

### Les traitements que je dois effectuer

```

interface Vlan1
nameif inside
security-level 100
ip address 172.16.1.1 255.255.255.0
!
interface Vlan2
nameif outside
security-level 0
ip address 200.1.1.2 255.255.255.240
!
interface Vlan3
no forward interface Vlan1
nameif dmz
security-level 50
ip address 10.1.1.1 255.255.255.0
!
object network INTERNET
subnet 172.16.1.0 255.255.255.0
object network SERVER
host 10.1.1.5
!
route outside 0.0.0.0 0.0.0.0 200.1.1.1 1
!
access-list DMZOUT extended permit tcp any any eq www
access-list DMZOUT extended permit icmp any any

```

```

!
!
access-group DMZOUT in interface outside
object network INTERNET
nat (inside,outside) dynamic interface
object network SERVER
nat (dmz,outside) static 200.1.1.4

class-map inspection_default
match default-inspection-traffic
!
policy-map globa_policy
class inspection_default
inspect icmp
!
service-policy globa_policy global
!
telnet 172.16.1.0 255.255.255.0 inside
telnet timeout 5
ssh timeout 5
!
dhcpd dns 8.8.8.8
dhcpd auto_config outside
!
dhcpd address 172.16.1.5-172.16.1.10 inside
dhcpd enable inside

```

### **Configuration ISP (routeur)**

```

ISP# conf t
ISP(config)# int g0/0
ISP(config-int)# ip address 8.8.8.1 255.255.255.0
ISP(config-int)# no shutdown
ISP(config)# int g0/1
ISP(config-int)# ip address 200.1.1.1 255.255.255.240
ISP(config-int)# no shutdown

```

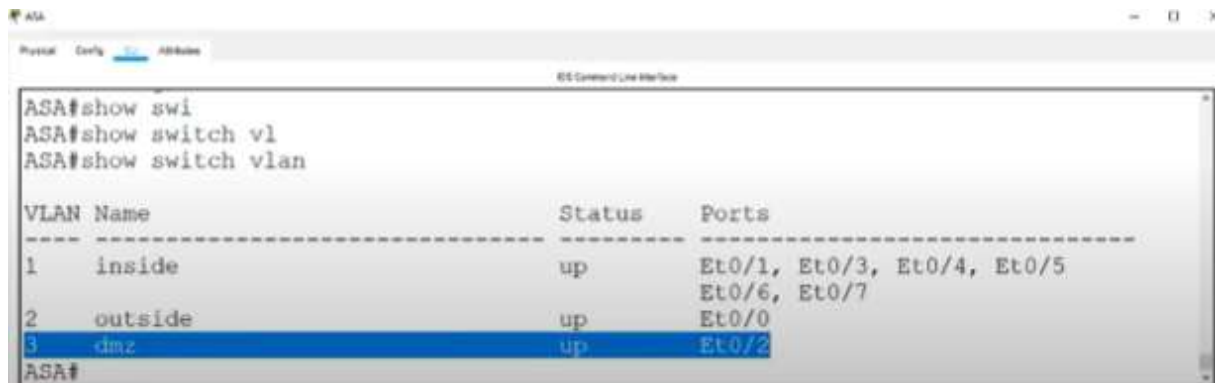
### **Configuration firewall ASA**

```

ASA# conf t

```

```
ASA(config) # int vlan 1
ASA(config-if) #ip address 172.16.1.1 255.255.255.0
ASA(config-if) # nameif inside
ASA(config-if) #security-level 100
ASA(config-if) #exit
ASA(config)# int e0/1
ASA(config-if)#switchport access vlan 1
ASA(config-if)# exit
ASA(config) # int vlan 2
ASA(config-if) #ip address 200.1.1.2 255.255.255.240
ASA(config-if) # nameif outside
ASA(config-if) #security-level 0
ASA(config-if) #exit
ASA(config)# int e0/0
ASA(config-if)#switchport access vlan 2
ASA(config-if)# exit
ASA(config) # int vlan 3
ASA(config-if) # nameif dmz
ERROR : this license does not allow configuring mor than 2 interfaces
ASA(config-if) #no forward interface vlan 1
ASA(config-if) # nameif dmz
ASA(config-if) # ip address 10.1.1.1 255.255.255.0
ASA(config-if) # security-level 50
ASA(config-if) #exit
ASA(config)# int e0/2
ASA(config-if)#switchport access vlan 3
ASA# show switch vlan
```



