Projet SCOP-TI Amélioration d'une infrastructure informatique

Sommaire

I — P	rés	entation du projet	3
A	/	Contexte	3
E	3/	Objectifs	3
C	2/	Diagramme prévisionnel de Gantt	3
0)/	Schéma réseau	4
E	/	Plan d'adressage réseau	4
F	/	Table de routage de PfSense Scop-Ti	4
II – I	Dér	oulement du projet	5
A	\mathbf{V}	Installation du routeur PfSense	5
E	3/	Configuration du routeur par interface Web	8
	B	- 1 – Configuration du pare-feu (Firewall) PfSense	. 10
	B	- 2 – Configuration de l'agent relais DHCP	. 12
	B	– 3 – Redirection de port	. 13
C	2/	Mise en place du site Web	. 14
	C	– 1 – Installation du site	. 14
	C	- 2 – Sécurisation du site	. 15
III –	Tu	toriel	. 16
A	\	Installation et configuration de l'AD/DNS	. 16
E	3/	Installation du serveur DHCP sur Windows Serveur 2012	. 19
	B	- 1 – Installation du DHCP	. 21
	B	- 2 – Configuration du rôle DHCP	. 22
C	2-	Gestionnaire de mot de passe	. 27
0) –	Installation d'un DNS récursif avec Unbound	. 28
IV –	Ch	arte informatique	. 30
A	\	Champ d'application	. 30
	A	- 1 – Utilisateurs	. 30
	A	- 2 – Système d'information et de communication	. 30
E	8/	Confidentialité des paramètres d'accès	. 30
C	:/	Protection des ressources sous la responsabilité de l'utilisateur	. 31
0)/	Accès à Internet	. 31
E	/	Données personnelles	. 32
F	/	Contrôle des activités	. 32
	F	– 1 – Contrôles automatisés	. 32
C	5/	Sanctions	. 33
F	۱/	Entrée en vigueur	. 33

I – Présentation du projet

A/ Contexte

Vous venez d'intégrer l'équipe d'administration systèmes et réseaux de la SCOP et vous êtes en charge de la migration et de l'amélioration du SI. L'infrastructure informatique est vieillissante. L'entreprise dispose de 60 postes clients sous Windows 7 et d'un vieux serveur servant aux sauvegardes.

B/ Objectifs

Les différentes manipulations seront effectuées virtuellement dans la ferme de serveurs sous VMware vSphere 5.

L'objectif de notre projet est de créer 4 sous-réseaux (Production, Administratif, Serveurs, DMZ) séparé par un routeur. Dans le réseau Serveurs, il faudra créer un serveur Windows Server 2016 avec : Active Directory, DHCP, DNS faisant autorité, partage de fichiers. Dans le réseau DMZ, il faudra créer un serveur Débian pour héberger le site Web de l'entreprise. Il faudra créer un serveur Débian pour le DNS récursif ainsi qu'un dossier partagé par utilisateur et par groupe avec les droits nécessaire. Il faudra mettre en place un service de sauvegarde sur un NAS Synology, ainsi qu'avoir des mots de passe fort sur tous les équipements stocké dans un gestionnaire de mots de passe.



C/ Diagramme prévisionnel de Gantt

D/ Schéma réseau



E/ Plan d'adressage réseau

Nom du ss réseau	Nombre hôtes	Masque	@ sous réseau	@ Diffusion
Production	30	/27	10.0.0.0	10.0.031
Administration	30	/27	10.0.0.32	10.0.0.63
Serveur	14	/28	10.0.0.64	10.0.0.79
DMZ	14	/28	10.0.0.80	10.0.0.95

F/ Table de routage de PfSense Scop-Ti

Nom sous-réseau	Destination	Masque	Passerelle	Interface
Production	10.0.0.0	/27	10.0.0.30	10.0.0.30
Administratif	10.0.0.32	/27	10.0.0.62	10.0.0.62
Serveur	10.0.0.64	/28	10.0.0.78	10.0.0.78
DMZ	10.0.0.80	/28	10.0.0.94	10.0.0.94
Route par défaut	0.0.0.0	/0	172.16.127.254	172.16.20.107

II – Déroulement du projet

A/ Installation du routeur PfSense

Rappel sur qu'est-ce qu'un routeur :

Le routeur est un appareil physique ou virtuel qui fait la liaison entre Internet et les terminaux rattachés à cette dernière. Sa principale fonction est de router les flux Internet sur les réseaux.

Nous avons choisi de faire un routeur PfSense. C'est un routeur/pare-feu open source basé sur le système d'exploitation FreeBSD. Il utilise un pare-feu, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il s'administre à distance depuis une interface web ce qui rend la prise en main plus agréable.

Configuration requise :

	Minimale	Recommandée
Processeur	500 MHz	1 GHz
Mémoire vive	256 Mo	1 Go
Stockage	> 1 Go	

Tout d'abord, nous avons crée une nouvelle machine virtuel avec :

- l'image ISO de pfSense téléchargeable depuis le site officiel
- 5 cartes réseau
- 1 Go de RAM
- 8 Go d'espace de stockage

Nous allons démarrer la machine et lancer l'installation. Pour une utilisation du clavier en français faite comme ci-dessous et continuer avec « fr.acc.kbd keymap » :





Il va falloir partitionner le disque et il sera fait de manière automatique et enfin lancer le redémarrage.



Une fois le redémarrage fait, on va pouvoir assigner les interfaces de notre machine virtuelle aux interfaces du routeur en choisissant l'option « **1** ».

Il va aussi nous demandez si nous voulons configurez des interfaces VLAN mais cela ne sera pas utile pour notre projet donc mettre « **n** ».

Starting syslogdone. Starting CRON done. pfSense 2.4.4-RELEASE amd64 Thu Sep 2 Bootup complete	0 09:03:12 EDT 2018	1) Assign Interfaces 2) Set interface(s) IP address 3) Reset webConfigurator password 4) Reset to factory defaults	10) Filter Logs 11) Restart webConfigurator 12) PHP shell + pfSense tools 13) Update from console
FreeBSD/amd64 (pfSense.localdomain) (ttyv0)	6) Halt system	14) Enable Secure Shell (SSNG) 15) Restore recent configuration
UMware Virtual Machine - Netgate Devi	ce ID: 2cdc19884432240deef2	7) Ping host 8) Shell	16) Restart PHP-FPM
*** Welcome to pfSense 2.4.4-RELEASE	(amd64) on pfSense ***	Enter an option: 1	
WAN (wan) -> ем0 -> LAN (lan) -> ем1 ->		Valid interfaces are:	
 Ø) Logout (SSH only) 1) Assign Interfaces 2) Set interface(s) IP address 3) Reset webConfigurator password 4) Reset to factory defaults 5) Reboot system 6) Halt system 7) Ping host 8) Shell 	 9) pfTop 10) Filter Logs 11) Restart webConfigurator 12) PHP shell + pfSense tools 13) Update from console 14) Enable Secure Shell (sshd) 15) Restart PHP-FPM 	ем0 00:0c:29:a2:5a:b1 (up) Inte ем1 00:0c:29:a2:5a:d9 (up) Inte ем2 00:0c:29:a2:5a:c5 (dоwn) Inte ем3 00:0c:29:a2:5a:c5 (down) Inte ем4 00:0c:29:a2:5a:bb (down) Inte вм4 00:0c:29:a2:5a:bb (down) Inte Do VLANs need to be set up first? If VLANs will not be used, or only for say no here and use the webConfigurat	1(R) PRO/1000 Legacy Network Connection 1. 1(R) PRO/1000 Legacy Network Connection 1. r optional interfaces, it is typical to or to configure VLANs later, if required.
Enter an option:		Should VLANs be set up now [y:n]? n	

