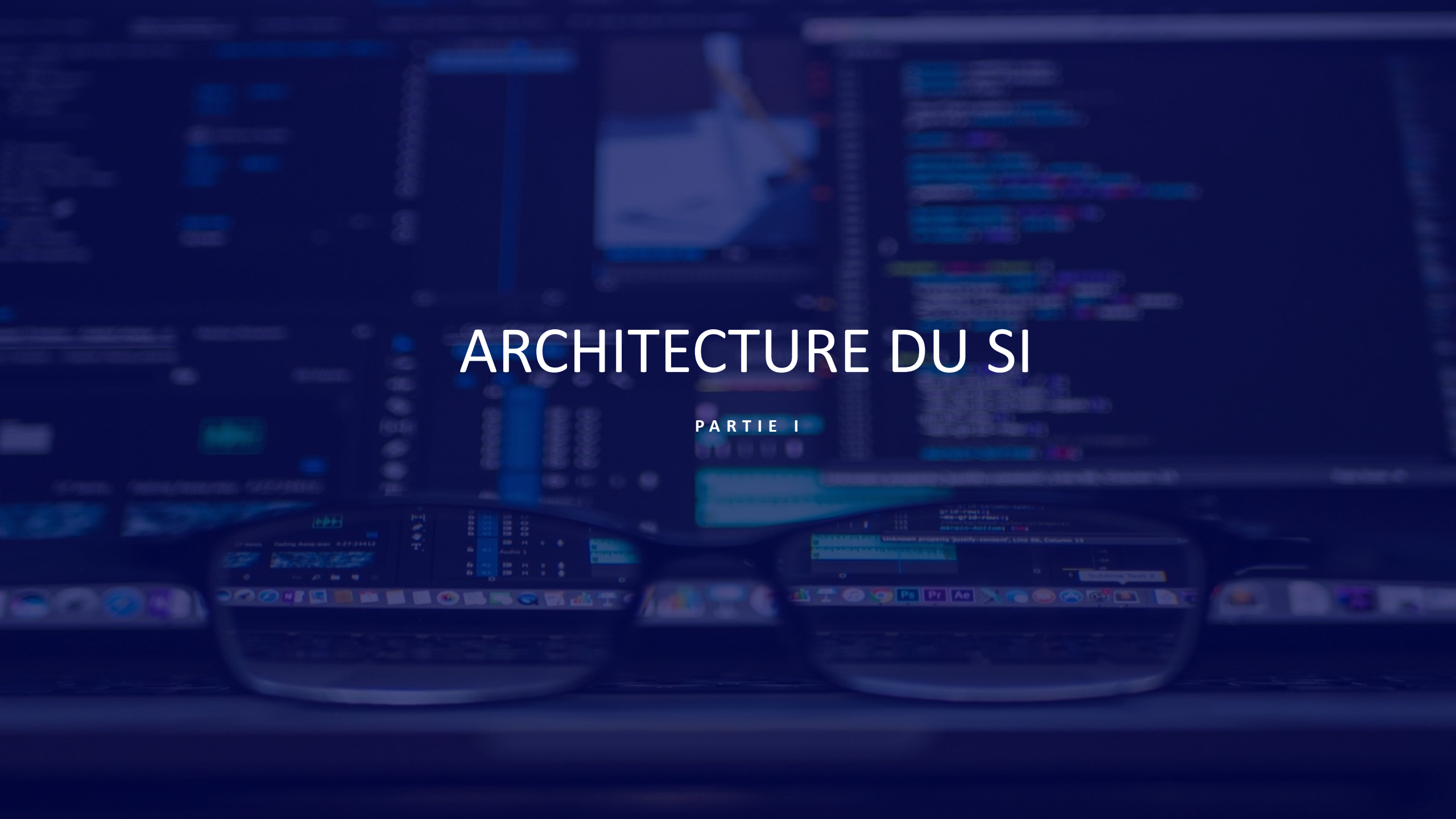
> *Journalisation **Linux***

> *Journalisation **Windows***

> *Journalisation sur le **Pare-feu***

> *Journalisation sur le **Commutateur***

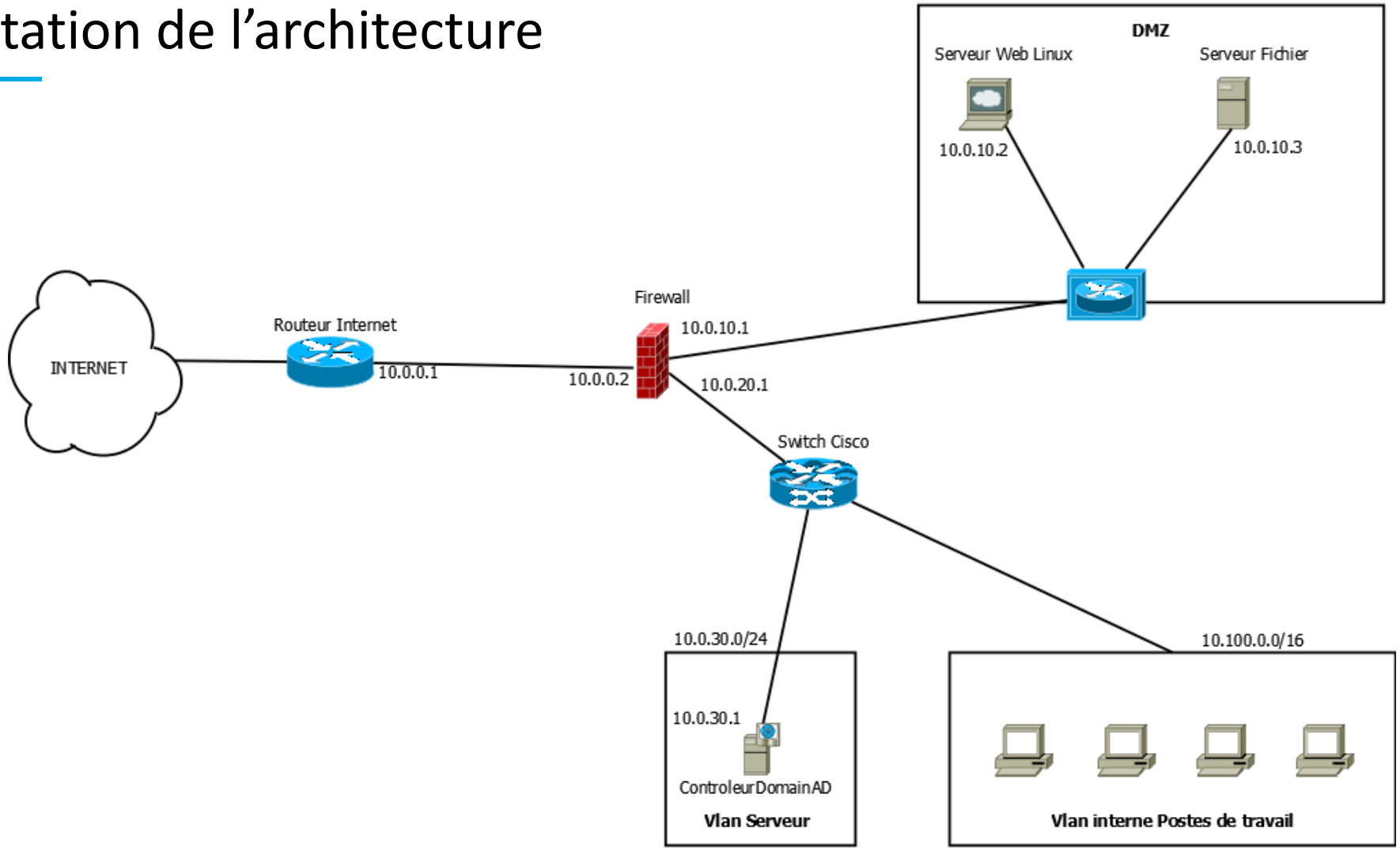
