LISTE DES TABLEAUX

LISTE DES FIGURES

GLOSSIAIRE

MAC (Medium Access Control) : couche logicielle qui a pour rôle de structurer les bits d'information en trames adaptées au support physique et de gérer les adresses physiques des cartes réseaux (Adresses MAC)

DHCP (Dynamic Host Configuration Protocol) : permet, à partir d'un serveur, de télécharger la configuration réseau vers un ordinateur (adresse IP, paramètre TCP/IP, etc.)

DNS (Domain Name System) : service de noms reposant sur des serveurs et permettant de convertir un nom en une adresse IP

EAP (Extensible Authentication Protocol) : protocole de communication réseau embarquant de multiples méthodes d'authentification, pouvant être utilisé sur les liaisons point à point, les réseaux filaires et les réseaux sans fil

FQDN (Fully Qualified Domain Name) : est un nom de domaine qui révèle la position absolue d'un nœud dans l'arborescence DNS en indiquant tous les domaines de niveau supérieur jusqu'à la racine.

LDAP (Lightweight Directory Access Protocol) : est à l'origine un protocole permettant l'interrogation et la modification des services d'annuaire. Il a cependant évolué pour représenter une norme pour les systèmes d'annuaires.

MAB (Mac Authentication Bypass) : authentification de niveau 2 basée sur les adresses MAC et fournie par Cisco

802.1X : standard permettant de contrôler l'accès aux équipements du réseau

AAA (Authentication, Authorization, Accounting) : AAA correspond à un protocole qui réalise trois fonctions : l'authentification, l'autorisation, et la traçabilité

ACL (Access Control List) : les ACLs servent principalement au filtrage des paquets sur les interfaces physiques

CHAP (Challenge Handshake Authentication Protocol) : protocole d'authentification pour PPP à base de challenge, ce qui le rend bien plus sûr que son précédent PAP.

CA (Certificate Authority) : a pour mission, après vérification de l'identité du demandeur du certificat, de signer, émettre et maintenir les certificats

CPP (Client Provisioning Portal) : portail appartenant à la plate-forme ISE et permettant de fournir les Agents NAC

CWA (Central Web Authentication) : portail Web qui permet aux utilisateurs de s'inscrire et de s'authentifier. Aussi, elle peut inclure la validation de posture (CPP).

PPP : Point-to-Point Protocol (PPP, *protocole point à point*) est un protocole de transmission pour l'internet, décrit par le standard RFC 1661, fortement basé sur HDLC, qui permet d'établir une connexion de type liaison entre deux hôtes sur une liaison point à point. Il fait partie de la couche liaison de données (couche 2) du modèle OSI.

CHAP : Le protocole CHAP (*Challenge Handshake Authentication Protocol*), défini par la RFC 1994 est un protocole d'authentification basé sur la résolution d'un « défi » (en anglais « *challenge* »), c'est-à-dire une séquence à chiffrer avec une clé et la comparaison de la séquence chiffrée ainsi envoyée.

PAP : Le protocole PAP (*Password Authentication Protocol*) est, comme son nom l'indique, un protocole d'authentification par mot de passe. Le protocole PAP a été originalement utilisé dans le cadre du protocole PPP.

REFERENCES

Cisco Systems Description de la gamme Cisco NAC [En ligne]. - 2006. - 4 Février 2015.

Network Access Control (Contrôle d'accès au réseau) [En ligne]. - 2007. - 2 Mars 2015.

Compréhension des composants NAC de base Centre d'aide LANDESK [En ligne] // site Web

Pujolle Guy : Les réseaux [Livre]. - [s.l.] : Eyrolles, 2008. - p. 880.

Vincent REMAZEILLES : La sécurité des réseaux avec Cisco [Livre]. -[s.l.] : Editions ENI, 2009.p 40.

Le contrôle d'accès : http://www.frame.fr/index.php?page=controle-d-acces-reseau

NAC principe : https://www.blackbox.fr/fr-fr/page/24894/Information/Technique/black-box-explique/LAN/nac--controle-dacces-reseau

Installation de l'ISE : http://www.cisco.com/c/en/us/td/docs/security/ise/1-1-1/installation_guide/ise_install_guide/ise_vmware.html

CISCO ISE : http://www.cisco.com/web/FR/products/security/cisco_ise.html

Les VLANs : http://www-igm.univ-mlv.fr/~dr/XPOSE2006/SURZUR-DEFRANCE/vlanport.html