PROJET TEST CISCO ASA 5520

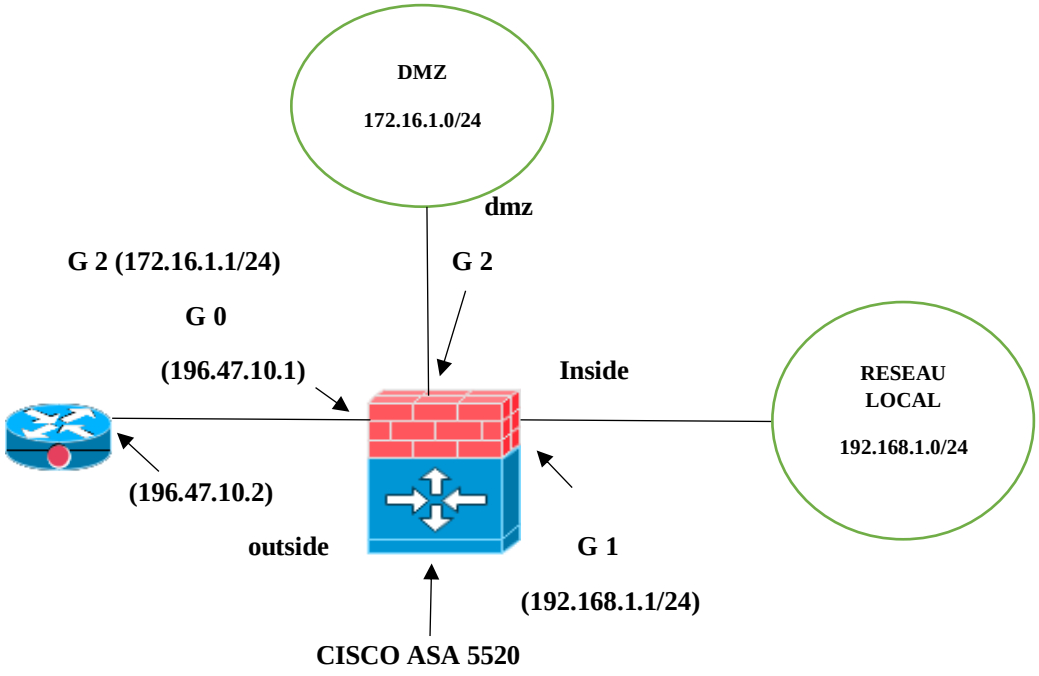
Présentation du ASA 5520

	Description
1	Slots pour Security Services Modules (SSM)
2	2 ports USB 2.0
3	Interface de management Out of Band (OOB)
4	4 ports FastEthernet

	Description
5	Slot pour carte Flash
6	Indicateurs LED Power, Status, Active, VPN, Flash
7	Port Console série
8	Port auxiliaire

PROJET 1 : configurations de base

L'entreprise SETIS Ivoire Technologie à un réseau composé d'éléments suivants :



Le pare-feu CISCO ASA 5520 de l'entreprise SETIS Ivoire Technologie est connecté à 3 entités essentielles de son infrastructure réseau :

- L'adresse du réseau local de SETIS est 192.168.1.0/24
- L'entreprise à 2 serveurs dans sa DMZ (172.16.1.0/24) pour les accès de certains utilisateurs distants :

- Un serveur web (172.16.1.2/24)
- Un serveur de messagerie (172.16.1.3/24)

- SETIS Technologie a louée une plage d'adresse publique (196.47.10.1-196.47.10.5) pour ces besoins.

I. Configurations de base

ciscoasa>

ciscoasa> **enable**

Password:

ciscoasa# **show version**

Cisco Adaptive Security Appliance Software **Version 8.4(2)**

Hardware: ASA 5520, 1024 MB RAM, CPU Pentium II 1000 MHz

Internal ATA Compact Flash, 256MB

BIOS Flash unknown @ 0x0, 0KB

0: Ext: GigabitEthernet0 : address is 0000.ab8b.f500, irq 0

1: Ext: GigabitEthernet1 : address is 0000.ab8b.f501, irq 0

2: Ext: GigabitEthernet2 : address is 0000.ab8b.f502, irq 0

3: Ext: GigabitEthernet3 : address is 0000.ab8b.f503, irq 0

ciscoasa# **conf t**

ciscoasa(config)#

ciscoasa(config)# **interface GigabitEthernet 0**

ciscoasa(config-if)# **ip address 196.47.10.1 255.255.255.0**

ciscoasa(config-if)# **no sh**

ciscoasa(config-if)# **nameif outside**

INFO: Security level for "outside" set to 0 by default.

