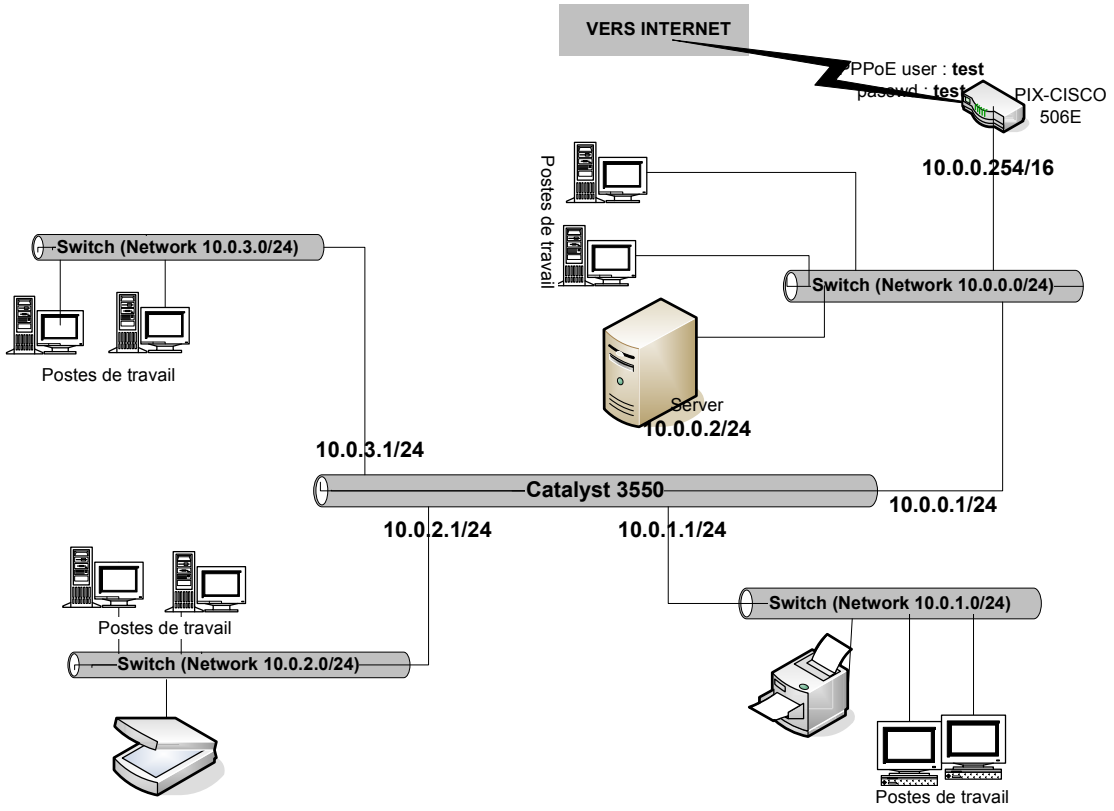
Configuration d'un PIX

Le PIX de Cisco est équipement de niveau IP qui peut faire à la fois du NAT, NATP et du routage (RIP, OSPF, ..).

Notre PIX possède deux interfaces réseaux : une connectée sur le réseau local (inside, en général Ethenet1), et l'autre sur l'Internet (outside, en général Ethernet0)
Nous allons voir comment le configurer pour qu'il serve de passerelle Internet à 4 réseaux IP privés : 10.0.0.0/24, 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24 ; donc évidement, il devra être configuré pour faire du PAT. La carte interne du PIX est reliée à un équipement tel qu'un catalyst 3550 sur lequel se trouvent connectés les quatre réseaux.

Voir schéma :



La question est maintenant de savoir comment configurer le PIX de telle sorte que tous réseaux puissent sortir sur l'Internet, et comment rediriger certains services de l'extérieur (comme le web, la messagerie, …) vers le serveur en 10.0.0.2 ???

1. Configuration du PAT

"The PIX Firewall associates internal addresses with global addresses using a NAT identifier (NAT ID). For example, if the inside interface has NAT ID 5, then hosts making connections from the inside interface to another interface (perimeter or outside) get a substitute (translated) address from the pool of global addresses associated with NAT ID 5.

