



INF8402
Sécurité des réseaux fixes et mobiles
Groupe 1

Lab1 – Analyse d'informations par Wireshark et
introduction à ASA

Soumis à : [REDACTED]

[REDACTED]
Le 18 septembre 2024

Poste de travail : 20

2.2.2 Exploration de votre environnement (5 points)

Q1 Il y a 4 interfaces réseaux

```
X:\>ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : L4708-20
Suffixe DNS principal . . . . . : gigl.polymtl.ca
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS : gigl.polymtl.ca
gi.polymtl.ca

Carte Ethernet Ethernet :

Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . :
Description. . . . . : Intel(R) PRO/1000 GT Desktop Adapter
Adresse physique . . . . . : 90-E2-BA-49-F6-17
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui

Carte Ethernet Ethernet 4 :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : VMware Virtual Ethernet Adapter for VMnet1
Adresse physique . . . . . : 00-50-56-C0-00-01
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::3cd3:5321:cc89:fc1d%4(préfééré)
Adresse IPv4. . . . . : 192.168.254.1(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . :
IAID DHCPv6 . . . . . : 167792726
DUID de client DHCPv6. . . . . : 00-01-00-01-2E-32-65-50-90-E2-BA-49-F6-17
NetBIOS sur Tcpip. . . . . : Activé

Carte Ethernet Ethernet 3 :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : VMware Virtual Ethernet Adapter for VMnet8
Adresse physique . . . . . : 00-50-56-C0-00-08
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::70ae:9b5a:2e05:8790%3(préfééré)
Adresse IPv4. . . . . : 192.168.142.1(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : 27 août 2024 01:14:45
Bail expirant. . . . . : 1 septembre 2024 13:45:16
Passerelle par défaut. . . . . :
Serveur DHCP . . . . . : 192.168.142.254
IAID DHCPv6 . . . . . : 184569942
DUID de client DHCPv6. . . . . : 00-01-00-01-2E-32-65-50-90-E2-BA-49-F6-17
Serveur WINS principal . . . . . : 192.168.142.2
NetBIOS sur Tcpip. . . . . : Activé

Carte Ethernet Ethernet 2 :

Suffixe DNS propre à la connexion. . . : gigl.polymtl.ca
Description. . . . . : Intel(R) Ethernet Connection (11) I219-LM
Adresse physique . . . . . : FC-34-97-BF-A5-B2
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::d2c5:3ba4:874a:ba18%8(préfééré)
Adresse IPv4. . . . . : 132.207.29.120(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : 27 août 2024 01:14:45
Bail expirant. . . . . : 2 septembre 2024 01:14:07
Passerelle par défaut. . . . . : 132.207.29.1
Serveur DHCP . . . . . : 132.207.180.12
IAID DHCPv6 . . . . . : 217855127
DUID de client DHCPv6. . . . . : 00-01-00-01-2E-32-65-50-90-E2-BA-49-F6-17
Serveurs DNS. . . . . : 132.207.185.70
                        132.207.185.73
                        132.207.180.14
                        132.207.144.2
                        132.207.144.3
Serveur WINS principal . . . . . : 132.207.180.14
NetBIOS sur Tcpip. . . . . : Activé
Liste de recherche de suffixes DNS propres à la connexion :
gigl.polymtl.ca
gi.polymtl.ca
```

Figure 1.1 : Interfaces réseau

Q2) Quels sont les paramètres réseau de la carte Intel I217-V : (0.5 point)

a) ASUSTek COMPUTER INC

FC-34-97	(hex)	ASUSTek COMPUTER INC.
FC3497	(base 16)	ASUSTek COMPUTER INC.
		15, Li-Te Rd., Peitou, Taipei 112, Taiwan
		Taipei Taiwan 112
		TW

Figure 2.1 : Fabricant de la carte réseau

b) Adresse IP : 132.207.29.120 (voir figure 1.1)

c) Masque réseau : 255.255.255.0 (voir figure 1.1)

d) Lorsque le client vient de se connecter au réseau il émet une requête à tous les périphériques connectés au réseau et c'est le serveur DHCP qui lui répond avec une adresse IP

e) Adresse IPv6 : fe80::d2c5:3ba4:874a:ba18%8 (voir figure 1.1)

f) Serveur DHCP : 132.207.180.12 (voir figure 1.1)

g) Serveur DNS : 132.207.185.70 (voir figure 1.1)

h) Serveur WINS : 132.207.180.14 (voir figure 1.1)

Q3) Un serveur WINS (Windows Internet Name Service) est un service utilisé dans les réseaux Microsoft pour résoudre les noms NetBIOS (Network Basic Input/Output System) en adresses IP. La différence avec DNS est que le serveur WINS est utilisé uniquement dans le réseau LAN Microsoft pour résoudre les noms NetBIOS alors que le serveur DNS peut être utilisé dans tous les réseaux pour résoudre les noms de domaine en IP.