ciscoasa(config-if)#**exit**

ciscoasa(config)#

ciscoasa(config)# **interface GigabitEthernet 1**

ciscoasa(config-if)# **ip address 192.168.1.1 255.255.255.0**

ciscoasa(config-if)# **no sh**

ciscoasa(config-if)# **nameif inside**

INFO: Security level for "inside" set to 100 by default.

ciscoasa(config-if)#**exit**

ciscoasa(config)#

ciscoasa(config)# **interface GigabitEthernet 2**

ciscoasa(config-if)# **ip address 172.16.1.1 255.255.255.0**

ciscoasa(config-if)# **no sh**

ciscoasa(config-if)# **nameif dmz**

INFO: Security level for "dmz" set to 0 by default.

ciscoasa(config-if)#

ciscoasa(config-if)# **security-level 50**

ciscoasa(config-if)# **exit**

ciscoasa(config)# **exit**

ciscoasa# **wr**

ciscoasa#

ciscoasa# **sh nameif**

Interface	Name	Security
GigabitEthernet0	outside	0
GigabitEthernet1	inside	100
GigabitEthernet2	dmz	50

ciscoasa#

ciscoasa# **conf t**

ciscoasa(config)#

ciscoasa(config)#**route outside 0.0.0.0 0.0.0.0 196.47.10.2**

II. Configuration du NAT (Network Address Translation)

Le pare feu CISCO ASA supporte 4 types de NAT :

- **Dynamic NAT :** Son principe est de translater des adresses sources d'une interface avec un niveau de sécurité élevé vers une plage (pool) d'adresses IP d'un niveau de sécurité moins élevé. Par exemple sur version du ASA (IOS antérieur à 8.3) la commande **« nat »** définie quel intervalle d'hôte (réseau local) sera translaté ensuite la commande **« global »** indique vers quel pool (adresses mappées) le trafic passera.
- **PAT :** connu aussi sous le nom de translation « many to one ». Dans ce cas un groupe d'adresses IP sont mappées au profit d'une seule
- **Static NAT :** permet un mappage permanent entre l'adresse réel et le pool d'adresses mappées. L'adresse réel doit être dans une zone avec un niveau de sécurité plus élevé que celle de la zone des adresses mappées. Le « static NAT » permet avec une ACL

appropriée de permettre un accès à des personnes de l'extérieur entrant par le « outside » d'avoir accès à un serveur situé dans la DMZ. Le « static NAT » permet une communication bidirectionnelle.

- **Identity NAT :** « identity NAT » permet à une adresse privée de n'être pas translatée. Cela est utilisée dans les configurations de VPN où nous avons besoin d'exempter la trafic VPN de l'opération de NAT.

- **Application**

ciscoasa# **conf t**

ciscoasa(config)# **object network pool_mappe_1**

ciscoasa(config-network-object)# **range 172.16.1.2 172.16.1.5**

ciscoasa(config-network-object)# **exit**

ciscoasa(config)# **object network pool_mappe_2**

ciscoasa(config-network-object)# **range 196.47.10.1 196.47.10.5**

ciscoasa(config-network-object)# **exit**

ciscoasa(config)#

ciscoasa(config)# **object network inside_vers_dmz**

ciscoasa(config-network-object)# **subnet 192.168.1.0 255.255.255.0**

ciscoasa(config-network-object)# **nat (inside,dmz) dynamic pool_mappe_1**

ciscoasa(config-network-object)# **exit**

ciscoasa(config)# **object network inside_vers_outside**

ciscoasa(config-network-object)# **subnet 192.168.1.0 255.255.255.0**

ciscoasa(config-network-object)# **nat (inside,outside) dynamic pool_mappe_2**

ciscoasa(config-network-object)# **exit**

ciscoasa(config)# **object network dmz_vers_outside**

ciscoasa(config-network-object)# **subnet 172.16.1.0 255.255.255.0**

ciscoasa(config-network-object)# **nat (dmz,outside) dynamic pool_mappe_2**

ciscoasa(config-network-object)# **exit**

ciscoasa(config)#

ciscoasa(config)# **object network serveur_web**

ciscoasa(config-network-object)# **host 172.16.1.2**

ciscoasa(config-network-object)# **nat (dmz,outside) static 196.47.10.3 service tcp 80 80**

