Mercredi 28 Novembre 2018

Le réseau à l’heure de la RGPD

D-Link

Rappel : RGPD pourquoi faire ?

- Créer un **cadre renforcé et harmonisé** de la protection des données en tenant compte des évolutions technologiques (cloud, IoT, big data….)
- Renforcer **les droits des individus** (extension de la loi Informatique et Liberté au territoire européen)
- Renforcer **les responsabilités** de toute la chaîne d'acteurs qui manipulent les données personnelles
- Obliger **la prise en compte de la vie privée** à la conception de tout service qui collecte des données personnelles (privacy by design)

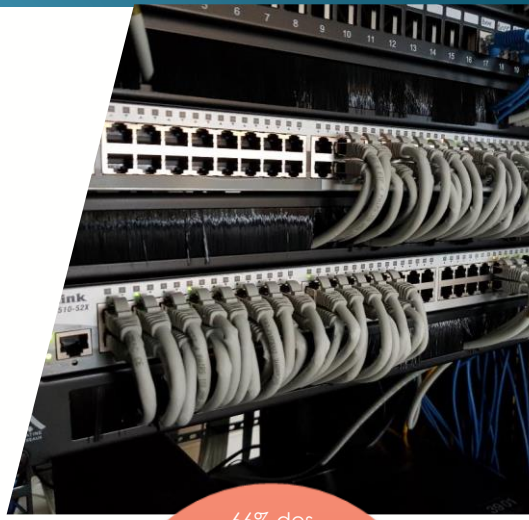
Les enjeux de RGPD

La RGPD impose le principe de mises en œuvre de **« mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque »** (article 32 du règlement Europe 2016/769 du 27 avril 2016).

Le réseau dans une entreprise aujourd'hui et les risques encourus

- **Menace :** Intrusion physique dans les locaux et/ou incendie
  Vol du matériel informatique, destruction, perte d'activité
- **Menace :** Panne disque dur
  Perte définitive de données (Absence de sauvegarde externe)
- **Menace :** Panne partielle ou générale du système informatique
  Impossibilité de poursuite rapide d'activité
- **Menace :** Réseau ouvert, sans sécurité
  Fuite de données confidentielles et/ou mise hors service du système
- **Menace :** Attaque cybercriminelle
  Fuite de données confidentielles et/ou mise hors service du système
- **Menace :** Mauvaises pratiques utilisateurs
  Fuite de données confidentielles et/ou mise hors service du système

** Selon le rapport 2018 Privileged Access Threat de Bomgar*



66% des entreprises reconnaissent qu'elles ont peut-être été victimes d'une faille causée par l'accès de tiers au sein même de leur réseau*

Le réseau à l'état de l'art

Les recommandations de l'ANSSI

L'agence nationale de la sécurité des systèmes d'information est chargée par le gouvernement de lutter contre les cyber menaces. Plus particulièrement pour les entreprises, opérateurs et organisations classés comme d'importance vitale pour la sécurité du pays. La plus grande menace est aujourd'hui celle des cybercriminels dormants.

