

# *Cryptographie-Sécurité Services*

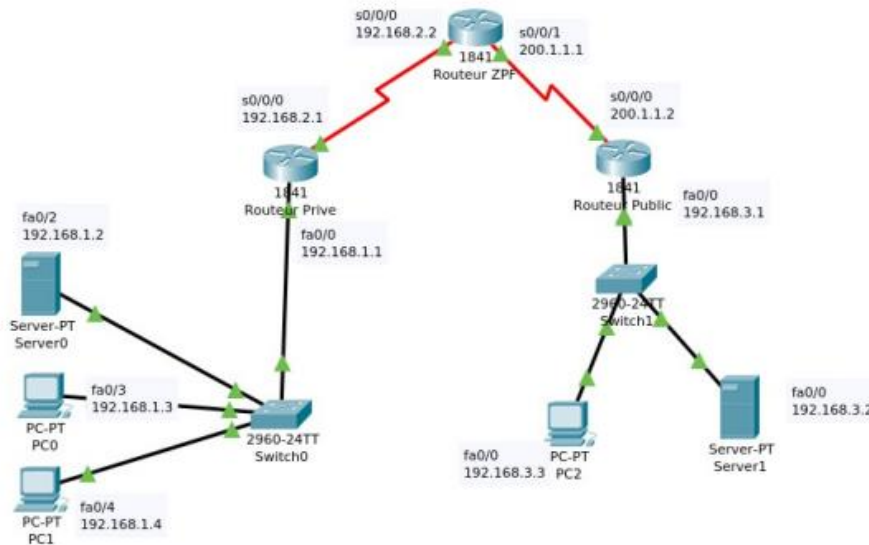
## Zone-Based Policy Firewall-1



Réalisé Par :

Yossra safi chetouan

## TP : configurer un Routeur Zone-Based Policy Firewall (Zfw)



Configuration du Routeur privé :

```
Router Privé

Physical  Config  CLI  Attributes

IOS Command Line Interface

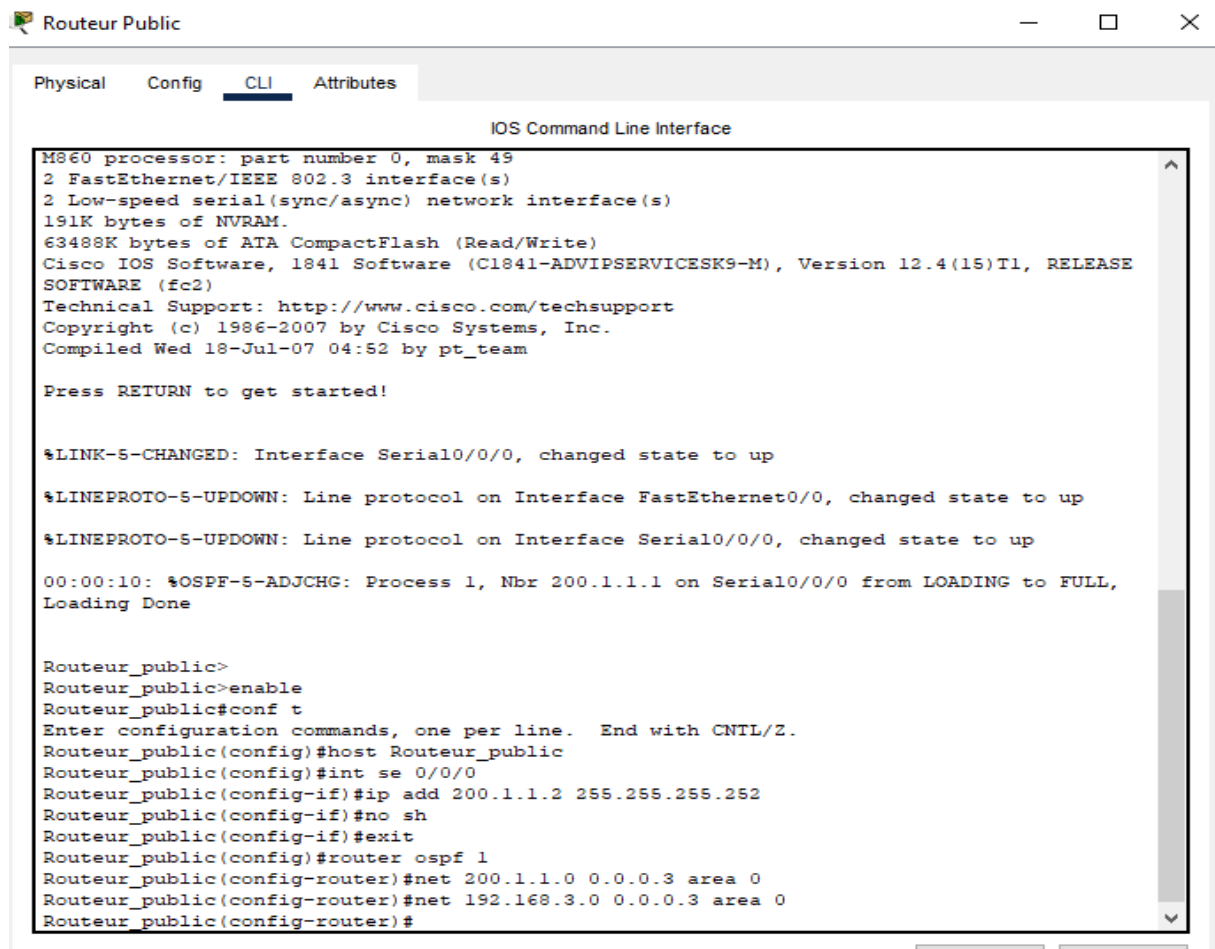
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

Press RETURN to get started!

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 200.1.1.1 on Serial0/0/0 from LOADING to FULL,
Loading Done

Routeur_privé>enable
Routeur_privé#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Routeur_privé(config)#host Routeur_privé
Routeur_privé(config)#int se 0/0/0
Routeur_privé(config-if)#ip add 192.168.2.1 255.255.255.252
Routeur_privé(config-if)#no sh
Routeur_privé(config-if)#router ospf 1
Routeur_privé(config-router)#net 192.168.1.0 0.0.0.255 area 0
Routeur_privé(config-router)#net 192.168.2.0 0.0.0.3 area 0
Routeur_privé(config-router)#exit
Routeur_privé(config)#router ospf 1
Routeur_privé(config-router)#net 192.168.1.0 0.0.0.255 area 0
Routeur_privé(config-router)#net 192.168.2.0 0.0.0.3 area 0
Routeur_privé(config-router)#
```