Il va falloir entrer le nom des interfaces correspondant au WAN¹, au LAN² et les interfaces restantes aux options en fonction des réseaux attribués dans les paramètres de la machine virtuelle, puis valider :



Enter the WAN interface name or 'a' for auto-detection (ем0 ем1 ем2 ем3 ем4 ог а): ем0 Enter the LAN interface name or 'a' for auto-detection NOTE: this enables full Firewalling/NAT mode. (em1 em2 em3 em4 a or nothing if finished): em1 Enter the Optional 1 interface name or 'a' for auto-detection (em2 em3 em4 a or nothing if finished): em2 Enter the Optional 2 interface name or 'a' for auto-detection (em3 em4 a or nothing if finished): em3 Enter the Optional 3 interface name or 'a' for auto-detection (em4 a or nothing if finished): em4 $\,$ The interfaces will be assigned as follows: WAN -> емЯ LAN \rightarrow em1 OPT1 \rightarrow em2 OPT2 \rightarrow em3 -> ем4 OPT3 Do you want to proceed [y:n]? y

Ensuite entrer l'option « 2 » pour configurer les adresses IP sur chaque interfaces, puis sur

«1» pour choisir l'interface WAN : Enter an option: 2 Available interfaces: ЫАМ (ем0 – dhcp, d LAN (ем1 – static) OPT1 (ем2) OPT2 (ем3) OPT3 (ем4) dhcp6) 45 Enter the number of the interface you wish to configure: 1 Configure IPv4 address WAN interface via DHCP? (y/n) n Enter the new WAN IPv4 address. Press <ENTER> for none: > 172.16.20.108 Subnet Masks are entered as bit counts (as in CIDR notation) in pfSense. e.g. 255.255.255.0 = 24 255.255.0.0 = 16 = 8 255.0.0.0 Enter the new WAN IPv4 subnet bit count (1 to 31): For a WAN, enter the new WAN IPv4 upstreaм gateway address. For a LAN, press <ENTER> for none: or a LAN, press 172.16.127.254 Configure IPv6 address WAN interface via DHCP6? (y∕n) n Enter the new WAN IPv6 address. Press <ENTER> for none: Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y Please wait while the changes are saved to WAN... Reloading filter... Reloading routing configuration... DHCPD. Restarting webConfigurator... The IPv4 WAN address has been set to 172.16.20.108/17 Press <ENTER> to continue.

¹ Interfaces WAN (Wide Area Network) : réseau informatique ou réseau de télécommunication couvrant une grande zone géographique (Internet).

² Interfaces LAN (Local Area network) : utilisée pour connecter les câbles de connexion aux périphériques de réseau local, tels que des ordinateurs et des commutateurs dans une zone limitée.

Il faudra refaire la même manipulation pour chaque interface pour obtenir ceci :

The IPv4 OPT3 address has been set to	10.0.0.30/27
Press <enter> to continue. VMware Virtual Machine - Netgate Devic</enter>	ce ID: 49b344910cd909f2f6b0
*** Welcome to pfSense 2.4.4-RELEASE	(amd64) on pfSense ***
ЫАN (wan) –> емй –> ∪4:	172.16.20.108/17
LAN (lan) $\rightarrow em1 \rightarrow v4$:	10.0.62/27
OPT1 (opt1) \rightarrow em2 \rightarrow v4:	10.0.0.94/28
ОРТ2 (opt2) -> ем3 -> ∨4:	10.0.78/28
ОРТЗ (opt3) -> ем4 -> ∨4:	10.0.0.30/27
0) Logout (SSH only)	9) pfTop
1) Assign Interfaces	10) Filter Logs
2) Set interface(s) IP address	11) Restart webConfigurator
3) Reset webConfigurator password	12) PHP shell + pfSense tools
4) Reset to factory defaults	13) Update froм console
5) Reboot system	14) Enable Secure Shell (sshd)
6) Halt system	15) Restore recent configuration
7) Ping host	16) Restart PHP-FPM
8) Shell	
Enter an option:	

Une fois que toute les interfaces sont configurées, On va faire un **reboot** (« 5 ») pour être sur que tout les paramètres indiquées soient bien pris en compte.

B/ Configuration du routeur par interface Web

Il faut maintenant à partir d'un sous-réseau crée précédemment (Admin, DMZ, Serveur, Prod) :

- → Créer une nouvelle machine virtuelle possédant une interface graphique.
- → Dans votre navigateur web préféré, entrer l'adresse ip correspondant à l'interface WAN pour arriver sur la page de configuration.
- → Par défaut : login admin et mot de passe pfsense

🚮 Login		× +				
← → ⊂ 1	۵	0	% 172.16.20.108		··· 🖂 🕁	III\ © ≡
	ofs	en	se			Login to pfSense
				SIGN IN		
				admin		
				••••••		
				SIGN IN		
		<u> </u>	pfSense	a is developed and maintained by Netgate. © ESF 2004.	- 2019 View license.	16:42
	1000		2			- 12 Tel 12 20/03/2019

Après connexion, il faut entrer le nom du routeur ainsi que le nom de domaine. On peut aussi renseigner les adresses des serveurs DNS si vous en avez mais il est possible de le faire plus tard.

🗾 pfSense.localdomain - Wizard: 🗙 🕂		- 0
← → C @) 172.16.20.108/wizard.php?xml=setup_wizard.xml	∭\ @ ≡
	System + Interfaces + Firewall + Services + VPN + Status + Diagnostics + Help +	•
WARNING: The 'a	dmin' account password is set to the default value. Change the password in the User Manager.	
Wizard / pt	Sense Setup / General Information	0
Step	2 of 9	
General Infor	On this screen the general pfSense parameters will be set.	
Ho	tname routeur-plSense EXAMPLE: myserver	
	Iocal.scopti.fr EXAMPLE: mydomain.com	
	The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To us manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the w	e the vizard.
Primary DNS	Server	
Secondary DNS	Server	
Overri	le DNS ☑ Allow DNS servers to be overridden by DHCP/PPP on WAN	
	> Next	
🚱 🌔 📜 🚺	E Contraction of the second se	▲ 16:45 20/03/2019

Il sera aussi possible de configurer l'interface WAN à partir d'ici mais c'est déjà fait pour nous. Il faudra **décocher** les 2 cases pour que les adresses IP privées puissent se connecter par l'interface WAN. **Continuer** l'installation jusqu'au redémarrage.

figuration	
IP Username	
TP Password	
TP password Reveal password characters	
I IP Address	
plocalsubnet 32	
e IP Address	
I on demand Enable Dial-On-Demand mode This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connec connection of the link is delayed until qualifying outgoing traffic is detected.	action. The interface is configured, but the actual
Ide timeout If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection this feature.	is brought down. An idle timeout of zero disables
Networks	
1918 Private Networks Block private networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved for private networks as per RF loopback addresses (127/8). This option should generally be left turned on, unless the WAN network I	FC 1918 (10/8, 172.16/12, 192.168/16) as well as lies in such a private address space, too.
gon networks	
Ion networks 📰 Block non-Internet routed networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet should never appear in the Internet routing table, and obviously should not appear as the source addre	assigned by IANA. Bogons are prefixes that ess in any packets received.
> Next	
jon net	Block non-Internet routed networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet should never appear in the Internet routing table, and obviously should not appear as the source addr Nort

BTS SIO 1 – Lycée Blaise Pascal – PPE 2

On va pouvoir ensuite **renommer** les interfaces pour plus de **facilité** dans le menu « Interfaces ».

