INF8402 – Sécurité des réseaux fixes et mobiles

Automne 2021

TP3 : ASA - Configuration par ligne de commande

7 Décembre 2021

1.4.2 Configuration de la machine ASA (accès au mode console)

```
POLYFW01> login
Username: polymtl
Password: *****
POLYFW01# show running-config
: Saved
:
ASA Version 8.4(2)
!
hostname POLYFW01
domain-name polymtl.ca
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
 nameif INSIDE
 security-level 0
 ip address 192.168.64.5 255.255.255.0
!
interface GigabitEthernet1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet2
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
dns server-group DefaultDNS
 domain-name polymtl.ca
pager lines 24
mtu INSIDE 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 192.168.64.0 255.255.255.0 INSIDE
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
username polymtl password 2dE0/ajHvPdifYEB encrypted privilege 15
```

```
username polymtl password 2dE0/ajHvPdifYEB encrypted privilege 15
!
!
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
crashinfo save disable
Cryptochecksum:474355e0aa1e35a339418af0ef7d805f
: end
```

Figure 1 : Commande "***show running-config***" sur le ASA.

```
POLYFW01# show ip
System IP Addresses:
Interface                  Name                IP address      Subnet mask     Method
GigabitEthernet0           INSIDE              192.168.64.5    255.255.255.0   CONFIG
Current IP Addresses:
Interface                  Name                IP address      Subnet mask     Method
GigabitEthernet0           INSIDE              192.168.64.5    255.255.255.0   CONFIG
POLYFW01#
```

Figure 2 : Commande "***show ip***" sur le ASA.

1.4.3 Configuration du réseau de la machine virtuelle Windows 10

```
Windows IP Configuration

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

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-37-66-7B
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d84c:5ef0:ced:bc3a%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.199.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.199.5
   DHCPv6 IAID . . . . . . . . . . . : 50334761
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-30-79-01-00-0C-29-37-66-7B
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Figure 3 : Configuration de la VM Windows 10.

1.4.4 Configuration de la machine ASA (accès au mode console)

```
POLYFW01# configure terminal
POLYFW01(config)# http 192.168.199.0 255.255.255.0 INSIDE
POLYFW01(config)# int GigabitEthernet0
POLYFW01(config-if)# ip address 192.168.199.5 255.255.255.0
POLYFW01(config-if)#
```

Figure 4 : Configuration de l'interface INSIDE de manière statique.

```
POLYFW01(config-if)# show running-config
: Saved
:
ASA Version 8.4(2)
!
hostname POLYFW01
domain-name polymtl.ca
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
 nameif INSIDE
 security-level 0
 ip address 192.168.199.5 255.255.255.0
!
interface GigabitEthernet1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet2
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
dns server-group DefaultDNS
 domain-name polymtl.ca
pager lines 24
mtu INSIDE 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 192.168.64.0 255.255.255.0 INSIDE
http 192.168.199.0 255.255.255.0 INSIDE
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
username polymtl password 2dE0/ajHvPdifYEB encrypted privilege 15
!
!
prompt hostname context
no call-home reporting anonymous
```

```
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DD
CEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
crashinfo save disable
Cryptochecksum:3bfbb34be1c8050619c09ae2ccbe587c
: end
```

Figure 5 : Commande "***show running-config***" après configuration de l'interface INSIDE sur le ASA.

```
POLYFW01(config-if)# show ip
System IP Addresses:
Interface                Name                IP address      Subnet mask     Method
GigabitEthernet0         INSIDE              192.168.199.5   255.255.255.0   manual
Current IP Addresses:
Interface                Name                IP address      Subnet mask     Method
GigabitEthernet0         INSIDE              192.168.199.5   255.255.255.0   manual
POLYFW01(config-if)#
```

Figure 6 : Commande "***show ip***" après configuration de l'interface INSIDE sur le ASA.

Config Bitnami :

```
"/etc/network/interfaces" 13 lines, 341 characters written
bitnami@linux:~$ sudo cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
        address 192.168.126.100
        netmask 255.255.255.0
        gateway 192.168.126.5
bitnami@linux:~$
```

```
Last login: Mon Dec  6 21:41:50 UTC 2021 on tty1
Welcome to Ubuntu 14.04.2 LTS (GNU/Linux 3.13.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
bitnami@linux:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ff:6c:11
          inet addr:192.168.126.100  Bcast:192.168.126.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feff:6c11/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:648 (648.0 B)
          Interrupt:17 Base address:0x1080

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:65536  Metric:1
          RX packets:32 errors:0 dropped:0 overruns:0 frame:0
          TX packets:32 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2368 (2.3 KB)  TX bytes:2368 (2.3 KB)

bitnami@linux:~$ _
```

Figure 7 : Configuration de la VM Bitnami.

Config Kali :

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.100  netmask 255.255.255.0  broadcast 192.168.11.255
        inet6 fe80::20c:29ff:fe45:b539  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:45:b5:39  txqueuelen 1000  (Ethernet)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 2163 (2.1 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 28  bytes 1748 (1.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 1748 (1.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# ip r
default via 192.168.11.5 dev eth0 proto static metric 100
192.168.11.0/24 dev eth0 proto kernel scope link src 192.168.11.100 metric 100
root@kali:~#
```

Figure 8 : Configuration de la VM Kali Linux.

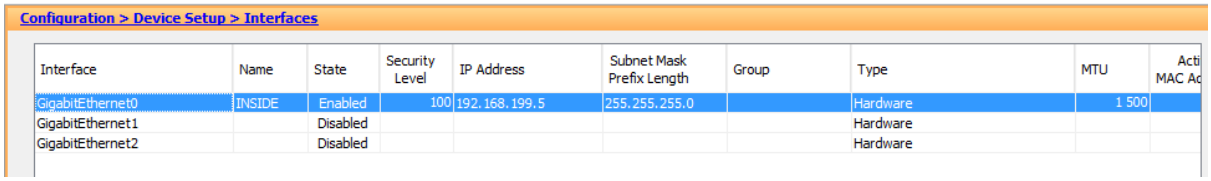
Q1) Quelle est la commande qui permet de fixer le niveau de sécurité de l'interface INSIDE à 100? (1 point)

On utilise tout d'abord la commande "***interface GigabitEthernet0***" pour sélectionner et commencer la configuration de l'interface GigabitEthernet0 qui est l'interface INSIDE. Par la suite on configure le niveau de sécurité de l'interface INSIDE à 100 à l'aide de la commande suivante : "***security-level 100***".

```
POLYFW01(config-if)# interface GigabitEthernet0
POLYFW01(config-if)# security-level 100
POLYFW01(config-if)#
```

Figure 9 : Commandes permettant de
configurer le niveau de sécurité de l'interface INSIDE à 100.

