Bacpro SEN TR
firewall IPTABLES

MRIM Château-Blanc

version du 17/01/2009

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. « gestion ».
- 1 ordinateur PC Client XP pro. «production».
- 1 ordinateur PC Centos Linux server équipé de 2 interfaces réseau Ethernet. "arwen"

Travail à réaliser :

- S'informer ...

- Se connecter ...

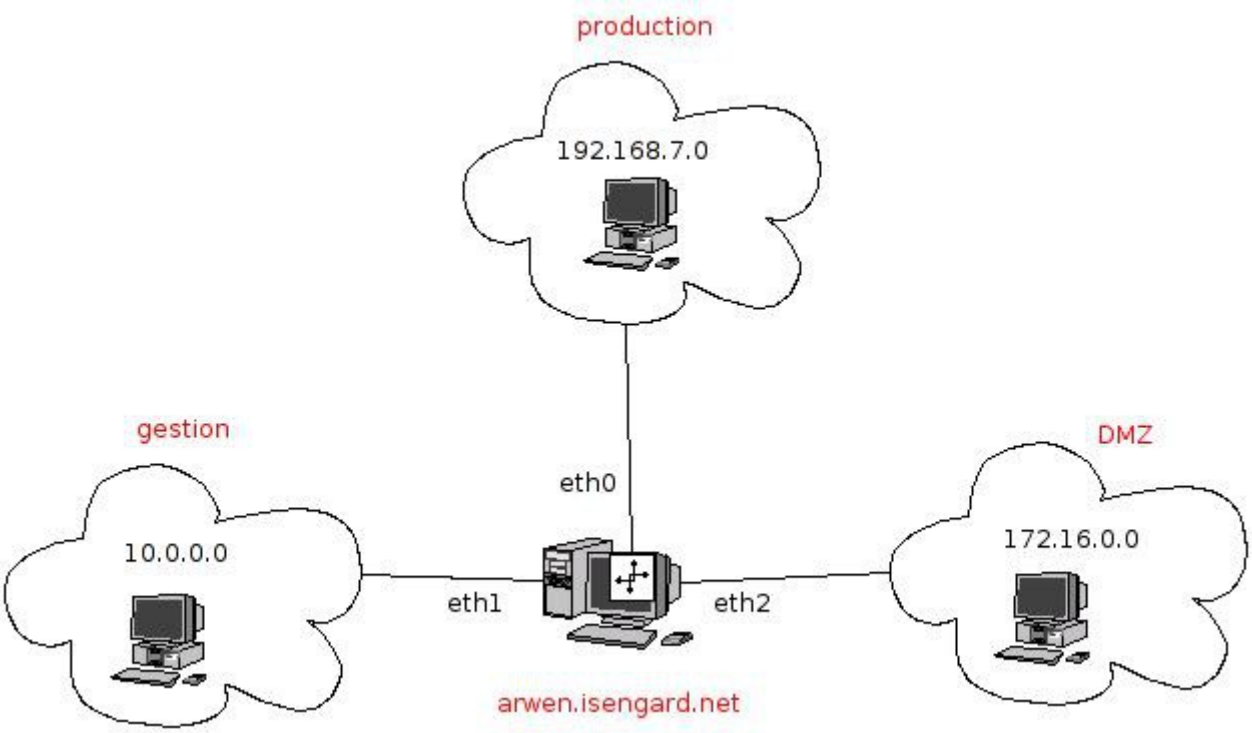
- Configurer ...

- Tester ...

Configuration IP du routeur Arwen	
OS	Centos 5.3 server
RAM	256Mo
Nom DNS	arwenXX
interface eth0	**192.168.7.2XX** (255.255.255.0)
interface eth1	**10.0.0.2XX** (255.255.255.0)
passerelle	192.168.7.254
DNS primaire	192.168.7.252
DNS secondaire	80.118.192.111

IP SCHEMA DU RESEAU

Le réseau est composé de 2 ou 3 sous-réseaux (qui sont souvent des VLAN). Ces réseaux doivent être isolés, mais on souhaite souvent que certaines données puissent être échangées entre ces VLAN, on va donc écrire des règles (ACL = Access Control List) pour définir ce qui est autorisé à passer ou non.



