TP : Mise en place des ACL sous Cisco Packet Tracer

Alyssia – Gad – BTS SIO SISR

Vérifications finales :

- Ping VLAN 10 -> VLAN 20 -> doit être bloqué

PC0 -> ping 192.168.20.10 -> Cela prouve que le ping est bloqué (ACL appliquée sur VLAN 10).

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- Accès HTTP/HTTPS VLAN 10 → VLAN 30 : doit être fonctionnel PC0 -> Web Browser

L'interface du serveur web s'affiche correctement après saisie de l'adresse http://192.168.30.10.
Cela prouve que la communication HTTP entre le VLAN 10 (utilisateurs) et le VLAN 30 (DMZ) est autorisée par l'ACL.

L'accès web fonctionne, preuve du filtrage sélectif de l'ACL.

- Vérifier que les flux autorisés sont corrects et les flux interdits bloqués.

PC0 -> ping 192.168.20.10

```
C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Le ping du VLAN 10 vers le VLAN 20 échoue.
Cela prouve que les flux non autorisés par l'ACL (trafic vers les serveurs internes) sont correctement bloqués.

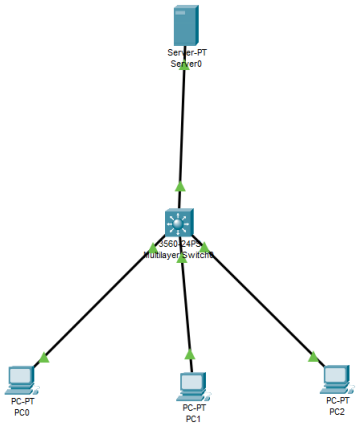
Ping vers la DMZ -> ping 192.168.30.10

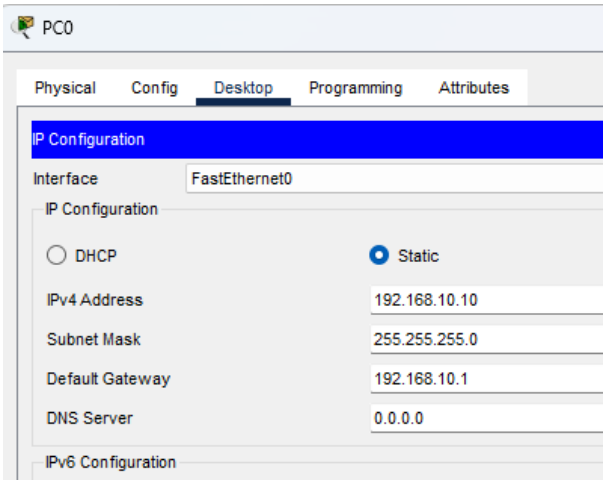
```
C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

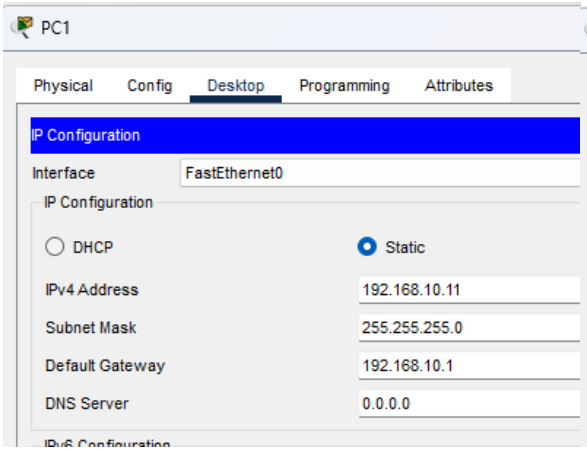
Le ping vers la DMZ est bloqué.
Cela montre que seuls les flux spécifiquement autorisés (HTTP/HTTPS) sont permis, les autres sont filtrés.