Partie III – Cas pratique



ARCHITECTURE DU SI

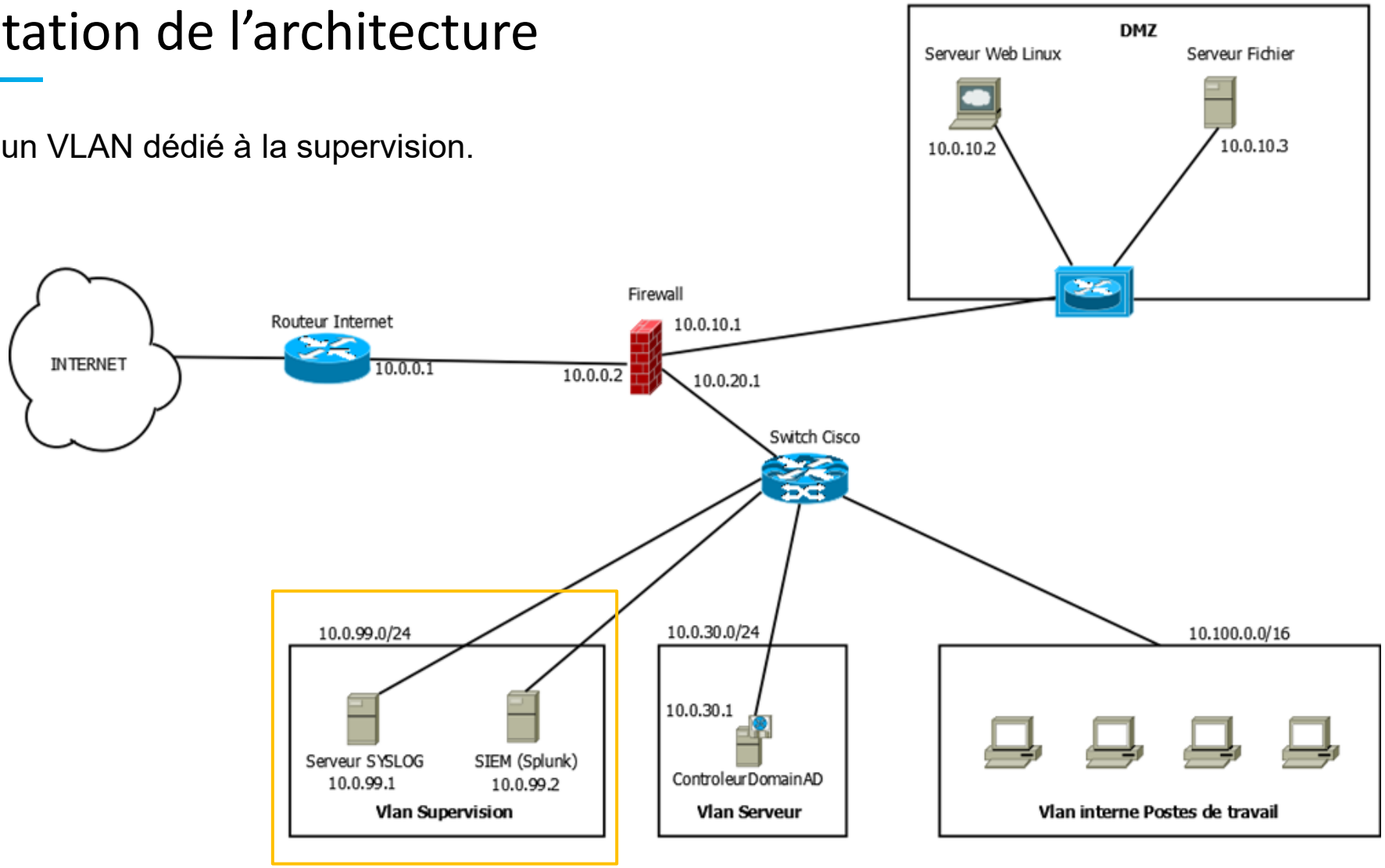
PARTIE I

Présentation de l'architecture



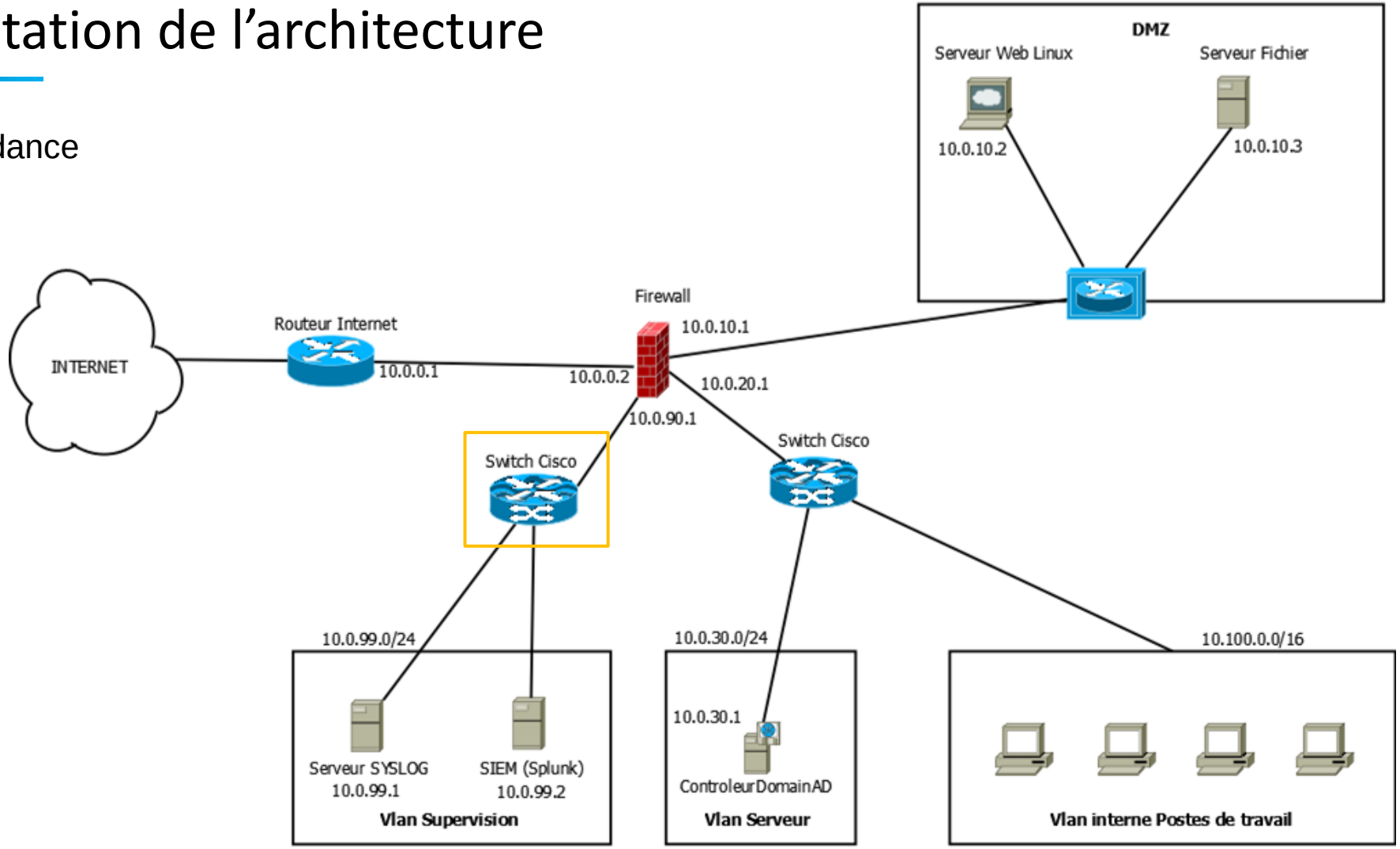
Présentation de l'architecture

- Ajout d'un VLAN dédié à la supervision.



