## PROJET VPN-IPSec nomade ASA5505

La situation professionnelle repose sur la mise en place d'un VPN nomade sur un Cisco asa5505.

Afin de réaliser cette situation, deux PC ainsi qu'un routeur Cisco 1841 et un pare-feu Cisco asas5505 fonctionnels sont utilisés. Nous avons aussi les logiciels Cisco ASDM et Cisco VPN-Client afin de mettre en place et d'utiliser le VPN nomade.



Le but du projet est de se connecter à partir de la machine 88.88.88.89 au réseau 192.168.1.0 via un tunnel VPN IPSec configuré sur le pare-feu ASA5505.

## 1) Configuration du tunnel VPN IPSec via ASDM

Dans ce tuto, on sous-entend que ASDM est déjà fonctionnel pour administrer le ASA5505( voir PROJET PARE-FEU ASA5505)

Commençons maintenant la configuration du Tunnel Vpn Ipsec. Accédez à Wizard > Ipsec VPN Wizard... .



On accède alors à cette fenêtre on nous demande le type de VPN Souhaité.

Site to Site est une configuration VPN destinée à sécuriser l'échange entre deux sites et deux réseaux entier, tandis que Remote Access est destinée aux travailleurs à distance qui souhaitent accéder, sécuriser, modifier le réseau d'un seul site.

VPN Wizard	<b>x</b>
VPN Wizard	VPN Tunnel Type (Step 1 of)
Branch	Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.
Home	VPN Tunnel Type: Site-to-Site VPN
Corporate Network	⊖ Site-to-site
	VPN Remote Access      Cocal     Remote     Remote
The The	VPN Tunnel Interface: outside 👻
	Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.
	< Back Next > Finish Cancel Help

## Nous utiliserons le Client VPN Cisco

付 VPN Wizard	X
VPN Wizard	Remote Access Client (Step 2 of)
Branch	Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.
EE ISP	VPN Client Type:
597 110	O Cisco VPN Client, Release 3.x or higher, or other Easy VPN Remote product
Home	Microsoft Windows client using L2TP over IPsec
Corporate	Specify the PPP authentication protocol. If a protocol is not specified on the remote client, do not specify it.
FILE JAN	PAP CHAP MS-CHAP-V1 MS-CHAP-V2 EAP-PROXY
	Specify if the dient will send tunnel group name as - username@tunnelgroup.
	Client will send tunnel group name as username@tunnelgroup.
TTTT	If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.
	< Back Next > Finish Cancel Help

Définition du mot de passe et du nom du tunnel pour établir la connexion.

🚰 VPN Wizard						
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)					
Branch Branch SP Branch Branch	The ASA allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote client. Authentication Method © Pre-shared key					
Corporate	Pre-Shared Key: password					
Network	Certificate					
The state	Certificate Signing Algorithm: rsa-sig					
	Certificate Name:					
Z-4441111	Challenge/response authentication (CRACK)					
The	Tunnel Group					
- I LI	Tunnel Group Name: VPNIP					
CA-						
	<back next=""> Finish Cancel Help</back>					

Utilisation du compte local, l'étape suivante en permet la création si elle n'a pas encore été faite.

付 VPN Wizard		2
VPN Wizard	Client Authentication (Step 4 of)	
Brandh Brandh F ISP Home Home	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step. To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below. To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window.	
Network	Authenticate using the local user database	
The state	Authenticate using an AAA server group	
	AAA Server Group Name: New	

On crée un utilisateur, ici VPNTEST et un mot de passe, ici password.

🔂 VPN Wizard			×
VPN Wizard	User Accounts (Step 5 of 11)		
Branch Branch	Add new users into the user authenticati or to remove them from the database, gr Users/AAA > User Accounts in the main <i>i</i>	on database. To edit existing e o to Configuration > Device Ma ASDM window.	entries in the database inagement >
Home	User to Be Added		
Corporate Network	Username:	root VPNTES	ſ
CINE IN	VPNTEST	Add >>	
A CONTRACTOR	Password (optional):	Delete	
- THUM			
TTTT	Confirm Password (optional):		
A			
		<back next=""> Finis</back>	h Cancel Help

