

# **Configuration et listes d'accès pour un routeur CISCO**

## ***commandes et exemples***

V2.15  
Modif : 06/03/2001

**Rédacteurs :** *Philippe Leca CNRS/UREC, Philippe Weill CNRS/IPSL, Olivier Porte CNRS/DSI*

**Merci aux relecteurs :** *Joël Marchand*

### **Avertissement :**

Ce document n'est pas un cours ni un ensemble de recommandations mais juste un mémo technique sur quelques commandes et des exemples de configurations pour les routeurs de type CISCO.

Ce n'est qu'un des chaînons pour la mise en place d'une politique de sécurité sur un réseau.

Ces configurations ne doivent en aucun cas être utilisées « tel quel » et doivent impérativement être adaptées et validées sur votre site. Malgré tous nos efforts, Les configurations décrites ici ne sont pas exemptes d'erreurs ou d'omissions.

La diffusion et la reproduction de ce document ne peut se faire que avec l'accord d'un des rédacteurs ou de l'Urec (Unité Réseau du CNRS).

<b>COMMANDES DE CONFIGURATION.....</b>	<b>3</b>
CONNEXION SUR LE ROUTEUR.....	3
IDENTIFICATION.....	3
VISUALISATION ET MODIFICATION DE LA CONFIGURATION :.....	3
SAUVEGARDE DE LA CONFIGURATION DU ROUTEUR SUR UN SERVEUR.....	3
CHARGEMENT DE LA CONFIGURATION À PARTIR D'UN SERVEUR TFTP.....	4
COMMANDES DE TESTS ET DE VISUALISATION DE L'ÉTAT DU ROUTEUR.....	4
TYPES DE COMMANDES DE CONFIGURATION.....	5
COMMANDES DE ROUTAGE.....	5
EXEMPLE DE CONFIGURATION.....	7
EXEMPLE DE CONFIGURATION ROUTEUR 1 PORT ETHERNET/ 1 PORT SÉRIE .....	10
<b>ACCESS LIST : FILTRAGE.....</b>	<b>11</b>
COMMANDES GLOBALES.....	12
Les listes d'accès simples (ou standard).....	12
Les listes d'accès étendues.....	12
MASQUE.....	13
COMMANDES PAR INTERFACES.....	13
VISUALISATION.....	13
MODIFICATION ET/OU SUPPRESSION.....	13
FILTRAGE.....	13
EXEMPLE DE CONFIGURATIONS AVEC ACCESS LIST : « FILTRES PEU SERRÉS ».....	15
EXEMPLE DE CONFIGURATIONS AVEC ACCESS LIST : « FILTRES TRÈS SERRÉS ».....	21
EXEMPLE DE CONFIGURATIONS AVEC ACCESS LIST : « FILTRES TRÈS TRÈS SERRÉS ».....	25
REMARQUES .....	29
D'AUTRES FILTRES .....	31
Limitation de l'accès à mon routeur avec telnet : .....	31
Filtres en sortie .....	31
Filtres sur ICMP.....	32
<b>SURVEILLANCE ET ADMINISTRATION.....</b>	<b>35</b>
SNMP ET MRTG.....	35
ANALYSE DES LOGS.....	36
<b>RÉFÉRENCES.....</b>	<b>37</b>

## Commandes de configuration

### Connexion sur le routeur

La première fois via une console connectée sur le port console. Au démarrage, on rentre dans le setup permettant de rentrer les paramètres de bases et les adresses IP des différentes interfaces si la mémoire non volatile est vide.

Les fois suivantes, on se connecte au routeur en utilisant telnet @ip-interfaces.

### Identification

2 modes d'identification.

Mode utilisateur (user) : le mot de passe est demandé lors de la connexion via telnet ou à la console

Mode administrateur (privileged ou enable

>enable

>mot de passe

### Visualisation et modification de la configuration :

>conf term      *pour entrer dans l'éditeur de configuration et la modifier.*

>CTR+Z          *pour sortir de l'éditeur.*

>write terminal      *pour visualiser la configuration en mémoire non volatile*

>write memory      *pour sauvegarder la nouvelle configuration en mémoire non volatile*

>write erase      *effacer la configuration*

>exit              *fin de la session*

> ?                *liste des commandes disponibles. Attention elle est différente suivant le mode d'identification.*

>reload          *réinitialisation du routeur (reboot)*

>show running-config      *pour visualiser la configuration en cours*

Toutes les commandes peuvent être rentrées sous forme complète ou sous forme abrégée :

Write memory          ⇔      wr mem

Int eth1                ⇔      interface ethernet 1

### Sauvegarde de la configuration du routeur sur un serveur.

On peut sauvegarder la configuration du routeur sur un serveur du réseau via TFTP.

Il faut d'abord mettre en place un serveur TFTP correctement. On suppose que /tftpboot est le répertoire de chargement du serveur tftp.

Créer une enveloppe vide sur le serveur TFTP : cp /dev/null /tftpboot/nom\_cisco.conf

Passer en mode "enable" sur le Cisco

> write net

Remote host [x.y.z.u]?

```
Name of configuration file to write [nom_cisco.conf]?  
Write file nom_cisco.conf on host x.y.z.u? [confirm]  
#####  
Writing b11i1-config !! [OK]  
>quit
```

La configuration est sauvegardée dans /tftpboot/nom\_cisco.conf  
x.y.z.u correspond à l'adresse IP du serveur TFTP de votre réseau.

Si ça ne fonctionne pas pensez à vérifier les droits du fichier /tftpboot/nom\_cisco.conf.

## **Chargement de la configuration à partir d'un serveur TFTP**

De même on peut charger la configuration via un serveur TFTP. Cette méthode présente l'avantage de pouvoir écrire tranquillement sa configuration via un éditeur de texte et la charger quand on veut.

Sur le serveur TFTP, changer provisoirement les droits du fichier de configuration :

```
#chmod 444 /tftpboot/nom_cisco.conf  
Il faut ensuite se connecter sur le routeur en mode enable.
```

```
>configure network  
Host or network configuration file [host]?  
Address of remote host [x.y.z.u]?  
Name of configuration file [nom_cisco.conf]?  
Configure using nom_cisco.conf from x.y.z.u? [confirm]  
Loading nom_cisco.conf from x.y.z.u (via Ethernet1):  
[OK - 3389/32444 bytes]  
>write memory  
>quit
```

```
Restaurer enfin les droits du fichier nom_cisco.conf  
#chmod 222 /tftpboot/nom_cisco.conf
```

## **Commandes de tests et de visualisation de l'état du routeur**

```
>show int      visualiser l'état des interfaces  
  
>sh ip route   visualiser les routes IP  
  
>sh ip arp  
>sh ip protocols  
  
>ping @IP  
  
>sh ip traffic compte les trames à destination du routeur (et non toutes celles qui passent).  
  
>show ip accounting access-violations      interrogation des logs des ACL  
  
>clear ip accounting  
  
>sh version  
>sh controllers  
>sh mem  
>sh process    pour surveiller la charge du routeur
```

>sh proc mem	<i>visualisation de la mémoire utilisée et disponible</i>
>sh flash	<i>visualisation de la mémoire flash utilisée et disponible</i>

## **Types de commandes de configuration**

### **Commandes globales**

Elles s'adressent à la totalité du routeur  
>hostname toto

### **Commandes par interfaces (sous-commandes)**

Elles s'adressent à une partie du routeur.  
>int type N° *dans l'éditeur de configuration, pour spécifier quelle interface va être configurée.*  
>int eth 1 *configuration de l'interface ethernet 1*  
>ip address x.y.z.y 255.255.255.0 *déclaration de l'adresse IP de l'interface ethernet 1*  
>int serial 1 *configuration de l'interface série 1*

## **Commandes de routage**

### **Routage statique :**

>ip route network mask address/interface (distance)  
*définition d'une route statique :*  
*network : réseau à atteindre*  
*distance : utile que pour modifier les priorités standards*  
*(statique 1, igrp 100, ospf 110, rip 120, egp 140)*

### **Routage dynamique : RIP**

>router rip  
>network network-number  
*mise en place du protocole rip avec diffusion et écoute du réseau network-number (il doit être directement connecté au routeur).*

### **Routage dynamique : IGRP**

>router igrp  
>network network-number

### **Routage dynamique : EGP**

>router egp remote-as  
>neighbor @IP

### **Routage dynamique : BGP**

>autonomous-system numéro-AS  
>router bgp 65535  
>neighbor @IP-voisin remote-as numéro-AS-voisin  
>neighbor @IP-voisin description Routage avec FT  
>neighbor @IP-voisin version 4  
>neighbor @IP-voisin soft-reconfiguration inbound  
>no auto-summary

