Windows et Active Directory

Maintien en condition de sécurité

Firewall

Administration sécurisée

SR v2019

Windows et Active Directory

Maintien en condition de sécurité

SR v2019

MCS
Généralités

- Afin de garantir le MCS du système, il est nécessaire de garantir au minimum l'application des correctifs de sécurité du système et de l'ensemble des applications

- Cela nécessite de
  - Veiller aux alertes de sécurité publiées par l'éditeur (Microsoft Security Response Center - MSRC) ou un CSIRT (Computer Security Incident Response Team (ex : CERT-FR)
  - Disposer des mises à jour
  - Déployer les mises à jour
  - Contrôler l'application des mises à jour

MCS

Windows Update : types de mises à jour

- **Critical Update** : problème spécifique, critique et non lié à la sécurité
- **Security Update** : problème spécifique lié à la sécurité
- **Security-Only Quality Update** : regroupement de toutes les nouvelles mises à jour de sécurité pour un mois donné et pour un produit donné
- **Update** : problème spécifique, non critique et non lié à la sécurité
- **Feature Pack** : Ajout de nouvelles fonctionnalités
- **Update Rollup** : Regroupement de hotfixes, critical updates, security updates et updates
- **Monthly Rollup** : Ensemble de mises à jour cumulatives mensuelles
- **Service Pack** :
  - Regroupement de tous les hotfixes, critical updates, security updates et updates
  - Corrections diverses
  - Ajout de nouvelles fonctionnalités

MCS

Windows Update : types de mises à jour

- **Definition Update** : Anti-virus, sites web malveillants, anti-spam
- **Tool** : Utilitaire ou fonctionnalité
- **Driver** : Pilote

- Windows 10
  - SAC – Semi-Annual Channel ≠ LTSC – Long Term Servicing Channel
  - Service Update
    - Regroupement cumulatif de correctifs de sécurité et de mises à jour
    - 1 par mois
  - Feature Update
    - Nouvelle version de Windows 10
    - Ajout de fonctionnalités
    - Distribuée sous forme d'une installation complète du système
    - 1 à 2 par an

MCS

Windows Update : Bulletin de sécurité et article KB

Exploitability Assessment

The following table provides an exploitability assessment for this vulnerability at the time of original publication.

Publicly Disclosed	Exploited	Latest Software Release	Older Software Release	Denial of Service
Yes	No	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not Applicable

Affected Products | CVSS Score

Affected Products

The following software versions or editions are affected. Versions or editions that are not listed are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, see the Microsoft Support Lifecycle.

Product ▲	Platform	Article	Download	Impact	Severity	Supersedence
Windows 10 Version 1709 for 32-bit Systems		4093112	Security Update	Security Feature Bypass	Important	4088776
Windows 10 Version 1709 for x64-based Systems		4093112	Security Update	Security Feature Bypass	Important	4088776
Windows Server, version 1709 (Server Core Installation)		4093112	Security Update	Security Feature Bypass	Important	4088776

MCS

Windows Update : cycle de vie

- 10 ans de support
  - Support principal
    - minimum 5 ans
  - Support étendu
    - minimum 5 ans

Type of support	Mainstream support phase	Extended support phase	Self-help online support
Request to change product design and features	✓	✗	
Security updates	✓	✓	
Non-security updates	✓	☆	Access to freely available online content, such as Knowledge Base articles, online product information, and online support WebCasts
Complimentary support[1] included with license, licensing program[2] or other no-charge support programs	✓	✗[3]	
Paid-support (including pay-per-incident Premier and Essential Support)	✓	✓	

✓ Available ✗ Not available ☆ Only available with Extended Hotfix Support Not available for Desktop Operating System consumer products

*Please Note: Microsoft's Support Lifecycle Policy does not apply to all products. To see the specific support start and end dates by applicable product, you can search the Support Lifecycle Product Database.

[1] Refers to phone support and online support options.

[2] For example, support incidents acquired through the Software Assurance program for server products.

[3] Limited complimentary support may be available (varies by product).

