

Rapport SAÉ 21

Construire un réseau informatique pour petite structure

G. Urvoy-Keller, M. Lance

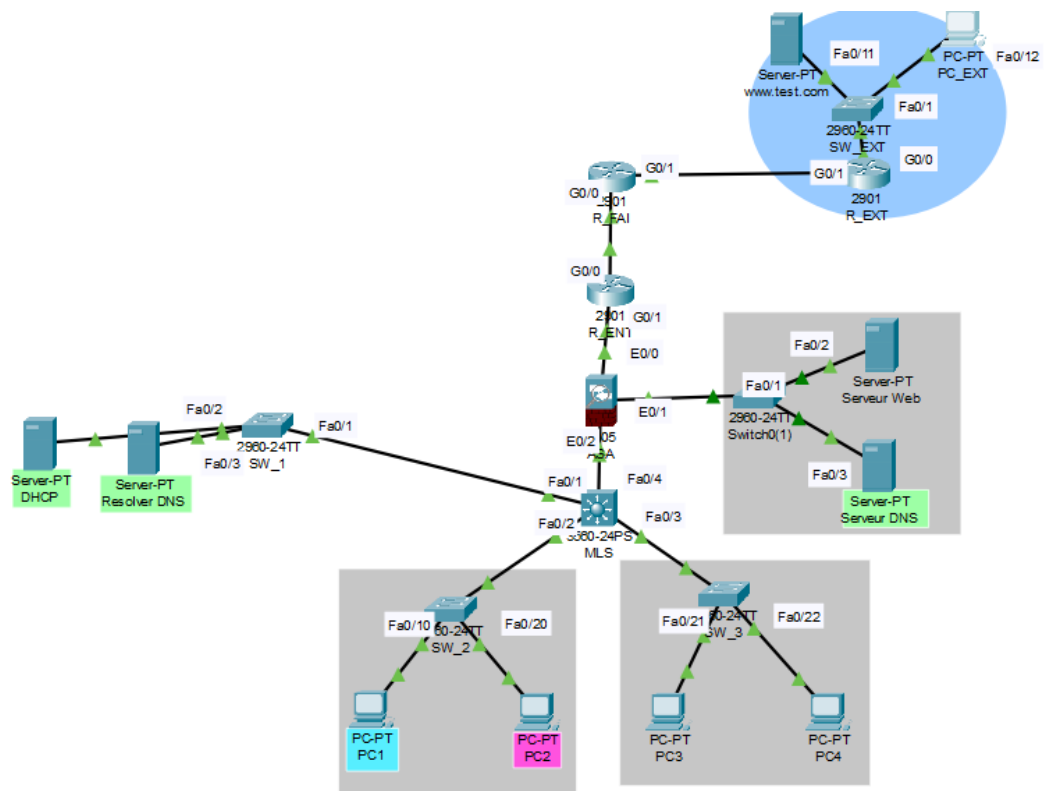


Plan d'adressage IP de base :

Sur la page suivante vous trouverez l'adressage IP de base auquel nous nous sommes référées tout au long de notre S.A.É. Il peut y avoir eu des changements vers la fin notamment sur les hôtes internes avec l'activation et la mise en place du service DHCP.



Avec les interfaces sur chacun des équipements réseaux :



Étape 1 : Construction de cœur de réseau avec les commutateurs d'accès et le Multi-layer.

On configure dans un tout premier temps le Multilayer switch :

Switch(config)#hostname MLS → On renomme le Switch

création des vlan + nomination :

```
MLS(config)#vlan 30
MLS(config-vlan)#name ServeursInternes
MLS(config-vlan)#vlan 10
MLS(config-vlan)#name RH
MLS(config-vlan)#vlan 20
MLS(config-vlan)#name Ingenierie
```

→ On attribue un nom à chaque vlan pour différencier les unités mais cela reste d'ordre facultatif.

On configure le mode trunk ou le lien multi-vlan :

Le mode "trunk" est, rappelons-le, un protocole de communication qui permet de regrouper plusieurs connexions réseau en une seule.

- augmente la bande passante
- optimiser l'utilisation des ressources

```
MLS(config)#interface fa0/1
MLS(config-if)#switchport trunk encapsulation dot1q
MLS(config-if)#switchport mode trunk
```

```
MLS(config)#interface fa0/2
MLS(config-if)#switchport trunk encapsulation dot1q
MLS(config-if)#switchport mode trunk
```

```
MLS(config-if)#interface fa0/3
MLS(config-if)#switchport trunk encapsulation dot1q
MLS(config-if)#switchport mode trunk
```

Affectation des vlan sur une interface :

```
MLS(config-vlan)#interface vlan 10
MLS(config-if)#ip address 172.15.1.1 255.255.255.0
MLS(config-if)#exit
```

```
MLS(config)#interface vlan 20
MLS(config-if)#ip address 172.15.2.1 255.255.255.0
MLS(config-if)#exit
```

```
MLS(config)#interface vlan 30
MLS(config-if)#ip address 172.15.3.1 255.255.255.0
MLS(config-if)#exit
```

Autorisation du routage au sein du MultilayerSwitch :

```
MLS(config)#ip routing
```

À partir de ce moment-là, les vlans sont capables de communiquer entre elles à condition qu'elles soient dans le même vlan.

Nous allons maintenant configurer chacun des trois switchs afin que tous les hôtes du LAN puissent communiquer entre eux, quelle que soit leur vlan d'appartenance.

CONFIGURATION SW_1 :

Activation du mode multi-vlan (trunk):

```
Switch(config)#hostname SW_1
SW_1(config)#interface Fa0/1
SW_1(config-if)#switchport mode trunk
SW_1(config-if)#exit
```

Ajout des vlans :

```
SW_1(config)#vlan 10
SW_1(config-vlan)#vlan 20
SW_1(config-vlan)#vlan 30
```

Affectation VLAN au SW_1 :

```
SW_1(config)#interface range fa0/2-3
SW_1(config-if-range)#switchport mode access
SW_1(config-if-range)#switchport access vlan 30
```

CONFIGURATION SW_2 :

```
SW_2(config)#interface fa0/2
SW_2(config-if)#switchport mode trunk
```

```
SW_2(config)#vlan 10
SW_2(config-vlan)#vlan 20
SW_2(config-vlan)#vlan 30
```

```
SW_2(config-if)#int fa0/20
SW_2(config-if)#switchport mode access
```

```
SW_2(config-if)#switchport access vlan 20
```

```
SW_2(config-if)#int fa0/10
```

```
SW_2(config-if)#switchport mode access
```

```
SW_2(config-if)#switchport access vlan 10
```

CONFIGURATION SW_3 :

```
Switch(config)#hostname SW_3
```

```
SW_3(config)#int fa0/3
```

```
SW_3(config-if)#switchport mode trunk
```

```
SW_3(config-if)#vlan 10
```

```
SW_3(config-vlan)#vlan 20
```

```
SW_3(config-vlan)#vlan 30
```

```
SW_3(config-vlan)#interface range fa0/21-22
```

```
SW_3(config-if-range)#switchport mode access
```

```
SW_3(config-if-range)#switchport access vlan 20
```

Étape 2 : Ajout de l'ASA et du service DHCP.

1.

CONFIGURATION DU MLS :

```
MLS(config)#int fa0/4
```

```
MLS(config-if)#no switchport
```

→ Désactive le niveau 2 et fait passer le MLS au niveau 3 (la couche réseau, où le routage se produit) afin de lui assigner une adresse IP pour le connecter au réseau d'interconnexion 192.168.10.0/30.

configuration de l'adresse IP sur l'interface fa0/4 :

```
MLS(config-if)#ip address 192.168.10.1 255.255.255.252
```

```
MLS(config-if)#no shut
```

CONFIGURATION DE L'ASA :

```
ciscoasa(config)#hostname ASA
```

```
ASA(config)#int G1/4
```

```
ASA(config-if)#ip address 192.168.10.2 255.255.255.252
ASA(config-if)#no shut
```

2.

- On active le service DNS sur le resolver DNS au sein des serveurs internes.
- On y ajoute la correspondance entre l'adresse ip et le nom de domaine du serveur WEB comme suit :

Resolver DNS

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type

Address

No.	Name	Type	Detail
0	www.test.com	A Record	8.8.8.1

☐ Top

Lorsqu'un client effectue une requête DNS pour www.test.com, le serveur DNS répond avec l'adresse IP associée à cet enregistrement A, permettant ainsi au client d'établir une connexion avec le serveur externe. L'enregistrement A signifie "Adress" et est donc utilisé pour résoudre un nom de domaine en adresse IP.

Les enregistrements NS (Name Server) sont utilisés pour définir les serveurs de noms autoritaires pour une zone donnée, tandis que les enregistrements MX (Mail Exchange) sont utilisés pour spécifier les serveurs de messagerie associés à un domaine.

3.

