

Architecture Réseau Multi-Zones

Sécurité par Segmentation et Filtrage Zone-Based

1 Vue d'ensemble

Cette architecture réseau implémente une approche de sécurité par défense en profondeur (Defense in Depth) basée sur la segmentation en zones de confiance distinctes. Le principe fondamental repose sur le modèle **Zero Trust** : aucune zone ne fait implicitement confiance à une autre, et tout flux inter-zones doit être explicitement autorisé par le pare-feu central.

L'architecture se compose de cinq zones principales :

- **WAN** (Internet) : zone hostile externe
- **DMZ** : zone démilitarisée pour services publics
- **VPN** : accès distant sécurisé
- **LAN** : réseau interne d'entreprise
- **ADMIN** : zone d'administration et monitoring

2 Description des zones

2.1 Zone WAN – Internet Public

- **Rôle** : Représente l'Internet public et les utilisateurs externes
- **Niveau de confiance** : **AUCUN** (zone hostile)
- **Adressage** : 203.0.113.0/24
- **Équipements** :
 - wan-client (203.0.113.100) : utilisateur légitime
 - wan-attacker (203.0.113.200) : attaquant potentiel
- **Flux autorisés** : Accès HTTPS uniquement vers la DMZ (port 443)
- **Restrictions** : Aucun accès direct au LAN ou à l'administration

2.2 Zone DMZ – Services Publics

- **Rôle** : Héberge les services exposés sur Internet (zone sacrifiée)
- **Niveau de confiance** : **FAIBLE**
- **Adressage** : 172.16.1.0/24
- **Équipements** :

- web1 (172.16.1.10) : serveur Apache ACTIF
- web2 (172.16.1.11) : serveur Apache PASSIF (HA)
- VIP (172.16.1.100) : IP virtuelle pour haute disponibilité
- **Services exposés** : HTTPS (443), HTTP redirigé vers HTTPS
- **Caractéristiques** :
 - Cluster actif/passif avec basculement automatique (Heartbeat)
 - Ne peut pas initier de connexions vers le LAN
 - Administration SSH uniquement depuis la zone ADMIN

2.3 Zone VPN – Accès Distant Sécurisé

- **Rôle** : Point d'accès pour utilisateurs et administrateurs distants
- **Niveau de confiance** : **MOYEN** (après authentification)
- **Adressage** : 10.8.0.0/24
- **Équipement** : vpn-server (10.8.0.1) OpenVPN
- **Mécanisme** :
 - Authentification par certificats x509 (TLS)
 - Attribution dynamique d'IP (10.8.0.10-254)
 - Accès conditionnel selon profil utilisateur
- **Flux autorisés après connexion** :
 - Profil administrateur : accès à la zone ADMIN
 - Profil utilisateur : accès à la zone LAN

2.4 Zone LAN – Réseau Interne

- **Rôle** : Réseau d'entreprise, ressources internes sensibles
- **Niveau de confiance** : **ÉLEVÉ**
- **Adressage** : 192.168.10.0/24
- **Équipements** :
 - lan-client1/2 (192.168.10.10/11) : postes de travail
 - lan-server (192.168.10.50) : serveur interne
- **Restrictions strictes** :
 - Aucun accès direct depuis WAN ou DMZ
 - Accès Internet via NAT traversant le pare-feu
 - Consultation DMZ autorisée (lecture seule)
 - Accessible uniquement via VPN pour utilisateurs externes

2.5 Zone ADMIN – Administration et Monitoring

- **Rôle** : Gestion, administration et surveillance du réseau
- **Niveau de confiance** : **TRÈS ÉLEVÉ**
- **Adressage** : 192.168.100.0/24

- **Équipements** :
 - `admin-station` (192.168.100.10) : poste d'administration
 - `ids-server` (192.168.100.20) : système de détection d'intrusion (Snort)
- **Privilèges spéciaux** :
 - Administration SSH de toutes les zones
 - Monitoring complet du trafic réseau (IDS en mode promiscuous)
 - Corrélation des logs pare-feu et IDS
- **Contraintes de sécurité** :
 - Accès obligatoire via VPN préalable
 - Authentification par clés SSH uniquement (pas de mot de passe)
 - IP source restreinte

3 Pare-feu Central

Le pare-feu principal constitue le point de contrôle unique de l'architecture. Il implémente un **Zone-Based Policy Firewall (ZPF)** avec les caractéristiques suivantes :

- **Politique par défaut** : DENY ALL (tout trafic bloqué)
- **Filtrage stateful** : suivi des connexions TCP/UDP établies
- **Journalisation** : tous les flux bloqués sont enregistrés
- **Interfaces réseau** :
 - `eth0` (203.0.113.1) : vers WAN
 - `eth1` (172.16.1.1) : vers DMZ
 - `eth2` (10.8.0.1) : vers VPN
 - `eth3` (192.168.10.1) : vers LAN
 - `eth4` (192.168.100.1) : vers ADMIN

4 Matrice de flux inter-zones

Source → Dest.	WAN	DMZ	VPN	LAN	ADMIN
WAN	OK	HTTPS :443	NON	NON	NON
DMZ	Retour*	OK	NON	NON	NON
VPN	OK	~	OK	OK	Admin seul
LAN	NON	Lecture	NON	OK	NON
ADMIN	NON	SSH :22	OK	SSH :22	OK

TABLE 1 – Matrice de flux autorisés. OK = autorisé, NON = bloqué, ~ = conditionnel, *stateful

5 Mécanismes de sécurité

5.1 Segmentation réseau

Chaque zone opère sur un sous-réseau distinct avec des switches dédiés, éliminant toute communication directe inter-zones sans validation par le pare-feu.

5.2 Chiffrement des communications

- **HTTPS/TLS** : communications web chiffrées (certificats SSL)
- **SSH** : administration sécurisée avec authentification par clés RSA
- **OpenVPN/TLS** : tunnel VPN chiffré avec certificats x509

5.3 Détection d'intrusion (IDS)

Le serveur Snort surveille le trafic réseau en temps réel et détecte :

- Scans de ports (Nmap, reconnaissance)
- Tentatives de brute-force SSH
- Attaques applicatives (SQL injection, XSS, RCE)
- Anomalies de trafic

5.4 Haute disponibilité

Le cluster web actif/passif avec IP virtuelle (VIP) assure la continuité de service en cas de défaillance du serveur principal. Le mécanisme Heartbeat détecte les pannes et bascule automatiquement le trafic.

6 Conclusion

Cette architecture implémente les principes de sécurité fondamentaux :

- **Zero Trust** : aucune confiance implicite entre zones
- **Defense in Depth** : multiples couches de protection
- **Least Privilege** : accès minimum nécessaire
- **Fail Secure** : politique de blocage par défaut

Elle garantit une séparation stricte entre ressources publiques (DMZ), internes (LAN) et critiques (ADMIN), tout en maintenant la traçabilité complète des flux via journalisation centralisée et corrélation IDS.