Configuration d’un réseau sécurisé multi-sites avec « pfSense »

Livrable 1 : Maquettage du réseau

Antivackis Vanessa

Cailleau Dylan

Forest Jules

Haton Tom

Table des matières

Description du maquettage du réseau

Représentation de l’architecture du réseau

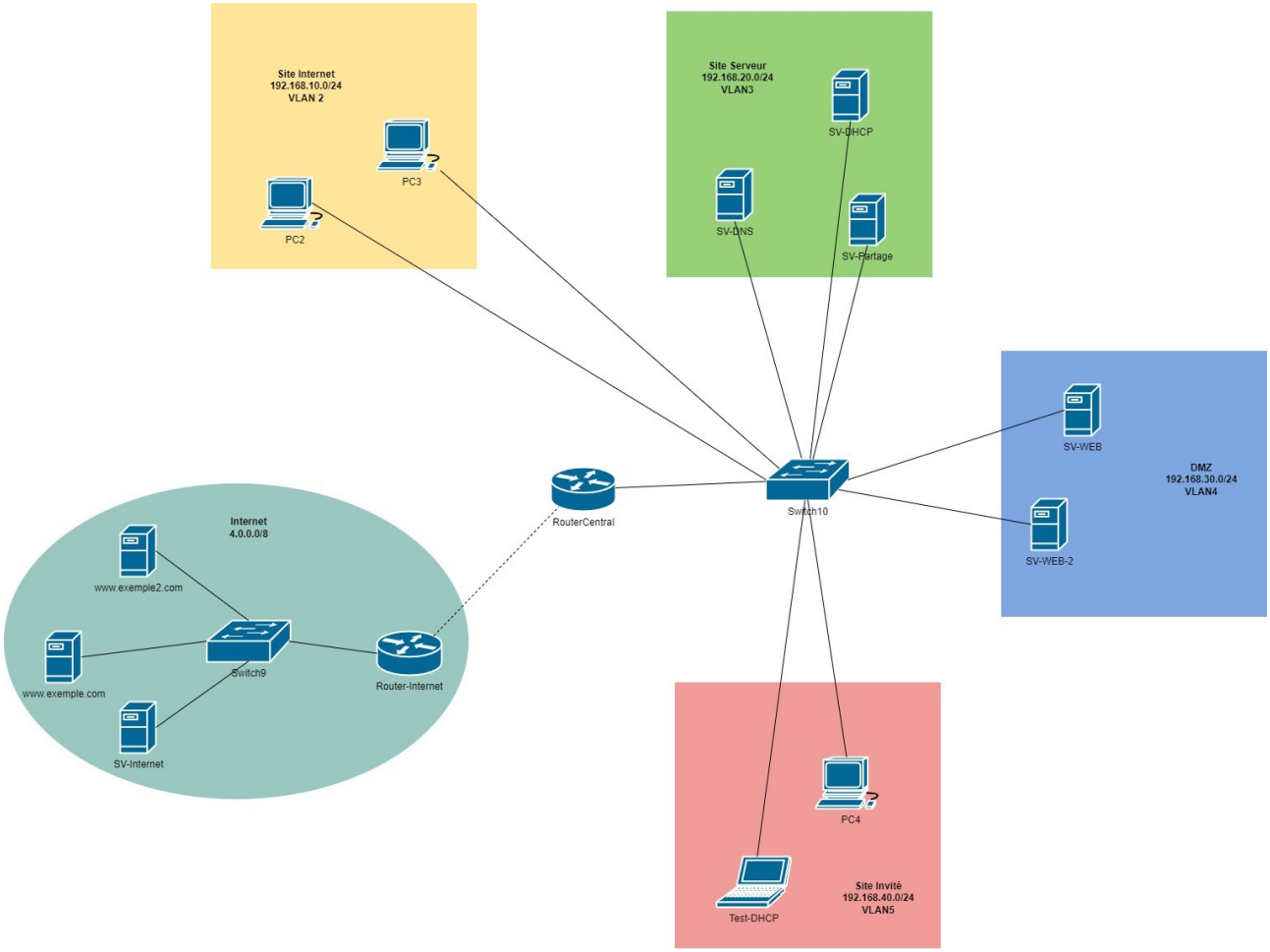
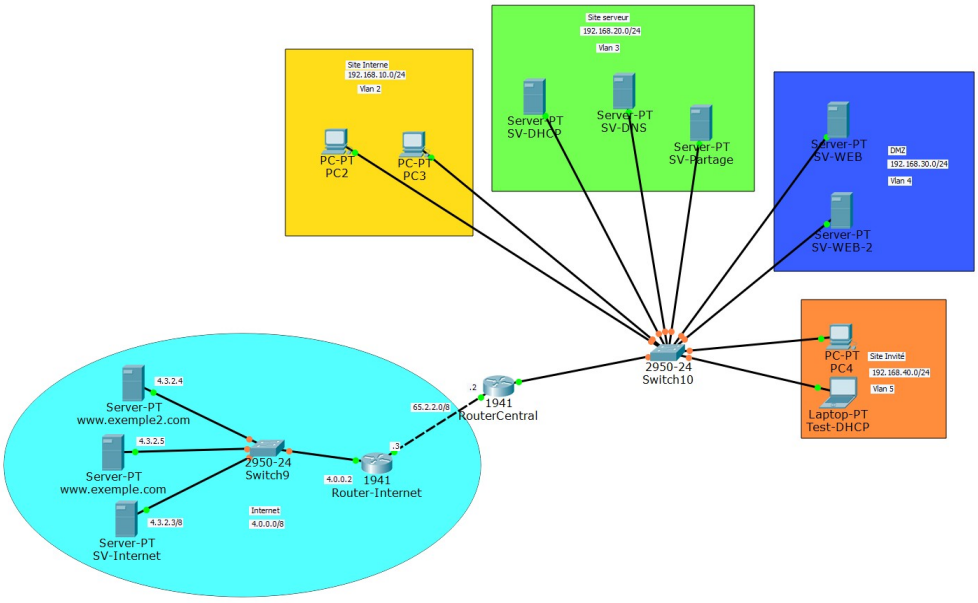


