Objectif

- Mise en route d'un Firewall dans une configuration standard, c'est à dire :
    - à l'interface entre les domaines privé et public,
    - avec des clients internes qui veulent utiliser l'Internet,
    - avec des services internes à rendre publics,
    - avec un VPN d'interconnexion.

Matériel

- 2 ASA 5510 ou PIX 515 ou PIX 525
- 3 routeurs standards (28xx, 18xx)
- 1 switch 2950 avec fonction VLAN
- Petit matériel

Architecture logique

L'adressage des branches est choisi de manière à pouvoir ajouter autant de branches que désiré :

- réseau interne :192.168.x.0/24
- interconnexion interne : 172.16.x.0/29
- DMZ (si utilisé) : 10.10.x.0/24
- interconnexion à l'Internet : 172.16.x0.0/29

Un réseau représente les machines de l'Internet :

- 10.0.0.0/24

Les réseaux 10.0.0.0/24 et 172.16.x0.0/29 sont considérés comme publics

Architecture physique

Les segments d'interconnexion à l'Internet (172.16.x0.0/29) peuvent être assez nombreux (selon la quantité de matériel disponible). Ils sont donc réalisés avec le switch 2950, à l'aide des VLANs.
Le segment correspondant au réseau 172.16.x0.0/29 est disponible sur la prise numéro x du switch 2950.
Le routeur « Internet » est relié au 2950 par un lien en mode « trunk », et assure ainsi le routage entre les segments d'interconnexion, et le réseau 10.0.0.0/24. Pour le segment x, le numéro de VLAN et le nom de la sous interface du routeur Internet sont égaux à x.

Par ailleurs, les segments d'interconnexion interne (172.16.x.0/24) sont réalisés avec un câble droit qui relie directement le routeur x au firewall x.

Services nécessaires

- Machine Internet (10.0.0.158) : client web, client ssh (putty), serveur web
- RT1 : client telnet, serveur telnet (console d'administration)
- 192.168.1.1 : client telnet, client web, serveur ssh
- 10.10.2.1 : serveur web

- RT2 : serveur telnet (consle d'administration)
- 192.168.1.1 : client web

Mise en œuvre

Etape 1 Configuration de base

- Réaliser l'architecture physique :
  - utiliser des couleurs différentes pour chaque branche
  - ne pas oublier le 2950 qui n'apparaît pas sur le schéma logique
  - vérifier l'état des liens avec les LEDs sur les interfaces des équipements
- Création des segments d'interconnexion :
  - créer les VLANs sur le 2950
  - activer 802.1q sur le lien vers le routeur « Internet »
- Activation des interfaces :
  - paramétrer les adresses IP des équipements réseau, et des ordinateurs
  - vérifier l'état des liens avec les LEDs sur les interfaces des équipements
- Résolution du routage (sans protocole de routage car non souhaitable dans ce cas) :
  - configurer la passerelle sur chaque ordinateur
  - RT1 : passerelle
  - FW1 : route vers 192.168.1.0/24 et passerelle par défaut
  - même chose pour la branche 2 (et toutes les autres)
  - remarque : le routeur Interne ne connaît que les réseaux «publics », c'est-à-dire 172.16.x0.0/29 et 10.0.0.0/24, il ne routera pas de paquets à destination des 192.168.x.0/24 ni vers 10.10.x.0/24
- Activation des services :
  - sur les machines
  - sur les routeurs

A la fin de cette étape, aucune communication n'est possible à travers les firewalls.