Q4) Connectivité : il y a connectivité entre tous les ordinateurs

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:2a:59:03
          inet addr:192.168.142.134  Bcast:192.168.142.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe2a:5903/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:725 errors:0 dropped:0 overruns:0 frame:0
          TX packets:131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:51148 (49.9 KB)  TX bytes:15544 (15.1 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:285 errors:0 dropped:0 overruns:0 frame:0
          TX packets:285 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:107649 (105.1 KB)  TX bytes:107649 (105.1 KB)

msfadmin@metasploitable:~$ ping 192.168.142.135
PING 192.168.142.135 (192.168.142.135) 56(84) bytes of data.
64 bytes from 192.168.142.135: icmp_seq=1 ttl=128 time=0.369 ms
64 bytes from 192.168.142.135: icmp_seq=2 ttl=128 time=0.401 ms
_
```

Figure 4.1 : IP + ping sur la VM Metasploitable2

```
C:\Users\GIGL>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-NK77LRQ
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain


Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-6C-34-87
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b812:9699:9457:b21e%7(Preferred)
IPv4 Address. . . . . : 192.168.142.135(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 1 septembre 2024 13:29:12
Lease Expires . . . . . : 1 septembre 2024 14:14:12
Default Gateway . . . . . : 192.168.142.2
DHCP Server . . . . . : 192.168.142.254
DHCPv6 IAID . . . . . : 50334761
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-66-5B-AF-00-0C-29-6C-34-87
DNS Servers . . . . . : 192.168.142.2
Primary WINS Server . . . . . : 192.168.142.2
NetBIOS over Tcpip. . . . . : Enabled


Tunnel adapter isatap.localdomain:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : localdomain
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes


C:\Users\GIGL>ping 192.168.142.134

Pinging 192.168.142.134 with 32 bytes of data:
Reply from 192.168.142.134: bytes=32 time<1ms TTL=64
Reply from 192.168.142.134: bytes=32 time<1ms TTL=64
Reply from 192.168.142.134: bytes=32 time<1ms TTL=64
Reply from 192.168.142.134: bytes=32 time<1ms TTL=64
```

Figure 4.2 : IP + ping sur la VM Windows 10

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.142.136 netmask 255.255.255.0 broadcast 192.168.142.255
      inet6 fe80::20c:29ff:fe2a:5903/64 scopeid 0x20<link>
      ether 00:0c:29:2a:59:03 txqueuelen 1000 (Ethernet)
      RX packets 38 bytes 3168 (3.0 KiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 274 bytes 16965 (16.5 KiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1000 (Local Loopback)
      RX packets 273 bytes 26188 (25.5 KiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 273 bytes 26188 (25.5 KiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# ping 192.168.142.135
PING 192.168.142.135 (192.168.142.135) 56(84) bytes of data.
64 bytes from 192.168.142.135: icmp_seq=1 ttl=128 time=0.899 ms
64 bytes from 192.168.142.135: icmp_seq=2 ttl=128 time=0.462 ms
64 bytes from 192.168.142.135: icmp_seq=3 ttl=128 time=0.419 ms
64 bytes from 192.168.142.135: icmp_seq=4 ttl=128 time=0.454 ms
^C
--- 192.168.142.135 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3055ms
rtt min/avg/max/mdev = 0.419/0.558/0.899/0.198 ms
root@kali:~# ping 192.168.142.134
PING 192.168.142.134 (192.168.142.134) 56(84) bytes of data.
64 bytes from 192.168.142.134: icmp_seq=1 ttl=64 time=0.751 ms
64 bytes from 192.168.142.134: icmp_seq=2 ttl=64 time=0.401 ms
64 bytes from 192.168.142.134: icmp_seq=3 ttl=64 time=0.420 ms
^C
--- 192.168.142.134 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2055ms
rtt min/avg/max/mdev = 0.401/0.524/0.751/0.160 ms
root@kali:~#
```

Figure 4.3 : IP + ping sur la VM Kali

Q5) Il y a connectivité

Q6)

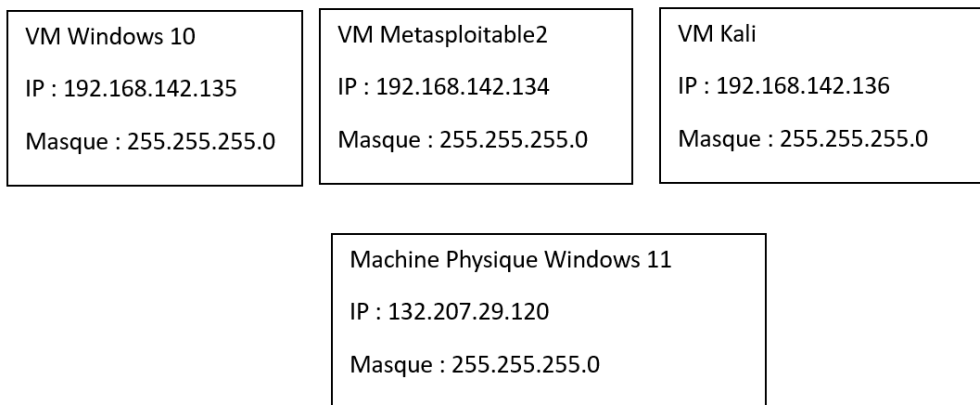


Figure 6.1 : Diagramme de la configuration

2.3 TCP/UDP

Q7) On peut voir cette connexion car l'analyseur a placé l'interface en mode Promiscuous et dans ce mode on est capable de capturer tout le trafic réseau même s'il ne nous est pas destiné. Également les cartes réseaux des VM ont été configurées en mode bridge ce qui crée un LAN entre elles d'où le fait qu'elle puissent communiquer entre elles et puisque l'analyseur est sur le même réseau, il peut intercepter toutes les communications entre les machines.