Vous trouverez ci-dessous une capture de l'ASDM qui permet de prouver que le niveau de sécurité de l'interface INSIDE a bien été mis à 100.



Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	Group	Type	MTU	Acti MAC Ac
GigabitEthernet0	INSIDE	Enabled	100	192.168.199.5	255.255.255.0		Hardware	1 500	
GigabitEthernet1		Disabled					Hardware		
GigabitEthernet2		Disabled					Hardware		

Figure 10 : Preuve que le niveau de sécurité de l'interface INSIDE a été mis à 100.

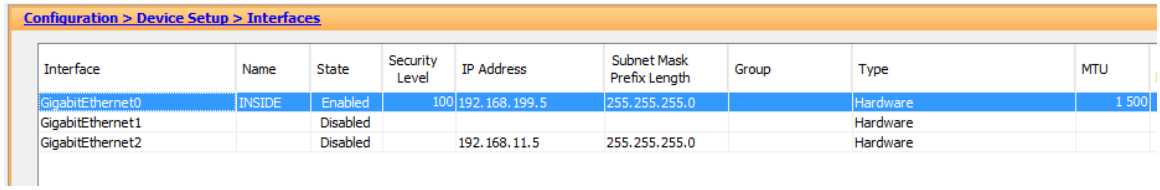
Q2) Quelle(s) commande(s) permet(tent) de configurer l'interface GigabitEthernet2 telles que présentée dans le tableau 1? (2 points)

On utilise tout d'abord la commande "***interface GigabitEthernet2***" pour sélectionner et commencer la configuration de l'interface GigabitEthernet2. Par la suite, on assigne l'adresse IP 192.168.11.5 avec le masque 255.255.255.0 à l'interface grâce à la commande suivante : "***ip address 192.168.11.5 255.255.255.0***".

```
POLYFW01(config)# int GigabitEthernet2
POLYFW01(config-if)# ip address 192.168.11.5 255.255.255.0
POLYFW01(config-if)#
```

Figure 11 : Commandes permettant de configurer l'interface GigabitEthernet2.

Vous trouverez ci-dessous une capture de l'ASDM qui permet de prouver que la configuration de l'interface GigabitEthernet2 a bien été faite.



Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	Group	Type	MTU
GigabitEthernet0	INSIDE	Enabled	100	192.168.199.5	255.255.255.0		Hardware	1 500
GigabitEthernet1		Disabled					Hardware	
GigabitEthernet2		Disabled		192.168.11.5	255.255.255.0		Hardware	

Figure 12 : Preuve que la configuration de l'interface GigabitEthernet2 a bien été faite.

Q3) Il est possible de constater que l'interface GigabitEthernet2 ne possède pas de nom. Quelle commande permet de nommer l'interface GigabitEthernet2 à OUTSIDE? (1.5 points)

Avec l'interface GigabitEthernet2 sélectionnée, nous avons utilisé la commande "***nameif OUTSIDE***" pour nommer l'interface GigabitEthernet2 OUTSIDE.

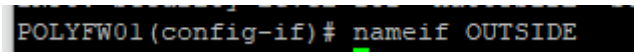


Figure 13 : Commande permettant de nommer l'interface GigabitEthernet2 OUTSIDE.

Vous trouverez ci-dessous une capture de l'ASDM qui permet de prouver que l'interface GigabitEthernet2 a bien été renommée à OUTSIDE.

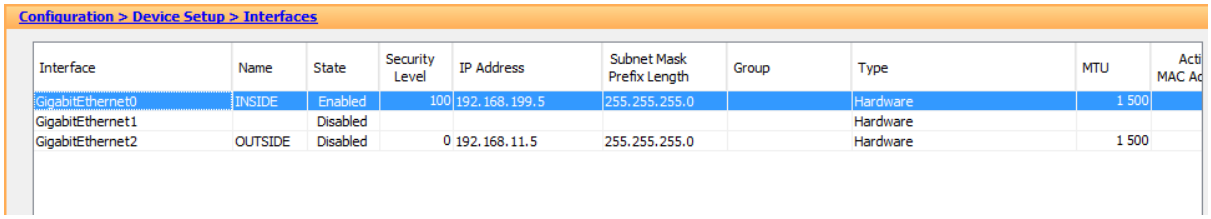


Figure 14 : Preuve que l'interface GigabitEthernet2 a été renommée à OUTSIDE.

Q4) Encore sur ASDM, il est possible de constater que l'interface GigabitEthernet2 n'est pas activée. Quelle commande permet d'activer cette interface? (2 points)

Pour activer l'interface GigabitEthernet2, il faut encore une fois l'avoir sélectionnée puis il faut utiliser la commande suivante : "***no shut***" ou "***no shutdown***".

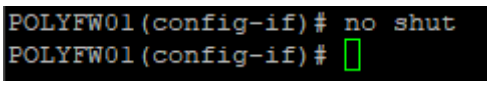


Figure 15 : Commande permettant d'activer l'interface GigabitEthernet2 (OUTSIDE).

Vous trouverez ci-dessous une capture de l'ASDM qui permet de prouver que l'interface GigabitEthernet2 a bien été activée.

