

# **ISMIN**

## **Architecture d'entreprise Orientée Services**

**DURÉE 6 HEURES**

Au cours de ce TP vous allez finaliser la construction d'un réseau d'entreprise doté d'un embryon d'architecture « orientée services ».

Vous allez créer une DMZ sur le routeur du siège « HQ » et y installerez un serveur Web.

Vous allez configurer le routeur HQ pour qu'il assure des services de Firewall.

Vous mettrez ensuite des tunnels GRE entre les différents sites de façon à ce que les machines internes puissent communiquer entre elles sans contraintes « NAT ».

Enfin, vous installerez des services DHCP et DNS.

### **Nota Bene :**

- N'utilisez que le mode CLI (command line interface) pour réaliser vos configurations.
- Packet Tracer plante sauvagement de temps en temps => **sauvegardez fréquemment votre fichier !**

## **Partie 1 – Configuration d'une DMZ et d'un serveur Web**

### **Etape 1 : Reprenez la situation finale du TP 3 et procédez aux modifications suivantes**

Faites une sauvegarde de la configuration courante du routeur HQ !

Sur HQ allez sur l'onglet « Physical »

Eteignez le routeur HQ

Ajoutez une interface Ethernet : WIC-1ENET

Redémarrez le routeur HQ

Intégrez un serveur sur votre espace de travail

Connectez ce serveur à la nouvelle interface Ethernet de HQ

Configurez le serveur avec l'ip : 10.77.77.80 / 24

Nommée ce serveur : « Web »

Sur HQ, configurez la nouvelle interface avec l'ip : 10.77.77.254 / 24

Ajoutez une entrée NAT statique pour associer 10.77.77.80 à l'adresse publique : 81.255.255.53

Sur HQ ajoutez la nouvelle interface dans le process « NAT inside »

Vérifiez la connectivité entre le serveur Web et le routeur HQ

Sur le serveur Web, allez dans l'onglet « Config » et stoppez tous les services sauf le service HTTP

Sauvegardez vos configurations

### **Commandes :**

```
HQ(config)#conf t
```

```
HQ(config)#interface Ethernet0/0/0
```

```
HQ(config-if)#ip address 10.77.77.254 255.255.255.0
```

```
HQ(config-if)#ip nat inside
```

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

```
HQ(config-if)#exit
```

```
HQ(config)#ip nat inside source static 10.77.77.80 81.255.255.53
```

## Etape 2 : Sécurisation du serveur Web

Sur HQ créez une liste de contrôle d'accès en entrée sur l'interface externe qui interdit tout trafic vers le serveur Web sauf les trafics http (port 80).

Vérifiez que vous pouvez atteindre le serveur Web à partir des machines externes (autres que celles qui sont dans le réseau interne).

Sur HQ créez une liste de contrôle d'accès en entrée sur l'interface interne qui interdit tout trafic vers le serveur Web sauf les trafics http (port 80). Veillez à autoriser les trafics vers les autres destinations.

Sur HQ, créez une liste de contrôle d'accès qui interdit tout trafic initié par une machine du réseau DMZ.

Sauvegardez vos configurations

### Commandes :

```
HQ(config)#ip access-list extended Outside
HQ(config-ext-nacl)#permit tcp any host 81.255.255.53 eq www
HQ(config-ext-nacl)#exit
HQ(config)#int fa0/1
HQ(config-if)#ip access-group Outside in
HQ(config-if)#exit
```

```
HQ(config)#ip access-list extended Inside
HQ(config-ext-nacl)#permit tcp any host 10.77.77.80 eq www
HQ(config-ext-nacl)#deny ip any host 10.77.77.80
HQ(config-ext-nacl)#permit any any
HQ(config-ext-nacl)#exit
HQ(config)#int fa0/0
HQ(config-if)#ip access-group Inside in
HQ(config-if)#exit
```

```
HQ(config)#ip access-list extended DMZSecurity
HQ(config-ext-nacl)#permit tcp 10.77.77.0 0.0.0.255 any established
HQ(config-ext-nacl)#deny ip any any
HQ(config)#int e0/0/0
HQ(config-if)#ip access-group DMZSecurity in
```

## Etape 3 : Configuration des services Firewall sur HQ

Le service « inspect » permet de caractériser un trafic sortant pour se préparer à accepter le futur trafic en retour. Le Firewall crée ainsi une liste de contrôle d'accès éphémère qui laissera passer le ou les paquets en réponse du trafic sortant.

