Monter un réseau d'administration

Guide et bonne pratiques

Groupe 14

01

Introduction

Enjeux, contexte et généralité

Enjeux

- Ressources d'administration = **cibles privilégiées**

- Ressources d'administration:
  - **Postes** d'administration
  - **Outils** d'administration *(ex: portail web de configuration)*
  - **Infrastructures** d'administration *(ex: concentrateur VPN)*
  - **Administrateurs**

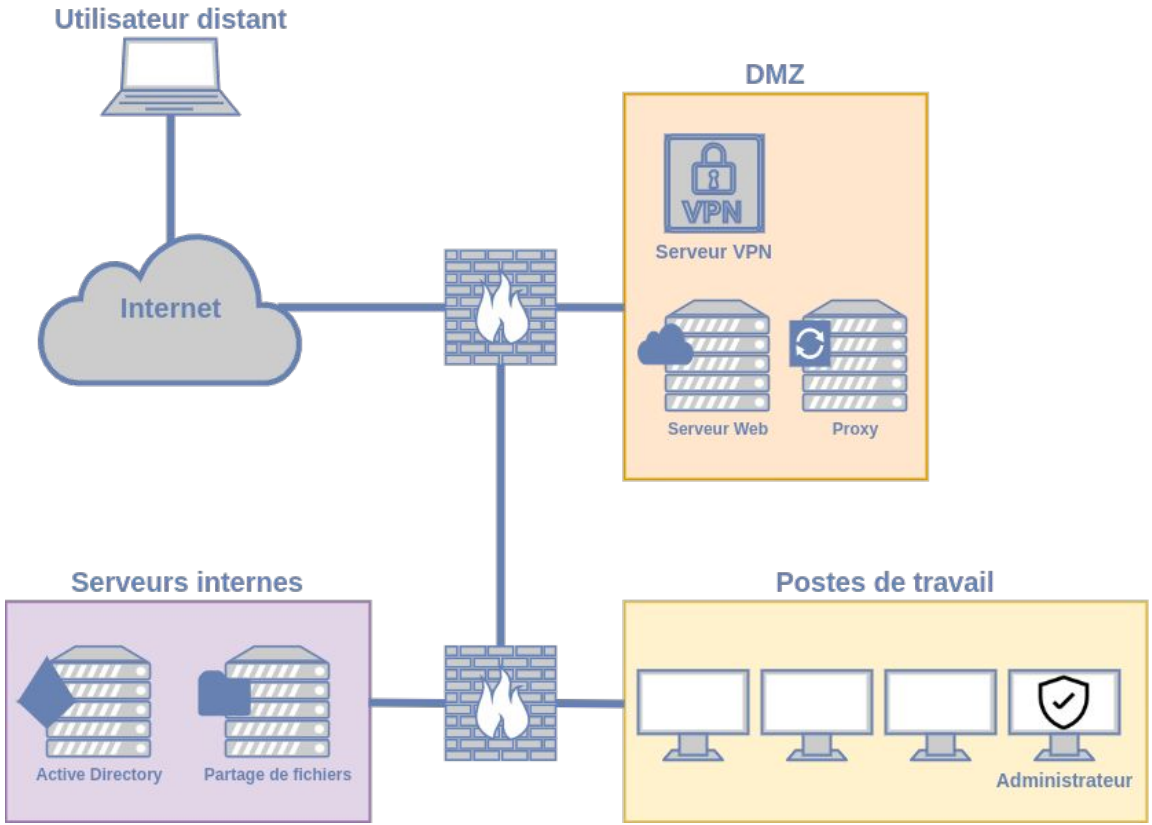
- Protection du SI d'administration et du SI administré

Actions d'administration:

Ensemble des actions d'installation, de suppression, de modification et de consultation de la configuration d'un système participant au SI et susceptible de modifier le fonctionnement ou la sécurité de celui-ci.

Contexte

- **Exemple** d'un SI fictif
- Mise en application **progressive**
- **Pas de solution unique** de construction de réseau !