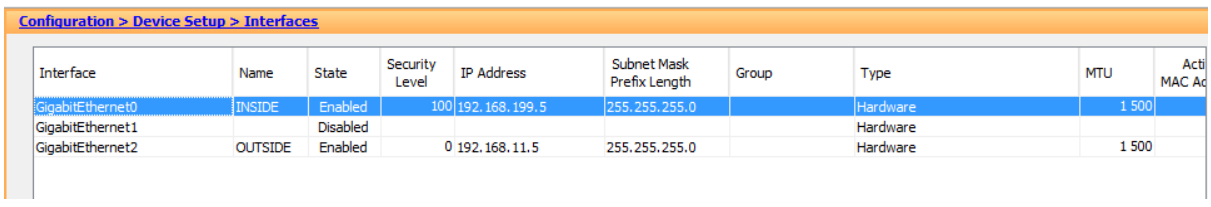


Figure 16 : Preuve que l'interface GigabitEthernet2 a été activée.

Q5) Quelle(s) commande(s) permet(tent) de créer un NAT pour permettre à tous les utilisateurs des réseaux « INSIDE » d'aller vers internet. (2 points)

Tout d'abord, nous créons un objet réseau qui représente le sous réseau INSIDE grâce aux commandes "***object network INSIDE-NETWORK***" et "***subnet 192.168.199.0 255.255.255.0***". Pour cet objet réseau nous configurons une règle de NAT dynamique qui va faire la traduction d'adresse de port quand une machine de l'interface INSIDE veut communiquer avec internet et donc avec OUTSIDE. Nous faisons cela grâce à la commande suivante : "***nat (INSIDE,OUTSIDE) dynamic interface***".

```
POLYFW01(config)# object network INSIDE-NETWORK
POLYFW01(config-network-object)# subnet 192.168.199.0 255.255.255.0
POLYFW01(config-network-object)# nat (INSIDE,OUTSIDE) dynamic interface
```

Figure 17 : Commandes permettant de créer un NAT pour permettre à tous les utilisateurs du réseau « INSIDE » d'aller vers internet.

Vous pouvez voir la règle NAT créée dans le ASDM dans la capture ci-dessous.

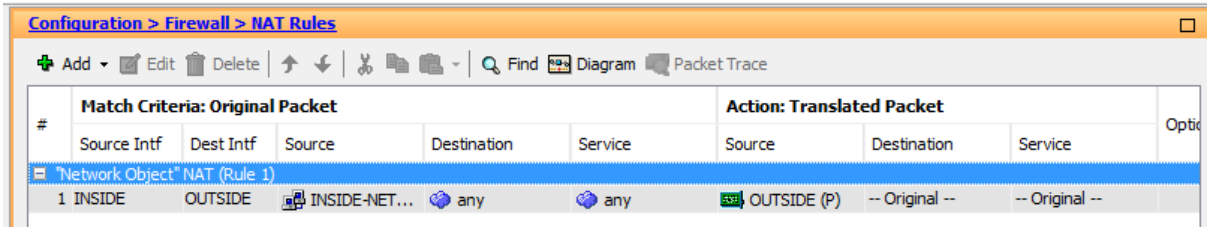


Figure 18 : Règle NAT dans le ASDM.

Référence :

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115904-asa-config-dmz-00.html#anc11

Q6) Quelle commande permet d'ajouter une route statique? (1.5 points) N'oubliez pas de préciser ces paramètres dans votre commande : « OUTSIDE », IP Address « 0.0.0.0 » (Any), Netmask « 0.0.0.0 », Gateway IP « serveur WINS de l'interface VMnet8 ».

Nous sommes, tout d'abord, allés chercher l'adresse IPv4 du serveur Wins de VMnet 8. Comme vous pouvez le voir ci-dessous, l'IP est 192.168.11.2.

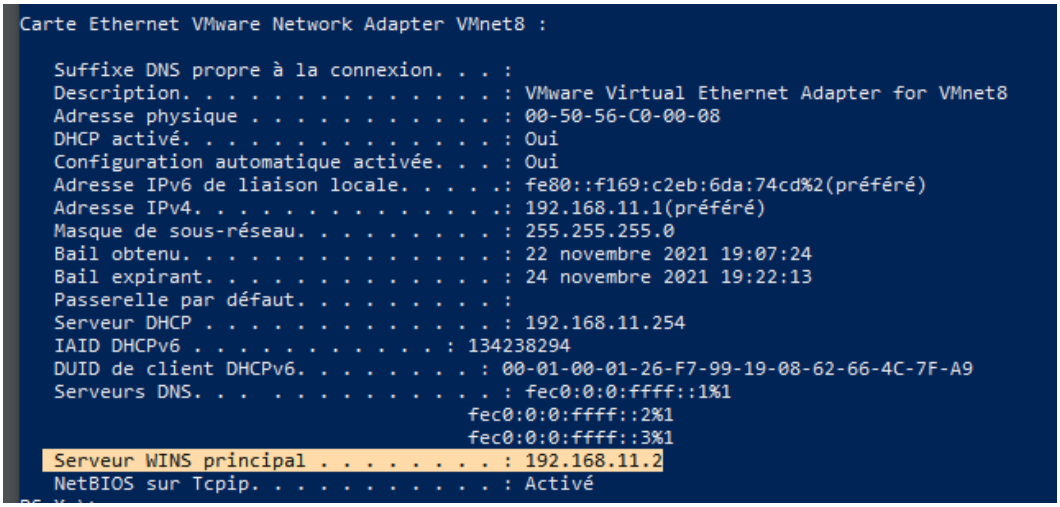


Figure 19 : Adresse IPv4 du serveur WINS de VMnet 8.

Nous avons ensuite sélectionné l'interface OUTSIDE et nous avons créé la route statique grâce à la commande suivante : "***route OUTSIDE 0.0.0.0 0.0.0.0 192.168.11.2***".

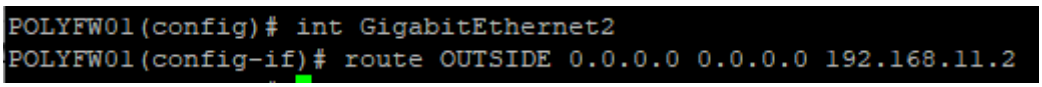


Figure 20 : Commande permettant d'ajouter une route statique.

La route statique est maintenant visible dans le ASDM comme vous pouvez le remarquer ci-dessous.

