

TP CONFIGURATION AVEC PACKET TRACER

PAR : Dr. KIE VICTOIRE

ENNONCE :

Configuration de pare-feu avec packet tracer

Adressage

- Réseau interne : 192.168.1.0/24
- Réseau externe : 192.168.2.0/24

Topologie Le réseau se compose de deux réseaux, un réseau interne et un réseau externe. Le réseau interne est connecté au réseau externe par un pare-feu.

Réseau interne 192.168.1.0/24

PC1 192.168.1.10

PC2 192.168.1.20

Réseau externe 192.168.2.0/24 PC3 192.168.2.10

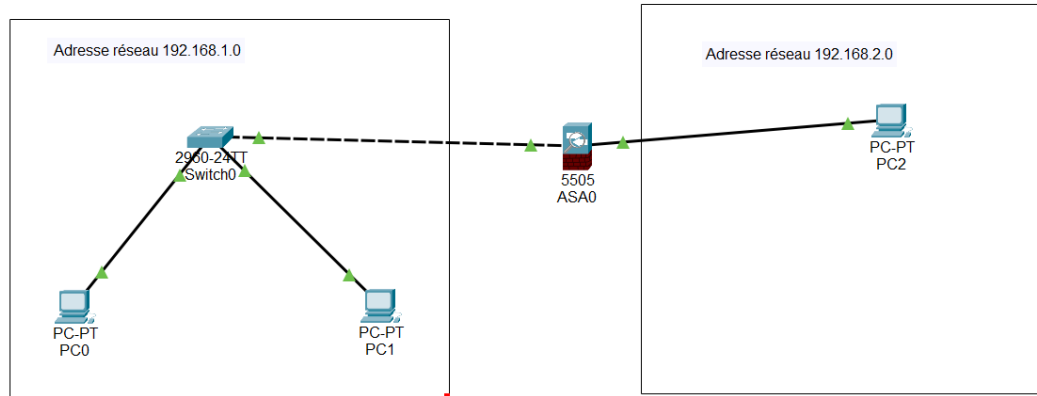
Exercice 1 : Configurer un pare-feu statique

1. Ouvrir Packet Tracer et créer un nouveau projet
2. Ajout d'un pare-feu, de deux ordinateurs sur le réseau interne et d'un ordinateur sur le réseau externe
3. Configuration de l'adressage IP des périphériques
4. Configuration du pare-feu
 - a) Activation de pare-feu
 - b) Ajout d'une règle filtrage pour autoriser le trafic TCP et UDP entre le réseau interne et le réseau externe sur tous les ports
5. Testez la configuration en envoyant un message du trafic entre les ordinateurs du réseau interne et du réseau externe

Exercice 2 : Configurer un pare-feu dynamique

1. Configuration du pare-feu
2. Ajout d'une règle de filtrage pour autoriser le trafic TCP et UDP entre le réseau interne et le réseau externe sur les ports 80 et 443
3. Ajout d'une règle de filtrage pour bloquer tout le trafic provenant d'un autre ordinateur sur le réseau externe
4. Test de la configuration en envoyant un message du trafic entre les ordinateurs du réseau interne et du réseau externe.