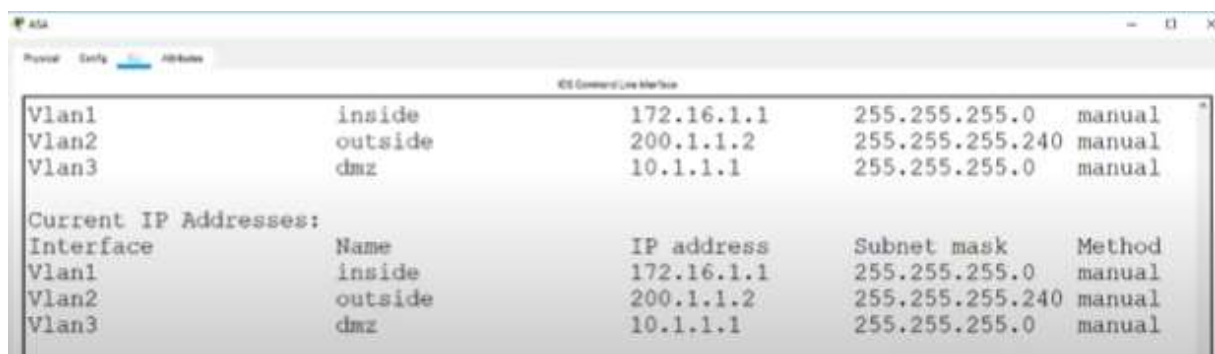
```

ASA#show swi
ASA#show switch vl
ASA#show switch vlan

VLAN Name                Status    Ports
-----
1    inside                up        Et0/1, Et0/3, Et0/4, Et0/5
2    outside                up        Et0/6, Et0/7
3    dmz                    up        Et0/2
ASA#

```

ASA# show ip address



```

Vlan1        inside        172.16.1.1    255.255.255.0  manual
Vlan2        outside       200.1.1.2    255.255.255.240 manual
Vlan3        dmz          10.1.1.1     255.255.255.0  manual

Current IP Addresses:
Interface    Name        IP address    Subnet mask    Method
Vlan1        inside     172.16.1.1    255.255.255.0  manual
Vlan2        outside    200.1.1.2    255.255.255.240 manual
Vlan3        dmz        10.1.1.1     255.255.255.0  manual

```

ASA# show interface ip brief



```

Ethernet0/5    unassigned    YES unset    down
Ethernet0/6    unassigned    YES unset    down
Ethernet0/7    unassigned    YES unset    down
Vlan1          172.16.1.1    YES manual   up
Vlan2          200.1.1.2    YES manual   up

```

ASA# conf t

ASA(config)# dhcpd address 172.16.1.5-172.16.1.10 inside

ASA(config)# dhcpd dns 8.8.8.8

ASA(config)# dhcpd enable inside

Dans PC A apres l'activation de dhcp

Ping 172.16.1.1

Le ping fonctionne

Si je ping 8.8.8.8

Non fonctionnel

Revenir au firewall ASA :

```
ASA(config)# route outside 0.0.0.0 0.0.0.0 200.1.1.1
```

Essaye une autre fois de pinguer de même pc vers le serveur 8.8.8.8

Non fonctionnel

Revenir au firewall ASA :

```
ASA(config)#object network INTERNET
```

```
ASA(config-network-object)# subnet 172.16.1.0 255.255.255.0
```

```
ASA(config-network-object)# nat (inside, outside) ?
```

```
ASA(config-network-object)# nat (inside, outside) dynamic interface
```

```
ASA(config-network-object)# exit
```

```
ASA(config)# access-list ?
```

```
ASA(config)# access-list INTERNET permit ?
```

```
ASA(config)# access-list INTERNET permit tcp any any eq 80
```

```
ASA(config)# access-list INTERNET permit icmp any any
```

```
ASA(config)# access-group INTERNET in interface outside
```

```
ASA(config)# route outside 0.0.0.0 0.0.0.0 200.1.1.1
```

```
ASA(config)# exit
```

Try now to ping from pc to server 8.8.8.8 :

Ping 8.8.8.8

Fonctionnel

Aussi

Ping 8.8.8.10

Fonctionnel

Et l'inverse n'est pas réalisable : on ne peut pas pinguer du pc 8.8.8.1. to un pc en interne 172.16.1.5  
le résultat est unreachable