Pour la réalisation de ce TP, vous aurez besoin de 3 machines virtuelles : client, production et routeur (arwen)

Configuration IP du client "production"	
OS	Windows XP
RAM	128Mo
Nom DNS	productionXX
Adresse IP/masque	**192.168.7.1XX** (255.255.255.0)
passerelle	192.168.7.2XX
DNS primaire	80.118.192.111
DNS secondaire	

Configuration IP du client "gestion"	
OS	Windows XP
RAM	128Mo
Nom DNS	gestionXX
Adresse IP/masque	**10.0.0.1XX** (255.255.255.0)
passerelle	10.0.0.2XX
DNS primaire	80.118.192.111
DNS secondaire	

IP ROUTAGE ET FILTRAGE

Installation du routeur/firewall "arwen"

Voir le tutoriel : http://www.cvardon.fr/tutos/divers_Installation_de_Centos5-serveur.html

(en y incluant l'installation de Webmin)

Configuration des interfaces Ethernet du routeur/firewall "arwen"

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

ifconfig eth0 192.168.7.2XX

- Connectez-vous à l'interface d'administration Webmin d'Arwen : https://192.168.7.2XX:10000

  Aller dans *Réseau => Configuration réseau* et configurer les 2 interfaces, la passerelle et le dns

Installation des machines virtuelles XP

Installer ces machines avec les paramètres indiquées ci-dessus.

N'oubliez pas de désactiver le pare-feu de Windows XP .

Créez un partage "production" sur la machine "production" et un partage "gestion" sur la machine "gestion

Créez un fichier "production.txt" dans le partage "production" et un "gestion .txt" dans le partage "gestion"

Installer un partage web ("EasyPHP1.7") sur chacune des machines "production" et "gestion".

Créer une page "index.html" avec le texte "VLAN PRODUTION" en taille "h1" et "centré" au milieu de la page sur la machine "production" et le texte "VLAN GESTION" sur la machine "gestion".

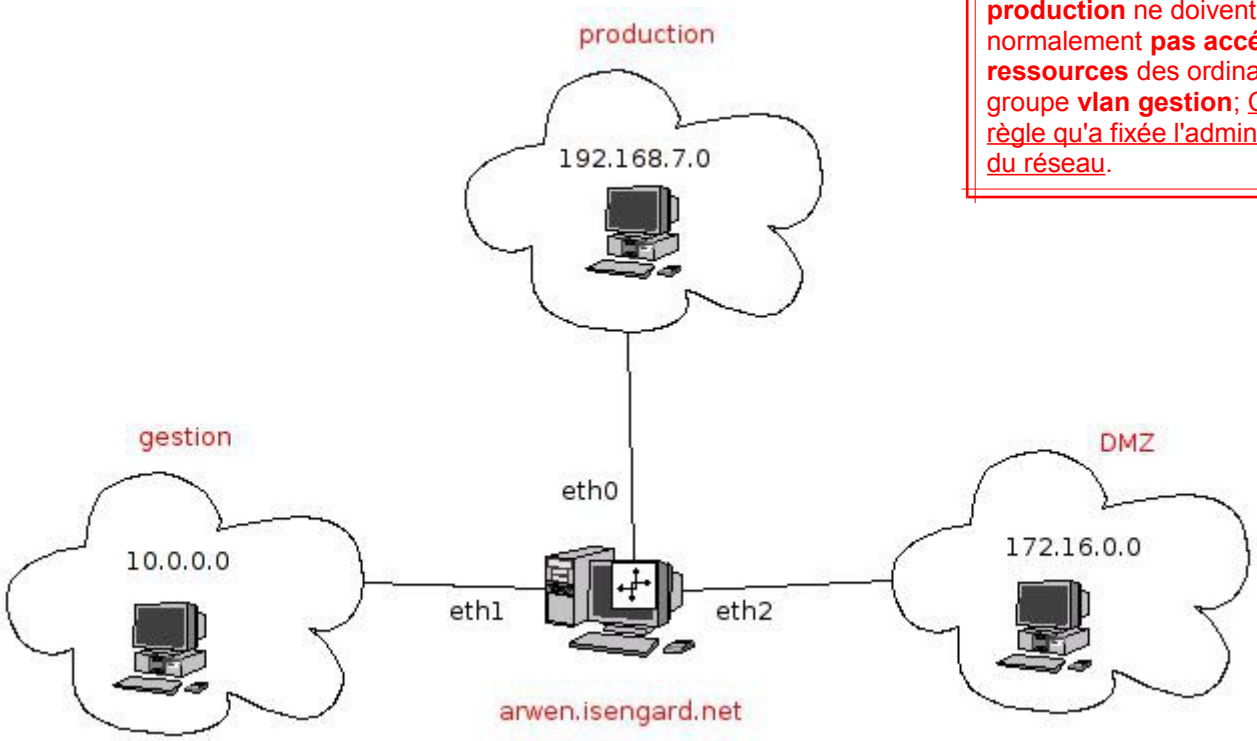
OBJECTIFS DU TP

L'administrateur a fixé les 6 règles suivantes :

