Multisites S.A. module «réseau IP»

version du 17/01/2009

TP N°3 : Installation du routeur firewall iptables

Nom : **Prénom :** **Classe :** **Date :**	**Appréciation** :	**Note** :
Objectifs : - Être capable d'installer le service de routage et filtrage (firewall)		**durée** : 3h

Matériel :

- 1 ordinateur PC Client XP pro. « legolas ».
- 1 ordinateur PC Client XP pro. «dns-h».
- 1 ordinateur PC Eole Linux AMON « arwen » équipé de 3 interfaces réseau Ethernet.

Travail à réaliser :

- S'informer ...

- Se connecter ...

- Configurer ...

- Tester ...

Configuration IP du routeur Arwen	
Module	Réseau IP
Nom DNS	arwen
interface eth0	192.168.7.254 (255.255.255.0)
interface eth1	10.0.0.254 (255.255.255.0)
interface eth2	172.16.0.254 (255.255.255.0)
passerelle	adsl (10.0.0.253)
DNS primaire	192.168.7.252
DNS secondaire	80.118.192.111

Configuration du routeur iptables Arwen

- Vérifier les connexions physiques des interfaces Ethernet en tapant :

mii-tool

Relever les informations fournies par mii-tool :

eth0 :_____

eth1 :_____

eth2 :_____

- Configurez l'interface **eth0** d'Arwen :

ifconfig eth0 192.168.7.254

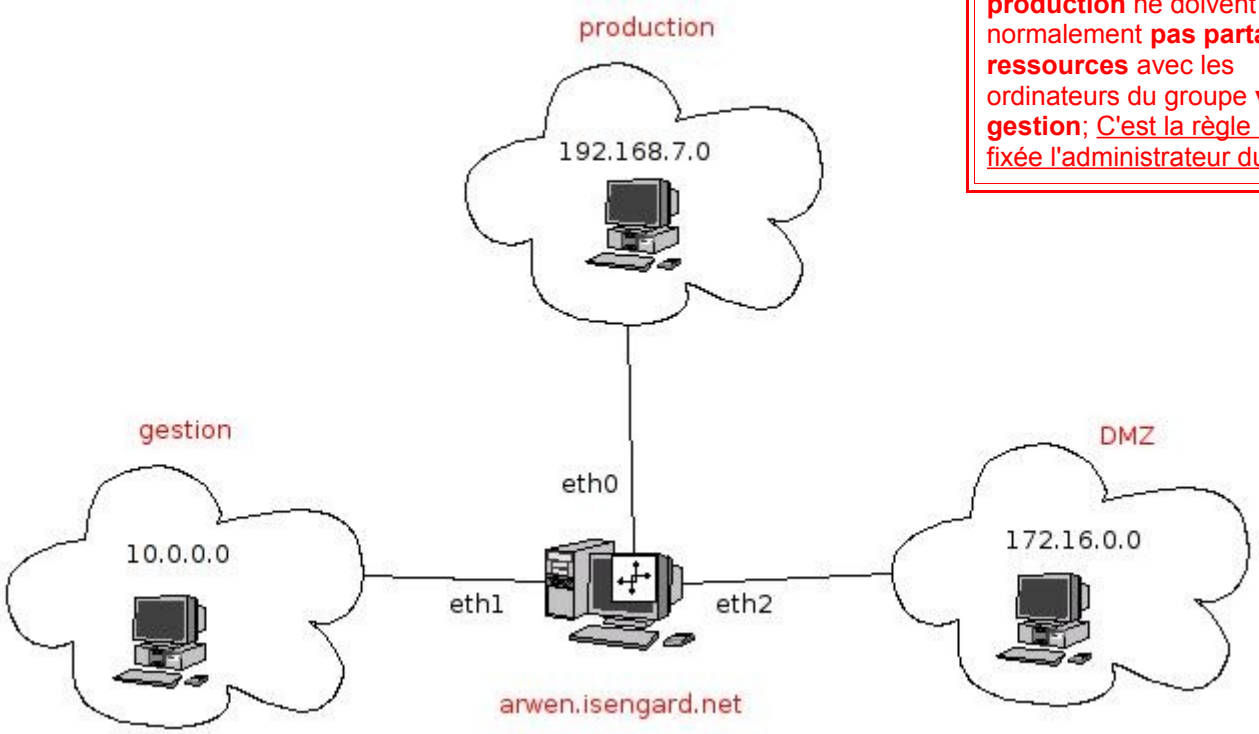
- Connectez-vous à l'interface d'administration Webmin d'Arwen : https://192.168.7.254:10000

  Aller dans *Réseau => Configuration réseau* et configurer les 3 interfaces, la passerelle et le dns

Configuration IP du routeur Arwen	
Module	Réseau IP
Nom DNS	**Arwen**
interface **eth0**	192.168.7.254 (255.255.255.0)
interface **eth1**	10.0.0.254 (255.255.255.0)
interface **eth2**	172.16.0.254 (255.255.255.0)
passerelle	adsl (10.0.0.253)
DNS primaire	192.168.7.252
DNS secondaire	80.118.192.111

Routage entre vlans

Les ordinateurs du **vlan production** ne doivent normalement **pas partager de ressources** avec les ordinateurs du groupe **vlan gestion**; C'est la règle qu'a fixée l'administrateur du réseau.



information

Le rôle d'un routeur est de connecter deux réseaux IP. **Un réseau IP est caractérisé par son adresse de réseau** (ex : voir ci-dessus); il peut s'agir d'une adresse publique (WAN) ou privée (LAN). Deux réseaux IP ne peuvent pas communiquer sans l'utilisation d'un ou plusieurs routeurs. **Le routage se fait au niveau 3 du modèle OSI** : il est indépendant des technologies utilisées pour la liaison (couche OSI 1 et 2)

- **Le routage n'étant pas encore activé**, faire un : **ping** de **192.168.7.136** vers **10.0.0.232**

  (c'est-à-dire : ping de l***egolas*** dans **production** vers ***solo*** dans **Gestion**)

➔ Quel est le résultat ? _____ (normalement : pas de réponse)

➔ Pourquoi ? _____

- **Activer le routage** avec *Webmin->réseaux->Configuration->Passerelle et routage*

  Cliquer sur : « *agir comme un routeur : oui* » , puis valider.