	:16.20.108/interfaces.php?if=lan 👐 🗑 🏠	
COMMUNITY EDITION System	- Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help -	۲
Interfaces / Adm	in (em1) 🕱 🖬	ald \varTheta
The Admin configuration ha The changes must be applie Don't forget to adjust the Di	is been changed. de to take effect. ICP Server range if needed after spolying.	anges
General Configuration	n	
Enable	V Enable interface	
Description	Admin Enter a description (name) for the interface here.	
IPv4 Configuration Type	Static IPv4	
	None	
IPv6 Configuration Type		
IPv6 Configuration Type	INCREMENDANCE This field can be used to modify ('spool') the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxxxxxxx or leave blank.	
IPv6 Configuration Type MAC Address MTU	INCONCONCONCER This field can be used to modify ('spoof') the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxxxx or leave blank. If this field is blank, the adapter's default MTU will be used. This is tribuild 1500 break but can vary in some circomstances.	
MAC Address MTU MSS	INCLUSIONCOLOGY This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxxxxxxxx or isave black. If this field is black, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances. B	
IPv6 Configuration Type MAC Address MTU MSS	INCONCENCENT This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: reconcencercore of lase blank. If the field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances. If a value is entered in this field, them MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effe	fect.

B - 1 – Configuration du pare-feu (Firewall) PfSense

<u>Objectif d'un pare-feu :</u> outil informatique conçu pour protéger les données d'un réseau en définissant une politique de sécurité. Il contrôle les applications et les flux de données.

Dans le menu « Firewall » -> « Rule », créer une nouvelle règle qui autorise tout et supprimer les règles existantes sur chaque interface.

🚮 routeur-pfSense.loca	Iscopti.fr 🗙 🕂								9	×
(←) → C* @	③ 172.16.	20.108/firewall_rules_edit.phpi	?if=wan&after=-1			… 🖂 🕁		hin P		Ξ
	Edit Firewall Rule									*
	Action	Pass								
		Choose what to do with pack Hint: the difference between whereas with block the pack	kets that match the criteria s block and reject is that with tet is dropped silently. In eith	pecified below. reject, a packet (TCP RST or I er case, the original packet is	CMP port unreachable fo discarded.	or UDP) is returned to the send	er,			
	Disabled	🔲 Disable this rule								
		Set this option to disable thi	s rule without removing it fro	m the list.						
	Interface	WAN								
		Choose the interface from w	hich packets must come to	match this rule.						
	Address Family	IPv4								
		Select the Internet Protocol	version this rule applies to.	100						
	Protocol	Any Choose which IP protocol th	is rule should match.							-
	Source									
	Source	🗐 Invert match.	any		Source Address	1	*			
	Destination									
	Destination	🔄 Invert match.	any		Destination Add	Iress /	(w)			
	Extra Options									
	Log	Log packets that are han Hint: the firewall has limited the Status: System Logs: Se	idled by this rule local log space. Don't turn o <mark>ttings</mark> page).	n logging for everything. If doi	ng a lot of logging, consi	ider using a remote syslog ser	ver (see			
	Description	A description may be entere log.	d here for administrative refe	erence. A maximum of 52 char	acters will be used in th	e ruleset and displayed in the f	irewall			
🚱 🙋 i	📋 🖸 🍯						·B - 18 10 6		17:06 03/2011	

Maintenant dans « Firewall » -> « **NAT** »-> « Outbound » puis sélectionner « Manuel » et supprimer toutes les règles existantes :

P	ort Fi	orward	1:1 0.	stbound N	Pt						
0	utbo	ound NA1	ſ Mode								
			Mode	0		0				0	
			Au	utomatic outbou	ind NAT	Hybrid Outbound	NAT M	Manual Outb	ound NAT	Disable Outbound NAT	
			ru	le generation.	h	rule generation.	und (ule generati AON - Advar	on.	rule generation. (No Outbound NAT rules)	
			in	cluded)		NAT + rules below) (Outbound N/	AT)	(10 0000000 1111 1000)	
				_							
				🖹 Save							
М	app	ings									
7		Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Por	Static Port	Description	Actions
7	~	WAN	127.0.0.0/8	*	*	500	WAN addres	s *	~	Auto created rule for ISAKMP - localhost to WAN	100
7	*	WAN	127.0.0.0/8		*	3 x	WAN addres	s *	24	Auto created rule - localhost to WAN	/0±
V	~	WAN	::1/128	*		500	WAN addres	s *	~	Auto created rule for ISAKMP - localhost to WAN	100
V	~	WAN	::1/128		•		WAN addres	s *	x ;	Auto created rule - localhost to WAN	100
V	~	WAN	10.0.0.32/27	7 *	*	500	WAN addres	s *	~	Auto created rule for ISAKMP - ADMIN to WAN	100
7	~	WAN	10.0.32/27	7 *		*	WAN addres	s *	24	Auto created rule - ADMIN to WAN	100
7	~	WAN	10.0.0.80/28	8 *	*	500	WAN addres	s *	~	Auto created rule for ISAKMP - DMZ to WAN	100
V	~	WAN	10.0.0.80/28	B *	э.	*	WAN addres	s *	x ¢	Auto created rule - DMZ to WAN	100
2	~	WAN	10.0.0.64/28	в *	*	500	WAN addres	s *	~	Auto created rule for ISAKMP - SERVEUR to WAM	100
	~	WAN	10.0.0.64/28	8 *	•	*	WAN addres	s *	24	Auto created rule - SERVEUR to WAN	100
V		WAN	10.0.0/27	*	*	500	WAN addres	s *	*	Auto created rule for ISAKMP - PROD to WAN	100
7	~										

La **Network Address Translation** (NAT) permet de « transformer » une adresse privée en adresse publique afin de pouvoir avoir accès à l'extérieur.

Il y a 2 types NAT :

- NAT dynamique : associe des adresses privées à une seule adresse publique, permet d'économiser des adresses.
- NAT statique : une adresse publique pour une adresse privée.

