Filtrage d'accès

Préliminaires

TOUJOURS VÉRIFIER QUE VOUS UTILISEZ DU MATÉRIEL EN ÉTAT. Ne jamais supposer que les personnes vous ayant précédé ont fait le ménage !

1. Vérifiez que vos machines ont les interfaces intégrées câblées correctement
2. **Si** vous utilisez le switch vérifiez que sa conf est "vide" (`show run, show vlan`)
3. **Si** vous utilisez le routeur vérifiez que sa conf est "vide"
4. Si vos conf ne sont pas "vide" passez à l'étape nettoyage en fin de TP pour y remédier

1 Objectif

Le but de ce TP est de vous faire concevoir les règles de filtrage nécessaire à la sécurisation d'un site en fonction d'un cahier des charges donné.

2 Rappels

L'architecture matérielle d'un réseau (DMZ, sous-réseaux,...) n'est efficace du point de vue sécurité que si elle est complétée par des mécanismes qui limitent les trafics avec l'Internet et les différents sous-réseaux. Sur les routeurs cela peut être réalisé de différentes façons :

— Par contrôle du routage :
ne pas annoncer (ne pas faire connaître) un sous-réseau au routeur d'accès de l'entreprise permet de rendre inatteignables les machines de ce sous-réseau puisque inconnu des tables de routage nationales et internationales. (remarque : l'installation d'une traduction d'adresses permet avant tout de pallier une pénurie d'adresses publiques IPv4 et n'a pas pour vocation première d'être un élément de sécurité).

— Par filtrage statique sur les adresses IP :
interdire tout le trafic vers ou depuis certaines machines, certains sous-réseaux.

— Par filtrage statique sur les numéros de ports associés à des adresses IP :
autoriser l'utilisation de certaines applications vers ou depuis certaines machines ou sous-réseaux.

— Par filtrage dynamique pour des applications (telle que la téléphonie sur IP) qui utilisent des numéros de ports dynamiques.

2.1 Généralités

Il existe deux politiques de filtrage :

1. "tout ce qui n'est pas interdit est autorisé" :
on filtre ce que l'on ne veut pas et on laisse passer le reste.

2. "tout ce qui n'est pas permis est interdit" :
   on laisse passer certains trafics et on interdit tout le reste.

La première est plutôt adaptée aux routeurs de *backbone*. En effet, ils ne connaissent pas tous les réseaux sources ou destinations des paquets qu'ils voient passer ; ils ne peuvent donc pas faire une description complète des transferts à autoriser et interdire tout le reste. Ils sont contraints à interdire les transferts précisément identifiés par l'administrateur et autoriser tout le reste. L'administrateur réseaux d'une entreprise maîtrise bien l'architecture des différents réseaux qui la composent, il peut mettre en œuvre l'une ou l'autre des politiques de filtrage sur son routeur d'entrée d'entreprise. La seconde est cependant préférable pour les routeurs d'entrée d'entreprise car elle présente une protection plus efficace que la première.

2.2 Les différentes étapes de mise en œuvre d'une ACL

1. Analyser le cahier des charges pour mettre en évidence les besoins de filtrage en fonction de la politique de sécurité.
2. Déterminer les règles et les différents paramètres de filtrage d'accès IP.
3. Coder ces règles puis produire des ACLs (Access Control List).
4. Appliquer ces règles aux interfaces concernées.
5. Vérifier la configuration.
6. Contrôler/tester le fonctionnement.

Vous trouverez en annexe un descriptif des commandes principales.