### **Blocage de la diffusion du routage dynamique sur une interface :**

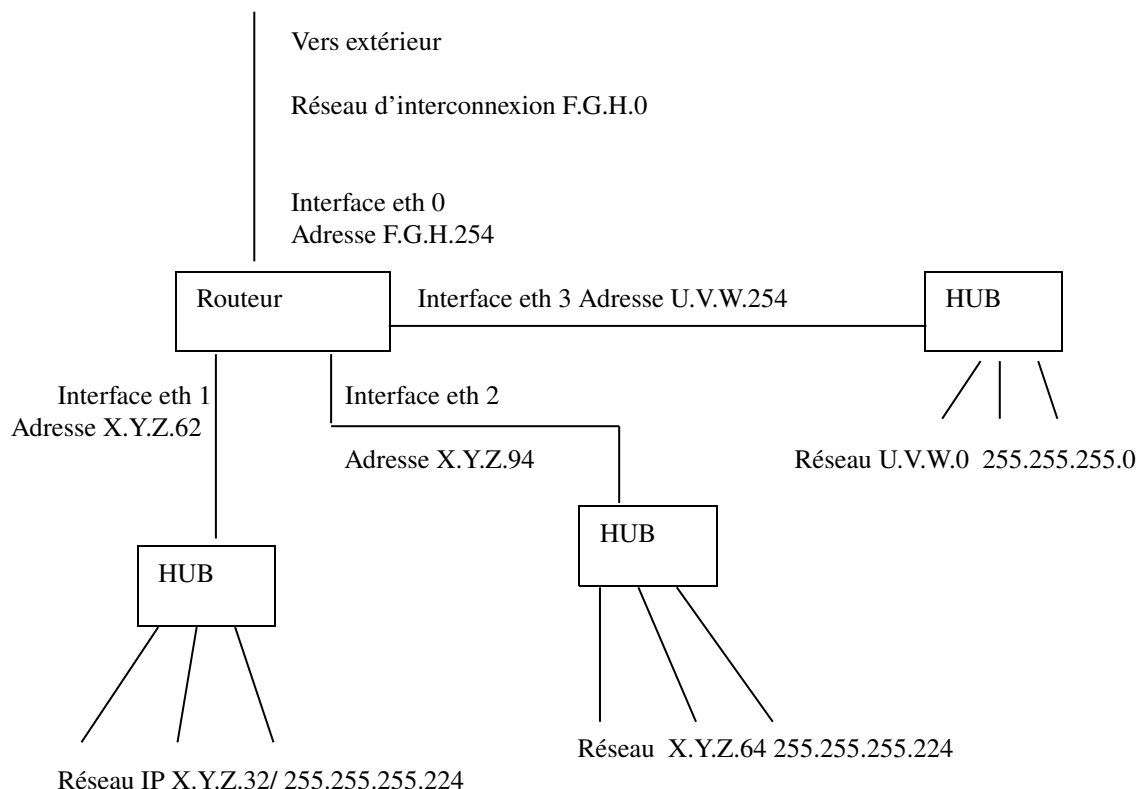
>passive-interface <nom-interface>  
*interdire la diffusion des annonces d'un protocol de routage sur une interface.*

**Route par défaut**

```
>ip route 0.0.0.0 0.0.0.0 @sortie
```

*route par défaut. Attention dans le cas de réseau avec subnet. Il faut rajouter en route par défaut, la route vers le réseau complet (cf. exemple )*

## Exemple de configuration



Le caractère ! indique un commentaire,

*! les commandes globales*

**no service config**

*! par défaut, émission de requêtes TFTP à l'adresse de broadcast pour vérifier que la configuration n'a pas été modifiée. La commande permet d'arrêter ces envois.*

**no service tcp-small-servers**

**no service udp-small-servers**

*! Le routeur implémente les services echo (ports TCP et UDP numéro 7), discard (ports TCP et UDP numéro 9), chargen (ports TCP et UDP numéro 19). Ces 2 commandes permettent de les dévalider.*

**no ip source-route**

*! le routeur ne doit pas router de paquets IP comportant l'option "Source routing". L'option "Source routing" permet à l'émetteur d'un paquet IP de spécifier le chemin que doit prendre le paquet pour accéder à sa destination, indépendamment des tables de routages des routeurs traversés. Le destinataire devra utiliser le chemin inverse pour le retour ( option -g de traceroute )*

**logging X.Y.Z.1**

*! le serveur de log est la machine X.Y.Z.1*

**logging facility auth**

*! permet d'utiliser le mécanisme de syslog pour journaliser sur un serveur externe les événements importants recensés ( arrêts, modifications de config, trace de tous les paquets ayant satisfait un élément marqué "log" dans une ACL ) sur le routeur.*

*! commandes spécifiques à une interface :*

*! on met interface ethernet 1 ou interface eth 1*

**interface ethernet 1**

**ip address X.Y.Z.62 255.255.255.224**

```

! déclaration de l'adresse IP de l'interface 1
no ip redirects
! rejets des paquets icmp redirect ( évite modification de la politique de routage ).

int eth 2
ip address X.Y.Z.94 255.255.255.224
! déclaration de l'adresse IP de l'interface 2
no ip redirects

int eth 3
ip address U.V.W.254 255.255.255.0
no ip redirects

int eth 0
ip address F.G.H.254 255.255.255.0
no ip redirects
!-----
! pour le routage 2 possibilités :
! Routage statique : suffisant si derrière ces réseaux
! il n'y a pas d'autres routeurs, ou si les modifications d'infrastructures
! sont rares
!ou
! Routage dynamique
!
!Il faut choisir l'une des deux méthodes.
!
!-----
!configuration en cas de routage statique
!-----
!
ip route F.G.H.0 255.255.255.0 eth0
ip route U.V.W.0 255.255.255.0 eth3
ip route X.Y.Z.64 255.255.255.224 X.Y.Z.94
! au choix on met le nom de l'interface ou l'@IP
ip route X.Y.Z.32 255.255.255.224 eth1

ip route X.Y.Z.0 255.255.255.0 eth0
! a rajouter obligatoirement. Le routeur considère qu'il connaît toute la classe C X.Y.Z. 0 à cause des
! routes vers eth1 et eth2. Il faut spécifier une route pour le reste des subnet.
ip route 0.0.0.0 0.0.0.0 eth0
! route par défaut
!-----
!configuration en cas de routage dynamique avec le protocole RIP-
!-----
router rip
! mise en œuvre du routage dynamique RIP, puis déclaration des réseaux
network X.Y.Z.0
network F.G.H.0
network U.V.W.0
passive-interface ethernet1
passive-interface ethernet2
passive-interface ethernet3
! la commande passive-interface permet de ne pas redistribuer
! les annonces RIP vers les interfaces indiquées.
ip route 0.0.0.0 0.0.0.0 eth0
! route par défaut. A indiquer uniquement si elle n'est pas propagée via RIP

```



```
!-----  
! fin de configuration du routage  
!-----  
no ip classless  
    ! permet d'utiliser des masques de réseaux variables
```

### Exemple de configuration routeur 1 port ethernet/ 1 port série

```
!  
version 11.2  
no service udp-small-servers  
no service tcp-small-servers  
!  
hostname HECTOR  
!  
enable secret 5 $1$h38O$2EDwI4.4VhiOA21Ayw9gs.  
enable password cisco  
!  
ip subnet-zero  
ip domain-name foo.bar.com  
ip name-server x.y.z.1  
!  
interface Ethernet0  
  ip address x.y.z.4 255.255.255.0  
!  
interface Serial0  
  ip unnumbered Ethernet0  
!  
router rip  
  redistribute static  
  network x.y.z.0  
!  
no ip classless  
ip route      0.0.0.0      0.0.0.0      x.y.z.1  
ip route      a.b.c.0      255.255.255.192      Serial0  
!  
line con 0  
line vty 0 4  
  password cisco  
  login  
!  
end
```

## Access List : filtrage

Les ACL ( Access Lists ) sont des règles appliquées à chaque paquet IP transitant à travers le routeur avec comme paramètres :

- l'adresse IP de l'émetteur du paquet
- l'adresse IP du destinataire du paquet
- le type du paquet : tcp, udp, icmp, ip.
- le port de destination du paquet ( si le type est TCP ou UDP )

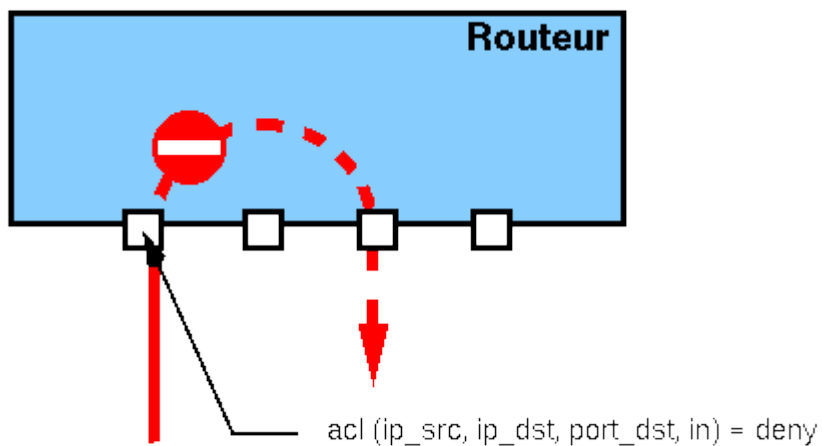
Pour un paquet donné, l'ACL rend deux valeurs

- deny : le paquet est rejeté
- permit : le paquet peut transiter par le routeur

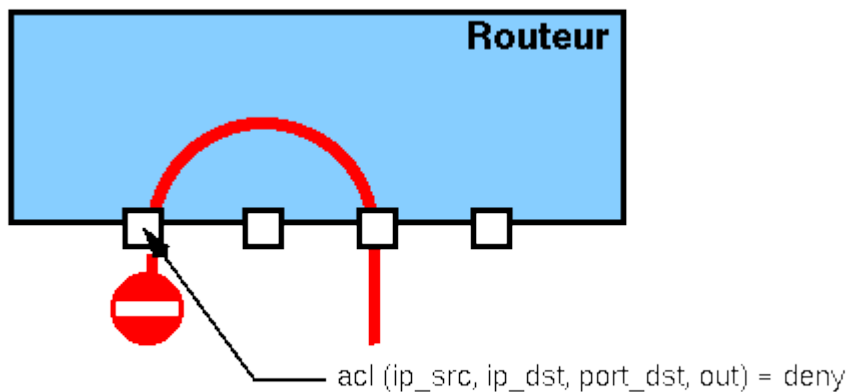
On associe à chaque interface du routeur une ACL. On peut aussi préciser le sens du trafic, c'est à dire in ou out, pour que selon l'ACL s'applique aux paquets entrant dans l'interface du routeur ou bien aux paquets sortant de l'interface du routeur.