On va créer une nouvelle règle en autorisant tout les protocoles et tous les sous-réseaux :

🖬 routeur-pfSense.local.scopti.fr 🗙 📑				- 6	×
(← → ୯ 🏠	① 172.16	.20.108/firewail_nat_out_edit.php?id=0 🗵	☆ I		=
	System	 Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help - 	€)		Î
Firewall,	/ NAT /	Dutbound / Edit	Θ		
	Disabled	🔟 Disable this rule			
	Do not NAT	Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules In most cases this option is not required.			
	Interface	WAN The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.			
Add	ress Family	IPv4 HPv6 Select the Internet Protocol version this rule applies to.			
	Protocol	any Choose which protocol this rule should match. In most cases "any" is specified.			
	Source	Any Image: Constraint of the outbound NAT mapping. / 24 Image: Constraint of the outbound NAT mapping. Port or Rang	je		
	Destination	Any	ja		
		Not Invert the sense of the destination match.			
Translatio	n				
	Address	Interface Address Connections matching this rule will be mapped to the specified Address.			
🚯 💋 📜 🚺	۲		FR - 18 📆 🕼	17:36 20/03/2019	

B-2-Configuration de l'agent relais DHCP

Protocole DHCP :



1/ DHCP Discover : le poste client va emmètre une trame de diffusion pour trouver un serveur DHCP

2/ DHCP Offer : le serveur va proposer une configuration réseau au client (adresse IP, masque, passerelle, ...)

3/ DHCP Request : le client va signaler au serveur qu'il accepte la configuration.

4/ DHCP Ack : le serveur indique au client que l'ensemble est validé et que l'échange peut terminer.

L'agent relais DHCP est un programme activé sur une ou plusieurs interfaces de la machine servant de relais DHCP au client. Il sera capable de relayer la trame de diffusion (DHCP Discover) dans les autres sous réseaux et ainsi, on peut gérer plusieurs sous-réseaux avec un seul serveur DHCP.

Pour configurer le relais DHCP, il faut aller dans le menu « Services » -> « DHCP Relay » en sélectionnant les sous-réseaux voulu et l'adresse IP du serveur DHCP.

Relay						
ation						
Enable DHCP relation	y on interface					
ADMIN DMZ SERVEUR PROD						
Interfaces without an	n IP address wil	I not be shown.				
Append circuit ID If this is checked, the	and agent ID to e DHCP relay wi	requests Il append the ciri	uit ID (pfSen	se interface nu	mber) and the agent	ID to the DHCP r
10.0.0.65						
This is the IPv4 addr requests are relayed.	ess of the serve	r to which DHCP				
	Relay ation Enable DHCP rela DMZ SERVEUR PACO HoterSacea HoterSacea Append circuit ID If this is checked, thi 10.0.0.65 This is the IPA4 addi	Relay ation ■ Enable DHCP relay on interface DM2 SERVEUR PROO Netrofaces without an IP address with Interfaces without an IP address with If this is checked, the DHCP relay with 10.0.0.65 This is the IPv4 address of the server requests are melayed.	Relay ation Enable DHCP relay on interface Enable DHCP relay on interface DM2 SERVEUR SERVEUR FIGO Interfaces suthout an IP address will not be shown. Append circuit ID and agent ID to requests If this is checked, the DHCP relay will append the circ 10.0.0.65 This is the IP-4 address of the server to which DHCP requests are nelawed.	Relay ation Enable DHCP relay on interface ADM: DM2 SERVEUR PROD Therfaces will not be shown. Append circuit ID and agent ID to requests If this is checked, the DHCP relay will append the circuit ID (pfSen 10.0.0.45 This is the IPA4 address of the server to which DHCP requests are relayed.	Relay ation Enable DHCP relay on interface Enable DHCP relay on interface SERVEUR SERVEUR SERVEUR Therfaces sufficient an IP address will not be shown. Append circuit ID and agent ID to requests If this is checked, the DHCP relay will append the circuit ID (pfSense interface nu 10.0.0.65 This is the IPV4 address of the server to which DHCP requests are nelawed.	Ation Image: Enable DHCP relay on interface Image: Enable DHCP relay will append the circuit ID (plSense interface number) and the agent Image: Image: Enable DHCP relay will append the circuit ID (plSense interface number) and the agent Image: Image: Enable DHCP relay will append the circuit ID (plSense interface number) and the agent Image: Image: Enable DHCP relay will append the circuit ID (plSense interface number) and the agent Image: Image: Enable DHCP relay will append the circuit ID (plSense interface number) and the agent Image: Image: Enable DHCP relay will append the circuit ID (plSense interface number) and the agent Image: Imag

B - 3 - Redirection de port

La redirection de port consiste à rediriger des paquets réseaux reçus sur un port donné d'un ordinateur ou un équipement réseau vers un autre appareil ou réseau sur un port donné. C'est utile pour accéder à un périphérique ou à un service connecté à Internet à partir de n'importe où dans le monde.

Nous allons faire une **redirection de port** dans le menu « System/Adavanced/ Admin Acces » en commençant par changer le port d'accès à l'interface Web qui est **8080** par défaut.

On va maintenant faire en sorte que tout ce qui arrive par l'interface WAN sur le port 8080 soit **redirigé** vers le site Web qui se trouve dans le sous-réseau **DMZ**

Firewall / NAT /	Port Forward / Edit						
Edit Redirect Entry							
Disabled	Disable this rule						
No RDR (NOT)	Disable redirection for tra	affic matching this rule					
	This option is rarely needed.	Don't use this without the	rough knowledge of the	e implications.			
Interface	WAN		~				
	Choose which interface this	rule applies to. In most ca	ses "WAN" is specified.				
Protocol	TOP						
FIGUCCO	Choose which protocol this	rule should match. In mos	t cases "TCP" is specifi	ed.			
Source	Cisplay Advanced						
Destination	Invert match.	WAN address		~		1	
		Туре			Address/mask		
Destination port range	HTTP		HTTP	~			
	From port	Custom	To port		Custom		
	Specify the port or port rang	e for the destination of the	e packet for this mappir	ng. The 'to' fiel	d may be left empty if only	mapping a single port.	
Redirect target IP	10.0.0.81						
	Enter the internal IP address e.g.: 192.168.1.12	of the server on which to	map the ports.				
Redirect target port	HTTP		~				
	Port Custom						
	Specify the port on the mach calculated automatically).	nine with the IP address er	ntered above. In case of	a port range,	specify the beginning port	of the range (the end port w	

Zone démilitarisée (DMZ) : c'est un sous-réseau qui est séparé du réseau local et isolé par un pare-feu. Il permet de mettre les machines qui sont accessibles depuis Internet et qui non pas besoin d'accéder au réseau local.

C/ Mise en place du site Web

C-1-Installation du site

Tout d'abord, nous avons crée une machine virtuel (VMWare Workstation 14) sous Debian9 et lui attribuer une configuration IP fonctionnelle. Une fois installé, nous allons mettre à jour le système :

\$ sudo apt-get update
\$ sudo apt-get upgrade

On installe ensuite apache2, php7.0, php7.0-mysql, serveur mysql :

\$ sudo apt-get install apache2 php7.0 php7.0-mysql mysqlserver

On redémarre le service apache2 :

\$ sudo service apache2 restart

On télécharge ensuite Wordpress depuis le site officiel :

\$ wget https://fr.wordpress.org/wordpress-5.1-fr FR.tar.gz

On désarchive le dossier Wordpress :

\$ tar zxvf wordpress-5.1-fr_FR.tar.gz

On supprime le dossier html pour y mettre Wordpress :

\$ sudo rm -R /var/www/html

On copie le dossier désarchivé dans le dossier par défaut d'apache2 :

\$ sudo cp -R wordpress /var/www/html

On attribue ensuite l'utilisateur www-data et le groupe www-data comme propriétaires du dossier /var/www/html :

\$ sudo chown -R www-data:www-data /var/www/html/

On démarre le serveur mysql :

\$ sudo service mysql start

On change ensuite le mot de passe de l'utilisateur root de mysql :

\$ sudo /usr/bin/mysql_secure_installation

On se connecte en root à mysql :

\$ mysql -u root -p

(Si vous êtes connecté en root sur votre machine, il n'est plus nécessaire d'indiquer le mot de passe pour l'utilisateur root de mysql depuis debian 9)

On crée ensuite un nouvel utilisateur qui servira à Wordpress :

mysql> CREATE USER scopti@localhost IDENTIFIED BY
@t&SCaub\$b#J';

On crée ensuite la base de données qui sera utilisé par Wordpress :

mysql> CREATE DATABASE scopti;

Puis on donne un accès total à l'utilisateur « scopti » sur la base de données scopti :

mysql> GRANT ALL PRIVILEGES ON scopti.* TO scopti@localhost;

Une fois les commandes tapées, il faut taper l'adresse IP de votre serveur qu'on a précédemment configuré sur un navigateur Web, cela nous enverra sur l'interface Web et où il faudra rentrer des données.