3 Manipulation

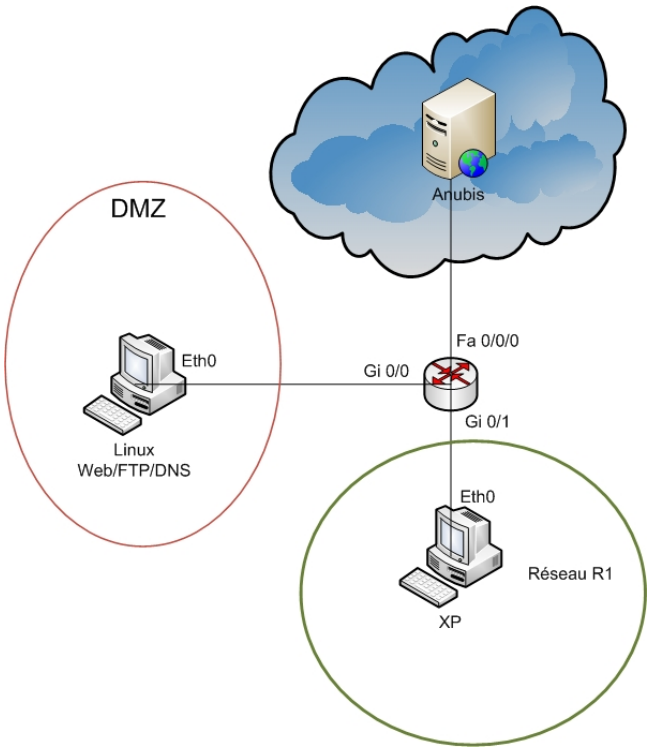
3.1 Installation préalable

Ouvrez un navigateur web sur l'URL suivant : `http://148.60.12.25/TP_filtrage`. Téléchargez tous les fichiers se trouvant dans le répertoire. Donnez les droits d'exécution au fichier `script.sh` puis exécutez le. Suite à cette petite manipulation vous disposez maintenant des fichiers de configuration minimaux pour vos serveurs DNS, FTP et votre proxy.

Attention néanmoins, le fichier de configuration a été modifié de manière très brutale, juste pour avoir un proxy transparent en moins de 3 secondes (pour les besoins du TP) mais sans AUCUN contrôle. Il est bien entendu évident qu'il est hors de question de l'utiliser en environnement réel.

3.2 Le réseau expérimental

Configurez votre poste comme sur le schéma.



Réseau DMZ	11.11.X.0/24
Réseau R1	21.21.X.0/24
PC Linux eth0	11.11.X.1/24
PC XP	21.21.X.1/24
Anubis	30.30.30.30/24
Routeur Gi0/0	11.11.X.254/24
Routeur Gi0/1	21.21.X.254/24
Routeur Fa0/0/0	30.30.30.X/24

3.3 Vérifiez la connectivité entre toutes les machines

Avant de configurer des ACL, on vérifie toujours que le réseau est bien configuré et que tout est accessible (au moins ce qui doit l'être). Dans votre fichier `/etc/hosts` ajoutez une ligne 11.11.X.1 _none_ (attention, ce nom peut changer, il vous est donné par le message d'erreur au démarrage de proftpd). Démarrez votre proxy et vos serveurs Web/DNS/FTP (squid3, bind9, proftpd).

Configurez le Firefox de votre PC windows pour qu'il utilise votre proxy :

dans le menu `Outils/Option/Avancé`, l'onglet `réseau` puis `Paramètres`, cochez `configuration manuelle du proxy` et placez l'adresse de votre proxy ainsi que le port 3128 dans les cases du Proxy HTTP.

Vérifiez que les serveurs Web, DNS et FTP de votre machine et de la machine Anubis sont bien accessibles par tous vos PC. Pour vérifier le FTP actif : commande `ftp`, pour vérifier le FTP passif : firefox. Login/MdP : anonymous/anonymous.

3.4 Cahier des charges

Chaque question vient augmenter le nombre de contraintes du cahier des charges. Les consignes suivantes doivent être respectées scrupuleusement.

Il ne devra jamais apparaître dans vos ACL, une ligne contenant `permit any any`
Vous n'utiliserez que des listes étendues
Si vous positionnez une restriction en IN il doit y avoir le symétrique en OUT

Question 1 *Fermez tous les accès sur les 3 interfaces de votre routeur.*

Nous allons ouvrir petit à petit les accès nécessaires. Vos règles seront les plus complètes et précises possible.

Question 2 *Toutes les machines du réseau R1 ont accès au service DNS de la DMZ. Pour la vérification, votre zone s'appelle :* `mazone.` *et contient au moins la machine* `toto`.