Les versions antérieures à la version 10 ne disposent que de "out".

### IN



### OUT



( Merci à Roland Dirlewanger a qui j'ai piqué les dessins : <http://www.dr15.cnrs.fr/Cours/ACL-Cisco/> )

Les règles sont parcourues séquentiellement et le **test s'arrête lorsque le paquet testé vérifie une règle.**  
En général, on essaye de mettre les règles les plus utilisées en début de liste.

**Si aucune règle n'est vérifiée, le résultat est négatif (deny) :** tout ce qui n'est pas autorisé est interdit.

## **Commandes globales**

Il existe deux types de listes d'accès :

### **Les listes d'accès simples (ou standard).**

```
>access-list no_acl permit|deny ip_src m_src
avec
no_acl : les numéros d'ACL sont compris entre 0 et 99
ip_src : adresse IP source
m_src : masque associé à ip_src. Inverse du masque de l'adresse IP. Ils permettent de décrire un
ensemble d'adresses. Attention: ces masques sont totalement indépendants des masques de sous-
réseaux.
```

Exemple

```
>access-list 27 permit 134.4.253.26 0.0.0.0
```

```
>int eth 0
```

```
>ip access-group 27 in
```

Seule l'adresse IP 134.4.253.26 est autorisée à entrer sur le réseau connecté à eth 0

### **Les listes d'accès étendues.**

```
>access-list no_acl [permit|deny] [tcp|udp|icmp|ip] ip_src m_src ip_dest
m_dst [expr] [log]
```

avec :

no\_acl : les numéros d'ACL sont compris entre 100 et 199

On spécifie le type de paquet (TCP, UDP, ICMP). Le type IP est la réunion des trois autres.

m\_src et m\_dst sont des masques associés respectivement à ip\_src ou ip\_dest. Ils permettent de décrire un ensemble d'adresses. Attention: ces masques sont totalement indépendants des masques de sous-réseaux qui peuvent être associés à ip\_src ou ip\_dst.

A partir de la version 11, certains raccourcis ont été introduits dans la syntaxe, notamment les mots-clés "host" et "any".

expr : {lt|gt|eq|ne} num-port (pour tcp et udp, rien si ip ou icmp). Depuis la version 11 on peut indiquer le numéro de port ou le nom du service (smtp ou 25 par exemple) :

Operand	Alias	Parameters	Result
<	lt	port#	true if port is less than given value
>	gt	port#	true if port is greater than given value
=	eq	port#	true if port is equal to than given value
!=	ne	port#	true if port is not equal to than given value
<=	le	port#	true if port is less than or equal to given value
=>	ge	port#	true if port is greater than or equal to given value

log : depuis la version 11, permet d'envoyer au syslog un signal en cas de deny.

**A partir de la version 11, deux raccourcis de notations ont été introduits :**

**host adresse\_ip**

pour désigner une adresse IP. Par exemple,

"host 194.15.100.1" et "194.15.100.1 0.0.0.0" désignent la même adresse IP, "194.15.100.1".

**any**

pour désigner n'importe quelle adresse IP. Cette notation est équivalente à

"0.0.0.0 255.255.255.255".

## **Masque**

Si bit à analyser : bit à 0 dans le masque

Si bit à ignorer : bit à 1 dans le masque

Pour vérifier si une adresse IP appartient à une famille :

prendre l'adresse IP

appliquer le masque, c'est-à-dire mettre à 0 dans l'adresse IP tous les bits qui sont à 1 dans le masque.

comparer le résultat obtenu à l'adresse générique de la famille.

Exemples d'adresses génériques et de masques :

194.15.100.0 0.0.0.255	Toutes les adresses IP du réseau 194.15.100.0
194.15.100.1 0.0.0.0	L'adresse IP 194.15.100.1
0.0.0.0 255.255.255.255	Toute adresse IP.
194.15.100.0 0.0.0.63	Toutes les adresses IP comprises entre 194.15.100.0 et 194.15.100.63
194.15.100.192 0.0.0.63	Toutes les adresses IP comprises entre 192.9.200.192 et 194.15.100.255
134.4.0.254 0.0.255.0	Toutes les adresses IP de la forme 134.4.x.254.

## **Commandes par interfaces**

>interface type n°

>ip access-group no\_acl {in | out }

*On applique l'access list no\_acl en entrée ou en sortie de l'interface type n°*

## **Visualisation**

>sh access-lists

>sh access-lists num-acl

## **Modification et/ou suppression**

Pour supprimer une liste :

>no access-list no\_acl

Pour modifier une liste, il faut d'abord la supprimer puis la réécrire. D'où l'intérêt de sauvegarder et charger la configuration via un serveur tftp pour modifier le fichier texte.

## **Filtrage**

Tous les cas ci dessous sont bien sûr à adapter en fonction des architectures réseaux et des particularités du site.

Ce sont des cas avec une architecture réseau très simple. La mise en place de filtres « en réel » demande une bonne connaissance de son réseau et de ses services et une concertation avec les utilisateurs.

A chaque fois on applique les filtres sur deux types d'interface :

**- sur l'interface du campus (ACL 101 dans les exemples) :** en général on y met des filtres pas trop contraignants pour laisser ensuite à chaque entité sa politique de filtrages. Il faut au moins filtrer en entrée :

- les adresses sources avec une adresse de son réseau (anti-spoofing),
- les adresses privées,
- ICMP sur des adresses de réseaux ou de broadcast,
- les ports UDP reconnus comme dangereux

**- sur l'interface du laboratoire (ACL 102 dans les exemples) :** en fonction des politiques retenues le filtrage sera très différent ( cf exemples). Mais inutile de refiltrer ici des paquets déjà filtrés sur l'entrée du campus. C'est sur cette interface qu'on appliquera une politique du style :

- j'autorise spécifiquement l'accès à mes services
- je bloque le reste des services de mon réseaux.

Ou :

- J'autorise certains services sur mes serveurs réseaux ( www, ftp, messagerie, ...)
- Je bloque l'accès sur mes serveurs pour les autres services
- J'autorise le reste sur mon réseau

Avec éventuellement la gestion d'exceptions :

- Je bloque l'accès depuis un réseau dangereux
- J'autorise l'accès complet depuis un réseau amis
- Etc etc...

Dans le cas d'une architecture simple ou lorsque la politique de sécurité est commune à tous le campus ou laboratoire, on peut réunir les deux filtres dans un seul.

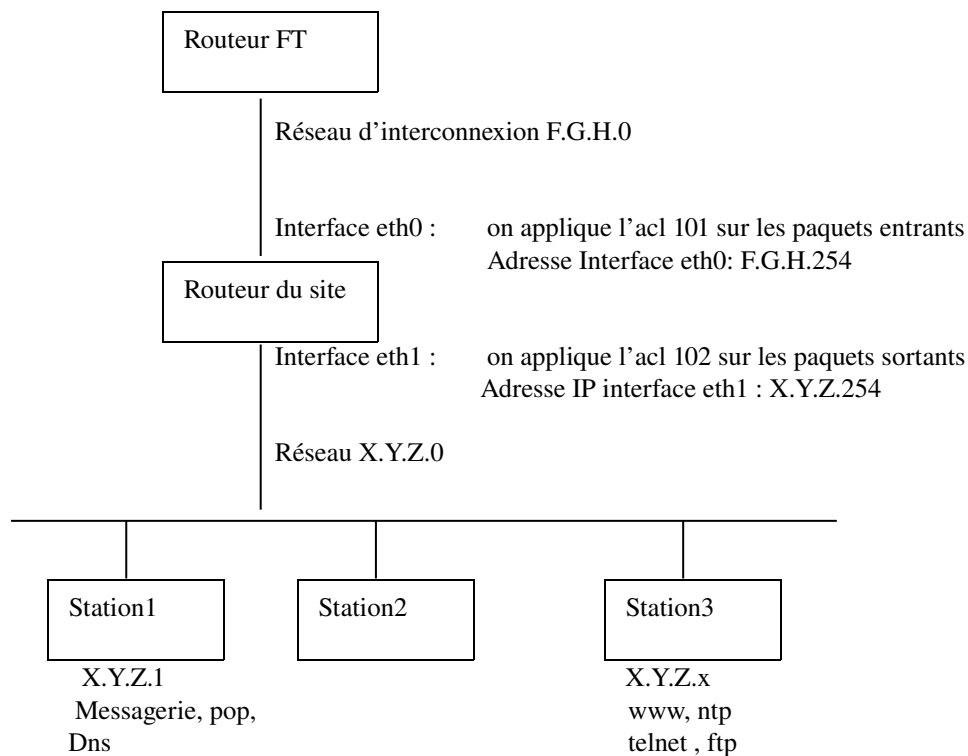
La mise en place de filtres sur les paquets entrant de mon réseau n'est pas transparente pour les utilisateurs. Cela va avoir des incidences sur les services qui seront accessibles de l'intérieur vers l'extérieur ( cf le paragraphe « Remarques » après les exemples).