#### Définition d'un POOL d'adresses pour les ou la connexions



DNS



👩 VPN Wizard



Enfin une fenêtre récapitulative de la configuration va apparaitre



### On peut voir que notre profile VPN a été créé

isco ASDM 7.1 for ASA - 192.168.1	254		B 10 51 (2)	a San Maria I		- 0
View Tools Wizards Winds	ow Help				Type topic to search Go	adral
Home R Configuration Mor	vitoring 🔚 Save 🔇 Refresh 🔇 Back	C Porward 💡 Help				CISC
note Access VPN d Q	Configuration > Remote Access VPII >	Network (Client) Access > IPsec(IKEv1) Connection Profi	PS			
troduction	Annual Table forms					
etwork (Client) Access	Foshie interfaces for IPsec access.					
AnyConnect Connection Profiles						
AnyConnect Client Profile	Interface A	low Access				
AnyConnect Client Software	inside	14 I				
Dynamic Access Policies		head .				
Psec(IKEy 1) Connection Profiles						
ecure Mobility Solution	The second second second second					
ddress Assignment	V Bypass interface access ists for indour	105 YPTY Sessions				
ess SSLVEN Arress	Access lists from group policy and user poli	cy always apply to the traffic.				
PN Remote	and the second se					
ocal Users	Connection Profiles					
e Desktop Manager	Connection profile (tunnel group) specifies	a how user is authenticated and other parameters. You can configu	e the mapping from certificate to connection profile here.			
age Localization	🗣 Add 🖪 Edit 📋 Delete					
Server	Nama	Ibra: Foshad	1779/JPres Enabled	Authantication Samar Group	Group Ballon	
	Defe dB AGroup	19 ACC 0 10000	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	1004	Difference	
ced	DefaultWEBVPNGroup	v	2	LOCAL	DfltGrpPolicy	
	VENEP			LOCAL	VPMIP	
, nice Setup						
note Access VPN						

Une dernière étape est nécessaire pour faire fonctionner le tunnel VPN IPSec sur le pare-feu asa5505 :

Crée la règle de NAT suivante :

G Cisco ASDM 7.1 for ASA - 192.168.	3.1.254						
File View Tools Wizards Wind	dow Help						
Home 🆧 Configuration 🔯 Mo	lonitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 F						
Firewall 과 무	Configuration > Firewall > NAT Rules						
Access Rules	🗣 Add 🗸 🎯 Edit 📋 Delete   🛧 🖌 🕌						
Service Policy Rules	Match Criteria: Original Packet						
	" Source Intf Dest Intf Source						
Public Servers	"Network Object" NAT (Rule 1)						
URL Filtering Servers	1 inside outside 📲 obj_any						
Objects							
🗄 🖟 Unified Communications							
🗄 📲 Advanced							
付 Add NAT Rule	×						
Match Criteria: Original Packet							
Source Interface: Any	Destination Interface: Any						
Source Address: any	Destination Address: any						
	any						
Action: Translated Packet							
Source NAT Type: Static	•						
Source Address: Original	Destination Address: Original						
Fall through to interface PAT	Service: Original						
Options							
✓ Enable rule							
Translate DNS replies that match this rule							
Direction: Both 🗸							
Description:							
ОК	Cancel Help						
L							

Voici la règle crée :

Firewall	a 4	Conf	iguration > F	irewall > NA	<u>T Rules</u>							
Access Rules			Add 👻 📝 Edit	👔 Delete	🛧 🗲   🐰 🖻 🏨 -   🔍 Find 🖭 Diagra	ım 🥂 Packet Trace						
C Service Policy Rules			Match Crite	eria: Original	Packet			Action: Translat	ed Packet		Ontions	Description
Filter Rules		·	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service	Options	Description
- B Public Servers		1	Any		🤣 any	🥎 any	🧇 any					
			Any	Any	🏟 any	🏟 any	🧼 any	Original (S)	Original	Original		
- Threat Detection		81	Network Object	"NAT (Rule 2)								
Objects		2	inside	outside	all obj_any	🏟 any	🌍 any	outside (P)	Original	Original		