I. EXERCICE 1 : CONFIGURER UN PARE-FEU STATIQUE



Topologie du Réseau

PC0

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.10

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address

Link Local Address FE80::201:C7FF:FE58:2CDE

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

PC1

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.20

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address

Link Local Address FE80::20A:41FF:FE06:EB73

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

Configuration du réseau interne : PC1 et PC2

PC2

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.2.10

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::201:C9FF:FE47:B205

Default Gateway

DNS Server

802.1X

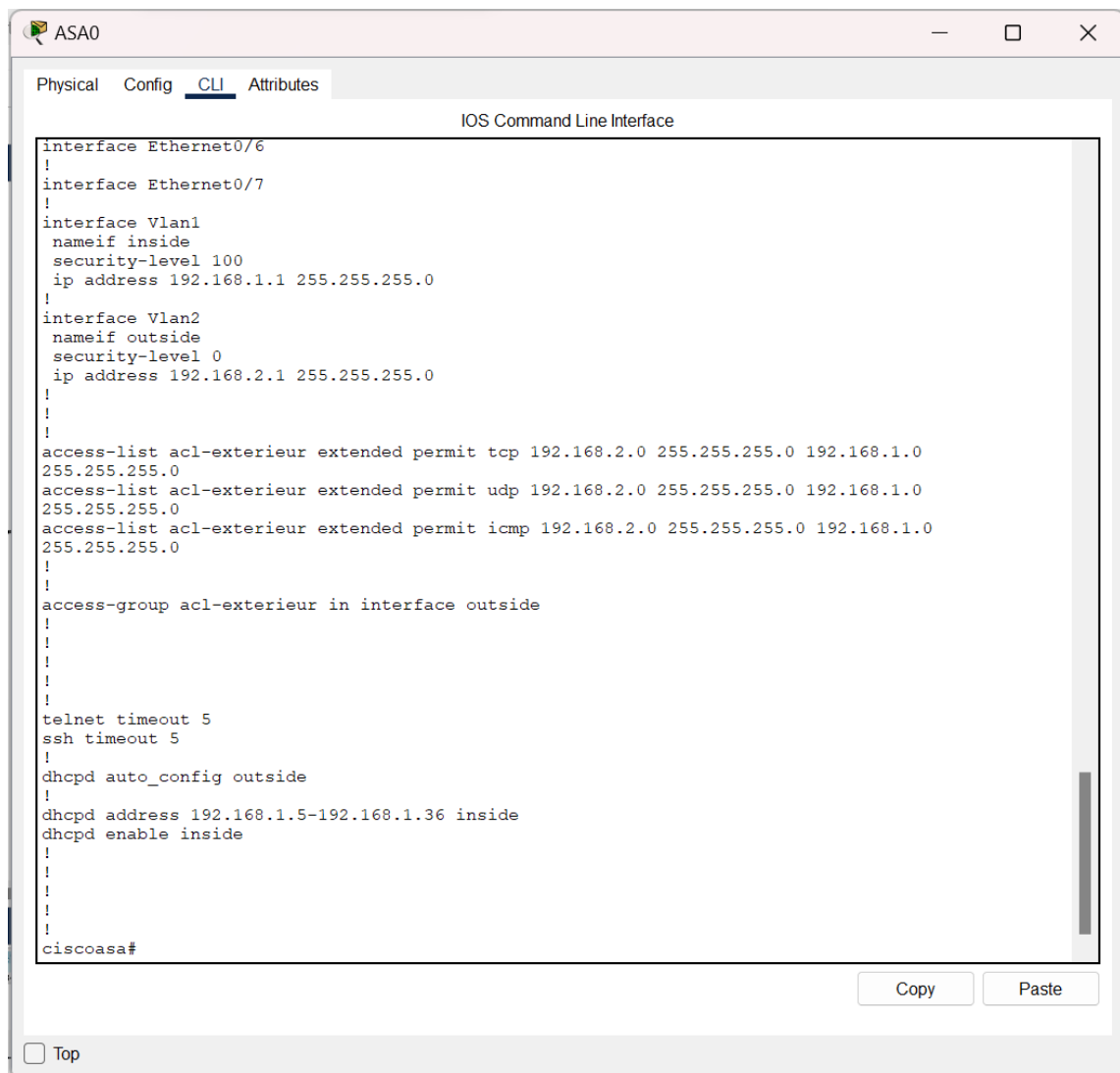
☐ Use 802.1X Security

Authentication MD5

Username

Password

Configuration du réseau externe : PC3