## Exemple de configurations avec access list : « filtres peu serrés »

**Politique:** "tout ce qui n'est pas explicitement interdit est autorisé"

→ on interdit d'abord explicitement

→ puis tout le reste on laisse passer



*! access-list de contrôle de ce qui rentre sur le réseau d'établissement ( acl 101 )*

*! marche sur les versions CISCO postérieures à 11.xx ( à cause de host et deny et log )*

*! Cette ACL est appliquée en entrée du campus.*

*! Politique :*

*! les adresses sources avec une adresse de son réseau (mascarade d'adresse IP),*

*! les adresses privées,*

*! ICMP sur des adresses de réseaux ou de broadcast,*

*! les ports UDP reconnus comme dangereux*

*J'autorise des utilisateurs externes suivant leurs catégories :*

*! ENNEMIS Rien n'est autorisé*

*!-----*

*! déclaration de l'acl 101*

*!-----*

*!*

*! Je vide les access-list courantes*

*!*

*no access-list 101*

*!*

*! Interdire le <<source routing>>*

*!*

*no ip source-route*

*!*

```

! Eviter la mascarade d'adresse IP : mon adresse de réseau ne doit pas entrer.
!
access-list 101 deny ip X.Y.Z.0 0.0.0.255 any
!
! Interdiction de ICMP (ping) sur l'adresse broadcast et l'adresse de réseau
! attention si le réseau est subnetté, pensez aux adresses de sous réseaux et aux adresses
! de broadcast des sous réseaux.
! ou mettre " no ip directed-broadcast" sur chaque interface
access-list 101 deny icmp any host X.Y.Z.255 log
access-list 101 deny icmp any host X.Y.Z.0 log
!
! J'autorise ICMP sur toutes mes machines
access-list 101 permit icmp any X.Y.Z.0 0.0.0.255
!
! Si on fait du multicast décommenter le permit
! si non décommenter le deny
!
! access-list 101 deny ip 224.0.0.0 15.255.255.255 any log
! access-list 101 permit ip 224.0.0.0 15.255.255.255 any log
!
!
! Virez les ENNEMIS tout de suite et pour tout ( Si vous en avez :- )
! Interdiction du réseau T.U.V.0/24
access-list 101 deny ip T.U.V.0 0.0.0.255 any log
!
! Éviter des attaques douteuses.
!
! From CIAC
! ne pas laisser entrer les réseaux suivants
! 0.0.0.0/8 - Historical Broadcast
! 10.0.0.0/8 - RFC 1918 Private Network
! 127.0.0.0/8 - Loopback
! 169.254.0.0/16 - Link Local Networks
! 172.16.0.0/12 - RFC 1918 Private Network
! 192.0.2.0/24 - TEST-NET
! 192.168.0.0/16 - RFC 1918 Private Network
! 240.0.0.0/5 - Class E Reserved
! 248.0.0.0/5 - Unallocated
! 255.255.255.255/32 - Broadcast
! 224.0.0.0/4 - Class D Multicast
! ( SAUF si on fait du Multicast - Attention Rip V2 )
!
access-list 101 deny ip 0.0.0.0 0.255.255.255 any log
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 169.254.0.0 0.0.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.0.2.0 0.0.0.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 240.0.0.0 7.255.255.255 any log
access-list 101 deny ip 248.0.0.0 7.255.255.255 any log
access-list 101 deny ip 255.255.255.255 0.0.0.0 any log
!
! je filtre tous les ports connus comme dangereux ( enfin connus à un instant t )
!
! filtres certains ports UDP supérieurs à 1023 et dangereux :
! IRC (6665-6670, 7000),
! Back orifice (31337), Netbus (12345,12346)

```



```

! Mstream(6723, 12754 15104,TCP), Mstream zombies(6838 7983 9325 10498,UDP))
access-list 101 deny udp any any eq 6665 log
access-list 101 deny udp any any eq 6666 log
access-list 101 deny udp any any eq 6667 log
access-list 101 deny udp any any eq 6668 log
access-list 101 deny udp any any eq 6669 log
access-list 101 deny udp any any eq 6670 log
access-list 101 deny udp any any eq 7000 log
access-list 101 deny udp any any eq 1604 log
access-list 101 deny udp any any eq 31337 log
access-list 101 deny tcp any any eq 31337 log
access-list 101 deny udp any any eq 12345 log
access-list 101 deny udp any any eq 12346 log
access-list 101 deny tcp any any eq 6723 log
access-list 101 deny udp any any eq 6838 log
access-list 101 deny udp any any eq 7983 log
access-list 101 deny udp any any eq 9325 log
access-list 101 deny udp any any eq 10498 log
access-list 101 deny tcp any any eq 12754 log
access-list 101 deny tcp any any eq 15104 log
!
! filtres pour les denis de services syn00 et attaque ddos
!
access-list 101 deny udp any any eq 65000 log
access-list 101 deny tcp any any eq 65000 log
access-list 101 deny udp any any eq 16660 log
access-list 101 deny tcp any any eq 16660 log
access-list 101 deny udp any any eq 60001 log
access-list 101 deny tcp any any eq 60001 log
access-list 101 deny udp any any eq 27444 log
access-list 101 deny udp any any eq 34555 log
access-list 101 deny tcp any any eq 1524 log
access-list 101 deny tcp any any eq 27665 log
access-list 101 deny udp any any eq 27665 log
access-list 101 deny udp any any eq 31335 log
!
! filtres certains services venant de l'ext
! bootp (67 UDP), , tftpd(69,UDP), syslog(514,UDP), sunrpc(111,TCP/UDP), snmp(161,UDP)
! xdmcp(177,UDP), login(513,TCP), shell(514,TCP), RDP (3389), Netbios (1001,1002),
! imap (143 TCP – attention vous pouvez en avoir besoin...), ipx(213,UDP/TCP), wins(1512,UDP/TCP)
! microsoft (135->139), 6000->6002 X, 161,162 SNMP
! 194 irc, 111 portmap, 511->515 r-commande et lpr, nfs
! 2000->2003 openwin, 79 finger
! 512 → 515, r-command et lpd
access-list 101 deny udp any any eq bootps log
access-list 101 deny udp any any eq tftp log
access-list 101 deny tcp any any eq 87 log
access-list 101 deny tcp any any eq 95 log
access-list 101 deny udp any any eq 111 log
access-list 101 deny tcp any any eq 111 log
access-list 101 deny udp any any eq 135 log
access-list 101 deny tcp any any eq 135 log
access-list 101 deny udp any any eq 136 log
access-list 101 deny tcp any any eq 136 log
access-list 101 deny udp any any eq 137 log
access-list 101 deny tcp any any eq 137 log
access-list 101 deny udp any any eq 138 log

```

```

access-list 101 deny tcp any any eq 138 log
access-list 101 deny udp any any eq 139 log
access-list 101 deny tcp any any eq 139 log
access-list 101 deny udp any any eq 143 log
access-list 101 deny tcp any any eq 143 log
access-list 101 deny tcp any any eq 144 log
access-list 101 deny tcp any any range 161 162 log
access-list 101 deny udp any any range 161 162 log
access-list 101 deny udp any any eq 177 log
access-list 101 deny udp any any eq 194 log
access-list 101 deny tcp any any eq 194 log
access-list 101 deny tcp any any eq 213 log
access-list 101 deny udp any any eq 213 log
access-list 101 deny tcp any any eq exec log
access-list 101 deny udp any any eq biff log
access-list 101 deny udp any any eq who log
access-list 101 deny udp any any eq syslog log
access-list 101 deny tcp any any eq 512 log
access-list 101 deny tcp any any eq 513 log
access-list 101 deny tcp any any eq 514 log
access-list 101 deny udp any any eq 514 log
access-list 101 deny tcp any any eq 515 log
access-list 101 deny udp any any eq 1001 log
access-list 101 deny udp any any eq 1002 log
access-list 101 deny udp any any eq 1494 log
access-list 101 deny tcp any any eq 1494 log
access-list 101 deny udp any any eq 1604 log
access-list 101 deny tcp any any eq 1604 log
access-list 101 deny udp any any eq 1512 log
access-list 101 deny tcp any any eq 1512 log
access-list 101 deny udp any any eq 2000 log
access-list 101 deny udp any any eq 2001 log
access-list 101 deny udp any any eq 2002 log
access-list 101 deny udp any any eq 2003 log
access-list 101 deny udp any any eq 2049 log
access-list 101 deny tcp any any eq 2049 log
access-list 101 deny udp any any eq 3389 log
access-list 101 deny udp any any eq 6000 log
access-list 101 deny udp any any eq 6001 log
access-list 101 deny tcp any any eq 6000 log
access-list 101 deny tcp any any eq 6001 log
!
! ...et autoriser tout le reste.
access-list 101 permit ip any any
!
!
!Fin de déclaration de l'acl 101
!-----
! Déclaration de l'acl 102
!-----
!
Les filtres :
!      seuls les services usuels (telnet, mail, ftp, www, dns) sont
!      accessibles sur mes serveurs et pas d'autres services.
!      J'interdis un réseau « peu sur » sauf pour m'envoyer des mails
!      tout le reste est autorisé ( je surveille mes serveurs réseaux et pas le reste)
!

