Rapport VPN isec

Ce rapport présente en la mise en place d'un tunnel IPsec entre deux sites distants. L'objectif de cette mission était d'établir une connexion sécurisée et fiable entre deux LAN (réseaux locaux) utilisant des pare-feu Stormshield. Pour cela, nous avons configuré un premier Stormshield, créé une règle dans les paramètres VPN IPsec pour établir un lien entre le LAN du Stormshield A et le LAN du stormshield B. Ensuite, nous avons appliqué des règles de filtrage pour autoriser la communication entre ces deux réseaux. Enfin, nous avons répété les mêmes étapes pour le deuxième Stormshield et testé la communication entre les sites.

La première étape a été de configurer le premier Stormshield pour établir le tunnel IPsec. Nous avons paramétré les informations nécessaires, notamment créé une règle dans les paramètres VPN IPsec pour établir un lien sécurisé entre les deux LAN.

Pour cela il fallait ajouter une règle de site à site en précisant comme adresse local le network intérieur du Stormshield A, mettre en correspondant le réseau intérieur du Stormshield B et ajouter dans la case réseau distant l’ip de l’interface du Stormshield B auxquelles nous sommes branchés.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Une fois le tunnel IPsec établi, nous configurons les règles de filtrage appropriées pour autoriser la communication entre les deux LAN. Cela impliquait d'ajouter des règles spécifiques dans le pare-feu du Stormshield pour permettre le trafic entrant et sortant entre les réseaux.

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

Pour cela nous activons une règle qui autorise l’accès avec en source notre réseau intérieur du Stormshield A via le tunnel que nous avons créé pour appliquer la règle du site à site et comme destination, l’interface WAN sur laquelle nous sommes branchés, et nous activons une deuxième règle qui autorise la même chose mais de l’autre sens. C’est-à-dire depuis l’interface WAN via le VPN en source puis notre réseau intérieur en destination.

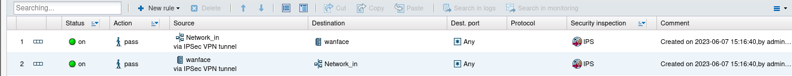
Nous avons à ce stade configurer le Stormshield A pour le tunnel VPN entre deux sites.

Il faut maintenant recommencer ces mêmes configurations mais de l’autre côté, sois sur le Stormshield B.

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquementVoici ci-dessous la règle permettant de faire un lien VPN entre le réseau intérieur du Stormshield B et le réseau intérieur du Stormshield A via l’interface du Stormshield A sur laquelle nous sommes branchés.

Ensuite, ci-dessous les règles dans les filtrages qui ont été ajoutés pour permettre cette fois ci la communication du réseau intérieur du Stormshield B via le tunnel que nous avons créé à l’interface WAN sur laquelle nous sommes branchés (première règle). Et la même chose de l’autre côté en autorisant l’accès avec comme source l’interface WAN via le VPN ou nous sommes branchés et la destination qui est notre réseau intérieur.



Suite à cela nous branchons des PC Clients sur chaque côté des réseaux intérieurs des Stormshield, sois un pc brancher au LAN du Stormshield A et un PC branché au LAN du Stormshield B.

Notre adresse réseau du LAN A est 192.168.1.0/24

Notre réseau du LAN B est 192.168.215.0/24

Voici ci-dessous un ping d’un client dans le LAN A à l’interface du réseau LAN B. Nous pouvons apercevoir que nous avons une IP en 192.168.1.1 et que nous communiquons avec une IP du LAN en face sois 192.168.215.254.

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement