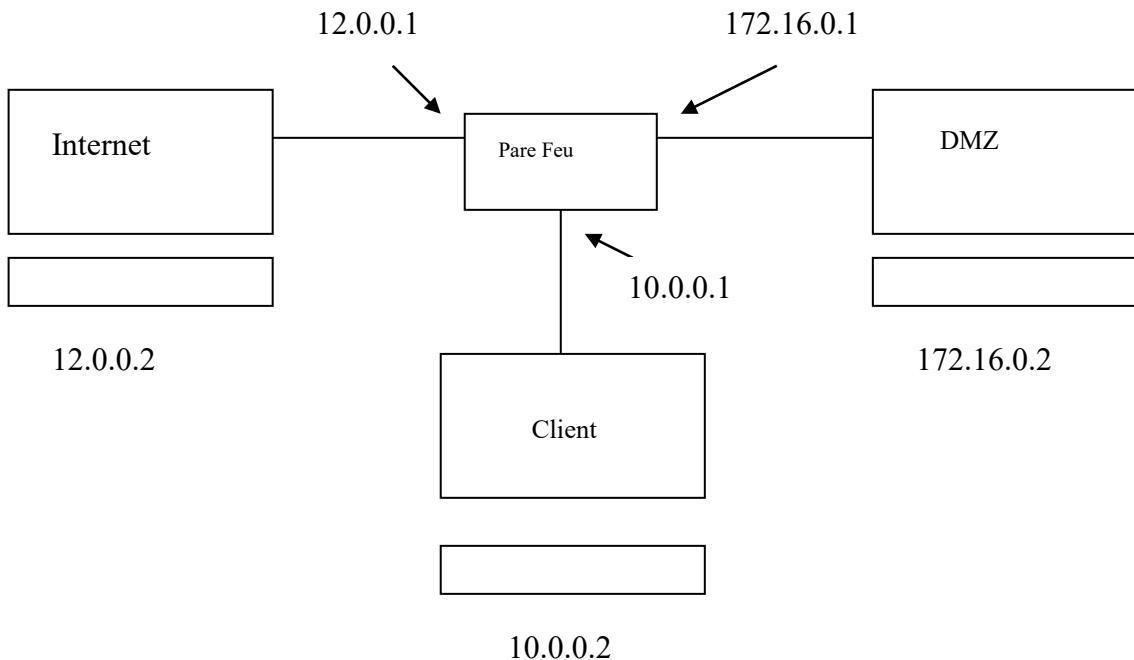


TP Sécurisation d'un réseau privé

Routeur filtrant – Zone DéMilitarisée – Nat Pat - Proxy

Public(s)	Section de BTS Informatique de gestion option :ARLE
Savoir(s)	C21 Installer et configurer un microordinateur C22 Installer et configurer un réseau
Capacité(s)	C22 Installer et configurer un réseau C26 Installer un routeur
Objectif(s)	<ul style="list-style-type: none">• Sécuriser les échanges en centralisant les flux sur le serveur PROXY• La redirection permet masquer l'adresse IP du serveur Web privé
Professeur	Christophe CHITTARATH



Le but de cette PTI est de sécuriser un réseau privé en déployant les différentes technologies étudiées en classe, à savoir : le protocole NAT-PAT (Network Adresse Protocol – Port Adresse Protocol), le serveur Proxy, le Pare-Feu, et la DMZ ...etc

Première partie

Questions :

- a) Que signifie la DMZ ? Que trouve t-on en général dans cette zone ? son rôle et ses intérêts ?

Première étape :

Création d'un team contenant quatre machines virtuelles suivantes :

hostname	Système d'exploitation	Nombre de cartes réseaux	N° réseau		
Pare_Feu	Serveur 2003	3	12.0.0.1 / 8	172.16.0.1 /16	10.0.0.1 /8
Internet	Serveur 2016	1	IP : Passerelle :		
DMZ	Serveur 2016	1		IP : Passerelle :	
ClientW10	W10 professionnel	1			IP : Passerelle :

La configuration et les tests préalables de la connectivité :

- Configurer la propriété TCP/IP des postes selon le schéma et le tableau ci-dessus.
- Pinguer les postes entre eux.

Optionnel :

- | |
|---|
| c) Activer le service Telnet sur différents postes. |
| d) Disposer un compte avec un mot de passe sur chaque poste |
| e) Puis tester la connexion Telnet sur l'ensemble des postes. |

Premier scénario :

- a. Les postes LAN peut pinguer (ICMP) les postes DMZ.
- b. Les postes LAN peut utiliser Telnet sur les postes DMZ.
- c. Aucun flux initié des postes DMZ vers LAN n'est possible.

1) Sur l'interface 10.0.0.1

- a) On autorise les postes du réseau 10.0.0.0 / 8 d'aller vers le réseau 12.0.0.0 / 8 avec les 2 protocoles suivants :

ICMP type=8, code=0

Telnet port source n'importe lequel, port destination=23

Puis cocher l'option : rejeter tous les paquets à l'exception....

Tester ICMP : **pingue 12.0.0.2** résultat = _____

Tester Telnet : **telnet 12.0.0.2** résultat = _____

- b) On va bloquer tous les flux initiés à partir du réseau 12.0.0.0 vers réseau 10.0.0.0 en maintenant la configuration dans a)

- Avant d'implémenter la règle de blocage, on teste d'abord les flux ICMP et Telnet du réseau 12 vers réseau 10. Résultat : _____

Implémentons maintenant la règle de blocage :

Sur l'interface 12.0.0.2 , en entrée on configure :

Réseau source : 12.0.0.0 /8

Réseau destination : 10.0.0.0 / 8 Protocoles=tous, port = tous

Cocher : recevoir les paquets à l'exception....

Tester ICMP : **pingue 12.0.0.2** résultat = _____

Tester Telnet : **telnet 12.0.0.2** résultat = _____

On bloque les flux venant du réseau 12, ainsi que les flux ICMP et Telnet venant de du réseau 10

Toujours sur l'interface 12.0.0.1

Supprimer la règle existante puis rajouter les deux règles suivantes :

Réseau source 12. réseau destination 10. ICMP code=0, type=0

Réseau source 12. réseau destination 10. telnet protocole=TCP établi port destinataire comme expéditeur=tous

Puis cocher l'option : rejeter tous les paquets à l'exception....