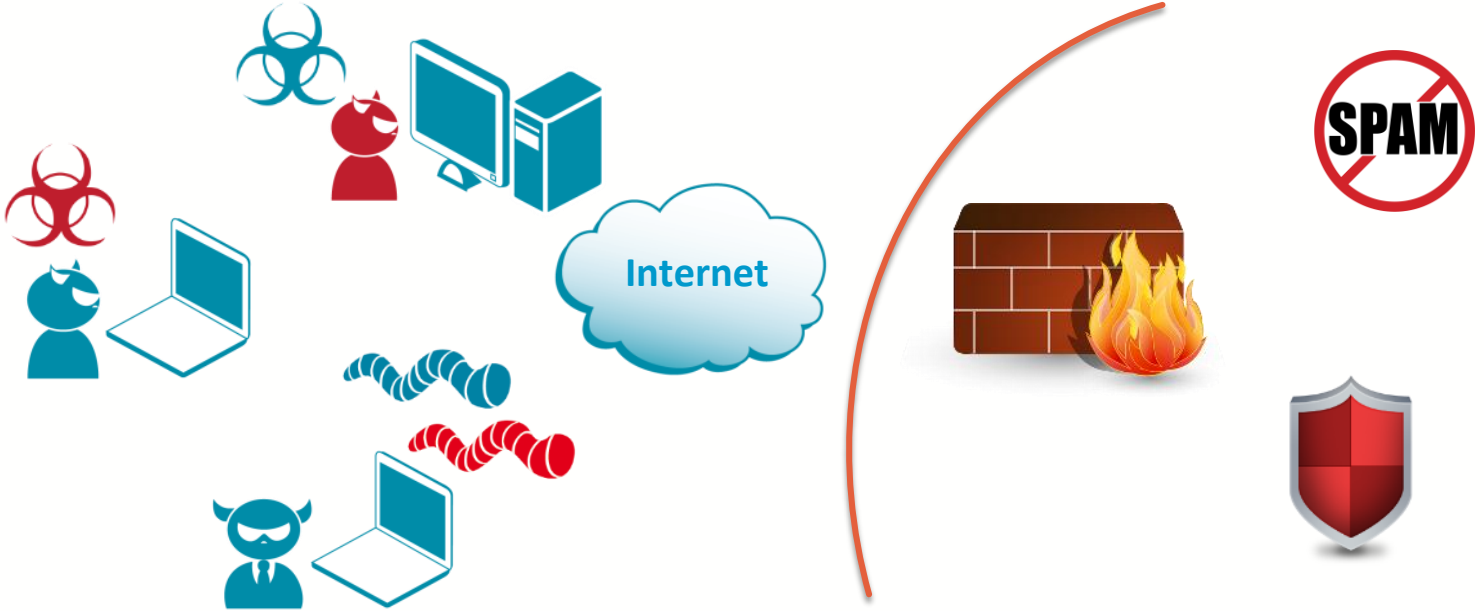
Elle publie régulièrement des guides de bonnes pratiques et des recommandations liés à la sécurisation des systèmes d'information.
Dont celui-ci le 12/07/2016: « RECOMMANDATIONS POUR LA SÉCURISATION D'UN COMMUTATEUR DE DESSERTE » (https://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-securisation-dun-commutateur-de-desserte/)

Ces recommandations impliquent une mise en place de pratiques et de fonctions exigeantes, l'utilisation de matériels et de protocoles complexes avec un niveau de paramétrage élevé. Même si le document commence par les bases.

Le réseau avec un niveau de sécurité raisonnable

La protection à l'entrée du réseau, une évidence

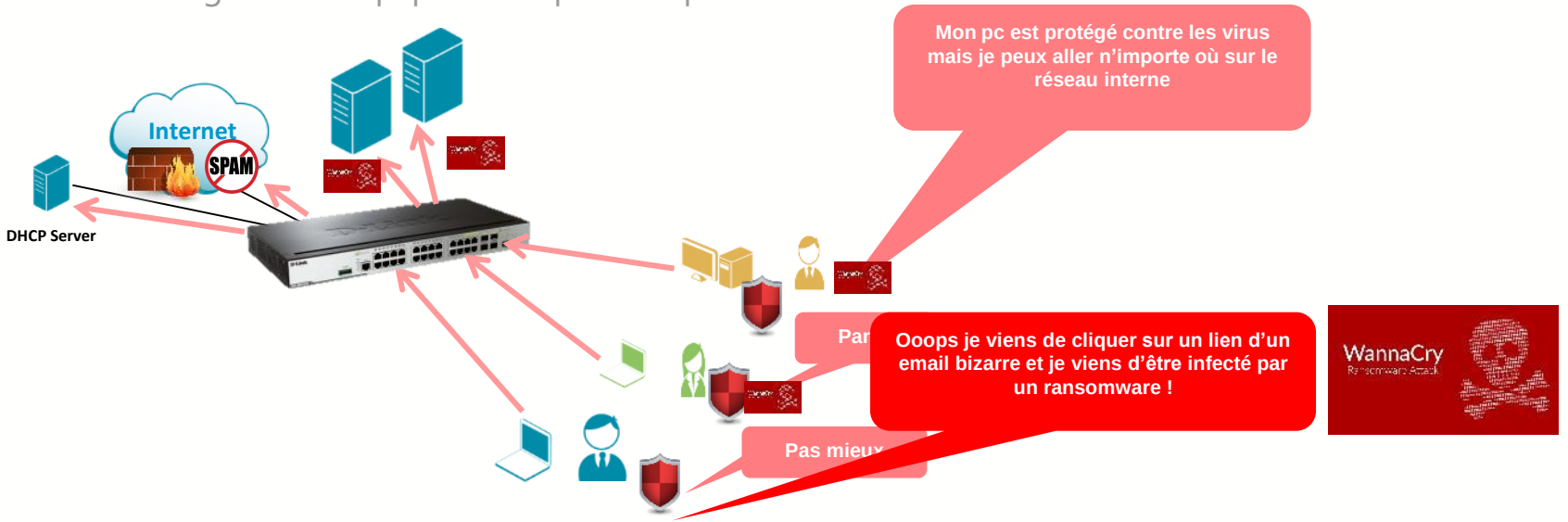
Il est aujourd'hui évident qu'il faut installer un pare-feu pour sécuriser la connexion Internet, un antispam et un antivirus pour protéger les machines.