## Configuration du Routeur public :



The screenshot shows a Cisco IOS Command Line Interface (CLI) window titled "Routeur Public". The window has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" currently selected. The CLI displays the following text:

```
IOS Command Line Interface
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

Press RETURN to get started!

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 200.1.1.1 on Serial0/0/0 from LOADING to FULL,
Loading Done

Routeur_public>
Routeur_public>enable
Routeur_public#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Routeur_public(config)#host Routeur_public
Routeur_public(config)#int se 0/0/0
Routeur_public(config-if)#ip add 200.1.1.2 255.255.255.252
Routeur_public(config-if)#no sh
Routeur_public(config-if)#exit
Routeur_public(config)#router ospf 1
Routeur_public(config-router)#net 200.1.1.0 0.0.0.3 area 0
Routeur_public(config-router)#net 192.168.3.0 0.0.0.3 area 0
Routeur_public(config-router)#
```

## Configuration du Routeur zfw :

Physical
Config
CLI
Attributes

IOS Command Line Interface

```

Routeur_Zfw>enable
Routeur_Zfw#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Routeur_Zfw(config)#host Routeur_Zfw
Routeur_Zfw(config)#ip ssh version 2
Routeur_Zfw(config)#class-map type inspect match-any priv-allow-class
Routeur_Zfw(config-cmap)#match protocol telnet
Routeur_Zfw(config-cmap)#match protocol http
Routeur_Zfw(config-cmap)#match protocol icmp
Routeur_Zfw(config-cmap)#match protocol tcp
Routeur_Zfw(config-cmap)#policy-map type inspect pmap
Routeur_Zfw(config-pmap)#class type inspect priv-allow-class
Routeur_Zfw(config-pmap-c)#inspect
Routeur_Zfw(config-pmap-c)#class type inspect class-default
Routeur_Zfw(config-pmap-c)#exit
Routeur_Zfw(config-pmap)#exit
Routeur_Zfw(config)#zone security prive
Routeur_Zfw(config-sec-zone)#zone security public
Routeur_Zfw(config-sec-zone)#zone-pair security priv-pub source prive destination public
Routeur_Zfw(config-sec-zone-pair)#service-policy type inspect pmap
Routeur_Zfw(config-sec-zone-pair)#exit
Routeur_Zfw(config)#int se 0/0/0
Routeur_Zfw(config-if)#ip add 192.168.2.2 255.255.255.252
Routeur_Zfw(config-if)#clo r 64000
Routeur_Zfw(config-if)#zone-member security prive
Routeur_Zfw(config-if)#no sh
Routeur_Zfw(config-if)#int se 0/0/1
Routeur_Zfw(config-if)#ip add 200.1.1.2 255.255.255.252
