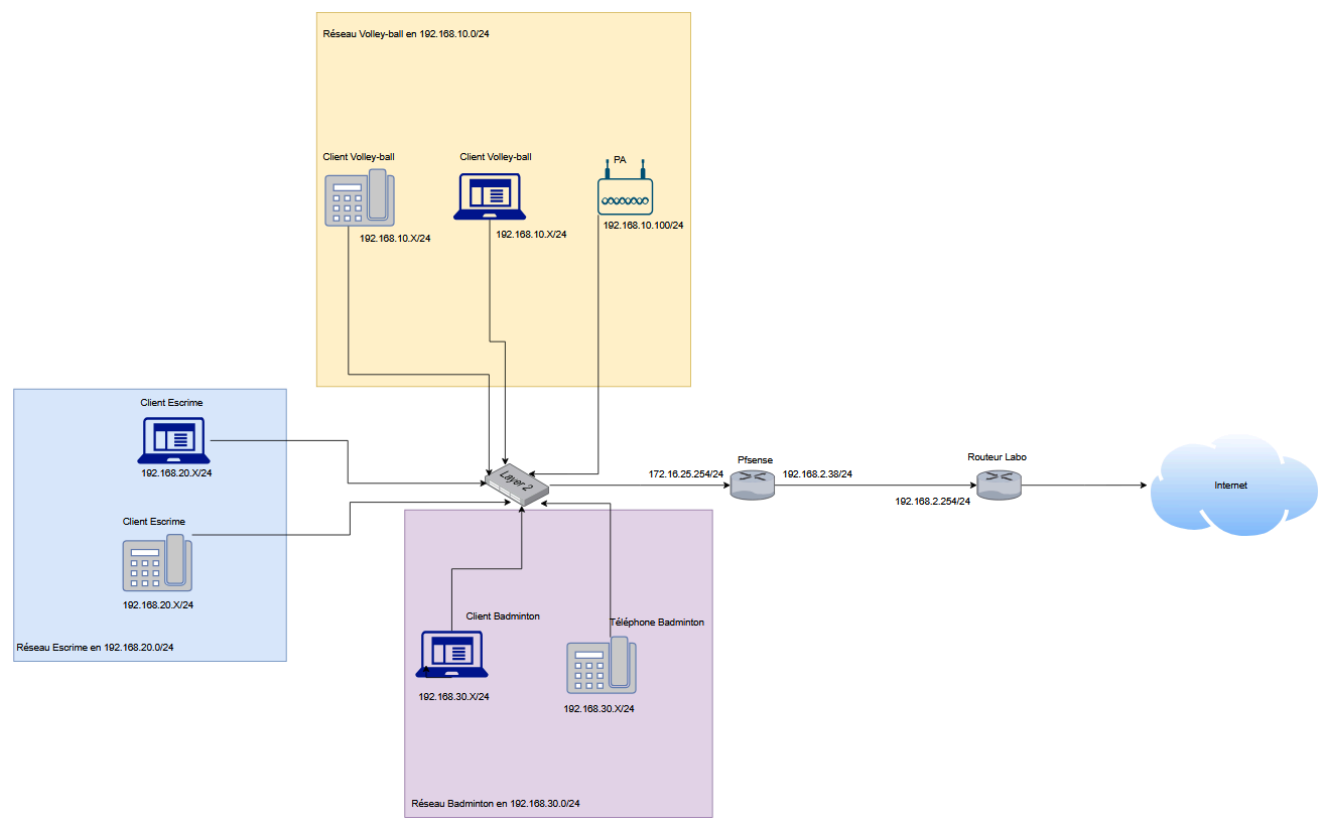


Secure-Voip (06/04/2025)

Schéma réseau :



Lien : [schéma réseau](#)

Planning : [redmine-mlz.ddns.net](#)

Tableau Configuration :