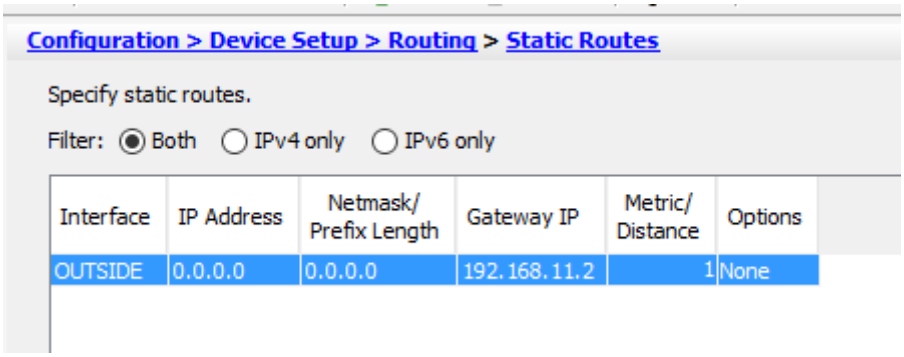


Figure 21 : Route statique créée visible dans le ASDM.

Grâce à la mise en place du NAT dans la question 5 et à la mise en place de la route statique ci-dessus, nous avons pu nous connecter à internet avec la VM Windows 10 comme vous pouvez le voir ci-dessous.

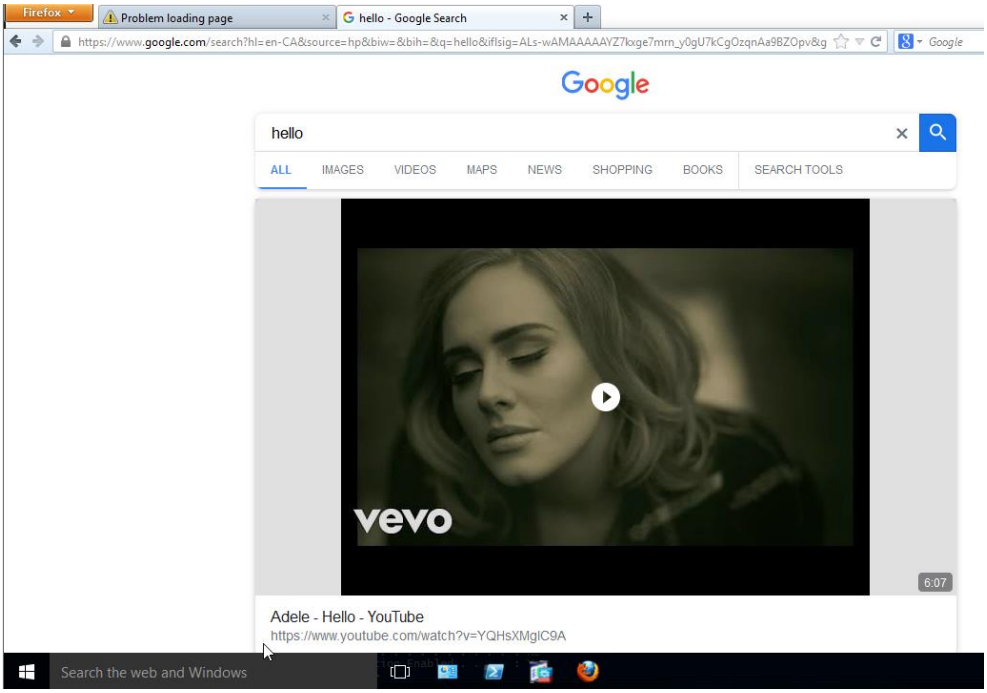


Figure 22 : Connection à internet avec la VM Windows 10.

Q7) À ce stade, vous devriez avoir internet sur la machine window 10. De la même façon, donnez accès à internet à la machine bitnami. Vous devez expliciter toutes les commandes à l'aide de captures d'écran. Montrez que vous avez accès à Internet en utilisant l'outil curl

a) Quelle configuration statique avez-vous utilisé? Vous pouvez présenter la configuration que vous avez utilisez dans le fichier /etc/network/interfaces (2 points)

Vous trouverez ci-dessous la configuration statique de l'interface réseau de la VM Bitnami. Son adresse IPv4 est 192.168.126.100 et sa passerelle par défaut a pour IPv4 192.168.126.5.

```
"/etc/network/interfaces" 13 lines, 341 characters written
bitnami@linux:~$ sudo cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
        address 192.168.126.100
        netmask 255.255.255.0
        gateway 192.168.126.5
bitnami@linux:~$
```

Figure 23 : Fichier /etc/network/interfaces de la VM Bitnami.

Nous avons aussi mis en place l'interface DMZ grâce aux commandes que vous trouverez dans la capture d'écran ci-dessous. Ces commandes sont sensiblement les mêmes que celles utilisées pour la mise en place de l'interface OUTSIDE.

```
POLYFW01(config)# int GigabitEthernet1
POLYFW01(config-if)# ip address 192.168.126.5 255.255.255.0
POLYFW01(config-if)# security
POLYFW01(config-if)# security-level 50
POLYFW01(config-if)# nameif DMZ
POLYFW01(config-if)# no shut
POLYFW01(config-if)#
```

Figure 24 : Set up de l'interface DMZ.

Vous trouverez ci-dessous la preuve que l'interface DMZ a bien été configurée.

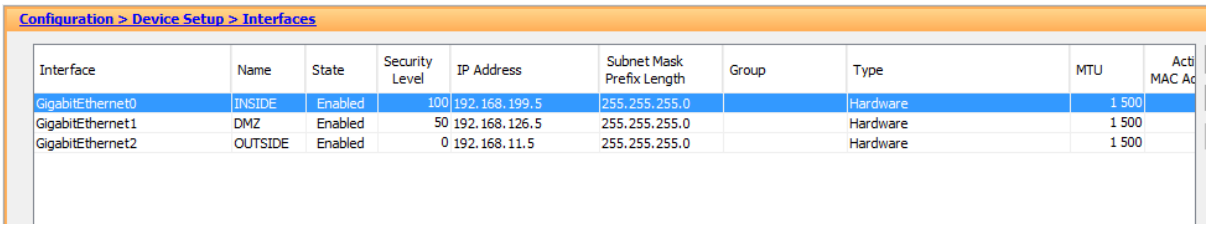


Figure 25 : Preuve que l'interface DMZ a été configurée.

b) Quelle commande NAT permet à tous les utilisateurs du réseau « DMZ» d'aller vers internet? (2 points)

Les commandes que nous avons exécutées pour connecter les utilisateurs du réseau «DMZ» vers internet sont sensiblement les mêmes que celles utilisées dans la question 5 pour connecter le réseau INSIDE vers OUTSIDE qui est connecté à internet.

