Rapport de Configuration – Cisco ASA Firewall

1. Introduction

Ce rapport présente la configuration de base d'un pare-feu Cisco ASA réalisée dans le cadre d'un laboratoire de formation. L'objectif est de mettre en place la configuration des interfaces, un serveur DHCP interne, ainsi que l'accès sécurisé via SSH.

2. Contexte du Laboratoire

Le laboratoire est composé d'un pare-feu Cisco ASA connecté à trois zones :
- **OUTSIDER** : Zone externe (Internet)
- **INSIDER** : Réseau interne de l'entreprise
- **DMZ** : Zone démilitarisée pour héberger des services publics

Le fichier .pkt fourni permet de visualiser et simuler cette configuration dans Cisco Packet Tracer.

3. Configuration des Interfaces

Interface	Nom (nameif)	Security-Level	Adresse IP	Masque
GigabitEthernet1/1	OUTSIDER	0	20.20.20.1	255.255.255.0
GigabitEthernet1/2	INSIDER	100	192.168.10.1	255.255.255.0
GigabitEthernet1/3	DMZ	70	10.10.10.1	255.255.255.240

4. Configuration du Serveur DHCP interne

- Plage d'adresses : **192.168.10.101 à 192.168.10.199** (INSIDER)
- DNS : **8.8.8.8**
- Activation : **dhcpd enable INSIDER**

5. Configuration SSH

- Authentification locale activée : aaa authentication ssh console LOCAL
- Autorisation des connexions SSH depuis le réseau interne : ssh 192.168.10.0 255.255.255.0 INSIDER
- Timeout : **3 minutes**
- Connexion : ssh -l ADM 192.168.10.1
- Identifiants :
  - Username : **ADM**
  - Password : **ADM123**

6. Résumé et Bonnes Pratiques

Cette configuration permet de sécuriser l'accès au pare-feu tout en distribuant des adresses IP automatiquement aux hôtes internes.
Pour améliorer la sécurité, il est recommandé de :
- Utiliser des mots de passe complexes

- Limiter encore davantage les plages IP autorisées pour SSH
- Mettre en place une ACL pour filtrer le trafic entre zones

7. Ressources Associées

- Fichier de configuration Packet Tracer : *LAB 17 CISCO ASA FIREWARE BASIC CONFIGURATION DHCP SSH.pkt*
- Fichier de notes : *NOTE.txt*