```

```

! Je vide les access-list courantes
no access-list 102
!
! Interdire les connexions entrantes de Sites particuliers (par exemple le réseau A.B.C.0)
! Mais autoriser leur mail ( 25 ) et DNS ( 53 )
!
access-list 102 permit tcp A.B.C.0 0.0.0.255 any eq 25
access-list 102 permit tcp A.B.C.0 0.0.0.255 any eq 53
access-list 102 deny tcp A.B.C.0 0.0.0.255 any
access-list 102 deny udp A.B.C.0 0.0.0.255 any
!
!
! Protéger nos machines très sensibles : pas d'IP avec l'extérieur
! X.Y.Z.SENSIBLE et X.Y.Z.SYSLOG (même pas en sortie)
access-list 102 deny ip any host X.Y.Z.SENSIBLE log
access-list 102 deny ip any host X.Y.Z.SYSLOG log
!
! Accepter les VRAIS AMIS pour tout ??
! ( est ce bien eux ou sont t'ils spoofés - Peut être trop dangereux )
! autorisation du réseau E.F.G.0/24 pour tout
access-list 102 permit ip E.F.G.0 0.0.0.255 any log
!
! on veut protéger ses serveurs réseaux (et uniquement eux)
!
! Filtres sur le serveur de messagerie, dns et pop : X.Y.Z.1 :
!
! Autorise le port 113 (RFC 931) sur mon serveur
access-list 102 permit tcp any host X.Y.Z.1 eq 113
!
! Accès au DNS
access-list 102 permit udp any host X.Y.Z.1 eq domain
access-list 102 permit tcp any host X.Y.Z.1 eq domain
!
! accès smtp ( messagerie )
access-list 102 permit tcp any host X.Y.Z.1 eq smtp
!
! accès pop
access-list 102 permit tcp any host X.Y.Z.1 eq 110
!
! on bloque le reste sur ce serveur et on log pour voir les tentatives d'accès
access-list 102 deny ip any host X.Y.Z.1 log
!
! Filtres sur le serveur www, telnet, ftp et ntp : X.Y.Z.2
! NTP
access-list 102 permit udp any host X.Y.Z.2 eq ntp
!telnet
access-list 102 permit udp any host X.Y.Z.2 eq telnet
! FTP connexion de contrôle et de données
access-list 102 permit tcp any host X.Y.Z.2 eq ftp
access-list 102 permit tcp any host X.Y.Z.2 eq ftp-data
! WWW
access-list 102 permit tcp any host X.Y.Z.2 eq www
! on bloque le reste sur ce serveur et on logue
access-list 102 deny ip any host X.Y.Z.2 log
!
! ...et autoriser tout le reste.
access-list 102 permit ip any any
!

```

*!fin de déclaration de l'acl 102*

*! Déclaration au niveau de l'interface eth0*

*!*

interface Ethernet0

ip address F.G.H.254 255.255.255.0

*! l'ACL numéro 101 s'applique pour les paquets qui entrent dans le routeur par l'interface Ethernet 0*

ip access-group 101 in

*! Le routeur doit conserver une trace de tous les paquets rejetés pour cause de violation d'une ACL*

*! associée à cette interface.*

*! Le routeur conserve dans une table :*

*! l'adresse IP de l'émetteur du paquet*

*! l'adresse IP du destinataire du paquet*

*! le nombre de tentatives*

*! la taille cumulée des paquets rejetés*

ip accounting access-violations

no ip proxy-arp

*! rejets broadcast icmp*

no ip directed-broadcast

*! Rejets des paquets icmp redirect ( évite modification de la politique de routage).*

no ip redirects

interface Ethernet1

*!description - Connexion réseau local -*

ip address X.Y.Z.254 255.255.255.0

*! l'ACL numéro 102 s'applique pour les paquets qui sortiront vers mon réseau par l'interface Ethernet 1*

ip access-group 102 out

ip accounting access-violations

no ip proxy-arp

*!filtres broadcast icmp*

no ip directed-broadcast

no ip redirects

**Remarque :**

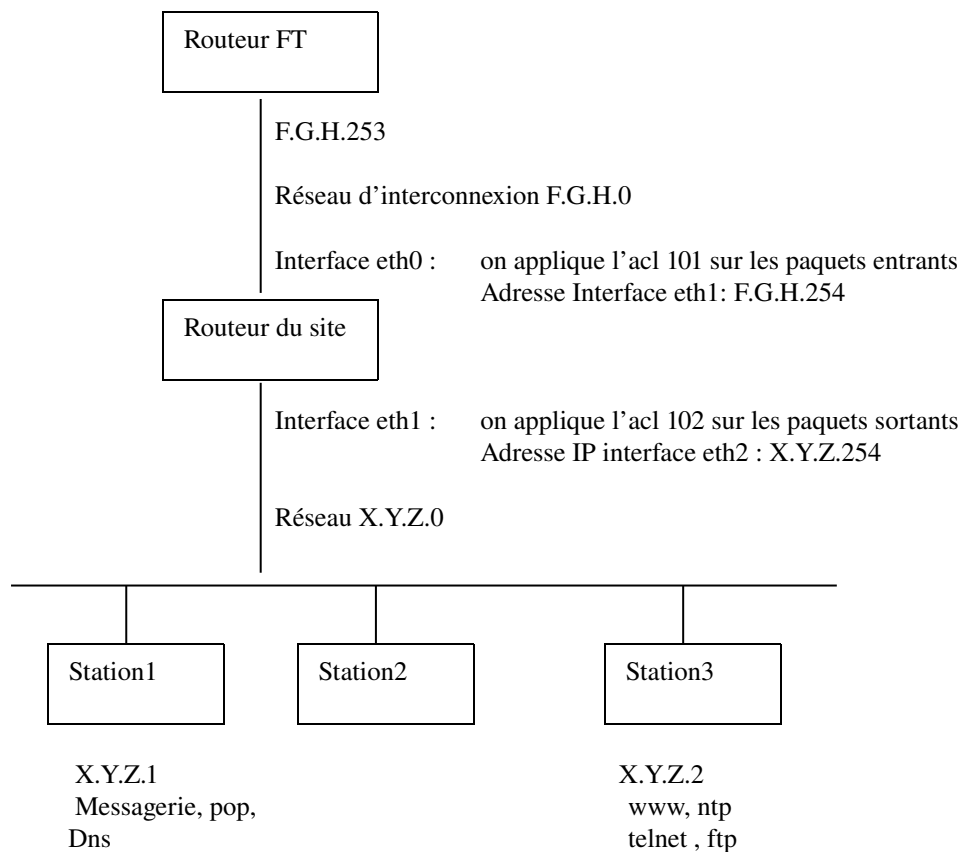
Contrairement aux deux exemples suivants, cette politique ne modifie pas les services disponibles pour les utilisateurs.

## Exemple de configurations avec access list : « filtres très serrés »

**Politique:** "tout ce qui n'est pas explicitement autorisé est interdit"

- on interdit d'abord explicitement
- on autorise ce qu'on veut
- puis on bloque ce qui reste.

**Note :** l'ACL 101 n'est pas remise ici mais c'est la même que dans l'exemple « filtres peu serrés ».



*! access-list de contrôle de ce qui rentre sur le réseau d'établissement ( acl 101 )*

*! et de ce qui rentre dans mon réseau (acl102)*

*! Marche sur les versions CISCO postérieures à 10.xx*

*!-----*

*! Déclaration de l'acl 101*

*!-----*

*!*

**Voir l'acl 101 de l'exemple « filtres peu serrés ».et insérer avant la fin :**

*! Permettre à notre routeur de dialoguer avec son voisin*

*! mais à personne d'atteindre notre routeur de l'extérieur.*

*! ( à modifier si nécessaire)*

*! sauf en ICMP*

access-list 101 permit ip host F.G.H.253 host F.G.H.254

access-list 101 permit icmp any host F.G.H.254

*!autoriser rip V2*

access-list 101 permit udp host F.G.H.253 224.0.0.0 15.255.255.255

*!*

*!Fin de déclaration de l'acl 101*

```

!-----
! Déclaration de l'acl 102
!-----
!
! Les filtres :
!   - seuls les services usuels (telnet, mail, ftp, www, dns, pop, ntp) sont
!     accessibles, et ce, seulement vers les machines qui hébergent de tels services.
!   - Je spécifie particulièrement certains réseaux (les ennemis et les amis)
!   - tout le reste est interdit
!
! Je vide les access-list courantes
no access-list 102
!
!
! J'autorise ICMP sur toutes mes machines (cf remarques sur icmp)
access-list 102 permit icmp any X.Y.Z.0 0.0.0.255
!
! Protéger nos machines très sensibles : pas d'IP avec l'extérieur
! X.Y.Z.SENSIBLE et X.Y.Z.SYSLOG (même pas en sortie)
access-list 102 deny ip any X.Y.Z.SENSIBLE 0.0.0.0 log
access-list 102 deny ip any X.Y.Z.SYSLOG 0.0.0.0 log
!
! Accepter les VRAIS AMIS pour tout ??
! ( est ce bien eux ou sont t'ils spoofés - Peut être trop dangereux )
! autorisation du réseau E.F.G.0/24 pour tout
access-list 102 permit ip E.F.G.0 0.0.0.255 any log
!
! Le filtre des ports dangereux a été fait au niveau de l'interface ethernet 1. C'est bien sur
! à adapter en fonction de votre architecture.
!
! J'autorise les connexions tcp établie ( donc initiées depuis l'intérieur).
! cf : http://www.urec.cnrs.fr/cours/Reseau/tcp-ip/sld053.htm
!
access-list 102 permit tcp any X.Y.Z.0 0.0.0.255 established
!
! Pour pouvoir faire du ftp sortant et non passif : j'autorise les connexions
! sur des ports > 1024 en provenance des serveurs ftp
access-list 102 permit tcp any eq 20 X.Y.Z.0 0 0.0.0.255 gt 1023
!
!
! Filtres sur le serveur de messagerie, dns et pop : X.Y.Z.1 :
!
! Autorise le port 113 (RFC 931) sur mon serveur
access-list 102 permit tcp any host X.Y.Z.1 eq 113
!
! Accès au DNS
access-list 102 permit udp any host X.Y.Z.1 eq domain
access-list 102 permit tcp any host X.Y.Z.1 eq domain
!
! accès smtp ( messagerie)
access-list 102 permit tcp any host X.Y.Z.1 eq smtp
!
! accès pop
access-list 102 permit tcp any host X.Y.Z.1 eq 110
!
! Filtres sur le serveur www, telnet, ftp et ntp : X.Y.Z.2
! NTP
access-list 102 permit udp any host X.Y.Z.2 eq ntp