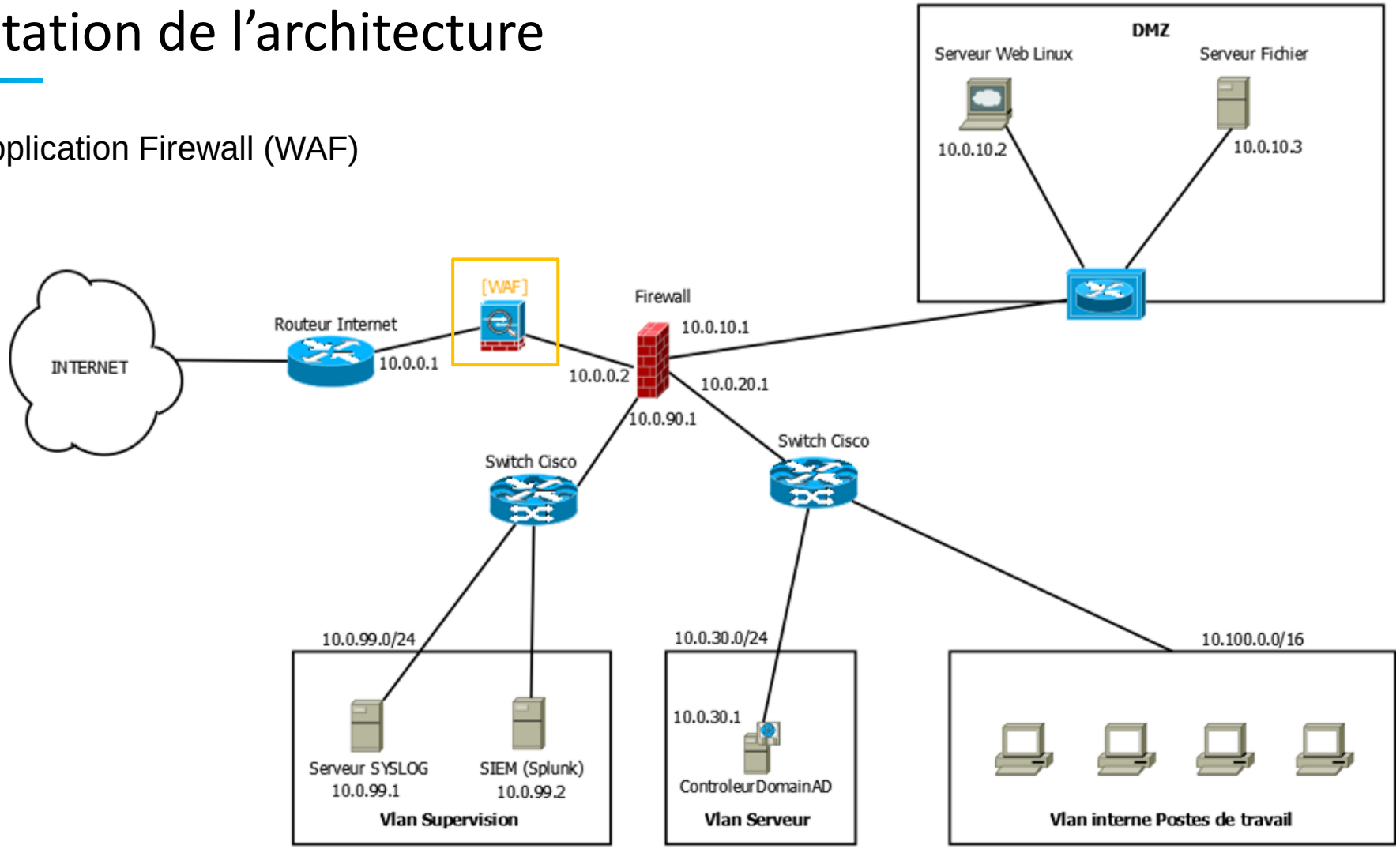
Présentation de l'architecture

- Redondance



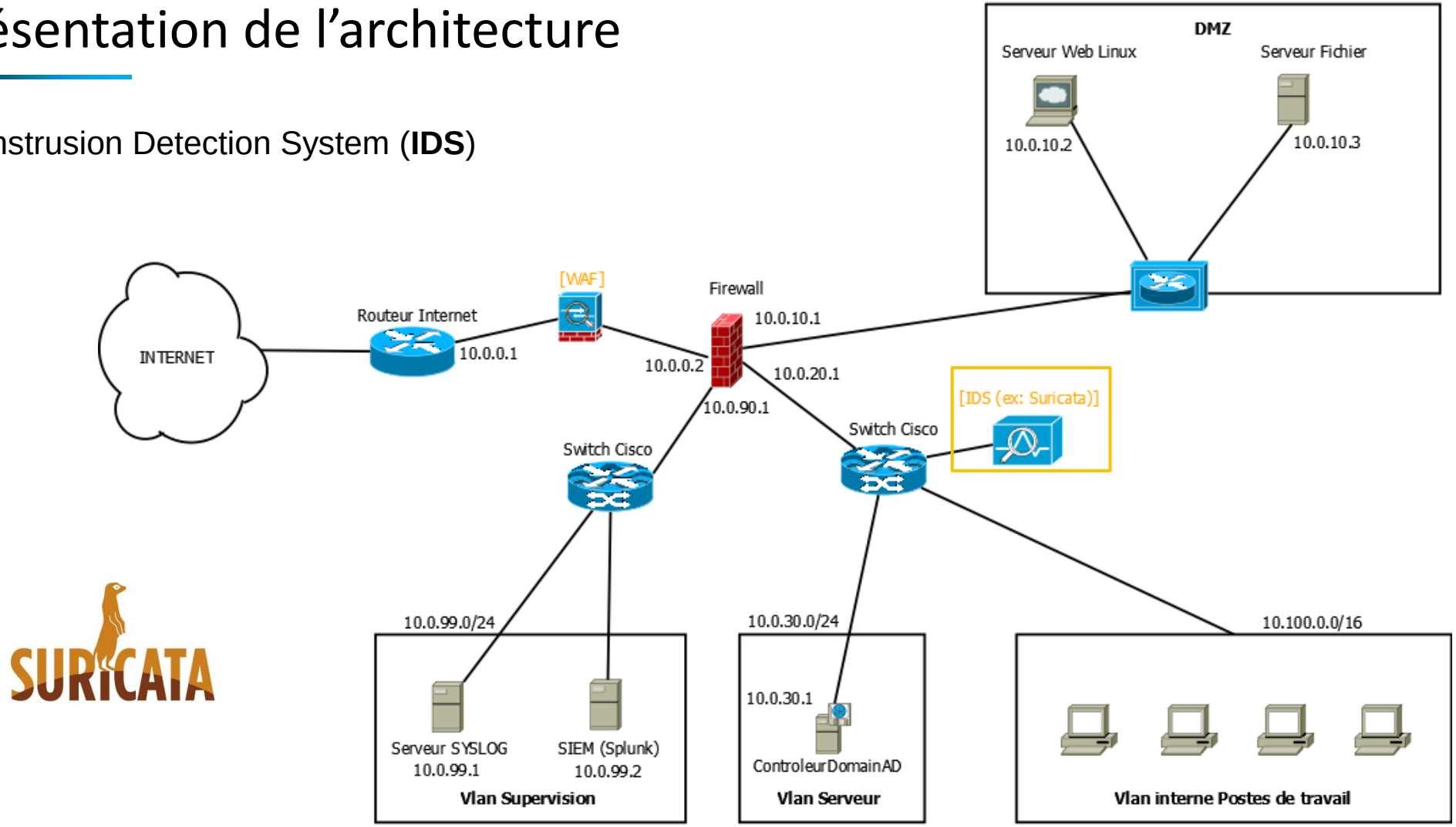
Présentation de l'architecture