Q8) Couches OSI

La couche 4 : Transport : le protocole utilisé est ICMP

La couche 3 : Réseau : on a l'adresse IP source et de destination

La couche 2 : Liaison : on a les adresses MAC source et de destination

La couche 1 : Physique : transmission binaire sous forme de signal numérique ou analogique

No.	Time	Source	Destination	Protocol	Length	Info
→	1 0.000000000	192.168.142.1	192.168.142.134	ICMP	74	Echo (ping) request id=0x0001, seq=2257/53512, ttl=128 (reply in 2)
←	2 0.000101587	192.168.142.134	192.168.142.1	ICMP	74	Echo (ping) reply id=0x0001, seq=2257/53512, ttl=64 (request in 1)
→	3 1.010049147	192.168.142.1	192.168.142.134	TCP	74	Echo (ping) request id=0x0001, seq=2257/53512, ttl=128 (reply in 1)
▶ Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0						
▶ Ethernet II, Src: Vmware_2a:59:03 (00:0c:29:2a:59:03), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)						
▶ Internet Protocol Version 4, Src: 192.168.142.134, Dst: 192.168.142.1						
▶ Internet Control Message Protocol						

Figure 8.1 : Paquet Wireshark

Q9) Comme on peut le voir sur la capture ci-dessous, FTP transfère les informations en clair c'est-à-dire sans les crypter ou les chiffrer c'est la raison pour laquelle en suivant la trace des paquets FTP on a pu obtenir le nom d'utilisateur et le mot de passe de l'utilisateur initiant la connexion. On conclut donc que c'est un protocole peu sécurisé car les données ne sont pas chiffrées.

```
Wireshark · Follow TCP Stream (tcp.stream eq 42) · wireshark_eth0_20240906200733_xG0TVN

220 (vsFTPd 2.3.4)
AUTH TLS
530 Please login with USER and PASS.
AUTH SSL
530 Please login with USER and PASS.
USER msfadmin
331 Please specify the password.
PASS msfadmin
230 Login successful.
```

Figure 9.1 : Trace FTP

Q10) Oui on peut intercepter et voir l'image même

Cette capture montre qu'une image a bien été transmise entre les 2 machines

```
STOR Capture.PNG
150 Ok to send data.
226 Transfer complete.
PASS
```

Figure 10.1 : Image envoyée

Pour reconstituer l'image il faut suivre les étapes suivantes :