```

```

!telnet
access-list 102 permit udp any host X.Y.Z.2 eq telnet
! FTP connexion de contrôle et de données
access-list 102 permit tcp any host X.Y.Z.2 eq ftp
access-list 102 permit tcp any host X.Y.Z.2 eq ftp-data
! WWW
access-list 102 permit tcp any host X.Y.Z.2 eq www
!
! Si on a d'autres serveurs à mettre c'est le moment...
! sur ce réseau il n'y a rien d'autres
! ../.
!
! Si multicast
!
access-list 102 permit ip 224.0.0.0 15.255.255.255 any log
!
! autorise tout le UDP au dela de 1023
access-list 102 permit udp any X.Y.Z.0 0.0.0.255 gt 1023
!
! interdit tout les autres TCP
access-list 103 deny tcp any X.Y.Z.0 0.0.0.255 log
!
! interdit tout les autres UDP
access-list 103 deny udp any X.Y.Z.0 0.0.0.255 log
!
! autorise tout le reste
!
access-list 102 permit ip any any
!
! Déclaration au niveau de l'interface eth0
!
interface Ethernet0
ip address F.G.H.254 255.255.255.0
! l'ACL numéro 101 s'applique pour les paquets qui entrent dans le routeur par l'interface Ethernet 1
ip access-group 101 in
! Le routeur doit conserver une trace de tous les paquets rejetés pour cause de violation d'une ACL
! associée à cette interface.
! Le routeur conserve dans une table :
! l'adresse IP de l'émetteur du paquet
! l'adresse IP du destinataire du paquet
! le nombre de tentatives
! la taille cumulée des paquets rejetés
ip accounting access-violations
!filtres broadcast icmp
no ip directed-broadcast
no ip proxy-arp
! Rejets des paquets icmp redirect ( évite modification de la politique de routage ).
no ip redirects

interface Ethernet1
!description - Connexion réseau local -
ip address X.Y.Z.254 255.255.255.0
! l'ACL numéro 102 s'applique pour les paquets qui sortent du routeur par l'interface Ethernet 2
ip access-group 102 out
ip accounting access-violations
!filtres broadcast icmp
no ip directed-broadcast
no ip proxy-arp

```

no ip redirects

**Remarque :**

Cette configuration filtre tous les services mais laisse passer les paquets UDP > 1023 permettant de ne pas trop contraindre les utilisateurs avec des services particuliers.

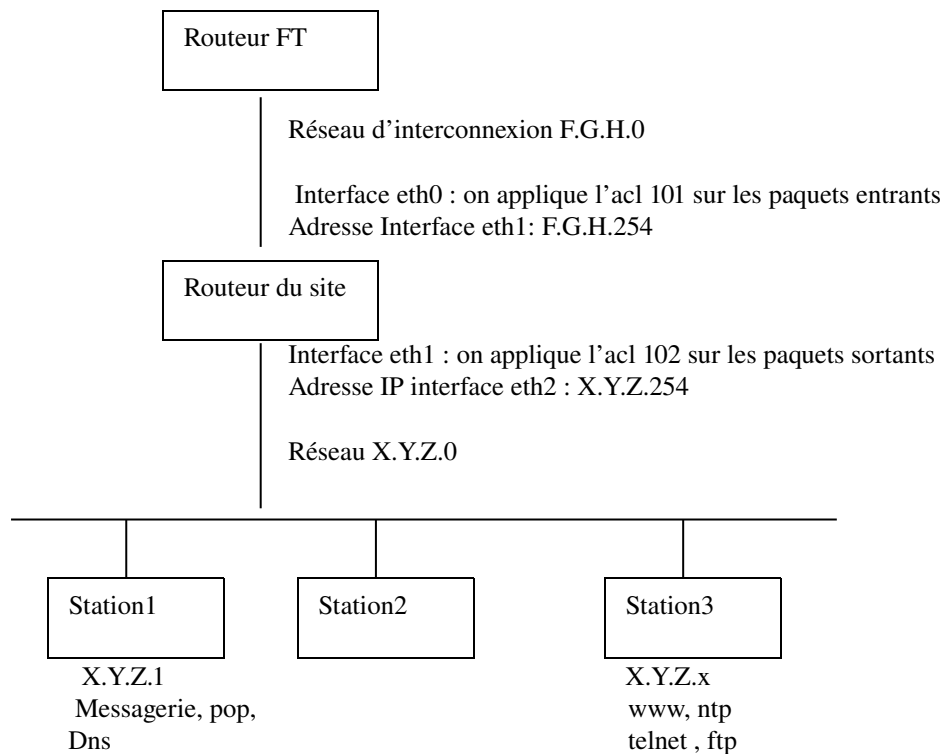


## Exemple de configurations avec access list : « filtres très très serrés »

**Politique:** "tout ce qui n'est pas explicitement autorisé est interdit"

- on interdit d'abord explicitement
- on autorise ce qu'on veut
- puis on bloque ce qui reste.

**Note :** l'ACL 101 n'est pas remise ici mais c'est la même que dans l'exemple « filtres peu serrés ».



*! access-list de contrôle de ce qui rentre sur le réseau d'établissement ( acl 101 )*

*! et de ce qui rentre dans mon réseau (acl102)*

*! Marche sur les versions CISCO postérieures a 10.xx*

*!-----*

*! Déclaration de l'acl 101*

*!-----*

*!*

**Voir l'acl 101 de l'exemple « filtres peu serrés ».et rajouter :**

*! Permettre a notre routeur de dialoguer avec son voisin*

*! mais a personne d'atteindre notre routeur de l'extérieur.*

*! ( a modifier si necessaire)*

*! sauf en ICMP.*

access-list 101 permit ip host F.G.H.253 host F.G.H.254

access-list 101 permit icmp any host F.G.H.254

*!autoriser rip V2*

access-list 101 permit udp host F.G.H.253 224.0.0.0 15.255.255.255

*!*

*!*

*!Fin de déclaration de l'acl 101*

*!-----*

*! Déclaration de l'acl 102*

```

!-----
! Les filtres :
!   - seuls les services usuels (telnet, mail, ftp, www, dns, pop, ntp) sont
!     accessibles, et ce, seulement vers les machines qui hébergent de
!     tels services.
!   - tout le reste est interdit (même les ports UDP > 1024)
!
! Je vide les access-list courantes
no access-list 102
!
! Interdiction de ICMP (ping) sur l'adresse broadcast et l'adresse de réseau
! attention si le réseau est subnetté, pensez aux adresses de sous réseaux et aux adresses
! de broadcast des sous réseaux.
access-list 102 deny icmp any host X.Y.Z.255 log
access-list 102 deny icmp any host X.Y.Z.0 log
!
! J'autorise ICMP sur toutes mes machines
access-list 102 permit icmp any X.Y.Z.0 0.0.0.255
!
! Protéger nos machines très sensibles : pas d'IP avec l'extérieur
! X.Y.Z.SENSIBLE et X.Y.Z.SYSLOG (même pas en sortie)
access-list 102 deny ip any X.Y.Z.SENSIBLE 0.0.0.0 log
access-list 102 deny ip any X.Y.Z.SYSLOG 0.0.0.0 log
!
! Accepter les VRAIS AMIS pour tout ??
! ( est ce bien eux ou sont t'ils spoofés - Peut être trop dangereux )
! autorisation du réseau E.F.G.0/24 pour tout
access-list 102 permit ip E.F.G.0 0.0.0.255 any log
!
! Le filtre des ports dangereux a été fait au niveau de l'interface ethernet 1. C'est bien sur
! à adapter en fonction de votre architecture.
!
! J'autorise les connexions tcp établie ( donc initiée depuis l'intérieur).
! cf : http://www.urec.cnrs.fr/cours/Reseau/tcp-ip/sld053.htm
!
access-list 102 permit tcp any X.Y.Z.0 0.0.0.255 established
!
! Pour pouvoir faire du ftp sortant et non passif : j'autorise les connexions
! sur des ports > 1024 en provenance des serveurs ftp
access-list 102 permit tcp any eq 20 X.Y.Z.0 0 0.0.0.255 gt 1023
!
! J'autorise mon serveur DNS secondaire extérieur à consulter le primaire
! et à répondre aux requêtes de mes clients
access-list 102 permit tcp @IP-secondaire eq 53 X.Y.Z.0 0.0.0.255 gt 1023
access-list 102 permit udp @IP-secondaire eq 53 X.Y.Z.0 0.0.0.255 gt 1023
! a voir pour les clients microsoft : ça marche sans les deux lignes ci dessous mais des paquets
! sont filtrés
!access-list 102 permit tcp @IP-secondaire eq 53 X.Y.Z.0 0.0.0.255 eq 137
!access-list 102 permit udp @IP-secondaire eq 53 X.Y.Z.0 0.0.0.255 eq 137
!
! J'autorise un serveur DNS externe à répondre aux requêtes de mes clients
access-list 102 permit udp @IP-dnsexterne eq 53 X.Y.Z.0 0.0.0.255 gt 1023
!
! Filtres sur le serveur de messagerie, dns et pop : X.Y.Z.1 :
!
! Autorise le port 113 (RFC 931) sur mon serveur
access-list 102 permit tcp any host X.Y.Z.1 eq 113
!