CONFIGURATION DU SERVEUR DHCPv4 :

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: DHCP-VLAN30

Default Gateway: 172.15.3.1

DNS Server: 172.15.3.31

Start IP Address: 172.15.3.1

Subnet Mask: 255.255.255.0

Maximum Number of Users: 254

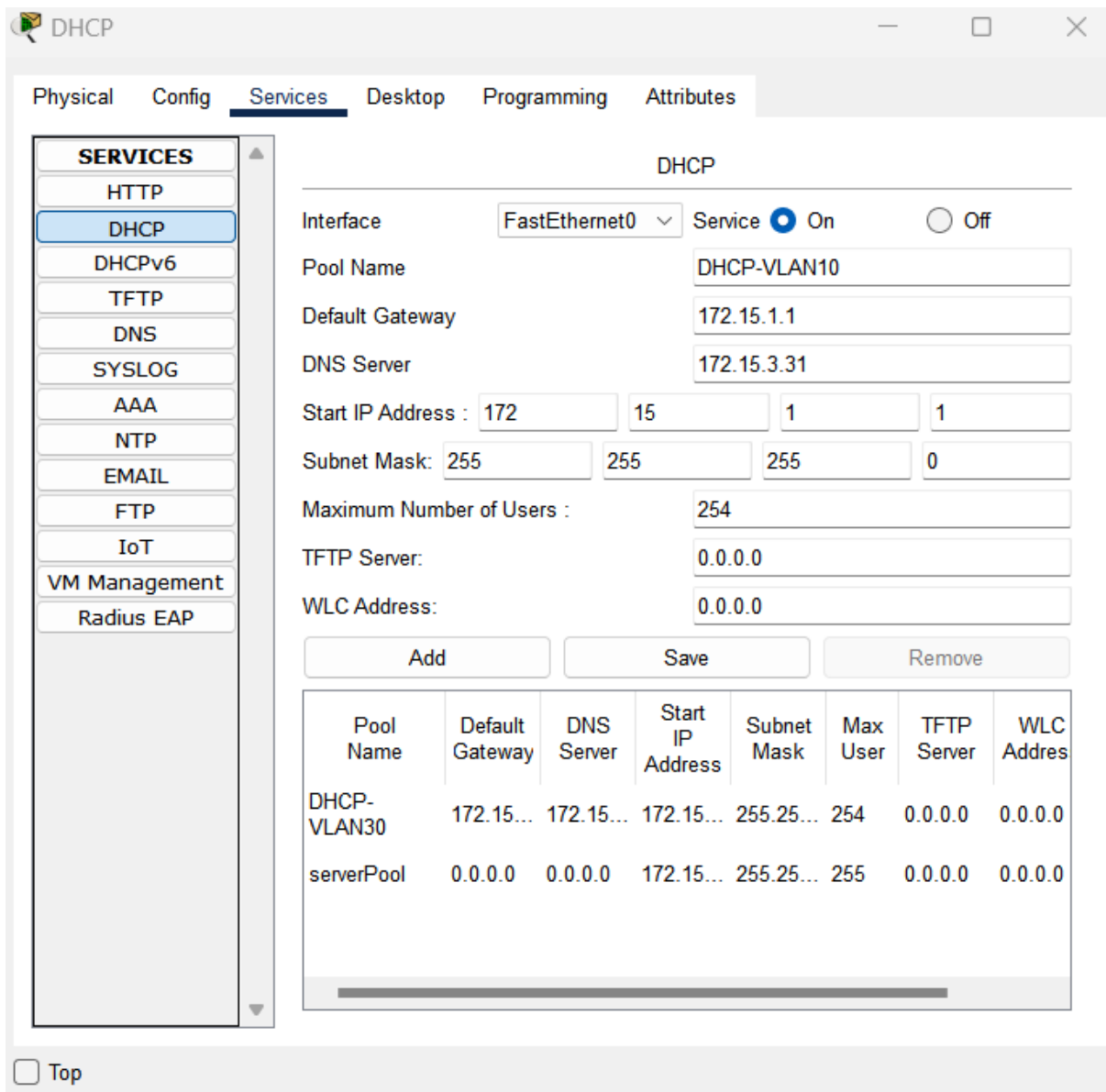
TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Buttons: Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
DHCP-VLAN30	172.15...	172.15...	172.15...	255.25...	254	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	172.15...	255.25...	255	0.0.0.0	0.0.0.0

☐ Top



SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: DHCP-VLAN20

Default Gateway: 172.15.2.1

DNS Server: 172.15.3.31

Start IP Address: 172 15 2 2

Subnet Mask: 255 255 255 0

Maximum Number of Users: 254

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Buttons: Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	W Adc
DHCP-VLAN20	172.15...	172.15...	172.15...	255.25...	254	0.0.0.0	0.0.
DHCP-VLAN30	172.15...	172.15...	172.15...	255.25...	254	0.0.0.0	0.0.
DHCP-VLAN10	172.15...	172.15...	172.15...	255.25...	254	0.0.0.0	0.0.

☐ Top

Dans le serveur DHCP situé dans la zone des serveurs internes au sein de la VLAN 30, on configure un pool par Vlan, afin que chaque hôte de chaque vlan puisse acquérir une adresse automatiquement s'ils le souhaitent.

Pour ce faire on crée donc 3 pools d'adresses, un pour chaque vlan avec comme configuration :

- Le pool name pour les différencier.
- L'adresse de la passerelle du réseau de la VLAN sélectionnée.
- L'adresse du serveur DNS qui sera utilisé pour la translation d'adresse, qui est le resolver DNS dans la zone des serveurs internes.
- La première adresse pouvant être utilisée du pool.

- Le masque du réseau concerné par le pool.
- Le nombre d'utilisateur pouvant acquérir une adresse automatiquement via ce pool.

CONFIGURATION DU MULTILAYER SWITCH :

Afin que chaque vlan puisse se référer à un même serveur DHCP, on utilise une commande suivante sur le MultiLayer Switch au sein de chaque vlan comme suit :

```
MLS>en
```

```
MLS#conf t
```

```
MLS(config)#interface vlan 30
```

```
MLS(config-if)#ip helper-address 172.15.3.30
```

```
MLS(config-if)#interface vlan 10
```

```
MLS(config-if)#ip helper-address 172.15.3.30
```

```
MLS(config-if)#interface vlan 20
```

```
MLS(config-if)#ip helper-address 172.15.3.30
```

```
MLS(config-if)#end
```

```
MLS#write
```

Les requêtes DHCP provenant des autres VLANs seront redirigées vers le serveur DHCP dans le VLAN serveur (VLAN 30) à l'aide de "ip-helper address" configurées sur le MLS. Nous pouvons donc ainsi utiliser un unique serveur DHCP pour tous les VLANs au lieu d'en avoir un par VLAN.

Cela fonctionne ! Exemple ci-dessous sur le PC3 situé dans la VLAN20 :

The screenshot shows the configuration window for PC3, specifically the 'Desktop' tab. The 'IP Configuration' section is active, showing settings for the 'FastEthernet0' interface. The 'DHCP' option is selected, and a message indicates 'DHCP request successful.' The IPv4 Address is 172.15.2.2, Subnet Mask is 255.255.255.0, Default Gateway is 172.15.2.1, and DNS Server is 172.15.3.31. The 'IPv6 Configuration' section shows 'Static' selected, with a Link Local Address of FE80::260:5CFF:FE8B:AA66. The '802.1X' section shows 'Use 802.1X Security' unchecked, 'Authentication' set to MD5, and empty fields for Username and Password. A 'Top' button is at the bottom left.

PC3

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IPv4 Address 172.15.2.2

Subnet Mask 255.255.255.0

Default Gateway 172.15.2.1

DNS Server 172.15.3.31

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::260:5CFF:FE8B:AA66

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

Étape 3 : Ajout de la DMZ et du routeur du FAI.

La configuration de l'ASA :

Passons à la sécurité de l'ASA CISCO 5505. Sur Packet Tracer il est initialement défini avec un vlan 1 et un vlan 2. Pour nous assurer que leur configuration soit correcte, il nous faut les définir manuellement tel que ci-dessous.

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.10.2 255.255.255.252
!
interface Vlan2
nameif outside
security-level 0
ip address 192.168.11.253 255.255.255.252
!
interface Vlan3
no forward interface Vlan1
nameif dmz
security-level 50
ip address 192.168.1.254 255.255.255.0
```

→ À noter: le 'no forward interface vlan 1' est utilisé dans packet Tracer dans le but de pouvoir ajouter une troisième interface : la vlan 3 qui représente l'interface 'dmz'.

On observe ainsi que chaque interface a un 'security-level' différent. En effet, lors de la définition d'une interface de l'asa, il est nécessaire de spécifier un 'security-level' en fonction de la zone où l'on se trouve. Pour plus de précisions :

- Concernant l'interface vlan 1 : Cette Vlan représente l'interface 'inside' dont le niveau de sécurité est généralement défini à 100, ce qui est le niveau de sécurité le plus élevé. En effet l'interface 'inside' est connectée au réseau interne de l'entreprise, le réseau de confiance où se trouvent les ressources sensibles de l'entreprise : les postes de travail, les serveurs internes par exemple.
- Concernant l'interface vlan 3 : Cette Vlan représente l'interface 'dmz' (Zone démilitarisée) où le niveau de sécurité est généralement inférieur à celui de l'interface 'inside' et supérieur à celui de l'interface 'outside', dans notre cas nous l'avons situé au milieu : à 50. Les serveurs hébergés dans la DMZ peuvent être configurés pour fournir des services aux utilisateurs externes tout en étant isolés des ressources internes critiques.
- Concernant l'interface vlan 2 : Cette Vlan représente l'interface 'outside' au niveau de sécurité le plus bas, à 0. Il s'agit du réseau externe à l'entreprise, non fiable. En effet,

l'entreprise ne contrôle pas ce qui se passe à l'extérieur et il faut protéger les ressources de l'entreprise des potentiels risques.

Concernant le trafic entre ces trois zones définies de manière distinctive, le flux de trafic sortant depuis l'interface 'inside' vers des interfaces de niveau de sécurité inférieur comme pour la dmz ou les réseaux externes est autorisé. Cependant ce n'est pas le cas dans le sens inverse : le trafic entrant depuis des interfaces à niveaux de sécurité inférieurs vers des niveaux de sécurité supérieurs ne sera pas autorisé sauf dans le cas où des règles programmées sur l'asa fassent effet.

Après configuration de l'ASA, nous implémenterons ces règles sous forme de listes de contrôles d'accès (ACL) appliquées aux interfaces correspondantes, afin d'avoir un contrôle sécurisé sur le trafic entrant et sortant.

On affecte ensuite aux interfaces correspondantes les vlans avec le mode 'switchport access' :

```
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
switchport access vlan 3
```

Il est ensuite important de s'occuper du routage statique. Afin d'établir une connectivité entre l'ASA et les hôtes du réseau interne, il faut spécifier des routes statiques vers chacun des réseaux locaux :

```
ASA(config)#route inside 172.15.1.0 255.255.255.0 192.168.10.1
ASA(config)#route inside 172.15.2.0 255.255.255.0 192.168.10.1
ASA(config)#route inside 172.15.3.0 255.255.255.0 192.168.10.1
ASA(config)#route outside 0.0.0.0 0.0.0.0 192.168.11.254
```

Et sur le MultilayerSwitch également où nous avons configuré une route par défaut :

```
MLS(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.2
```

Enfin nous avons configuré une route vers l'interface de la vlan 3 connectée directement à l'interface de la DMZ afin de pouvoir accéder à ses hôtes.

