### PROJET PARE-FEU ASA5505

La situation professionnelle repose sur la mise en place d'un pare-feu Cisco asa5505 entre deux réseaux distincts dans le but de les interconnecter comme dans le schéma ci-dessous :



Afin de réaliser cette situation, deux PC ainsi qu'un routeur Cisco 1841 et un pare-feu Cisco asas5505 sont utilisés. Nous avons aussi les logiciels Cisco ASDM et Putty afin d'administrer le routeur et le pare-feu.

### 1) Configuration du routeur :

Dans un premier temps on configure les deux interfaces du routeur comme dans le schéma :



## 2) Configuration du ASA5505

Etape 1: Configurer l'interface vlan inside : ASA5505 (config) # interface vlan 1 ASA5505 (config-if) # nameif inside ASA5505 (config-if) # security level 100 ASA5505 (config-if) # ip address 192.168.1.254 255.255.255.0 ASA5505 (config-if) # no shut

#### **BECQUET Jean-Baptiste**

Etape 2: Configurer l'interface vlan outside : ASA5505 (config) # interface vlan 2 ASA5505 (config-if) # nameif outside ASA5505 (config-if) # security level 0 ASA5505 (config-if) # ip address 192.168.2.1 255.255.255.0 ASA5505 (config-if) # no shut

Etape 3: Attribuer Ethernet 0/0 au VLAN 2 : ASA5505 (config) # interface ethernet0/0 ASA5505 (config-if) # switchport access vlan 2 ASA5505 (config-if) # no shut

Etape 4: Activez les interfaces de repos sans arrêt : ASA5505 (config) # interface ethernet0/1 ASA5505 (config-if) # no shut Faites de même pour ethernet0 / 1 à 0/7.

Etape 5: Configurez route par défaut vers l'extérieur : ASA5505 (config) # route outside 0.0.0.0 0.0.0.0 192.168.2.1 1

Le ASA5505 est donc configurer ainsi :