MCS

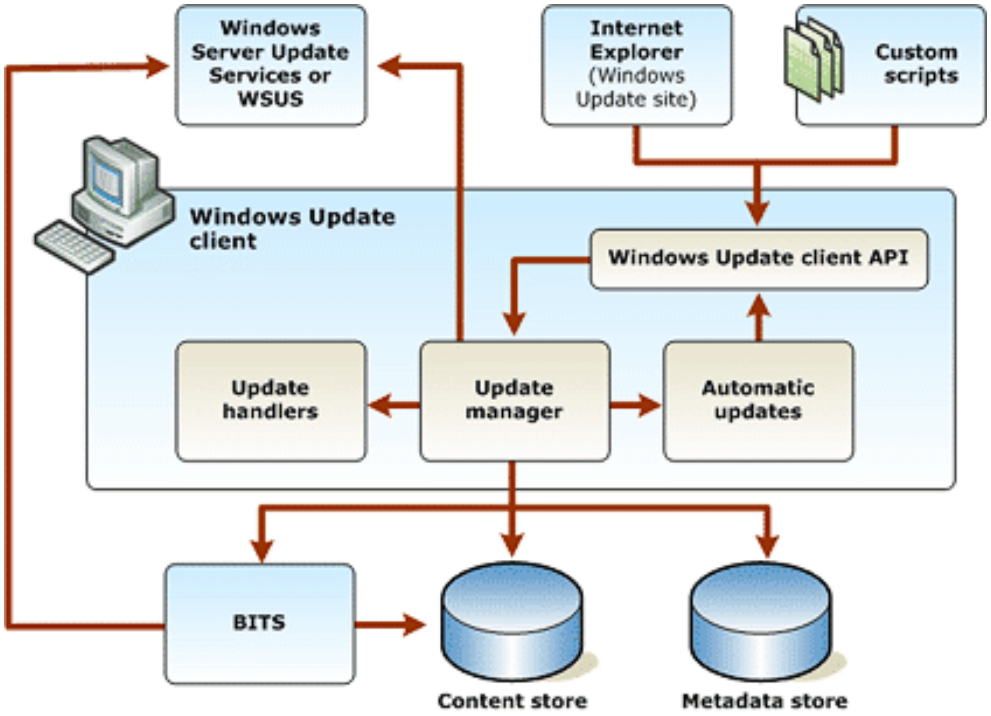
Windows Update : cycle de vie

Produit	Disponibilité	Dernier Service Pack	Fin de support principal	Fin de support étendu
Windows Server 2003	28/05/2013	13/03/2007	13/07/2010	14/07/2015
Windows Server 2003 R2	05/03/2006	13/03/2007	13/07/2010	14/07/2015
Windows Server 2008	06/05/2008	29/04/2009	13/01/2015	14/01/2020
Windows Server 2008 R2	22/10/2009	22/01/2011	13/01/2015	14/01/2020
Windows Server 2012	30/10/2012		10/09/2018	10/10/2023
Windows Server 2012 R2	25/11/2013		10/09/2018	10/10/2023
Windows Server 2016	15/10/2016		11/01/2022	11/01/2027
Windows XP	31/12/2001	21/04/2008	14/04/2009	08/04/2014
Windows Vista	25/01/2007	29/04/2009	10/04/2012	11/04/2017
Windows 7	22/10/2009	22/02/2011	13/01/2015	14/01/2020
Windows 8	30/10/2012			12/01/2016
Windows 8.1	13/11/2013		09/01/2018	10/01/2023
Windows 10	29/07/2015			14/10/2025
Windows 10 Enterprise 2015 LTSB	29/07/2015		13/10/2020	14/10/2025
Windows 10 Enterprise 2016 LTSB	02/08/2016		12/10/2021	13/10/2026
Windows 10 version 1507	29/07/2015		09/05/2017	
Windows 10 version 1511	10/11/2015		10/10/2017	November Update
Windows 10 version 1607	02/08/2016		10/04/2018	Anniversary Update
Windows 10 version 1703	11/04/2017		09/10/2018	Creators Update
Windows 10 version 1709	17/10/2017		09/04/2019	Fall Creators Update
Windows 10 version 1803	30/04/2018		12/11/2019	April 2018 Update
Windows 10 version 1809	13/11/2018		12/05/2020	Redstone 5

