Bacpro SN RISC
firewall IPTABLES

version du 27/01/2019

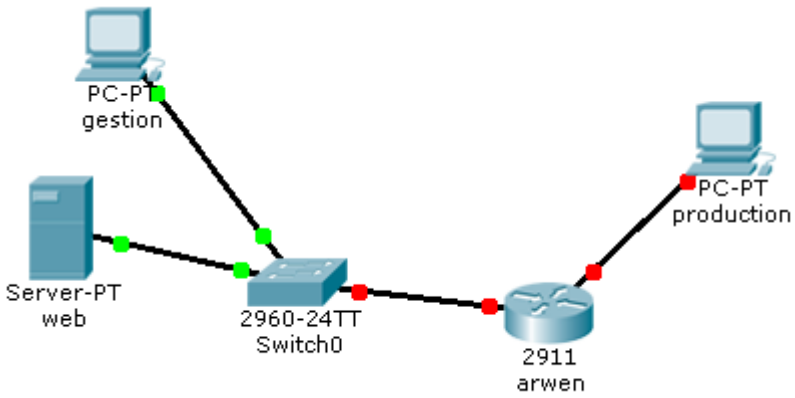
Installation du routeur firewall iptables

Nom : _____ **Prénom :** _____ **Classe :** **Date :**	**Appréciation** : (6 points d'autonomie si n'utilisez pas le "support")	**Note** : **/90**

Objectifs :
- Être capable d'installer le service de routage et filtrage (firewall)

durée : 3h

Matériel :
- 1 ordinateur Client XP pro. Virtuel « gestion ».
- 1 ordinateur Client XP pro. Virtuel «production».
- 1 serveur Debian Linux Virtuel (Serveur "web" 10.X.0.80)
- 1 routeur Debian Linux Virtuel équipé de 2 interfaces réseau Ethernet. "arwen"

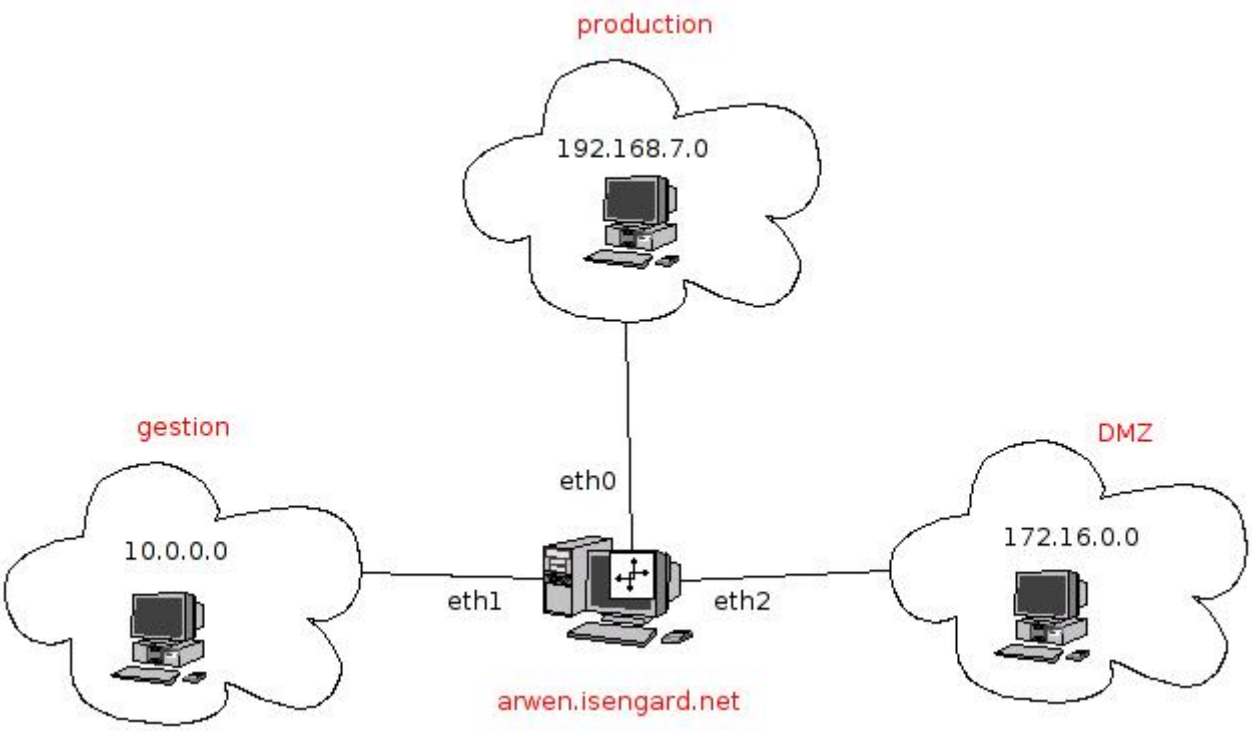


Compétences visées :