Créez sur l'interface Outside une règle d'inspection pour les trafics tcp, udp et icmp.

### Commandes :

```
HQ(config)#ip inspect name SecurePolicy tcp
HQ(config)#ip inspect name SecurePolicy ud
HQ(config)#ip inspect name SecurePolicy icmp
```

```
HQ(config)#int fa0/1
HQ(config-if)#ip inspect SecurePolicy out
```

## Etape 4 : Test de connectivité

Faites un ping d'une machine interne vers un des routeurs du réseau

Faites une connexion http d'une machine externe vers l'ip publique du serveur Web: 81.255.255.53

Faites une connexion http d'une machine interne vers l'ip privée du serveur Web: 10.77.77.80

Si tous ces tests sont réussis, passez à l'étape suivante.

## Partie 2 – Configuration d'un réseau privé à base de tunnels GRE

### Etape 1 : Configuration du routeur HQ

Configurez deux interfaces tunnel sur le routeur HQ de façon à avoir la configuration suivante :

```
interface Tunnel0
 ip address 10.2.1.2 255.255.255.252
 tunnel source FastEthernet0/1
 tunnel destination 81.255.255.65
!
!
interface Tunnell
 ip address 10.3.1.2 255.255.255.252
 tunnel source FastEthernet0/1
 tunnel destination 81.255.255.81

!
```

### Etape 2 : Configuration du routeur HOST 2

Configurez une interface tunnel correspondante sur le routeur HOST2.

#### Commandes :

```
HOST2(config)#int tunnel 0

%LINK-5-CHANGED: Interface Tunnel0, changed state to up
HOST2(config-if)#?
  exit      Exit from interface configuration mode
  ip        Interface Internet Protocol config commands
  no        Negate a command or set its defaults
  shutdown  Shutdown the selected interface
  tunnel    protocol-over-protocol tunneling
HOST2(config-if)#tunnel ?
  destination destination of tunnel
  source       source of tunnel packets
HOST2(config-if)#tunnel source ?
  Ethernet      IEEE 802.3
  FastEthernet  FastEthernet IEEE 802.3
  GigabitEthernet GigabitEthernet IEEE 802.3z
  Loopback      Loopback interface
  Serial        Serial
HOST2(config-if)#tunnel source fa0/1
HOST2(config-if)#tunnel destination 81.255.255.49
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to
up
HOST2(config-if)#ip address 10.2.1.1 255.255.255.252
HOST2(config-if)#exit
```

### Etape 3 : Configuration du routeur HOST 3

Configurez une interface tunnel correspondante sur le routeur HOST3, de façon à avoir la configuration suivante :

```
interface Tunnell
 ip address 10.3.1.1 255.255.255.252
 tunnel source FastEthernet0/1
 tunnel destination 81.255.255.49

!
```

#### Etape 4 : Modification de la liste de contrôle d'accès « Outside » sur HQ

Le protocole Generic Routing Encapsulation (GRE) permet de transporter tous types de protocoles dans des paquets IP.

Modifiez la liste de contrôle d'accès en entrée sur le routeur HQ pour obtenir la configuration suivante :

```
ip access-list extended Outside
 permit gre host 81.255.255.65 host 81.255.255.49
 permit gre host 81.255.255.81 host 81.255.255.49
 permit tcp any host 81.255.255.53 eq www
!
```

**Tip :** copiez l'ACL Outside sur Bloc Notes. Recopiez la première ligne et insérez un « no » devant. Puis insérez après la seconde ligne les deux « permit gre ». Recopiez ensuite le tout sur votre routeur en mode config.

#### Etape 5 : Modification des listes de contrôles « NatList » sur tous les routeurs

Les trafics encapsulés dans les tunnels GRE ne doivent subir de translations d'adresses, car nous voulons justement pouvoir rester en adressage privé entre les différents établissements. Pour cela, vous allez exclure ces trafics du service NAT.