MCS

Windows Update : architecture

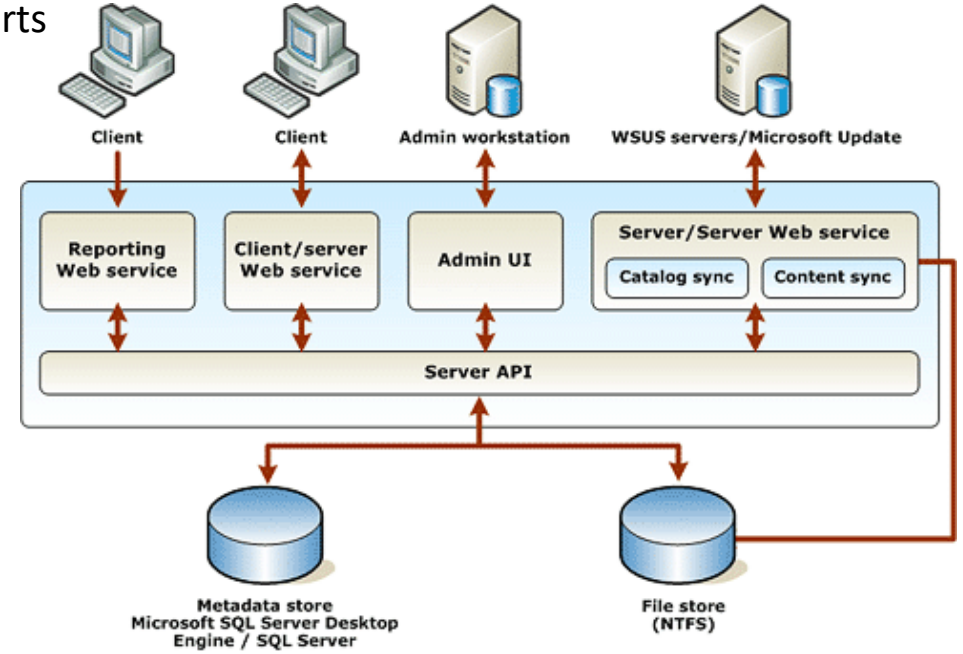
- WUA (Windows Update Agent)
  - Détermine les mises à jour nécessaires, les télécharge depuis des sites Microsoft Update ou un serveur WSUS (Windows Server Update Services)
  - Service Windows Update (WUAUSERV)
  - %WINDIR%\SOFTWAREDISTRIBUTION



MCS

Windows Update : architecture

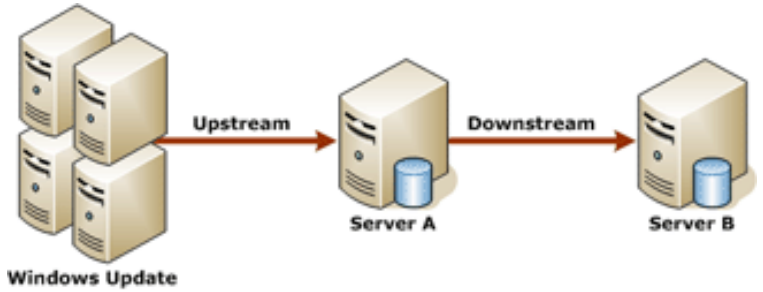
- Serveur de déploiements
  - Microsoft Update
    - Postes isolés et connectés à Internet
  - WSUS (Windows Server Update Services)
    - Sélection des mises à jour et du déploiement par groupes de clients
    - Inventaire des clients et du déploiement des mises à jour
    - Génération de rapports



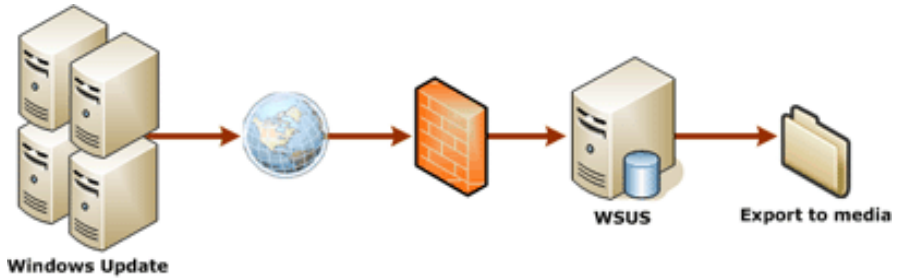
MCS

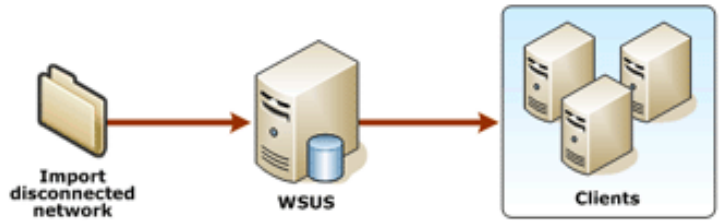
Windows Update : architecture

- Serveur de déploiements
  - WSUS (Windows Server Update Services)
    - Cascades de serveurs