ciscoasa(config-network-object)# **exit**

ciscoasa(config)# **object network serveur_mail**

ciscoasa(config-network-object)# **host 172.16.1.3**

ciscoasa(config-network-object)# **nat (dmz,outside) static 196.47.10.4 service tcp 25 25**

ciscoasa(config-network-object)# **exit**

ciscoasa(config)# **exit**

ciscoasa# **wr**

Remarques :

- Le premier numéro (25 ou 80) est le port d'écoute sur le serveur
- Le second numéro (25 ou 80) est le port mappé visible depuis l'extérieur

III. Configuration des ACL (Access Control Lists)

Pour créer les ACL on applique généralement les règles suivantes :

ciscoasa(config)# **access-list "nom de l'ACL" [line numéro de la ligne] [extended] {deny| permit}protocol "adresse source" "masque" [port source de l'opérateur] "adresse de destination" "masque" [port destination de l'opérateur]**

Pour appliquer les ACL crées on utilise la syntaxe suivante :

ciscoasa(config)# **access-group "nom de l'ACL" [in | out] interface "nom de l'interface"**

- **nom de l'ACL :** nom descriptif de l'ACL c'est ce même nom qui est utilisé dans la commande « acces-group »
- **numéro de la ligne :** chaque entrée de ACL à son propre numéro de ligne
- **extended :** terme à utiliser si vous spécifiez l'adresse source et destination dans l'ACL
- **deny| permit** : permet de spécifier si le trafic est autorisé ou bloqué
- **protocol** : spécifie le protocole concerné par ce trafic (IP, TCP, UDP, etc)
- **"adresse source" "masque" :** cela est fait pour spécifier l'adresse IP source et le masque de sous réseaux d'où vient le trafic en question. Si ce trafic provient d'une seule adresse on peut utiliser le mot « **host** » sans le masque. On pourra utiliser le mot « **any** » pour indexer toutes adresses.
- **port source de l'opérateur :** cela représente le numéro de port source d'où est originaire ce trafic. Les mots clés de l'opérateur peuvent être :
    - « gt (greater than) » : strictement supérieur
    - « eq (equal) » : égal
    - «Neq (Not equal) » : pas égal à
    - « range » : plage de ports

  Mais si aucun n'est spécifier ASA considère que cela concerne tous les ports

- **"adresse destination" "masque" :** cela est fait pour spécifier l'adresse IP destination et le masque de sous réseaux vers qui ce trafic est destiné. Si ce trafic est destiné à seule adresse on peut utiliser le mot « **host** » sans le masque. On pourra utiliser le mot « **any** » pour indexer toutes adresses.

- **port destination de l'opérateur :** cela représente le numéro de port destination vers qui est destiné ce trafic. Les mots clés de l'opérateur peuvent être :
    - « gt (greater than) » : strictement supérieur
    - « eq (equal) » : égal
    - «Neq (Not equal) » : pas égal à
    - « range » : plage de ports

  Mais si aucun n'est spécifier ASA considère que cela concerne tous les ports

- **Application**

✓ Ecrivons la règle d'accès qui permettra un accès depuis l'extérieur au serveur web qui se trouve dans la DMZ

ciscoasa(config)# **access-list ACCES_SERVEUR_WEB extended permit tcp any host 172.16.1.2 eq 80**

ciscoasa(config)# **access-group ACCES_SERVEUR_WEB in interface outside**

✓ Ecrivons la règle d'accès qui permettra un accès depuis l'extérieur du serveur mail qui se trouve dans la DMZ

ciscoasa(config)# **access-list ACCES_SERVEUR_MAIL extended permit tcp any host 172.16.1.3 eq 25**

