

Symantec ProxySG V6.6 – Administration basique

Formation Informatique / Réseaux et Sécurité / Sécurité



Le cours d'administration basique Symantec ProxySG v6.6 est un cours d'introduction aux options de déploiement et à la gestion des différentes fonctionnalités clés offertes par la solution ProxySG v6.6. C'est un cours d'introduction et conçu pour les étudiants qui découvrent Proxy SG.

OBJECTIFS

- Réussir la certification **Symantec ProxySG V6.6 – Administration basique**
- Comprendre les concepts basés sur **Symantec ProxySG V6.6 – Administration basique**
- Comprendre les fondamentaux et la méthodologie
- Préparer, Réviser et Acquérir les trucs et astuces de l'examen **Symantec ProxySG V6.6 – Administration basique**.

PUBLIC

Le cours Symantec « BlueCoat ProxySG – Administration basique » est destiné aux étudiants qui souhaitent maîtriser les fondamentaux de Symantec BlueCoat ProxySG. Il est conçu pour les étudiants qui n'ont pas suivi de cours de formation antérieurs sur le ProxySG.

PRE-REQUIS

Les étudiants doivent avoir une compréhension de base des concepts de réseau, tels que les réseaux locaux (LAN), Internet, la sécurité et les protocoles IP.

PROGRAMME

Module 1 : Introduction à la passerelle Web sécurisée Symantec ProxySG

- Décrire les fonctions d'un serveur proxy
- Différencier les serveurs proxy des pare-feu
- Décrire les principales fonctionnalités et avantages de Symantec ProxySG
- Les différents modèles ProxySG
- Ressources communautaires en ligne de Symantec

Module 2 : Options de déploiement de sécurité ProxySG

- 3 méthodes de déploiement du réseau
- 3 rôles possibles du ProxySG
- Module 3 : console de gestion ProxySG
- Relation entre la console de gestion et la CLI ProxySG
- Fonction principale des principaux domaines de la console de gestion
- Accéder à l'aide intégrée et à la documentation du produit Symantec

Module 4 : Interception de trafic utilisant des services proxy

- Comprendre les fonctions des services proxy, des auditeurs et des types de proxy
- Décrire les trois services proxy les plus courants
- Expliquer comment les paramètres d'interception et de contournement affectent ce qui arrive au trafic réseau passant par le ProxySG
- Expliquer la fonction des paramètres du service proxy global commun

Module 5 : protocole de transfert hypertexte (HTTP)

- Comprendre comment une connexion est lancée sur la couche de transport
- Identifier les composants d'une URL HTTP
- Expliquer les deux types de messages HTTP: requête et réponse
- Identifier les codes de réponse communs

Module 6 : Introduction au Gestionnaire de politique visuelle

- La relation entre le VPM, le CPL et la console de gestion
- L'ordre de traitement par défaut pour les couches et les règles de la politique
- Les déclencheurs et les actions qui peuvent être utilisés dans la politique d'écriture
- Identifier les types d'objets que le VPM prend en charge
- Quelques recommandations à suivre lors de l'utilisation du VPM pour créer une stratégie

Module 7 : filtrage du contenu Web

- Les principaux concepts de filtrage Web
- Les bases de données de la catégorie primaire
- Les types de catégories disponibles pour la politique
- Comment BlueCoat WebFilter et WebPulse fonctionnent ensemble

Module 8 : Utilisation de l'Intelligence de menace pour défendre le réseau



A retenir

Durée : **2 jours** soit 14h.
Réf. **SYMBA**

☎ 01 42 93 52 72

Dates des sessions

Paris
25/06/2018
01/10/2018

Cette formation est également proposée en formule **INTRA-ENTREPRISE.**



Inclus dans cette formation



Coaching Après-COURS

Pendant 30 jours, votre formateur sera disponible pour vous aider. CERTyou s'engage dans la réalisation de vos objectifs.

100%
SATISFACTION
GARANTIE

Votre garantie 100% SATISFACTION

Notre engagement 100% satisfaction vous garantit la plus grande qualité de formation.

- Le Global Intelligence Network
- Les niveaux de géolocalisation et de risque de menace et leur utilisation dans une politique

Module 9 : Assurer des téléchargements sécurisés Comment le malware peut être transmis via http

- Les méthodes, avantages et inconvénients de la détection du type de fichier
- Considérations pour décider quel contenu bloquer les sources possibles de logiciels malveillants

Module 10 : Notification de l'utilisateur des politiques d'utilisation d'Internet

- Expliquer la fonction et les différents composants des pages d'exception intégrées et personnalisées
- Décrire les objets "Notify User"
- Identifier les types de pages pouvant être envoyées aux utilisateurs en utilisant les objets Notify User
- Décrire les pages splash et les pages de coaching en utilisant les objets Notify User dans le VPM

Module 11 : Accès à l'ouverture de session sur ProxySG

- Décrire, à haut niveau, comment le ProxySG effectue l'enregistrement d'accès
- Décrire les composants d'une installation de journal d'accès ProxySG
- Identifier les installations de journal et les formats de journal par défaut
- Décrire les cas d'utilisation courante pour le téléchargement périodique et continu des journaux d'accès

Horaires, Planning et Déroulement de cette formation

Horaires

- Formation de 9h00 (9h30 le premier jour) à 17h30.
- Deux pauses de 15 minutes le matin et l'après-midi.
- 1 heure de pause déjeuner

DEROULEMENT

- Les horaires de fin de journée sont adaptés en fonction des horaires des trains ou des avions des différents participants.
- Une attestation de suivi de formation vous sera remise en fin de formation.
- Cette formation est organisée pour un maximum de 14 participants.

PROCHAINES FORMATIONS

[Réussir la Certification Gestion de Projet PMP du PMI](#)

[Réussir la Certification PRINCE2 Foundation](#)

[Réussir les Certifications PRINCE2 Foundation et PRINCE2 Practitioner](#)

[Réussir la Certification ITIL Foundation](#)

[Réussir la Certification Agile certifié SCRUM Master](#)

[Réussir les Certifications TOGAF Certified et TOGAF Foundation](#)

Retrouvez cette formation sur notre site :

[Symantec ProxySG V6.6 – Administration basique](#)