Contexte	Réseau IP	N° tel	login	serveur asterisk	VLAN
Volley-ball	192.168.10.0/24	1101	martin	192.168.10.253	10
Escrime	192.168.20.0/24	1201	ismail	192.168.20.253	20
Badminton	192.168.30.0/24	1301	louis	192.168.30.253	30

Configuration asterisk :
extensions.conf:

```
root@louis-Xbt:/etc/asterisk# cat extensions.conf
[general]
static = yes
writeprotect = yes
clearglobalvars = yes

[volleyball]

exten => _11XX,1,DIAL(SIP/${EXTEN},20)
exten => _11XX,2,VoiceMail(${EXTEN}@escrime)
exten => _11xx,2,VoiceMail(${EXTEN}@badminton)

exten => 1199,1,Answer()
exten => 1199,2, VoiceMailMain(${CALLERID(num)}@escrime)
exten => 1199,2, VoiceMailMain(${CALLERID(num)}@badminton)
exten => _12XX,1,Goto(escrime,${EXTEN},1)
exten => _12XX,1,Goto(badminton,${EXTEN},1)

[escrime]

exten => _12XX,1,DIAL(SIP/${EXTEN},20)
exten => _12XX,2,VoiceMail(${EXTEN}@volleyball)
exten => _12xx,2,VoiceMail(${EXTEN}@badminton)

exten => 1299,1,Answer()
exten => 1299,2, VoiceMailMain(${CALLERID(num)}@volleyball)
exten => _11XX,1,Goto(volleyball,${EXTEN},1)
exten => _13XX,1,Goto(badminton,${EXTEN},1)

[badminton]

exten => _13XX,1,DIAL(SIP/${EXTEN},20)
exten => _13XX,2,VoiceMail(${EXTEN}@volleyball)
exten => _13xx,2,VoiceMail(${EXTEN}@escrime)

exten => 1399,1,Answer()
exten => 1399,2, VoiceMailMain(${CALLERID(num)}@volleyball)
exten => 1399,2, VoiceMailMain(${CALLERID(num)}@escrime)
exten => _11XX,1,Goto(volleyball,${EXTEN},1)
exten => _12XX,1,Goto(escrime,${EXTEN},1)
root@louis-Xbt:/etc/asterisk#
```

user.conf:

```
root@louis-Xbt:/etc/asterisk# cat users.conf
[general]
hasvoicemail = yes
hassip = yes

[template](!)
type = friend
host = dynamic
dtmfmode = rfc2833
disallow = all
allow = ulaw
allow = alaw

#Utilisateur volleyball
[1101](template)
fullname = martin
username = m1101
secret = martin
mailbox = 1101
context = volleyball

#Utilisateur escrime
[1201](template)
fullname = ismail
username = i1201
secret = ismail
mailbox = 1201
context = escrime

#Utilisateur badminton
[1301](template)
fullname = louis
username = l1202
secret = louis
mailbox = 1301
context = badminton
```

Voicemail.conf:

```
root@louis-Xbt:/etc/asterisk# cat voicemail.conf
[general]
maxmsg = 100
maxsecs = 0
minsecs = 0
maxlogin = 3
review = no
saycid = no

[volleyball]
1101 => 1234, martin

[escrime]
1201 => 1234, ismail

[badminton]
1301 => 1234, louis
```

Configuration des VLAN :

Dans notre infrastructure, notre serveur ipbx est dans l'obligation de tagger les trames. Pour que la configuration soit permanente j'ai décidé d'utiliser un fichier netplan.