If you decide not to use NAT to protect internal addresses from exposure on outside networks, assign those addresses NAT ID 0, which indicates to the PIX Firewall that translation is not provided for those addresses. Refer to the *Cisco PIX Firewall Command Reference* for configuration information."

Y'a pas meilleure explication que le texte en anglais de Cisco, mais en gros, ça signifie que pour faire du NAT ou du PAT, il faut au moins 2 lignes de commandes, une commençant par **global** qui permet en fait de spécifier la ou les adresses IP publiques (ou rarement privées) qui vont être utilisées pour sortir et donc qui seront vues de l'extérieur, et une autre commençant par **nat** qui permet de définir les réseaux qui seront natés.

Exemple :

```
global (outside) 1 196.200.201.5 netmask 255.255.255.224
nat (inside)  1  0.0.0.0  0.0.0.0  0  0
```

Dans cet exemple NAT_ID=1
Permettre à n'importe quelle machine (**0.0.0.0 0.0.0.0**) venant de l'interface interne (**inside**) de sortir sur l'Internet (**outside**) en utilisant l'IP publique **196.200.201.5/27**. Une seule IP pour le NAT, donc ça devient du PAT.
Autre manière d'écrire :

```
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

interface signifie qu'on fera du PAT en utilisant l'IP de l'interface externe.
Autre exemple :

```
nat (inside) 1 10.1.0.0 255.255.0.0
nat (inside) 2 10.2.0.0 255.255.0.0
global (outside) 1 192.168.1.1
global (outside) 2 209.165.200.225
```

Les machines du réseau en 10.1.0.0/16 sortiront avec l'IP 192.168.1.1
Les machines du réseau 10.2.0.0/16 sortiront avec l'IP 209.165.200.225

2. Contrôler les accès de l'extérieur : A partir d'ACL

```
access-list acl_out_in permit tcp any any eq pop3
access-list acl_out_in permit tcp any any eq http
access-list acl_out_in permit tcp any any eq imap4
access-list acl_out_in permit tcp any any eq smtp
```

```
access-list acl_out_in permit tcp 196.200.201.0 255.255.255.0 any
eq ssh
```
Ces 5 lignes de commandes permettent de créer une acl appelée **acl_out_in**. Cette acl autorise les services **pop3**, **http**, **imap4**, **smtp**, de n'importe quelle IP vers n'importe quelle autre, et autorise du ssh du réseau 196.200.201.0/24 vers toute IP.
Il reste donc à l'appliquer en entrée sur l'interface outside avec cette commande :
```
access-group acl_out_in in interface outside
```

3. Configurer les redirections de ports depuis l'extérieur

Syntaxe générale : *static* [(*internal_if_name*, *external_if_name*)] {tcp|udp} {*global_ip*|interface} *global_port local_ip local_port* [netmask *mask*]

Exemple :
```
static (inside,outside) tcp interface www 10.0.0.2 www netmask
255.255.255.255 0 0
static (inside,outside) tcp interface smtp 10.0.0.2 smtp netmask
255.255.255.255 0 0
static (inside,outside) tcp interface pop3 10.0.0.2 pop3 netmask
255.255.255.255 0 0
static (inside,outside) tcp interface ssh 10.0.0.2 ssh netmask
255.255.255.255 0 0
static (inside,outside) tcp interface imap4 10.0.0.2 imap4 netmask
255.255.255.255 0 0
```
On redirige donc ainsi les requêtes venant de l'extérieur (mot clé **interface**) sur pour les ports 80 (**www**), 25 (**smtp**), 110 (**pop3**), 22 (**ssh**) et 143 (**IMAP**) sur la machine **10.0.0.2**.

4. Configurer les interfaces réseaux

Carte interne :
La carte interne correspond à l'interface ethernet0 (qui a été nommée **inside**)
```
ip address inside 10.0.0.254 255.255.0.0
```

Carte externe : (Configuration du PPPoE)
Username = test
Password = test