Sur les routeurs HQ, HOST2 et HOST3, modifiez la liste NatList de façon à avoir la configuration suivante :

```
ip access-list extended NatList
 deny ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
 permit ip any any
```

#### Etape 6 : Tests de connectivité

Du routeur HQ tapez la commande : ping 10.2.1.1, puis ping 10.3.1.1.  
Si les deux ping sont réussis passez à l'étape suivante.

### Partie 3 – Routage interne

#### Etape 1 : Etat actuel du routage

Placez-vous en mode « Simulation ». D'une machine interne de HOST2, utilisez l'outil « enveloppe » pour essayer de pinger une machine du réseau interne de HQ.  
Que remarquez-vous ? Où s'arrête le paquet ? Que diagnostiquez-vous ?

Faites un « sh ip route » sur les routeurs HQ, HOST2 et HOST3. Voyez-vous les autres réseaux internes ?

#### Etape 2 : Activation de OSPF sur tous les routeurs

Activez le protocole de routage OSPF sur le réseau 10.0.0.0 / 8 sur les routeurs HQ, HOST2 et HOST3 (désactivez tout autre protocole de routage s'il en existe un).

**Tip :** Ecrivez sur "Bloc Notes" les lignes suivantes, puis recopiez-les sur tous les 3 routeurs.

```
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
```

### Etape 3 : Tests de connectivité entre HOST2 et HOST3

Avec l'outil « Enveloppe » pingez à partir d'une machine interne de HOST2, une machine interne de HOST3. Suivez le paquet en mode simulation pour voir par où passe le paquet.

Que remarquez-vous ?

### Etape 4 : Test de connectivité avec HQ

Avec l'outil « Enveloppe » pingez à partir d'une machine interne de HOST2 (ou de HOST3), une machine interne de HQ.

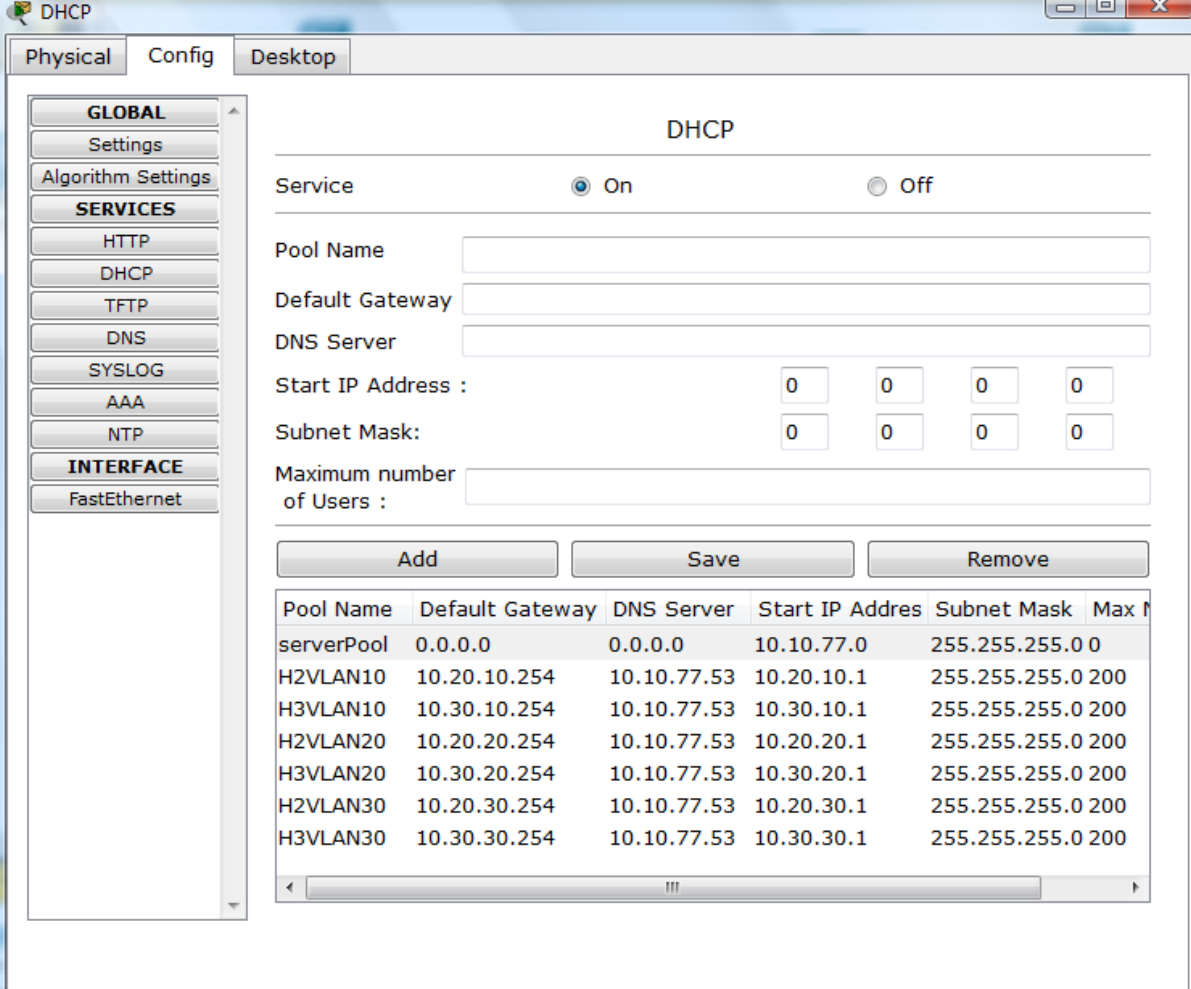
Que constatez-vous ?