- Web Application Firewall (WAF)



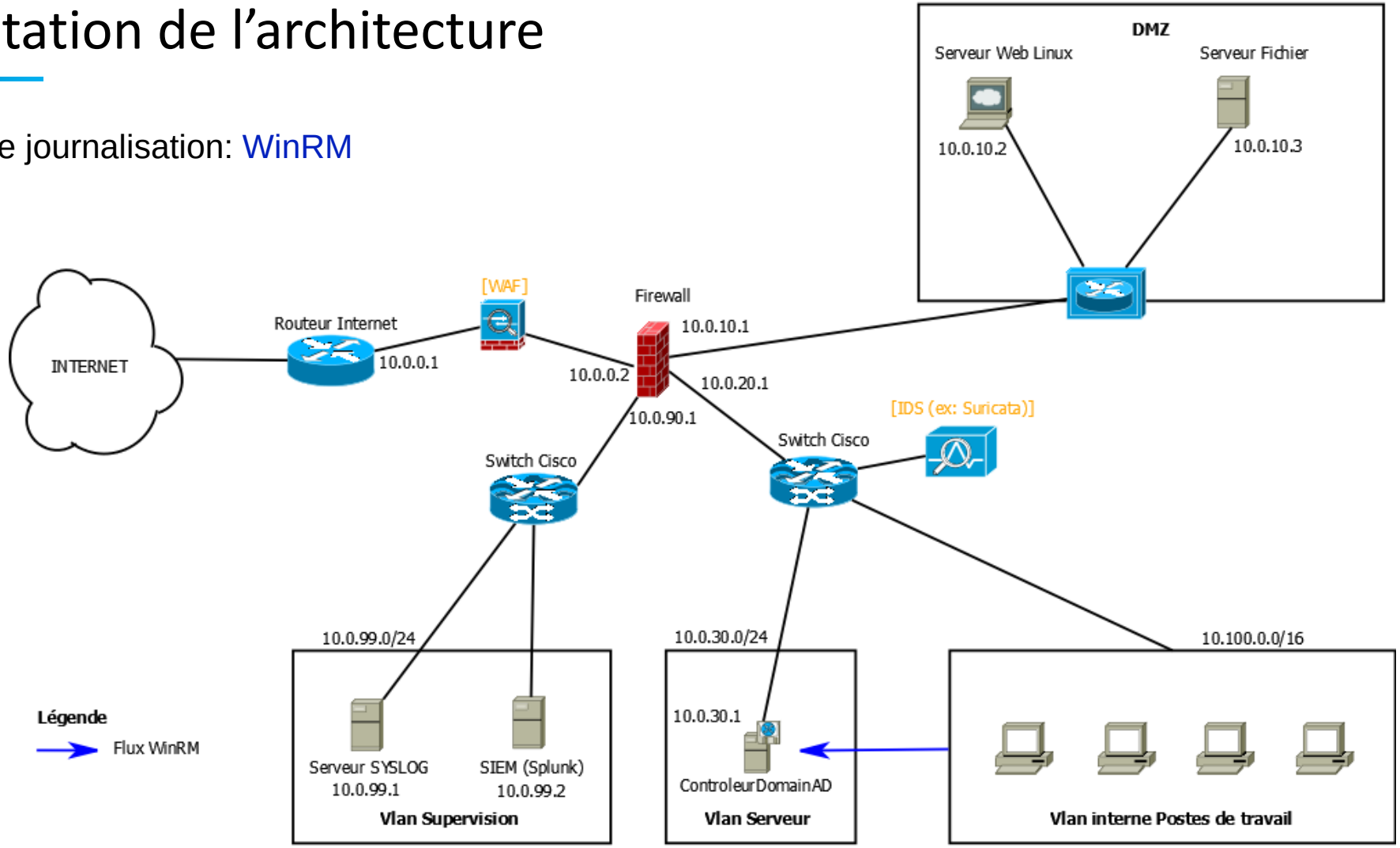
Présentation de l'architecture

- Instrusion Detection System (**IDS**)