C-2-Sécurisation du site

- → Il faut supprimer le compte admin car il est proposé par défaut donc massivement utilisé par les pirates pour accéder au site. Il faut créer un nouvel utilisateur avec tout les droits administrateurs pour pouvoir le supprimer. Attention avant de supprimer le compte admin, il faut attribuer tous les articles et les liens au nouvel utilisateur crée.
- → Modifier l'adresse de connexion qui elle aussi est par défaut.
- ➔ Toujours être à jour

۲

III – Tutoriel

Au préalable, nous avons installé un Windows Server 2012 sur une machine virtuelle (VMWare vSphere).

A/ Installation et configuration de l'AD/DNS

L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows.

Pour installer l'AD (Active Directory), dans le Gestionnaire de serveur cliquez sur « **Gérer** » (en haut à droite).

Ensuite, cliquez sur « Ajouter des rôles et des fonctionnalités ».

Cliquez sur « **Suivant** », laissé cocher ce qui est par défaut : Installation basée sur un rôle ou une fonctionnalité, puis cliquez sur « **Suivant** ».

Ensuite, cliquez à nouveau sur « Suivant ».

Maintenant, cocher le rôle « Services AD DS », puis cliquer sur « Ajouter des fonctionnalités ».

Cliquez ensuite sur « Suivant » (3 fois).

Cliquez maintenant sur « Installer ».

Vous obtenez ceci :





Une fois la configuration terminée, cliquer sur « Fermer ». Nous allons promouvoir ce serveur en contrôleur de domaine, en cliquant sur le drapeau jaune, puis « promouvoir ce serveur en contrôleur de domaine ».

🚵 Assis	tant Configuration des services de domaine Active Directory	_ 0 X
Configuration de déploie Options du contrôleur de Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Sélectionner l'opération de déploiement Ajouter un contrôleur de domaine à un domaine existant Ajouter un nouveau domaine à une forêt existante Ajouter un nouveau domaine à une forêt existante Ajouter une nouvelle forêt Spécifiez les informations de domaine pour cette opération Nom de domaine racine :	SERVEUR CIBLE DC
	< Précédent Suivant > Installe	Annuler

Cliquer sur Ajouter une nouvelle forêt, et renseigner le nom de votre domaine. Dans mon cas « local.scopti.fr ».

Pour poursuivre, cliquez sur « Suivant ».

📥 Assis	tant Configuration des services (de domaine Active Directory	/ <u> </u>
Options du contró Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Sélectionner le niveau fonctionnel de Niveau fonctionnel de la forêt : Niveau fonctionnel de la forêt : Niveau fonctionnel du domaine : Spécifier les fonctionnalités de contra Serveur DNS (Domain Name Syst Catalogue global (GC) Contrôleur de domaine en lectur Taper le mot de passe du mode de n Mot de passe : Confirmer le mot de passe :	la nouvelle forêt et du domaine ra Windows Server 2008 R2 Windows Server 2012 R2 ôleur de domaine em) e seule (RODC) estauration des services d'annuaire ••••••• •••••••	SERVEUR CIBLE DC
	<	Précédent Suivant >	Installer Annuler

NB : Si dans votre architecture vous disposez d'un serveur antérieur à Windows 2012. Je vous recommande de mettre en niveau fonctionnel de la forêt le nom de l'OS antérieur de votre infrastructure.

Cliquez sur « Suivant » pour poursuivre

Une erreur apparaît sur l'écran suivant. Ce message survient, car aucun serveur DNS n'est installé sur la machine. Cliquez simplement sur « Suivant » pour le créer

Ensuite, indiquer un nom NetBIOS au domaine « SCOPTI ».

🚡 Assis	tant Configuration des services de domaine Active Directory	_ 0 X
Options suppléme	SERVEUR CIBLE DC	
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire. Le nom de domaine NetBIOS :	
	En savoir plus sur la options supplémentaires	
	< Précédent Suivant > Installer	Annuler

Cliquez sur « Suivant ». Laisser les valeurs de l'écran suivant par défaut (NTDS et SYSVOL).

Spécifier l'emplacement de la base d	le données AD DS, des fichiers journaux et	de SYSV <mark>O</mark> L
Dossier de la base de données :	C:\Windows\NTDS	
Dossier des fichiers journaux :	C:\Windows\NTDS	
Dossier SYSVOL :	C:\Windows\SYSVOL	

Puis cliquez sur « Suivant ».

L'installation est prête et un récapitulatif est affiché pour vérifier la configuration.

Cliquez sur « Suivant ».

Une vérification système est effectuée, cliquer sur « Installer ».

Le serveur va ensuite redémarrer automatiquement.

Le login se fait maintenant avec votre compte et mot de passe du domaine.

Votre contrôleur de domaine est maintenant prêt.

B/ Installation du serveur DHCP sur Windows Serveur 2012

Dans ce tutoriel nous allons voir ensemble une installation complète simpliste de l'outil DHCP sur un Windows Serveur 2012. Cependant pour aller un peu plus loin, il est important de comprendre certaines terminologies.

Terminologie :

<u>Étendue</u> : Une *étendue* est la plage consécutive complète des adresses IP probables d'un réseau. Les étendues désignent généralement un sous-réseau physique unique de votre réseau auquel sont offerts les services DHCP. Les étendues constituent également pour le serveur le principal moyen de gérer la distribution et l'attribution d'adresses IP et de tout autre paramètre de configuration associé aux clients du réseau.

<u>Étendue globale</u> : Une *étendue globale* est un regroupement administratif des étendues pouvant être utilisé pour prendre en charge plusieurs sous-réseaux logiques IP sur le même

sous-réseau physique. Les étendues globales contiennent uniquement une liste d'étendues membres ou d'étendues enfants qui peuvent être activées ensemble.

<u>Plage d'exclusion</u> : Une *plage d'exclusion* est une séquence limitée d'adresses IP dans une étendue, exclue des offres de service DHCP. Les plages d'exclusion permettent de s'assurer que toutes les adresses de ces plages ne sont pas offertes par le serveur aux clients DHCP de votre réseau.

Pool d'adresses : Une fois que vous avez défini une étendue DHCP et appliqué des plages d'exclusion, les adresses restantes forment le *pool d'adresses* disponible dans l'étendue. Les adresses de pool peuvent faire l'objet d'une affectation dynamique par le serveur aux clients DHCP de votre réseau.