Diagramme de l'architecture réseau



Topologie de l'architecture réseau

Configuration des interfaces réseaux

Afin de reproduire cette configuration, vous aurez besoin du logiciel « Cisco Packet Tracer ».

Pour configurer en ligne de commande, chacun des différents composants, cliquez sur le composant concerné puis allez dans l'onglet « CLI ».

Pour commencer, choisissez le routeur 1941 et reliez-le au commutateur 2950-24 avec un lien plein de type « Copper Straigth-Through ».

Nous allons configurer, en ligne de commande, le routeur :

```
enable
configure terminal
hostname RouterCentral ← Nom donné à ce routeur
```

On commence ici par configurer les différents VLANs constitués d'une adresse IP et d'un relais DHCP.

```
interface GigabitEthernet0/0.2 ← VLAN 2 | Site Interne
 encapsulation dot1q2 ← Encapsulation de commutation du réseau
 ip address 192.168.10.1 255.255.255.0 ← Adresse IP
 ip helper-address 192.168.20.2 ← Relais DHCP
exit

interface GigabitEthernet0/0.3 ← VLAN 3 | Site Serveur
 encapsulation dot1Q 3
 ip address 192.168.20.1 255.255.255.0
 ip helper-address 192.168.20.2
 ip access-group Serveur in
 ip nat inside
exit

interface GigabitEthernet0/0.4 ← VLAN 4 | DMZ
 encapsulation dot1Q 4
 ip address 192.168.30.1 255.255.255.0
 ip helper-address 192.168.20.2
exit

interface GigabitEthernet0/0.5 ← VLAN 5 | Site Invité
 encapsulation dot1Q 5
 ip address 192.168.40.1 255.255.255.0
 ip helper-address 192.168.20.2
exit

interface GigabitEthernet0/1
 ip address 65.2.2.2 255.0.0.0
exit

ip route 0.0.0.0 0.0.0.0 65.2.2.3 ← Configuration d'une route statique pour tous les réseaux représentés par «0.0.0.0/0»
```

Nous allons commencer, en ligne de commande, par configurer le commutateur :

```
enable
configure terminal
hostname Switch10 ← Nom donné à ce commutateur
```

```
interface FastEthernet0/24
 switchport trunk allowed vlan 2-5 ← Spécification des VLANs 2 à 5 autorisés sur l'interface
 switchport mode trunk ← Configuration du port pour qu'il transmette à plusieurs réseaux VLAN
exit
```

Zone LAN des serveurs internes (DNS, DHCP, Partage de fichiers)

Dans cette zone, nous utiliserons un réseau privé à l'adresse 192.168.20.0/24.

