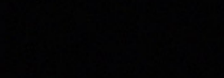
Les fondamentaux

Présentation de la menace

Schéma d'une attaque

INTERNET

INTRANET



DMZ

CIBLE

Serveurs

Clients

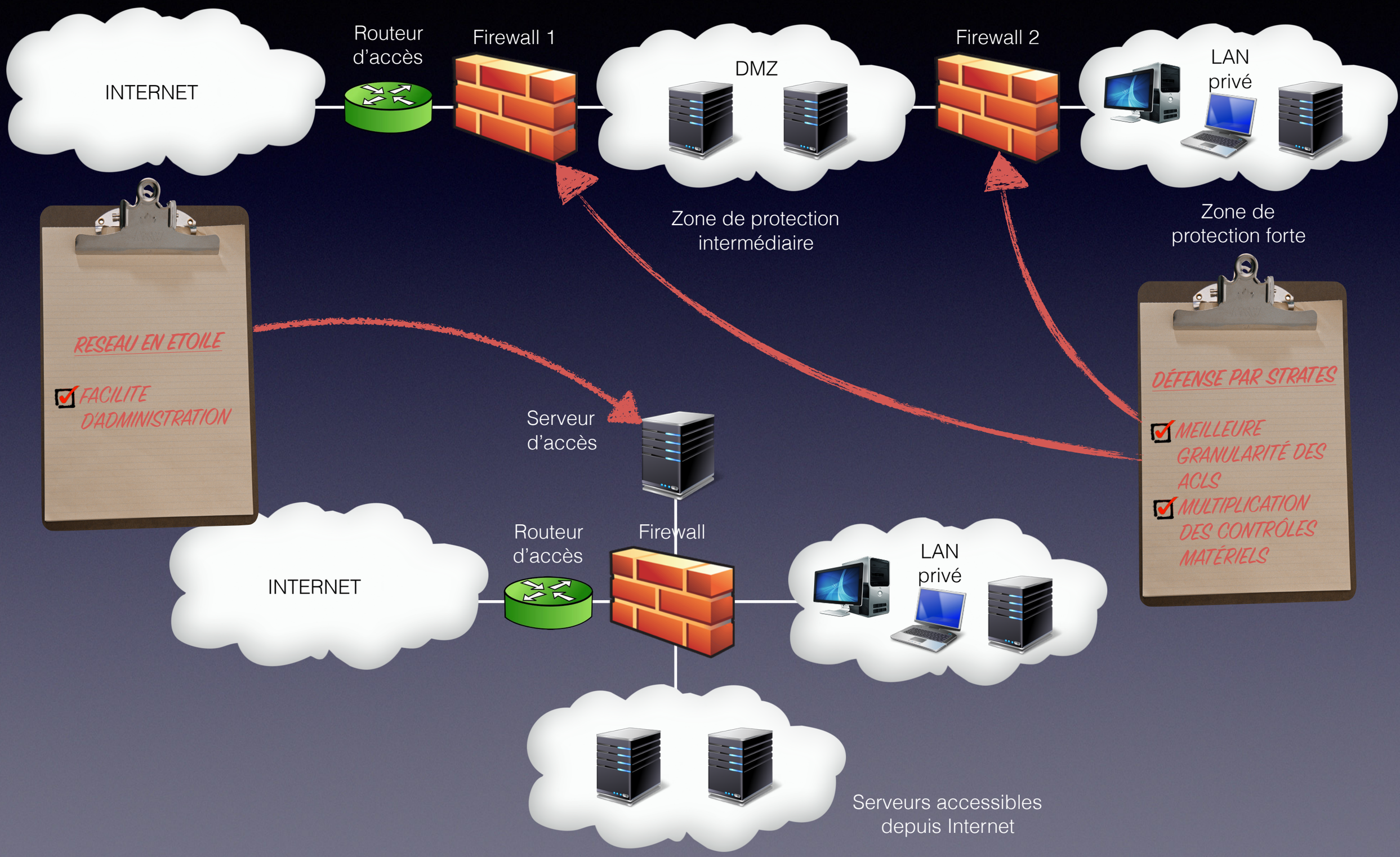
MENACE EXTERNE