Bail : Un *bail* est un intervalle de temps, spécifié par un serveur DHCP, pendant lequel un ordinateur client peut utiliser une adresse IP affectée. Lorsqu'un bail est accordé à un client, le bail est *actif*. Avant l'expiration du bail, le client doit renouveler le bail de l'adresse auprès du serveur. Un bail devient *inactif* lorsqu'il arrive à expiration ou lorsqu'il est supprimé du serveur. La durée d'un bail détermine sa date d'expiration et la fréquence avec laquelle le client doit le renouveler auprès du serveur.

<u>Réservation</u> : Utilisez une *réservation* pour créer une affectation de bail d'adresse permanente par le serveur DHCP. Les réservations permettent de s'assurer qu'un périphérique matériel précis du sous-réseau peut toujours utiliser la même adresse IP.

Types d'options : Les *types d'options* sont d'autres paramètres de configuration client qu'un serveur DHCP peut affecter lors du service de baux aux clients DHCP.

<u>Classes d'options</u> : Une *classe d'options* est un moyen pour le serveur de continuer à gérer les types d'options proposés aux clients. Lorsqu'une classe d'options est ajoutée au serveur, les clients de cette classe peuvent être fournis en types d'options spécifiques à la classe pour leur configuration.

Avant de commencer :

Il est nécessaire de configurer son serveur en **IP fixe** et de l'avoir renommé. Nommer votre serveur en fonction de la convention de nommage de votre entreprise. Ici, nous installerons le rôle DHCP sur notre contrôleur de domaine, celui-ci porte déjà le nom **sr-serv-WinServ-PPE-serveurDHCP-DNS-AD** et **local.scopti.fr** pour **Domain Controller**.

B – 1 - Installation du DHCP

Depuis le Gestionnaire de serveur, cliquer sur l'étape Gérer puis Ajouter des rôles et fonctionnalités.

Sélectionner le type d'installation « Installation basée sur un rôle ou une fonctionnalité »

Sélectionnez le serveur de destination, pour votre serveur DHCP, et cliquez sur Suivant.

Vous êtes maintenant sur la fenêtre de sélection des rôles. Nous allons donc installer le rôle DHCP. Pour cela, cocher simplement **DHCP** dans la fenêtre de sélection des rôles. Enfin, cliquer sur **Suivant**.

Sélectionner des	Assistant Ajout de rôles et de fonctionnalités	SERVEUR DE DESTINATION
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs	Sélectionnez un ou plusieurs rôles à installer sur le serveur sélec Rôles	serv1-WIN_2012.local.scopti.fr tionné. Description L'accès à distance offre une connectivité transparente, toujours
Fonctionnalités Confirmation Résultats	Hyper-V Serveur d'applications Serveur de télécopie Serveur DHCP (Installé) Serveur DNS (Installé) Serveur Web (IIS) Services AD DS (Installé) Services AD DS (Installé) Services AD FS (Active Directory Federation Service) Services AD LDS (Active Directory Lightweight Directory Rights Manage) Services d'activation en volume V	active et toujours gérée basée sur DirectAccess. L'accès à distance fournit des services VPN traditionnels, y compris la connectivité de site à site (succursale ou nuage). Le routage fournit des fonctionnalités de routage traditionnelles, y compris la traduction d'adresses réseau et d'autres options de connectivité.
	< <u>P</u> récédent Sui <u>v</u> an	t > Installer Annuler

Des fonctionnalités supplémentaires sont automatiquement sélectionnées pour vous, ajoutez-les.

Après avoir ajouté des rôles, vous pouvez ajouter des fonctionnalités supplémentaires. En général, toutes les caractéristiques qui sont nécessaires pour soutenir le rôle de cible sont déjà sélectionnées de sorte que vous pouvez simplement cliquer sur le bouton **Suivant** pour continuer.

Vous aurez alors quelques infos sur le rôle que vous êtes en train d'ajouter (« Serveur DHCP »). Cliquez sur **Suivant** <u>après en avoir pris connaissance</u>.

Vous devez maintenant **confirmer** l'ajout du rôle DHCP sur votre serveur. Cliquez sur **Installer**.

Votre serveur est maintenant en cours d'installation, après quelques minutes, l'installation sera terminée. L'installation du rôle DHCP ne nécessite pas de redémarrage du serveur.

R.	Assistant Ajout de rôles et de fonctionnalités
Progression de l	'installation Serveur de destination Serveur de destination
Avant de commencer Type d'Installation Sélection du serveur Rôles de serveurs Fonctionnal(tés Serveur DHCP Confirmation Résultats	Afficher la progression de l'installation Installation de fonctionnalité Installation démarrée sur Serv1-WIN_2012.local.scopt.fr Outils d'administration de serveur distant Outils d'administration de rôles Outils du serveur DHCP Serveur DHCP
	Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche. Exporter les paramètres de configuration < Précédent Suivant > Fermer Annuler

Maintenant que votre serveur DHCP est installé, il faut le configurer. Pour cela, depuis le Gestionnaire de serveur, vous devriez avoir une alerte (Configuration post-déploiement), cliquez sur **Terminer la configuration DHCP**.

Gestionnaire de se	rveur				-
e bord	• @ 🍢	Gérer	Outils	Afficher	Aide
e total de serveurs : 1 1 DHCP 1 Facilité de gestion Événements Services Performances Résultats BPA	Configuration post-déploie Configuration requise pour : Serveur DHCP à SERV Terminer la configuration DHCP Installation de fonctionnalité Configuration requise. Installation réussie sur 28DC-zerobuglab. Ajouter des rôles et fonctionnalités Détails de la tâche				

B – 2 – Configuration du rôle DHCP

Ici on va autoriser DHCP dans le domaine, pour cela il vous faudra un compte administrateur du domaine.

Vous pouvez utiliser le compte sur lequel vous êtes actuellement connecté ou bien un autre compte. Une fois le compte choisi cliquez sur **Valider**.

1	Assistant Configuration post-installation DHCP
Autorisation Description Autorisation Recurse	Assistant Configuration post-installation DHCP
	< Précédent Suivant > Valider Annuler

L'assistant Configuration post installation DHCP va alors créer des groupes de sécurité dans ADDS et autoriser le serveur DHCP. Cliquez sur **Fermer**.

On a passé la partie la plus simple, passons aux choses sérieuses, la configuration des étendues (aussi appelé Scopes).

Pour créer vos étendues, lancer la console DHCP via votre gestionnaire de serveur.



Depuis cette console, vous allez pouvoir **créer vos étendues DHCP**. Nous allons créer notre première étendue IPv4 pour que les clients puissent obtenir une adresse IP automatiquement.

Effectuer un clic droit sur IPv4, puis sélectionner « Nouvelle étendue... ».

Donnez un nom à votre nouvelle étendue.