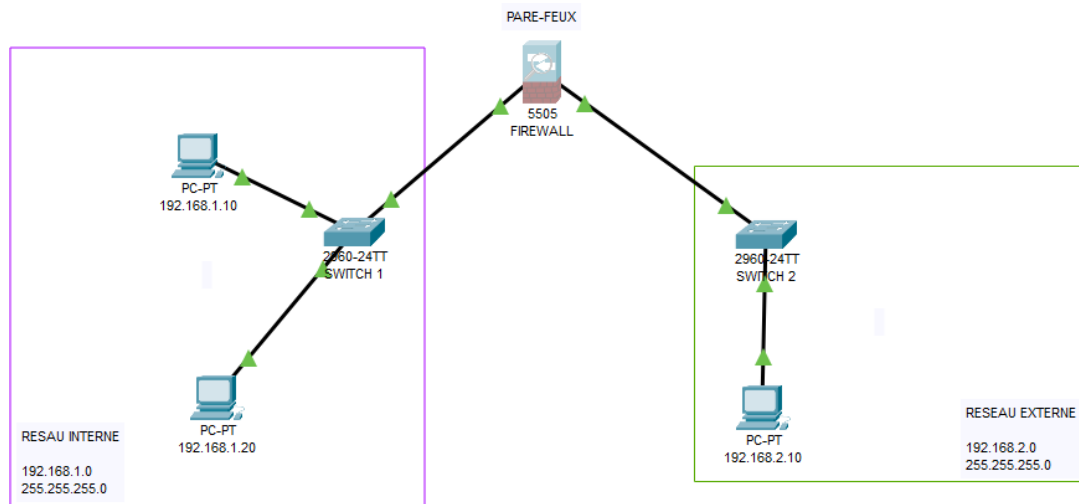
The screenshot shows a window titled "ASA0" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The configuration text is as follows:

```
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 192.168.2.1 255.255.255.0
!
!
!
access-list acl-exterieur extended permit tcp 192.168.2.0 255.255.255.0 192.168.1.0
255.255.255.0
access-list acl-exterieur extended permit udp 192.168.2.0 255.255.255.0 192.168.1.0
255.255.255.0
access-list acl-exterieur extended permit icmp 192.168.2.0 255.255.255.0 192.168.1.0
255.255.255.0
!
!
access-group acl-exterieur in interface outside
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
!
!
!
!
ciscoasa#
```

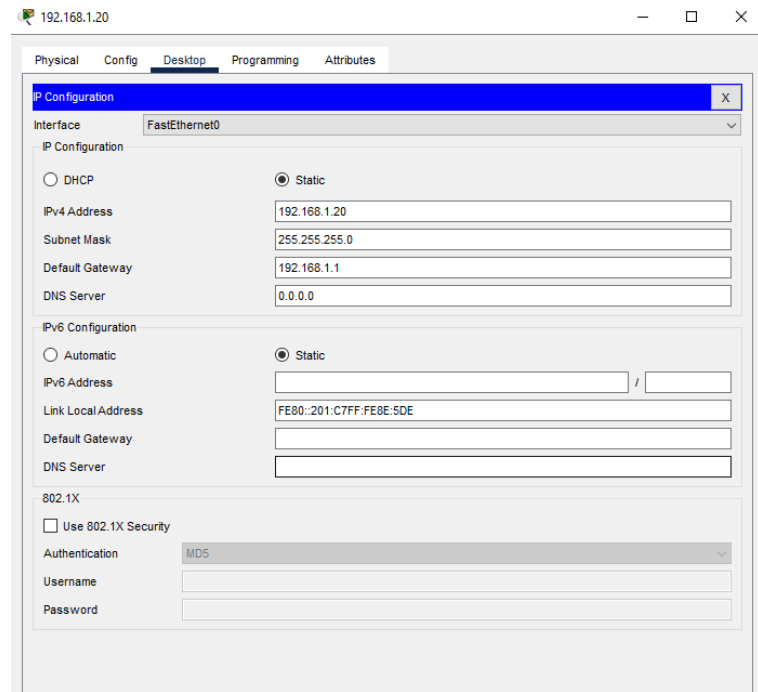
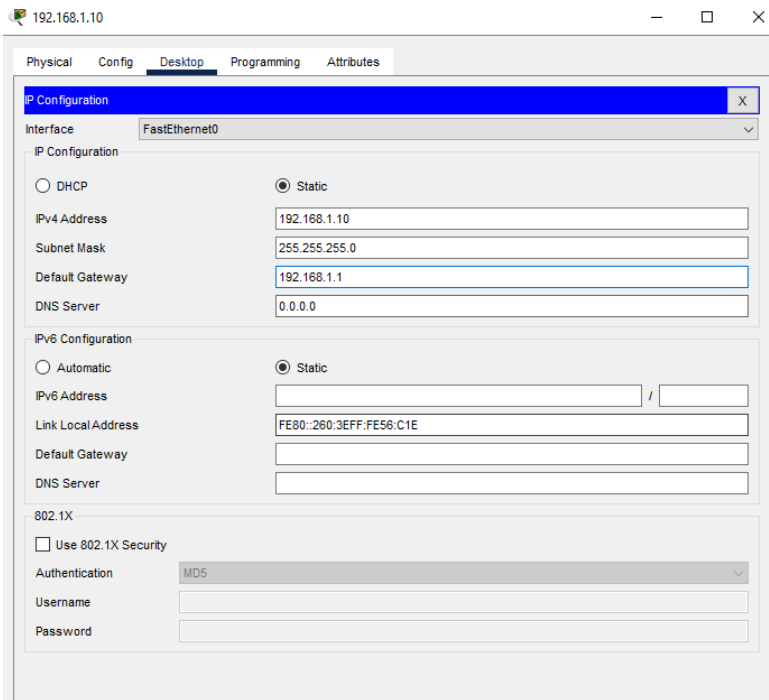
At the bottom right of the CLI window, there are "Copy" and "Paste" buttons. At the bottom left of the window, there is a "Top" button with a checkbox.