Nous créons un objet réseau qui représente le sous réseau DMZ grâce aux commandes "***object network DMZ-NETWORK***" et "***subnet 192.168.126.0 255.255.255.0***". Pour cet objet réseau nous configurons une règle de NAT dynamique qui va faire la traduction d'adresse de port quand une machine de l'interface DMZ veut communiquer avec OUTSIDE et donc internet. Nous faisons cela grâce à la commande suivante : "***nat (DMZ,OUTSIDE) dynamic interface***". Vous trouverez le détail des commandes qui permettent à tous les utilisateurs du réseau « DMZ» d'aller vers internet ci-dessous.

```
POLYFW01(config-network-object)# object network DMZ-NETWORK
POLYFW01(config-network-object)# subnet 192.168.126.0 255.255.255.0
POLYFW01(config-network-object)# nat (DMZ,OUTSIDE) dynamic interface
POLYFW01(config-network-object)#
```

Figure 26 : Commandes permettant aux utilisateurs du réseau « DMZ» d'aller vers internet.

Vous trouverez ci-dessous le résumé des règles NAT créées grâce à l'invité de commande.

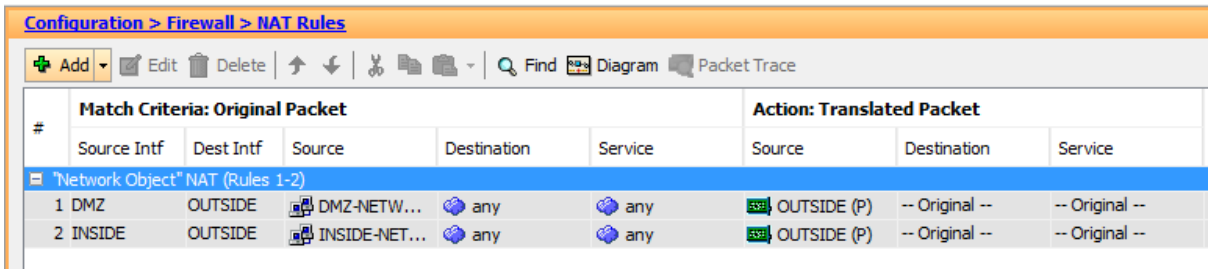


Figure 27 : Résumé des règles NAT créées grâce à l'invité de commande.

Nous avons ensuite cherché l'adresse IP de google.com car nous n'avions pas inscrit de serveur DNS dans la configuration IP de la VM Bitnami donc elle n'était pas capable de résoudre les noms de domaine. L'adresse IP de google.com était 172.217.13.142 comme vous pouvez le voir ci-dessous.

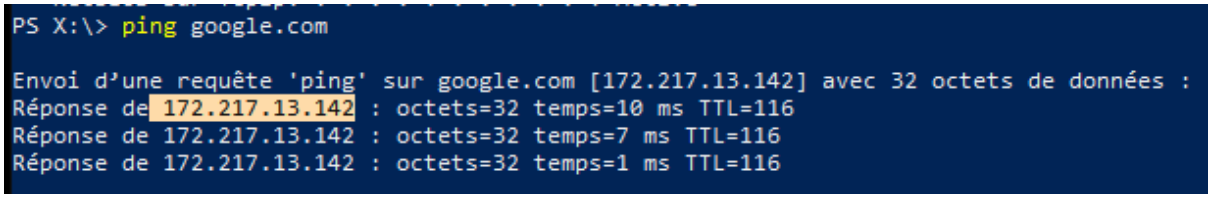


Figure 28 : Adresse IPv4 de google.com.

Pour tester la connexion à internet de la VM Bitnami, nous avons utilisé la commande curl. Comme vous pouvez le voir ci-dessous, nous avions bien accès à internet.

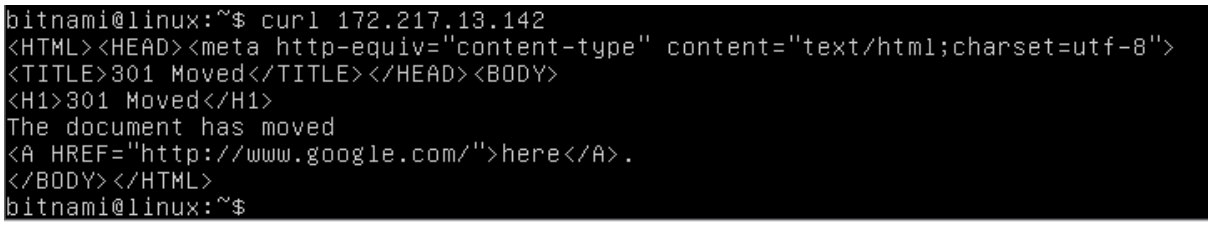


Figure 29 : Commande curl vers l'adresse IPv4 de google.com.

Q8) Quelle(s) commande(s) permet(tent) à Kali Linux d'accéder à Internet?

a) Quelle configuration statique avez-vous utilisé? Vous pouvez présenter la configuration que vous avez utilisez dans le fichier /etc/network/interfaces (2 points)

Vous trouverez ci-dessous la configuration statique de la VM Kali Linux.