Question 3 *Seules les machines dont l'adresse est comprise entre 21.21.X.1 et 21.21.X.31 ont accès aux serveur FTP de la DMZ. Arrangez-vous pour que cela fonctionne pour le FTP actif et pour le FTP passif. Vous pouvez pour faciliter la configuration decommentez et modifiez (ou pas) la ligne* `passive port`*, du fichier* `/etc/proftpd/proftpd.conf` *sans oubliez de redémarrer le serveur.*

Question 4 *Internet à le droit de venir consulter le serveur web de la DMZ.*

Question 5 *Les serveurs DNS de l'Internet ont le droit de venir interroger le serveur DNS de la DMZ.*

Question 6 *Les machines du réseau R1 utilise un proxy pour aller sur Internet (protocole http et https). Le proxy est dans la DMZ et tourne sur le port 3128. Il relaie ensuite les requête vers internet. Permettez à R1 d'aller sur Internet*

Question 7 *Affinez l'accès de R1 à l'Internet en autorisant l'accès que pendant une plage horaire de 2h. Pour vos tests vous pouvez soit faire varier la plage horaire, soit modifier l'heure du Cisco avec la commande* `clock set`.

4 Annexe

4.1 ACL DIRECTE (ou numérotée)

`access-list acl_number autres_paramètres`
acl_number
<1-99>IP standard access list
<100-199>IP extended access list
<1100-1199>Extended 48-bit MAC address access list
<200-299>Protocol type-code access list
<700-799>48-bit MAC address access list

Plusieurs règles peuvent s'appliquer sur la même ACL (avec le même *acl_number*) dans l'ordre où elles sont écrites
Exemple de syntaxe : access-list 1 deny 172.16.1.0 0.0.0.255
Cette ACL filtre les paquets provenant du réseau 172.16.1.0/24

For ICMP, you can also use the following syntax :
{deny — permit} icmp source source-wildcard destination destination-wildcard [icmp-type [icmp-code] — icmp-message] [precedence precedence] [tos tos] [log — log-input] [time-range time-range-name] [fragments]

For IGMP, you can also use the following syntax :
{deny — permit} igmp source source-wildcard destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [log — log-input] [time-range time-range-name] [fragments]

For TCP, you can also use the following syntax :
{deny — permit} tcp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [established] [precedence precedence] [tos tos] [log — log-input] [time-range time-range-name] [fragments]

For UDP, you can also use the following syntax :
{deny — permit} udp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [precedence precedence] [tos tos] [log — log-input] [time-range time-range-name] [fragments]

`source`
Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source :
— Use a 32-bit quantity in four-part dotted-decimal format.
— Use the any keyword as an abbreviation for a source and source-wildcard of 0.0.0.0 255.255.255.255.
— Use host source as an abbreviation for a source and source-wildcard of source 0.0.0.0.

`source-wildcard`
Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard :
— Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore.
— Use the any keyword as an abbreviation for a source and source-wildcard of 0.0.0.0 255.255.255.255.
— Use host source as an abbreviation for a source and source-wildcard of source 0.0.0.0.

`protocol`
Name or number of an Internet protocol. The protocol argument can be one of the keywords eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, or udp, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the ip keyword.

Note When the icmp, igmp, tcp, and udp keywords are entered, they must be followed with the specific command syntax that is shown for the ICMP, IGMP, TCP, and UDP forms of the deny/permit command.

icmp
Denies only ICMP packets. When you enter the icmp keyword, you must use the specific command syntax shown for the ICMP form of the deny/permit command.

igmp

Denies only IGMP packets. When you enter the igmp keyword, you must use the specific command syntax shown for the IGMP form of the deny/permit command.

tcp
Denies only TCP packets. When you enter the tcp keyword, you must use the specific command syntax shown for the TCP form of the deny/permit command.

udp
Denies only UDP packets. When you enter the udp keyword, you must use the specific command syntax shown for the UDP form of the deny/permit command.

`destination`
Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination :
— Use a 32-bit quantity in four-part dotted-decimal format.
— Use the any keyword as an abbreviation for the destination and destination-wildcard of 0.0.0.0 255.255.255.255.
— Use host destination as an abbreviation for a destination and destination-wildcard of destination 0.0.0.0.

`destination-wildcard`
Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard :
— Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore.
— Use the any keyword as an abbreviation for a destination and destination-wildcard of 0.0.0.0 255.255.255.255.
— Use host destination as an abbreviation for a destination and destination-wildcard of destination 0.0.0.0.