Routeur_Zfw(config-if)#
00:11:04: %OSPF-5-ADJCHG: Process 1, Nbr 200.1.1.2 on Serial0/0/1 from FULL to DOWN,
Neighbor Down: Interface down or detached

Routeur_Zfw(config-if)#
00:11:11: %OSPF-5-ADJCHG: Process 1, Nbr 200.1.1.2 on Serial0/0/1 from LOADING to FULL,
Loading Done

Routeur_Zfw(config-if)#

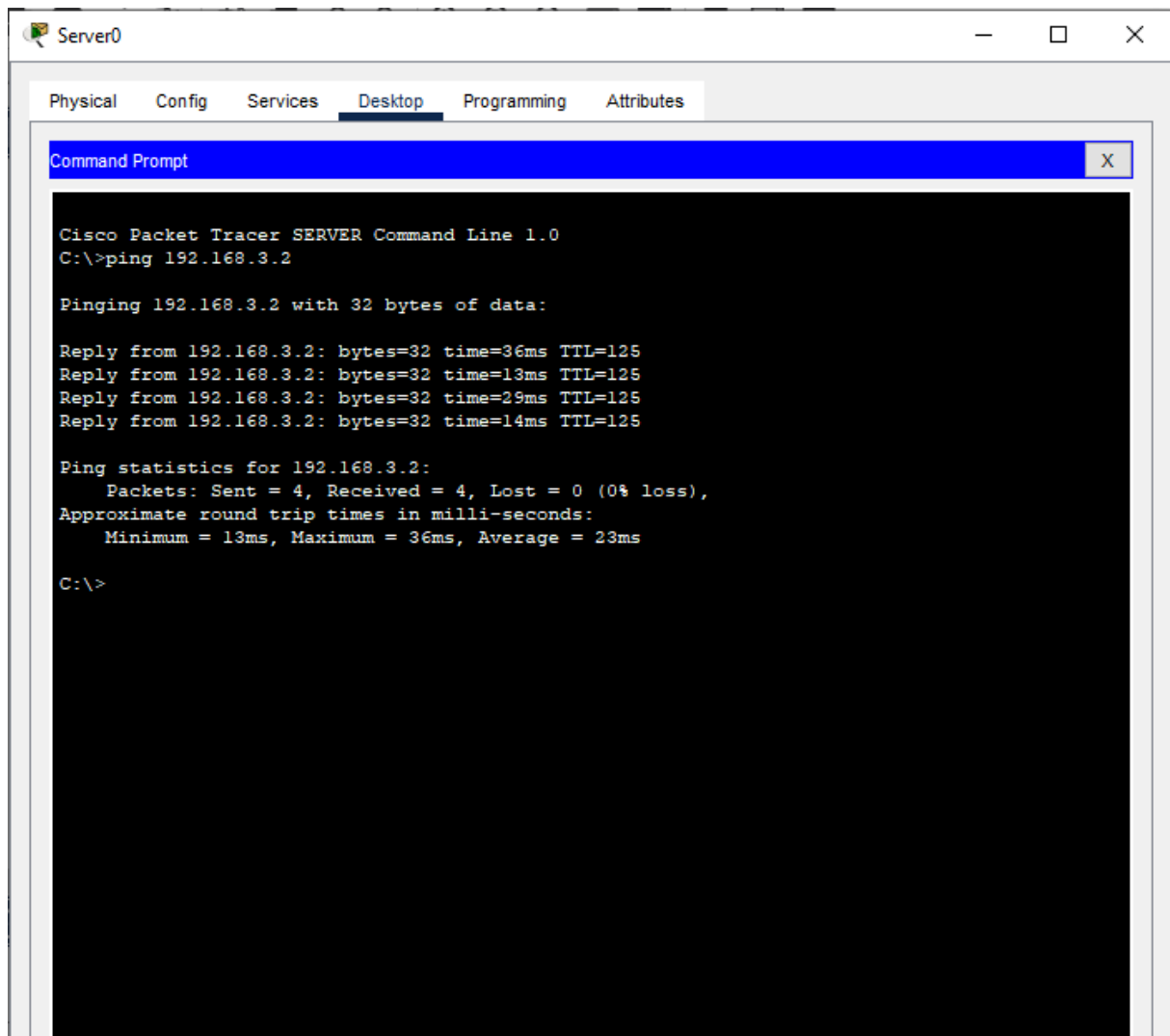
Routeur_Zfw(config-if)#zone-member security public
Routeur_Zfw(config-if)#clo r 64000
Routeur_Zfw(config-if)#no sh
Routeur_Zfw(config-if)#router ospf 1
Routeur_Zfw(config-router)#net 192.168.2.0 0.0.0.3 area 0
Routeur_Zfw(config-router)#net 192.168.2.0 0.0.0.3 area 0
Routeur_Zfw(config-router)#net 200.1.1.0 0.0.0.3 area 0
Routeur_Zfw(config-router)#

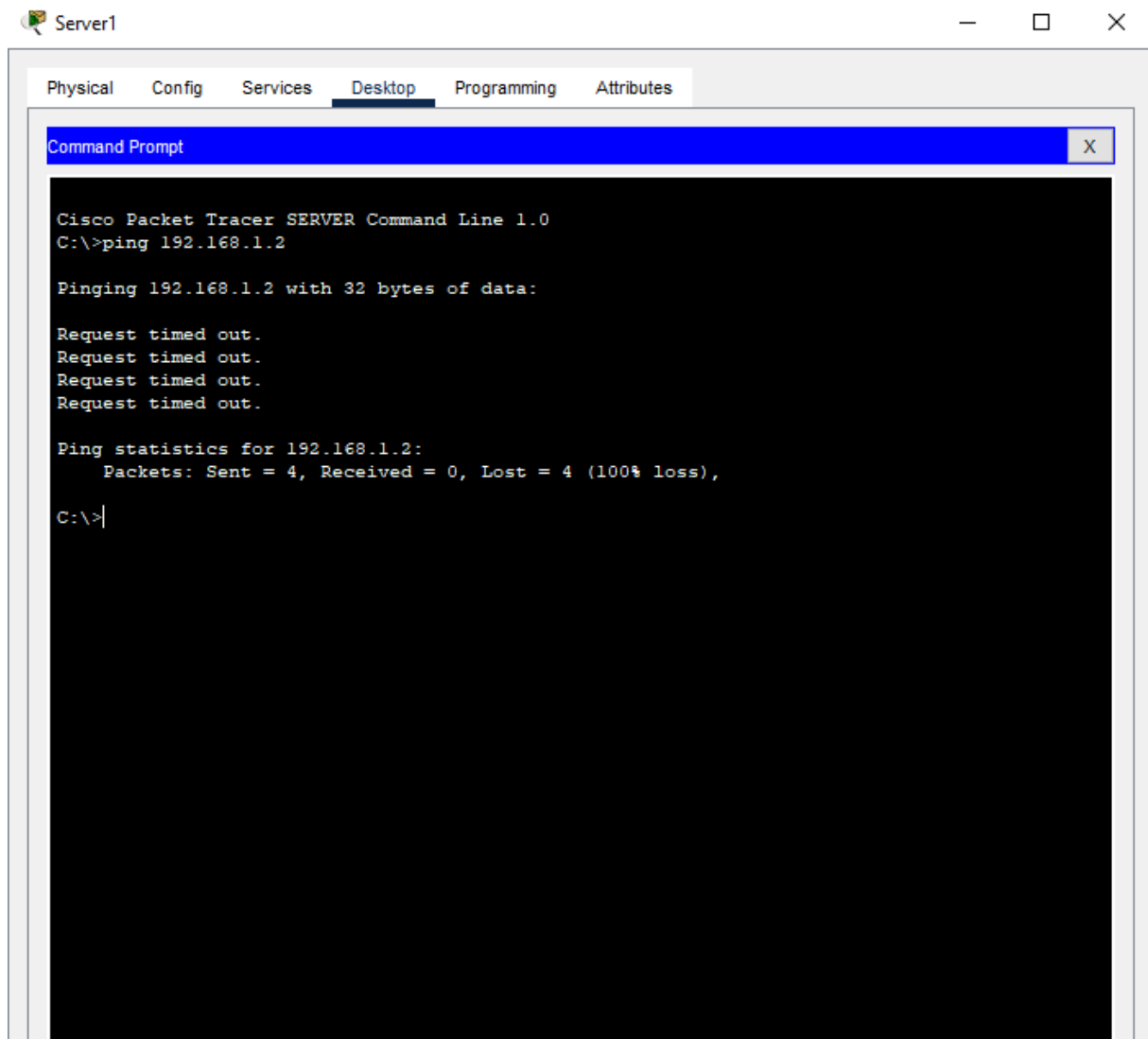
```

### Test de Configuration du ZFW

<div> Realtime Simulation </div>									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	Route...	Routeur P...	ICMP		0.000	N	0	(edit)
	Failed	Route...	Routeur Pr...	ICMP		0.000	N	1	(edit)
	Successful	Server0	Routeur P...	ICMP		0.000	N	2	(edit)

tester ftp entre les deux serveurs ftp( privé et publique)





tester http entre les deux serveurs web( privé et publique)