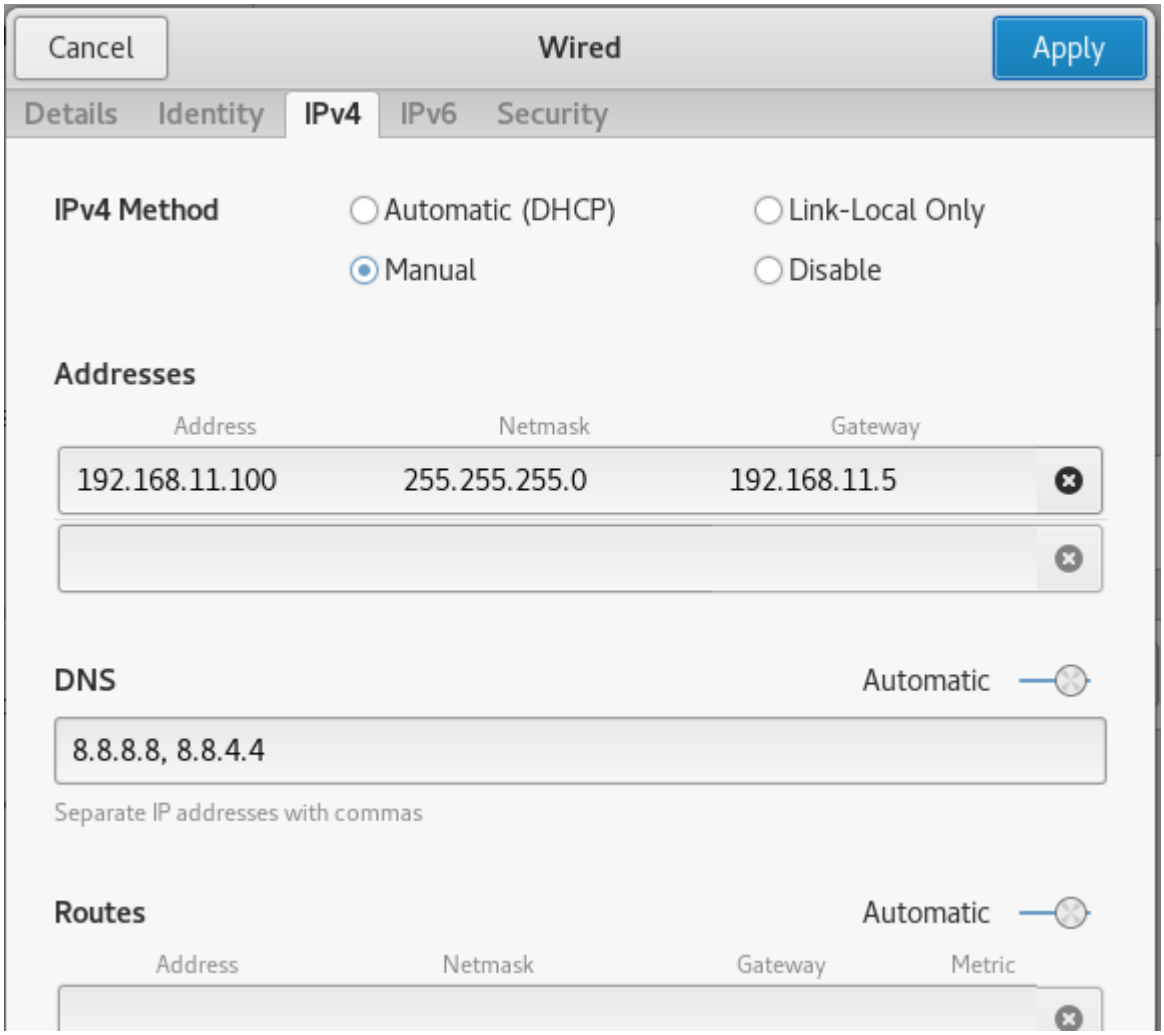


Figure 30 : Configuration statique de la VM Kali Linux.

b) Quelle commande NAT permet à tous les utilisateurs du réseau « OUTSIDE » d'aller vers internet? (2 points)

Normalement toutes les machines du réseau OUTSIDE sont, par défaut, connectées à internet. Dans notre cas, nous sommes dans un environnement éducatif donc nous devons ajouter un objet réseau et une configuration de NAT comme effectué pour la DMZ et le INSIDE. Vous trouverez les commandes effectuées dans la capture ci-dessous.

```
POLYFW01(config-network-object)# object network OUTSIDE-NETWORK
POLYFW01(config-network-object)# subnet 192.168.11.0 255.255.255.0
POLYFW01(config-network-object)# nat (OUTSIDE,OUTSIDE) dynamic interface
```

Figure 31 : Commande permettant aux utilisateurs de OUTSIDE d'aller vers internet.

De plus, par défaut, il n'y a aucune règle d'accès mise en place pour la zone OUTSIDE donc aucune communication n'est possible. Nous avons donc rajouté une règle pour que nos paquets puissent transiter. Vous trouverez la règle d'accès dans la capture ci-dessous.