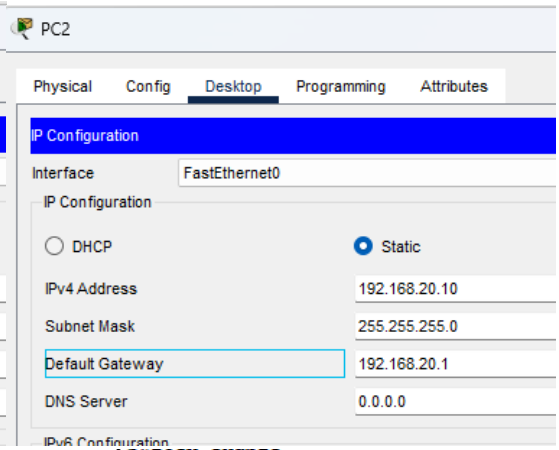
Les tests effectués confirment que les flux sont filtrés selon la politique définie :

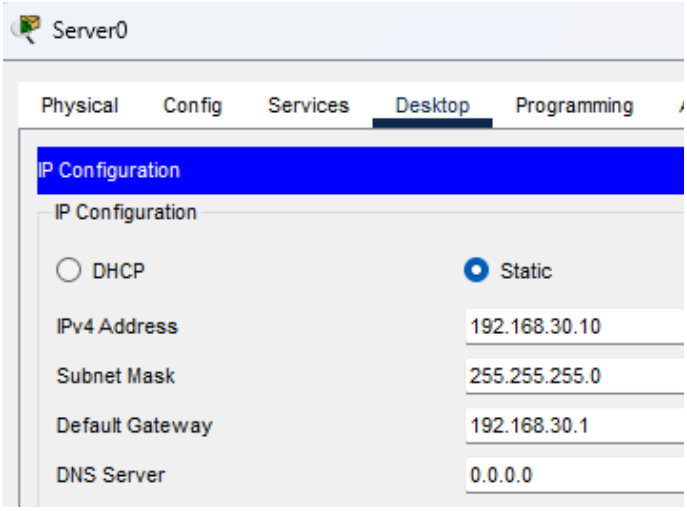
- Les flux interdits (VLAN10 → VLAN20, ping non autorisé) sont bloqués.
- Les flux autorisés (HTTP/HTTPS vers VLAN30) sont accessibles.



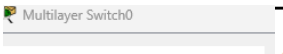









```
Switch#show running-config
Building configuration...

Current configuration : 1931 bytes
!
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
ip routing
!
!
!
!
 --More--
```




```
!
hostname Switch
!
!
!
!
!
!
ip routing
!
!
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 --More--
```

```
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
 --More--
```

```
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
 --More--
```

```
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 mac-address 00d0.ba1c.e901
 ip address 192.168.10.1 255.255.2
 ip access-group 100 in
!
interface Vlan20
 mac-address 00d0.ba1c.e902
 --More--
```

```
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 mac-address 00d0.ba1c.e901
 ip address 192.168.10.1 255.255.255.0
 ip access-group 100 in
!
interface Vlan20
 mac-address 00d0.ba1c.e902
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan30
 mac-address 00d0.ba1c.e903
 ip address 192.168.30.1 255.255.255.0
!
ip classless
!
ip flow-export version 9
!
!
access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 100 permit tcp 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 eq www
access-list 100 permit tcp 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 eq 443
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any established
!
!
!
!
!
!
line con 0
 --More--
```

Configuration switch :

Switch# show running-config

ip routing
vlan 10
name USERS
vlan 20
name SERVER
 vlan 30
name DMZ

interface FastEthernet0/1
switchport mode access
switchport access vlan 10

interface FastEthernet0/2
switchport mode access
switchport access vlan 10

interface FastEthernet0/3
switchport mode access
switchport access vlan 20

interface FastEthernet0/4

```
switchport mode access
switchport access vlan 30
interface Vlan10
ip address 192.168.10.1 255.255.255.0
ip access-group 100 in no shutdown
interface Vlan20
ip address 192.168.20.1 255.255.255.0
no shutdown

interface Vlan30
ip address 192.168.30.1 255.255.255.0
no shutdown

access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 100 permit tcp 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 eq 80
access-list 100 permit tcp 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 eq 443
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any established
end

copy running-config startup-config
```