Le réseau avec un niveau de sécurité raisonnable

La sécurité à la périphérie du réseau, souvent oubliée

La sécurité de la « multiprise » informatique est loin d'être aussi répandue, de même pour le Wi-Fi. La première vulnérabilité d'un réseau se trouve aux points d'entrée des utilisateurs, filaires et sans fil. Il est donc nécessaire de configurer les équipements pour empêcher toute tentative d'intrusion.



Les bonnes pratiques pour un réseau sécurisé

Enterprise

Sécurité physique

Limiter l'accès physique aux commutateurs et prises réseau aux seules personnes habilitées

Désactiver

Désactiver toutes les prises du réseau non utilisées

Programmation horaire PoE

Renforcer l'accès

Renforcer les accès au réseau par mot de passe clients en authentifiant les utilisateurs au préalable

Renforcer les contrôles

Ajouter le contrôles des adresses MAC et IP des équipements connectées par la fonction IMPB

D-Link
Building Networks for People

Mais aussi

L'administration des commutateurs :

- Dédier/limiter l'administration des commutateurs à une interface physique
- Utiliser le protocole *SSH v2* pour une administration à distance
- Désactiver *Telnet*
- Désactiver à minima le serveur *HTTP*, idéalement le *HTTPS*
- Réaliser un filtrage pour l'accès administrateur des commutateurs (*ACL, filtrage pare feu*,…)

Cloisonnement des réseaux :

- Séparer dans l'idéal les réseaux critiques physiquement
- Mise en place de *VLAN* manuel (éviter les protocoles automatiques comme *GVRP*, *VTP*,…)
- Le *VLAN* par défaut ne doit jamais être utilisé
- Mettre en place la fonction *Traffic Segmentation*

Disponibilité :

- Activation du *DHCP Snooping/DHCP Server Screening* pour limiter les attaques par usurpation du serveur DHCP
- Mise en place de l'*IMPB* pour restreindre l'accès à un commutateur à un certain nombre d'utilisateurs autorisés (vérification leur paire d'adresse IP-MAC)
- Activer le *Loop Back Detection (LBD)* pour garantir une haute disponibilité des commutateurs d'accès et plus généralement du réseau complet
- Activer le *Safeguard Engine* afin de préserver les attaques par saturation de la CPU

Mais aussi

Synchronisation horaire et journalisation :

- Configurer le *NTP*
- Activer l'envoi des journaux des commutateurs vers un serveur externe

Supervision :

- La supervision *SNMP* en version 3 (minimum v2c)
- Programmer des alertes avec notifications par emails

Gestion du parc, maintien en condition opérationnelle :

- Mettre à jour régulièrement les commutateurs
- Une gestion centralisée du parc permet de faciliter la maintenance du SI
- Sauvegarder les configurations après chaque modification