```

```

! Acces au DNS
access-list 102 permit udp any host X.Y.Z.1 eq domain
access-list 102 permit tcp any host X.Y.Z.1 eq domain
!
! accès smtp ( messagerie)
access-list 102 permit tcp any host X.Y.Z.1 eq smtp
!
! accès pop
access-list 102 permit tcp any host X.Y.Z.1 eq 110
!
! Filtres sur le serveur www, telnet, ftp et ntp : X.Y.Z.2
! NTP
access-list 102 permit udp any host X.Y.Z.2 eq ntp
!telnet
access-list 102 permit udp any host X.Y.Z.2 eq telnet
! FTP connexion de contrôle et de données
access-list 102 permit tcp any host X.Y.Z.2 eq ftp
access-list 102 permit tcp any host X.Y.Z.2 eq ftp-data
! WWW
access-list 102 permit tcp any host X.Y.Z.2 eq www
!
! Si on a d'autres serveurs à mettre c'est le moment...
! sur ce réseau il n'y a rien d'autres
!../..
!
! Si multicast
!
access-list 102 permit ip 224.0.0.0 15.255.255.255 any log
!

! On bloque tout le reste
!
access-list 102 deny ip any any log
!
! Déclaration au niveau de l'interface eth0
!
interface Ethernet0
ip address F.G.H.254 255.255.255.0
! l'ACL numéro 101 s'applique pour les paquets qui entrent dans le routeur par l'interface Ethernet 1
ip access-group 101 in
! Le routeur doit conserver une trace de tous les paquets rejetés pour cause de violation d'une ACL
! associée à cette interface.
! Le routeur conserve dans une table :
!   l'adresse IP de l'émetteur du paquet
!   l'adresse IP du destinataire du paquet
!   le nombre de tentatives
!   la taille cumulée des paquets rejetés
ip accounting access-violations
no ip proxy-arp
!filtres broadcast icmp
no ip directed-broadcast
! Rejets des paquets icmp redirect ( évite modification de la politique de routage ).
no ip redirects

interface Ethernet1
!description - Connexion réseau local -
ip address X.Y.Z.254 255.255.255.0
! l'ACL numéro 102 s'applique pour les paquets qui sortent du routeur par l'interface Ethernet 2

```

```
ip access-group 102 out
ip accounting access-violations
! filters broadcast icmp
no ip directed-broadcast
no ip proxy-arp
no ip redirects
```

## Remarques

### 1/ différences entre les exemples 2 et 3 (« filtres très serré » et « filtres très très serrés »)

Les exemples 2 et 3 filtrent en entrée tous les services pour n'autoriser que les services connus. Le reste est bloqué. Par contre l'exemple 2 autorise les ports UDP > à 1023 alors que ce n'est pas fait dans l'exemple 3.

Section à développer.

### 2/ la règle established

la ligne « *access-list 102 permit tcp any X.Y.Z.0 0.0.0.255 established* » permet de laisser passer en entrée de mon réseau tous les segments TCP (contenu dans un datagramme IP) entrant dont la connexion a été initiée depuis l'intérieur du réseau (le bit d'acquiescement de paquet ou de fin de connexion est positionné). Si une connexion est initiée à partir de l'intérieur de mon réseau, tout paquet en retour aura un de ces drapeaux positionnés, donc le paquet passera grâce à cette règle..

On trouve maintenant un certain nombre d'attaques positionnant le bit XX du segment TCP pour faire croire à une connexion établie.

### 2 / Incidence sur les services accessibles par mes utilisateurs : exemple du FTP.

Le réseau est complètement filtré interdisant de nombreux services certes de l'extérieur vers l'intérieur mais aussi de l'intérieur vers l'extérieur.

Exemple de problèmes avec le protocole FTP sur la machine X.Y.Z.1:

on n'a rien filtré dans le sens intérieur vers extérieur. Par contre en entrée sur cette machine tout est filtré sauf les ports correspondants à ses services.

Le service FTP utilise 2 numéros de ports : un pour le contrôle (commandes et réponses), le port 21, l'autre pour le transfert de données, le port 20. Cette connexion est ouverte puis fermée à chaque transfert.

Si j'initie une connexion FTP à partir d'une machine A située à l'intérieur de mon réseau vers une machine B située sur un site distant, la connexion va se faire vers le port 21 du serveur B.

On aura pour la machine A, un port source > 1024, pour la machine B un port destination égale à 21, le tout en TCP.

Le serveur B répondra vers le port > à 1024 avec un port source de 21. Comme la connexion est initiée par la machine A, les filtres laisseront passer le paquet ( grâce à la ligne *access-list 102 permit tcp any X.Y.Z.0 0.0.0.255 established* ). Tout le début de la connexion ( connexion, identification, contrôle) se fera de cette manière : initiée par l'appelant A. Par contre l'échange des données se fait par le port 20 et est initiée par l'appelé (B) après avoir reçu une commande sur le port 21. Vu du routeur, les paquets ayant pour @IP source la machine B, port source 20 et à destination de la machine A port > 1024, semblent initiés par la machine B donc filtrés. D'où l'intérêt de la ligne « *access-list 102 permit tcp any eq 20 X.Y.Z.0 0 0.0.0.255 gt 1023* ».

Au niveau des échanges TCP :

Sens	Port machine A	port machine B	
→	38025	21	initiation de la connexion
←	38025	21	réponse ( ack)
→	38025	21	ack
←	38025	21	demande login
../..			
→	38025	21	envoi commande ls
←	38025	21	réponse ( ack)
←	38025	20	envoi données

Ici le port de départ 38025 est attribué de manière dynamique et sera différent à chaque connexion (mais supérieur à 1023)

Laisser passer les paquets TCP établis ne suffit plus, car la connexion est initiée par B

C'est un peu faire un trou pour en boucher un autre. Un pirate bien intentionné pourra bidouiller son application et attaquer le réseau en faisant semblant de venir d'un port source égale à 20...

C'est pourquoi je pense que le filtrage des ports UDP/TCP dangereux mis dans l'ACL 101 reste indispensable.

### **Et le mode passif ?**

La ligne « *access-list 102 permit tcp any eq 20 X.Y.Z.0 0 0.0.0.255 gt 1023* » n'est pas forcément obligatoire. Sans elle on pourra toujours faire du FTP de l'intérieur vers l'extérieur à condition d'utiliser le mode passif de FTP (à voir dans les options du client FTP – tous n'acceptent pas ce mode). Avec cette option, le transfert se fera via des ports > à 1024 et donc non filtrés. Le mode passif demande au SERVER de se mettre "à l'écoute" d'un port de données (différent du port par défaut et > à 1024) et d'attendre une demande de connexion plutôt que de prendre l'initiative d'en établir une sur réception d'une commande de transfert. La réponse à cette commande précise l'adresse et le port sur lesquels le serveur s'est mis en écoute. Les paquets sont alors autorisés grâce à la règle « established »

D'autres problèmes se retrouveront pour toutes les machines filtrées de manière forte. On peut arranger les choses au moins pour ftp et telnet, mais on ne pourra pas prendre en compte tous les services ( netmeeting à besoin du port 1720, irc ou toutes applications jouant sur des ports > 1024).

### **3/ filtres des ports UDP dangereux**

L'acl 101 filtre entre autre les ports UDP et TCP réputés comme dangereux. Cette liste est valable à un instant T et doit être adaptée et vérifiée.

L'exemple 3 (« filtres très très serrés ») bloque tous les ports UDP et TCP sauf ceux autorisés. Cette liste peut alors paraître inutile. Mais la ligne concernant l'autorisation du FTP, « *access-list 102 permit tcp any eq 20 X.Y.Z.0 0 0.0.0.255 gt 1023* » (il peut y avoir d'autres ouvertures spécifiques), ouvre une brèche dangereuse et nécessite du coup encore le filtre sur les ports dangereux.

Vous pouvez consulter une liste de ports utilisés par des « chevaux de troie » :

[http://packetstorm.securify.com/trojans/Trojan\\_Ports\\_List.r\\_m](http://packetstorm.securify.com/trojans/Trojan_Ports_List.r_m)

### **4/ no service udp-small-servers**

cette commande globale permet de proscrire l'écho udp.

## D'autres filtres

### Limitation de l'accès à mon routeur avec telnet :

```
! On n'autorise l'accès au Cisco que depuis mon réseau X.Y.Z.0
!  
access-list 98 permit X.Y.Z.0.0 0.0.0.255  
!  
line con 0  
exec-timeout 0 0  
password 7 XXXXXXXXXXXXXXXXXXXXXXXX  
login  
line aux 0  
line vty 0 4  
password 7 XXXXXXXXXXXXXXXXXXXXXXXX  
access-class 98 in  
login  
!  
end
```

### Filtres en sortie

Plusieurs possibilités pour les filtres en sortie suivant ce qu'on faire :

- se prémunir contre des attaques venant de l'intérieur de son réseau vers l'extérieur
- bloquer l'accès à certains services
- bloquer les adresses privées
- bloquer les ports de denie de services distribuées

exemple :

```
no access-list 110  
access-list 110 deny ip any X.Y.Z.0 0.0.0.255 (anti-spoofing)  
access-list 110 deny ip 127.0.0.0 0.255.255.255 any (reseaux privés)  
access-list 110 deny ip 10.0.0.0 0.255.255.255 any  
access-list 110 deny ip 172.16.0.0 0.15.255.255 any  
access-list 110 deny ip 192.168.0.0 0.0.255.255 any  
access-list 110 deny ip any 0.0.0.0 255.255.255.0  
access-list 110 deny ip any 0.0.0.255 255.255.255.0  
access-list 110 deny ip any X.Y.Z.255 0.0.0.255 pour un /24  
access-list 110 deny ip any X.Y.Z.63 0.0.0.192 pour un /26  
access-list 110 deny ip any X.Y.Z.31 0.0.0.224 pour un /27  
! eventuellement si vous avez ds doutes  
! port udp des attaques ddos et syn00  
!  
access-list 110 deny udp any any eq 65000 log  
access-list 110 deny tcp any any eq 65000 log  
access-list 110 deny udp any any eq 16660 log  
access-list 110 deny tcp any any eq 16660 log  
access-list 110 deny udp any any eq 60001 log  
access-list 110 deny tcp any any eq 60001 log  
access-list 110 deny udp any any eq 27444 log  
access-list 110 deny udp any any eq 34555 log  
access-list 110 deny tcp any any eq 27665 log  
access-list 110 deny udp any any eq 27665 log  
access-list 110 deny udp any any eq 31335 log  
!  
! blocage d'un service: exemple avec IRC
```

```

!
access-list 110 deny  udp  any any range 6665 6670 log
access-list 110 deny  tcp  any any range 6665 6670 log
access-list 110 deny  udp  any any eq 7000 log
access-list 110 deny  tcp  any any eq 7000 log
!
! blocage de l'accès a Napster, scour et/ou gnutella
! attention les numéros de ports sont configurables
!
! napster : tcp 6697, 6699, 8875, 7777
access-list 110 deny  tcp  any any eq 6697 log
access-list 110 deny  tcp  any any eq 6699 log
access-list 110 deny  tcp  any any eq 8875 log
access-list 110 deny  tcp  any any eq 7777 log
! scour tcp 6346
access-list 110 deny  tcp  any any eq 6346 log
! gnutella tcp 9001
access-list 110 deny  tcp  any any eq 9001 log
!
! et ne pas oublier
! tout le reste : GO
access-list 110 permit ip any any