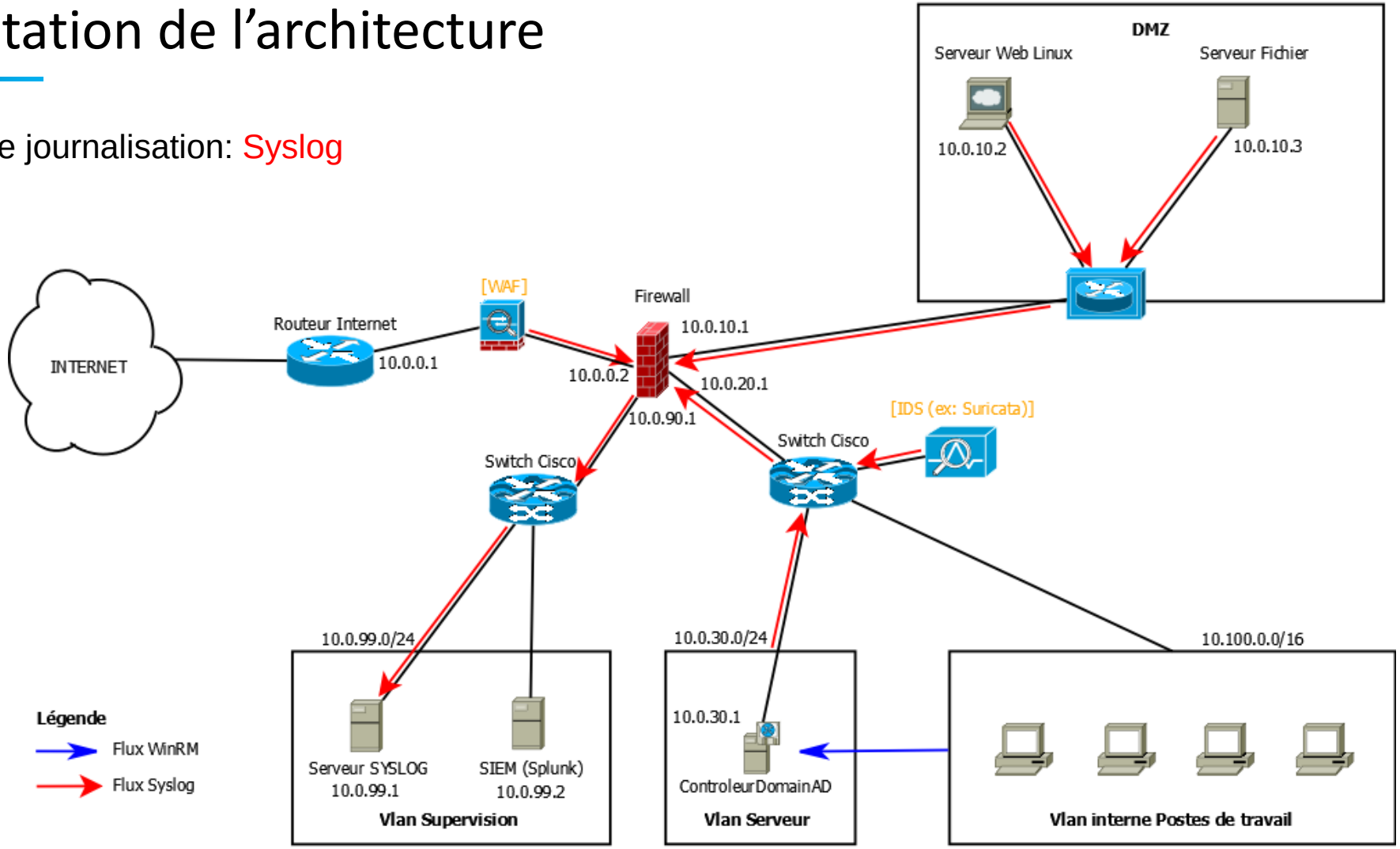
Présentation de l'architecture

- 3 flux de journalisation: WinRM



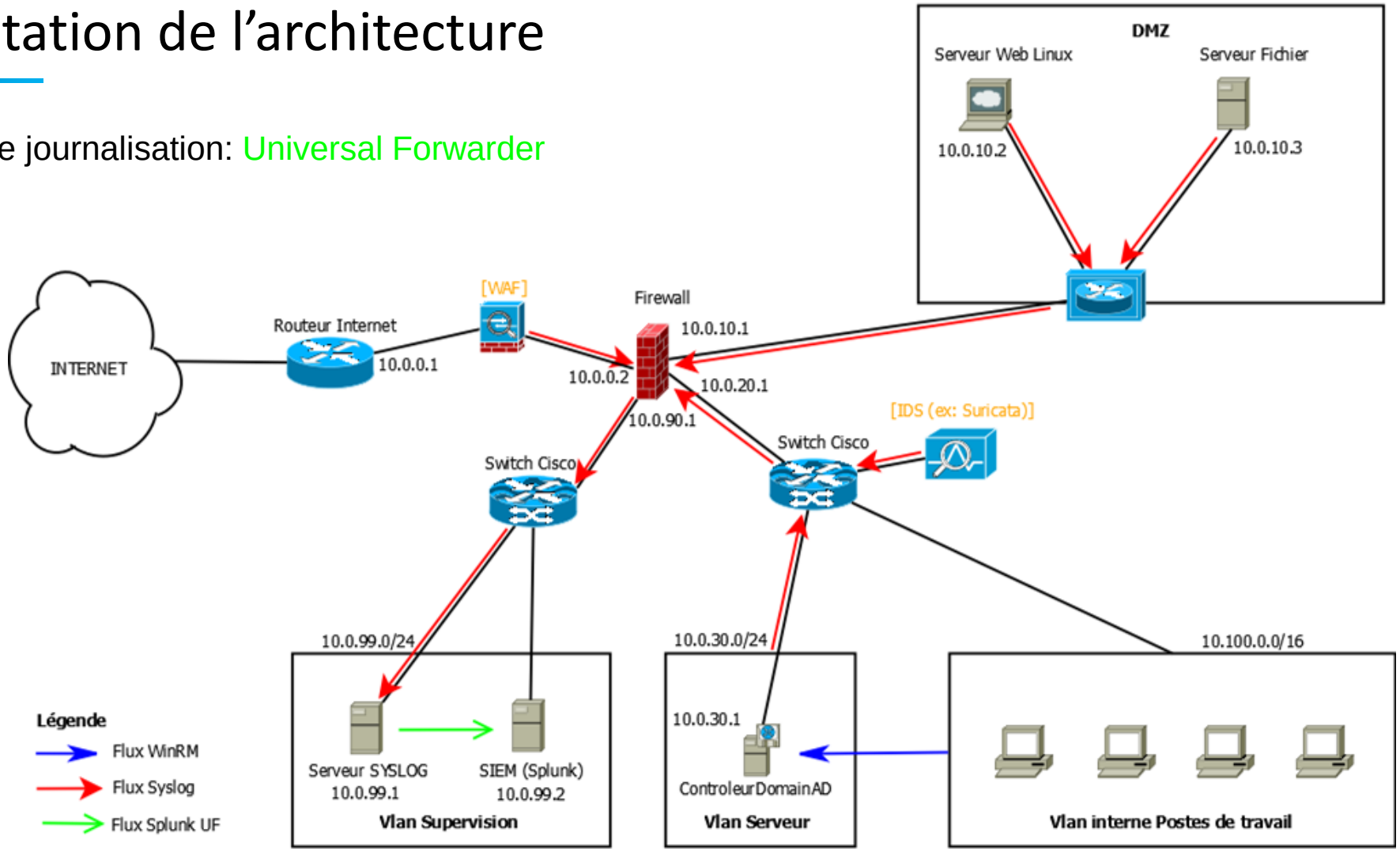
Présentation de l'architecture

- 3 flux de journalisation: Syslog

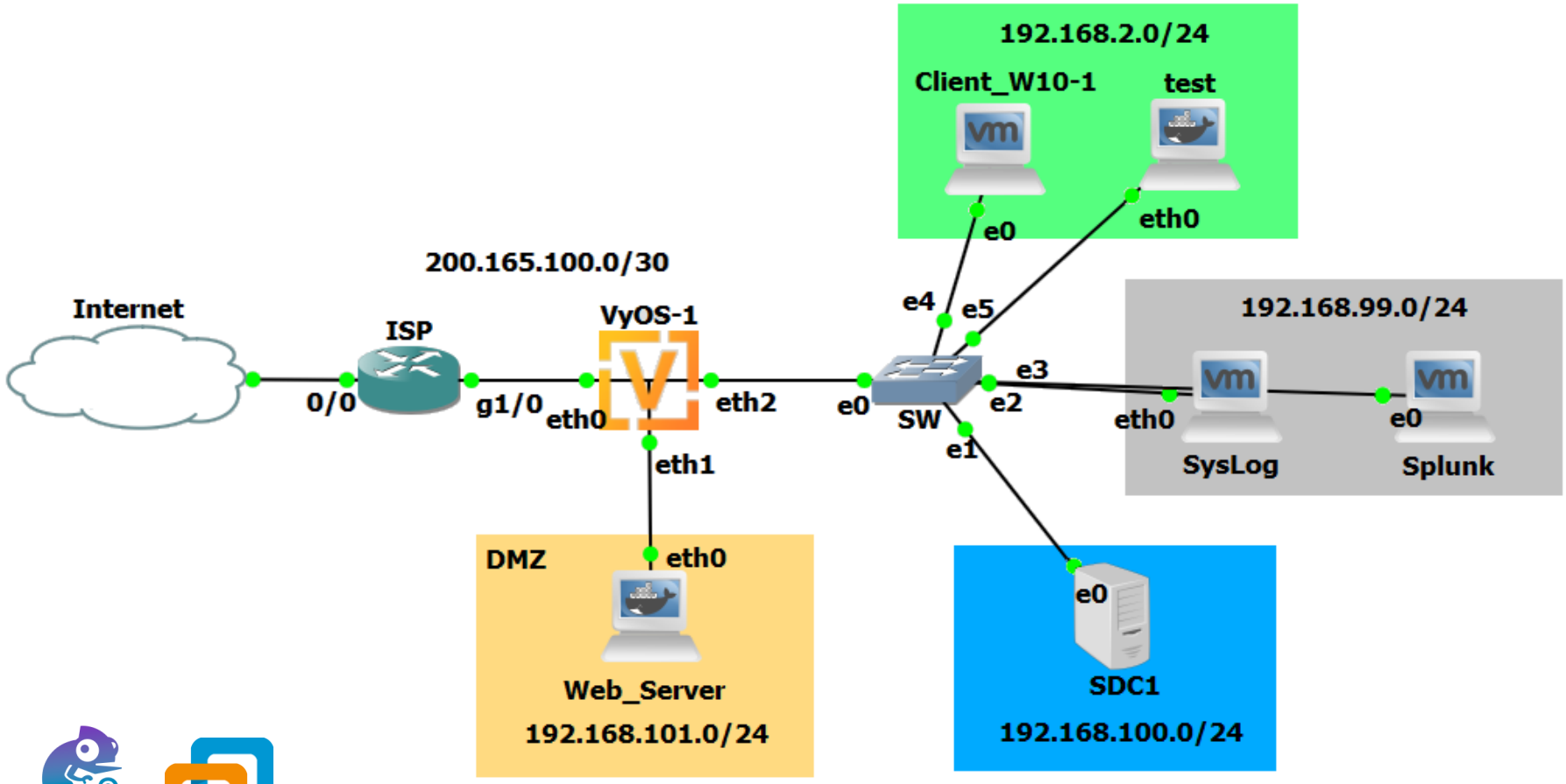


Présentation de l'architecture

- 3 flux de journalisation: Universal Forwarder



Architecture simplifiée



MISE EN OEUVRE

PARTIE II

Mise en œuvre

Serveur Syslog-NG

2 instances de centralisation des logs: Serveur Syslog-NG et SIEM

- 4 grand concepts de configuration

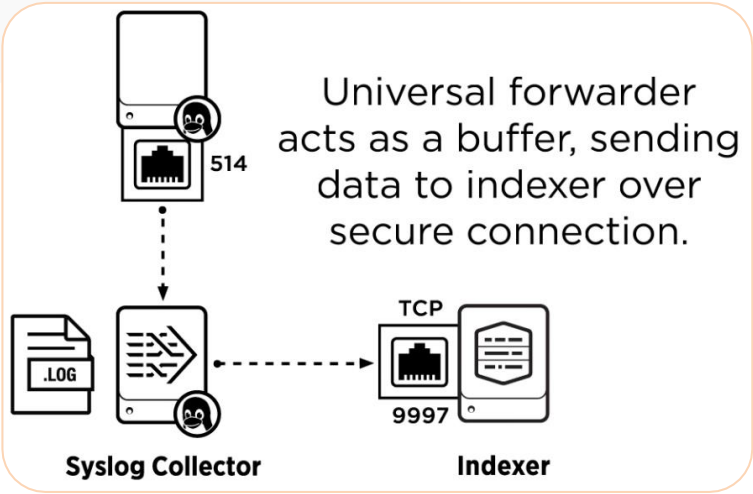
```
# SOURCE
source s_syslog {
  default-network-drivers();
};
```

```
# DESTINATION
destination d_SW_cisco { file("/var/log/syslog/SW/$HOST/$DAY-cisco-catalyst.log"); };
…
destination d_all { file ("/var/log/syslog/ALL/$HOST/$DAY-catch_all.log"); };
```

```
# FILTRE
filter f_SW_cisco { match("%CATALYST" value("PROGRAM")) or match("%CATALYST" value("MESSAGE")); };
…
filter f_all { not (filter(f_SW_cisco) or filter(f_FW_VYoS) ); };
```

```
# INSTRUCTION D'ENVOIE
log { source(s_network); filter(f_SW_cisco ); destination(d_SW_cisco ); };
…
log { source(s_network); filter(f_all); destination(d_all); };
```