1. Sélectionner un paquet FTP-DATA -> faire follow ensuite TCP Stream

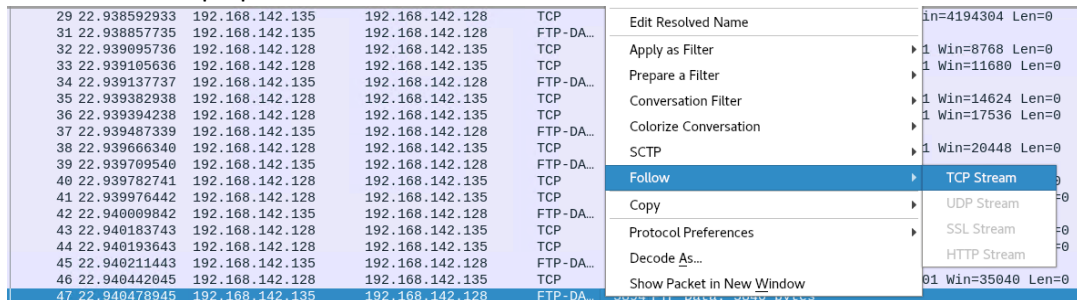


Figure 10.2 : Étape 1

2. Sélectionner Raw dans la nouvelle fenêtre et enregistrer

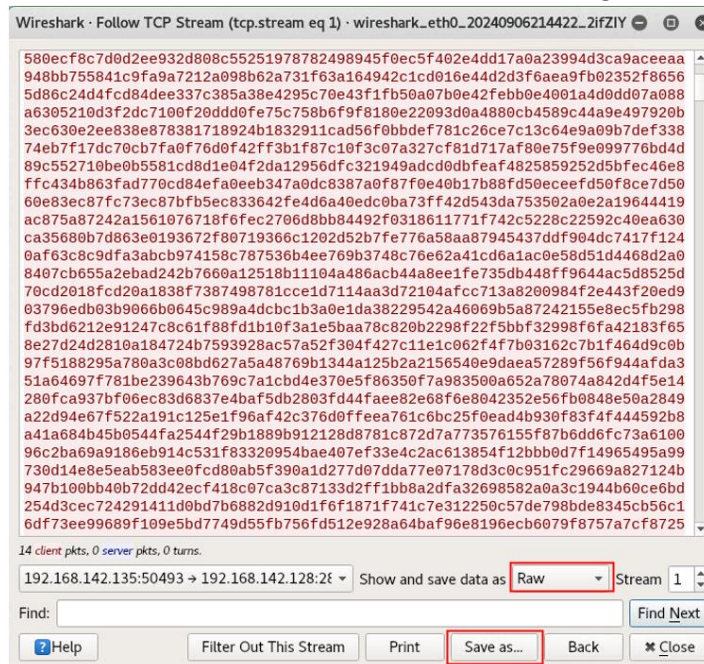


Figure 10.3 : Étape 2.1

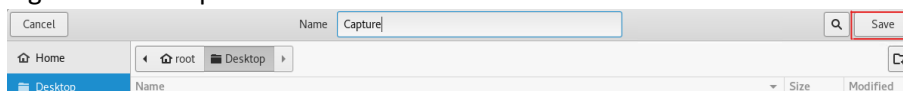


Figure 10.4 : Étape 2.2

3. On obtient l'image envoyée



Figure 10.5 : Image envoyée

2.5 SFTP

Q11) L'empreinte digitale permet de confirmer l'identité du serveur et de s'assurer qu'on ne se connecte pas à un serveur malveillant.

Q12) Étant donné que SFTP est une connexion sécurisée on ne peut pas lire directement les informations d'authentification ou même les données envoyées dans Wireshark on peut cependant obtenir les informations suivantes :

- La version de ssh : SSH-2.0-FileZilla_3.34.0
- Les algorithmes d'échange de clés : ecdh-sha2-nistp256
- Les algorithmes d'encryption : aes256-ctr

```
SSH-2.0-FileZilla_3.34.0
.....}...;....Y.m)z.....curve25519-sha256@libssh.org,ecdh-sha2-
nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-
exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-
sha1,rsa2048-sha256,rsa1024-sha1,diffie-hellman-group1-sha1...Wssh-
ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-
rsa,ssh-dss...aes256-gcm@openssh.com,aes256-ctr,aes256-cbc,rijndael-
cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-gcm@openssh.com,aes128-
ctr,aes128-cbc,chacha20-poly1305@openssh.com,blowfish-ctr,blowfish-cbc,
3des-ctr,3des-cbc,arcfour256,arcfour128...aes256-gcm@openssh.com,aes256-
ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-
gcm@openssh.com,aes128-ctr,aes128-cbc,chacha20-
poly1305@openssh.com,blowfish-ctr,blowfish-cbc,3des-ctr,3des-
cbc,arcfour256,arcfour128...hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-
md5,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha1-96-
etm@openssh.com,hmac-md5-etm@openssh.com...hmac-sha2-256,hmac-sha1,hmac-
sha1-96,hmac-md5,hmac-sha2-256-etm@openssh.com,hmac-sha1-
```

Figure 12.1 : Paquets enregistrés dans Wireshark après un échange SFTP

Q13) Je peux utiliser Wireshark pour effectuer la surveillance du trafic réseau et ainsi identifier toutes les communications non chiffrées afin d'apporter les changements adéquats et mieux sécuriser le réseau.

Q14) Dans des conditions où les configurations sont correctement effectuées et les outils sont tous à jour, il n'est pas possible d'intercepter l'image car la connexion est encryptée. Un hacker pourra écouter les informations transmises avec Wireshark mais étant donné que la connexion est cryptée, il ne sera pas en mesure de la décrypter.

3.2 Informations générales et tableau de bord des ASA

Q15)

Le modèle d'ASA est : ASA 5520

La version de ASA est : 8.4(2)

La type de licence est : VPN Plus



Figure 15.1 : Informations générales sur ASA

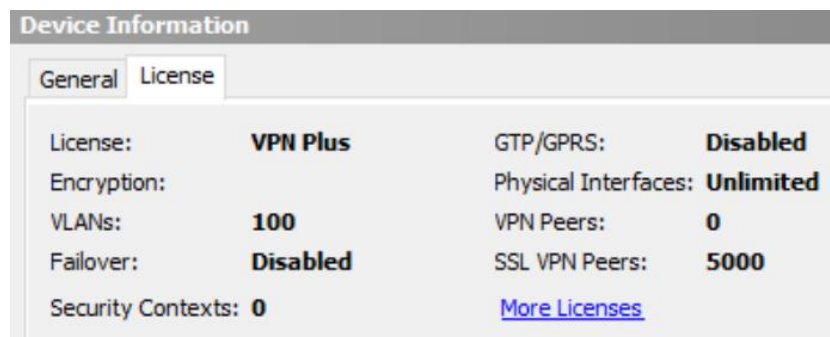


Figure 15.2 : Licence de l'ASA

Q16) ASA est un dispositif de sécurité qui combine plusieurs fonctionnalités essentielles pour protéger les réseaux d'entreprise. En effet, il joue à la fois le rôle de pare feu et de VPN, offrant ainsi une protection complète contre les menaces internes et externes en filtrant le trafic.