Configuration IP du routeur Arwen	
OS	Debian 8.6 server
RAM	768Mo
Nom DNS	arwen**Y**
interface eth1	**192.168.Y.254** (255.255.255.0)
interface eth0	**10.X.Y.254** (255.255.0.0)
passerelle	10.X.0.254
DNS primaire	10.0.0.254
DNS secondaire	8.8.8.8

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 créer 3 machines virtuelles : client, production et routeur (arwen) ; le serveur web existe déjà.

Configuration IP du client "production"	
OS	Windows XP
RAM	128Mo
Nom DNS	production**Y**
Adresse IP/masque	**192.168.Y.1** (255.255.255.0)
passerelle	192.168.**Y**.254
DNS primaire	8.8.8.8
DNS secondaire	

Configuration IP du client "gestion"	
OS	Windows XP
RAM	128Mo
Nom DNS	gestion**Y**
Adresse IP/masque	**10.X.Y.1** (255.255.255.0)
passerelle	10.**X.Y**.254
DNS primaire	8.8.8.8
DNS secondaire	

IP ROUTAGE ET FILTRAGE

Installation du routeur/firewall "arwen"

- Voir le tutoriel : http://cvardon.fr/tutos/divers_Installer_un_serveur_Debian_8.html

Installer le logiciel Webmin :

- apt-get update
- wget http://www.webmin.com/download/deb/webmin-current.deb
- dpkg --install webmin-current.deb (ne pas tenir compte des messages d'erreur)
- apt-get install -f

Configuration des interfaces Ethernet du routeur/firewall "arwen"

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

ifconfig eth0 10.X.Y.254 netmask 255.255.0.0

- Connectez-vous à l'interface d'administration Webmin d'Arwen : https://10.X.Y.254:10000

Chercher ***Network Configuration (Activated at boot)*** dans les menus et configurer les 2 interfaces eth0 et eth1, puis la passerelle par défaut et les DNS (vous devez connaître les termes anglais correspondants!!)

Paramètres IP de eth0 et eth1 (adresses IP, masque, adresse mac)

(on doit voir les paramètres des deux interfaces!!)

(6 points)

en lettres noires sur fond blanc !!

Taper la commande "route -n" (pour vérifier l'adresse de la passerelle)

Coller la copie d'écran

(2 points)

en lettres noires sur fond blanc !!

Faire un "ping -c 1 www.google.fr" (pour vérifier l'adresse dns et la connexion)

Coller la copie d'écran

(2 points)

en lettres noires sur fond blanc !!

- Rebooter le serveur et vérifier les paramètres IP. (en cas d'erreur, refaire la configuration)

➔ Coller ci-dessous les copies d'écran demandées :

Paramètres IP des clients Windows XP

(faire un "ipconfig/all" sur chaque machine et coller les copies d'écran)

(adresse ip, masque, passerelle, dns)

(4 points)

en lettres noires sur fond blanc !!

Installation des machines virtuelles XP

Installer ces machines avec les paramètres indiquées ci-dessus.