Maintenant on va configurer de façon qu'on peut pinguer de internet vers le DMZ

Revenir au firewall ASA :

```
ASA(config)#object network SERVER
```

```
ASA(config-network-object)# host 10.1.1.5
```

```
ASA(config-network-object)# nat (dmz, outside) static 200.1.1.4
```

```

ASA(config-network-object)# exit
ASA(config)# access-list DMZOUT permit tcp any any eq 80
ASA(config)# access-list DMZOUT permit icmp any any
ASA(config)# access-group DMZOUT in interface outside
ASA(config)# exit
ASA(config)# class-map inspection_default
ASA(config-cmap)# match ?
ASA(config-cmap)# match ?
ASA(config-cmap)# match default-inspection-traffic
ASA(config-cmap)# exit
ASA(config)# policy-map globa_policy
ASA(config-pmap)# class inspection_default
ASA(config-pmap-c)# inspect ?
ASA(config-pmap-c)# inspect icmp
ASA(config-pmap-c)# exit
ASA(config)# service-policy globa_policy global
ASA(config)# end
ASA# wr mem

ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#match ?

```

mode commands/options:

access-list Access List name

any Match any packets

default-inspection-traffic Match default inspection traffic:

ctiqbe----tcp--2748 dns-----udp--53

ftp-----tcp--21 gtp-----udp--2123,3386

h323-h225-tcp--1720 h323-ras--udp--1718-1719

http-----tcp--80 icmp-----icmp

ils-----tcp--389 ip-options-----rsvp

mgcp-----udp--2427,2727 netbios---udp--137-138

radius-acct---udp--1646 rpc-----udp--111

rsh-----tcp--514 rtsp-----tcp--554

sip-----tcp--5060 sip-----udp--5060

skinny----tcp--2000 smtp-----tcp--25

sqlnet----tcp--1521 tftp-----udp--69

waas-----tcp--1-65535 xdmcp-----udp--177

ciscoasa(config-cmap)#match default-inspection-traffic

ciscoasa(config-cmap)#exit

```
ciscoasa(config)#policy-map globa_policy
ciscoasa(config-pmap)#class inspection_de
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#ins
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#exit
ciscoasa(config)#service-pol
ciscoasa(config)#service-policy globa_policy global
ciscoasa(config)#end
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 63172f58 780b372f 79627f29 23586050
```

1555 bytes copied in 2.541 secs (611 bytes/sec)

[OK]

```
ciscoasa#
ciscoasa#
```

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.2.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 203.1.1.2 255.255.255.0
!
interface Vlan3
 no forward interface Vlan1
 nameif dmz
 security-level 99
 ip address 192.168.100.1 255.255.255.0
!
object network DMZ-NAT
 subnet 192.168.100.0 255.255.255.0
object network INSIDE-NAT
 subnet 192.168.2.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 203.1.1.1 1
!
!
!
!
object network DMZ-NAT
 nat (dmz,outside) dynamic interface
object network INSIDE-NAT
 nat (inside,outside) dynamic interface
!
```

## **Application**

ciscoasa(config)#configure factory-default 172.16.1.1 255.255.255.0

WARNING: The boot system configuration will be cleared.

The first image found in disk0:/ will be used to boot the system on the next reload.

Verify there is a valid image on disk0:/ or the system will not boot.

Begin to apply factory-default configuration:

Clear all configuration

WARNING: DHCPD bindings cleared on interface 'inside', address pool removed

Executing command: interface Ethernet 0/0

Executing command: switchport access vlan 2

Executing command: no shutdown

Executing command: exit

Executing command: interface Ethernet 0/1

Executing command: switchport access vlan 1

Executing command: no shutdown

Executing command: exit

Executing command: interface Ethernet 0/2

Executing command: switchport access vlan 1

Executing command: no shutdown

Executing command: exit

Executing command: interface Ethernet 0/3

Executing command: switchport access vlan 1



Executing command: no shutdown

Executing command: exit

Executing command: interface Ethernet 0/4

Executing command: switchport access vlan 1

Executing command: no shutdown

Executing command: exit

Executing command: interface Ethernet 0/5

Executing command: switchport access vlan 1

Executing command: no shutdown

Executing command: exit

Executing command: interface Ethernet 0/6

Executing command: switchport access vlan 1

Executing command: no shutdown

Executing command: exit

Executing command: interface Ethernet 0/7

Executing command: switchport access vlan 1

Executing command: no shutdown

Executing command: exit

Executing command: interface vlan2

Executing command: nameif outside

INFO: Security level for "outside" set to 0 by default.

Executing command: no shutdown

Executing command: ip address dhcp setroute

Executing command: exit

Executing command: interface vlan1

Executing command: nameif inside

INFO: Security level for "inside" set to 100 by default.

Executing command: ip address 172.16.1.1 255.255.255.0

Executing command: security-level 100

Executing command: allow-ssc-mgmt

ERROR: SSC card is not available

Executing command: no shutdown

Executing command: exit

Executing command: object network obj\_any

Executing command: subnet 0.0.0.0 0.0.0.0

Executing command: nat (inside,outside) dynamic interface

Executing command: exit

Executing command: http server enable

Executing command: http 172.16.1.0 255.255.255.0 inside

Executing command: dhcpd address 172.16.1.5-172.16.1.36 inside

Executing command: dhcpd auto\_config outside

Executing command: dhcpd enable inside

Executing command: logging asdm informational

Factory-default configuration is completed

ciscoasa(config)#

ciscoasa(config)#

ciscoasa(config)#

ciscoasa(config)#

ciscoasa(config)#

ciscoasa(config)#

ciscoasa(config)#

ciscoasa(config)#interface vlan 1

ciscoasa(config-if)#nameif inside

ciscoasa(config-if)#ip address 172.16.1.1 255.255.255.0

ciscoasa(config-if)#security-level 100

ciscoasa(config-if)#exit

ciscoasa(config)#int ethernet 0/1

ciscoasa(config-if)#switchport access vlan 1

ciscoasa(config-if)#exit

ciscoasa(config)#int vlan 2

ciscoasa(config-if)#nameif outside

ciscoasa(config-if)#ip address 200.1.1.2 255.255.255.240