IoT et Sécurité

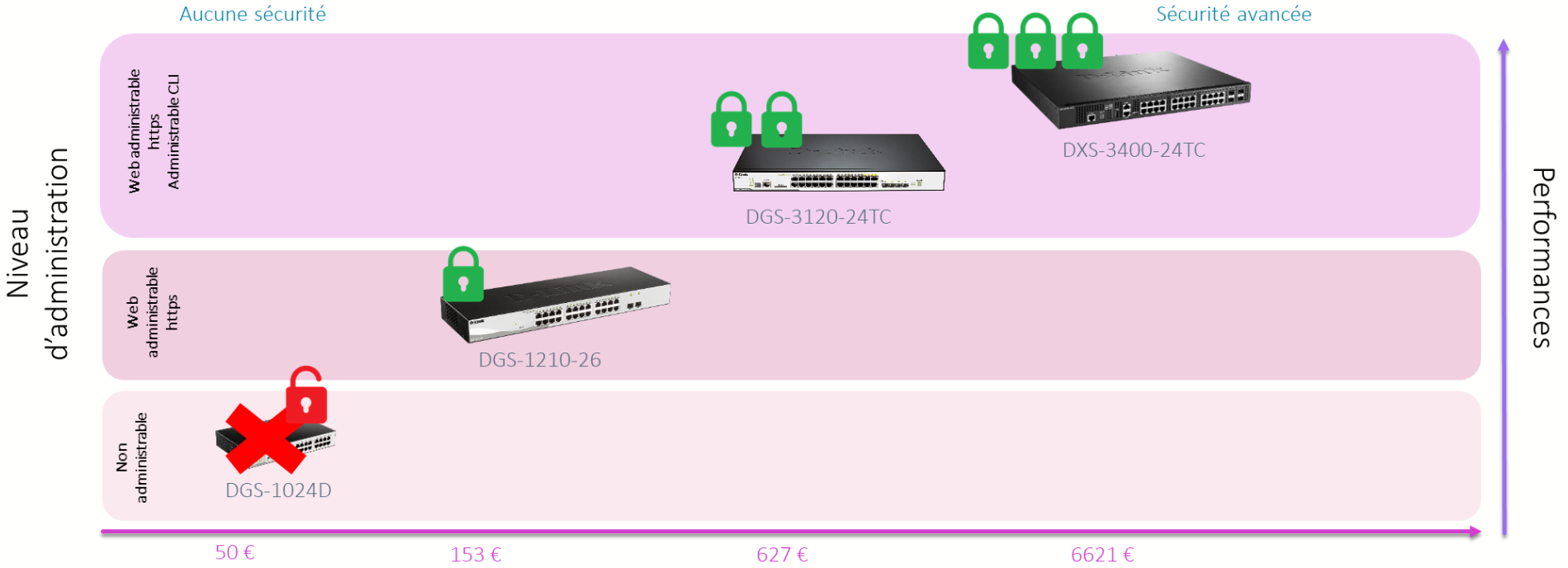
- **L'Internet des objets IP** s'invite dans les réseaux des entreprises
- **Smart City** mais aussi **Smart Building**
- **Gestion de systèmes intelligents** via divers capteurs, prises, caméras et pilotés par Smartphone.
- Autant d'entrées supplémentaires pour les Hackers
- VLAN dédié **IoT**
- Contrôle des adresses IP des objets.
- Activation sur plage horaire

Intégration d'un système de vidéosurveillance

- **Contrôle des accès physiques** au site (Portes, fenêtres, parking…)
- **Contrôle des équipements et locaux** sensibles (Salle serveurs, stock, laboratoire…)
- Enregistrement sur **plage horaire**, sur **détection de mouvements, masque de vie privée**
- Activation du PoE sur plage horaire ?
- **VLAN dédié vidéo**
- Contrôle des adresses IP des caméras.

Réseau administrable obligatoire

Le niveau de commutation doit être en cohérence avec le niveau de sécurité attendue



L'offre infrastructure tertiaire

	Accès	Agrégation			Cœur			
	Série 1000	Série 1100	Série 1210	Série 1510	Série 3000	Série 3120	Série 3630	Série 3400/3600
Niveau	Non administrable	Smart L2	Smart L2+	Smart L3 Light	L2+	L2/L2+	L3 Light/L3/L3+	
PoE/PoE+*	●	●	●	●	●	●	●	
10 GbE		● série DXS	● série DXS	●	●	●	●	● complet
Stacking				●		●	●	●
Redondance électrique					●	●	●	●
Usage	Distribution Accès/Data	Mono usage Data/Voix/Vidéo	Double usage Data/Voix/Vidéo	Cœur de réseau	Distribution	Distribution Cœur de Réseau	Cœur de réseau	Cœur de réseau
Client type	TPE/Artisan	TPE/Artisan		PME	PME ETI Opérateurs		PME ETI Opérateurs	PME ETI Opérateurs DATACENTER
Nombre de postes	< 24	< 50		< 150	< 300		< 2000	> 2000