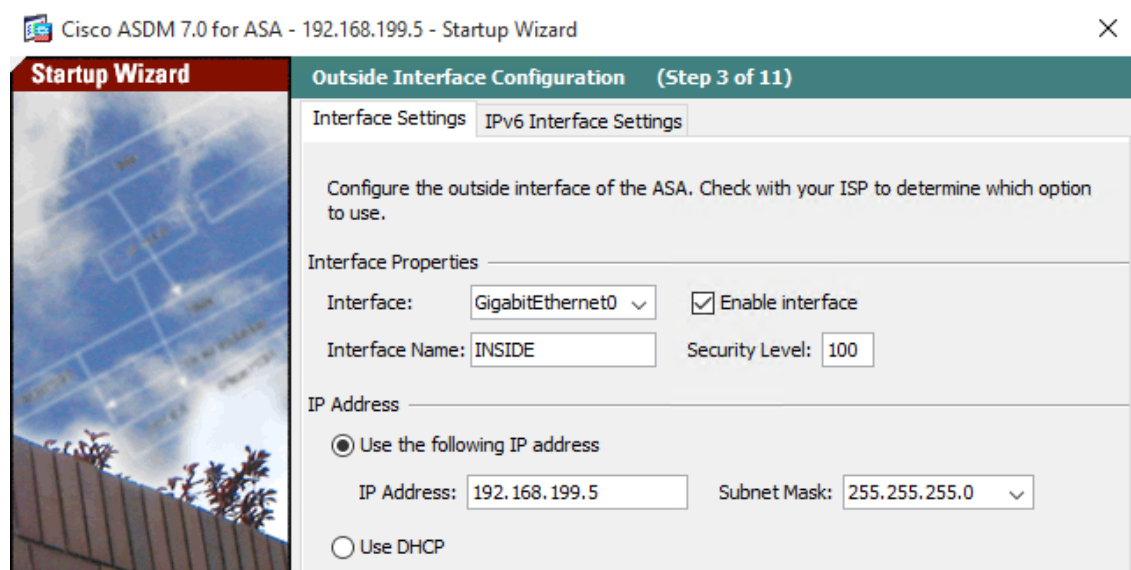
Q17) Il y a 3 interfaces présentes sur l'ASA dont une qui est configurée et son nom est GigabitEthernet0 avec une zone de nom INSIDE. Selon la licence du ASA que nous avons, on peut avoir jusqu'à 100 interfaces/zones (100 VLANs possibles) (Voir la figure 15.2).

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	Group	Type
GigabitEthernet0	INSIDE	Enabled	0	192.168.199.5	255.255.255.0		Hardware
GigabitEthernet1		Disabled					Hardware
GigabitEthernet2		Disabled					Hardware

Figure 17.1 : Interface ASA

3.3 Assistants (Wizards)

Q18) Le niveau de sécurité est une valeur numérique comprise entre 0 et 100 qui détermine le degré de confiance accordé à cette interface par rapport aux autres ce qui reflète le niveau de sécurité du réseau d'où proviennent les paquets traversant l'interface. Plus le nombre est élevé plus le niveau de confiance est élevé. INSIDE est à 100, car c'est le réseau interne et il est considéré comme sécuritaire alors que l'interface OUTSIDE est à 0, car les paquets qui y passent proviennent d'internet qui est un réseau moins sécuritaire, car tout le monde y a accès.



Cisco ASDM 7.0 for ASA - 192.168.199.5 - Startup Wizard

Startup Wizard

Outside Interface Configuration (Step 3 of 11)

Interface Settings | IPv6 Interface Settings

Configure the outside interface of the ASA. Check with your ISP to determine which option to use.