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.254 255.255.255.0
!
interface Vlan2
nameif outside
security-level 0
ip address 192.168.2.1 255.255.255.0
object network obj_any
nat (inside,outside) dynamic interface
route outside 0.0.0.0 0.0.0.0 192.168.2.1 1
```

**BECQUET** Jean-Baptiste

## 3) Installation CISCO ASDM :

On utilise CISCO ASDM afin d'administrer le ASA5505 via une interface graphique.

Etapes 1: Crée un utilisateur en ligne de commande sur le ASA :

ASA5505 (config-if) # username root password root privilege 15

Ici le login est root le mot de passe est root et l'utilisateur possède tous les droits.

Etapes2 : Installer ASDM :

(On sous-entend que java est installer sur le poste)

Via le navigateur Mozilla, il vous faut accéder à l'adresse de l'interface inside en https.

Ici : <u>https://192.168.1.254/</u>

A Connexion non sécurisée	× +		
(i) https://192.168.1.254		C Recherche	〃 ☆ 自 ♣
	La connevion n'est na	s sécurisée	
		s securisee	
	Les propriétaires de 192.168.1.254 ont mal configure Firefox ne s'est pas connecté à ce site web.	é leur site web. Pour éviter que vo	s données ne soient dérobées,
	En savoir plus		
	Retour		Avancé

Il faut ensuite ajouter une exception a Mozilla pour accéder à la page et cliquer sur « run asdm » :

🕑 🛅 🛈 🐔   https://192.168.1.254/adm	n/public/index.html v d	Rechercher
	Gisco ASDM 7.1(2)	cisco
	Cisco ASDM 7.1(2) provides an intuitive graphical user interface th configure and manage your Cisco security appliances.	iat makes it easy to set up,
	Cisco ASDM can run as a local application or as a Java Web Start :	application.
	Run Cisco ASDM as a local application	
	When you run Cisco ASDM as a local application, it connects to your so desktop using SSL. Running Cisco ASDM as an application has these a	acurity appliance from your dvantages:
	You can invoke ASDM from a desktop shortcut. No browser is r     One desktop shortcut allows you to connect to <i>multiple</i> security	equired. appliances.
	Install ASDM Launcher	
	Run Cisco ASDM as a Java Web Start application	
	<ul> <li>Click <i>Run ASDM</i> to run Cisco ASDM.</li> <li>Click <i>Run Startup Wizard</i> to run the Startup Wizard. The Status step by step, the initial configuration of your security appliance.</li> </ul>	tup Wizard walks you through,
	Run ASDM Run	Startup Wizard
	Copyright © 2006-2012 Cisco Systems, Inc. All righ	its reserved.

#### Puis ajouter une exception à java :





Enfin, cliquez sur lancer l'exécutable télécharger et suivez les instructions :

Avertisse	ement de s	écurité				X
Vou La co	l <b>lez-vou</b> s onnexion à	s continuer ce site Web n	? 'est pas sécurisée.			
	$\land$	Site Web	: https://192.168.1.	254:443		
Rema	<b>arque :</b> le Plu	e certificat n'est pa s d'informations	as valide et ne permet j	pas de vérifier l'ide	ntité de ce site Web	
					Continuer	Annuler
Avertissem	ent de sécur	ité			X	J
Voule	z-vous ex	cécuter l'appl	lication ?			
Voule	z-vous ex	xécuter l'appl Nom :	lication ? com.cisco.launc	her.Launcher		
Voule	z-vous e>	cécuter l'appl Nom : Editeur :	lication ? com.cisco.launc	her.Launcher		
Voule	z-vous ex	cécuter l'appl Nom : Editeur : Emplacement :	lication ? com.cisco.launc Cisco Systems https://192.168.1.254	her.Launcher		
Voule:	z-vous ex	cécuter l'appl Nom : Editeur : Emplacement : <b>2tte applicatio</b> r	lication ? com.cisco.launc Cisco Systems https://192.168.1.254 a peut représenter	her.Launcher un risque de sé	curité	