```
ASA(config)#route dmz 172.15.3.0 255.255.255.0 192.168.1.1 1
```

Définition des listes de contrôles d'accès sur le pare-feu.

Étant donné que le réseau externe ne peut pas accéder au réseau interne selon la configuration de base d'un ASA, il faut établir une ACL dans le but d'autoriser l'envoi de données d'un réseau externe vers un réseau interne à une seule condition : qu'un hôte du réseau interne ait initié la connexion tcp.

ainsi voici la liste d'accès correspondante OUT_IN :

```
ASA(config)#access-list OUT_IN extended permit icmp any any echo-reply
ASA(config)#access-list OUT_IN extended permit tcp any any
```

```
ASA(config)#access-group OUT_IN out interface inside
```

Ensuite, le serveur web se trouvant dans la zone de la DMZ de l'entreprise, il est important que les utilisateurs externes puissent y accéder. Pour cela il faut autoriser le trafic uniquement pour des connexions sur les ports 80 et 443 afin d'accéder au serveur WEB www.entreprise.com tel que :

```
ASA(config)#access-list web extended permit tcp any any eq www
ASA(config)#access-list web extended permit tcp any any eq 443
```

```
ASA(config)#access-group web out interface dmz
```


Pour s'assurer que le trafic des données ait lieu et renforcer la sécurité, nous avons défini encore un paramètre sur notre ASA, à savoir une classe d'inspection du trafic icmp comme ci-dessous :

```
class-map inspection_default
match default-inspection-traffic
!
policy-map global_policy
class inspection_default
inspect icmp
!
service-policy global_policy interface dmz
```

- On définit donc une classe d'inspection par défaut 'inspection_default' utilisée pour identifier le trafic devant être davantage surveillé.
- La commande 'match default-inspection-traffic' permet d'associer la classe venant d'être initiée 'inspection_default' aux critères de trafic d'inspection (inspection des protocoles HTTP, FTP, DNS, ICMP par exemple).
- On définit ensuite une 'policy-map global_policy' pour spécifier qu'un trafic doit être inspecté.
- On indique ensuite sous cette politique que la classe 'inspection-default' sera concernée par cette politique.
- Puis sous cette class on lui attribue le critère de trafic d'inspection correspondant au trafic ICMP qui sera inspecté, avec la commande 'inspect icmp'
- Enfin, on applique la politique à l'interface DMZ : 'service-policy global_policy interface dmz'.

Avec cette configuration, la sécurité du réseau de la dmz a été renforcée en initiant l'inspection du trafic des paquets ICMP.

Configuration du NAT statique et dynamique sur le routeur R_ENT :

Pour que les réseaux internes à l'entreprise aient accès aux ressources externes dont celles d'Internet, nous avons mis en place une traduction d'adresse (Network Address Translation) au sein du routeur R_ENT.

On définit tout d'abord les interfaces 'nat inside' et 'nat outside' du routeur R_ENT:

```
interface GigabitEthernet0/1
ip address 192.168.11.254 255.255.255.252
ip nat inside
duplex auto
speed auto
```

```
interface GigabitEthernet0/0
ip address 1.1.1.1 255.255.255.0
ip nat outside
duplex auto
speed auto
```

Ainsi, le mieux est de configurer une N.A.T. dynamique en attribuant à tous les hôtes du réseau interne la même adresse en **overload** donc, celle de l'interface vers Internet du routeur R_ENT avec le pool d'adresse fourni par le Fournisseur d'Accès Internet : 1.1.1.0/24, tel que :

On commence par créer une access-list spécifiant tous les réseaux privés de l'entreprise devant être traduits en adresse ipv4 publique :

```
R_ENT(conf)#access-list 3 permit 172.15.1.0 0.0.0.255
R_ENT(conf)#access-list 3 permit 172.15.2.0 0.0.0.255
R_ENT(conf)#access-list 3 permit 172.15.3.0 0.0.0.255
R_ENT(conf)#access-list 3 permit 192.168.1.0 0.0.0.255
```

On entre ensuite le pool attribué par le F.A.I. :

```
R_ENT(conf)#ip nat pool FAI 1.1.1.1 1.1.1.1 netmask 255.255.255.0
```

Enfin on applique le nat dynamique en liant l'ACL n°3 qui concerne les adresses ipv4 privées devant être traduites selon le pool FAI attribué :

```
R_ENT(conf)#ip nat inside source list 3 pool FAI overload
```

Ensuite on applique du nat statique pour traduire l'adresse du serveur web de la dmz afin qu'il soit accessible sur une adresse publique et routable sur internet, à savoir : 1.1.1.253, avec la commande :

```
R_ENT(conf)#ip nat inside source static 192.168.1.7 1.1.1.253
```

Après avoir configuré l'ASA et le routeur R_ENT, nous avons rencontré un problème de connectivité. Nos hôtes des différentes VLans du LAN réussissaient à se transmettre des paquets icmp avec l'asa. Cependant il n'était pas possible d'établir une connexion avec le routeur R_ENT. Dans un premier temps nous avons défini une route par défaut sur le MLS, tel que

```
MLS(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.2
```

et une route vers les réseaux de l'entreprise sur le routeur R_ENT :

```
R_ENT(config)#ip route 172.15.1.0 255.255.255.0 192.168.11.253
R_ENT(config)#ip route 172.15.2.0 255.255.255.0 192.168.11.253
R_ENT(config)#ip route 172.15.3.0 255.255.255.0 192.168.11.253
```

R_ENT(config)#ip route 192.168.1.0 255.255.255.0 192.168.11.253

Suite à cela,

	Successful	PC1	R_ENT	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC2	R_ENT	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC3	R_ENT	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC4	R_ENT	ICMP		0.000	N	3	(edit)	(delete)

→ Les paquets envoyés des hôtes du réseau local peuvent envoyer des paquets ICMP à travers l'asa,

	Failed	R_ENT	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Failed	R_ENT	PC3	ICMP		0.000	N	1	(edit)	(delete)
	Failed	R_ENT	PC4	ICMP		0.000	N	2	(edit)	(delete)

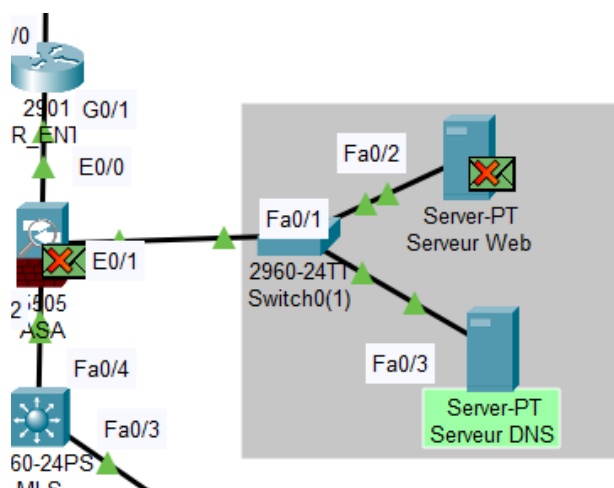
→ Et grâce aux règles appliquées au pare-feu, le réseau extérieur ne peut pas se connecter aux hôtes du réseau local..

On constate notamment que :

	Successful	PC1	Serveur Web	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC2	Serveur Web	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC3	Serveur Web	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC4	Serveur Web	ICMP		0.000	N	3	(edit)	(delete)

Les hôtes des différents Vlans sont capables d'envoyer un paquet au serveur WEB de la DMZ.

Mais voici un autre problème que nous rencontrons, les hôtes du réseau local ne peuvent pas accéder au serveur DNS situé dans la zone de la DMZ



Cela provient d'un problème interne à la zone démilitarisée au niveau de la couche 2, et lorsque l'on regarde de plus près avec le mode simulation, on remarque que le serveur DNS envoie un paquet ARP à ses voisins et ne trouve pas son réseau.

PDU Information at Device: Serveur Web

OSI Model Inbound PDU Details

At Device: Serveur Web
Source: Serveur DNS
Destination: Broadcast

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer2: Ethernet II Header 0090.2BA9.3A93 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 172.15.3.33, Dest. IP: 172.15.3.254	Layer2
Layer 1: Port FastEthernet0	Layer1

1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.
3. The frame is an ARP frame. The ARP process processes it.
4. The ARP frame is a request.
5. The ARP request's sender IP address is in a different network than the receiving port.
6. The ARP process drops the frame.

Challenge Me << Previous Layer Next Layer >>

La trame est donc supprimée.

Nous avons configuré le serveur DNS de cette manière :

☒ Static

172.15.3.33

255.255.255.0

172.15.3.254

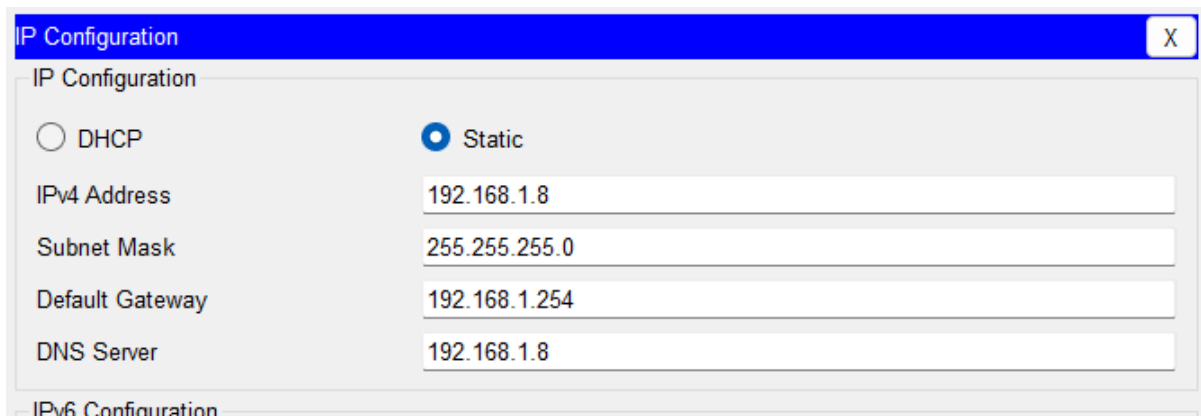
0.0.0.0

Nous pensions que comme le serveur DNS se situait dans la vlan 30 alors il devait avoir cette adresse comme ci-dessus, nous avons essayé de configurer sur l'asa l'interface de la vlan 30 avec comme adresse IP celle de la passerelle du serveur DNS, à savoir : 172.15.3.254.

Voici ce que nous avons configuré sur l'ASA :