## 2) CISCO VPN client

Remarque : Sous Windows 10 l'installation est plus particulière et nécessite quelques manipulations. Suivre le Tutoriel : <u>https://www.dominicdesbiens.com/articles/comment-installer-et-faire-fonctionner-le-client-faire-fonctionner-le-client-cisco-vpn-5-x-avec-windows-10.html</u>

## Sur CISCO VPN client, sélectionner nouveau :

👌 status: Dis	sconnected   \	VPN Client -	Version 5.0	.07.0440	
Entrées de co	onnexion Sta	tut Certific	ats Journal	l Options Aide	
Connecter	tin Nouveau	F 🗟 Importer	Modifier	Supprimer	ululu CISCO
Entrées de co	nnexion Ce	ertificats J	oumal		

Comme vous pouvez le voir il faut entrer les informations précédemment configurées sur le ASA5505.

Hôte : IP de l'interface outside de l'ASA5505.

Nom : « tunnel-group-name » configuré précédemment.

VPN Client   Propriétés de "VPNIP"							
Entrée de connexion : VPNIP Description : VPNIP CISCO							
Hôte : 192.168.2.1							
Authentification Transport Serveurs secondair	es Accès commuté						
Authentification du groupe     Aut	hentification Mutuel du groupe						
Nom : VPNIP							
Mot de passe :							
Confirmer mot de passe :							
C Authentification du certificat Nom : Envoyer la chaîne de certificat AC							
Effacer mot de passe utilisateur	Enregistrer Annuler						

Ensuite il suffit de se connecter au VPN précédemment ajouté :

Ø VPN CI	ient   Authentif	ication d'utili	sateur pour	"VPNIP"	×
Le serveu l'utilisateur	r requiert les inform	ations suivante	es pour compl	éter l'authe	entification de
diala cisco	Nom d'utilisateur : Mot de passe :	VPNTEST	ОК	_	Annuler

Une fois connecté au VPN, une nouvelle carte réseau est activée et une adresse du VPN pool lui a été attribuée :

Connexion au réseau local Réseau 10 Realtek PCIe GBE Family Contre Connexion au réseau local 5 Activé Cisco Systems VPN Adapter for	oller Connexion au réseau local 2 Désactivé Realtek PCI GBE Family Controller <b>loopback</b> Désactivé Carte de bouclage Microsoft	Connexion au réseau local 3 Désactivé TAP-Windows Adapter V9 VirtualBox Host-Only Network Activé VirtualBox Host-Only Ethernet Ad
<ul> <li>Propriétés de Connexion au réseau los</li> <li>Gestion de réseau</li> <li>Partage</li> </ul>	cal 5 🔀	
Général Les paramètres IP peuvent être dé réseau le permet. Sinon, vous deve appropriés à votre administrateur r Obtenir une adresse IP autom Obtenir une adresse IP autom Obtenir une adresse IP suivante : Adresse IP : Masque de sous-réseau :	ersion 4 (TCP/IPv4)	
Passerelle par défaut : Obtenir les adresses des servi- Ottiliser l'adresse de serveur Di Serveur DNS préféré : Serveur DNS auxiliaire : Valider les paramètres en qui	192.168.1.1         eurs DNS automatiquement         NS suivante :         8.8.8.8         4.2.2.2         ttant	
	OK Annuler	

# 3) TEST du tunnel VPN

Afin de tester que la connexion VPN est bien établie, on test de joindre un serveur web en 192.168.1.106 et on test de ping la machine en 192.186.1.54 :



bonjour sisr 192.168.1.106

C:\Users\etudiantsio>ping 192.168.1.54 Envoi d'une requête 'Ping' 192.168.1.54 avec 32 octets de données : Réponse de 192.168.1.54 : octets=32 temps=2 ms TTL=128 Réponse de 192.168.1.54 : octets=32 temps=1 ms TTL=128 Réponse de 192.168.1.54 : octets=32 temps=1 ms TTL=128 Réponse de 192.168.1.54 : octets=32 temps=1 ms TTL=128 Statistiques Ping pour 192.168.1.54: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), Durée approximative des boucles en millisecondes : Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms C:\Users\etudiantsio>

On voit que la communication s'effectue bien.