ciscoasa(config)# **access-group ACCES_SERVEUR_MAIL in interface outside**

✓ Écrivons la règle qui permettra au trafic de la DMZ de passer par le pare feu ASA

ciscoasa(config)# **access-list TRAFIC_DMZ extended permit ip any any**

ciscoasa(config)# **access-group TRAFIC_DMZ in interface dmz**

Pour voir un ACL on procède comme suit :

ciscoasa(config)# **show access-list "nom ACL"**

Pour rendre un ACL inactive on procède comme suit : on met "**no**" devant l'ACL

✓ Nous allons utiliser le système des ACL pour bloquer l'accès au site **www.monsite.ci** aux heures de travail.

ciscoasa# **conf t**

ciscoasa(config)# **dns domain-lookup outside**

ciscoasa(config)# **dns server-group DefaultDNS**

ciscoasa(config-dns-server-group)# **name-server 8.8.8.8**

ciscoasa(config-dns-server-group)# **domain-name google.com**

ciscoasa(config-dns-server-group)# **exit**

ciscoasa(config)# **object network obj-www.monsite.ci**

ciscoasa(config-network-object)# **fqdn www.monsite.ci**

ciscoasa(config-network-object)# **exit**

ciscoasa(config)# **object network obj-monsite.ci**

ciscoasa(config-network-object)# **fqdn monsite.ci**

ciscoasa(config-network-object)# **exit**

ciscoasa(config)#

ciscoasa(config)# **time-range heure_travail**

ciscoasa(config-time-range)# **periodic weekdays 08:00 to 12:00**

ciscoasa(config-time-range)# **periodic weekdays 14:00 to 17:00**

ciscoasa(config-time-range)# **exit**

ciscoasa(config)# **access-list BLOQUE_SITE extended deny ip any object obj-www.monsite.ci**

ciscoasa(config)# **access-list BLOQUE_SITE extended deny ip any object obj-monsite.ci**

ciscoasa(config)# **access-list BLOQUE_SITE extended deny tcp any any eq www time-range heure_travail**

ciscoasa(config)# **access-group BLOQUE_SITE in interface inside**

ciscoasa(config)#**exit**

ciscoasa#**wr**

- ✓ création d'un ACL sur l'interface « outside » qui permet seulement un « echo-reply » pour des besoins de « troubleshooting »

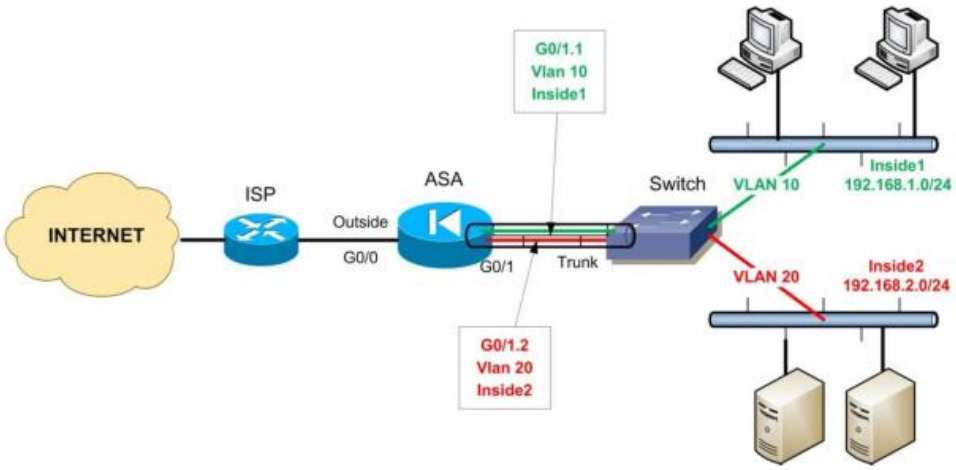
ciscoasa(config)#**access-list PING_EXT extended permit icmp any any echo-reply**

ciscoasa(config)# **access-group PING_EXT in interface outside**

PROJET 2 : couplage ASA avec des VLAN

Nous supposons que dans ce projet le réseau de l'entreprise SETIS Ivoire Technologie a évolué en 2 sous réseaux (192.168.1.0/24 et 192.168.2.0/24).