Les téléphones sont dans des VLANs différents et pour qu'ils puissent communiquer entre eux via le serveur IPBX, le trafic doit traverser les frontières des VLANs. Le taggage des trames permet donc au serveur IPBX de gérer ce trafic inter-VLAN. En taggant les trames, le serveur IPBX peut filtrer, router et permettre la communication seulement entre les VLANs pour les appels VoIP, tout en bloquant le reste du trafic. Cela permet au serveur IPBX de contrôler précisément quelles trames peuvent circuler entre les VLANs.

```
louis@louis-Xbt:~$ cat /etc/netplan/01-network-manager-all.yaml
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s8:
      dhcp4: no

  vlans:
    vlan.10:
      id: 10
      link: enp0s8
      addresses: [192.168.10.253/24]
      dhcp4: no
    vlan.20:
      id: 20
      link: enp0s8
      addresses: [192.168.20.253/24]
      dhcp4: no
    vlan.30:
      id: 30
      link: enp0s8
      addresses: [192.168.30.253/24]
      dhcp4: no
```

Filtrage:

Pour filtrer au niveau de l'ipbx on a utilisé l'utilitaire iptables

```
iptables -A INPUT -p udp --dport 5060 -j ACCEPT #autorise
connexion sip

#Autorise le trafic sip provenant des différents vlans
iptables -A INPUT -i vlan.10 -p udp --dport 5060 -j ACCEPT
iptables -A INPUT -i vlan.20 -p udp --dport 5060 -j ACCEPT
iptables -A INPUT -i vlan.30 -p udp --dport 5060 -j ACCEPT
```

```
iptables -A OUTPUT -o enp0s3 -j ACCEPT # Accepte trafic vers internet
```

```
iptables -A INPUT -j DROP #Bloque tout le trafic entrant  
iptables -A OUTPUT -j DROP #Bloque tout le trafic sortant
```

Paramétrage des actifs :

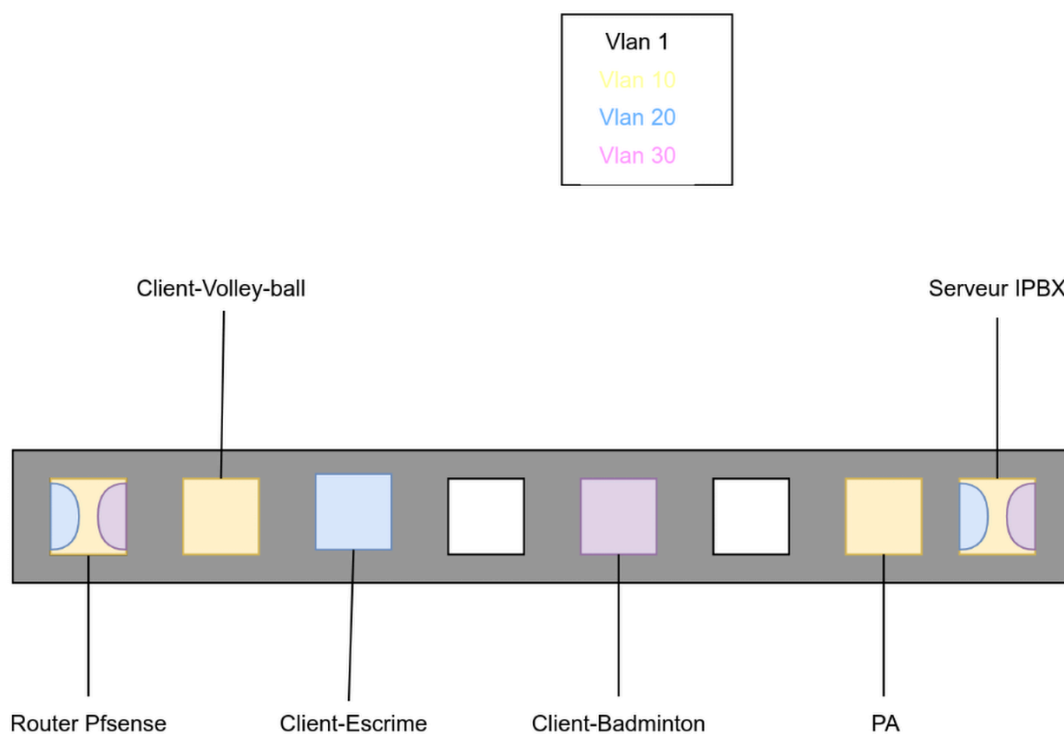
1. Switch:

