Protection NPS par ports

Sommaire

Principes

La norme 802.3 est l'implémentation ethernet de l'authentification 802.1x.
En même temps que l'authentification, le serveur NPS renvoie le VLAN untagged sur lequel se fera la connexion.

Lorsqu'un périphérique réseau est raccordé à un port de switch, il y a deux cas de figure:

Ordinateur sur lequel le 802.3 est activé

- L'oridnateur fait une demande d'authentification 802.1x au switch.
- Le switch la répercute au serveur NPS qui la vérifie auprès du DC. L'ordinateur doit donc appartenir au domaine.
- Si l'ordinateur est reconnu, le groupe AD dans lequel il se trouve va déterminer quel VLAN sera ouvert sur le port concerné (par exemple, VLAN 12 pour "&stations-tech")
- Le serveur NPS renvoie l'accord de connexion et le VLAN demandé au switch.

Périphérique réseau non 802.3 .

- Le périphérique (ordinateur, client léger, téléphone) fait une demande d'authentification par Mac-Address, car il n'es pas paramétré pour le 802.3
- Le switch la répercute au serveur NPS, qui la vérifie auprès d'une liste de masques de MAC connues.
- Si la MAC est reconnue, la connexion est acceptée et le VLAN correspondant renvoyé

L'authentification peut être activée ou désactivée individuellement pour chaque port de switch

- Un port sur lequel elle est désactivée utilise le paramétrage de vlan du switch (Tagged et Untagged), sans authentification.
- Un port suir lequel elle est activée utilise les VLAN Tagged paramétrés sur le switch et le VLAN untagged renvoyé par le NPS, à condition que l'authentification soit effective.
- Si l'authentification échoue, les VLAN Tagged ne passent pas. C'et le Guest VLAN untagged qui est utilisé, par exemple DMZ-PRESTA.

Haute disponibilité.

- On peut déclarer jusqu'à 15 serveurs RADIUS
- Si un serveur ne répond pas, le switch interroge le suivant.
- Si aucun serveur ne répond, les ports ne sont plus authentifiés.
- Il peut alors être souhaitable de désactiver l'authentification de manière globale.

Paramétrage

Switches : Radius

Attention : le NPS ne fonctionne que sur un port déjà affecté à un Vlan Untagged. Utiliser le Vlan 13 ou 17 (quand il sera en place)

Sur le switch, passer en mode Config

A tout moment, pour vérifier la configuration:

- show port-access ? (affiche le menu)
- show port-access config
- show port-access summary

Vérifier la config d'authentification

- show radius
- show authentication

Toutes les étapes sont **obligatoires**.

Ajouter / supprimer un serveur Radius

- (no) radius host <ip-address>
- Les serveurs Radius sont 192.168.2.93. et 94

Ajouter la une clé globale (identique à celle du modèle stocké sur le serveur NPS, voir plus bas dans "Paramétrage client Radius")

- radius key <chaine clé>

Nombre de tentatives d'authentification si erreur de mot de passe <1-10>. Valeur suggérée : 2

- aaa authentication num-attempts 2 <1-10>

Temps en minutes pendant lequel un serveur Radius défaillant sera ignoré <1-1440>. Valeur suggérée : 5

- radius-server dead-time 5 <1-1440>

Temps d'attente en secondes avant qu'un serveur Radius soit considéré "dead" <1-15> : Valeur suggérée : 4

- radius-server timeout 4 <1-15>

Nombre de tentatives d'authentification en cas de non réponse du serveur 1 <1-5>. Valeur suggérée :1

- radius-server retransmit 1 <1-5>

Router toutes les demandes d'authentification 802.1x vers le Radius en EAP

- aaa authentication port-access eap-radius

Router toutes les demandes d'authentification MAC vers le Radius en PEAP : ne fonctionne malheureusement pas.
Utilisé pour l'authentification par MAC avec un user AD. La différenciation par range MAC ne peut pas distinguer un client léger d'un portable.

- ~~aaa authentication mac-based peap-mschapv2~~

Il faut donc utiliser le CHAP et activer l'enregistrement des mots de passes dans la Policy Stratégies de comptes du domaine.

- aaa authentication mac-based chap-radius

Il faut aussi que le format de mac-address corresponde au nom d'utilisateur AD : nn-xx-nn-xx-nn-xx (multi-dash)

- aaa port-access mac-based addr-format multi-dash

Définir le VLAN des clients non authentifiés (par exemple 5 pour DMZ-PRESTA)

- (no) aaa port-access mac-based 1-48 unauth-vid 5

Désactiver le GVRP (le switch ne doit pas créer dynamiquement les vlans)

- no aaa port-access gvrp-vlans

Déploiement

Attention : toujours activer l'Authenticator avant le Mac-based, sinon coupure de connexion pour les utilisateurs.
La désactivation se fait dans l'ordre inverse.