DHCP			_ D X	Assistant Nou	velle étendue					
Fichier Act	ion Affichage ?					Nom de l'étendue	5			
2 DHCP	Contenu de DHCP		État Actions			Vous devez toumir un nom pour identitier l'étendue. Vous avez aussi la possibilité de fournir une description.				
⊿ serv1-v	vin_2012.local.scopti.fr	serv1-win_2012.local.scopti.fr		DHCP	*					
	Afficher les statistiques Nouvelle étendue Nouvelle étendue de multidiffusion		Autres actions		actions •	Tapez un nom et une description pour cette étendue. Ces informations vous permettront d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.				
	Configurer un basculement Répliquer les étendues de basculement				Nom	Nom : SR-Nom_de_votre_reseau				
	Définir les classes des utilisateurs Définir les classes des fournisseurs					Description :				
	Réconcilier toutes les étendues									
	Définir les options prédéfinies Actualiser									
	Propriétés									
	Aide									
		< <u> </u>	1	>			< Précédent Suivant > Annuler			

Vous pouvez maintenant définir la plage d'adresses IP pour cette étendue. Cliquez ensuite sur **Suivant**.

Vous pouvez si vous le souhaitez, ajouter une ou plusieurs **plages d'exclusions**. Ce sont les adresses qui ne seront pas distribuées par le serveur DHCP (par exemple son adresse ipv4).

La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de l'étendue que vous êtes en train de créer, par défaut, le bail est limité à 8 jours. Vous pouvez le modifier suivant vos besoins. Par exemple si vous créer un serveur DHCP pour un réseau WiFi public, un bail de 24H est suffisant.

Assistant Nouvelle étendue
Durée du bail La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.
La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.
De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.
Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.
Limitée à :
Jours : Heures : Minutes :
< Précédent Suivant > Annuler

Lors de la Configuration des paramètres DHCP, cliquez sur « **Oui, je veux configurer ces options maintenant** » puis cliquez sur Suivant.

Lors de la configuration des paramètres DHCP, vous allez **pouvoir ajouter la passerelle par défaut**, c'est cette passerelle qui sera ajoutée sur tous les clients de l'étendue.

Assistant Nouvelle étendue	Assistant Nouvelle étendue	
Configuration des paramètres DHCP	Routeur (passerelle par défaut)	
Vous devez configurer les options DHCP les plus courantes pour que les clients	Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être	
puissent utiliser l'étendue.	distribués par cette étendue.	
Lorsque les clients obtiennent une adresse, ils se voient attribuer des options DHCP,	Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients,	
telles que les adresses IP des routeurs (passerelles par défaut), des serveurs DNS, et	entrez l'adresse ci-dessous.	
les paramètres WINS pour cette étendue.	Adresse IP :	
Les paramètres que vous sélectionnez maintenant sont pour cette étendue et ils	Ajouter	
remplaceront les paramètres configurés dans le dossier Options de serveur pour ce	10.0.0.30	
serveur.	Supprimer	
Voulez-vous configurer les options DHCP pour cette étendue maintenant ?	Monter	
	Descendre	
< Précédent Suivant > Annuler	< Précédent Suivant > Annuler	

Même chose au niveau du serveur DNS, ajouter la ou les adresses des serveurs DNS que vous souhaitez utiliser.

	Assistant N	louvelle étendue			
Nom de domaine et serve DNS (Domain Name Syste clients sur le réseau.	urs DNS m) mappe et tra	aduit les noms de domaines utilis	iés par les		
Vous pouvez spécifier le doma résolution de noms DNS.	ne parent à util	iser par les ordinateurs clients su	ir le réseau pour la		
Domaine parent : local.s	local.scopti.fr				
Pour configurer les clients d'éte les adresses IP pour ces serve Nom du serveur :	endue pour qu'i urs.	ls utilisent les serveurs DNS sur Adresse IP :	le réseau, entrez		
dns.local.scopti.fr		+: + +	Ajouter		
	Résoudre	10.0.0.65	Supprimer		
			Monter		
			Descendre		
		< Précédent Suiva	nt > Annuler		
		[construction]			

Si vous utilisez des serveurs WINS, ajoutez-les ici. Cliquez ensuite sur suivant.

Vous pouvez maintenant activer l'étendue maintenant ou ultérieurement.

Répéter autant de fois qu'il vous est nécessaire cette opération.

Maintenant, dès lors ou vous connecterez des clients sur votre réseau, le DHCP attribuera une adresse IP en fonction de la plage que vous avez créé.



Et voila, votre serveur DHCP est fonctionnelle dans ces grandes lignes. PS : Pour que votre serveur DHCP puisse fonctionner dans vos sous-réseau ip n'oubliez pas de mettre en place l'agent DHCP de votre routeur, sinon il y aura des dysfonctionnements.

C – Gestionnaire de mot de passe

	KeePass	Dashlane	LastPass
Avantages	Hachage de 256 bits (AES et Twofish) - Stock les mots de passe dans un fichier crypté sur l'appareil utilisateur - Recommandé par l'ANSSI - Gratuit	- AES-256 - Interface - 50 mots de passe	 AES 256 bits avec SHA-256 PBKDF2 et hachage salt Interface Possède une version gratuite
Inconvénients	Interface	Version gratuite limitée	Par navigateur web
Système d'exploitation	- Windows (98 à 10), - OS X - Linux	- Mac - Windows - Linux	- Windows - Mac - Linux

Tableau comparatif de gestionnaire de mot de passe :

Notre choix se portera sur le gestionnaire de mot de passe KeePass (Version 2.42), il est assez complet malgré l'interface un peu vieillissante, la recommandation de ce gestionnaire par l'ANSSI montre que c'est une source sûre pour nous protéger d'éventuelles attaques.

Présentation de KeePass :

C'est un gestionnaire de mot de passe open source gratuit (certifié OSI et recommandé par l'ANSSI) qui va nous aider à gérer nos mots de passe de manière sécurisée. On peut mettre tous nos mots de passe dans une base de données, qui est verrouillée avec une clé principale ou un fichier de clé. Il nous suffit donc de ne mémoriser qu'un seul mot de passe principal ou de sélectionner le fichier de clé pour déverrouiller l'ensemble de la base de données. Les bases de données sont cryptées à l'aide des algorithmes de cryptage les plus fiables et les plus sécurisés du moment (AES et Twofish).

Source : <u>https://keepass.info/</u>

Facultatif : Télécharger le fichier French dans Translation (également sur le site) qu'il faut extraire, récupérer le fichier « French.Ingx » et le coller dans le dossier KeePass Password Safe 2 > Languages.

Lancer KeePass, cliquer sur **CLOSE** puis cliquez sur le menu **VIEW** puis choisir le langage voulu, validez et confirmer le redémarrage.

KeePass est désormais en français.

Créer la base de données qui contiendra tout les mots de passes qui se sera sécurisé par un mot de passe unique dont il est conseillé de mettre un mot de passe fort et pouvoir s'en souvenir car il n'y aura aucune possibilité pour le récupérer.

Partage du fichier :

Pour avoir accès à la base de données du gestionnaire de mot de passe par les différents comptes administrateurs, il faut au préalable avoir créé un réseau de partage accessible par les différents postes administrateurs et y partager un dossier inaccessible à d'autres.

Ensuite, créer un dossier partagé, accessible que pour les administrateurs qui contiendra la base de données du gestionnaire de mot passe. Cela va permettre d'avoir accès au mot de passe de n'importe quel poste sur le réseau avec un compte administrateur.