Voule L'exécu Risque	z-vous ex votion de ce : cette applii votre ordina sont inconnu connaissiez l	xécuter l'appl Nom : Editeur : Emplacement : ette application cation sera exécuté teur et vos informal ues. Il est donc reco a source.	lication ? com.cisco.launce Cisco Systems https://192.168.1.254 a peut représenter te sans restriction d'accès, tions personnelles, Les informandé de ne pas exécut	her.Launcher un risque de sé ce qui peut représen rmations fournies ne er cette application à	curité ter un risque pour sont pas fiables ou moins que vous n'en	
Voule	z-vous ex voite of the applin voite of the applin	xécuter l'appl Nom : Editeur : Emplacement : Ette application cation sera exécuté teur et vos informan a source. le garantir que le ce lations	lication ? com.cisco.launce Cisco Systems https://192.168.1.254 a peut représenter te sans restriction d'accès, tions personnelles. Les info mmandé de ne pas exécut rtificat utilisé pour identifie	her.Launcher un risque de sé ce qui peut représen rmations fournies ne er cette application à r cette application n	curité ter un risque pour sont pas fiables ou moins que vous n'en a pas été révoqué.	
Voule L'exéct Risque Cochez	z-vous ex ution de ce : cette applia votre ordina sont inconnu connaissiez I Impossible d Plus d'inform la case ci-de	cécuter l'appl Nom : Editeur : Emplacement : Ette application cation sera exécuté teur et vos informan es. Il est donc reco a source. e garantir que le ce lations essous, puis cliqu	lication ? com.cisco.launce Cisco Systems https://192.168.1.254 a peut représenter 1 e sans restriction d'accès, tions personnelles. Les info mmandé de ne pas exécut rtificat utilisé pour identifie ez sur Exécuter pour d	her.Launcher un risque de sé ce qui peut représen rmations fournies ne er cette application à r cette application n' émarrer l'applicat	curité ter un risque pour sont pas fiables ou moins que vous n'en a pas été révoqué. ion	

📴 Cisco AS	DM-IDM Launcher v1.5(56)	
	Cisco ASDM-IDM Launcher	cisco
Enter usern	ame and password for 192.168.1.254	
Password:	••••	
	OK Close	👙   🔒



(Un raccourci sera créé sur le bureau

**BECQUET** Jean-Baptiste

Une fois connecter avec l'utilisateur créé precedement cette interface devrais apparaitre :

Gisco ASDM 7.1 for ASA - 192.168.1.254	8 41 No. 6 x	Trans Trade Vol. and The	Later Mark	
File View Tools Wizards Window Help			1	<u> </u>
🔥 Home 🖓 Configuration 📴 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🧳 Help				CISCO
Home				
Burvice Dashboard 🔞 Firewall Dashboard				
Device Information	Interface Status			
General License	Interface IP Address/Mask	Line	Link	Kbps
Host Name: ciscoasa	inside 192.168.1.254/24	<b>9</b> up	O up	8
ASA Version: 8.3(1) Device Uptime: 5d 23h 4m 0s	outside 192.166.2.1/24	Up Up	O up	0
ASDM Version: 7.1(2) Device Type: ASA 5505				
Total Flash: 128 MB Total Memory: 512 MB				
	Select an interface to view input and output Kbps			
VPN Sessions	Failover Status			
IPsec: 0 Clientiess SSL VPII: 0 AnyConnect Client: 0 Details	Falover not configured. Click the link to configure it.			Configure
System Resources Status	Traffic Status			
CPU Usage (percent)	Connections Per Second Usage			
	0 1161 1162 1163 1163 1163 1163	1163	11:54	1155
Memory Usage (MB)	outside' Interface Traffic Usage (Kbos)			
00 40 40 30 30 10 10 10 10 10 10 10 10 10 1				• • • •
115506 1151 1152 1153 1154 1155	11:51 11:52	11:53	11:54	11.95
Detals				
Latest ASDM System Messages				
Severity Date Time Systex ID Source IP Source Destination IP Destina Description				
▲ 6 Jun 06 2017 11:55:39 302015 192.168.1.54 54395 8.8.4.4 53 Built outbound UCP connection 22486 for outside:8.8.4.4/53 (8.8.4.4/53) to insi	ie: 192. 168. 1. 54/54395 (192. 168. 1. 54/54395)			A 🖬
▲ 6 Jun 06 2017 11:55:37 302015 192.168.1.54 53773 8.8.4.4 53 Bull autbound UDP connection 22485 for autside:8.8.4.4/53 (8.8.4.4/53) to insi	le: 192. 168. 1.54/53773 (192. 168. 1.54/53773)			E 32
