Fiche savoirs technologiques 5 : Filtrage protocolaire

Dans cette partie, vous allez reprendre l'architecture présentée dans la fiche N°1 et mettre en place des règles de filtrage afin de sécuriser l'accès à votre réseau et interdire certains flux. Phase 5 Filtrage protocolaire La mise en place d'une politique de filtrage, permet à l'administrateur de définir les règles qui permettront d'autoriser ou de bloquer les flux au travers de l'UTM Stormshield Network. Selon les flux, certaines inspections de sécurité (analyse antivirale, analyse antispam, filtrage URL, ...) peuvent être activées (nous détaillerons ces analyses dans le chapitre « Filtrage applicatif »). Les règles de filtrage définies doivent respecter la politique de sécurité de l'entreprise. 5.1 - Présentation des fonctionnalités Pour définir un flux, une règle de filtrage se base sur de nombreux critères ; ce qui offre un haut niveau de granularité. Parmi ces critères, il est notamment possible de préciser : l'adresse IP source et/ou destination ; la réputation et la géolocalisation de l'adresse IP source et/ou destination ; l'interface d'entrée et/ou sortie ; l'adresse réseau source et/ou destination ; le FQDN source et/ou destination ; la valeur du champ DSCP ; le service TCP/UDP (n° de port de destination) ; le protocole IP (dans le cas d'ICMP, le type de message ICMP peut être précisé) ; l'utilisateur ou le groupe d'utilisateurs devant être authentifié. Le nombre de règles de filtrage actives dans une politique est limité. Cette limite dépend exclusivement du modèle de firewall SNS. Le premier paquet appartenant à chaque nouveau flux reçu par le pare-feu est confronté aux règles de filtrage de la première à la dernière ligne. Il est donc recommandé d'ordonner au mieux les règles de la plus restrictive à la plus généraliste. Par défaut, tout trafic qui n'est pas autorisé explicitement par une règle de filtrage est bloqué. Les firewalls SNS utilisent la technologie SPI (Stateful Packet Inspection) qui leur permet de garder en mémoire l'état des connexions TCP et des pseudo-connexions UDP et ICMP afin d'en assurer le suivi et de détecter d'éventuelles anomalies ou attaques. La conséquence directe de ce suivi « Stateful » est l'autorisation d'un flux par une règle de filtrage uniquement dans le sens de l'initiation de la connexion ; les réponses faisant partie de la même connexion sont implicitement autorisées. Ainsi, nous n'avons nul besoin d'une règle de filtrage supplémentaire pour autoriser les paquets réponse d'une connexion établie au travers du firewall. La figure suivante présente l'ordre d'application des règles de filtrage et de NAT, il est important de noter que les paquets sont filtrés avant d'être « natés » c'est pourquoi nous avons mis au point les règles de NAT avec une politique Pass all.

Retour Accueil Stormshield

- Stormshield