Configuration du pare-feu : mise en place de l'ACL

II. EXERCICE 2 : CONFIGURER UN PARE-FEU DYNAMIQUE



Topologie du Réseau



Configuration RESEAU INTERNE : PC1 et PC2

192.168.2.10

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface **FastEthernet0**

IP Configuration

☐ DHCP ☒ Static

IPv4 Address

Subnet Mask

Default Gateway

DNS Server

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address

Link Local Address

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication

Username

Password

Configuration RESEAU EXTERNE : PC3

ASA0

Physical Config **CLI** Attributes

IOS Command Line Interface

```

!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp
!
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpcd auto_config outside
!
!
dhcpcd address 192.168.1.5-192.168.1.36 inside
dhcpcd enable inside
!

```

Copy Paste

```

!
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#conf term
ciscoasa(config)#int vlan1
ciscoasa(config-if)#nameif interne
ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#int vlan2
ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0ip address 192.168.2.1
255.255.255.0
ciscoasa(config-if)#security-level 100ip address 192.168.2.1no shutdownno shutdown
ciscoasa(config-if)#end
ciscoasa#show run
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0

```

Copy

Paste

Configuration initiale du pare-feu ASA5505

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

```

Test de vérification de la configuration (Succès)


```

interface Vlan1
 nameif interne
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif externe
 security-level 0
 ip address 192.168.2.1 255.255.255.0
!
!
!
access-list firewall_acl extended permit tcp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list firewall_acl extended permit udp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
!
!
access-group firewall_acl in interface externe
!
!
!
!
telnet timeout 5
ssh timeout 5
!
<--- More --->
ciscoasa#
ciscoasa#conf term
ciscoasa(config)#no access-list firewall_acl extended permit tcp 192.168.2.0
255.255.255.0 192.168.1.0 255.255.255.0
ciscoasa(config)#no access-list firewall_acl_dyn extended permit tcp 192.168.2.0
255.255.255.0 192.168.1.0 255.255.255.0 eq 80
ERROR: access-list <firewall_acl_dyn> does not exist
ciscoasa(config)#access-list firewall_acl_dyn extended permit tcp 192.168.2.0
255.255.255.0 192.168.1.0 255.255.255.0 eq 80
ciscoasa(config)#access-list firewall_acl_dyn extended permit udp 192.168.2.0
255.255.255.0 192.168.1.0 255.255.255.0 eq 80
ciscoasa(config)#access-list firewall_acl_dyn extended permit udp 192.168.2.0
255.255.255.0 192.168.1.0 255.255.255.0 eq 443
ciscoasa(config)#access-list firewall_acl_dyn extended permit tcp 192.168.2.0
255.255.255.0 192.168.1.0 255.255.255.0 eq 443
ciscoasa(config)#access-list firewall_acl_dyn extended deny tcp host 192.168.2.10
192.168.1.0 255.255.255.0
ciscoasa(config)#access-group firewall_acl_dyn in terminal externe
^
% Invalid input detected at '^' marker.