Ces 2 sous réseaux sont respectivement dans 2 VLANs (VLAN 10 et VLAN 20) comme présenté sur la figure ci-dessous :



Nous allons créer 2 sous interfaces que sont : G 1.1 et G 1.2 qui seront affectées respectivement au VLAN 10 et VLAN 20. Si l'on configure des sous interfaces sur une interface physique, pour rappel cette interface physique doit être connecté à un port « trunk » sur le switch.

Dans notre cas lorsque nous activerons les sous interfaces sur l'interface physique interne du ASA, il faut s'assurer qu'aucun trafic ne passe sur cette interface physique.

ciscoasa# **conf t**

ciscoasa(config)#

ciscoasa(config)# **interface GigabitEthernet 1**

ciscoasa(config-if)# **no nameif**

ciscoasa(config-if)# **no security-level**

ciscoasa(config-if)# **no ip address**

ciscoasa(config-if)# **exit**

ciscoasa(config)# **interface GigabitEthernet 1.1**

ciscoasa(config-subif)# **vlan 10**

ciscoasa(config-subif)# **nameif inside1**

ciscoasa(config-subif)# **security-level 80**

ciscoasa(config-subif)# **ip address 192.168.1.1 255.255.255.0**

ciscoasa(config-subif)# **exit**

ciscoasa(config)# **interface GigabitEthernet 1.2**

ciscoasa(config-subif)# **vlan 20**

ciscoasa(config-subif)# **nameif inside2**

ciscoasa(config-subif)# **security-level 90**

ciscoasa(config-subif)# **ip address 192.168.2.1 255.255.255.0**

ciscoasa(config-subif)# **exit**

ciscoasa(config)# **exit**

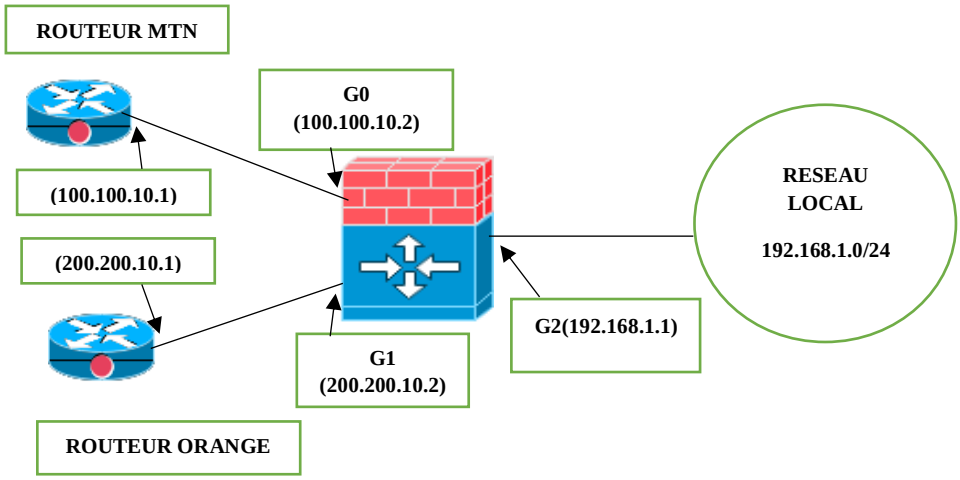
ciscoasa# **wr**

ciscoasa# **sh nameif**

PROJET 3 : basculement entre 2 FAI

Ce projet a pour but de présenter la configuration de 2 FAI avec CISCO ASA.

La configuration se fera selon le schéma ci-dessous :