```
interface Vlan30
  no nameif
  no security-level
  ip address 172.15.3.254 255.255.255.0
!
```

Seulement impossible d'envoyer un ping vers cette interface, il aurait peut-être fallu ajouter un 'nameif' pour que l'interface soit définie mais Packet Tracer étant limité, ce n'était pas possible, nos trois interface "vlan 1", "vlan 2" et "vlan 3" en no forward étant déjà prises. Nous avons donc changé la configuration du serveur DNS comme suit en l'ayant intégré au réseau de la DMZ : 192.168.1.0/24.



À présent, les hôtes du réseau interne peuvent avoir accès aux serveurs de la DMZ et se connecter au site www.entreprise.com.

En ce qui concerne le routeur R_FAI, voici la configuration que nous lui avons appliquée :

```
interface GigabitEthernet0/0
ip address 1.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 1.1.2.129 255.255.255.252
duplex auto
speed auto
```

Lors du mode simulation, le paquet ne trouvait pas le bon réseau dans sa table de routage, ainsi nous avons rajouté une route par défaut :

```
R_FAI(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.1
```

Étape 4 : Ajout du réseau publique 8.8.0.0/16 et interconnexion avec le FAI

À travers cette partie, nous allons configurer le réseau 8.8.0.0/16 avec des adresses IP statiques comme suit :

Pour le client extérieur :

The screenshot shows the 'PC_EXT' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is active, showing settings for the 'FastEthernet0' interface. The 'Static' radio button is selected for both IPv4 and IPv6 configurations. The IPv4 configuration includes a static IP address of 8.8.0.2, a subnet mask of 255.255.0.0, a default gateway of 8.8.0.254, and a DNS server of 1.1.1.252. The IPv6 configuration is also set to 'Static' with a link local address of FE80::260:70FF:FEB8:9B79. The 802.1X section is expanded, showing 'Use 802.1X Security' as unchecked, 'Authentication' set to 'MD5', and empty fields for 'Username' and 'Password'. A 'Top' button is located at the bottom left of the window.

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	8.8.0.2
Subnet Mask	255.255.0.0
Default Gateway	8.8.0.254
DNS Server	1.1.1.252
IPv6 Configuration	
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	/
Link Local Address	FE80::260:70FF:FEB8:9B79
Default Gateway	
DNS Server	
802.1X	
<input type="checkbox"/> Use 802.1X Security	
Authentication	MD5
Username	
Password	

☐ Top

Pour le serveur WEB www.test.com :

www.test.com

Physical Config Services **Desktop** Programming Attributes

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 8.8.0.1

Subnet Mask 255.255.0.0

Default Gateway 8.8.0.254

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::2D0:97FF:FE9B:A3E7

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

On configure ensuite les trois routeurs situés dans le réseau externe : R_ENT, R_FAI, R_EXT avec un routage dynamique E.I.G.R.P. (Enhanced Interior Gateway Routing Protocol) qui est un protocole de routage à vecteur de distance, utilisé principalement dans les réseaux d'entreprise pour l'échange d'informations de routage entre les routeurs.

Voici la configuration suivante qui a ainsi été apportée aux trois routeurs :

R_EXT :

```
router eigrp 100
network 8.8.0.0 0.0.255.255
network 1.1.2.128 0.0.0.3
no auto-summary
```

R_FAI :

```
router eigrp 100
network 1.1.2.128 0.0.0.3
network 1.1.1.0 0.0.0.255
no auto-summary
```

R_ENT :

```
router eigrp 100
network 192.168.11.252 0.0.0.3
network 1.1.1.0 0.0.0.255
no auto-summary
```

Sur chaque routeur on active le protocole eigrp avec un numéro de processus ici 100. On spécifie les réseaux directement connectés aux interfaces du routeur. L'option "no auto-summary" est utilisée pour désactiver cette fonctionnalité d'auto-résumé. Lorsque l'on configure "no auto-summary" dans EIGRP, cela indique au routeur de ne pas résumer automatiquement les réseaux lors de l'annonce des routes. Chaque sous-réseau est annoncé individuellement aux autres routeurs du réseau. Cette commande est souvent activée par défaut.

et on configure les adresses statiques sur les interfaces du routeur R_EXT de la manière qui suit :