ciscoasa(config)#access-group firewall_acl_dyn in interface externe
ciscoasa(config)#access-list firewall_acl_dyn extended deny udp host 192.168.2.10
192.168.1.0 255.255.255.0
ciscoasa(config)#show run

```

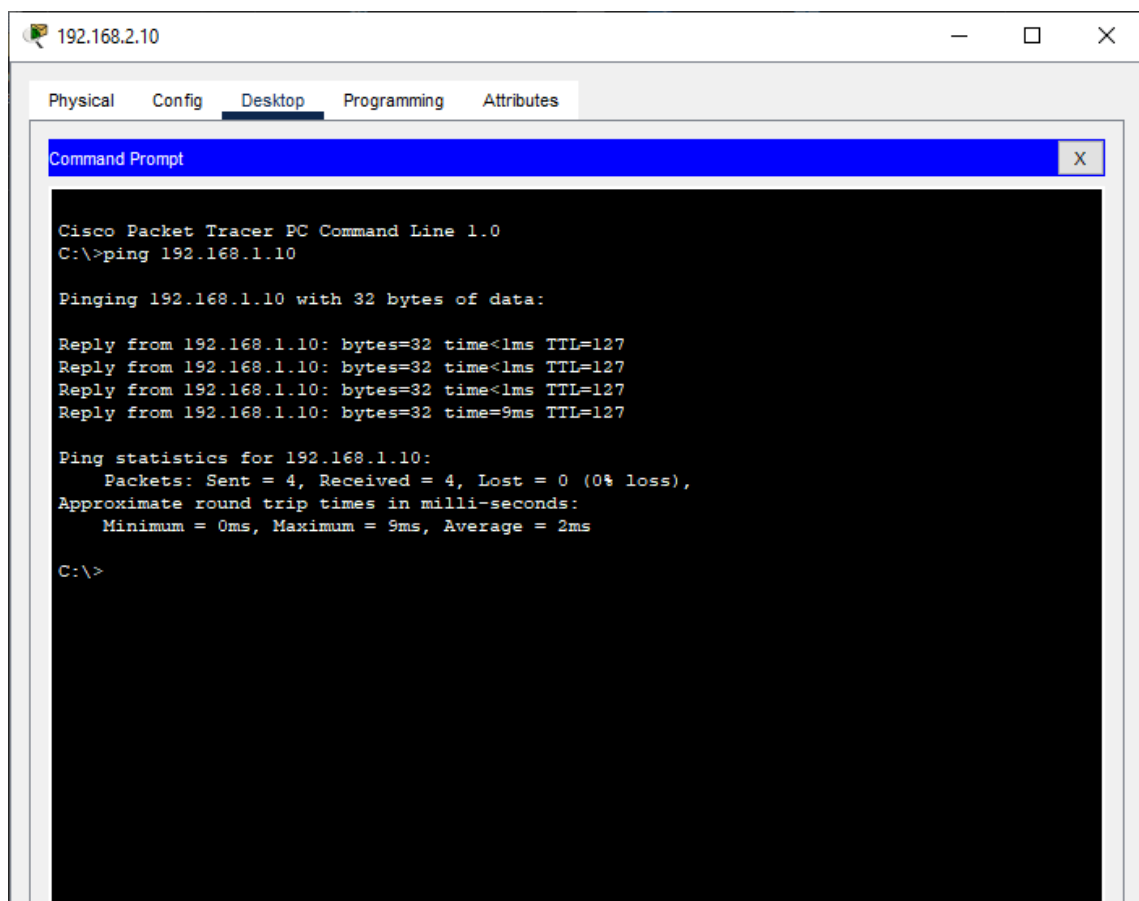
Configuration des règles d'accès