- **Vérifier** la prise en compte par le serveur en faisant :

  - **cat /proc/sys/net/ipv4/ip_forward**
  - le résultat doit être "1", sinon refaire la manipulation dans webmin.

➔ Le paramètre ip_forward est-il à "1" ? _____

➔ Vérifier les connexions réseaux suivantes :

PING	Résultat	Remarque
legolas (192.168.7.136) -> **arwen** (192.168.7.254)		
gandalf (172.16.0.1) -> **arwen** (172.16.0.254)		
legolas (192.168.7.136) -> **gandalf** (172.16.0.1)		[ce ping prouve que le routage fonctionne vers la DMZ]
legolas (192.168.7.136) -> **solo** (10.0.0.232)		[ce ping prouve que le routage fonctionne vers le vlan Gestion]

- Dans le cas présent, **le routeur permet à 3 réseaux locaux Ethernet de communiquer**.

Sur Internet, les routeurs relient des réseaux téléphoniques; ils doivent gérer des paramètres inconnus par le protocole IP, comme par exemple, le coût de passage, l'encombrement, etc... c'est pourquoi , on a besoin de protocoles de routage complémentaires à IP

➔ Citer deux protocoles de routages utilisés par les routeurs Internet :

_____

_____

Configuration du filtrage inter-vlans

Les ordinateurs du **vlan production** ne doivent normalement **pas partager de ressources** avec le ordinateurs du groupe **vlan gestion**; C'est la règle qu'a fixée l'administrateur du réseau.

Pour valider le fonctionnement du firewall : vous allez d'abord créer deux partages de ressources « pirates », puis **configurer le firewall de façon à les bloquer.**

- Créer un partage de fichier «pirate» que vous appellerez : "**test**" sur **solo** (10.0.0.232)
- Sur legolas, accéder à ce partage en ouvrant : **\\10.0.0.232\test**

➔ **conclusion** : accédez-vous à ce partage « pirate » ? _____*(normalement : OK)*

➔ Aller dans *Favoris réseau* sur **legolas** : voyez-vous le partage test ?
_____*(normalement : non)*

➔ **Expliquer** pourquoi *Favoris réseau* ne fonctionne pas : _____

- **Installation** d'un serveur WEB « pirate »
  - télécharger EasyPHP1.7
  - installer EasyPHP1.7 sur **legolas** (192.168.7.136)

- **Vérifier** l'accès au service web **depuis solo** (dans firefox ouvrir : **http://192.168.7.136**)
  ➔ conclusion : accédez-vous à ce partage web « pirate » ? _____*(normalement : OK)*

- **Mise en place du filtrage :**

- Créer une règle FORWARD : **Set default action to : drop**

  ➔ **Expliquer** cette règle : _____

- **Appliquer** en cliquant sur : **Apply configuration**

  ➔ **Vérifier** : avons-nous bloqué le fonctionnement du partage "test" et du serveur WEB « pirate » : _____ _____*(normalement : oui)*

Nous avons donc bloqué les connexions interdites; nous allons maintenant ajouter les règles nécessaires pour **débloquer** les connexions autorisées**.**

➔ **La connexion d'un poste *quelconque* vers le serveur WEB en DMZ est-elle bloquée ?** Pour le vérifier, essayer d'accéder au serveur web de **gandalf-v** (172.16.0.231) en ouvrant l'adresse : http://172.16.0.231 depuis firefox de l'ordinateur **legolas** (192.168.7.136);
résultat : _____ *(normalement : pas de réponse)*

➔ **Quel port TCP le service WEB (http) utilise-t-il?** _____

- Créer une règle FORWARD :

  Accept If protocol is TCP and destination is 172.16.0.231 and destination port is 80

- Créer une règle FORWARD :

  Accept If protocol is TCP and source is 172.16.0.231 and source port is 80

➔ Expliquer cette règle : _____

- **Appliquer** en cliquant sur : ***Apply configuration***
- **Re-verifier** l'accès au serveur web de **gandalf-v** (172.16.0.231)

➔ Pour le vérifier faire un http://172.16.0.231 depuis Legolas; *(normalement : OK)*

➔ **conclusion** : l'accès au serveur web a-t-il bien été débloqué par cette règle ? _____

➔ **Re-vérifier** l'accès au service web « pirate » de **legolas** depuis solo : **http://192.168.7.136**

➔ **conclusion** : accédez-vous à ce partage web « pirate » ? _____*(normalement : pas de réponse)*

➔ **Expliquer** pourquoi la règle que vous avez créée autorise le partage web de gandalf-v et pas le partage web de Legolas : _____

- Créer une règle FORWARD : **Accept If protocol is UDP and destinatation port is 53**
- Créer une règle FORWARD : **Accept If protocol is UDP and source port is 53**

➔ **Expliquer** ces règles : _____

Créer une règle FORWARD : **Si la destination n'est pas 10.0.0.0/24 et l'interface de sortie est eth1**

- Créer une règle FORWARD : **Si la source n'est pas 10.0.0.0/24 et l'interface d'entrée est eth1**

➔ **Expliquer** ces règles : _____

_____

- Appliquer en cliquant sur : **Apply configuration**