Interface Properties

Interface: GigabitEthernet0 ☒ Enable interface

Interface Name: INSIDE Security Level: 100

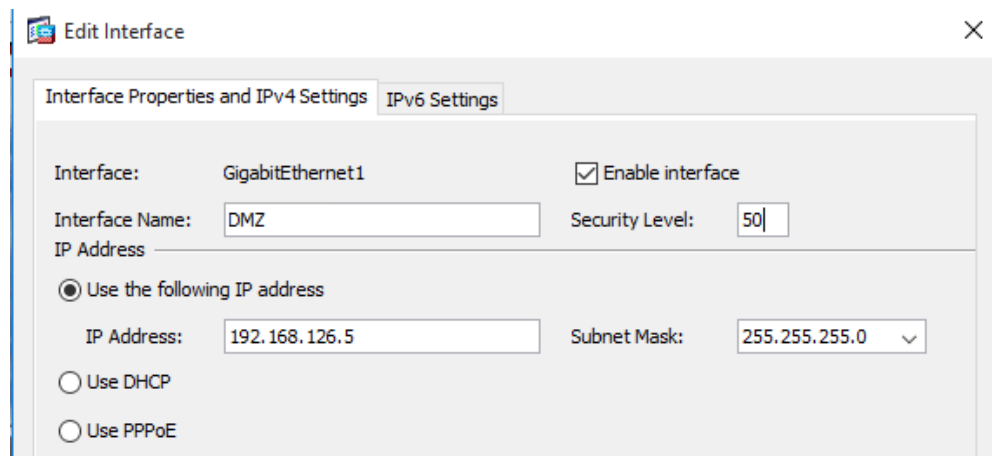
IP Address

☒ Use the following IP address

IP Address: 192.168.199.5 Subnet Mask: 255.255.255.0

☐ Use DHCP

Figure 18.1 : Configuration de l'interface GigabitEthernet0



Edit Interface

Interface Properties and IPv4 Settings | IPv6 Settings

Interface: GigabitEthernet1 ☒ Enable interface

Interface Name: DMZ Security Level: 50

IP Address

☒ Use the following IP address

IP Address: 192.168.126.5 Subnet Mask: 255.255.255.0

☐ Use DHCP

☐ Use PPPoE

Figure 18.2 : Configuration de l'interface GigabitEthernet1

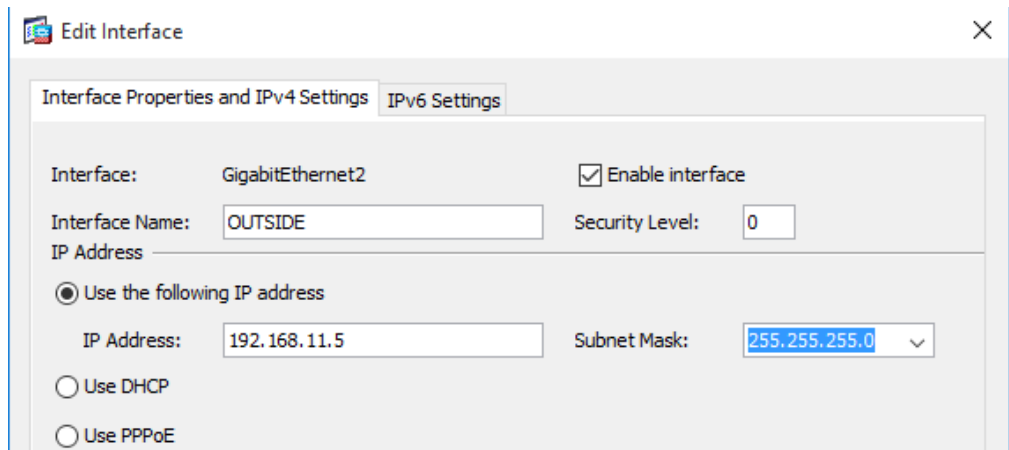


Figure 18.3 : Configuration de l'interface GigabitEthernet2

Q19) Cela dépend du comportement par défaut du dispositif. Le comportement par défaut sur Cisco ASA est de tout rejeter.

Q20) NAT traduit une adresse IP privée en une adresse IP publique et vice-versa. Chaque adresse IP privée est mappée à une adresse IP publique unique. Alors que PAT est une forme spéciale de NAT où plusieurs adresses IP privées sont traduites en une seule adresse IP publique, mais en différenciant les connexions via les numéros de port.

Q21) Les règles de pare-feu servent à contrôler le flux d'entrées et sorties du trafic Internet entre ce dernier et le réseau local. Elles servent à traiter les paquets selon des critères définis.


Les règles NAT servent à configurer et contrôler le trafic entre le réseau privé et le réseau public. Généralement, ces dernières sont appliquées sur les paquets qui sont passés et ont été acceptés par les règles de pare-feu.

Les règles de services (ou politiques de services) permettent d'appliquer des actions spécifiques sur le trafic réseau qui a été autorisé par les règles d'accès. En d'autres termes, une fois que le trafic a passé les règles de filtrage de base des règles d'accès, des politiques de service peuvent être appliquées pour offrir un traitement particulier à ce trafic. Un exemple de service peut être relié à la qualité de service (QoS) en donnant la priorité à certains types de trafic.

Q22) Le routage statique est un type de routage dans lequel il faut spécifier explicitement et manuellement le chemin entre deux routeurs. Les routes de ce type de routage ne peuvent pas être mises à jour automatiquement, contrairement au routage dynamique, il faut passer par des tables de routage créées manuellement pour cela. Les routes statiques ont pour avantages de consommer moins de bande passante et de ressources en CPU, mais ces dernières sont faites uniquement pour les réseaux de petite taille dont la topologie est très simple.

Les étapes que nous avons suivies pour que la machine virtuelle Windows 10 puisse aller sur internet sont les suivantes :

1. Tout d'abord, nous avons créé une règle de NAT statique. Cela nous a permis depuis l'interface INSIDE d'atteindre l'interface OUTSIDE qui est connectée à internet.