Choisissez trois (3) postes de serveur générique de type « Server-PT » et reliez-les avec un lien plein de type « Copper Straigth-Through ». avec le commutateur « Switch10 » sur les ports « FastEthernet0/3 », « FastEthernet0/4 » et « FastEthernet0/5 » respectivement.

On configure chacun de ces postes :

Cliquez sur le poste, allez dans l'onglet « Desktop » puis sur « IP Configuration ». On configurera chacun de ces postes avec l'adresse IP « 192.168.20.2 » puis « 192.168.20.3 » et enfin « 192.168.20.4 » ainsi qu'avec leur masque « 255.255.255.0 » et l'adresse passerelle « 192.168.20.1 ».

On configure maintenant le commutateur « Switch10 » :

```
enable
configure terminal

interface FastEthernet0/3
 switchport access vlan 3  ← Configuration du port qu'il appartienne uniquement au VLAN 3
 switchport mode access ← Configuration du port pour qu'il ne transmette des données que pour une seule VLAN
exit

interface FastEthernet0/4
 switchport access vlan 3
 switchport mode access
exit

interface FastEthernet0/5
 switchport access vlan 3
 switchport mode access
exit
```

Zone DMZ (pour les serveurs accessibles depuis l'extérieur)

La DMZ (Demilitarized Zone) est un sous-réseau isolé qui sépare un réseau local interne d'autres réseaux non sécurisées. Les réseaux non sécurisés sont représentés ici par les serveurs web ou tout autre service nécessitant un accès externe.

Les serveurs présents seront configurés pour être accessibles depuis Internet à trouver le routeur principal.

Dans cette zone, nous utiliserons un réseau privé à l'adresse 192.168.30.0/24.

Choisissez deux (2) postes de serveur générique de type « Server-PT » et reliez-les avec un lien plein de type « Copper Straigth-Through » avec le commutateur « Switch10 » sur les ports « FastEthernet0/6 » et « FastEthernet0/7 ».

On configure chacun de ces postes :

Cliquez sur le poste, allez dans l'onglet « Desktop » puis sur « IP Configuration ». On configurera chacun de ces postes avec l'adresse IP « 192.168.30.2 » puis « 192.168.30.3 » ainsi qu'avec leur masque « 255.255.255.0 » et l'adresse passerelle « 192.168.30.1 ».

On configure maintenant le commutateur « Switch10 » :

```
enable
configure terminal

interface FastEthernet0/6
 switchport access vlan 4
 switchport mode access
exit

interface FastEthernet0/7
 switchport access vlan 4
 switchport mode access
exit
```

Zone LAN des équipements utilisateurs

Dans cette zone, nous utiliserons un réseau privé à l'adresse 192.168.10.0/24.

Choisissez deux (2) postes d'ordinateur générique de type « PC-PT » et reliez-les avec un lien plein de type « Copper Straigth-Through » avec le commutateur sur les ports « FastEthernet0/1 » et « FastEthernet0/2 ».

On configure le commutateur :

```
enable
configure terminal

interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
exit

interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
exit
```

Cliquez sur un des postes d'ordinateur, allez dans l'onglet « Desktop » puis sur « IP Configuration ». Cochez le bouton « DHCP » et vous verrez le message « DHCP request successful ».

Zone Invité

Dans cette zone, nous utiliserons un réseau privé spécifique aux visiteurs temporaires, à l'adresse 19.168.40.0/24.

Choisissez deux (2) postes d'ordinateur générique dont un de type « PC-PT » et l'autre « Laptop-PT » et reliez-les avec un lien plein de type « Copper Straigth-Through » avec le commutateur sur les ports « FastEthernet0/8 » et « FastEthernet0/9 ».