Switches : Ports

Authenticator (802.1x)

Autoriser jusqu'à 32 clients par ports. La valeur 0 interdit le mac-based. La valeur par défaut est 1.

- (no) aaa port-access authenticator 1-48 client-limit 32 (8 sur les 2610)

Activer / désactiver globalement le 802.1x

- (no) aaa port-access authenticator active

Activer / désactiver le 802.1x par ports

- (no) aaa port-access authenticator <port-list>

Afficher la config et l'état du 802.1x

- show port-access authenticator

Port-access (Mac Address)

Autoriser plusieurs identifications de MAC Adress par port (défaut : 1)

- aaa port-access mac-based 1-48 addr-limit 32

Permettre aux MAC de changer de port (bougeotte en téléphonie pâr ex.)

- aaa port-access mac-based 1-48 addr-moves (disabled by default)

Activer / désactiver individuellement l'authentification par mac-address

- (no) aaa port-access mac-based <port-list>

Afficher la config et l'état du MAC Based

- show port-access mac-based

Postes Windows

Les postes Windows doivent recevoir par GPO:

- Démarrer en automatique le service "Configuration automatique du réseau cablé" (Dot3svc)
- Utiliser une stratégie de réseau filiaire (IEEE 802.3) reprenant les réglages suivants

RTENOTITLE	RTENOTITLE	RTENOTITLE

L'objet GPO résultant doit être **appliqué** (Cadenas sur l'icône)

Serveur NPS

Principes

Le serveur NPS propose tois types de stratégies. Les trois types sont traités dans l'ordere listé

- **Stratégies de demande de connexion** : Elles autorisent la connexion, à la condition expresse que l'authentifcation soit réussie. Ces stratégies peuvent:
  - Transmettre la demande d'authentification au serveur Radius intégré au NPS. C'est le cas des stratégies "Connexions locales" et "Connexions sans fil" (Mode "Authentifier les demandes sur ce serveur")
  - Ou bien traiter directement l'identification sans authentification. C'est le cas des stratégies par Mac-Adresses, qui paramètreront elles-même le VLAN. (Mode "Accepter les utilisateurs sans validation de l'identification"). Les clients légers, par exemple, seront identifiés sans être authentifiés.
- **Stratégies réseau** : Elles traitent l'authentifcation et le paramétrage demandés éventuellement par les "Stratégies de demande de connexion".
- **Stratégies de contrôle d'intégrité** : Couche supplémentaire de validation de la configuration des clients, que nous n'utilisons pas.

Paramétrage

Attention. Après chaque modification de la config NPS, il faut exporter la configuration et la réimporter sur les autres serveurs
RTENOTITLE

Clients RADIUS

On définit ici les périphériques réseau qui transmettront des demandes d'authentifcation.

Il faut définir chaque switch, avec son IP de management (dans le range 192.168.45.0/24)
Pour en ajouter un nouveau :

- Bouton droit sur "Clients RADIUS", faire "Nouveau"
- Sélectionner le modèle "Modèle de SW-EDGE-HP" puis décocher la case "Sélectionner". Les paramèr=tres restent.
- Régler le nom exact et l'IP du switch
- Dans "Secret partagé" choisissez le modèle "Clé RADIUS des switches de distribution"
- Ce modèle contienty la clé partagée avec tous les switches. On peut la voir en éditant le modèle dans "Gestion des modèles" et cliquant sur "Générer"

Stratégies de demande de connexion

On n'aura à définir que de nouvelles stratégies par **Mac-address**
Il y a **une** stratégie par masque de Mac-Address. Un masque correpond au 3 premières paires de caractères de la MAc, avec les tirest, et une astérisque. Par exemple **6c-2b-59-***
Paramétrer en suivant ce modèle. Bien choisir le VLAN untagged correpondant au type de périphérique. Les valeurs non montrées restent par défaut.

RTENOTITLE	RTENOTITLE
RTENOTITLE	RTENOTITLE

Stratégies réseau

On en créera de nouvelles pour un nouveau groupe d'ordinateurs du domaine, par exemple, et donc un nouveau VLAN
Il y a **une** stratégie par groupe d'ordinateurs (Workstation, Dev, Tech, etc...)
Paramétrer en suivant ce modèle. Les valeurs non montrées restent par défaut.

RTENOTITLE	RTENOTITLE
RTENOTITLE	RTENOTITLE