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

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

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

Coller les copies d'écran

de la configuration

des partages

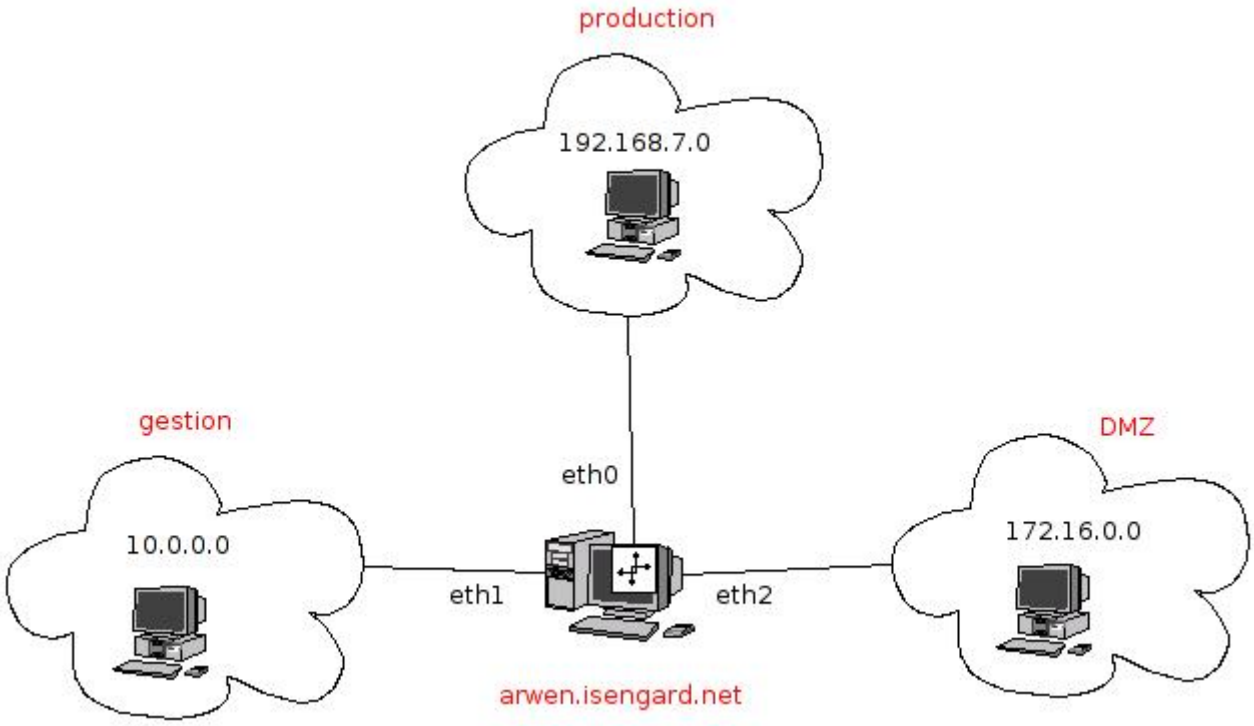
(2 points)

Routage entre vlans

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"



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 ? _____ **(2 points)**

information
La couche réseau de Linux Debian est capable de router les paquets venant de son interface **gestion** vers son interface **production** **C'est-à-dire de faire communiquer le réseau 192.168.Y.0 avec le réseau 10.X.Y.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 réseau suivantes, et coller une copie d'écran (en lettres noires sur fond blanc !!) :

PING	Résultat	coller les copies d'écran des "ping"
production (192.168.Y.____**)** -> **arwen (**192.168.Y.254**)**		**(2 points)**
gestion (10.X.Y.____**)** -> **arwen (**192.168.Y.254**)**		**(2 points)**
production (192.168.Y.____**)** -> **gestion** (10.X.Y.1_____)		**(2 points)**

- 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 :

_____ **(2 points)**

- Sur un réseau local **Ethernet ou s**ur Internet, les routeurs doivent déterminer le réseau de destination à partir de l'adresse IP et du masque de réseau; quelle opération logique utilise-t-on pour cela ? **(1 point)**

	192.168.123.2	=> @IP
	255.255.255.0	=> masque
=	192.168.123.0	=> **@réseau**

- Parfois au lieu d'utiliser le masque sous la forme 255.255.255.0, on utilise la notation 192.168.1.10 **/**24 comment appelle-t-on cette notation ? _____**(1 point)**

- Soit la table de routage suivante, quels sont les réseaux que ce routeur peut atteindre directement ? pour aller vers internet, quel autre routeur doit-il emprunter ? **(6 points)**

```
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
192.168.2.0     *               255.255.255.0   U     0      0        0 eth2
10.0.0.0        *               255.255.255.0   U     0      0        0 eth1
192.168.168.0   *               255.255.255.0   U     0      0        0 vmnet8
10.145.10.0     192.168.231.254 255.255.255.0   UG    0      0        0 eth0
192.168.173.0   *               255.255.255.0   U     0      0        0 vmnet1
192.168.224.0   *               255.255.248.0   U     0      0        0 eth0
link-local      *               255.255.0.0     U     1000   0        0 eth1
default         10.0.0.250      0.0.0.0         UG    100    0        0 eth1
```