    - Mode déconnecté





MCS
Windows Update : architecture

- Autres outils
  - Outil d'installation en « mode autonome » : wusa.exe
  - SCCM - System Center Configuration Manager
    - Produit payant
    - Gestion de grands parcs
    - Fonctions supplémentaires :
      - Gestion des correctifs
      - Inventaire matériel et logiciel
      - Prise de main à distance
      - Télédistribution d'application
  - MBSA – Microsoft Baseline Security Analyzer
    - Analyse de l'état de sécurité du système jusqu'à Windows 8.1 et Server 2012 R2
    - Guide dans la remédiation
    - Mode offline ou inline
    - Compatible MU, WSUS, SMS, SCCM

MCS
Antimalware

- Antimalware nécessaire (?) mais non suffisant

- Microsoft Windows Defender AntiVirus
  - Windows 8.1 et Windows 10
    - Disponible et activé par défaut
  - Windows Server 2012 R2
    - Disponible et activé uniquement en Server Core
    - Endpoint Protection with Configuration Manager (SCCM)
  - Windows Server 2016
    - Fonctionnalité à activer

MCS
Antimalware

- Configuration via
  - SCCM
  - Microsoft Intune
  - PowerShell
  - Windows Management Instrumentation (WMI)
  - Group Policy
- Quelques caractéristiques
  - Protection fournie par le cloud
  - Protection en temps réel
  - Mises à jour de protection dédiées
    - analyses BigData humaines et automatisées
    - machine-learning
    - recherche approfondie de résistance aux menaces

Windows et Active Directory

Firewall

SR v2019

FIREWALL

Windows Filtering Platform

- WFP a été introduit avec Windows Vista
- WFP permet en particulier :
  - La classification et le filtrage de paquets réseau (pare-feu, IDS, etc.)
  - La modification de paquets réseau (IPsec)
- WFP permet de filtrer selon les critères suivants :
  - Étendue : IP sources / IP destinations
  - Type d'interface réseau (local, distant, sans-fil)
  - Protocole / Port local / Port distant / Type ICMP
  - Programme
  - Service
  - Package d'application
  - Profil réseau (Public, Privé, Domaine)
  - Utilisateur

FIREWALL

Windows Filtering Platform

- Quelques fonctions de WFP
  - Fournit une infrastructure de filtrage de paquets dans laquelle les éditeurs de logiciels indépendants peuvent connecter des modules spécifiques de filtrage.
  - Fonctionne avec IPv4 et IPv6.
  - Fournit une sécurité au démarrage jusqu'à ce que le moteur de filtrage de base (BFE) puisse démarrer.
  - Gère le filtrage de connexion avec état et réassemblages de paquets.
  - Permet l'intégration des stratégies de filtrage IPsec et pare-feu.