```

!
access-list firewall_acl extended permit udp 192.168.2.0 255.255.255.0 192.168.1.0
255.255.255.0
access-list firewall_acl_dyn extended permit tcp 192.168.2.0 255.255.255.0 192.168.1.0
255.255.255.0 eq www
access-list firewall_acl_dyn extended permit udp 192.168.2.0 255.255.255.0 192.168.1.0
255.255.255.0 eq www
access-list firewall_acl_dyn extended permit udp 192.168.2.0 255.255.255.0 192.168.1.0
255.255.255.0 eq 443
access-list firewall_acl_dyn extended permit tcp 192.168.2.0 255.255.255.0 192.168.1.0
255.255.255.0 eq 443
access-list firewall_acl_dyn extended deny tcp host 192.168.2.10 192.168.1.0
255.255.255.0
access-list firewall_acl_dyn extended deny udp host 192.168.2.10 192.168.1.0
255.255.255.0
!
!
access-group firewall_acl_dyn in interface externe
!
!
<--- More --->

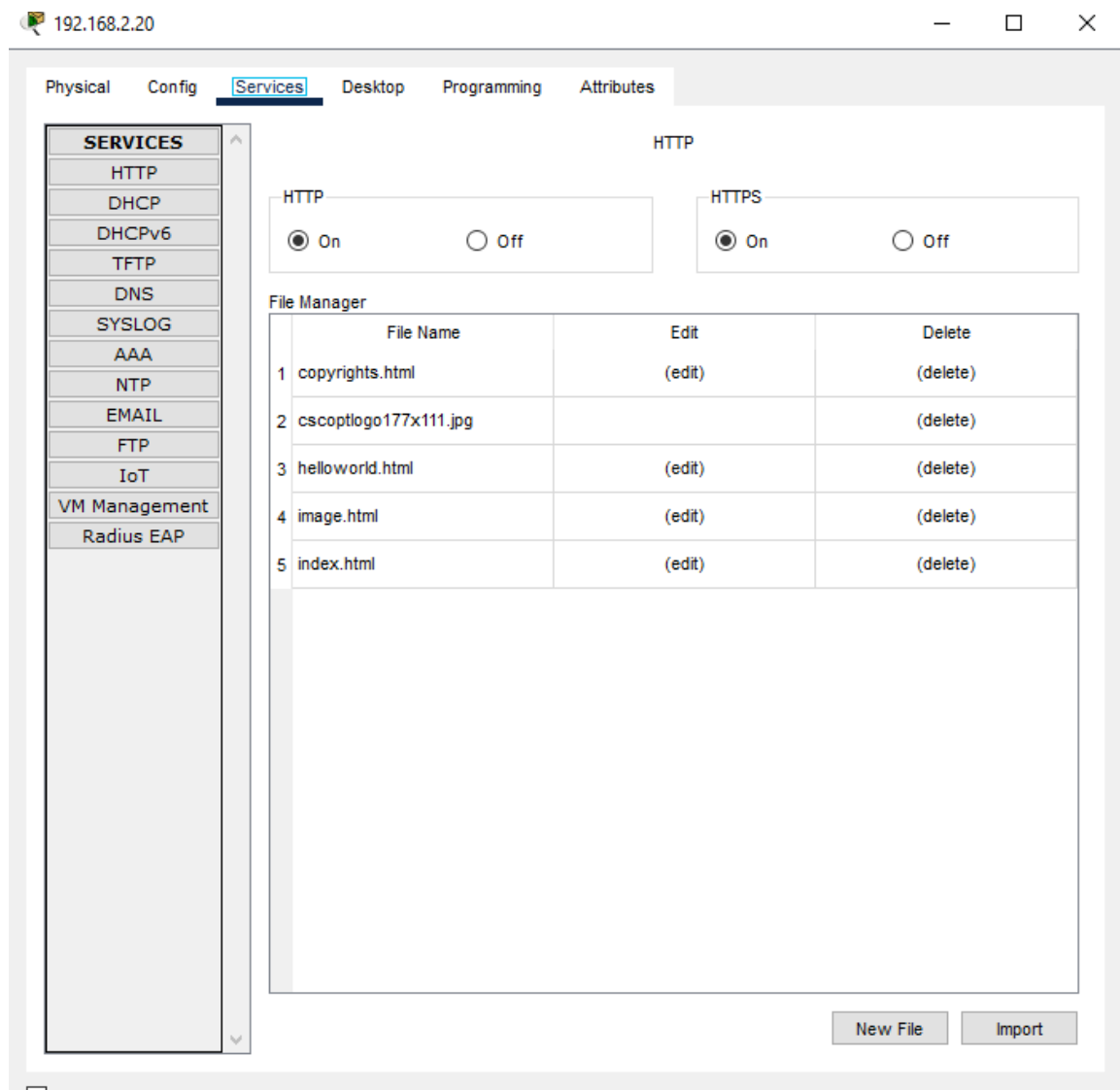
```

Résumé de la configuration de l'ACL

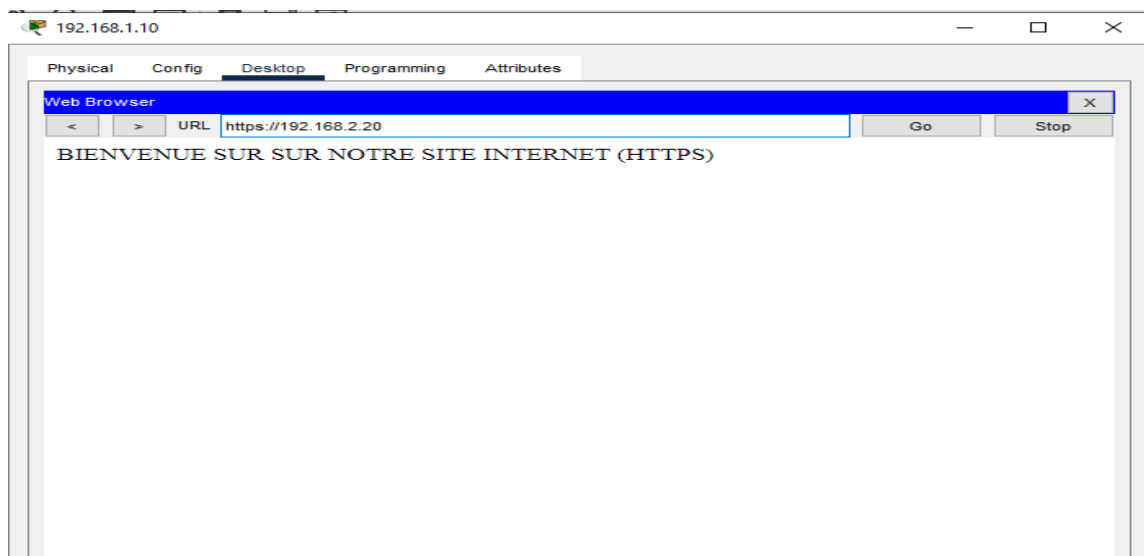
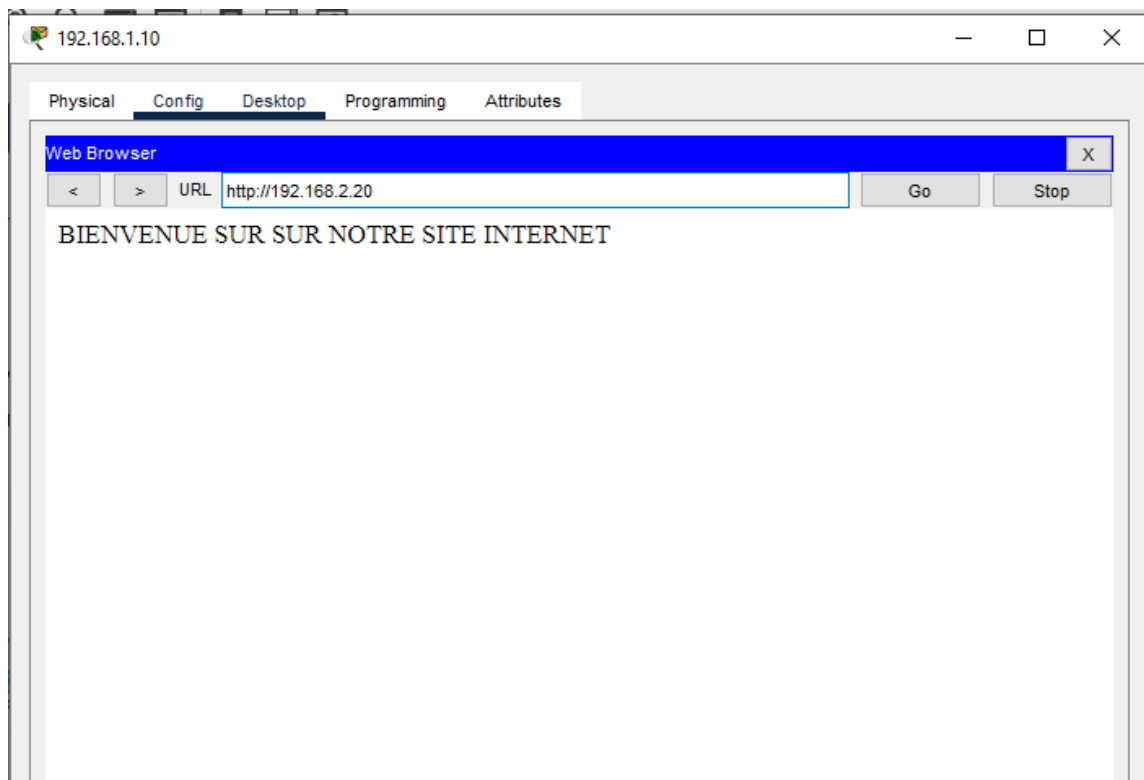


Test de vérification de la configuration (Succès)

Note : nous avons dû ajouter un serveur pour tester les communications sur les ports 80 ET 443.



Activation des services HTTP et HTTPS



Test de vérification HTTP et HTTPS (réussie)

Réponses aux questions

- a. Quels sont les avantages et les inconvénients des pare-feux statiques ?