On configure le commutateur :

```
enable
configure terminal
```

```
interface FastEthernet0/8
 switchport access vlan 5
 switchport mode access
exit

interface FastEthernet0/9
 switchport access vlan 5
 switchport mode access
```

Zone Internet (site représentant l’extérieur)

Choisissez un (1) routeur 1941 et un commutateur 2950-24 et reliez-les ensemble avec un lien plein. Ajoutez un lien de type « Copper Cross-Over » entre ce nouveau routeur et « RouterCentral ».

Nous allons configurer le nouveau routeur :

```
enable
configure terminal
hostname RouterInternet

interface GigabitEthernet0/0
 ip address 65.2.2.3 255.0.0.0
exit

interface GigabitEthernet0/1
 ip address 4.0.0.2 255.0.0.0
exit

ip route 0.0.0.0 0.0.0.0 65.2.2.2
```

On ajoute ensuite trois (3) autres serveurs de type « Server-PT » et on les relie respectivement sur ce nouveau commutateur un lien plein de type « Copper Straigth-Through ».

On configure chacun de ces postes :

Cliquez sur le poste, allez dans l’onglet « Desktop » puis sur « IP Configuration ». On configurera chacun de ces postes avec l’adresse IP « 4.3.2.4 » puis « 4.3.2.5 » et enfin « 4.3.2.3 » ainsi qu’avec leur masque « 255.0.0.0» et l’adresse passerelle « 4.0.0.2 ».

Configuration du pare-feu et des règles de filtrage

Nous utiliserons ici des listes de contrôle d’accès (ACL) car ces dernières sont des outils essentiels dans la configuration d’un pare-feu et de contrôle du trafic réseau sur Cisco Packet Tracer. Ils permettent de spécifier qui peut accéder à quelles ressources réseau, de filtrer le trafic en fonction de critères spécifiques et de prévenir les attaques de type "DDoS".

Protection des zones LAN

On cherche ici à protéger les zones LAN utilisateurs et serveurs internes qui sont les deux (2) sites à protéger des accès depuis l’extérieur.

Nous cherchons donc à bloquer tous les accès entrants vers les réseaux 192.168.10.0/24 et 192.168.20.0/24, mais également à autoriser les connexions sortantes depuis ces zones vers Internet ou la DMZ.

De plus, nous allons configurer la possibilité d’échanger avec le serveur DHCP pour demander une adresse IP.

On configure les ACLs correspondant sur « RouteurCentral » :

```
enable
configure terminal

ip access-list extended Interne ← Correspond au réseau 192.168.10.0/24
 permit udp any eq bootpc any eq bootps ← Autorisation des échanges DHCP
 permit udp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 eq domain ← Autorisation des échanges DNS
 permit ip 192.168.10.0 0.0.0.255 host 192.168.20.4 ← Échanges avec le serveur de partages de fichiers
 deny ip 192.168.10.0 0.0.0.255 192.168.20.4 0.0.0.255  ← Bloquer les flux vers VLAN Serveur
 permit tcp 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 eq 80 ← Accès aux services http de la DMZ
 permit tcp 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 eq 443 ← Accès aux services https de la DMZ
 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 ← Bloquer les flux vers VLAN DMZ
 deny ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255 ← Bloquer les flux vers VLAN Invite
 permit ip 192.168.10.0 0.0.0.255 any ← Accès à tout autre service et réseau
exit

interface GigabitEthernet0/0.2
 ip access-group Interne in ← ACL « Interne » entrant
exit

ip access-list extended Serveur
 permit tcp host 192.168.20.4 any
 permit tcp any eq 20 any
 permit udp any any eq domain
 permit udp any any eq bootps
 permit udp any any eq bootpc
 permit tcp any any eq www
 permit tcp any any eq 443
 deny ip any any
exit

interface GigabitEthernet0/0.3
 ip access-group Serveur in
exit
```

Configuration des ACLs pour le serveur de partage FTP

```
ip access-list extended BlocServeurPartage
 deny tcp any host 192.168.20.4 eq 21
 deny tcp any host 192.168.20.4 range 50000 51000
 deny ip any host 192.168.20.4
 permit ip any any
exit

interface GigabitEthernet0/1
 ip access-group BlocServeurPartage in ← Bloque les flux vers le serveur de partage
exit
```

Cette dernière partie fut la plus compliquée à réaliser. Il fallait que nous pensions à configurer le NAT en conséquences avec du FTP passif afin que toutes les données et interaction aevc les postes autorisés puisse communiquer avec le serveur de partage.

