

Mise en œuvre d'un équipement de gestion unifiée des menaces informatiques

Situation 1 : Premiers paramétrages d'un pare-feu sur un site de l'entreprise

Fiches Stormshield associées :

- Fiche 1 – Initialiser un Pare-feu SNS
- Fiche 2 – Prise en main d'un Pare-feu SNS
- Fiche 3 – Gestion des journaux
- Fiche 4 – Configuration du réseau

La phase d'analyse préalable est terminée. Elle a abouti sur un schéma réseau logique et votre architecture est maquettée sur Packet Tracer.

L'architecture relative au siège de CUB est opérationnelle.

Vous travaillerez en binôme, et chacun aura en charge une agence : Anvers, Barcelone ou Californie.

I Configuration des commutateurs de l'infrastructure

Cette partie doit éventuellement être modifiée par le professeur en fonction de l'infrastructure du réseau de sa section.

Les commutateurs pour le réseau du siège sont opérationnels. Des modifications doivent être effectuées pour permettre l'interconnexion avec les agences.

Par ailleurs, il est nécessaire d'ajouter un nouveau commutateur par agence pour l'interconnexion des différents services (administration, production et client).

1. Lister les éléments de configuration à effectuer sur les commutateurs de l'infrastructure. *Une fois validés, ces paramétrages seront réalisés par le professeur.*
2. Configurer le commutateur SW-LAN-XX (avec XX correspondant au nom de votre agence).

II Configuration de base du pare-feu Stormshield

Le pare-feu SN210 que vous venez de recevoir est en configuration usine. Si ce n'est pas le cas, il est nécessaire de remettre sa configuration à zéro en suivant la procédure présente dans la fiche 1.

Il vous est donc demandé dans un premier temps d'assurer les premières configurations du boîtier afin que ce dernier soit fonctionnel au sein de votre agence.



Pour cette première configuration, vous aurez uniquement besoin d'un poste client, votre équipement ne sera intégré à l'infrastructure qu'une fois que ces paramétrages réalisés.

1. Renommer le pare-feu (exemple pour l'agence d'Anvers : FW-Anvers).
2. Assurez-vous que la stratégie de complexité des mots de passe préconisée par l'ANSSI est effective pour le compte administrateur.
3. Assurez-vous que l'horodatage des événements est bien correct. Pour cela la date et l'heure doivent correspondre au fuseau horaire Europe/Paris et doivent être synchronisées sur les serveurs NTP de la société Stormshield.



À ce stade la synchronisation est préparée mais ne sera effective que lorsque le pare-feu sera connecté à Internet.

4. Pourquoi est-il primordial que l'ensemble des pare-feu de l'entreprise CUB soit synchronisé sur des serveurs NTP ?
5. L'accès au log est par défaut restreint. Il faut, en effet, effectuer une démarche spécifique (clic sur un lien) pour accéder à toutes les données et cet accès est alors lui-même tracé. Expliquez-en les raisons.
6. Configurer les interfaces réseaux du pare-feu afin que cela corresponde à ce que vous avez défini précédemment dans votre schéma réseau logique. *Si des VLAN sont implémentés, la création de sous-interfaces pour assurer le routage inter-VLAN est recommandée.*
7. Dans le menu Filtrage et NAT, appliquer temporairement la politique de filtrage « Pass All » afin d'éviter des blocages ou erreurs liés à cette dernière.
8. Procéder à l'intégration physique des nouveaux équipements (commutateur et pare-feu).
9. Réaliser une recette de la situation à l'aide de tests de connectivité entre les équipements de votre agence mis en place.
10. Procéder à la sauvegarde de votre configuration.

NB : Dans le cadre de cette activité, il a été décidé, pour des contraintes organisationnelles, de n'avoir qu'un seul pare-feu réalisant le filtrage interne et externe ainsi que le routage inter-vlan. Dans une situation optimale, l'utilisation d'un pare-feu interne et d'un pare-feu externe de constructeurs différents est conseillée. Le routage inter-vlan devrait être réalisé par le pare-feu interne ou un commutateur de niveau 3 avec ACL dédié à cet usage.

III Analyse du routage et configuration de la translation d'adresse

1. Rédiger la table de routage du pare-feu. Attention ! **Ne pas oublier que le réseau WAN est un réseau public.**
2. Déterminer quelle adresse IP présente sur le réseau WAN doit servir de passerelle au pare-feu en cours de configuration pour aller sur Internet. Puis créer un objet réseau afin que cette adresse IP soit représentée dans l'interface d'administration.
3. Utiliser cet objet afin de pouvoir implémenter la table de routage sur votre pare-feu.

Les adresses IP privées utilisées sur les différents sites sont des adresses IP privées (RFC 1918), c'est-à-dire non routables sur Internet et donc également non routables sur le réseau WAN public de CUB.

4. Proposer et paramétrer une solution technique permettant aux adresses IP privées de votre site de pouvoir communiquer sur le réseau WAN public et Internet.
5. Peut-on joindre le pare-feu général CUB puis les serveurs présents dans la DMZ du siège de l'entreprise ? Proposer une analyse des résultats obtenus.

Rappel pour les professeurs : la production est validée pour le firmware SNS 4.3.15 ou ultérieure (branche LTS).

6. Si le firmware XXXX n'est pas présent, mettre à jour le firmware du pare-feu.

Après la mise à jour du firmware, il se peut que les logs ne soient plus accessibles, il est nécessaire d'ajouter un support tel qu'une carte SD.

7. Procéder à cet ajout.
8. Réaliser une recette permettant de valider les objectifs de la situation 1.
9. Pour conclure, lister les objets réseaux implicites et explicites que vous avez eu besoin de mobiliser précédemment.

Documents

Document 1 – Extrait des recommandations de l'ANSSI concernant la sécurité relative aux mots de passe

Voici quelques recommandations :

- Utilisez un mot de passe unique pour chaque service. En particulier, l'utilisation d'un même mot de passe entre sa messagerie professionnelle et sa messagerie personnelle est impérativement à proscrire ;
- Choisissez un mot de passe qui n'a pas de lien avec vous (mot de passe composé d'un nom de société, d'une date de naissance, etc.) ;
- Ne demandez jamais à un tiers de générer pour vous un mot de passe ;
- Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent ;
- Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles ;
- Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur Internet), encore moins sur un papier facilement accessible ;
- Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle ;
- Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe choisis.
- La robustesse d'un mot de passe dépend en général d'abord de sa complexité, mais également de divers autres paramètres, expliqués en détail dans le document Recommandations de sécurité relatives aux mots de passe.

Si vous souhaitez une règle simple : choisissez des mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux).

Deux méthodes pour choisir vos mots de passe :

1. La méthode phonétique : « J'ai acheté huit cd pour cent euros cet après-midi » deviendra ght8CD %E7am ;
2. La méthode des premières lettres : la citation « un tien vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.