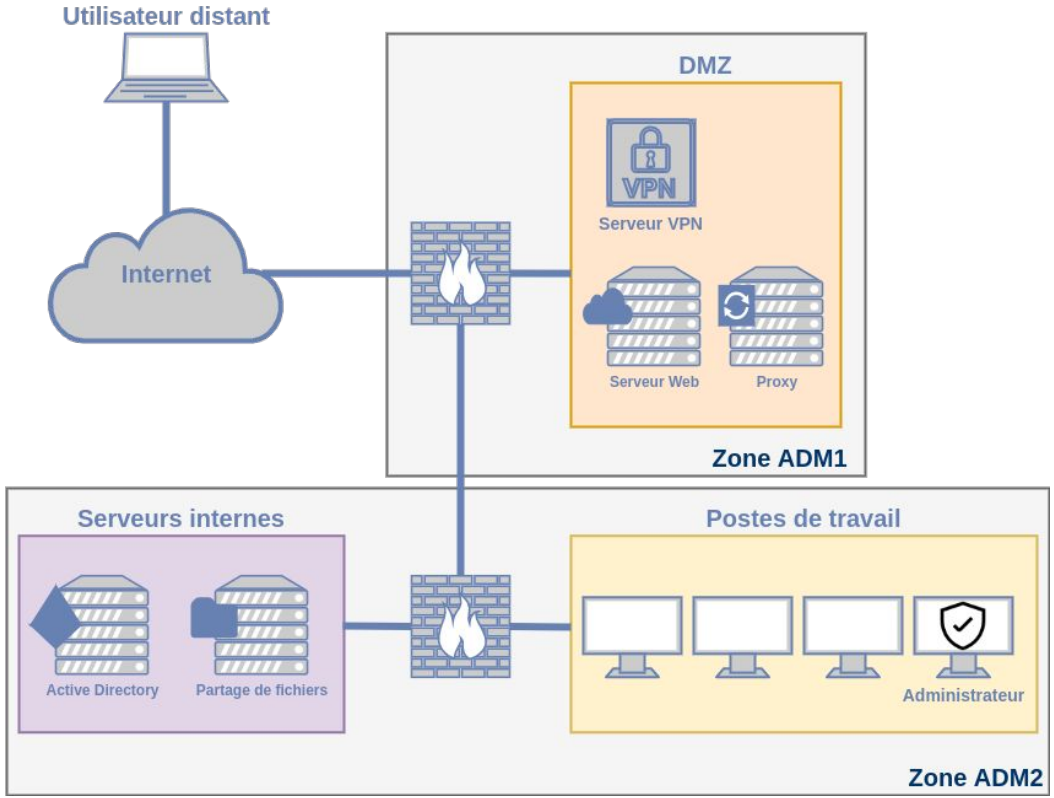
Généralités

- **Analyse** de risque du SI d'administration ( tous les ans)
- **Découpage** en zone homogènes ( changements majeurs)
- Critères d'homogénéité:
  - Criticité métier
  - Organisationnel *(ex: administration interne ou externe)*
  - Exposition
  - Réglementation *(ex: PCI-DSS, données médicales)*
  - Zones géographiques
- **Cloisonnement** de ces zones *(filtrage, chiffrement, authentification)*

Zones

- Exemple d'**identification de zones**
  - Zone ADM1 pour les **serveurs exposés**
  - Zone ADM2 pour les **machines internes**

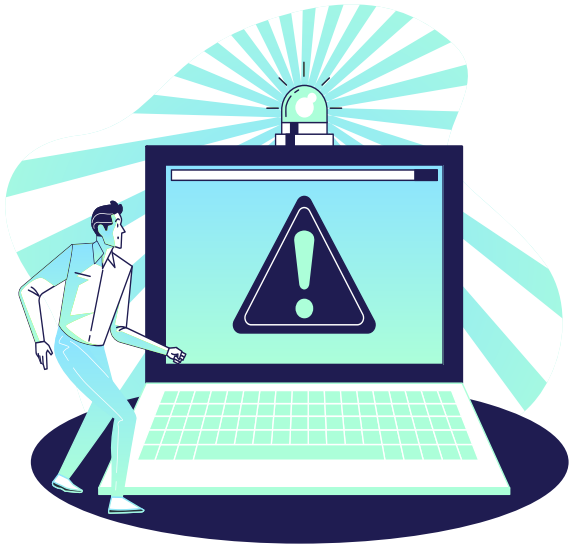
- Zones administrées par **groupes d'admin différents**



02 Postes d'administrations

Administrateurs, cas d'usage et procédures de sécurisation

Poste d'administration



- Accès étendus et privilégiés → **Composant critique** du SI
- Traite des **informations sensibles** pour le SI (configurations, mots de passe, dossiers d'architecture…)
- Nécessite une **sécurisation physique** et logicielle pour éviter toute compromission
- L'entité doit garder la maîtrise sur le poste d'administration → **pas de BYOD**