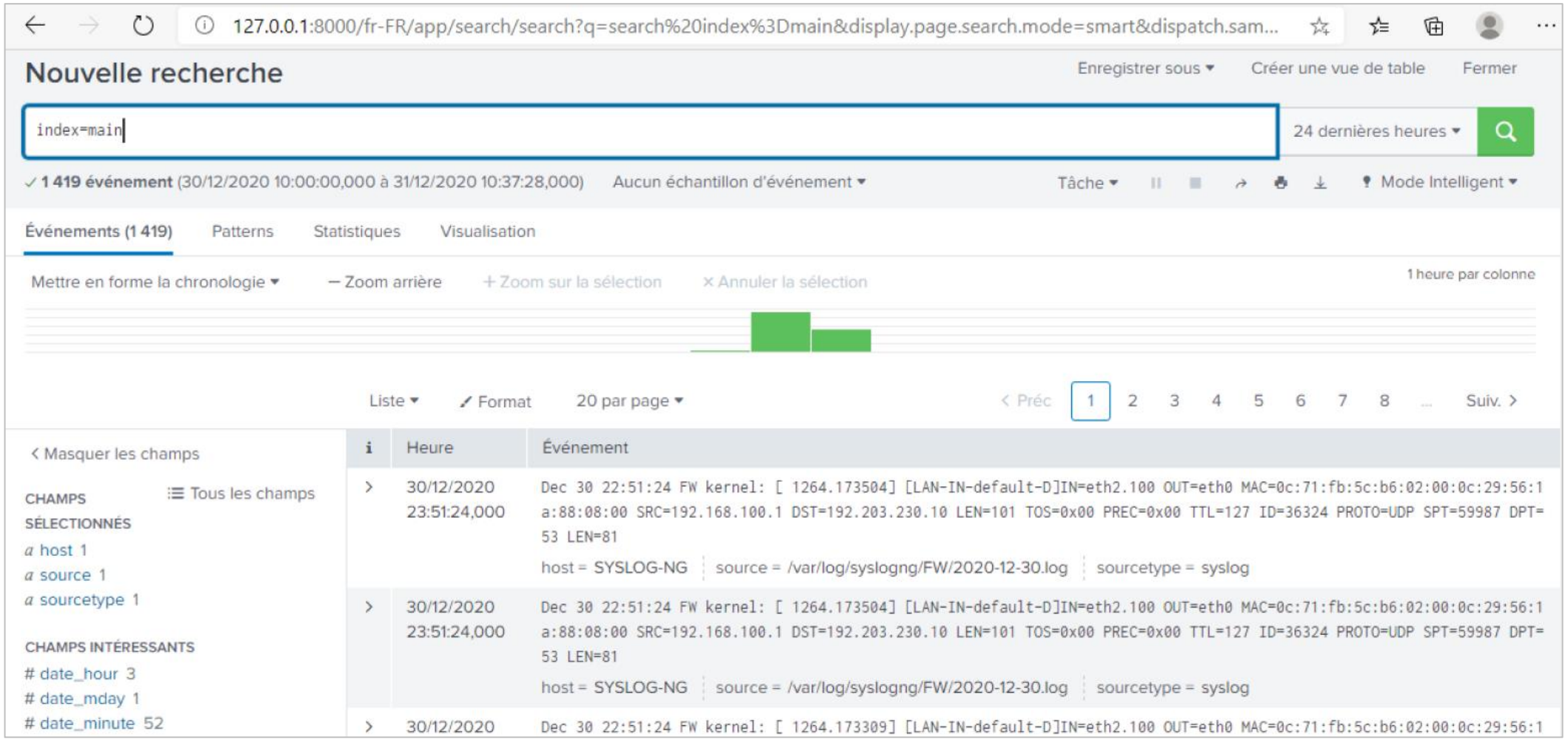
- Vers Splunk : Universal Forwarder (UF), *inputs.conf* & *outputs.conf*



Mise en œuvre

SIEM Splunk®

- Installation sous Windows
- Configuration d'une réception sur le port 9997



Mise en œuvre

Journalisation Linux

- Durcissement de la configuration *Apache*, journalisation des accès, etc.
- Installation et configuration de *Auditd*

  Note technique - Recommandations de configuration d'un système GNU/Linux (ANSSI, 2016).

```
# Execution de insmod, rmmod et modprob
#   -w audit du contenu du répertoire
#   -p x : accès en exécution
-w /sbin/insmod -p x
-w /sbin/modprob -p x
-w /sbin/rmmod -p x

# Journaliser les modifications dans /etc/
#   -p wa : accès en écriture et changement
-w /etc/ -p wa

# Journaliser le montage et démontage
#   -a : ajout d'une règle sur les appels systèmes
#   -S : appel système à surveiller
-a exit,always -S mount -S unmount
```

Extrait du fichier *auditd.rules*

- Installation et configuration de *Syslog-ng*

```
source s_apache_log_files {
    wildcard-file(
        base-dir("/var/log/apache2")
        filename-patter("*.log")
        recursive(yes)
        follow-freq(1)
    );
};
```