```

spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 8.8.0.254 255.255.0.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 1.1.2.130 255.255.255.252
duplex auto
speed auto

```

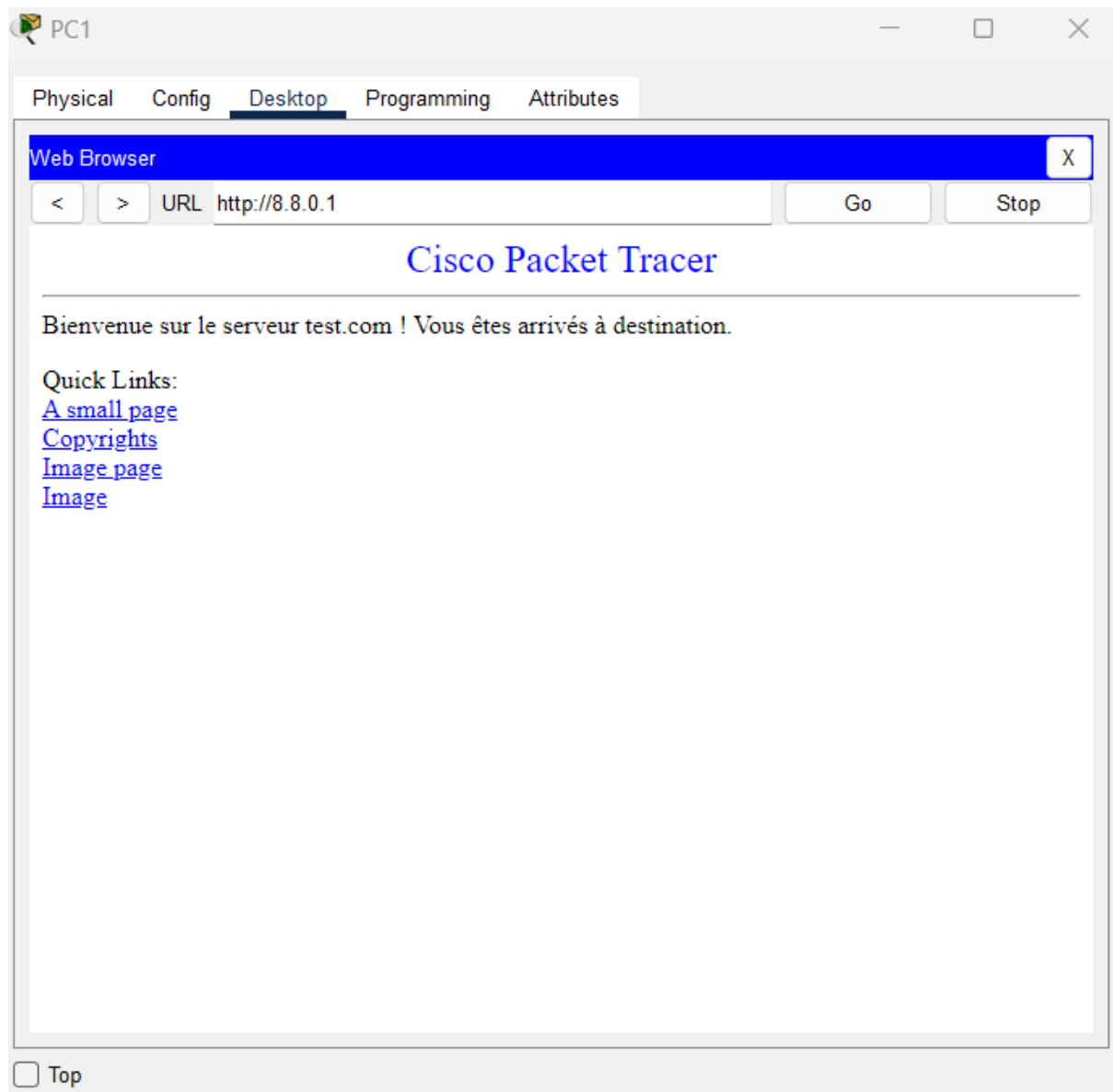
Enfin nous avons pour objectif d'effectuer les tests ultimes. Pour cela il faut dans un premier temps que les hôtes du réseau interne aient accès au serveur WEB situé dans le domaine 'www.test.com'. On vérifie d'abord que les hôtes puissent envoyer un paquet icmp vers le serveur web test :

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC2	www.test....	ICMP		0.000	N	0	(edit)	

Cela est possible car l'hôte PC2 provient d'une zone ayant un niveau de sécurité plus élevé (au maximum) que le serveur web qui provient de la zone de méfiance (au niveau de sécurité le plus bas). En effet :

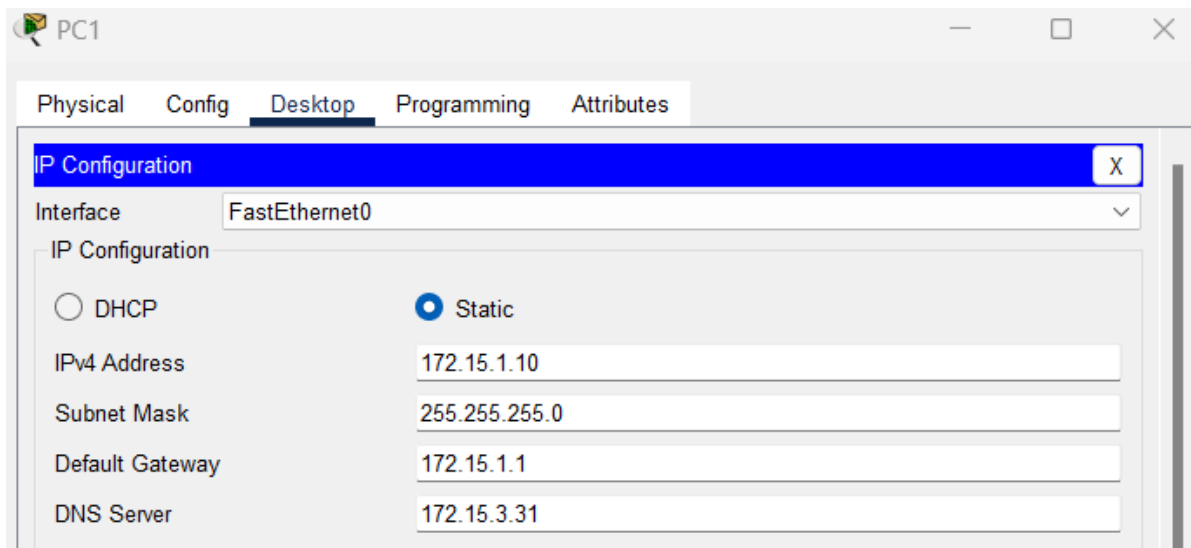
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC2	www.test....	ICMP		0.000	N	0	(edit)	(delete)
	Failed	www.t...	PC2	ICMP		0.000	N	1	(edit)	(delete)

On remarque que l'inverse n'est pas possible : le serveur web ne peut pas ping le PC2 du réseau interne de l'entreprise. On passe ensuite à l'étape suivante, on s'assure que les PCs du réseau interne puisse accéder au serveur web 'www.test.com' en renseignant dans l'URL l'adresse IP de celui ci :

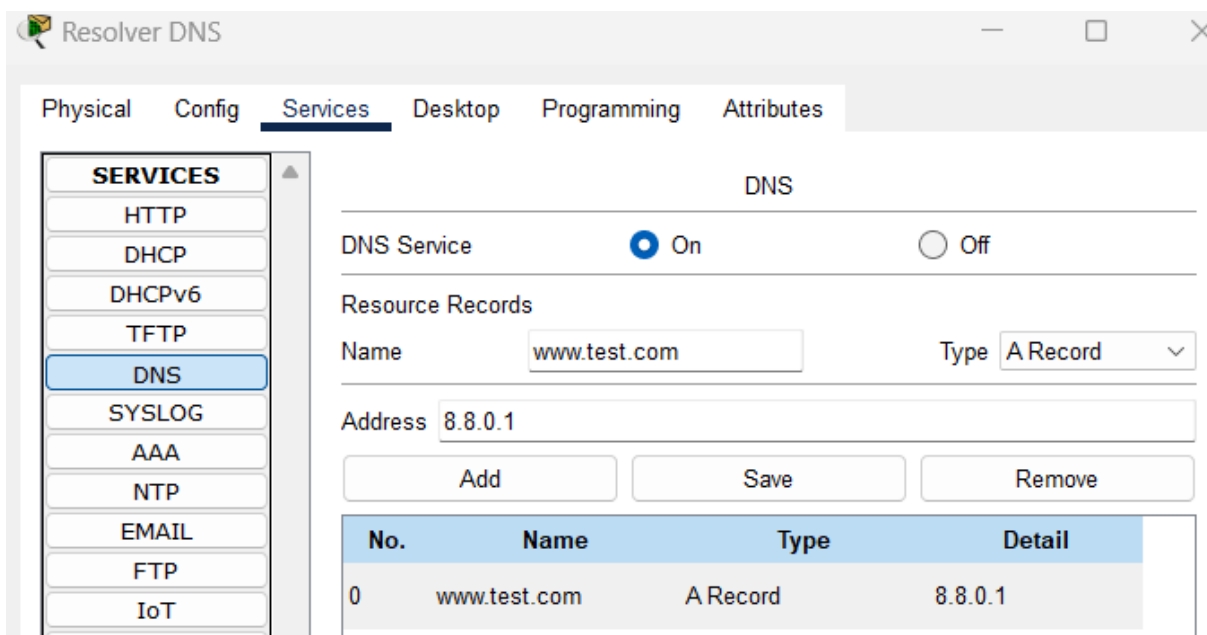


Cela est bien possible. On passe donc à l'ultime vérification : rentrer simplement le nom de domaine 'www.test.com' dans la barre de recherche du navigateur.

On s'assure que dans les paramètres de configuration des Pcs, il y ait comme étant renseigné l'adresse IP du resolver DNS situé avec les serveurs internes à l'entreprise, ci-exemple avec le PC1 du L.A.N. :



De plus il est nécessaire comme nous l'avons fait dans les étapes précédente, de renseigner au serveur DNS la traduction du nom et de l'adresse IP du serveur web, petit rappel ci-dessous :

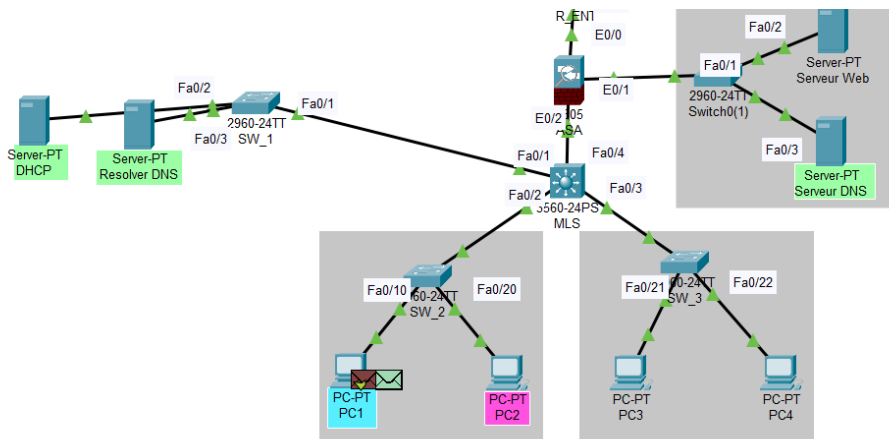
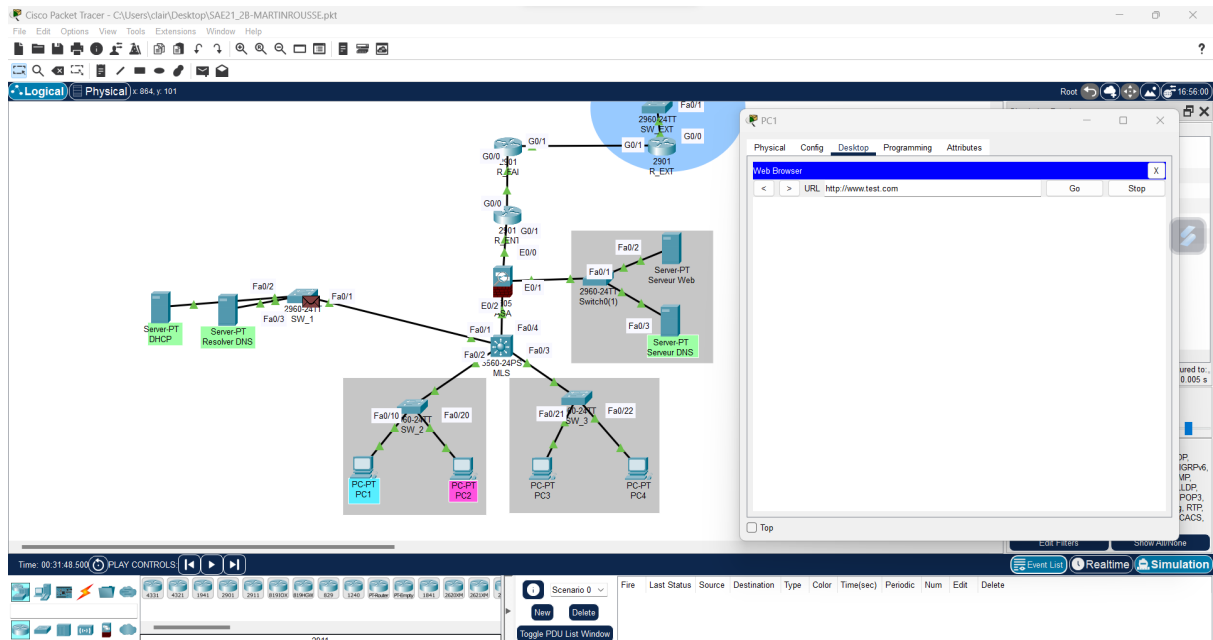


Maintenant nous allons tenter de nous connecter au serveur 'www.test.com' en rentrant le nom de domaine :

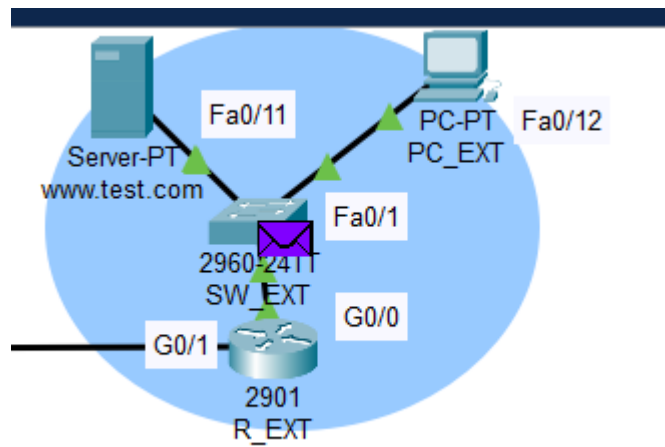
Une fois en mode simulation :

- Lorsque l'on appuie sur le bouton 'Go' après avoir renseigné le nom de domaine, nous pouvons visualiser une petite enveloppe se dirigeant non pas vers le serveur web, mais vers le resolver DNS. Il s'agit d'une requête vers le resolver dns afin d'acquérir la correspondance entre le nom de domaine venant d'être renseigné, et

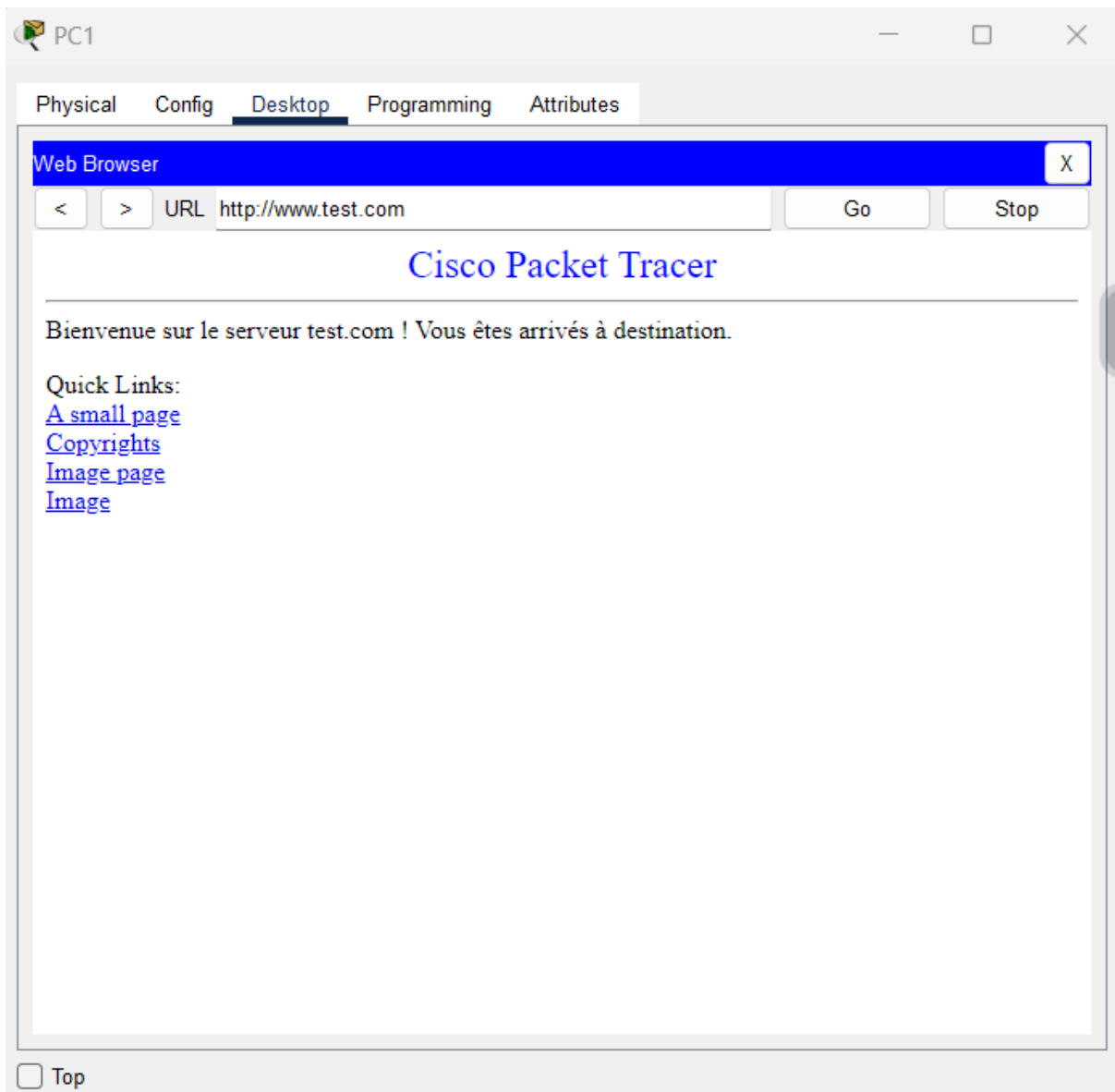
l'adresse ip destination correspondante, afin de la signaler au PC hôte pour qu'il puisse établir une connexion vers le serveur WEB.



Une fois l'enveloppe revenue au PC hôte, celui-ci aura acquis la connaissance de l'adresse destination du serveur WEB vers lequel il souhaite établir une connexion, et pourra envoyer une requête avec le protocole tcp sur le port 80 du serveur web 'www.test.com' en lançant une requête http et en initiant une connexion tcp pavec la petite enveloppe verte qui prends donc le relais.



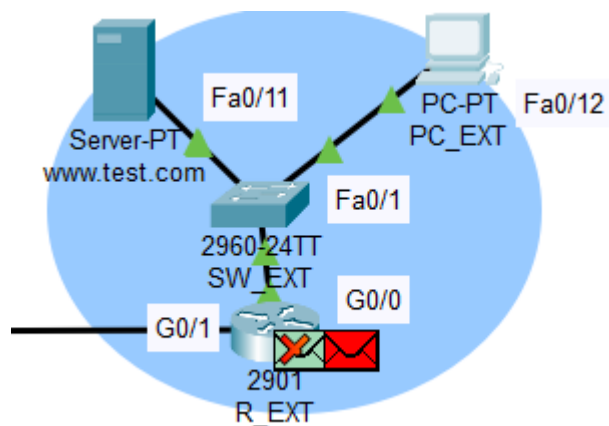
La réponse http au client du serveur web test sera cette petite enveloppe violette qui permettra l'acquisition des données du site et donc de la page web pour aboutir au résultat attendu, que vous visualiserez dans la vidéo du rapport :



Passons ensuite au second test ultime.

Le but de ce test est que le client du domaine 'test' puisse accéder au serveur web 'www.entreprise.com' via le DNS de la DMZ.

pour ce faire et pour commencer, nous allons faire en sorte que le client externe puisse accéder au serveur web en entrant uniquement l'adresse IP dans la barre de recherche :



On obtient un problème lorsque l'on lance le mode simulation.

PDU Information at Device: R_EXT

OSI Model

Inbound PDU Details

At Device: R_EXT
 Source: PC_EXT
 Destination: 192.168.1.7

In Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 8.8.0.2, Dest. IP: 192.168.1.7
Layer 2: Ethernet II Header 0060.70B8.9B79 >> 000A.41A8.1701
Layer 1: Port GigabitEthernet0/0

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer 3:
Layer2
Layer1

1. The routing table does not have a route to the destination IP address. The device drops the packet.
 2. The device sends back an ICMP Host Unreachable message.

Challenge Me

<< Previous Layer

Next Layer >>

Le routeur R_EXT ne connaît pas le réseau de destination du paquet, il ne la possède pas dans sa table de routage.

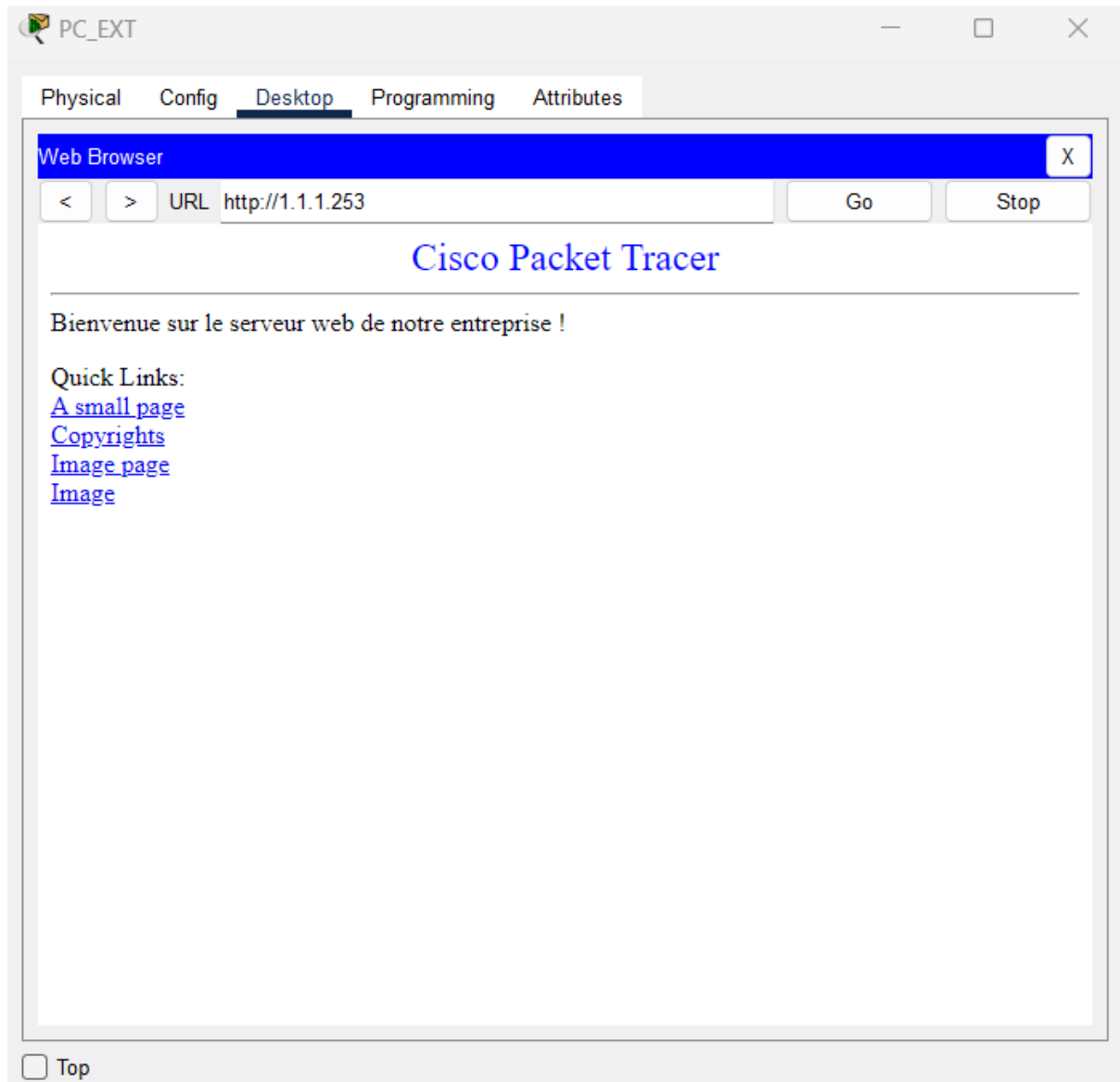
page 31

On renseigne donc une route par défaut sur celui-ci :