Configuration des Vlan:

- Vlan 10 volley-ball
 - Entendu dhcp : 192.168.10.0/24

- Vlan 20 Escrime
 - Entendu dhcp : 192.168.20.0/24

- Vlan 30 Badminton
 - Entendu dhcp : 192.168.30.0/24



Lien : [schéma vlan](#)

Sur le switch netgear on a donc créé les 3 vlan. Pour faire en sorte qu'un port soit en trunking on a tagger le port dans chaque vlan et on laisse admit all. Pour faire en sorte qu'un port soit seulement dans un seul vlan on met en untag dans le vlan ou il doit être et on laisse en non cocher pour les autres. On le règle également en admit all.

PVID Configuration

PORTS LAGS All GO TO INTERFACE GO

	Interface	PVID Configured (1 to 4093)	Current PVID	Acceptable Frame Types	Ingress Filtering	Port Priority (0 to 7)
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	g1	1	1	Admit All	Disable	0
<input type="checkbox"/>	g2	10	10	Admit All	Disable	0
<input type="checkbox"/>	g3	20	20	Admit All	Disable	0
<input type="checkbox"/>	g4	1	1	Admit All	Disable	0
<input type="checkbox"/>	g5	30	30	Admit All	Disable	0
<input type="checkbox"/>	g6	1	1	Admit All	Disable	0
<input type="checkbox"/>	g7	10	10	Admit All	Disable	0
<input type="checkbox"/>	g8	1	1	Admit All	Disable	0
<input type="checkbox"/>	g9	1	1	Admit All	Disable	0
<input type="checkbox"/>	g10	1	1	Admit All	Disable	0

PORTS LAGS All GO TO INTERFACE GO

Configuration routeur PFsense

Notre routeur a deux cartes réseau en pont sur le labo. La première en utilisant la carte enp0s3 qui est vers le labo (wan) et la seconde qui est la carte enp0s8 qui est vers notre switch (lan). Notre routeur pfsense va tagger les trames sortantes dans les vlan 10, 20 ou 30 en fonction de l'IP de destination. Cela va permettre à nos clients d'accéder à internet.

1-Création des interfaces dans chaque vlan

Interfaces / VLANs

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs







GREs


GIFs


Bridges

LAGGs

VLAN Interfaces

Interface	VLAN tag	Priority	Description	Actions
em0 (lan)	10		vlan-volleyball	 
em0 (lan)	20		vlan-escrime	 
em0 (lan)	30		vlan-badminton	 

Interfaces / Interface Assignments 

Interface has been added. 

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs





PPPs


GREs

GIFs

Bridges



LAGGs

Interface	Network port
WAN	em1 (08:00:27:53:f9:f0)
LAN	em0 (08:00:27:ed:30:f8) 
OPT1	VLAN 10 on em0 - lan (vlan-volleyball) 
OPT2	VLAN 20 on em0 - lan (vlan-escrime) 
OPT3	VLAN 30 on em0 - lan (vlan-badminton) 

 Save

Configuration des interfaces vlan:

vlan 10:

Interfaces / OPT1 (em0.10)  

General Configuration

Enable

☒ Enable interface

Description

OPT1

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

Static IPv4 Configuration


IPv4 Address

192.168.10.254

/ 24



IPv4 Upstream gateway

None

 Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).
Gateways can be managed by [clicking here](#).

vlan 20:

Interfaces / OPT2 (em0.20)  

General Configuration

Enable

☒ Enable interface

Description

OPT2

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

Static IPv4 Configuration	
IPv4 Address	192.168.20.254 / 24
IPv4 Upstream gateway	None + Add a new gateway
<small>If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by clicking here.</small>	

vlan 30:

Interfaces / OPT3 (em0.30)	
General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	OPT3 <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	Static IPv4
Static IPv4 Configuration	
IPv4 Address	192.168.30.254 / 24
IPv4 Upstream gateway	None + Add a new gateway
<small>If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by clicking here.</small>	