Windows et Active Directory

Administration sécurisée

SR v2019

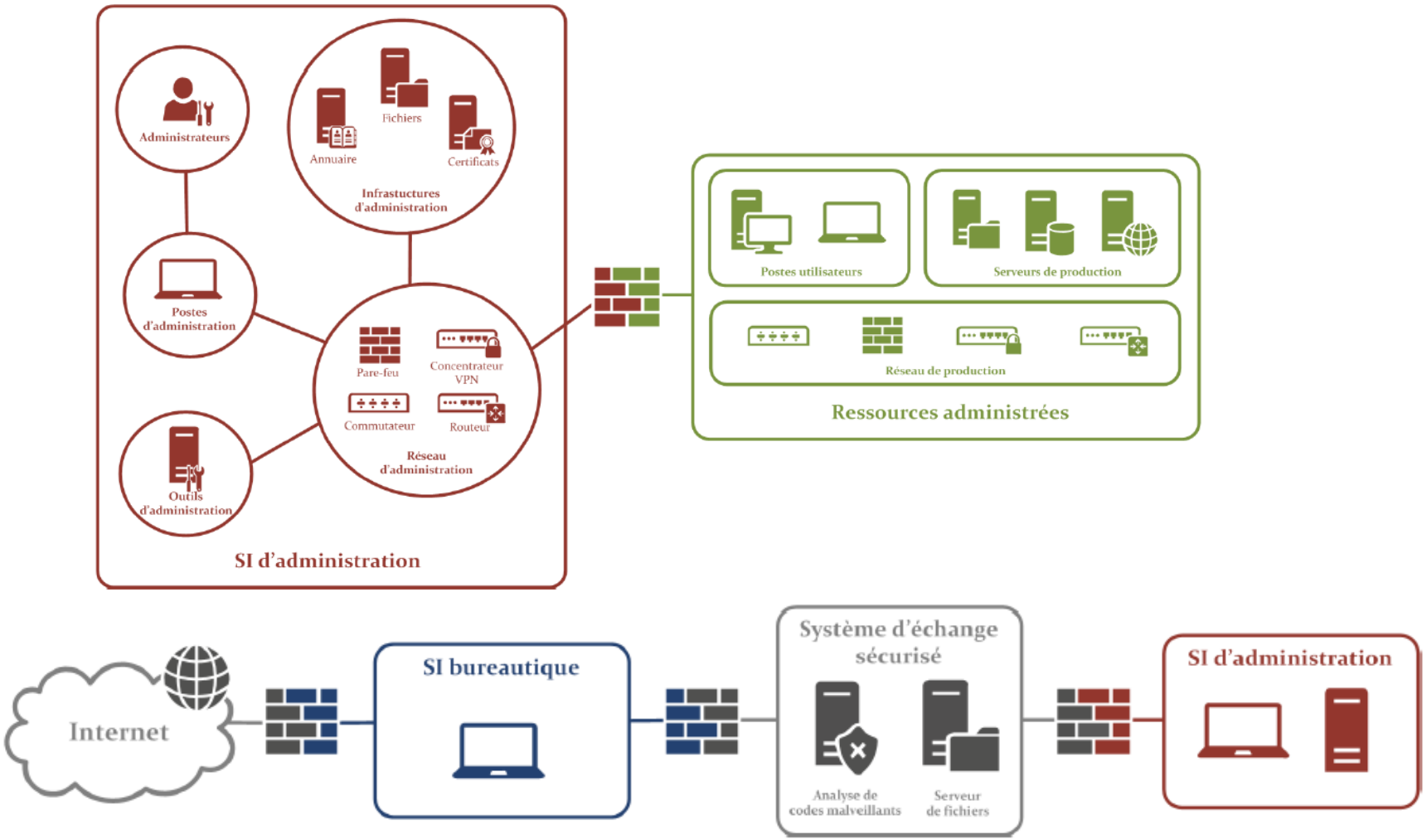
ADMINISTRATION SÉCURISÉE

Concepts de base

- Les recommandations suivantes sont extraites du guide de l'ANSSI « Recommandations relatives à l'administration sécurisée des systèmes d'information » du 24/04/2018.
- Définition : 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 susceptibles de modifier le fonctionnement ou la sécurité de celui-ci.
- Recommandations de base :
  - Création d'un compte utilisateur standard pour utiliser le SI hors administration et d'un ou plusieurs comptes d'administration dédiés aux actions d'administration
  - Un poste fixe ou portable utilisé pour les actions d'administration, dénommé poste d'administration (pas de poste personnel)
  - Un système d'information d'administration s'appuyant sur un réseau d'administration