`option option-name`
(Optional) Packets can be filtered by IP Options, as specified by a number from 0 to 255 or by the corresponding IP Option name, as listed in Table 1 in the "Usage Guidelines" section.

`precedence precedence`
(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by a name.

`tos tos`
(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by a name as listed in the "Usage Guidelines" section of the access-list (IP extended) command.

`log`
(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the logging

console command.)

`time-range time-range-name`
(Optional) Name of the time range that applies to this deny statement. The name of the time range and its restrictions are specified by the time-range and absolute or periodic commands, respectively.

`fragments`
(Optional) The access list entry applies to noninitial fragments of packets ; the fragment is either permitted or denied accordingly. For more details about the fragments keyword, see the " Access List Processing of Fragments" and " Fragments and Policy Routing" sections in the "Usage Guidelines" section.

`icmp-type`
(Optional for ICMP packet filtering) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.

`icmp-code`
(Optional for ICMP packet filtering) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.

`icmp-message`
(Optional for ICMP packet filtering) ICMP packets can be filtered by an ICMP message type name or an ICMP message type and code name. The possible names are listed in the "Usage Guidelines" section of the access-list (IP extended) command.

`igmp-type`
(Optional for IGMP packet filtering) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the "Usage Guidelines" section of the access-list (IP extended) command.

`operator`
(Optional) Compares source or destination ports. Operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).

If the operator is positioned after the source and source-wildcard arguments, it must match the source port. If the operator is positioned after the destination and destination-wildcard arguments, it must match the destination port.

The range operator requires two port numbers. Up to ten port numbers can be entered for the eq (equal) and neq (not equal) operators. All other operators require one port number.

`port`
(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the "Usage Guidelines" section of the access-list (IP extended) command.

TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.

`established`
(Optional) For the TCP protocol only : Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bit set. The nonmatching case is that of the initial TCP datagram to form a connection.

Note The established keyword can be used only with the old command-line interface (CLI) format. To use the new CLI format, you must use the match-any or match-all keywords followed by the + or - keywords and flag-name argument.

`{match-any | match-all}`
(Optional) For the TCP protocol only : A match occurs if the TCP datagram has certain TCP flags set or not set. You use the match-any keyword to allow a match to occur if any of the specified TCP flags are present, or you can use the match-all keyword to allow a match to occur only if all of the specified TCP flags are present. You must follow the match-any and match-all keywords with the + or - keyword and the flag-name argument to match on one or more TCP flags.

`{+ | -} flag-name`
(Optional) For the TCP protocol only : The + keyword allows IP packets if their TCP headers contain the TCP flags that are specified by the flag-name argument. The - keyword filters out IP packets that do not contain the TCP flags specified by the flag-name argument. You must follow the + and - keywords with the flag-name argument. TCP flag names can be used only when filtering TCP. Flag names for the TCP flags are as follows : urg, ack, psh, rst, syn, and fin.

Liste de quelques uns des principaux protocoles et ports associés

20	ftp-data		tcp
21	ftp		tcp
22	ssh	Connexion securisée Ã distance	tcp
23	telnet	Connexion en mode terminal	tcp
25	smtp		tcp
53	domain	Serveur DNS	tcp/udp
69	tftp		udp
80	http		tcp
110	Pop3		tcp
443	https	http sécurisé	tcp

Rappel : commande pour placer une ACL sur une interface

`ip access-group {acl_number | acl name} {in | out }`

5 Nettoyage

Pour remettre la salle en état. **Si** vous avez utilisez le routeur :
`Router#copy flash:base-1900.cfg startup-config`
Éteindre le routeur.

Si vous avez utilisé le switch :
`Switch# delete flash:vlan.dat` **si** vous avez fait des vlan
`Switch# erase startup-config`
Éteindre le switch

Recâbler correctement, si nécessaire les câbles gris sur les machines.

Sur le PC XP, repasser l'interface réseau en DHCP et éteindre la machine.
Attention les scripts suivants effacent tout
Sur le PC Linux, lancer le script `/script/init_machine.sh` puis le script `/script/init_reseau.sh`.