```
ciscoasa(config-if)#security-level 0
```

```
ciscoasa(config-if)#exit
```

```
ciscoasa(config)#int ethernet 0/0
```

```
ciscoasa(config-if)#switchport access vlan 2
```

```
ciscoasa(config-if)#exit
```

```
ciscoasa(config)#int vlan 3
```

```
ciscoasa(config-if)#nameif dmz
```

ERROR: This license does not allow configuring more than 2 interfaces with nameif and without a "no forward" command on this interface or on 1 interface(s) with nameif already configured.

```
ciscoasa(config-if)#no forward interface vlan 1
```

```
ciscoasa(config-if)#nameif dmz
```

INFO: Security level for "dmz" set to 0 by default.

```
ciscoasa(config-if)#ip address 10.1.1.1 255.255.255.0
```

```
ciscoasa(config-if)#sec
```

```
ciscoasa(config-if)#security-level 50
```

```
ciscoasa(config-if)#exit
```

```
ciscoasa(config)#int e
```

```
ciscoasa(config)#int ethernet 0/2
```

```
ciscoasa(config-if)#switch
```

```
ciscoasa(config-if)#switchport access vlan 3
```

```
ciscoasa(config-if)#
```

```
ciscoasa#
```

%SYS-5-CONFIG\_I: Configured from console by console

```
ciscoasa#show switch vlan
```

VLAN Name Status Ports

-----

1 inside up Et0/1, Et0/3, Et0/4, Et0/5

Et0/6, Et0/7

2 outside up Et0/0

3 dmz up Et0/2

```
ciscoasa#show ip address
```

System IP Addresses:

Interface Name	IP address	Subnet mask	Method
----------------	------------	-------------	--------

Vlan1	inside	172.16.1.1 255.255.255.0	CONFIG
-------	--------	--------------------------	--------

Vlan2	outside	200.1.1.2 255.255.255.240	manual
-------	---------	---------------------------	--------

Vlan3	dmz	10.1.1.1 255.255.255.0	manual
-------	-----	------------------------	--------

Current IP Addresses:

Interface Name	IP address	Subnet mask	Method
----------------	------------	-------------	--------

Vlan1	inside	172.16.1.1 255.255.255.0	CONFIG
-------	--------	--------------------------	--------

Vlan2	outside	200.1.1.2 255.255.255.240	manual
-------	---------	---------------------------	--------

Vlan3	dmz	10.1.1.1 255.255.255.0	manual
-------	-----	------------------------	--------

```
ciscoasa#
```