Guide recommandations ANSSI 2016

Recommandations pour la sécurisation d'un EAR.

1. Protocoles à désactiver sous *configure terminal*

RO(config)#no service tcp-small-servers
RO(config)#no service udp-small-servers
Les services TCP/IP simples sont des services internes appelés *small servers* tels que *echo* ports TCP et UDP n°7, *discard* ports TCP et UDP n°9, *chargen* ports TCP et UDP n°19, etc.
Selon la version de l'IOS, ils sont activés par défaut.

RO(config)#no service finger
Le service finger permet de lister les utilisateurs connectés sur le routeur.

RO(config)#no service config
Les routeurs peuvent charger leurs conf sur le réseau via TFTP, ils émettent des requêtes en diffusion sur chaque interface.

RO(config)#no ip bootp server
BOOTP est un protocole utilisé par certains matériels pour charger leur système d'exploitation au travers d'un réseau.

RO(config)#no ip source-route
Le routage par la source (Source-routing) est une option du protocole IP qui permet de spécifier le chemin que doit prendre le datagramme pour accéder à sa destination.

RO(config)#no ip subnet-zero
L'utilisation du sous-réseau « zéro », le premier d'un adressage par sous-réseau, est fortement déconseillée dans les RFC.

RO(config)#no ip http server
Le serveur HTTP permet la gestion du routeur à partir d'une interface HTML.

RO(config)#no ip http secure-server
Le serveur HTTPS permet la gestion du routeur à partir d'une interface HTML.

RO(config)#no ip domain-lookup
Désactive la résolution de nom.

RO(config)#no cdp run
Désactive le protocole CDP sur l'équipement actif (Cisco Discovery Protocole).

RO(config)#service password-encryption
Active le « chiffrement » on parlera ici plutôt de hachage des mots de passes dans le fichier de config.

RO(config)#no snmp-server
RO(config)#no snmp-server enable traps
SNMP est un protocole de supervision de réseau qui utilise un mécanisme de sécurité assez faible. Dans le cas où la supervision à l'aide du protocole SNMP ne serait pas mise en oeuvre, il faut désactiver l'agent SNMP.

RO(config)#no crypto pki trustpoint <TP-self-signed-123456789>
Supprime le certificat cré par défaut pour le serveur HTTPS (Série 4000 Cisco), le TP-self-signed-XXXXXXXXX se trouve dans le show run.

RO(config)#login on-failure log
RO(config)#login on-success log
Active la journalisation des authentifications.

RO(config)#vtp mode off
Désactive le vtp sur l'EAR.

RO(config)#service timestamps log datetime localtime show-timezone
Active l'horodatage des évènements journalisés en précisant l'heure locale et le fuseau horaire. Pratique pour les audits.

2. Protocoles à désactiver sous *config-if* (Niv 2 ou/et 3)

RO(config-if)#no ip redirected-broadcast
RO(config-if)#no ip unreachable
RO(config-if)#no ip mask-reply
RO(config-if)#no ip redirects
Le protocole ICMP utilise plusieurs messages d'information. Par exemple, le message "redirect" (redirection ICMP) permet d'informer un hôte du réseau d'une meilleure route pour atteindre une destination.

RO(config-if)#no ip proxy-arp
Un routeur Cisco peut se comporter comme un relais ARP (Proxy-ARP) et répondre à des requêtes ARP concernant des hôtes situés sur un autre segment.

RO(config-if)#no ip route-cache
RO(config-if)#no ip mroute-cache
Le mécanisme de cache de routage permet d'améliorer les performances grâce à la commutation rapide des paquets.
Sur les anciennes versions d'IOS (8.x et 9.x), le mécanisme de cache était vulnérable. Dans ce cas, il est préférable de le désactiver.

RO(config-if)#no cdp enable

L'écoute du trafic CDP sur un réseau permet d'obtenir les noms des routeurs, de leurs interfaces, les versions des matériels et des IOS.

RO(config-if)#no ntp disable

Le protocole NTP permet de synchroniser automatiquement les équipements d'un réseau avec une horloge de référence, atomique ou GPS.
Ce protocole, ou sa version simplifiée "SNTP", est disponible sur la plupart des IOS récents.

RO(config-if)#no snmp-server

SNMP est un protocole de supervision de réseau qui utilise un mécanisme de sécurité assez faible (nom de communauté circulant en clair). Dans le cas où la supervision à l'aide du protocole SNMP ne serait pas mise en oeuvre, il faut désactiver l'agent SNMP présent sur le routeur.
Attention pour désactiver correctement SNMP, il faut retirer de la configuration toutes les lignes concernées. La seule commande ***no snmp-server*** *n'efface pas les noms de communautés (même s'ils n'apparaissent plus dans le fichier de configuration !).*

RO(config-if)#no vtp

Désactive le protocole VTP sur l'interface.

RO(config-if)#no lldp transmit

Protocole standardisé de découverte réseau, permet aux équipements de différents fabriquant de se découvrir mutuellement.

SW(config-if)#switchport nonegotiate

Désactive m'émission de trames DTP.

3. Sources

- Recommandations pour la sécurisation d'un commutateur de desserte. Guide de l'ANSSI du 24 juin 2016.

- Recommandations pour la sécurisation des routeurs. Guide du CELAR du 11 juin 2007.