Linux Pratique, HS n°49

```
destination d_central_log_server {
    tcp(
        "192.168.99.1"
        port(6514)
        tls(
            ca_dir("/etc/syslog-ng/ca.d")
        )
        disk-buffer(
            mem-buf-length  (10000)
            disk-buf-size(2000000)
            reliable(no)
            dir("/tmp/disk-buffer")
        )
    );
};
```

Mise en œuvre

Journalisation Windows

- Activation et autorisation de *Windows Remote Management (**WinRM**)* sur les postes.
- Création d'un Abonnement dans l'observateur d'événements du serveur de collecte.
- Déploiement d'un outil *sysinternal* à l'aide d'une script: **Sysmon**

```
@ECHO OFF
if not exist "C:\windows\config.xml" (
copy /z /y "\\ SRVDC1\PARTAGES\config.xml" "C:\windows\"
)
if not exist "C:\windows\Sysmon64.exe" (
copy /z /y "\\ SRVDC1\PARTAGES\Sysmon64.exe" "C:\windows\"
)

sc query "Sysmon64" | Find "RUNNING"
If "%ERRORLEVEL%" EQU "1" (
goto startsysmon
)
:startsysmon
net start Sysmon64

If "%ERRORLEVEL%" EQU "1" (
goto installsysmon
)
:installsysmon
"C:\windows\Sysmon64.exe" /accepteula -i c:\windows\config.xml
```

Limite de la GPO: ne se lance qu'au démarrage, quid des équipements qui ne redémarrent pas ?