```
R_EXT(config)#ip route 0.0.0.0 0.0.0.0 1.1.2.129
```

On réessaie :

On saisit bien dans l'URL l'adresse tradaté du serveur web, configurée en N.A.T. statique au sein du routeur R_ENT :



On souhaite rajouter un service DNS lié à notre hôte test, pour cela nous avons choisi d'utiliser le serveur DNS au sein de la dmz.

Serveur DNS

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type **A Record** ▼

Address

No.	Name	Type	Detail
0	www.entreprise.com	A Record	1.1.1.253

☐ Top

On ajoute la correspondance avec le site web de l'entreprise (ayant une adresse IP traduite publiquement en 1.1.1.253)

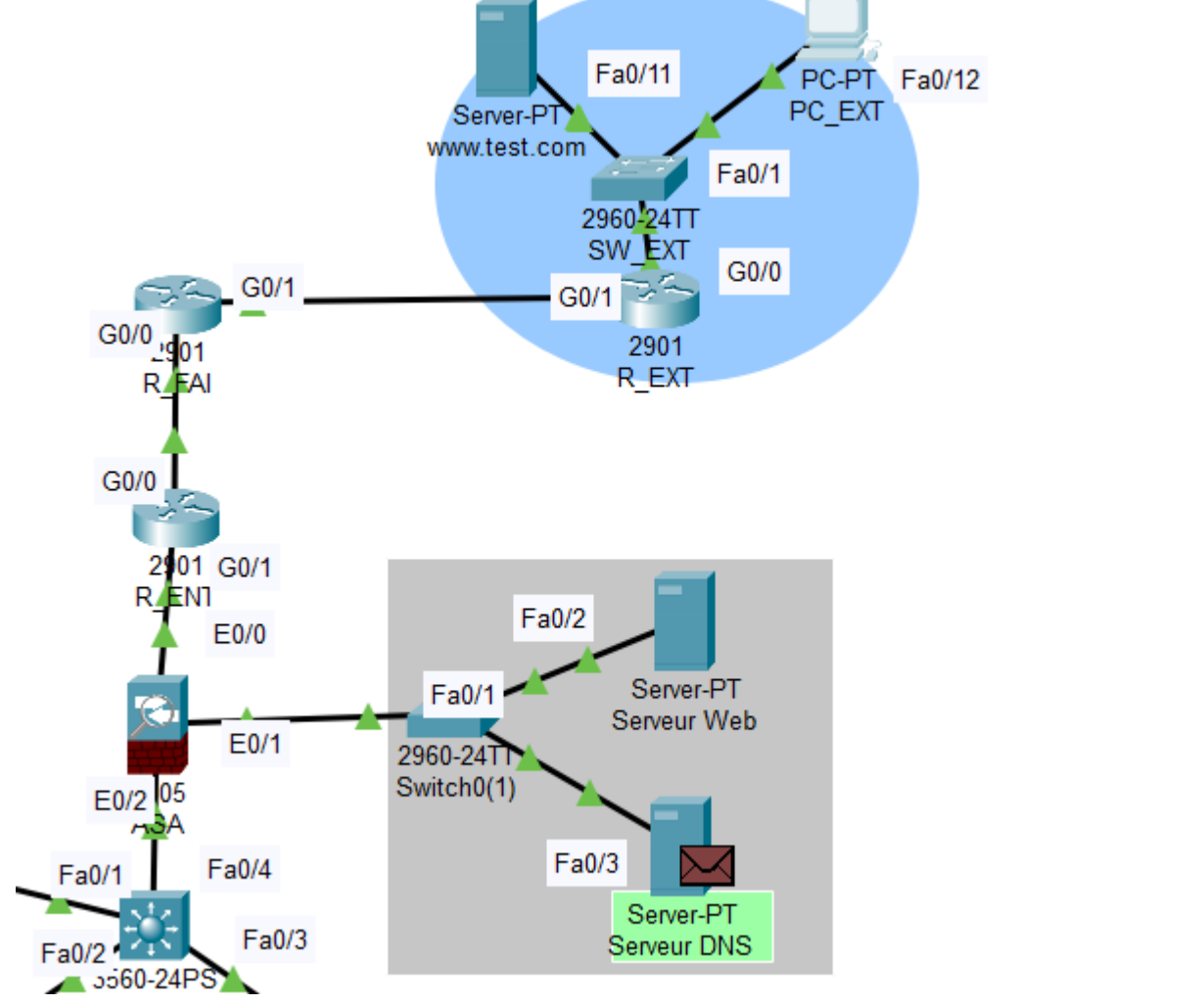
Il y a cependant quelques configurations à ajouter. En effet, le serveur dns possède une adresse IPv4 publique, nous allons faire en sorte qu'il soit accessible de manière analogue via une adresse privée dans le réseau fournit par le FAI, à savoir le réseau 1.1.1.0/24.

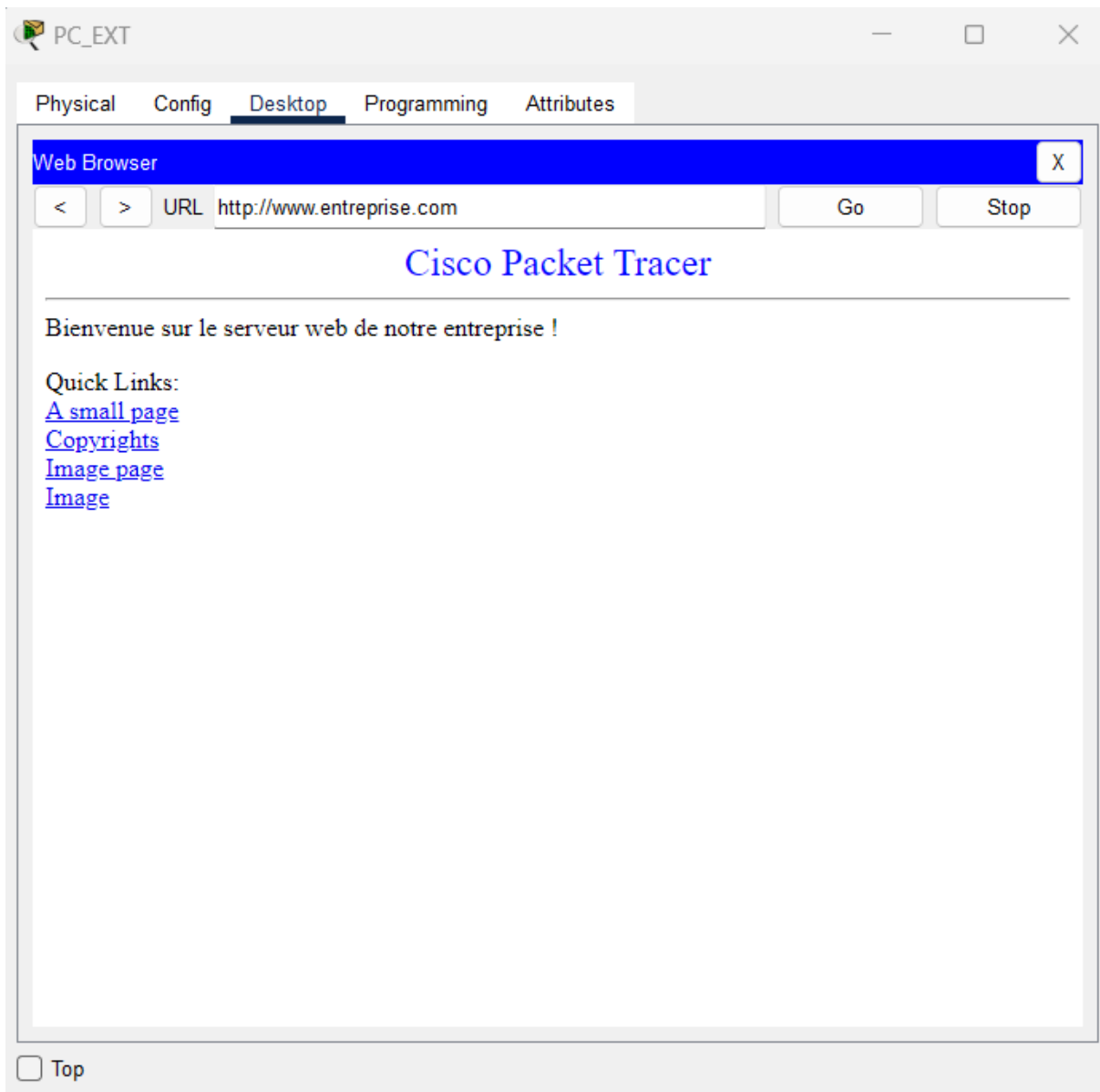
Nous lui attribuerons l'adresse 1.1.1.252 en appliquant la translation d'adresse N.A.T. sur le routeur R_ENT :