I. Configurations de base

ciscoasa> **enable**

ciscoasa# **conf t**

ciscoasa(config)#

ciscoasa(config)# **interface GigabitEthernet 0**

ciscoasa(config-if)# **ip address 100.100.10.2 255.255.255.0**

ciscoasa(config-if)# **no sh**

ciscoasa(config-if)# **nameif outside1**

ciscoasa(config-if)#**exit**

ciscoasa(config)# **interface GigabitEthernet 1**

ciscoasa(config-if)# **ip address 200.200.10.2 255.255.255.0**

ciscoasa(config-if)# **no sh**

ciscoasa(config-if)# **nameif outside2**

ciscoasa(config-if)#**exit**

ciscoasa(config)# **interface GigabitEthernet 2**

ciscoasa(config-if)# **ip address 192.168.1.1 255.255.255.0**

ciscoasa(config-if)# **no sh**

ciscoasa(config-if)# **nameif inside**

ciscoasa(config-if)#**exit**

ciscoasa(config)# **object network pool_mappe_MTN**

ciscoasa(config-network-object)# **range 100.100.10.2 100.100.10.5**

ciscoasa(config-network-object)# **exit**

ciscoasa(config)# **object network pool_mappe_ORG**

ciscoasa(config-network-object)# **range 200.200.10.2 200.200.20.5**

ciscoasa(config-network-object)# **exit**

ciscoasa(config)# **object network inside_vers_outside1**

ciscoasa(config-network-object)# **subnet 192.168.1.0 255.255.255.0**

ciscoasa(config-network-object)# **nat (inside,outside1) dynamic pool_mappe_MTN**

ciscoasa(config-network-object)# **exit**

ciscoasa(config)# **object network inside_vers_outside2**

ciscoasa(config-network-object)# **subnet 192.168.1.0 255.255.255.0**

ciscoasa(config-network-object)# **nat (inside,outside2) dynamic pool_mappe_ORG**

ciscoasa(config-network-object)# **exit**

II. Etapes de configuration

Voici les grandes étapes de la configuration du projet.

1. Utiliser la commande « **sla monitor** » pour spécifier le protocole à surveiller, l'adresse de la cible à surveiller qui est l'adresse routeur du FAI et le temps de test.
2. Utiliser la commande « **sla monitor schedule** » pour programmer le processus de surveillance qui est généralement configuré pour toujours fonctionner « **forever** » sachant la durée et temps de départ sont configurable.
3. Définir la première route statique qui doit être surveillé par la commande « **route** » avec l'option « **track** ».
4. Définir la seconde route statique qui est celle de sauvegarde en mettant sa métrique plus élevée que celui de la première route statique.

III. Application pratique

/*définition de l'ID du SLA*/

ciscoasa(config)# **sla monitor 100**

ciscoasa(config-sla-monitor)# **type echo protocol ipIcmpEcho 100.100.10.1 interface outside1**

/*définition de temps d'attente de réponse au test en millisecondes*/

ciscoasa(config-sla-monitor-echo)# **timeout 3000**

/*définition de la fréquence de répétition au test */

ciscoasa(config-sla-monitor-echo)# **frequency 5**

ciscoasa(config-sla-monitor)# **exit**

/*définition de début du process de surveillance maintenant de l'ID du SLA et exécution pour toujours*/

ciscoasa(config)# **sla monitor schedule 100 life forever start-time now**

/*Association du numéro d'identifiant de surveillance 10 avec le numéro d'identifiant de SLA 100 */

ciscoasa(config)# **track 10 rtr 100 reachability**

ciscoasa(config)# **route outside1 0.0.0.0 0.0.0.0 100.100.10.1 1 track 10**

ciscoasa(config)# **route outside2 0.0.0.0 0.0.0.0 200.200.10.1 254**

Pour rappel dans ce scénario le pare feu ASA va tester la disponibilité du routeur du premier FAI dans notre cas MTN (100.100.10.1) par des pings. S'il n'y a pas de réponse dans les 3 secondes le processus est répétée 5 fois si toujours pas de réponse, la route par défaut sera considérée comme défaillante et la route secondaire sera utilisée pour faire passer le trafic internet.

PROJET 4 : haute disponibilité entre 2 ASA

Le pare feu CISCO ASA supporte la haute disponibilité en 2 modes :

- Maître / Esclave connu avec sous le pseudo Active/Sandby (AS) ;
- Maître / Maître connu avec sous le pseudo Active/Active (AA).