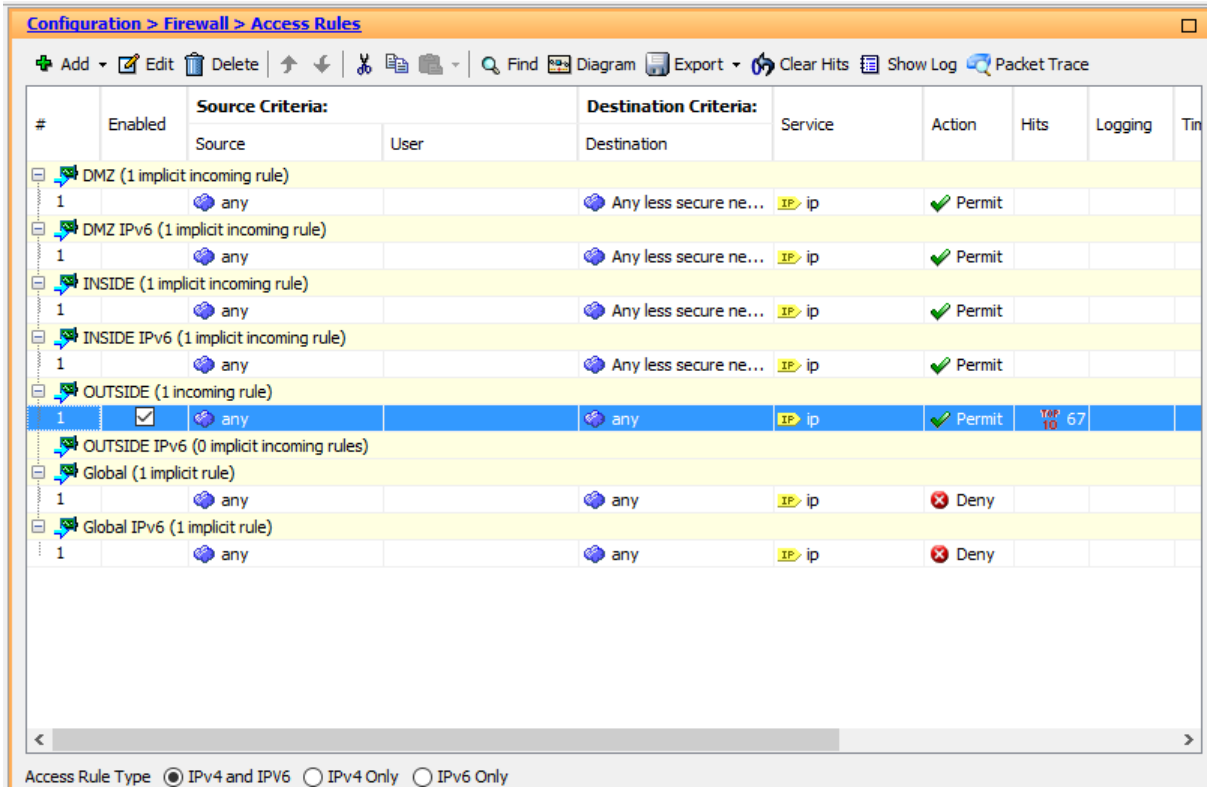


Figure 32 : Ajout d'une règle d'accès pour la zone OUTSIDE.

Vous trouverez ci-dessous le résumé des règles NAT créées grâce à l'invité de commande.

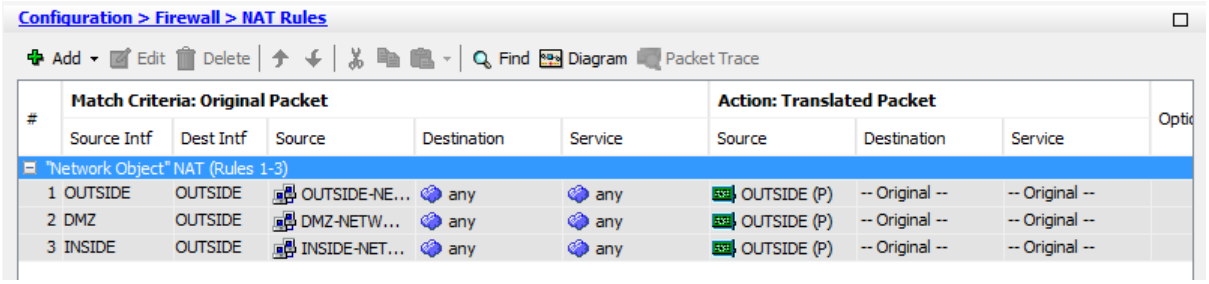


Figure 33 : Résumé des règles NAT créées grâce à l'invité de commande.

Une fois les étapes ci-dessus effectuées, nous avons testé notre connexion internet avec la machine Kali Linux. Comme vous pouvez le voir avec la capture d'écran ci-dessous, nous avions bien accès à internet.