```
R_ENT(config)#ip nat inside source 192.168.1.8 1.1.1.252
```

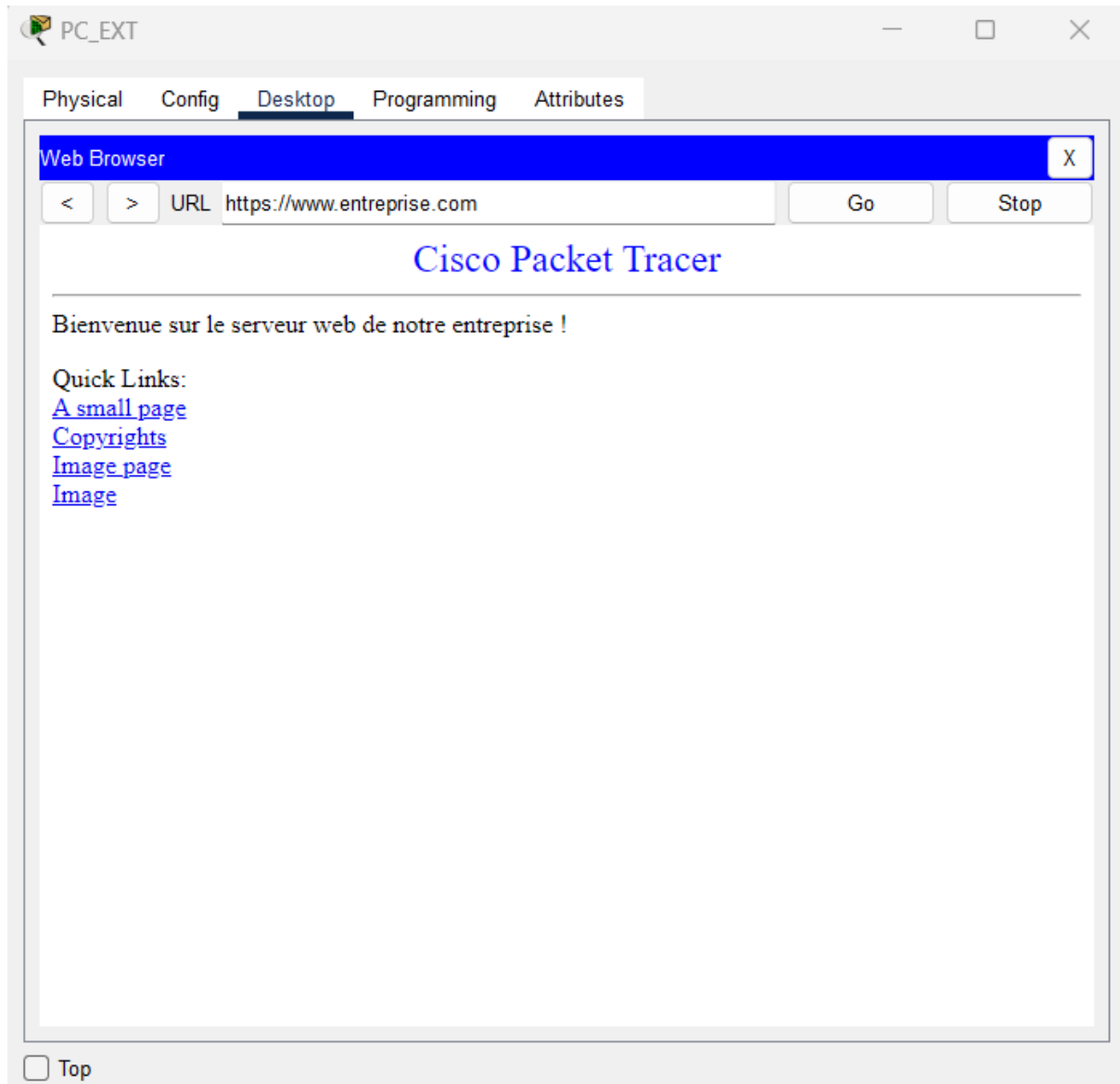
Ensuite il faut ajouter une configuration à l'asa, afin de permettre les connexions sur le port 53, pour que le client test puisse accéder au serveur DNS de l'entreprise. On ajoute donc une règle à l'access-list web comme suit :