 Edit NAT Rule ✕

Match Criteria: Original Packet

Source Interface: INSIDE Destination Interface: OUTSIDE

Source Address: any Destination Address: any

Service: any

Action: Translated Packet

Source NAT Type: Dynamic PAT (Hide)

Source Address: OUTSIDE Destination Address: -- Original --

☐ PAT Pool Translated Address: Service: -- Original --

☐ Round Robin

☐ Fall through to interface PAT

Options

☒ Enable rule

☐ Translate DNS replies that match this rule

☐ Disable Proxy ARP on egress interface

☐ Lookup route table to locate egress interface

Direction: Both

Description:

OK
Cancel
Help

Figure 22.1 : Étape 1

- Nous avons ensuite créé une route statique sur l'interface OUTSIDE avec comme Gateway le serveur WINS de VMNET8. Cela nous a permis de diriger le trafic vers le serveur WINS de VMNET8.

[Configuration](#) > [Device Setup](#) > [Routing](#) > [Static Routes](#)

Specify static routes.

Filter: ☒ Both ☐ IPv4 only ☐ IPv6 only

Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options
OUTSIDE	0.0.0.0	0.0.0.0	192.168.11.2	1	None

Figure 22.2 : Étape 2

3. Voici le sommaire de la règle de NAT que nous avons rajouté :

Configuration > Firewall > NAT Rules										
Match Criteria: Original Packet						Action: Translated Packet			Options	Description
#	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service		
1	INSIDE	OUTSIDE	any	any	any	OUTSIDE (P)	-- Original --	-- Original --		
Network Object NAT (No rules)										

Figure 22.3 : Étape 3

4. Grâce à cela, la VM Windows 10 avait accès à internet.

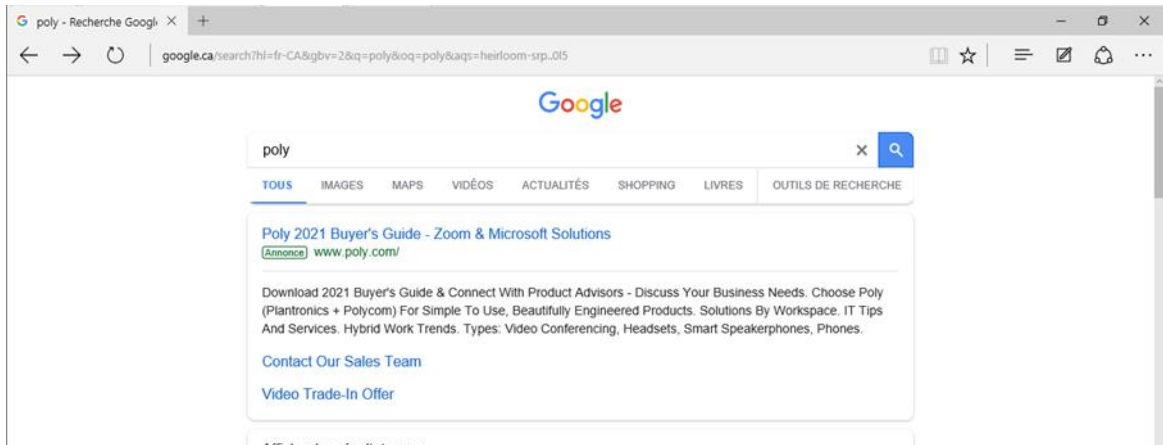


Figure 22.4 : Résultat d'accès à internet

Q23) Donner accès à internet à la machine Linux

1. Créer la règle NAT

Edit NAT Rule

Match Criteria: Original Packet

Source Interface: **DMZ** Destination Interface: **OUTSIDE**

Source Address: **any** Destination Address: **any**

Service: **any**

Action: Translated Packet

Source NAT Type: **Dynamic PAT (Hide)**

Source Address: **OUTSIDE** Destination Address: **-- Original --**

☐ PAT Pool Translated Address: Service: **-- Original --**

☐ Round Robin

☐ Fall through to interface PAT

Options

☒ Enable rule

☐ Translate DNS replies that match this rule

☐ Disable Proxy ARP on egress interface

☐ Lookup route table to locate egress interface

Direction: **Both**

Description:

OK **Cancel** **Help**

Figure 23.1 : Étape 1

2. Sommaire de la règle ajoutée

Configuration > Firewall > NAT Rules

#	Match Criteria: Original Packet					Action: Translated Packet			Options	Description
	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service		
1	INSIDE	OUTSIDE	any	any	any	OUTSIDE (P)	-- Original --	-- Original --		
2	DMZ	OUTSIDE	any	any	any	OUTSIDE (P)	-- Original --	-- Original --		

Network Object NAT (No rules)

Figure 23.2 : Étape 2

3. La route statique avait déjà été configurée la VM Linux a maintenant accès à internet

```
msfadmin@metasploitable:~$ curl google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
msfadmin@metasploitable:~$ _
```