ATTAQUE MENÉE PAR UN INDIVIDU ISOLÉ OU PAR UN GROUPE POTENTIELLEMENT PUISSANT ET ORGANISÉ

MENACE INTERNE

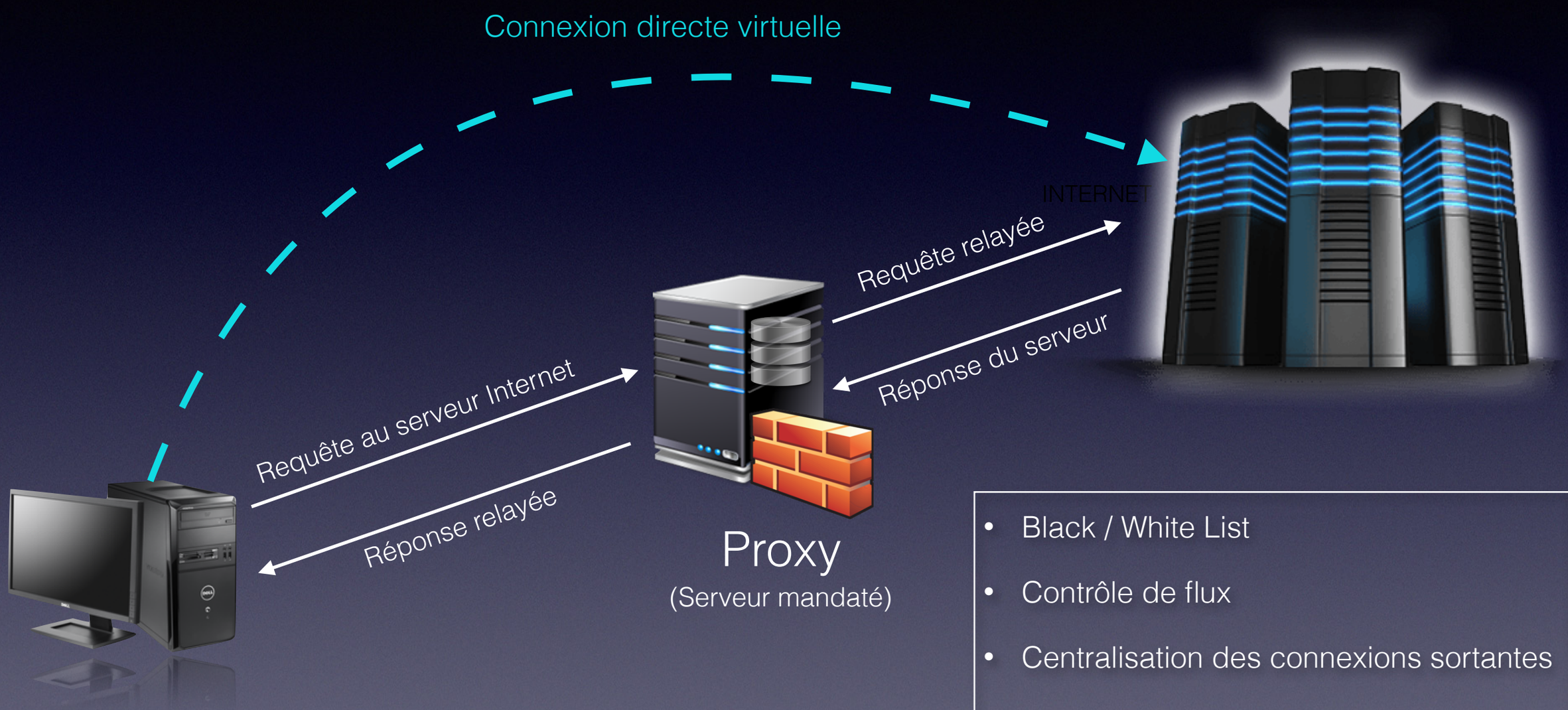
ATTAQUE MENÉE VOLONTAIREMENT (OU PAS) DEPUIS UN POSTE CLIENT OU TOUT AUTRE MACHINE DU SI INTERNE