Administrateurs

- Peut être interne ou externe *(employé ou sous-traitant)*
- **Loyauté**, **transparence** et **confidentialité**
- Charte informatique à faire signer
- **Formation** initiale et continue
- Sensibilisation à la protection physique du poste

Poste d'administration : Architecture

- Les administrateurs ont deux comptes : **privilégié** et **standard**
- Plusieurs options pour assurer la séparation des comptes :

  - Un poste d'administration **dédié**
    - *Poste pour les actions administrateurs et poste pour les actions utilisateurs*
  - Un poste d'administration **multi-niveaux**
    - *Deux environnements virtuels sur le même poste physique*
  - Un poste d'administration avec **accès distant** au SI bureautique
    - *Usage d'un poste d'administration avec accès au SI bureautique par connexion à distance*

Poste d'administration : Sécurisation

- Blocage des accès internet
  - *Sauf IP VPN en cas de nomadisme*
  - *Serveur relais pour les mises à jour*

- Sécurisation logicielle *(notamment Linux et Windows)*
  - *Désactivation des services inutiles*
  - *Applications des droits restreints*
  - *Activation du pare-feu local*
  - *Durcissement de configuration système*
  - *Activation des mécanismes de mise à jour*
  - *Chiffrement et filtre écran obligatoires en cas de nomadisme !*

- Pas de droit d'administration sur la machine !