Accès limité à la DMZ depuis Internet

On cherche ici à bloquez tout autre type de trafic qui est jugé non nécessaire depuis l'extérieur, mais également à autoriser les connexions HTTP/HTTPS, qui correspondent aux ports 80 et 443, vers les serveurs web de la DMZ depuis l'interface Internet.

On configure les ACLs correspondant sur « RouteurCentral » :

```
enable
configure terminal

ip access-list extended DMZ ← Correspond au réseau 192.168.30.0/24
 permit tcp 192.168.30.0 0.0.0.255 any eq www ← Autorisation des échanges http avec l'extérieur
 permit tcp 192.168.30.0 0.0.0.255 any eq 443 ← Autorisation des échanges https avec l'extérieur
 permit tcp 192.168.30.0 0.0.0.255 any established
 deny ip any any
exit

interface GigabitEthernet0/0.4
 ip access-group DMZ in
exit
```

Isolation du réseau Invité

On cherche ici à bloquer tous les accès depuis le réseau invité vers les autres zones, mais également à autoriser uniquement l'accès à Internet et au serveur DHCP.

On configure les ACLs correspondant sur « RouteurCentral » :

```
enable
configure terminal

ip access-list extended Invite ← Correspond au réseau 192.168.40.0/24
 permit udp any eq bootpc any eq bootps
 permit udp 192.168.40.0 0.0.0.255 192.168.20.3 0.0.0.255 eq domain ← Autorisation des échanges DNS
 permit tcp 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255 eq 80 ← Accès aux services http de la DMZ
 permit tcp 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255 eq 443 ← Accès aux services https de la DMZ

Les commandes suivantes permettent de refuser le flux d'accès aux autres vlan
 deny ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255
 deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
 deny ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255
 permit ip 192.168.40.0 0.0.0.255 any ← Accès à tout autre service et réseau
exit

interface GigabitEthernet0/0.5
 ip access-group Invite in
exit
```

Configuration du NAT (Network Address Translation)

Sortie Internet pour les zones LAN et Invité

Nous allons maintenant configurer le NAT/PAT pour les réseaux internes vers l'adresse publique de l'interface Internet. Cela permettra aux équipements internes d'accéder à Internet avec une adresse IP unique.

Le NAT (Network Address Translation) et le PAT (Port Address Translation) sont des techniques de traduction d'adresses IP utilisées pour résoudre les problèmes de manque d'adresses IP dans les réseaux.

On configure « RouteurCentral » :

```
enable
configure terminal

interface GigabitEthernet0/0.2
 ip nat inside ← NAT | Interface connectée au réseau local
exit

interface GigabitEthernet0/0.3
 ip nat inside
exit

interface GigabitEthernet0/0.4
 ip nat inside
exit

interface GigabitEthernet0/1
 ip nat outside ← NAT | Interface externe
exit

ip nat service ftp ← Serveur de partage

ip nat pool Pool_Interne 204.12.156.10 204.12.156.20 netmask 255.255.255.0 ← Configuration pool de traduction d’adresses IP pour le réseau Interne
ip nat pool Pool_Invite 204.12.157.10 204.12.157.20 netmask 255.255.255.0← Configuration pool de traduction d’adresses IP pour le réseau Invité
ip nat inside source list 1 pool Pool_Interne ← Configuration du NAT poru les paquets de données entrants dans le réseau
ip nat inside source list 2 pool Pool_Invite
access-list 3 permit 192.168.10.0 0.0.0.255 ← Autorise les paquets de données provenant de l'adresse IP 192.168.10.0 et de toutes les adresses IP du réseau
access-list 4 permit 192.168.40.0 0.0.0.255

ip nat inside source list 3 interface GigabitEthernet0/1 overload ← Configuration du NAT pour les paquets de données provenant de la liste d'accès 3.
ip nat inside source list 4 interface GigabitEthernet0/1 overload
```

Accès aux serveurs DMZ depuis Internet

Nous allons maintenant configurer le NAT statique pour traduire chaque adresses IP privées des serveurs dans la DMZ en une adresse IP publique. Cela permettra aux utilisateurs extérieurs d’accéder aux services de la DMZ en utilisant des adresses IP publiques.

