|  | GSB - Fiche d’instructions  **Mission 06 :**  **Mise en place de Firewalls Stateless et de DMZ** | **PPE 3-4**  **SISR** |
| --- | --- | --- |

**Sommaire**

| [1. Objectifs de la mission](#_heading=h.1fob9te)  [1.1 DMZ](#_heading=h.3znysh7)  [1.2 Politique de filtrage interne](#_heading=h.44sinio)  [1.3 Prévention des attaques de type DOS provenant du WAN](#_heading=h.26in1rg)  [1.4 Protection des clients du réseau](#_heading=h.lnxbz9)  [2. Tests des solutions](#_heading=h.35nkun2)  [3. Productions](#_heading=h.1ksv4uv) |
| --- |

## 

## 

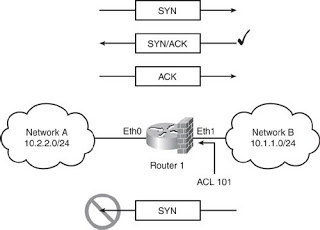
## 1. Objectifs de la mission

Votre management a décidé de renforcer sa politique de sécurité pour les serveurs et clients du site du siège. Vous devez ainsi mettre en place les 3 dispositifs suivants.

### 1.1 DMZ - Serveurs Web internet (public) et intranet

Vous devez disposer de 2 serveurs Web (sur le même système / @IP ou non) :

* Un serveur WEB internet public (ex port 80) inclus dans la DMZ car il a vocation à être à la fois accessible du LAN et du WAN sans mettre en danger le LAN en cas d’infection du serveur. Indice : on pourra exploiter l’option finale “established” dans les ACL TCP.
* Un serveur WEB intranet privé (ex : port 8000) disponible uniquement depuis le LAN et depuis le télétravailleur



### 

### ATTENTION (1) : IL VOUS FAUT IMPÉRATIVEMENT PRÉCISER AU PROF LES ADRESSES IP DES SERVEURS WEB ET AUTRES PRÉSENTS SUR PROXMOX; En effet le routeur WAN doit être paramétré afin de router les paquets à destination de ces serveurs via le lien série du routeur WAN de votre config, et non directement vers le routeur “SISR”

### ATTENTION (2) : AVANT DE METTRE EN PLACE VOS REGLES DE FILTRAGES, PENSEZ A INCLURE DES EXCEPTIONS PERMETTANT DE FAIRE DES PINGS (ICMP), DU TELNET AINSI QUE D’AUTORISER LES COMMUNICATIONS ISAKMP ENTRE LES 2 ROUTEURS VPN !!!

### 

### 1.2 Politique de filtrage interne

Afin de n’autoriser que les membres du service informatique à accéder aux terminaux virtuels des serveurs, vous réaliserez un filtrage entre le LAN des bureaux et les serveurs, ceci afin de n’autoriser que les postes du VLAN 10 (postes d’administration) à accéder aux ports telnet et SSH des serveurs



**ATTENTION** : IL VOUS FAUT IMPÉRATIVEMENT PRÉCISER AU PROF LES ADRESSES IP DES SERVEURS WEB ET AUTRES PRÉSENTS SUR PROXMOX; En effet le routeur WAN doit être paramétré afin de router les paquets à destination de ces serveurs via le lien série du routeur WAN de votre config, et non directement vers le routeur “SISR”

### 

### 

### 

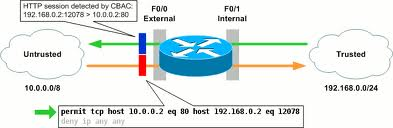
### 1.3 Prévention des attaques de type DOS provenant du WAN

Votre management vous impose de protéger votre serveur Web par des dispositifs de firewall *stateful* de type **interception** pour limiter l’effet des attaques de type DOS ou DDOS provenant du WAN.



### 1.4 Protection des clients du réseau

On vous demande de mettre en place un dispositif de CBAC (Context-Based Access List) afin de faire en sorte que toutes les réponses de requêtes provenant de serveurs du WAN correspondent bien à des requêtes préalables des clients du LAN. Le mécanisme CBAC permet la mise en place automatique et furtive d’ACL autorisant pendant un bref laps de temps le passage vers le LAN de paquets du WAN correspondant à des réponses à des requêtes effectuées peu de temps auparavant (de l’ordre de 1 à 2 secondes). Cette ACL est supprimée après le passage de la réponse (ou après le laps de temps max passé) de manière à éviter son exploitation par des réponses non-légitimes.



## 2. Tests des solutions

Vous devez organiser des tests unitaires et de non-régression pour chacun des dispositifs suivants :

* DMZ pour le serveur Web
* Politique de filtrage interne
* Firewall Stateful
* Mécanisme CBAC

Concernant les tests de non-régression, vous ferez en sorte que les dispositifs suivants (s’ils sont installés) ne soient pas affectés : IPSEC, RADIUS, DNS, ...

## 3. Productions

* Document synthétique de résultats des tests
* Fichier Packet Tracer comportant les mécanismes opérationnels