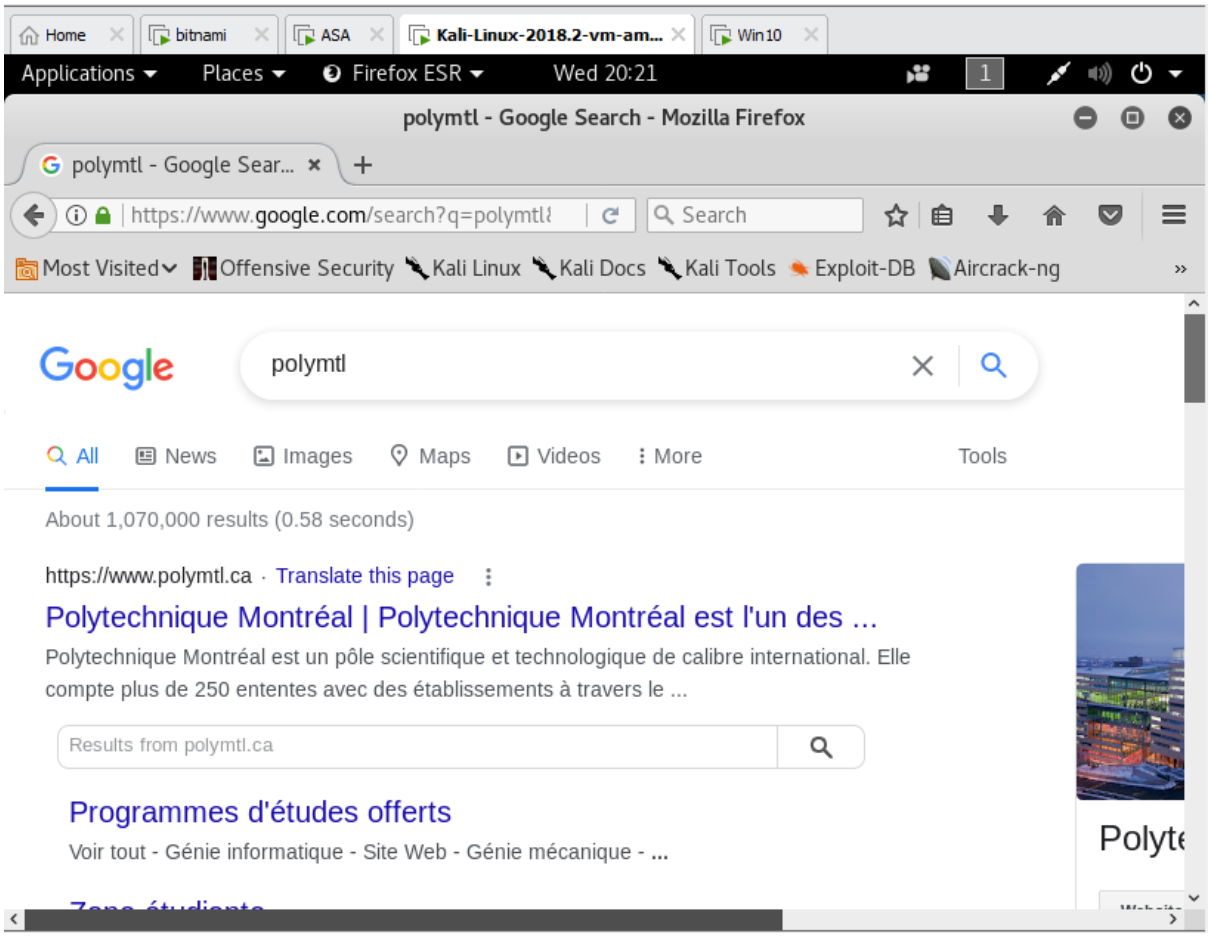


Figure 34 : Accès à internet avec la VM Kali Linux.

c) Quelle commande permet d'activer la communication entre deux hôtes d'une même interface afin qu'ils puissent communiquer entre eux? (2 points)

La commande permettant d'activer la communication entre deux hôtes d'une même interface afin qu'ils puissent communiquer entre eux est la suivante : "***same-security-traffic permit intra-interface***".

```
POLYFW01(config)# same-security-traffic permit intra-interface
POLYFW01(config)#
```

Figure 35 : Commande permettant d'activer la communication entre deux hôtes d'une même interface.

Vous trouverez ci-dessous la preuve que la communication entre deux hôtes d'une même interface est activée. En effet, comme vous pouvez le voir la case "***Enable traffic between two or more hosts connected to the same interface***" est cochée.

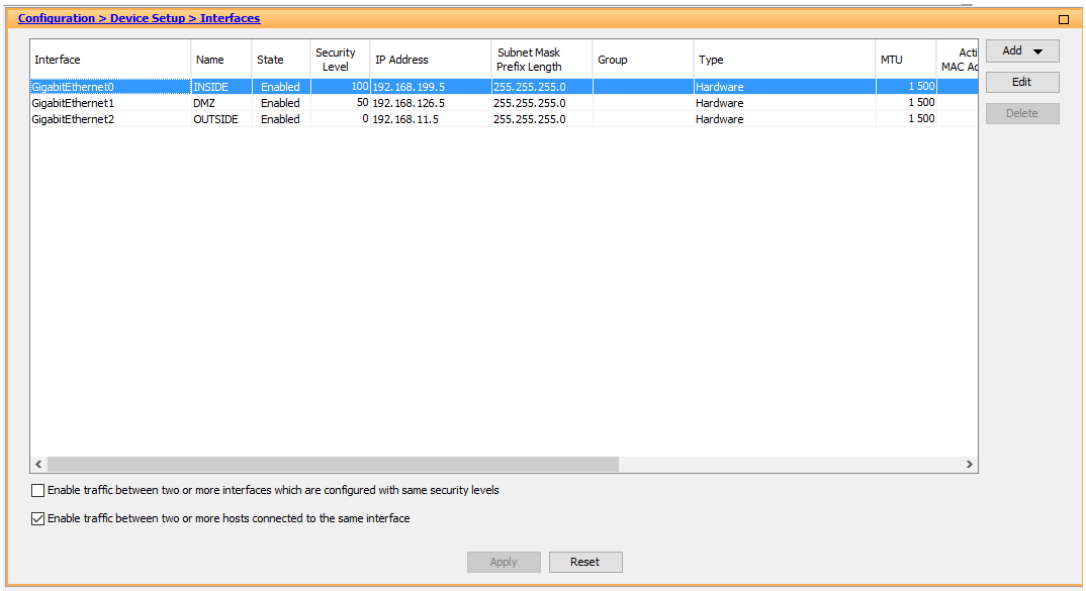


Figure 36 : Preuve que la communication entre deux hôtes d'une même interface est activée.

Dans le Pare-feu ASA exécutez la commande "show running-config" , et récupérez la configuration de l'ASA en ajoutant des captures d'écrans à votre rapport.

```
POLYFW01(config)# show running-config
: Saved
:
ASA Version 8.4(2)
!
hostname POLYFW01
domain-name polymtl.ca
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
 nameif INSIDE
 security-level 100
 ip address 192.168.199.5 255.255.255.0
!
interface GigabitEthernet1
 nameif DMZ
 security-level 50
 ip address 192.168.126.5 255.255.255.0
!
interface GigabitEthernet2
 nameif OUTSIDE
 security-level 0
 ip address 192.168.11.5 255.255.255.0
!
ftp mode passive
dns server-group DefaultDNS
 domain-name polymtl.ca
same-security-traffic permit intra-interface
object network INSIDE-NETWORK
 subnet 192.168.199.0 255.255.255.0
object network DMZ-NETWORK
 subnet 192.168.126.0 255.255.255.0
object network OUTSIDE-NETWORK
 subnet 192.168.11.0 255.255.255.0
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
access-list OUTSIDE_access_in extended permit ip any any
pager lines 24
logging enable
logging asdm informational
mtu INSIDE 1500
mtu OUTSIDE 1500
mtu DMZ 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
!
object network INSIDE-NETWORK
 nat (INSIDE,OUTSIDE) dynamic interface
object network DMZ-NETWORK
 nat (DMZ,OUTSIDE) dynamic interface
object network OUTSIDE-NETWORK
 nat (OUTSIDE,OUTSIDE) dynamic interface
access-group OUTSIDE_access_in in interface OUTSIDE
route OUTSIDE 0.0.0.0 0.0.0.0 192.168.11.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
```

```
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 192.168.64.0 255.255.255.0 INSIDE
http 192.168.199.0 255.255.255.0 INSIDE
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
username polymtl password 2dE0/ajHvPdifYEB encrypted privilege 15
!
!
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
crashinfo save disable
Cryptochecksum:c98e1718388b46104721200b9904af1d
: end
```

Figure 37 : Commande “***show running-config***” à la fin de notre TP.