Figure 23.3 : Résultat d'accès à internet

Q24) Ping DMZ à partir de la machine Windows 10

1. Créer une nouvelle "Service Policy Rules"

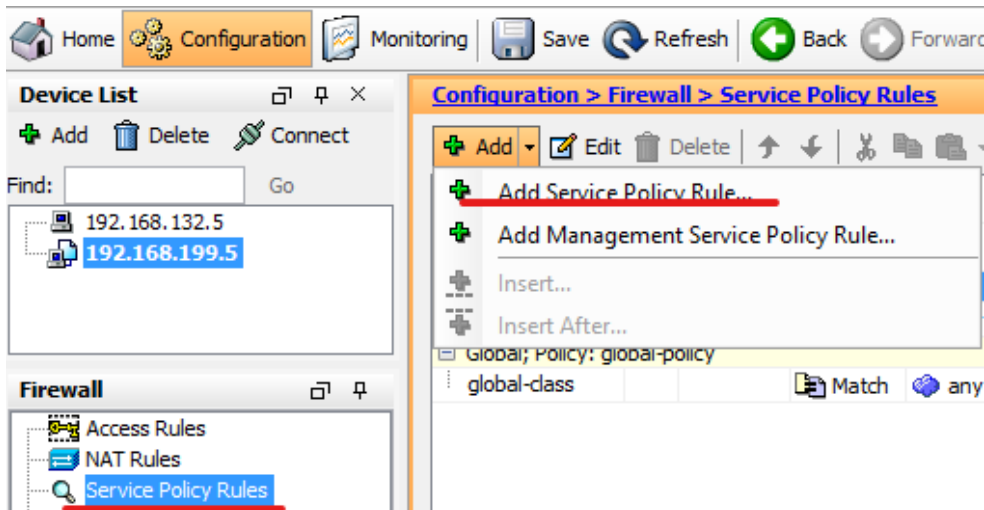


Figure 24.1 : Étape 1

2. Choisir l'interface sur laquelle appliquer la règle et faire next

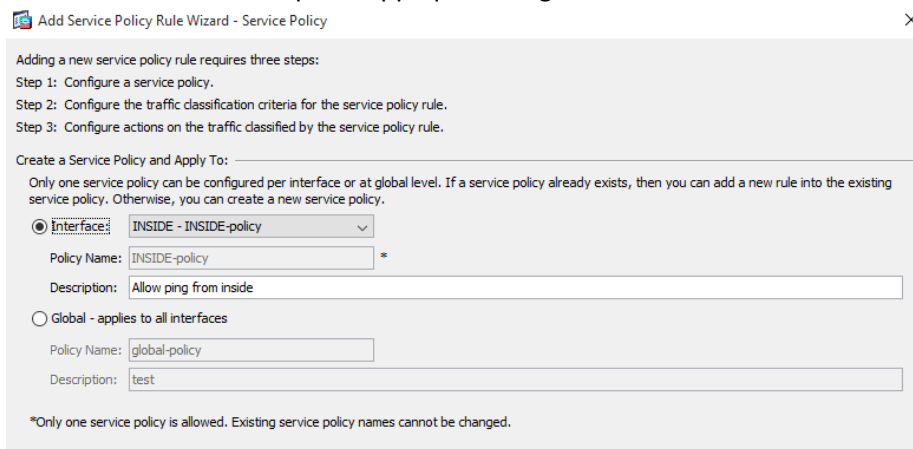


Figure 24.2 : Étape 2

3. Choisir "Default Inspection" Traffic et faire next

4. Choisir "ICMP" et faire finish

5. On obtient la règle

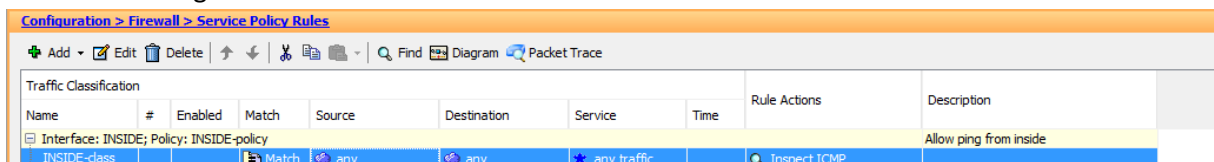


Figure 24.3 : Résultat de la règle

6. Et on peut maintenant faire des pings vers le réseau DBZ à partir de INSIDE mais pas de OUTSIDE

```
C:\Users\GIGL>ping 192.168.126.100

Pinging 192.168.126.100 with 32 bytes of data:
Reply from 192.168.126.100: bytes=32 time<1ms TTL=64
Reply from 192.168.126.100: bytes=32 time<1ms TTL=64
Reply from 192.168.126.100: bytes=32 time<1ms TTL=64
Reply from 192.168.126.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.126.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\GIGL>
```

Figure 24.4 : Résultat du ping à partir de INSIDE

```
root@kali:~# ping 192.168.126.100
PING 192.168.126.100 (192.168.126.100) 56(84) bytes of data.
^C
--- 192.168.126.100 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5111ms
```

Figure 24.5 : Résultat du ping à partir de OUTSIDE