- Liste et analyse antivirale des binaires

03 Réseaux d'administration

Zones d'administration, composants et sécurisation

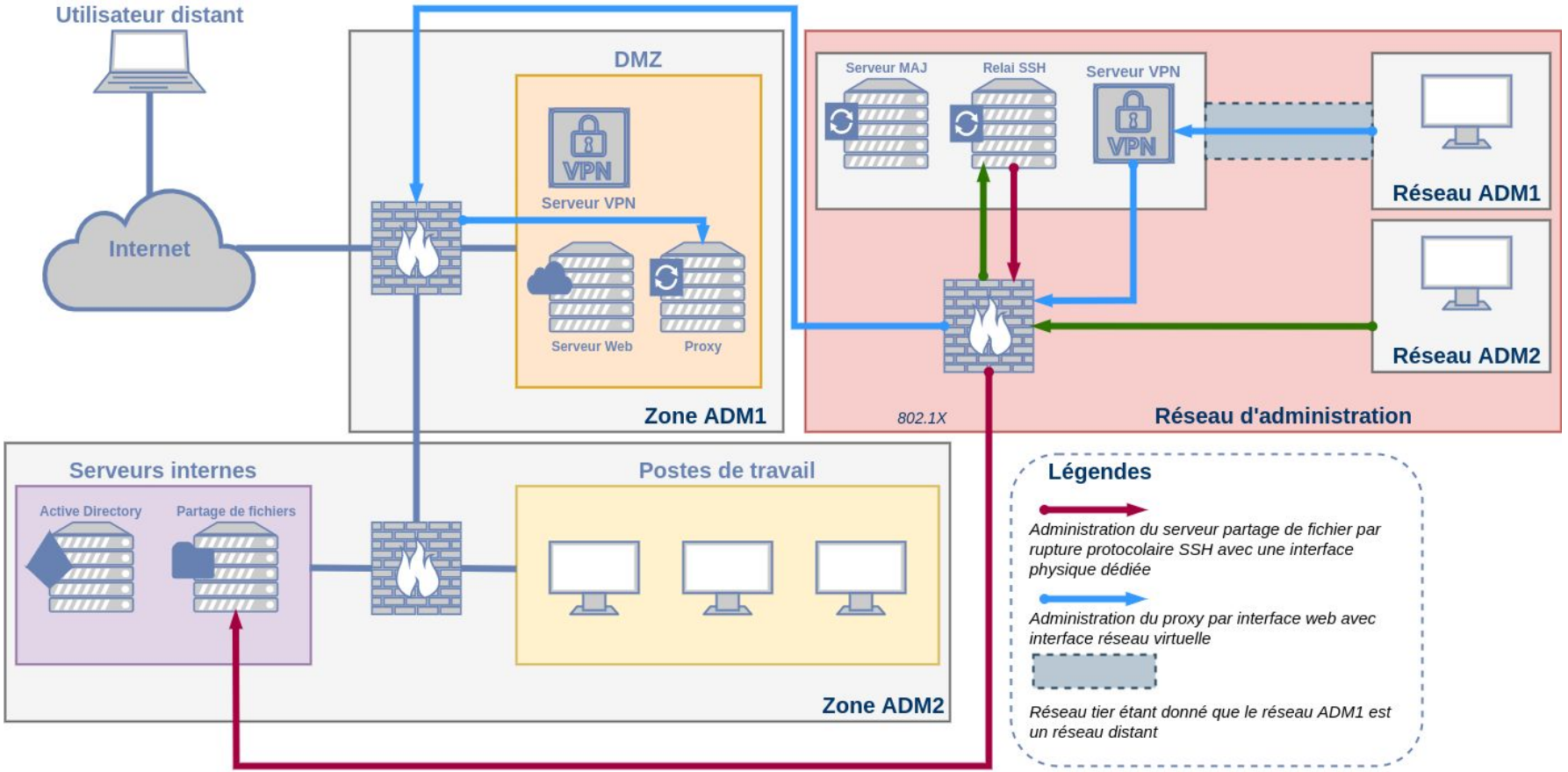
Réseaux d'administration

- Contient toutes les ressources d'administration
- Réseaux **physiques** dédiés, **à minima logique** *(VLAN, IPsec)*
- Authentification **802.1X** en protection des branchements
- **Filtrage** réseau **intra admin** entre les zones de confiance
- **Filtrage** réseau **vers la zone administrée**
- Protocoles avec **chiffrement et authentification** *(sinon IPsec)*

Ressources administrées

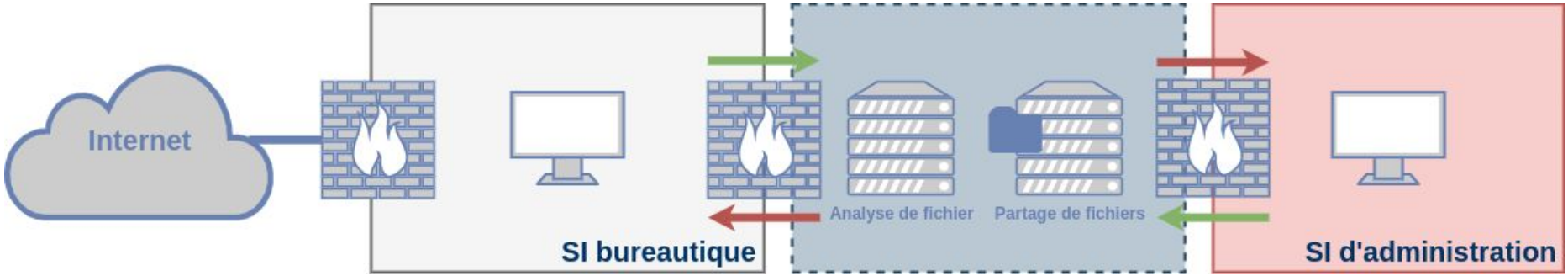
- **Interface réseau** d'administration **dédiée** *(physique ou logique)*
- Autorisation **seulement** de **connexion entrante** *(sauf sortie syslog)*
- Interdire les communications entre les ressources administrées
- Possible d'effectuer des **ruptures protocolaires**
  - Améliore la journalisation et la traçabilité
  - Coupe la confiance de bout en bout d'une connexion sécurisée
- Utilisation **IPsec** si le flux passe par un **réseau tier** *(ex: multi site)*

Exemple de réseau d'administration avec flux d'administration



Système d'échange de fichier

- Il peut être nécessaire de vouloir **échanger des fichiers** entre deux zones
  - *Documentations, fichiers de configuration…*
- Zone d'échange de fichiers avec **autorisation unilatérale**
- **Suppression périodique** des fichiers (tous les jours)