ADMINISTRATION SÉCURISÉE

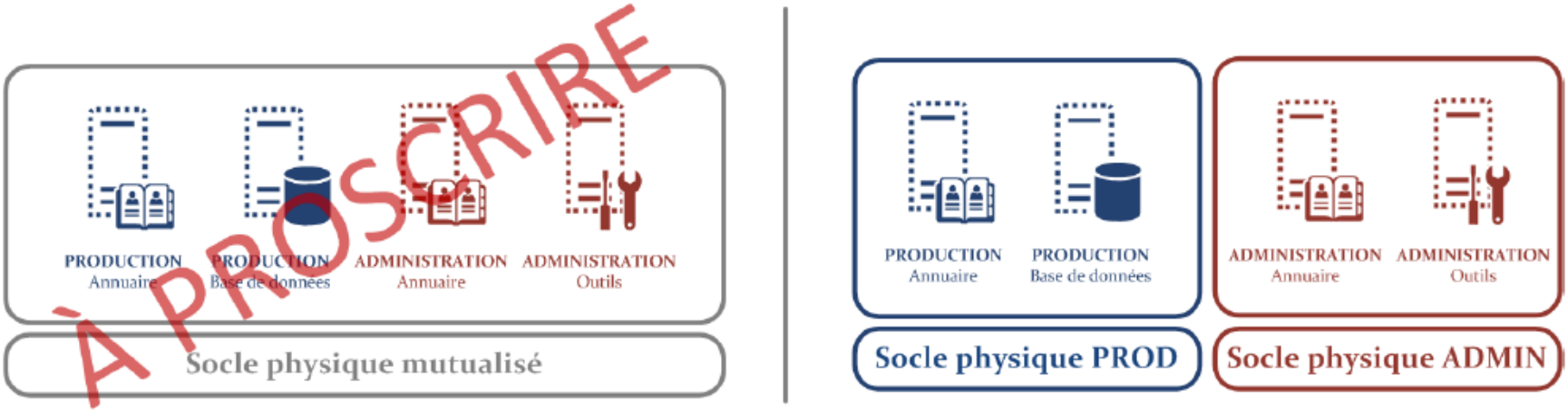
Concepts de base



ADMINISTRATION SÉCURISÉE

Concepts de base

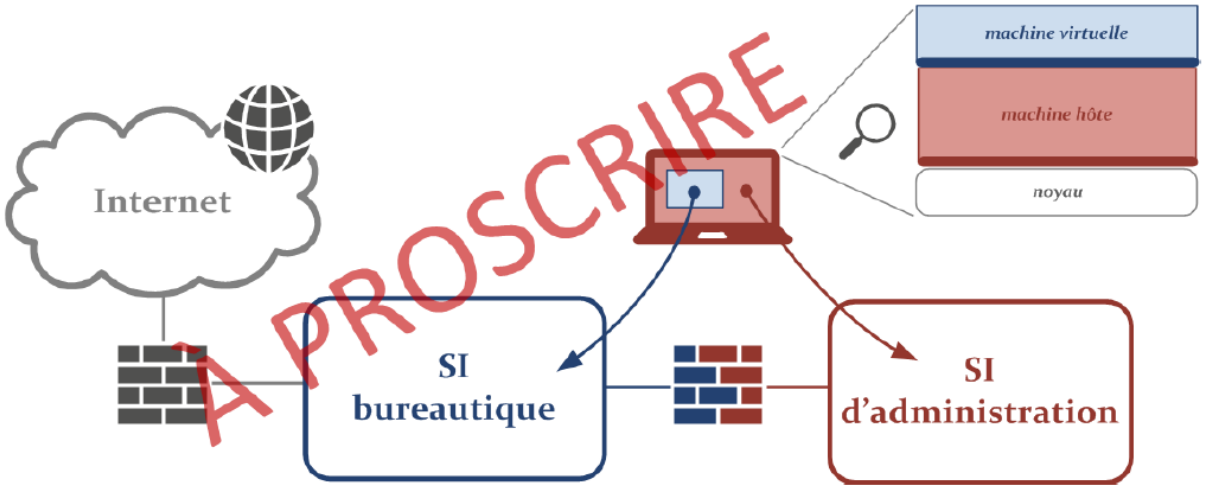
- Cloisonnement des socles physiques de virtualisation pour des serveurs