Réseaux accessibles directement	**1ère adresse IP du réseau**	**dernière adresse IP du réseau**	**interface**	

Routeur à emprunter pour aller vers internet :	**/1 pt**

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 au serveur web dans "gestion" (2) les utilisateurs de "production" doivent accéder au serveur web 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) :

Rappel : lors des tests (3) et (4), n'oubliez pas de faire les copies d'écran pour la page 5

Note : les réponses doivent être précises; par exemple, s'il y a un message d'erreur, vous devez le citer..

		Expliquer comment vous avez vérifié **(1 points par réponse)**
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 ?		*coller la copie d'écran (lettres noires sur fond blanc)*
La règle (6) est-elle respectée ?		*coller la copie d'écran (lettres noires sur fond blanc)*

Rappels sur l'accès aux service WEB et partage de fichier Microsoft
Vous devez connaître les méthodes d'accès (client) à ces services.

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 : _____ **(1 point)**

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

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

Note : les réponses doivent être précises; par exemple, s'il y a un message d'erreur, vous devez le citer..

		Expliquer comment vous avez vérifié **(2 points par réponse)**
La règle (4) est-elle respectée ?		
La règle (6) est-elle respectée ?		*coller la copie d'écran (lettres noires sur fond blanc)*

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 "gestion"

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

Note : les réponses doivent être précises; par exemple, s'il y a un message d'erreur, vous devez le citer..

		Expliquer comment vous avez vérifié **(2 points par réponse)**
La règle (1) est-elle respectée ?		

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) :

Note : les réponses doivent être précises; par exemple, s'il y a un message d'erreur, vous devez le citer..

		Explique comment tu as vérifié **(2 points par réponse)**
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.X.Y.0 and destination port is 80

- Créer une règle FORWARD :

Accept If protocol is TCP and source is 10.X.Y.0 and source port is 80

➔ Explique cette règle : _____

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

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

		Explique comment tu as vérifié **(1 point par réponse)**
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 3
L'administrateur a fixé la règle suivante : (3) les utilisateurs de "gestion" doivent accéder à un partage de fichier Microsoft dans "production"

- Remplis le tableau suivant en vérifiant si les règles sont bien respectées :

Note : les réponses doivent être précises; par exemple, s'il y a un message d'erreur, tu dois le citer..

		Explique comment tu as vérifié **(2 points par réponse)**
La règle (3) est-elle respectée ?		

➔ Quels ports TCP le service partage de fichier Microsoft utilise-t-il? _____**(2 points)**

- Créer une règle FORWARD :

Accept If protocol is TCP and destination is 192.168.Y.0 and destination port is 445

- Créer une règle FORWARD :

Accept If protocol is TCP and source is 192.168.Y.0 and source port is 445

➔ Expliquer cette règle : _____

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

- Remplis le tableau suivant en vérifiant si les règles sont bien respectées :

		Explique comment tu as vérifié **(2 points par réponse)**
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 5
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"

- Remplis le tableau suivant en vérifiant si les règles sont bien respectées :

Note : les réponses doivent être précises; par exemple, s'il y a un message d'erreur, tu dois le citer..

		Expliquer comment tu as vérifié **(2 points par réponse)**
Les règles (5) et (6) sont-elle respectées ?		*coller les copies d'écran (lettres noires sur fond blanc)*

➔ Quel protocole la commande "ping" utilise-t-il? _____**(2 points)**

➔ Quel est le message ICMP utilisé pour une demande de ping ? _____**(2 points)**

➔ Quel est le message ICMP utilisé pour une réponse au ping ? _____**(2 points)**

- Créer une règle FORWARD pour autoriser la demande de ping de gestion vers production : **(3 points)**

- Créer une règle FORWARD pour autoriser la réponse de ping de production vers gestion : **(3 points)**

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

- Remplis le tableau suivant en vérifiant si les règles sont bien respectées :

		Explique comment tu as vérifié **(2 points par réponse)**
La règle (5) est-elle respectée ?		*coller la copie d'écran (lettres noires sur fond blanc)*
La règle (6) est-elle respectée ?		*coller la copie d'écran (lettres noires sur fond blanc)*

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