04
Comptes d'administration

Identification, authentification, droits, journalisation et sauvegarde

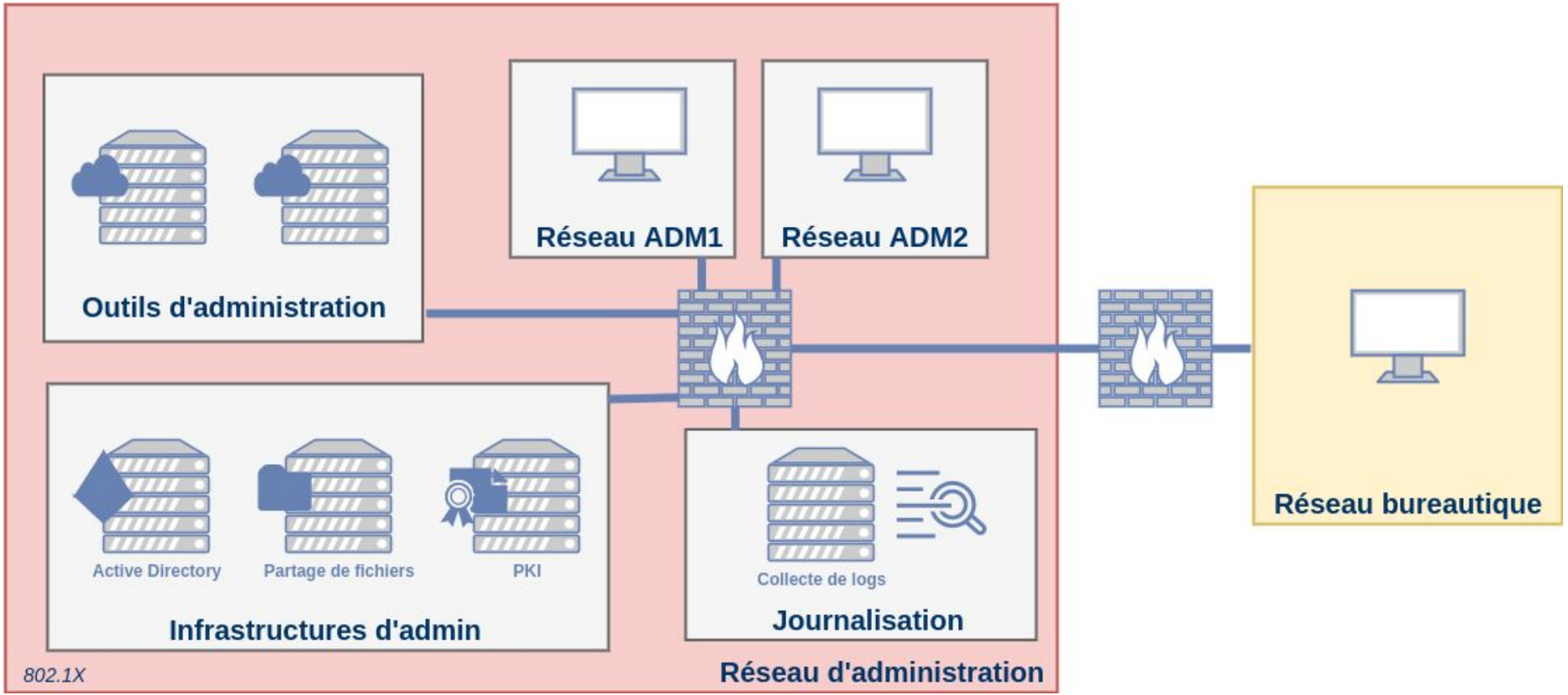
Comptes d'administration

- **Annuaire dédié** et **sécurisé** pour les comptes d'administration
- Utilisation de **comptes d'administration dédiés**
- **Mots de passe différents** entre tous les comptes
- Restrictions des comptes admin pour actions bureautiques *(bloquer sessions)*
- **Pas d'utilisation de compte natifs** et modification de leurs mots de passe
- Utilisation d'un **coffre-fort** de mots de passe

Comptes d'administration

- Convention de nommage *(ex: adm-cmartin, adm-0x234, …)*
- **Journalisation** des actions administrateurs
  - *Ouverture/Fermeture de session*
  - *Échec d'authentification*
  - *Gestion des comptes*
  - *Gestion des groupes de sécurité*
- **Processus organisationnel** de gestion de compte
- Authentification **double facteur**
- **Centralisation** de tous les comptes *(coffre fort de mot de passe)*
- Politique de sécurité et principe du **moindre privilège**