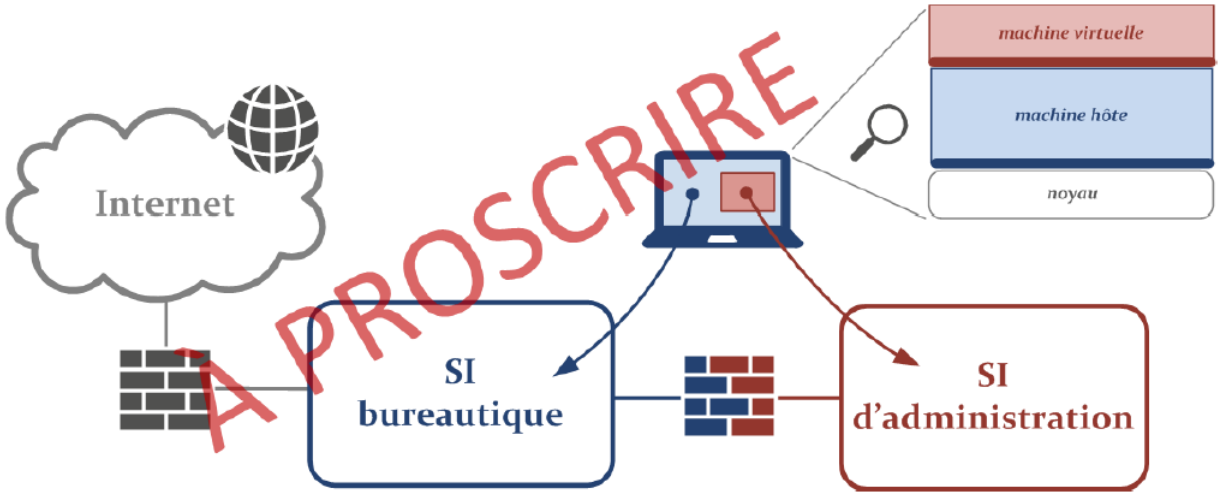
ADMINISTRATION SÉCURISÉE

Concepts de base

Poste d'administration hébergeant une machine virtuelle bureautique



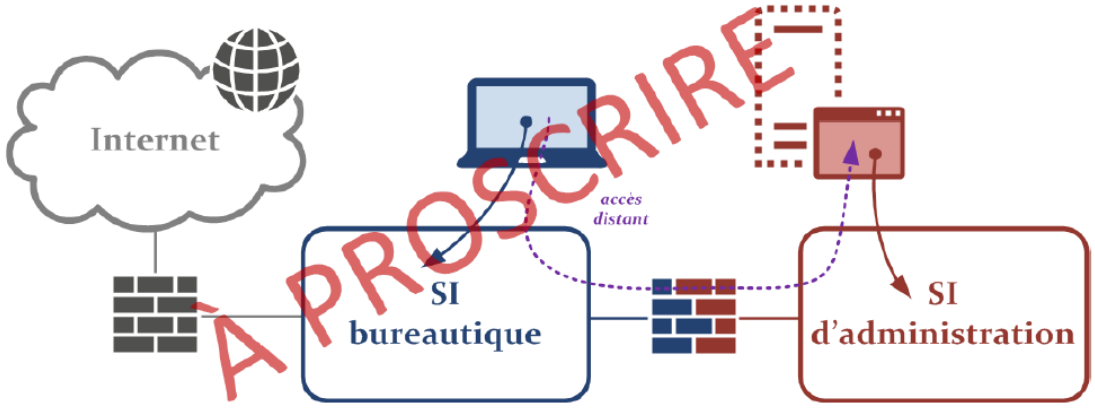
Poste bureautique hébergeant une machine virtuelle d'administration



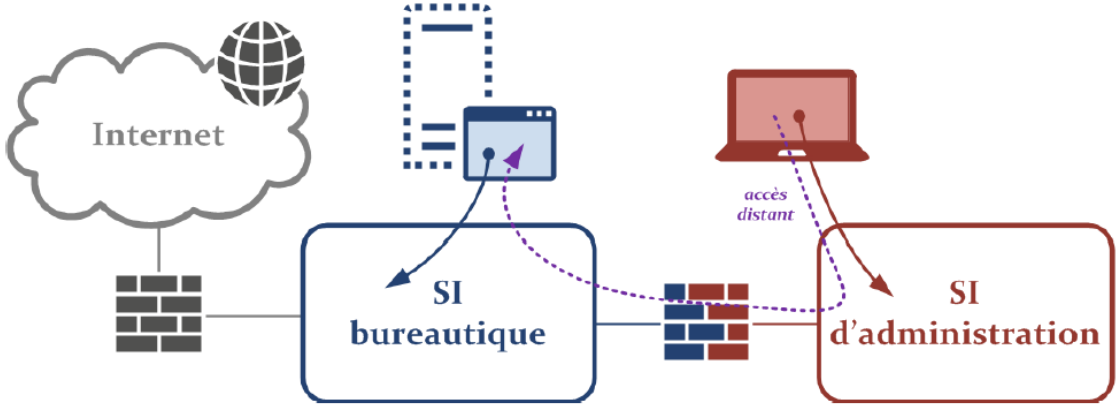
ADMINISTRATION SÉCURISÉE

Concepts de base

Poste bureautique physique avec accès distant à un environnement d'administration virtualisé



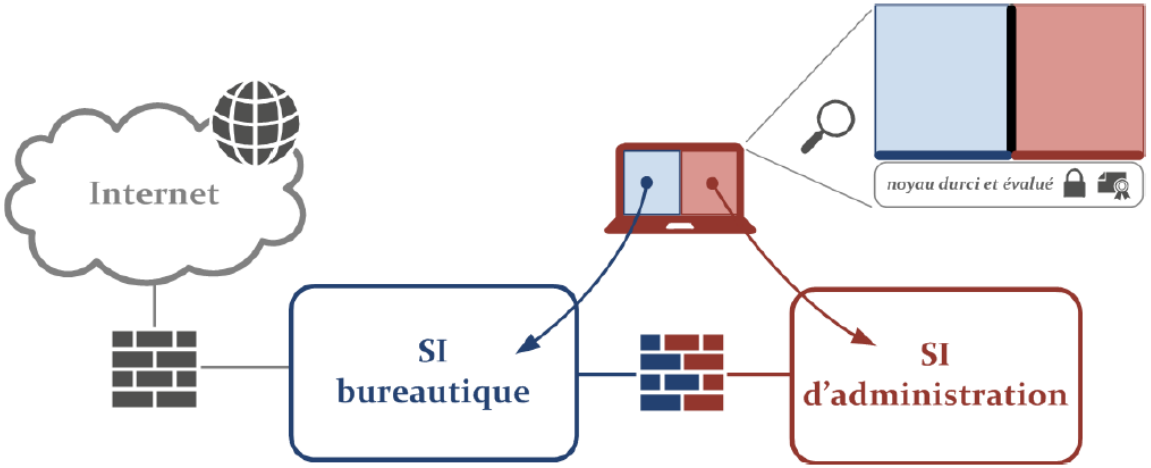
Poste d'administration physique avec accès distant à un environnement bureautique virtualisé



