Stormshield – Prise en main des fonctionnalités de base du pare-feu

Programme *(Mis à jour le 24/04/2024)*

Rappel sur les réseaux

- Les différentes topologies
- Le modèle OSI
- Calcul de sous réseaux
- Les plans d'adressage (privé, public, multicast …)
- Le routage statique

Présentation de Stormshield

- L'origine du projet
- Les fonctionnalités et plugins disponibles
- Les différentes installations possibles
- Les offres de support

Opérations de maintenance

- Présentation des interfaces (WAN, LAN, OPT1 …)
- Création des interfaces et renommage
- Présentation et personnalisation de l'interface
- Maintenance du pare-feu(redémarrage, mise à jour etc …)
- LAB 1 : mise à jour

Les objets réseaux

- Les différents objets réseaux et objets implicites
- Créations des alias (IPs, Groupes, Sous-Réseaux)

Règles de filtrage et NAT

- Quelques rappels sur la NAT et le modèle OSI
- La NAT (Network Adress Translation)
- Description – Dans quel cas utiliser de la NAT ?
- Les différents types de NAT possible
- Les IPs virtuelles
- LAB 2 : Tests de connectivité et mise en place de la NAT
- Le filtrage
- Quelques rappels sur IP et TCP
- Parefeu stateless vs parefeu stateful
- Mise en place de règles de filtrage
- LAB 3 : Création de règles sur différents types de trafic (icmp, http, ftp)

Problèmes courants et résolution

- Visualisation des journaux
- Résolution d'incident
  – Connectivité
  – Plan d'adressage et masque
  – Règles de routage
  – Règles de NAT
  – Règles de filtrage
- LAB 4 : Simulation d'incidents et aide à la résolution

Référence
THIS2325

Durée
3 jours / 21 heures

Prix HT / stagiaire
2550€

Objectifs pédagogiques

- Utiliser les fonctionnalités d'un pare-feu Stormshield
- Mettre en oeuvre une stratégie de sécurité avec Stormshield

Niveau requis

- Garantir avoir une connaissance de bases du modèle OSI, Windows, Unix, Réseau
- Une base en sécurité des systèmes d'information est requise (sécurité des réseaux, sécurité des systèmes, etc…)

Public concerné

- Responsables et Directeurs Informatiques, Qualité, Consultant et experts en Sécurité

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d'accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation de handicap peuvent avoir des besoins spécifiques pour suivre la formation. N'hésitez pas à nous contacter pour en discuter) équipée d'un ordinateur de dernière génération par stagiaire, réseau haut débit et vidéo-projection UHD
Documents supports de formation projetés
Apports théoriques, étude de cas concrets et exercices
Mise à disposition en ligne de documents supports à la suite de la formation

Dispositif de suivi de l'éxécution de l'évaluation des résultats de la formation

Feuilles d'émargement (signature électronique privilégiée)
Evaluations formatives et des acquis sous forme de questions orales et/ou écrites (QCM) et/ou mises en situation
Questionnaires de satisfaction (enquête électronique privilégiée)

Haute disponibilité

- Principes de la haute disponibilité
- Le fonctionnement sous Stormshield (modes, synchronisation)
- Opérations de maintenance en haute disponibilité
- LAB 5 : Mise en route d’un cluster Stormshield et tests de bascule

VPN

- Principes des VPN
- Le fonctionnement sous Stormshield (modes, synchronisation)
- Opérations de maintenance sur les VPN
- LAB 6 : Mise en œuvre des VPN

Conclusion

- Annexes : liens utiles, bibliographie et webographie