Création des serveur dhcp pour qu'il fonctionne dans chaque vlan :

Vlan 10 - volleyball

Services / DHCP Server / OPT1	
ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.	
WAN LAN OPT1 OPT2 OPT3	
General DHCP Options	
DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on OPT1 interface

Primary Address Pool

Subnet

192.168.10.0/24

Subnet Range

192.168.10.1 - 192.168.10.254

Address Pool Range

192.168.10.10

From

192.168.10.200

To

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools

+ Add Address Pool

If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Server Options

WINS Servers

WINS Server 1

WINS Server 2

DNS Servers

9.9.9.9

Vlan 20 - escrime

Services / DHCP Server / OPT2

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

WAN

LAN

OPT1

OPT2

OPT3

General DHCP Options

DHCP Backend

ISC DHCP

Enable

☒ Enable DHCP server on OPT2 interface

Primary Address Pool

Subnet

192.168.20.0/24

Subnet Range

192.168.20.1 - 192.168.20.254

Address Pool Range

192.168.20.10

From

192.168.20.200

To

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools

+ Add Address Pool

If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Server Options

WINS Servers

WINS Server 1

WINS Server 2

DNS Servers

9.9.9.9

Vlan 30 - badminton

Services / DHCP Server / OPT3

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

WAN LAN OPT1 OPT2 **OPT3**

General DHCP Options

DHCP Backend: ISC DHCP

Enable ☒ Enable DHCP server on OPT3 interface

Primary Address Pool

Subnet: 192.168.30.0/24

Subnet Range: 192.168.30.1 - 192.168.30.254

Address Pool Range: From To

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools: [+ Add Address Pool](#)

If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Server Options

WINS Servers:

DNS Servers:

Parti de martin et ismail :

Explication du mode opératoire (schéma pour décrire l'attaque MITM dans notre lab montrer comment on compte procéder):

Phase d'attaque

- Phase de reconnaissance (nmap scanner le port du service SIP ouvert sur le server asterisk)
- interception MITM avec bettercap ou un autre outils peux importe
- Expliquer les résultat obtenue

Contre mesure

- Expliquer comment se prémunir de l'attaque 2 option je pense
- Sécurité par obscurcissement (pas ouf mais peut faire perdre bcp de temps à l'attaquant) changer le port par défaut en un port de service
- Chiffrer la connection SIP avec TLS

Plan de test:

Test	Résultats attendus	Résultats obtenus
La ligue volleyball peut communiquer avec les autres ligue	Les clients de la ligue volleyball doivent pouvoir établir des appels uniquement avec les autres ligues en utilisant le protocole SIP, et non avec les autres types de communication.	SIP : Nous n'avons pas pu essayer puisque les appelle téléphonique ne fonctionne pas Autre protocole : Bien bloquer grâce au vlan et au filtrage
La ligue escrime peut communiquer avec les autres ligue	Les clients de la ligue escrime doivent pouvoir établir des appels uniquement avec les autres ligues via le protocole SIP.	Nous n'avons pas pu essayer puisque les appelle téléphonique ne fonctionne pas
La ligue badminton peut communiquer avec les autres ligue	Les clients de la ligue badminton doivent pouvoir établir des appels uniquement avec les autres ligues en utilisant le protocole SIP.	Nous n'avons pas pu essayer puisque les appelle téléphonique ne fonctionne pas
Les appelle téléphonique sont bien chiffré	Tous les appels SIP doivent être chiffrés, garantissant ainsi que la confidentialité des échanges téléphoniques est respectée.	Martin n'a pas eu le temps de le mettre en place

Problème rencontré :

- La communication téléphonique ne fonctionne pas. On penser que le problème rencontré était dû au vlan mais elle était dû à une mauvaise configuration de nos clients. On leur avait mis comme passerelle le routeur pfsense cependant on aurais du mettre le serveur ipbx.