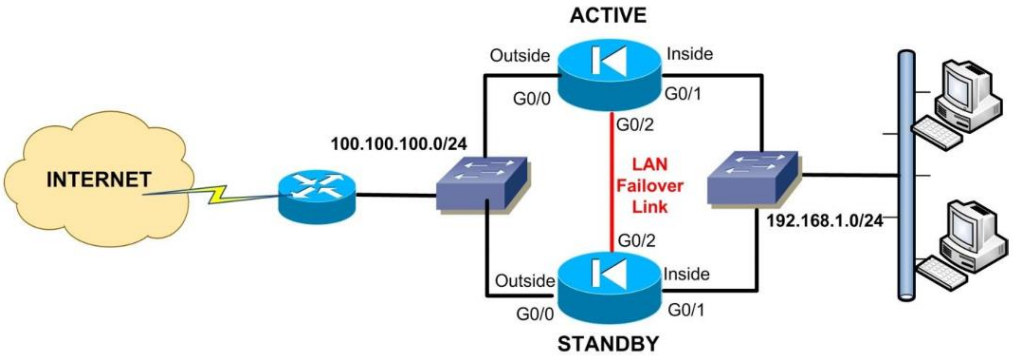
- **Sur les anciens modèles ASA 55xx :**

- 5505 ne supporte pas de haute disponibilité ;
- 5510 avec la licence de base ne supporte pas de haute disponibilité ;
- 5510 avec la licence « security plus » supporte la haute disponibilité en mode AS comme AA ;
- Tous les autres modèles (5520, 5540, 5550, 5580) supportent la haute disponibilité en mode AS comme AA ;

- **Sur les nouveaux modèles ASA 55xx-X :**

- 5512-X avec la licence de base ne supporte pas de haute disponibilité ;
- 5512-X avec la licence « security plus » supporte la haute disponibilité en mode AS comme AA ;
- Tous les autres modèles (5515-X, 5525-X, 5545-X, 5555-X, 5585-X) supportent la haute disponibilité en mode AS comme AA ;

Nous expliquerons la configuration de la haute disponibilité avec ASA selon le schéma ci-dessous :



- **Etape 1 : préparation du premier pare feu (Active)**

A cette première étape le pare feu qui sera utilisé en « standby » doit être déconnecté. Connecter les ports du ASA que vous allez pour le projet aux différents switches. Mettre les ports du ASA qui seront utilisés pour le projet en mode « full duplex » et fixer la vitesse de transmission à 100 en se plaçant en mode interface. Cela se fait par les commandes « **speed 100** » et « **duplex full** ».

Il faudra activer la fonctionnalité « **PortFast** » sur les ports des commutateurs qui seront connectés aux interfaces des ASA.

Réserver des adresses IP qui seront utilisés sur chaque ASA, une sera affectée au « active » et l'autre au « standby ».

Dans notre cas nous utiliserons sur l'interface « inside » :

- 192.168.1.1/24 pour le ASA « active » ;
- 192.168.1.2/24 pour le ASA « standby ».

Pour l'interface « outside » :

- 100.100.100.1/24 pour le ASA « active » ;
- 100.100.100.2/24 pour le ASA « standby ».

L'on doit aussi réserver des adresses pour le « failover link » qui doit être un réseau différent des 2 autres. Dans notre nous pourrons utiliser le réseau 192.168.99.0/24 et pourront donner :

- 192.168.99.1/24 pour le ASA « active » sur l'interface 2 ;

- 192.168.99.2/24 pour la ASA « standby » sur l'interface 2.

- **Etape 2 : configuration du réseau pour le « Failover Link » du premier pare feu (Active)**

Voici la processus de configuration du « Failover » :

/*définition du maître*/

ciscoasa(config)# **failover lan unit {primary|secondary}**

/*assigner l'interface choisie comme « failover link »*/

ciscoasa(config)# **failover lan interface « nom du failover » « nom de l'interface physique »**

/*activer le lien « failover »*/

ciscoasa(config)# **failover link « nom du failover » « nom de l'interface physique »**

/*assigner les adresses IP aux interfaces « active » et « standby »*/

ciscoasa(config)# **failover interface ip « nom du failover » « adresse IP » « masque » standby « adresse IP »**