```

avec au niveau de l'interface de sortie du campus ( eth0 sur nos exemples ) :

```

int eth0
ip access-group 110 out

```

## Filtres sur ICMP

Filtrer icmp est toujours problématique. C'est un protocole à la fois très utile mais aussi potentiellement dangereux. De nombreuses attaques sont basées dessus (« smurf » et autres joyeusetés). Parmi ses différentes fonctions on peut trouver : fragmentation (type 3, message du type "destination unreachable"), PATH MTU Discovery (type 4), drop des paquets, traceroute, ping, contrôle de flux.

Pour info, voici la liste complète des options dans le cas d'un Cisco :

<0-255>	ICMP message type
administratively-prohibited	Administratively prohibited
alternate-address	Alternate address
conversion-error	Datagram conversion
dod-host-prohibited	Host prohibited
dod-net-prohibited	Net prohibited
dscp	Match packets with given dscp value
echo	Echo (ping)
echo-reply	Echo reply
general-parameter-problem	Parameter problem
host-isolated	Host isolated
host-precedence-unreachable	Host unreachable for precedence
host-redirect	Host redirect
host-tos-redirect	Host redirect for TOS
host-tos-unreachable	Host unreachable for TOS
host-unknown	Host unknown
host-unreachable	Host unreachable
information-reply	Information replies
information-request	Information requests
log	Log matches against this entry
log-input	Log matches against this entry, including input interface



mask-reply	Mask replies
mask-request	Mask requests
mobile-redirect	Mobile host redirect
net-redirect	Network redirect
net-tos-redirect	Net redirect for TOS
net-tos-unreachable	Network unreachable for TOS
net-unreachable	Net unreachable
network-unknown	Network unknown
no-room-for-option	Parameter required but no room
option-missing	Parameter required but not present
packet-too-big	Fragmentation needed and DF set
parameter-problem	All parameter problems
port-unreachable	Port unreachable
precedence	Match packets with given precedence value
precedence-unreachable	Precedence cutoff
protocol-unreachable	Protocol unreachable
reassembly-timeout	Reassembly timeout
redirect	All redirects
router-advertisement	Router discovery advertisements
router-solicitation	Router discovery solicitations
source-quench	Source quenches
source-route-failed	Source route failed
time-exceeded	All time exceeded
time-range	Specify a time-range
timestamp-reply	Timestamp replies
timestamp-request	Timestamp requests
tos	Match packets with given TOS value
traceroute	Traceroute
ttl-exceeded	TTL exceeded
unreachable	All unreachables

**Pour ceux qui veulent filtrer le protocole icmp**, voici au moins ce qu'il faut autoriser :

```
access-list 102 permit icmp any any unreachable parameter-problem source-quench
time-exceeded ttl-exceeded packet-too-big
administratively-prohibited
```

```
access-list 102 deny icmp any any
```

**Autrement, pour ceux qui autorisent ping**, on peut limiter les excès éventuels en ajoutant ceci sur l'interface d'entrée :

```
rate-limit input access-group 2000 744000 10000 10000 conform-action transmit exceed-
action drop
```

avec :

```
access-list 2000 permit icmp any any echo-reply
access-list 2000 permit icmp any any echo
```

A noter que ça protège dans les deux sens : ainsi, vous protégez aussi le monde extérieur des smurfeurs qui auraient investi votre site.

Je crois que ça ne marche que avec les IOS 12.X et ... je n'ai pas testé.

**La ligne “no ip directed-broadcast”:**

Cette commande à mettre au niveau de chaque interface est équivalente aux deux règles suivantes :

```
deny icmp any 0.0.0.255 255.255.255.0
deny icmp any 0.0.0.0 255.255.255.0
```



### SNMP et MRTG

MRTG permet de récupérer n'importe quelle variable SNMP et de la « grapher ».

On ne parle pas ici de l'installation de MRTG, mais on donne uniquement des exemples pour quelques variables intéressantes sur les routeurs Cisco.

Pour une petite documentation sur l'installation de MRTG, cf : <http://www.urec.cnrs.fr/urecor/ars/mrtg.txt>

Pour pouvoir récupérer les variables SNMP de votre routeur, il faut activer SNMP et choisir votre nom de communauté (public ici) SNMP :

Commande globale :

`snmp-server community public RO 3`

Le chiffre 3 correspond à un numéro d'acl (histoire de continuer à filtrer l'accès aux variables SNMP).

#### **Quelques variables intéressantes avec un routeur CISCO :**

Je mets ci dessous les fichiers de configuration MRTG, `mrtg.cfg` à adapter suivant vos configurations. Dans tous ces fichiers, l'important est la variable « target ». Le reste est dans la doc MRTG.

**Les débits :** utiliser la commande `cfgmaker` de MRTG en l'appliquant à votre routeur pour créer un fichier `mrtg.cfg`.

#### **La CPU**

```
#####
# mrtg cpu
#####
WorkDir: /usr/local/apache/htdocs/mrtg/cpu/
Options[^]: gauge,growright,nopercent
Legend1[^]: Pourcentage d'utilisation CPU /5 min
LegendI[^]: &nbsp;:
YLegend[^]: %utilisation
ShortLegend[^]: % d'utilisation CPU
MaxBytes[^]: 999000000

Target[cpurouteur]: .1.3.6.1.4.1.9.2.1.58.0&.1.3.6.1.4.1.9.2.1.58.0:public@nom-routeur
Title[cpurouteur]: Utilisation CPU routeur /5 min
PageTop[cpurouteur]: <H2>Utilisation CPU routeur /5 min</H2>
LegendO[cpurouteur]:
```

#### **La mémoire disponible :**

```
#####
# mrtg mem
#####
WorkDir: /usr/local/apache/htdocs/mrtg/mem/

Options[^]: gauge,growright,nopercent
Legend1[^]: m&eacute;moire libre en octets
LegendI[^]: &nbsp;:
YLegend[^]: octets
ShortLegend[^]: octets de m&eacute;moire libre
MaxBytes[^]: 125000000

Target[memrouteur]: .1.3.6.1.4.1.9.2.1.8.0&.1.3.6.1.4.1.9.2.1.8.0: public@nom-routeur
Title[memrouteur]: M&eacute;moire libre routeur
```

PageTop[memrouteur]: <H2>M&eacute;moire libre routeur</H2>  
LegendO[memrouteur]:

### La variable rely

Cette variable donne une idée de la fiabilité des interfaces. Sa valeur doit être égale à 255 de manière constante. On peut l'appliquer à chacune des interfaces du routeur :

```
#####  
# mrtg rely  
#####
```

```
WorkDir: /usr/local/apache/htdocs/mrtg/rely/  
options[^]: gauge,growright,nopercent  
LegendI[^]:  
LegendI[^]: :  
YLegend[^]: :  
ShortLegend[^]:  
MaxBytes[^]: 999000000  
Language: french
```

```
Target[relyint1]:.1.3.6.1.4.1.9.2.2.1.1.22.1&.1.3.6.1.4.1.9.2.2.1.1.22.1: public@nom-routeur  
PageTop[relyint1]: <H2>Variable interface 1</H2>  
Title[relyint1]: Variable interface 1  
LegendO[relyint1]:
```

```
Target[relyint2]:.1.3.6.1.4.1.9.2.2.1.1.22.2&.1.3.6.1.4.1.9.2.2.1.1.22.2: public@nom-routeur  
PageTop[relyint2]: <H2> Variable interface 2</H2>  
Title[relyint2]: Variable interface 2  
LegendO[relyint2]:  
../..  
et ainsi de suite pour chacune des interfaces.
```

### Analyse des logs

Il est indispensable d'avoir un script qui analyse les logs récupérés.

Section à développer.

## Références

Filtres sur le site du CRU : <http://www.cru.fr/securite/1INDEXs/filtres-routeur.html>

Cours sur les filtres Cisco de Roland Dirlewanger : <http://www.dr15.cnrs.fr/Cours/ACL-Cisco/>

Filtres sur le site de l'Urec : <http://www.urec.cnrs.fr/cours/securite/commencer/3.0.0.filtres.html>

Cisco : <http://www.cisco.com/>

Internet Security Advisories : <http://www.cisco.com/warp/public/707/advisory.html>

Increasing Security on IP Networks : <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm>

Building Bastion Routers Using Cisco IOS by Brett and Variable K : <http://www.insecure.org/news/P55-10.txt>

<http://coombs.anu.edu.au/ipfilter/ip-filter.html>

Un générateur d'access list : <http://stef.u-picardie.fr/ftp/pub/cisco/Current/cisco-ACL/>