▲ 6 Jun 06 2017 11:55:37 302015 192.168.1.54 54395 8.8.88 53 Built outbound UDP connection 22484 for outside:8.8.8.8/53 (8.8.8.8/53) to insi				
🛦 6 Jun 06 2017 11:55:35 302015 192.168.1.54 53773 8.8.8.8 53 Built outbound UDP connection 22483 for outside:8.8.8.8/53 (8.8.8.8/53) to insi	le: 192. 168. 1. 54/54395 (192. 168. 1. 54/54395) le: 192. 168. 1. 54/53773 (192. 168. 1. 54/53773)			-

On peut vérifier dans l'onglet configuration les paramètres des interfaces ainsi que les ACL et le NAT automatiquement créé :

🚯 Home 🕰 Configuration 📴 Monitoring 🔚 Save 🔇 Refresh 🕤 Back 🕥 Forward 🦻 Help																
Device Setup	6	ф 🛛	Configur	ation > Device Set	up > Interface	<u>es</u>										
Startup Wizard			Interfac	es Switch Ports												
++++ Routing			Name	Switch Ports		Enabled	Security Level	IP Ade	dress		Subnet M Prefix Le	4ask ngth	Restri Traffic	ict flow	Backup Interface	VLAN
Route Maps			inside	Ethernet0/1, Et	hernet0/2, Et	Yes	100	192.16	58.1.254		255.255.	255.0				vlan 1
Pretix Rules			outside	e Ethernet0/0		Yes	C	192.16	58.2.1		255.255.	255.0				vlan2
Firewall		Configu	ration > Fi	rewall > Access Pules												
Red Access Dulos		comqu		ICHUI > PROCESS RUICS												
NAT Rules		💠 Add	🝷 📝 Edit	📋 Delete   🛧 🗲   🐰	, h 🛍 -   Q, F	Find 📴 Diagra	am 調 Export	- <b>()</b>	lear Hits 📗	Show Lo	ig 💐 Packi	et Trace				
Q Service Policy Rules				Source Criteria:	Destination Cr	iteria:										
AAA Rules		#	Enabled	Source	Destination		Service		Action	Hits	Logging	Time	Description			
Public Servers			ocido (1 impli	sit incoming rulo)	DEDUNDUN											
URL Filtering Servers			iside (1 impli	at incoming rate)	Any less secu	re petworks	TR. in		A Dormit				Implicit rule:	Permit all t	raffic to less secure	networks
Threat Detection			uteida (0 imr	licit incoming rules)	Arry less secu	I E HELWOIKS	<u>⊥e</u> ∕ ip		• Fernit				Implicit Fulc.	. r crinic dir c	runne to leas secure	- Hethorka
🕀 🔯 Objects			lobal (1 impli	icit rule)												
🗈 🙀 Unified Communications				any	iany		TP, in		C Denv				Implicit rule			
Image: Book of the second		-		- uny	- uny		<u> </u>		U Deny							
Firewall 과 무	Configu	ration > Fi	rewall > NAT	Rules												
Access Rules	🗣 Add	🔹 💕 Edit	💼 Delete   🗧	r ↓   3 h m m -   q n	nd 🔛 Diagram 🛲 Pa	cket Trace										
Q. Service Policy Rules	M	Match Criteria: Original Packet Action: Translated Packet														
Deg Filter Rules	" So	urce Intf	Dest Intf	Source	Destinat	ion		Service	Sou	irce	Destinatio	n S	ervice	opuons	Description	
- Dublic Servers	Network	ork Object"	NAT (Rule 1)													
URL Filtering Servers	1 ins	de	outside g	obj_any	🎱 any			🥥 any		outside (P)	Original		Original			

# 4) TEST de l'interconnexion des réseaux :

Pour finir, afin de tester la connexion entre les réseaux 192.168.1.0 et 88.88.88.0, j'ai installé un serveur web sur une machine qui a pour adresse 88.88.89.0 sur le réseau 88.88.88.0 et je tente d'y accéder via le pc sur le réseau interne qui a pour adresse 192.168.1.54

88.88.88.90						
$\leftarrow \rightarrow$ C $\triangle$	③ 88.88.88.90					
📙 Importés depuis Firefo	Cisco ASA - Remote A MR *How To* Configure a D How to enable Port					
bonjour sisr 88.88.88.9	0					
👞 Administrateur : C:\Windo	ws\system32\cmd.exe					
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés. C:\Users\etudiantsio>ipconig 'ipconig' n'est pas reconnu en tant que commande interne ou externe, un programme exécutable ou un fichier de commandes. C:\Users\etudiantsio>ipconfig Configuration IP de Windows						
Carte Ethernet Conne Suffixe DNS propr Adresse IPv6 de 1 Adresse IPv4 Masque de sous-ré Passerelle par dé	xion au réseau local : e à la connexion iaison locale fe80::f8ca:5629:d938:1a1a%11 192.168.1.54 seau 255.255.255.0 faut					