Les pare-feux statiques offrent une approche traditionnelle de la sécurité réseau. Leurs avantages incluent leur simplicité de configuration, leur stabilité opérationnelle et leur contrôle fin sur le trafic. Cependant, leur manque de flexibilité, leur gestion manuelle et leurs potentielles vulnérabilités en font des solutions moins adaptées aux environnements réseau en constante évolution.

- b. Quels sont les avantages et les inconvénients des pare-feux dynamiques ?

Les pare-feux dynamiques quant à eux, s'adaptent automatiquement aux changements dans le trafic et les menaces détectées, offrant ainsi une meilleure protection contre les attaques sophistiquées. Leur gestion simplifiée et leur capacité à détecter les menaces en temps réel sont des points forts. Cependant, leur complexité de configuration, leur coût potentiellement plus élevé et le risque de faux positifs sont des inconvénients à prendre en compte. L'utilisation des pare-feux font appelle à certaines règles de filtrage.

c. Quels sont les différents types de règles de filtrage ?

Les règles de filtrage des pare-feux peuvent être classées en plusieurs catégories, notamment le filtrage par adresse IP, par port, par protocole, par application et par contenu. Chaque type de règle offre un niveau de contrôle différent sur le trafic réseau, permettant ainsi de répondre à des besoins spécifiques en matière de sécurité.