Etape 2 Communications sortantes vers l'Internet

- Sur FWx : réaliser la translation dynamique des machines du réseau 192.168.x.0/24 vers l'adresse 172.16.x0.1 (celle de l'interface eth2 de FWx)

Essayer en faisant une requête web depuis 192.168.x.1 vers 10.0.0.158

Etape 3 Publication de services

- Réaliser la translation statique du service web de 10.10.2.1 vers l'adresse 172.16.20.2
- Appliquer l'ACL qui autorise l'entrée de requêtes web vers 172.16.20.2 dans FW2

Essayer en faisant une requête web depuis 10.0.0.158 vers 172.16.20.2

- Réaliser la translation statique du service ssh de 192.168.1.1 vers l'adresse 172.16.10.2
- Appliquer l'ACL qui autorise l'entrée de requêtes ssh vers 172.16.10.2 dans FW1

Essayer en lançant le client ssh putty sur 10.0.0.158, vers 172.16.10.2

Etape 4 Réalisation de l'interconnexion

- Sur FW1 : créer une ACL pour désigner les flux qui doivent passer dans le VPN (permit tcp 192.168.1.0 0.0.0.255 host 172.16.2.1 eq telnet)
- Sur FW2 : créer une ACL pour désigner les flux qui doivent passer dans le VPN (permit tcp host 172.16.2.1 eq telnet 192.168.1.0 0.0.0.255)
- Sur FW1 et FW2 :
    - créer une SA ISAKMP
    - créer une SA IPSec
    - créer une table des VPNs en désignat le FW distant par son adresse IP
    - lier les Sas et l'ACL à ce VPN
    - appliquer cette table des VPNs à l'interface outside

  Essayer depuis une fenêtre de commande de 192.168.1.1 en lançant un telnet vers 172.16.2.1

Etape 5 Jouer avec cette architecture

Session cliente sortante :

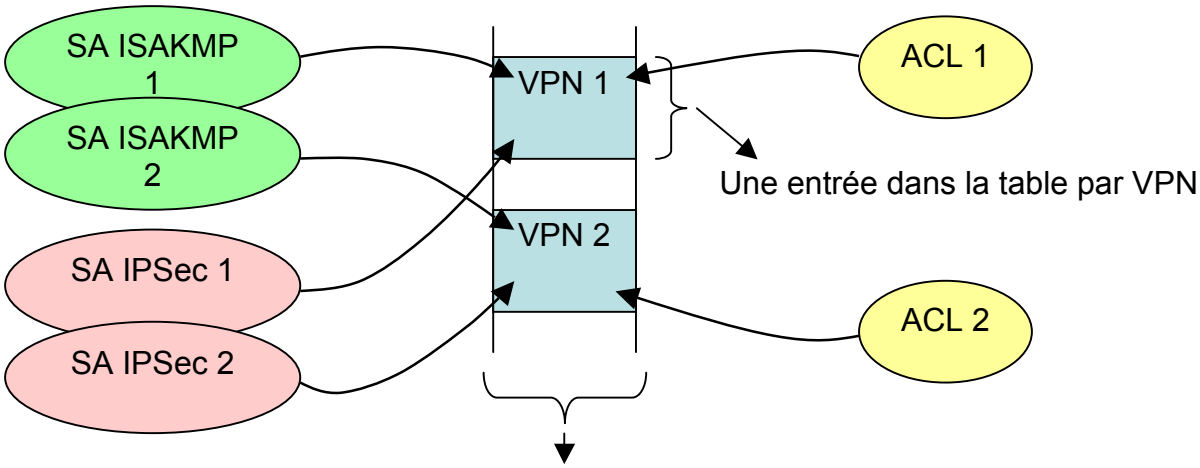
- établir une session http depuis 192.168.1.1, vers 10.0.0.158
- pour cela il faut :
    - résoudre le problème du routage
    - réaliser la translation dynamique des clients vers l'interface « outside » du firewall

Session cliente entrante :

- ouvrir un client ssh sur 10.0.0.158 et lancer une requête vers 172.16.10.2, cela permet la prise de contrôle de la machine 192.168.1.1
- pour cela, il faut :
    - résoudre le problème du routage
    - réaliser la translation statique du service ssh de 192.168.1.1 vers 172.16.10.2
    - appliquer une ACL qui laisse entrer les requêtes ssh par l' « outside » du firewall

Session privée entre les deux branches, à travers l'Internet :