** Selon les modèles.*

L’offre industrielle D-LINK

	Unmanaged	Managed L2	Managed L2+ SFP
	 PoE	 PoE	
	Série DIS-100E/G	Série DIS-300G	Série DIS-700G
Manageable SNMP	NON	Web, SNMP, CLI complète	Web, SNMP, CLI complète
PoE ou PoE+	jusqu’à 120W*	jusqu’à 240W* (dont 2 ports PoE++ pour le DIS-300G-14PSW)	NON
Nb de ports RJ45	4/5/8	6/8/10	-
Nb de ports SFP/SFP+		Jusqu’à 4 SFP	24 SFP et 4 SFP+
Plage de fonctionnement		-40° à +75°C	-10° à +65°C
Fonctionnalités		Fonctions d’admin. Complètes L2 Spanning tree Fast Failover Protection Rings VLAN, QoS	Fonctions d’admin. Complètes L2 Spanning tree Fast Failover Protection Rings VLAN, QoS, routage statique
Certifications	Shock - IEC 60068-2-27 / Freefall - IEC 60068-2-32 / Vibration - IEC 60068-2-6 IP30		
Montage/Alimentation	*RAIL DIN, mural* *12-58 VDC*, 48-58 VDC** *Alimentation redondante* *Connecteurs Alarme*	*RAIL DIN, mural* *12-58 VDC*, 48-58 VDC** *Alimentation redondante* *Connecteurs Alarme*	*Rack* *100/240 VAC*

** Selon les modèles.*

Les fonctionnalités disponibles par série

	Périphérie		Distribution			Cœur de réseau	
	Série 1100	Série 1210	Série 1510	Série 3000	Série 3120	Série 3630	Série 3400
Niveau	Smart L2	Smart L2+	Smart L3 Light	L2	L2/L2+	L3 Light/L3/L3+	
Loopback Detection (LBD)	●	●	●	●	●	●	●
D-Link Safeguard Engine	●	●	●	●	●	●	●
VLAN 802.1q	●	●	●	●	●	●	●
Private VLAN				●	●	●	●
Traffic Segmentation	●	●	●	●	●	●	●
IP Mac Port Binding (IMPB)		●	●	●	●		
ARP Spoofing Prevention		●	●	●	●	●	●
DHCP Server Screening		●	●	●	●	●	●
Authentification Radius/802.1X		●	●	●	●	●	●
Authentification TACACS+			●	●	●	●	●
BPDU Attack Protection			●	●	●	●	●
DoS Attack Prevention	●	●	●	●	●	●	●
Nombre de postes	< 50		< 150	< 300		< 2000	➢ 2000

Intégration du Wi-Fi

66% des entreprises reconnaissent qu'elles ont peut-être été victimes d'une faille causée par l'accès de tiers au sein même de leur réseau*

Gérer la puissance

Contrôle de la puissance d'émission du Wi-Fi par les bornes

Segmenter le Wi-Fi

Créer de multiples SSID avec VLAN associés et séparer les visiteurs

Programmer

Diffuser le signal Wi-Fi sur plage horaire et/ou activer le PoE sur plage horaire

PoE

Contrôler

Contrôler et faire la journalisation des accès utilisateurs

Ajouter le filtrage par adresses Mac

Gérer les logs

Obligation légale de conservation des activités de navigation sur Internet

** Selon le rapport 2018 Privileged Access Threat de Bomgar*

D-Link®
Building Networks for People

Gestion du Wi-Fi

Wi-Fi Autonome

☑ **AVANTAGES**

- Mise en œuvre simplifiée
- Adaptée aux petits réseaux
- Coûts maîtrisés

× **INCONVENIENTS**

- Peu évolutif
- Maintenance sommaire
- Tolérance à la panne limitée
- Itinérance limitée

Wi-Fi Cloud

☑ **AVANTAGES**

- Déploiement simplifié
- Gestion en ligne
- Gestion multi-site facilitée
- Coûts maitrisés

× **INCONVENIENT**

- Dépendance à un cloud externalisé

Wi-Fi Unifié

☑ **AVANTAGES**

- Maîtrise de la sécurité 100%
- Maintenance simplifiée
- Forte tolérance de panne
- Itinérance optimisée
- Evolutivité

× **INCONVENIENT**

- 1ère mise en œuvre plus complexe

Rôle du contrôleur

Administration centralisée
Gestion jusqu'à 1024 bornes avec itinérance sans coupure et 4 contrôleurs maximum

Balance des charges
Répartition des clients sur les bornes et les bandes de fréquences* sur le réseau sans-fil

Sécurité
Authentification 802.1x, WPA2-Entreprise, Radius, portail captif, filtrage @ MAC… et sécurité Firewall**

Ajustement automatique des canaux
Gestion avancée des canaux pour éviter et limiter les interférences

Adaptation de la puissance
En cas de défaillance d'un AP, la puissance des AP voisins augmente pour apporter une continuité de service

Programmation horaire
Paramétrage horaire pour une adaptation totale à l'environnement client

DWC-1000 Contrôleur Wi-Fi

- Prise en charge de 12 points d'accès de base
- Jusqu'à 66 points d'accès par ajout de licence additionnelle
- Option Firewall/VPN