D – Installation d'un DNS récursif avec Unbound

Le protocole **DNS** (*Domain Name System*) est un protocole de résolution de noms. Il permet d'associer un nom de domaine à un enregistrement. Le serveur récursif permet d'interroger les serveurs faisant autorité sur Internet pour résoudre le nom de domaine. Nous avons décidé d'utiliser Unbound pour faire le DNS récursif. Pour installer Unbound :

\$ sudo apt-get update \$ sudo apt-get upgrade \$ sudo apt-get install unbound Editer le fichier de configuration pour obtenir celui la :

\$ nano /etc/unbound/unbound.conf

Unbound configuration file for Debian.
See the unbound.conf(5) man page.
See /usr/share/doc/unbound/examples/unbound.conf for a commented # reference config file.
" # The following line includes additional configuration files from the # /etc/unbound/unbound.conf.d directory. include: "/etc/unbound/unbound.conf.d/*.conf"
server:
Interface d'ecoute IPv4 sur le reseau interface: 10.0.0.82 interface: 127.0.0.1
Autorise les reseaux renseignes a se servir du serveur DNS access–control: 10.0.0.0/8 allow access–control: 0.0.0.0/0 refuse
Cache la version d'Unbound et empeche de connaitre le nom du serveur et l'ID du service hide–version: yes hide–identity: yes
Autorisation de l'IPv4 do-ip4: yes do-udp: yes do-tcp: yes

On peut vérifier qu'il n'y est pas d'erreur sur le fichier :

\$ sudo unbound-chekconf /etc/unbound/unbound.conf

Il faut maintenant crée le fichier qui accueillera les logs :

\$ sudo mkdir /var/log/unbound

\$ sudo touch /var/log/unbound/unbound.log

\$ sudo chown -R unbound:unbound /var/log/unbound

Il faut renseigner son adresse IP dans le fichier resolv.conf :

\$ sudo nano /etc/resolv.conf

On peut enfin démarrer unbound :

\$ sudo service start unbound

IV – Charte informatique

L'entreprise SCOP TI met en œuvre un système d'information (SI) et de communication nécessaire à son activité, comprenant un réseau informatique.

Les employés, dans l'exercice de leurs fonctions sont conduits à accéder aux moyens de communication mis à leur disposition et a les utiliser. Ainsi, l'utilisation du système d'information (SI) et de communication doit être effectuée exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte.

A/ Champ d'application

A - 1 - Utilisateurs

La présente charte s'applique à l'ensemble des utilisateurs du SI et de communication de l'entreprise, quel que soit leur statut (y compris mandataires sociaux, intérimaires, stagiaires, visiteurs ...).

A - 2 - Système d'information et de communication

Le SI et de communication de l'entreprise est notamment constitué des éléments suivants : ordinateurs (fixes et/ou portables), périphériques, assistants personnels, réseau informatique (serveurs, routeurs et connectique), logiciels, fichiers, base de données et données ...

Pour des raisons de sécurité du réseau, le matériel personnel des salariés connecté au réseau de l'entreprise ou qui contiennent des informations concernant l'entreprise sont considérés comme faisant partie du système d'information et de communication.

B/ Confidentialité des paramètres d'accès

L'accès à certains éléments du SI (comme les sessions sur les postes de travail, le réseau, certaines applications ou certains services interactifs) est protégé par des paramètres de connexion (mots de passe et identifiants).

Ce sont des paramètres personnels à chaque utilisateur et doivent être gardés confidentiels. Ils permettent de contrôler l'activité des utilisateurs.

Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils seront à saisir à chaque accès et ne devront pas être conservés en mémoire dans le SI.

Le mot de passe à enregistrer doit respecter un certain degré de complexité et il sera à changer tous les 4 mois. Les consignes de sécurité sont élaborées par le service informatique afin de recommander les bonnes pratiques.

C/ Protection des ressources sous la responsabilité de l'utilisateur

L'entreprise met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du SI et de communication. A ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisions nécessaires à l'utilisation des ressources mises à disposition des utilisateurs.

Le service informatique est responsable du contrôle du bon fonctionnement du SI et de communication. Il veille à l'application des règles de la présente charte. Les membres du service informatique sont soumis au secret professionnel.

L'utilisateur est quant à lui est responsable des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit faire preuve de prudence.

En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel. Mais aussi en cas d'utilisation de matériel personnel, il appartient de veiller à l'utilisateur de veiller à la sécurité utilisé et à son innocuité.

L'utilisateur doit éviter d'installer des logiciels, de copier ou d'installer des fichiers susceptibles de créer des risques au sein de l'entreprise. Il doit dans tous les cas en alerter le service informatique.

L'utilisateur veille au respect de la confidentialité des informations en sa possession. Il doit en toutes circonstances veiller au respect de la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables. Il ne doit en aucun cas se livrer à une activité concurrente à celle de l'entreprise ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication.

D/ Accès à Internet

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par le < SERVICE INFORMATIQUE >. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites est interdite OU autorisée, sous réserve d'autorisation préalable du < SERVICE COMMUNICATION > OU autorisée. Un tel mode d'expression est susceptible d'engager la responsabilité de l'entreprise, une vigilance renforcée des utilisateurs est donc indispensable.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts de l'entreprise, y compris sur Internet.

E/ Données personnelles

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, définit les conditions dans lesquelles des traitements de données personnels peuvent être opérés. Elle institue au profit des personnes concernées par les traitements des droits que la présente invite à respecter, tant à l'égard des utilisateurs que des tiers.

Des traitements de données automatisés et manuels sont effectués dans le cadre des systèmes de contrôle, prévus dans la présente charte. Ils sont, en tant que de besoin, déclarés conformément à la loi du 6 janvier 1978. (Indiquer ici les traitements réalisés au sein de l'entreprise et les règles d'accès / modification / suppression)

Il est rappelé aux utilisateurs que les traitements de données à caractère personnel doivent être déclarés à la Commission nationale de l'informatique et des libertés, en vertu de la loi n° 78-17 du 6 janvier 1978. Les utilisateurs souhaitant réaliser des traitements relevant de ladite loi sont invités à prendre contact avec < CORRESPONDANT > avant d'y procéder.

F/ Contrôle des activités

F - 1 - Contrôles automatisés

Le système d'information et de communication s'appuie sur des fichiers journaux (" logs "), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'entreprise, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information. Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Sont notamment surveillées et conservées les données relatives :

- → à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications suppression de fichiers;
- → aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites web ou le

téléchargement de fichiers. L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

G/ Sanctions

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées la gravité des faits concernés.

Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un salarié, celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou événement particulier.

VIII. Information des salariés

La présente charte est affichée publiquement en annexe du règlement intérieur. Elle est communiquée individuellement à chaque salarié.

Le < SERVICE INFORMATIQUE > est à la disposition des salariés pour leur fournir toute information concernant l'utilisation des nouvelles technologies de l'information et de la communication (NTIC). Il informe les utilisateurs régulièrement sur l'évolution des limites techniques du système d'information et sur les menaces susceptibles de peser sur sa sécurité.

La présente charte et l'ensemble des règles techniques sont disponibles sur l'intranet de l'entreprise.

Des opérations de communication internes seront organisées, de manière régulière, afin d'informer les salariés sur les pratiques d'utilisation des NTIC recommandées.

Chaque utilisateur doit s'informer sur les techniques de sécurité et veiller à maintenir son niveau de connaissance en fonction de l'évolution technologique.

H/ Entrée en vigueur

La présente charte est applicable à compter du 25 mai 2019.