/*activer le mécanisme général de « failover »*/

ciscoasa(config)# **failover**

- **Application**

ciscoasa(config)# **interface GigabitEthernet 2**

ciscoasa(config-if)# **no sh**

ciscoasa(config)# **failover lan unit primary**

ciscoasa(config)# **failover lan interface HAUTEDISPO GigabitEthernet 2**

ciscoasa(config)# **failover link HAUTEDISPO GigabitEthernet 2**

ciscoasa(config)# **failover interface ip HAUTEDISPO 192.168.99.1 255.255.255.0 standby 192.168.99.2**

ciscoasa(config)# **failover**

- **Etape 3 : adressage de base du premier pare feu (Active)**

Après la configuration de la liaison « failover », avant toute configuration sur le second ASA l'on doit procéder à des configurations de base sur le premier en prenant soin de mentionner les adresses utilisées en tant que « active » et « standby » selon cette syntaxe :

ciscoasa(config)# **interface « nom interface »**

ciscoasa(config-if)# **ip address « adresse IP active » « masque » standby « adresse IP standby »**

- **Application**

ciscoasa(config)# **interface GigabitEthernet 1**

ciscoasa(config-if)# **nameif inside**

ciscoasa(config-if)# **security-level 100**

ciscoasa(config-if)# **ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2**

ciscoasa(config-if)#**exit**

ciscoasa(config)# **interface GigabitEthernet 0**

ciscoasa(config-if)# **nameif outside**

ciscoasa(config-if)# **security-level 0**

ciscoasa(config-if)# **ip address 100.100.100.1 255.255.255.0 standby 100.100.100.2**

- **Etape 4 : configuration du monitoring sur le premier pare feu (Active)**

L'évènement qui déclenche le mécanisme de « failover » est la défaillance d'une interface donnée. Nous devons donc donner les interfaces que nous voulons surveiller et donc en cas de défaillance de défaillance d'une de ces interfaces cela déclenchera le mécanisme de « failover ».

Voici la syntaxe de cette déclaration :

ciscoasa(config)# **monitor-interface « nom interface »**

- **Application**

ciscoasa(config)# **monitor-interface inside**

ciscoasa(config)# **monitor-interface outside**

on peut exclure les interfaces reliées à des pans réseaux pas critiques pour le fonctionnement de l'entreprise pour éviter que la défaillance de ceux-ci n'affecte le mécanisme de « failover ».

Voici la syntaxe pour résoudre ce problème :

ciscoasa(config)# **no monitor-interface « nom interface »**

- **Etape 5 : configuration du réseau pour le « Failover Link » du second pare feu (Sandby)**

Cette configuration est la seule à faire sur second pare feu. Pour le faire, allumer le second pare feu et connecter ces interfaces aux interfaces des switches réservées à cela. Il ne faut pas connecter pour le moment le lien « failover » entre les 2 pare feux.

La configuration sur le second ASA est sensiblement la même que celle effectuée sur le premier à l'étape 2.

- **Application**

ciscoasa(config)# **interface GigabitEthernet 2**

ciscoasa(config-if)# **no sh**

ciscoasa(config)# **failover lan unit secondary**

ciscoasa(config)# **failover lan interface HAUTEDISPO GigabitEthernet 2**

ciscoasa(config)# **failover link HAUTEDISPO GigabitEthernet 2**

ciscoasa(config)# **failover interface ip HAUTEDISPO 192.168.99.1 255.255.255.0 standby 192.168.99.2**

ciscoasa(config)# **failover**

ciscoasa(config)# **exit**

ciscoasa# **write memory**

- **Etape 5 : redémarrage du second pare feu (Sandby)**

On peut maintenant le câble de « failover » entre les 2 ASA. Après la connexion des 2 ASA on peut procéder au redémarrage du second ASA par la commande « **reload** ».

Au démarrage du second ASA le processus de réplication entre les 2 ASA peut commencer.

Durant ce processus l'on aura l'apparition de 2 messages essentiels :

- **Beginning Configuration Replication : Sending to Mate** ce message dénote du démarrage du processus de synchronisation.
- **End Configuration Replication to Mate** ce message marque la fin du processus de synchronisation.

A la fin de ce processus l'on devra taper la commande « **write memory »** sur le ASA « active » et cela sauvegardera cet état aussi bien sur le « active » que le « standby ».

On peut vérifier que processus a bien marché en tapant la commande « **show failover** ».

Dorénavant toute configuration devra être effectuée sur le « active » et toute enregistrement des configurations par la commande « **write memory** » s'appliquera aux 2 ASA.