On configure « RouteurCentral » :

```
enable
configure terminal

ip nat inside source static 192.168.30.3 204.12.155.3 ← Configuration d’un NAT statique pour traduire l’adresse privée 192.168.30 en 192.168.30.3
ip nat inside source static 192.168.30.2 204.12.155.2
```

Configuration du serveur DNS

Nous allons maintenant créer des « records ».

La création de records dans Cisco Packet Tracer dans le service DNS permet de configurer et de tester un serveur DNS virtuel, mais également de simuler des scénarios de dépannage et de former les utilisateurs en matière de réseaux et de sécurité.

Sur le serveur à l'adresse 192.168.20.3, cliquez sur l'onglet « Services » puis « DNS ». Nous allons créer les deux (2) records suivants :

- Name : monServeur, address : 192.168.30.2
- Name : monServeur2, address : 192.168.30.3
- Name : www.exemple.com, address : 4.3.2.5
- Name : www.exemple2.com, address : 4.3.2.4

Recettes du maquettage du réseau

Tests VLANs

Pour chacun des tests suivants, cliquez sur un poste d'ordinateur, sauf contre-indication, puis allez dans l'onglet « Desktop » puis « Terminal ».

Vérifier que les équipements dans chaque VLAN reçoivent une adresse IP correcte depuis le serveur DHCP.

Pour ce faire, on se place sur l'un des postes ordinateurs, et l'on va réinitialiser sa configuration IP en utilisant la commande : `ipconfig /release`.

Afin que le poste redemande une configuration, on utilise la commande suivante : `ipconfig /renew`.

Si la distribution à bien été effectuée, grâce à la commande `ipconfig /all`, on devrait être capable de savoir si le serveur DHCP est bien connue du vlan.

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::205:5EFF:FE85:BDB1
   IP Address.....: 192.168.10.4
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.10.1

PC>ipconfig /release

   IP Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: 0.0.0.0
   DNS Server.....: 0.0.0.0

PC>ipconfig /renew

   IP Address.....: 192.168.10.5
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.10.1
   DNS Server.....: 192.168.20.3

PC>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....: 0005.5E85.BDB1
   Link-local IPv6 Address.....: FE80::205:5EFF:FE85:BDB1
   IP Address.....: 192.168.10.5
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.10.1
   DNS Servers.....: 192.168.20.3
   DHCP Servers.....: 192.168.20.2
   DHCPv6 Client DUID.....: 00-01-00-01-63-65-D9-BD-00-05-5E-85-BD-B1
```

Illustration 1: Test pour le VLAN2

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::206:2AFF:FEE5:8E0B
   IP Address.....: 192.168.40.3
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.40.1

PC>ipconfig /release

   IP Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: 0.0.0.0
   DNS Server.....: 0.0.0.0

PC>ipconfig /renew

   IP Address.....: 192.168.40.3
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.40.1
   DNS Server.....: 192.168.20.3

PC>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....: 0006.2AE5.8E0B
   Link-local IPv6 Address.....: FE80::206:2AFF:FEE5:8E0B
   IP Address.....: 192.168.40.3
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.40.1
   DNS Servers.....: 192.168.20.3
   DHCP Servers.....: 192.168.20.2
   DHCPv6 Client DUID.....: 00-01-00-01-80-28-6C-DA-00-06-2A-E5-8E-0B
```

Illustration 2: Test pour le VLAN 4

Tester les options DHCP supplémentaires, comme les serveurs DNS (option 6).

A partir des VLANs Interne et Invité, on va vérifier si en utilisant la commande : `nslookup`, le serveur DNS est d'une part effectivement joignable et d'autre part qu'il renvoie effectivement la bonne adresse IP du site interrogé.