```
ASA(config)#access-list web extended permit udp any any eq 53
```





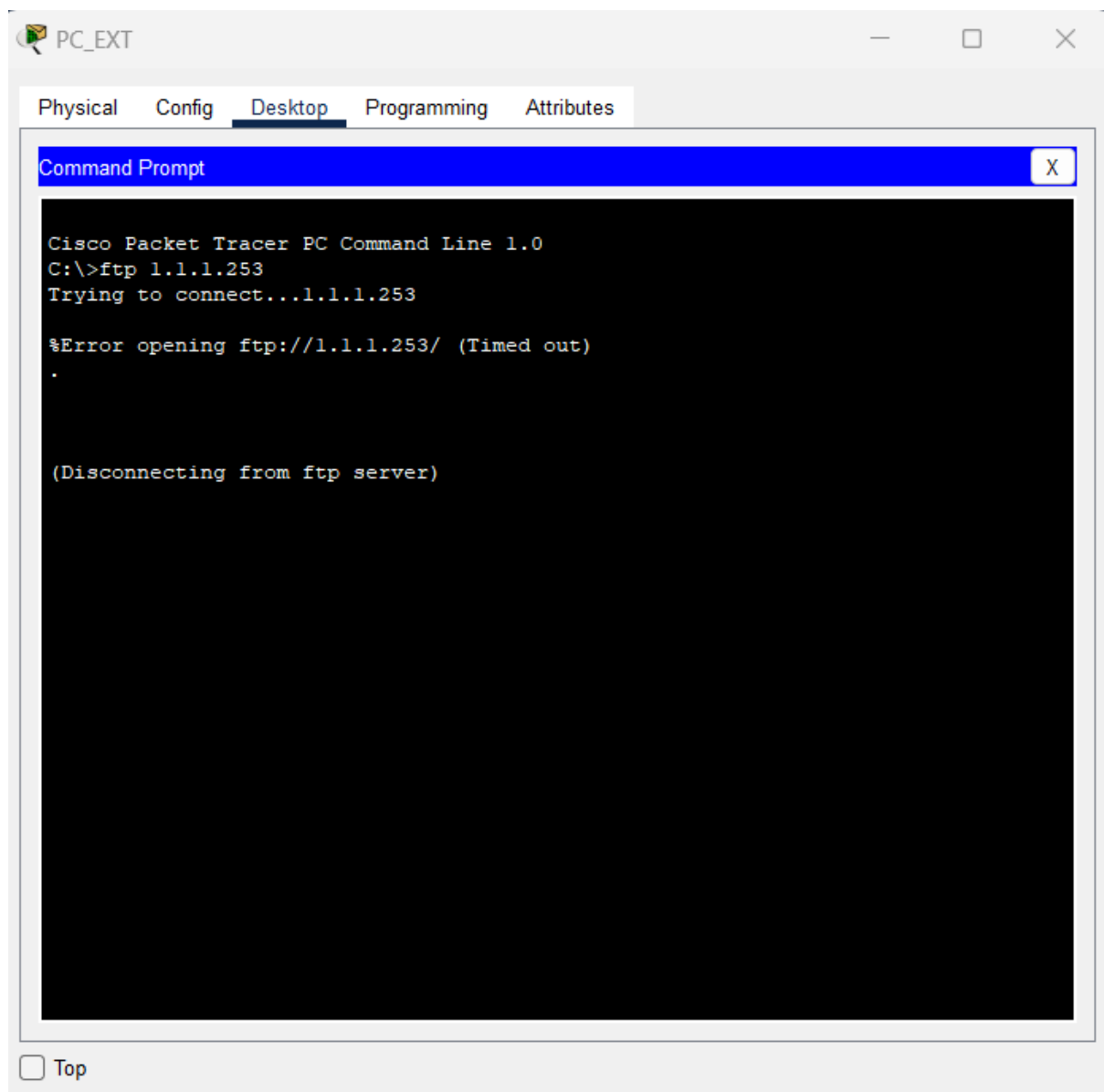
De même sur le port 443 en https :



On vérifie que la connexion à la dmz sur un autre port est impossible :

On essaie quelques exemples :

sur le port 21 avec le protocole FTP :



Sur le port 23 avec le protocole telnet :

```
C:\>telnet 1.1.1.253
Trying 1.1.1.253 ...
% Connection timed out; remote host not responding
C:\>
```

Conclusion

Dans le cadre de la SAÉ 21, nous avons réussi à mettre en place un réseau informatique complet pour une petite structure.

Nous avons identifié trois zones principales au sein de l'entreprise : le réseau interne, qui abrite les éléments et les ressources confidentielles nécessitant une sécurisation rigoureuse, la DMZ qui fait office de zone intermédiaire entre le réseau interne et le réseau externe, permettant d'échanger des ressources entre les deux zones, et enfin le réseau externe non fiable.

Pour garantir la sécurité du trafic entrant et sortant entre ces zones, nous avons configuré un pare-feu, l'ASA 5505. Grâce à des listes d'accès, nous avons autorisé uniquement le trafic provenant de connexions initiées en interne. De plus, nous avons permis le trafic provenant du réseau externe vers les serveurs de la DMZ sur les ports 80 et 443, et exceptionnellement sur le port 53 pour accéder au serveur DNS depuis le domaine 'test'.

Au sein du réseau interne, nous avons configuré plusieurs VLANs, ainsi qu'un serveur DHCP et un résolveur DNS fonctionnels. En externe, nous avons mis en place le NAT statique et dynamique, ce qui a permis aux hôtes du réseau interne d'accéder et d'échanger des données de manière sécurisée avec le réseau externe, en rendant les adresses IP privées routables sur Internet. De plus, nous avons configuré le protocole EIGRP à vecteur de distance en externe afin d'améliorer l'échange des informations entre les tables de routage des routeurs.

Après avoir franchi toutes ces étapes, nous avons pu effectuer avec succès les tests finaux.

Cette SAÉ a été extrêmement enrichissante pour nous, car elle nous a permis de développer des compétences approfondies dans l'utilisation et la configuration de l'ASA et du fonctionnement général d'un réseau d'entreprise.

Sources :

E.I.G.R.P. commande no auto-summary : <https://geek-university.com/eigrp-auto-summary/>

configuration asa :

https://www.cisco.com/c/fr_ca/support/docs/ip/network-address-translation-nat/118958-configure-asa-00.html

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/firewall/asa-96-firewall-all-config/inspect-service-policy.html>

Nous nous sommes aussi aidé des sources contenues dans le pdf d'énoncé du projet, à savoir :

https://www.youtube.com/watch?v=SLZS1mSc_VY&list=PLK-Bs6BGQBEP4HUmB1g27aIL4EPyXeLNx

<https://polar91.wordpress.com/category/networking/routing/>

<http://www.gomjabbar.com/2011/09/11/no-forward-interface-command-on-the-cisco-asa-5505-with-a-base-license/#sthash.UsvXlmdt.dpbs>

<https://polar91.wordpress.com/2017/09/27/configure-multilayer-switch-on-packet-tracer/>

<https://itexamanswers.net/21-7-5-packet-tracer-configure-asa-basic-settings-and-firewall-using-the-cli-answers.html>