Types d'architecture



Système de défense

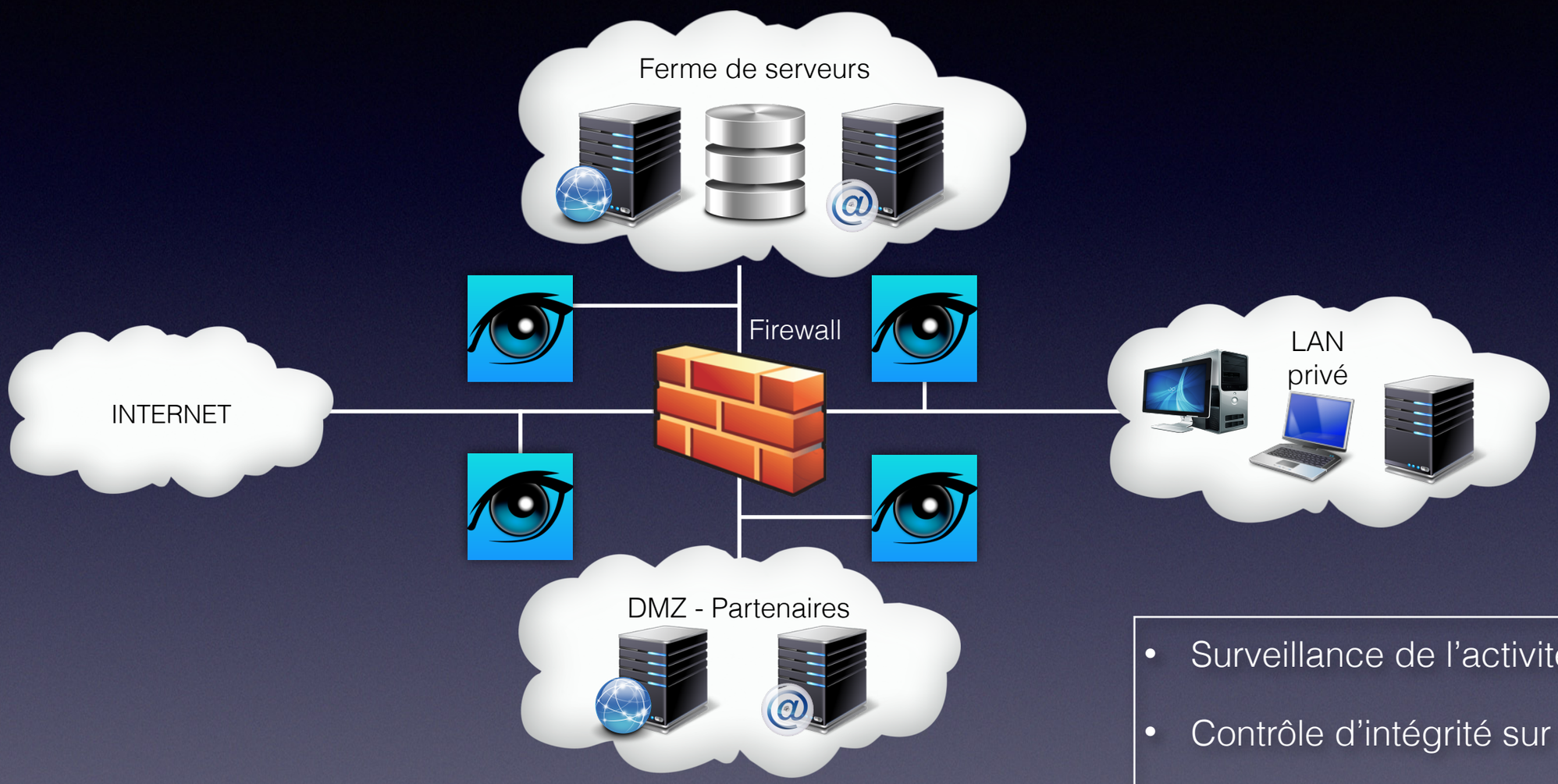
Proxyfication



- Black / White List
- Contrôle de flux
- Centralisation des connexions sortantes
- Log
- **Pas une sécurité en soi**

Système de défense

NIDS & HIDS



- Surveillance de l'activité sur le réseau
- Contrôle d'intégrité sur les postes clients
- Remontés d'alarmes
- Modification active des ACLs sur le réseau
- Ligne de défense en profondeur

Schéma d’une attaque

INTERNET

INTRANET

DMZ

CIBLE

Serveurs

Clients

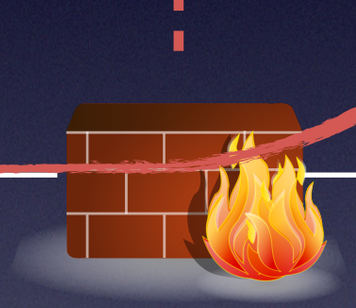
1. Identification de la cible

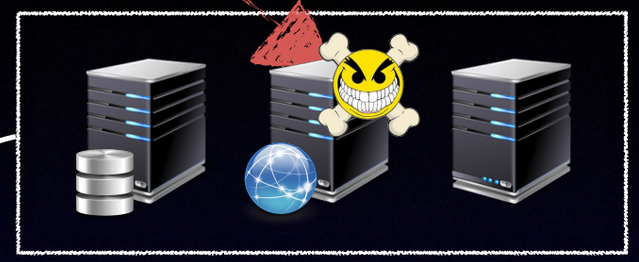
- ✓Recherche d’informations en sources ouvertes
- ✓Social Engineering
- ✓Prise d’empreinte des systèmes
- ✓Recherche de vulnérabilités