Voici la configuration du serveur DNS :

No.	Name	Type	Detail
0	monserveur	A Record	192.168.30.2
1	monserveur2	A Record	192.168.30.3
2	www.exemple.com	A Record	4.3.2.5
3	www.exemple2.com	A Record	4.3.2.4

Sur le poste PC3 (VLAN Interne), on entre les commandes : `nslookup www.exemple.com` et `nslookup www.exemple2.com`. On obtient ceci :

```
PC>nslookup www.exemple.com

Server: [192.168.20.3]
Address:  192.168.20.3

Non-authoritative answer:
Name:   www.exemple.com
Address:   4.3.2.5

PC>nslookup www.exemple2.com

Server: [192.168.20.3]
Address:  192.168.20.3

Non-authoritative answer:
Name:   www.exemple2.com
Address:   4.3.2.4
```

On effectue les mêmes test sur le PC4 (VLAN Invite) :

Tests ACLs

VLAN Invité et Interne isolés

Afin de tester les tentatives d'accès entre les VLAN Invité et Interne, nous utiliser la commande `ping` pour s'assurer qu'elles échouent.

Puis nous testons l'accès du VLAN Invité vers Internet, les services web ed la DMZ et le serveur DHCP. Pour cela :

- Nous tentons d'accéder à un serveur sur internet,
- Nous récupérons une adresse IP via DHCP,
- Nous tentons l'utilisation du `ping` vers un poste du VLAN Interne et échouons,
- Nous tentons l'utilisation du `ping` vers les serveurs autres que DHCP du VLAN Serveurs.

DMZ isolée vers Internet

Afin de vérifier que la DMZ est bien isolée, nous effectuons les tests suivants :

- Nous validons que les serveurs web soient accessibles depuis Internet via HTTP/HTTPS (ports 80 et 443),
- Nous vérifions que tout autre protocole (SSH, FTP, etc.) soit bloqué,
- Nous testons que les connexions sortantes depuis la DMZ, autres que HTTP et HTTPS, ne passent pas.

VLAN Serveurs

Afin de vérifier la configuration du VLAN serveur, nous effectuons les tests suivants :

- Nous testons que l'on ne peut accéder aux VLAN Interne et Invité en dehors des services DNS, DHCP et FTP,
  - Nous devons échouer lors du `ping` vers un poste du VLAN Interne,
  - Ainsi que vers un poste du VLAN Invité.

- Nous testons que les connexions depuis/vers Internet sont bloquées
  - Nous devons accéder à un serveur web d'internet,
  - Nous devons réussir lors du `ping` d'un serveur web d'internet.

Logs du pare-feu

Afin de vérifier le fonctionnement des ACLS, nous devons activer et analyser les journaux pour vérifier qu'aucune règle ACL ne permet de trafic non souhaité. Les commandes utilisées pourront être :

- `show logging`,
- `show logging detail`,
- `show access-lists`.

Tests NAT

NAT statique avec les serveurs DMZ

Pour le test suivant, cliquez sur un poste de serveur, puis allez dans l'onglet « Desktop » puis « Web Browser ».

Nous allons maintenant entrer l'adresse publique du serveur DMZ, soit `http://204.12.155.3` et `http://204.12.155.2`. Nous vérifions que la translation s'effectue correctement en allant sur « RouteurCentral », « CLI », à l'aide de la commande en ligne `show ip nat translations`.

Nous obtenons ceci :

```
RouterCentral#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside
global
---  204.12.155.2      192.168.30.2       ---                ---
---  204.12.155.3      192.168.30.3       ---                ---
tcp 204.12.155.2:1025  192.168.30.2:1025  4.3.2.3:80         4.3.2.3:80
tcp 204.12.155.2:80    192.168.30.2:80    4.0.0.3:1026
4.0.0.3:1026
tcp 204.12.155.3:1025  192.168.30.3:1025  4.3.2.3:80         4.3.2.3:80
tcp 204.12.155.3:80    192.168.30.3:80    4.0.0.3:1025
4.0.0.3:1025
tcp 204.12.155.3:80    192.168.30.3:80    4.0.0.3:1027
4.0.0.3:1027
```

NAT/PAT avec les VLANs

Afin de vérifier la translation des adresses privées en adresse publique, nous utilisation la commande `ping` depuis les VLANs 2 et 4 puis utilisation la commande `show ip nat translation` dans « RouteurCentral ».

Nous obtenons ceci :

```
RouterCentral#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside
global
icmp 65.2.2.2:2        192.168.10.4:2     4.0.0.3:2          4.0.0.3:2
icmp 65.2.2.2:4        192.168.40.3:4     4.0.0.3:4          4.0.0.3:4
```