```
vpdn group pppoe_group request dialout pppoe
vpdn group pppoe_group localname test
vpdn group pppoe_group ppp authentication pap
vpdn username test password test
```

pppoe_group est un nom (une chaîne de caractères), on aurait pu mettre pppoe_yerbynet à la place.
request dialout pppoe signifie qu'on veut faire du pppoe.
ppp authentication pap, la méthode d'authentification est le PAP (au lieu de CHAP ou MSCHAP)

5. Autres

Accès au PIX par Telnet : `telnet 10.0.0.2 255.255.255.255 inside`
Accès à l'interface web du PIX :

```
http server enable
http 10.0.0.0 255.255.255.0 inside
```

Ajout de routes statiques :

```
route inside 10.0.1.0 255.255.255.0 10.0.0.1 1
route inside 10.0.2.0 255.255.255.0 10.0.0.1 1
route inside 10.0.3.0 255.255.255.0 10.0.0.1 1
```

Nommage des interfaces :

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
```

Nommage du PIX : `hostname pixfirewall`
Nom de domaine : `domain-name yerbynet.com`
Route par défaut venant du PPPoE : `ip address outside pppoe setroute`

6. Exemple de config d'un PIX

```
: Saved
: Written by enable_15 at 10:36:11.153 UTC Fri Jan 6 2006
PIX Version 6.3(4)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password dMEZSP/wmYRP6B2p encrypted
passwd YdHipVojCP03HYYH encrypted
hostname pixfirewall
domain-name yerbynet.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
object-group service All tcp
  port-object eq www
  port-object eq ssh
  port-object eq pop3
  port-object eq https
```

```
  port-object eq smtp
  port-object eq imap4
access-list outside_access_in permit tcp any any eq pop3
access-list outside_access_in permit tcp any any eq https
access-list outside_access_in permit tcp any any eq imap4
access-list outside_access_in permit tcp any any eq smtp
access-list outside_access_in permit tcp 196.200.201.0 255.255.240.0
any eq ssh
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside pppoe setroute
ip address inside 10.0.0.254 255.255.0.0
ip audit info action alarm
ip audit attack action alarm
pdm location 10.0.0.2 255.255.255.255 inside
pdm location 10.0.0.2 255.255.255.255 outside
pdm location 10.0.0.0 255.255.255.0 inside
pdm logging informational 100
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) tcp interface https 10.0.0.2 https netmask
255.255.255.255 0 0
static (inside,outside) tcp interface smtp 10.0.0.2 smtp netmask
255.255.255.255 0 0
static (inside,outside) tcp interface pop3 10.0.0.2 pop3 netmask
255.255.255.255 0 0
static (inside,outside) tcp interface ssh 10.0.0.2 ssh netmask
255.255.255.255 0 0
static (inside,outside) tcp interface imap4 10.0.0.2 imap4 netmask
255.255.255.255 0 0
static (inside,outside) tcp interface www 10.0.0.2 www netmask
255.255.255.255 0 0
static (inside,outside) tcp interface 3306 10.0.0.2 3306 netmask
255.255.255.255 0 0
access-group outside_access_in in interface outside
route inside 10.0.1.0 255.255.255.0 10.0.0.1 1
route inside 10.0.2.0 255.255.255.0 10.0.0.1 1
route inside 10.0.3.0 255.255.255.0 10.0.0.1 1
timeout xlate 0:05:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225
1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
http server enable
http 192.168.1.0 255.255.255.0 inside
http 10.0.0.0 255.255.255.0 inside
no snmp-server location
```

```
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet 10.0.0.2 255.255.255.255 inside
telnet timeout 5
ssh 10.0.0.2 255.255.255.255 inside
ssh timeout 5
console timeout 0
vpdn group pppoe_group request dialout pppoe
vpdn group pppoe_group localname test
vpdn group pppoe_group ppp authentication pap
vpdn username test password test
terminal width 80
Cryptochecksum:4c7f6ce80b84cc9549290c42b026915d
: end
```

Sources :

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_book09186a0080172852.html
http://www.cisco.com/warp/public/110/mailserver_dmz.html
http://www.digicomp.ch/cours/C10.html
http://www.chinalinuxpub.com/doc/www.siliconvalleyccie.com/cisco-hn/dsl-pix.htm

Roger YERBANGA
www.rogeryerbanga.fr.st