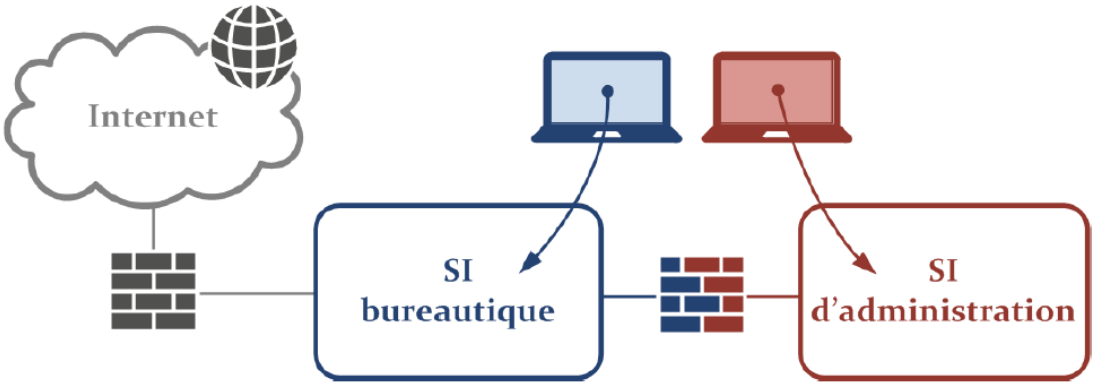
ADMINISTRATION SÉCURISÉE

Concepts de base

Poste d'administration multi-niveaux



Poste d'administration dédié



ADMINISTRATION SÉCURISÉE

Concepts de base

Recommandations : poste d'administration

- Bloquer tout accès à Internet depuis ou vers le poste d'administration
- Durcir le système d'exploitation du poste d'administration
  - désactivation des services inutiles
  - application de droits restreints au juste besoin opérationnel
  - activation et configuration du pare-feu local pour interdire toute connexion entrante et limiter les flux sortants au juste besoin
  - durcissement des configurations systèmes
    - GPO, Applocker, SRP, etc…
  - activation de l'ensemble des mécanismes de mise à jour
- Restreindre les droits d'administration sur le poste d'administration
- Limiter les logiciels installés sur le poste d'administration
- Chiffrer l'ensemble des périphériques de stockage utilisés pour l'administration

ADMINISTRATION SÉCURISÉE

Concepts de base

Recommandations : réseau d'administration

- Connecter les ressources d'administration sur un réseau physique dédié
- Connecter les ressources d'administration sur un réseau VPN IPsec dédié
- Appliquer un filtrage interne et périmétrique au SI d'administration
- Appliquer un filtrage local sur les ressources administrées
- Dédier une interface réseau physique d'administration
  - A minima dédier une interface réseau virtuelle d'administration
- Protéger les flux d'administration transitant sur un réseau tiers

Recommandations : identification, authentification et droits d'administration

- Utiliser des comptes d'administration dédiés
- Utiliser des comptes d'administration individuels

ADMINISTRATION SÉCURISÉE

Concepts de base

- Réserver les comptes d'administration aux seules actions d'administration
- Journaliser les événements liés aux comptes d'administration
  - ouvertures/fermetures de session
  - verrouillage des comptes
  - gestion des comptes
  - gestion des groupes de sécurité
- Stocker les mots de passe dans un coffre-fort de mots de passe
- Privilégier une authentification à double facteur pour les actions d'administration
- Privilégier une authentification centralisée
- Respecter le principe du moindre privilège dans l'attribution des droits d'administration
- Attribuer les droits d'administration à des groupes

ADMINISTRATION SÉCURISÉE

Concepts de base

Recommandations sur le MCS

- Réaliser scrupuleusement le MCS du SI d'administration
- Mettre en place des serveurs relais pour la récupération des mises à jour
- Valider les correctifs de sécurité avant leur généralisation

Recommandations sur le sauvegarde, la journalisation et la supervision de la sécurité

- Définir une politique de sauvegarde du SI d'administration
- Dédier une zone d'administration à la journalisation
- Centraliser la collecte des journaux d'événements