d. Comment configurer un pare-feu pour autoriser le trafic entre deux réseaux ?

Pour configurer un pare-feu afin d'autoriser le trafic entre deux réseaux, il est nécessaire d'identifier les interfaces correspondant à chaque réseau et de définir des règles de filtrage appropriées.

e. Comment configurer un pare-feu pour bloquer le trafic provenant d'une adresse IP ou d'un réseau spécifique ?

Pour configurer un pare-feu pour bloquer le trafic provenant d'une adresse IP ou d'un réseau spécifique :

1. Accédez à l'interface de configuration de votre pare-feu,
2. Identifiez la section ou l'option permettant de configurer les règles de filtrage ou les règles de pare-feu.
3. Ajoutez une nouvelle règle de filtrage ou de pare-feu.

4. Spécifiez l'adresse IP ou le réseau que vous souhaitez bloquer dans le champ approprié.
5. Définissez l'action à prendre pour le trafic provenant de cette adresse ou de ce réseau (par exemple, bloquer ou rejeter).
6. Sauvegardez et appliquez les modifications.
7. Assurez-vous que la règle de filtrage ou de pare-feu est correctement positionnée dans l'ordre de priorité pour qu'elle soit appliquée efficacement.
8. Testez la configuration pour vous assurer que le trafic est bloqué comme prévu.