(1) les utilisateurs de "gestion" doivent accéder à un serveur web situé dans "production"
(2) les utilisateurs de "production" doivent accéder à un serveur web situé dans "gestion"
(3) les utilisateurs de "gestion" doivent accéder à un partage de fichier Microsoft dans "production"
(4) les utilisateurs de "production" **ne** doivent **pas** accéder à un partage de fichier Microsoft dans "gestion"
(5) les utilisateurs de "gestion" peuvent faire un "ping" sur une machine situé dans "production"
(6) les utilisateurs de "production" **ne** peuvent **pas** faire un "ping" sur une machine situé dans "gestion"

Routage entre vlans

Les ordinateurs du **vlan production** ne doivent normalement **pas accéder aux ressources** des 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 **gestion** vers **production**

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

➔ Pourquoi ? _____

information
La couche réseau de Linux Centos est capable de router les paquets venant de son interface **gestion** vers sont interface **production** **C'est-à-dire de faire communiquer le réseau 192.168.7.0 avec le réseau 10.0.0.0** Pour cela il suffit d'**activer le routage** dans Webmin ou de modifier le fichier "sysctl.conf"

- **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
production (192.168.7.____**)** **-> arwen (**192.168.7.2XX**)**		
gestion (10.0.0.____**)** **-> arwen (**192.168.7.2XX**)**		
production (192.168.7.____**)** **-> gestion** (10.0.0.1_____)		[ce ping prouve que le routage fonctionne vers le vlan Gestion]

- Dans le cas présent, **le routeur permet à 2 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 : que se passe-t-il quand rien n'est filtré ?

Rappel des règles fixée par l'administrateur du réseau

L'administrateur a fixé les 6 règles suivantes :

(1) les utilisateurs de "gestion" doivent accéder à un serveur web situé dans "production"
(2) les utilisateurs de "production" doivent accéder à un serveur web situé dans "gestion"
(3) les utilisateurs de "gestion" doivent accéder à un partage de fichier Microsoft dans "production"
(4) les utilisateurs de "production" **ne** doivent **pas** accéder à un partage de fichier Microsoft dans "gestion"
(5) les utilisateurs de "gestion" peuvent faire un "ping" sur une machine situé dans "production"
(6) les utilisateurs de "production" **ne** peuvent **pas** faire un "ping" sur une machine situé dans "gestion"

Remplissez le tableau suivant en vérifiant si les règles sont bien respectées (oui/non) :

		Expliquer comment vous avez vérifié :
La règle (1) est-elle respectée ?		
La règle (2) est-elle respectée ?		
La règle (3) est-elle respectée ?		
La règle (4) est-elle respectée ?		
La règle (5) est-elle respectée ?		
La règle (6) est-elle respectée ?		

Rappels sur l'accès aux service WEB et partage de fichier Microsoft

- On accède à un partage WEB à l'aide d'un client web (ex : internet explorer, firefox, chrome...); dans le champ "url" on entre : "http://192.168.7.1XX" où 192.168.7.1XX correspond à l'adresse du serveur.

- On accède à un partage de fichier Microsoft en faisant un "démarrer" => "executer" => "\\192.168.7.1XX" où 192.168.7.1XX correspond à l'adresse du serveur.

Configuration du filtrage : Mise en place initiale du firewall

Information
Quand on configure un pare-feu (angl : firewall), on commence par sécurité à tout interdire par défaut. Puis on autorise certaines connexions au "compte-goutte"; ainsi on a pas de surprise...