- depuis une console sur 192.168.1.1, lancer un telnet sur 192.168.1.254, on a maintenant le contrôle du routeur RT1,
- depuis RT1, lancer un telnet sur 172.16.2.1, on gagne ainsi le contrôle de RT2 à travers le VPN (communication chiffrée par le VPN, et non pas par telnet), pour cela, sur chaque firewall :
    - créer l'ACL qui capte le flux à faire passer dans le VPN
    - créer les Sas ISAKMP et IPSec
    - créer la table des VPNs, et faire les liens avec l'ACL et les Sas
    - appliquer la table des VPNs à l'interface « outside » du firewall


SA ISAKMP 1
SA ISAKMP 2
SA IPSec 1
SA IPSec 2
VPN 1
VPN 2
ACL 1
ACL 2
Une entrée dans la table par VPN
Appliqué à une interface : 1 map par interface

Configuration : routeur «Internet»

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Internet
!
boot-start-marker
boot-end-marker
!
username admin password cisco
enable password lesecret
!
no aaa new-model
ip subnet-zero
no ip domain-lookup
!
ip cef
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!
interface FastEthernet0/0
 ip address 10.0.0.254 255.255.255.0
 no shutdown
 duplex auto
 speed auto
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!
interface FastEthernet0/1
 no ip address
 no shutdown
 duplex auto

 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1
 ip address 172.16.10.6 255.255.255.248
!
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 172.16.20.6 255.255.255.248
!
interface FastEthernet0/1.3
 encapsulation dot1Q 3
 ip address 172.16.30.6 255.255.255.248
!
interface FastEthernet0/1.4
 encapsulation dot1Q 4
 ip address 172.16.40.6 255.255.255.248
!
interface FastEthernet0/1.5
 encapsulation dot1Q 5
 ip address 172.16.50.6 255.255.255.248
!
interface FastEthernet0/1.6
 encapsulation dot1Q 6
 ip address 172.16.60.6 255.255.255.248
!
interface FastEthernet0/1.7
 encapsulation dot1Q 7
 ip address 172.16.70.6 255.255.255.248
!
interface FastEthernet0/1.8
 encapsulation dot1Q 8
 ip address 172.16.80.6 255.255.255.248
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!
ip classless
!
no ip http server
no ip http secure-server
!
line con 0
line aux 0
line vty 0 4
 login local
 transport input telnet
!
end
```

Configuration : switch 2950 «Internet»

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname switch-internet
!
ip subnet-zero
!
spanning-tree mode pvst
no spanning-tree optimize bpdu
transmission
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 1
interface FastEthernet0/2
 switchport access vlan 2
interface FastEthernet0/3
 switchport access vlan 3
interface FastEthernet0/4
 switchport access vlan 4
interface FastEthernet0/5
 switchport access vlan 5
interface FastEthernet0/6
 switchport access vlan 6
interface FastEthernet0/7
 switchport access vlan 7
interface FastEthernet0/8
 switchport access vlan 8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
 switchport mode trunk
interface GigabitEthernet0/1
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
no ip http server
!
line con 0
line vty 0 4
 password lesecret
 login
line vty 5 15
 password lesecret
 login
!
!
end
```

Configuration : R1

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
username admin password cisco
enable password cisco
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip subnet-zero
ip cef
!
interface FastEthernet0/0
 ip address 192.168.1.254 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1
 ip address 172.16.1.1 255.255.255.248
 duplex auto
 speed auto
 no shutdown
!
ip classless
!
! Resolution du routage
ip route 0.0.0.0 0.0.0.0 172.16.1.6
!
no ip http server
no ip http secure-server
!
line con 0
line aux 0
!
! Activation du serveur telnet
line vty 0 4
 login local
 transport input telnet
!
end
```

Configuration : R2

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Routeur2
username admin password cisco
enable password cisco
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip subnet-zero
ip cef
!
interface FastEthernet0/0
 ip address 192.168.2.254 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1
 ip address 172.16.2.1 255.255.255.248
 duplex auto
 speed auto
 no shutdown
!
ip classless
!
! Resolution du routage
ip route 0.0.0.0 0.0.0.0 172.16.2.6
!
no ip http server
no ip http secure-server
!
line con 0
line aux 0
!
! Activation du serveur telnet
line vty 0 4
 login local
 transport input telnet
!
end
```