Avez-vous une idée du problème ?

### Etape 5 : Pour résoudre ce problème, activez OSPF sur le commutateur de couche 3

## Partie 4 – Intégration des services : exemple de DHCP et DNS

### Etape 1 : Configuration du serveur DHCP



The screenshot shows the DHCP configuration window. The 'Service' is set to 'On'. The configuration fields are as follows:

- Pool Name: (empty)
- Default Gateway: (empty)
- DNS Server: (empty)
- Start IP Address: 0.0.0.0
- Subnet Mask: 0.0.0.0
- Maximum number of Users: (empty)

Buttons: Add, Save, Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max n
serverPool	0.0.0.0	0.0.0.0	10.10.77.0	255.255.255.0	0
H2VLAN10	10.20.10.254	10.10.77.53	10.20.10.1	255.255.255.0	200
H3VLAN10	10.30.10.254	10.10.77.53	10.30.10.1	255.255.255.0	200
H2VLAN20	10.20.20.254	10.10.77.53	10.20.20.1	255.255.255.0	200
H3VLAN20	10.30.20.254	10.10.77.53	10.30.20.1	255.255.255.0	200
H2VLAN30	10.20.30.254	10.10.77.53	10.20.30.1	255.255.255.0	200
H3VLAN30	10.30.30.254	10.10.77.53	10.30.30.1	255.255.255.0	200

Configurez le serveur DHCP avec les pools d'adresses internes de HOST2 et HOST3. Aidez-vous de l'image ci-dessus pour le plan d'adressage. Pensez à définir l'adresse du serveur DNS (10.10.77.53).

## Etape 2 : Configuration des relais DHCP sur HOST2 et HOST3

Sur les routeurs HOST 2 et HOST 3, configurez un relais DHCP sur chacune des sous-interfaces internes. Vous devriez obtenir une configuration similaire à celle-ci-dessous (exemple HOST2).

```
interface FastEthernet0/0.10
  encapsulation dot1Q 10
  ip address 10.20.10.254 255.255.255.0
  ip helper-address 10.10.77.67
  ip nat inside
!
interface FastEthernet0/0.20
  encapsulation dot1Q 20
  ip address 10.20.20.254 255.255.255.0
  ip helper-address 10.10.77.67
  ip nat inside
!
interface FastEthernet0/0.30
  encapsulation dot1Q 30
  ip address 10.20.30.254 255.255.255.0
  ip helper-address 10.10.77.67
  ip nat inside
!
```

## Etape 3 : Configuration les interfaces des PC des réseaux internes en mode DHCP

Configurez les interfaces des PC en mode DHCP.

Si le PC était précédemment configuré de façon statique, forcez le renouvellement d'adresse avec la commande > ipconfig / renew

## Etape 4 : Configuration du service DNS

Configurez une entrée DNS dans le serveur DNS : [www.ismin.fr](http://www.ismin.fr) – 10.77.77.80.

Testez ensuite une connexion web vers le serveur ismin en utilisant l'onglet « Web Browser ».