Schéma d’une attaque

INTERNET

INTRANET





DMZ

CIBLE

Serveurs

Clients

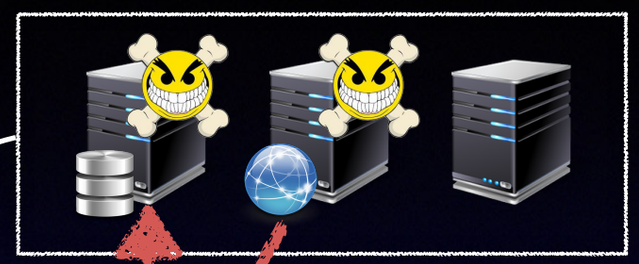
2. Intrusion de la cible

- ✓Exploitation des informations collectées
- ✓Intrusion d’un serveur web accessible par Internet
- ✓« Pillage » de la machine
- ✓Pérennisation

Schéma d’une attaque

INTERNET

INTRANET



DMZ

CIBLE

Serveurs

Clients

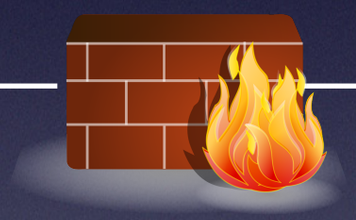
3. Rebond dans la DMZ

- ✓Analyse de l’environnement immédiat
- ✓Propagation au sein de la DMZ

Schéma d’une attaque

INTERNET

INTRANET



DMZ

CIBLE

Serveurs

Clients

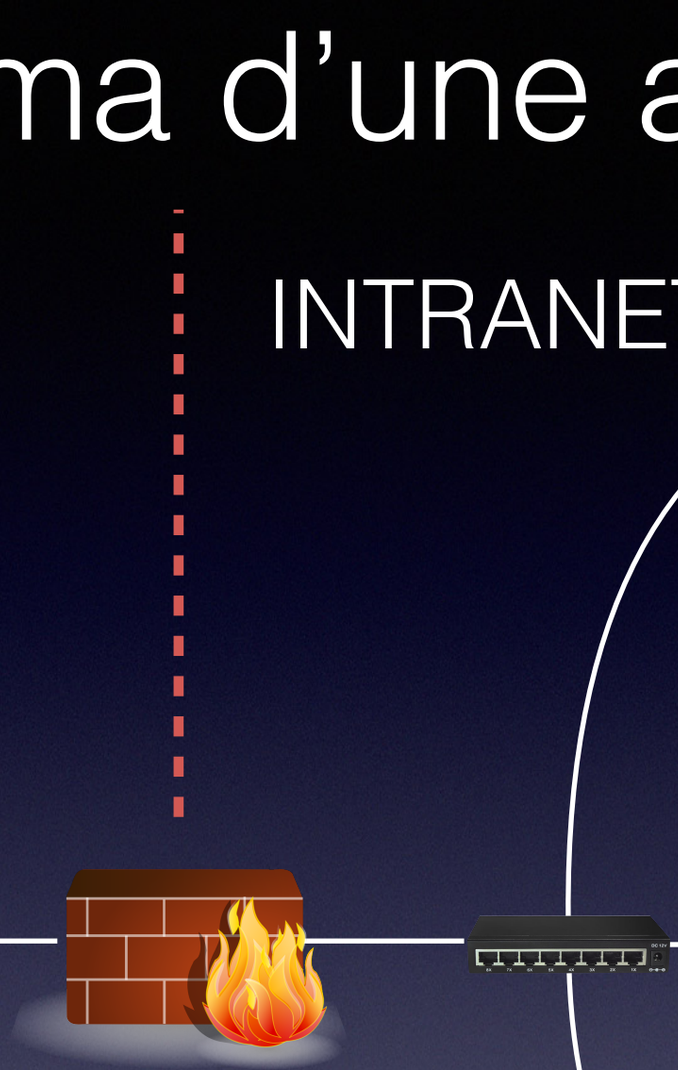
4. Piégeage d’un utilisateur

- ✓Piégeage du site Web
- ✓Piégeage via serveur Mail
- ✓Compromission d’un poste Utilisateur
- ✓Pillage du poste
- ✓Pérennisation

Schéma d’une attaque

INTERNET

INTRANET



DMZ

CIBLE

Serveurs

Clients

5. Récupération de données d’authentification

- ✓Propagation au sein des postes Utilisateurs
- ✓Analyse des échanges (mail…)
- ✓Piégeage du poste (Keylogger)
- ✓Dump de la base SAM
- ✓Récupération des mots de passe stockés localement
- ✓Connexion au coeur du réseau grâce aux données collectées

Questions ?