DWC-2000 Contrôleur Wi-Fi

- Prise en charge de 64 points d'accès de base
- Jusqu'à 256 point d'accès par ajout de licence additionnelle

** Technologie Band Steering - selon les modèles de bornes.*
*** En option sur le DWC-1000*

Les bornes Wi-Fi Unifiées

Outdoor

Indoor

DWL-6700AP
DWL-2600AP

- Wi-Fi N 300 Mbps
- Single ou Dual Radio
- Contrôlée ou autonome

Small business

DWL-6620APS
DWL-6610AP/APE
DWL-3610AP

- Wi-Fi AC jusqu'à 1300 Mbps
- Dual Radio ou selectable
- Couverture optimisée
- Smart antenna 2x2*
- Contrôlée ou autonome

Medium business

DWL-8710AP
DWL-8610AP
DWL-7620AP

- Wi-Fi AC jusqu'à 2100 Mbps
- Dual Radio ou Tri-Band
- Couverture optimisée
- Contrôlée ou autonome

Enterprise business

** Selon les modèles*

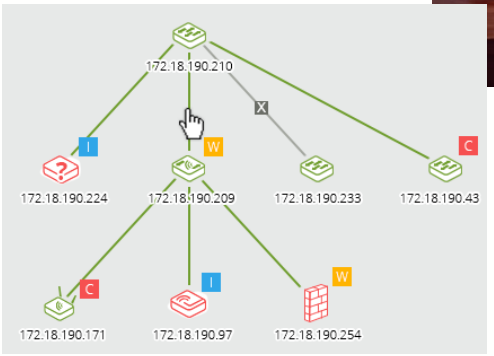
D-Link® Building Networks for People

La supervision du réseau

La plate-forme logicielle **D-View 7** est un outil de gestion réseau visant à gérer de manière centralisée les composantes d'une infrastructure IP des entreprises et collectivités.

GRATUIT

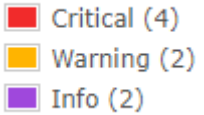
- **Gestion du filaire et du Wi-Fi**
- **Gestion multisite via un seul point**
- **Création de rôles d'administration**
  Monitoring de l'infrastructure



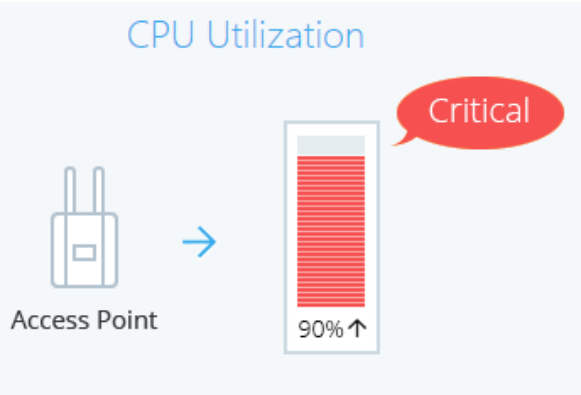
D-Link
Building Networks for People

Alertes sur événements

D-View 7 permet de mettre en place des alertes sur événements avec seuils personnalisables.
3 niveaux d'alertes sont disponibles : ***Critical, Warning, Information***



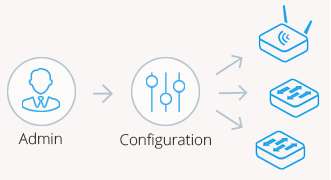
Paramètre de supervision	Seuil d'alerte	Type d'évènements
Error Packet	> 5Mpps	W Warning
CPU Utilization	> 90%	C Critical
Traffic Packet	> 10Mpps	I Info
Memory Utilization	> 80%	W Warning

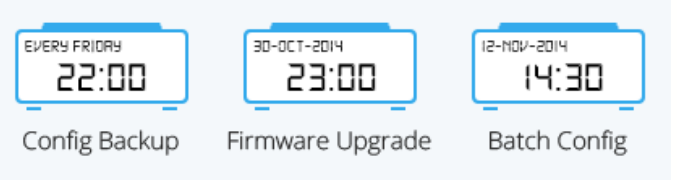


Tâches

D-View 7 vous permet la mise en place de tâches pour simplifier l'administration/supervision :

- Programmation unique ou périodique
- Backup des configurations
- Mise à jour firmware
- Configuration par lot
- Historisation des tâches





- Firmware upgrade
- Sauvegarde de config
- Configuration batch

- Quand les exécuter
- Unique, périodique

- Résultats
- Historique des tâches

Merci

D-Link®
Building Networks for People