Rappel des règles fixée par l'administrateur du réseau
(4) les utilisateurs de "production" **ne** doivent **pas** accéder à un partage de fichier Microsoft dans "gestion"
(6) les utilisateurs de "production" **ne** peuvent **pas** faire un "ping" sur une machine situé dans "gestion"

la règle que nous allons créer maintenant va tout interdire par défaut

- **Mise en place du filtrage :**

- Dans Webmin, aller sur "Réseau" => "Linux Firewall"
- Créer une règle FORWARD : **Set default action to : drop**

Explication : vous devez sélectionner "drop", puis cliquer sur "set default action"

➔ **Expliquer** cette règle : 

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

Remplissez le tableau suivant en vérifiant si les règles sont bien respectées (oui/non) :

		Expliquer comment vous avez vérifié :
La règle (4) est-elle respectée ?		
La règle (6) est-elle respectée ?		

Configuration du filtrage : règle 1

règle 1
L'administrateur a fixé la règle suivante : (1) les utilisateurs de "gestion" doivent accéder à un serveur web situé dans "production"

Remplissez le tableau suivant en vérifiant si les règles sont bien respectées (oui/non) :

		Expliquer comment vous avez vérifié :
La règle (1) est-elle respectée ?		

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

- Créer une règle FORWARD :

  Accept If protocol is TCP and destination is 192.168.7.0 and destination port is 80

- Créer une règle FORWARD :

  Accept If protocol is TCP and source is 192.168.7.0 and source port is 80

➔ Expliquer cette règle : _____

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

Remplissez le tableau suivant en vérifiant si les règles sont bien respectées (oui/non) :

		Expliquer comment vous avez vérifié :
La règle (1) est-elle respectée ?		

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

Configuration du filtrage : règle 2

règle 1
L'administrateur a fixé la règle suivante : (2) les utilisateurs de "production" doivent accéder à un serveur web situé dans "gestion"

Remplissez le tableau suivant en vérifiant si les règles sont bien respectées (oui/non) :

		Expliquer comment vous avez vérifié :
La règle (2) est-elle respectée ?		

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

- Créer une règle FORWARD :

  Accept If protocol is TCP and destination is 10.0.0.0 and destination port is 80

- Créer une règle FORWARD :

  Accept If protocol is TCP and source is 10.0.0.0 and source port is 80

➔ Expliquer cette règle : _____

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

Remplissez le tableau suivant en vérifiant si les règles sont bien respectées (oui/non) :

		Expliquer comment vous avez vérifié :
La règle (2) est-elle respectée ?		

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

Configuration du filtrage : règle 3

règle 1
L'administrateur a fixé la règle suivante : (3) les utilisateurs de "gestion" doivent accéder à un partage de fichier Microsoft dans "production"

Remplissez le tableau suivant en vérifiant si les règles sont bien respectées (oui/non) :

		Expliquer comment vous avez vérifié :
La règle (3) est-elle respectée ?		

➔ **Quel port TCP le service partage de fichier Microsoft utilise-t-il?** _____

- Créer une règle FORWARD :

  Accept If protocol is TCP and destination is 192.168.7.0 and destination port is 445

- Créer une règle FORWARD :

  Accept If protocol is TCP and source is 192.168.7.0 and source port is 445

➔ Expliquer cette règle : _____

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

Remplissez le tableau suivant en vérifiant si les règles sont bien respectées (oui/non) :

		Expliquer comment vous avez vérifié :
La règle (3) est-elle respectée ?		

➔ **conclusion** : l'accès au partage de fichier Microsoft a-t-il bien été débloqué par cette règle ? _____

Configuration du filtrage : règle 5

règle 1
L'administrateur a fixé la règle suivante : (5) les utilisateurs de "gestion" peuvent faire un "ping" sur une machine situé dans "production" (6) les utilisateurs de "production" **ne** peuvent **pas** faire un "ping" sur une machine situé dans "gestion"

Remplissez le tableau suivant en vérifiant si les règles sont bien respectées (oui/non) :

		Expliquer comment vous avez vérifié :
La règle (5) est-elle respectée ?		

➔ **Quel protocole la commande "ping" utilise-t-il? _____**

➔ **Quel est le message ICMP utilisé pour une demande de ping ? _____**

➔ **Quel est le message ICMP utilisé pour une réponse au ping ? _____**

- Créer une règle FORWARD pour autoriser la demande de ping de gestion vers production :

- Créer une règle FORWARD pour autoriser la réponse de ping de production vers gestion :

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

Remplissez le tableau suivant en vérifiant si les règles sont bien respectées (oui/non) :

		Expliquer comment vous avez vérifié :
La règle (5) est-elle respectée ?		
La règle (6) est-elle respectée ?		

➔ **conclusion** : le ping fonctionne-t-il de gestion vers production uniquement ? _____