Composition d'un réseau d'administration complet



05 Administration externe

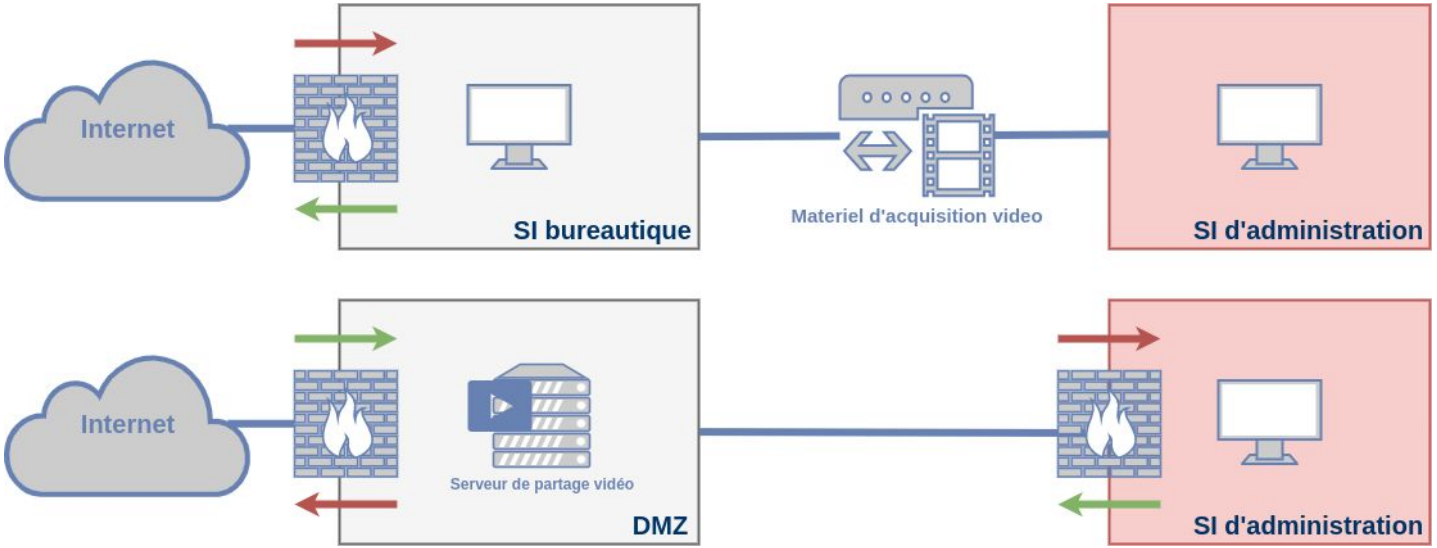
Prestataires et télé-assistance

Prestataires

- Différence entre l'administration par des tiers et la téléassistance
  - **Administration** : exécution d'action d'administration par **admin externe**
  - **Téléassistance** : assistance d'un **admin interne** par partage d'écran
- Risque d'attaque par la **chaîne d'approvisionnement**
- Acteurs qualifiés par l'ANSSI : qualification **PAMS**
- Concentrateur VPN *(IPsec)* dédié, distinct des administrateurs internes
- Création de **comptes dédiés** *(si possible annuaire dédié)*
- Imposer la **sécurité des postes**, contrôler et tracer les accès
  - *Processus organisationnel pour activation de comptes*
  - *Serveur de rebond temporaire (eteindre en fin de journée)*

Téléassistance

- Deux méthodes possibles:
  - *Utilisation d'un boitier d'acquisition vidéo faisant le lien admin - bureautique*
  - *Mise en place d'un serveur dédié pour le partage de vidéo*
- Dans le deuxième cas, il faut désactiver les options de contrôle à distance



06

Conclusion

Ressources et maintien en condition de sécurité

Conclusion

- La mise en place d'un réseau d'administration dépend de l'entité
  - *Choix de compromis selon les ressources disponibles*
  - *Dimensionnement selon la taille du SI*
  - *Choix des différents modes d'administration*
- Mise à jour de **sécurité** et **veille technologique** nécessaire en continu
- La passerelle de mise à jour doit être:
  - *Dédiée au SI d'administration*
  - *Isolée d'internet*
  - *Doit avoir un filtrage des URLs autorisés*
  - *Vérification d'intégrité et d'authenticité des fichiers*
- Plateforme de test avec validation des correctifs

RESSOURCES

- Recommandations relatives à l'administration sécurisé des systèmes d'information – ANSSI
- Recommandations de sécurité relative à la téléassistance – ANSSI
- Référentiel Général de Sécurité (RGS)
- Recommandations pour un usage sécurisé d'OpenSSH– ANSSI
- Méthode EBIOS – ANSSI
- Points de contrôle Active Directory – ANSSI
- Recommandations de sécurité relative à un système GNU/Linux – ANSSI
- Recommandations de déploiement du protocole 802.1X pour le contrôle d’accès à des réseaux locaux
- Recommandations de sécurité relatives à IPsec pour la protection des flux réseau