Mise en œuvre

Journalisation Pare-feu

Logs des règles par défaut des flux de gestion (SSH, WinRM, MMC, TerminalServer).

- Etablissement d'une matrice des flux pour configurer le pare-feu.
- Configuration de Rsyslog

```
auth.*;kern.notice;auth.*;kern.notice    @@192.168.99.1
```

Zone	Equipement Dest	IP Dest	Equipement Source	IP Source	Flux	Port Dest	Action	Firewall Name
VLAN 100	SRVDC1	192.168.101.1	LAN	192.168.2.0/24 192.168.99.0/24 192.168.100.0/24	DNS	TCP_UDP 53	ACCEPT	LAN-OUT
	SRVDC1	192.168.101.1	GUESTS	192.168.5.0/24	DHCP/BOOTP	UDP 67 UDP 68	ACCEPT	LAN-OUT
	SRVDC1	192.168.101.1	LAN	192.168.2.0/24 192.168.99.0/24 192.168.100.0/24	DHCP/BOOTP	UDP 67 UDP 68	ACCEPT	LAN-OUT
	SRVDC1	192.168.101.1	LAN	192.168.2.0/24 192.168.99.0/24 192.168.100.0/24	AD	TCP 88, 135, 139, 389, 445, 464, 636, 3268, 3269, 49152-65535 UDP 88, 123, 137, 138, 389, 636	ACCEPT	LAN-OUT
	SRVDC1	192.168.101.1	MGMT	192.168.99.0/24	MMC	TCP 135,444,5985	ACCEPT	LAN-OUT
	SRVDC1	192.168.101.1	MGMT	192.168.99.0/24	Terminal Server	TCP 3389	ACCEPT	LAN-OUT
	SRVDC1	192.168.101.1	*	0.0.0.0	*	*	DROP	LAN-OUT
VLAN 2	Utilisateurs	192.168.2.0/24	LAN	192.168.2.0/24 192.168.99.0/24 192.168.100.0/24	ICMP	-	ACCEPT	LAN-OUT
	Utilisateurs	192.168.2.0/24	MGMT	192.168.99.1 192.168.99.2	Terminal Server	TCP 3398	ACCEPT	LAN-OUT
	Utilisateurs	192.168.2.0/24	SRVDC1	192.168.101.1	WinRM, RPC	TCP 5985, 5986 TCP 445	ACCEPT	LAN-OUT
	Utilisateurs	192.168.2.0/24	*	0.0.0.0	*	*	DROP	LAN-OUT
INTERNET	INTERNET	0.0.0.0	LAN	192.168.2.0/24 192.168.99.0/24 192.168.100.0/24	HTTP/HTTPS	TCP 80 TCP 443	ACCEPT	LAN-IN

Mise en œuvre

Journalisation Commutateur

- Éléments de configuration de base

```
service timestamps
logging host 192.168.99.1 transport udp port 514
logging facility local5
logging trap debugging
logging userinfo
logging count
```

- Journalisation des changements dans la configuration

```
archive
 log config
  logging enable
  logging size 200
  notify syslog
  hidekeys
```

- Un Switch contient beaucoup d'éléments intéressants:
  - Accès sur le switch ;
  - Interfaces actives, changement d'état ;
  - Alerte des règles de sécurité (802.1X, port-security, dhcp-snooping, …) ;

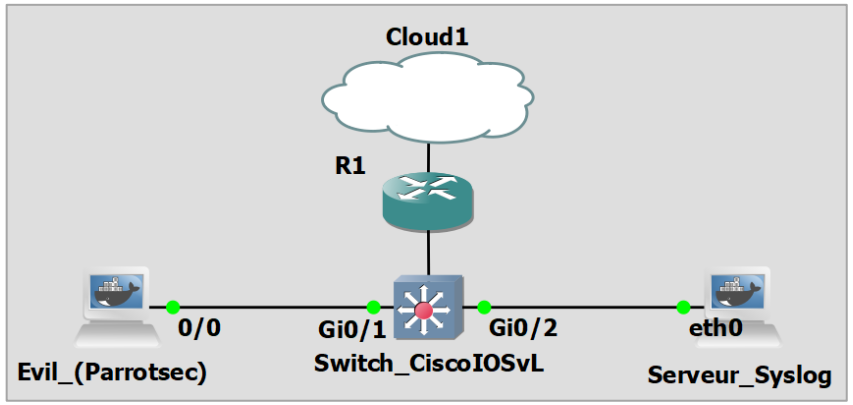
SCÉNARIO DE CORRÉLATION

PARTIE III

Scénario de corrélation

Attaque par force brute sur SSH

```
Hydra –l cisco –P /usr/share/wordlists/rockyou.txt
–t 2 ssh://192.168.99.253
```




```
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or
 for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-11-30 22:06:31
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous s
ession found, to prevent overwriting, ./hydra.restore
[DATA] max 6 tasks per 1 server, overall 6 tasks, 1009 login tries (l:1/p:1009), ~169 tries per task
```

```
%SSH-5-SSH2_CLOSE: SSH2 Session from 192.168.1.101 (tty = 0) for user 'root' using crypto cipher 'aes256-ctr', hmac 'hmac-sha1' closed
/var/log/cisco.log  sourcetype = cisco-too_small

%SSH-5-SSH2_USERAUTH: User 'root' authentication for SSH2 Session from 192.168.1.101 (tty = 0) using crypto cipher 'aes256-ctr', hmac 'hmac

/var/log/cisco.log  sourcetype = cisco-too_small

%SSH-5-SSH2_SESSION: SSH2 Session request from 192.168.1.101 (tty = 0) using crypto cipher 'aes256-ctr', hmac 'hmac-sha1' Succeeded
/var/log/cisco.log  sourcetype = cisco-too_small

%SSH-5-SSH2_CLOSE: SSH2 Session from 192.168.1.101 (tty = 0) for user 'admin' using crypto cipher 'aes256-ctr', hmac 'hmac-sha1' closed
/var/log/cisco.log  sourcetype = cisco-too_small
```

Merci de votre attention