Configuration : FW1

```
hostname FW1
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 172.16.1.6 255.255.255.248
 no shutdown
!
interface Ethernet0/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/2
 nameif outside
 security-level 0
 ip address 172.16.10.1 255.255.255.248
 no shutdown
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
! access-list pour l'entree des requetes ssh
access-list 110 extended permit ip any host 172.16.10.2 eq ssh
!
!!!!partie VPN
!
! definition des flux qui vont passer dans le VPN
access-list vpn permit ip 192.168.1.0 0.0.0.255 host 172.16.2.1
!
! Autorise l'entree de paquets IPsec
sysopt connection permit-ipsec
!
! Creation de la SA IPSec
crypto ipsec transform-set saipsec1 esp-des esp-sha-hmac
!
! Creation de la table des VPNs
crypto map map1 10 ipsec-isakmp
! Lien avec l'ACL VPN
crypto map map1 10 match address vpn
! Declaration de l'autre bout du tunel
crypto map map1 10 set peer 172.16.20.1
! Lien avec la SA IPSec
crypto map map1 10 set transform-set saipsec1
```

```
! Application de la table des VPNs à l'interface outside
crypto map map1 interface outside
!
! autorise l'entree de paquets ISAKMP
isakmp enable outside
!
! Creation de la SA ISAKMP
isakmp key lesecret address 172.16.20.1 netmask 255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
!
pager lines 24
mtu inside 1500
mtu dmz 1500
mtu outside 1500
no asdm history enable
arp timeout 14400

!!!!!partie translations
!
! Translations dynamiques
global (dmz) 10 interface
global (outside) 10 interface
nat (inside) 10 192.168.1.0 255.255.255.0
! On exclue les flux qui assent dans le VPN de la translation dynamique
nat (inside) 0 access-list vpn
! Translation statique
static (inside,outside) tcp 172.16.10.2 ssh 192.168.1.1 ssh netmask 255.255.255.255
! Autorise les requêtes ssh en entree vers 172.16.10.2
access-group 110 in interface outside

!!!partie routage
!
route inside 192.168.1.0 255.255.255.0 172.16.1.1 1
route outside 0.0.0.0 0.0.0.0 172.16.10.6 1


timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
```

```
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
service-policy global_policy global
end
```

Configuration : FW2

```
hostname FW2
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 172.16.2.6 255.255.255.248
 no shutdown
!
interface Ethernet0/1
 nameif dmz
 security-level 50
 ip address 10.10.2.254 255.255.255.0
 no shutdown
!
interface Ethernet0/2
 nameif outside
 security-level 0
 ip address 172.16.20.1 255.255.255.248
 no shutdown
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
!
access-list 110 extended permit ip any host 172.16.20.2 eq www
!
!!!! Partie VPN
!
access-list vpn permit ip host 172.16.2.1 192.168.1.0 0.0.0.255

sysopt connection permit-ipsec
crypto ipsec transform-set saipsec1 esp-des esp-sha-hmac
crypto map map1 10 ipsec-isakmp
crypto map map1 10 match address vpn
crypto map map1 10 set peer 172.16.10.1
crypto map map1 10 set transform-set saipsec1
crypto map map1 interface outside
isakmp enable outside
isakmp key lesecret address 172.16.10.1 netmask 255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 1
```

```
isakmp policy 10 lifetime 86400

pager lines 24
mtu inside 1500
mtu dmz 1500
mtu outside 1500
no asdm history enable
arp timeout 14400

!!!!! partie translations
!
global (dmz) 10 interface
global (outside) 10 interface
nat (inside) 10 192.168.2.0 255.255.255.0
! On exclue les flux qui assent dans le VPN de la translation dynamique
nat (inside) 0 access-list vpn
static (dmz,outside) tcp 172.16.20.2 www 10.10.2.1 www netmask 255.255.255.255
access-group 110 in interface outside

!!!! partie routage
!
route inside 192.168.2.0 255.255.255.0 172.16.2.1 1
route outside 0.0.0.0 0.0.0.0 172.16.20.6 1
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
end
```