

Symantec Sygate Enterprise Protection 5.1

DESCRIPTIF DU COURS

Ce cours d'une durée de cinq jours, dispensé par un formateur et comprenant des travaux pratiques couvre la conception et le déploiement de Symantec Policy Manager et Protection and Enforcement Agents. Vous apprendrez également à implémenter une protection accrue en installant Gateway, DHCP, and LAN 802.1x Enforcers pour les environnements sans fil.

Mode d'administration

Cours dispensé par un formateur

Durée

Cinq (5) jours

Objectifs du cours

A la fin de ce cours vous serez en mesure de :

- Identifier les composants produit et réseau.
- Installer, configurer, et administrer Policy Manager.
- Installer, configurer, et administrer les agents.
- Installer, configurer, et administrer Enforcers.
- Gérer les politiques de pare-feu avancées.
- Configurer la prévention d'intrusion.
- Utiliser Host Intrusion Prevention (HIPS).
- Créer des politiques d'intégrité de l'hôte.
- Améliorer la sécurité avec Symantec Network Access Control (SNAC).
- Distribuer des logiciels agents aux clients.

Audience concernée

Le cours *Symantec Sygate Enterprise Protection 5.1* est conçu pour les professionnels de l'informatique responsables de la conception et du déploiement de Symantec Policy Server et Symantec Security Agents et Enforcers. Ce cours est également conçu pour tout personnel de help desk de troisième niveau qui offre un support avancé sur le fonctionnement de la suite logicielle Symantec Enterprise Protection 5.1.

Prérequis

Vous devez avoir de bonnes connaissances sur le fonctionnement des pare-feux, de la prévention d'intrusion et de la définition de la politique de sécurité réseau, en plus de connaissances solides des protocoles de communication IP, Microsoft SQL Server, Windows 2000/2003 Server, et des solutions d'accès à distance et notamment les technologies VPN et réseaux WLAN.

Travaux pratiques

Ce cours comprend des travaux pratiques et des démonstrations vous permettant de tester vos nouvelles connaissances et les appliquer à votre environnement de production.

PLAN DU COURS

Identification des composants produit et réseau

- Positionnement des composants Symantec Sygate Enterprise Protection
- Description des fonctions de Symantec Sygate Enterprise Protection
- Contrôle de l'accès réseau à l'aide de Gateway, LAN (802.1x), et DHCP Enforcers
- Description des fonctions réseau d'un pare-feu d'application

Installation de Policy Manager

- Définition des conditions d'installation
- Utilisation de Policy Manager Console
- Installation de la base de données
- Partage de données entre bases de données

Gestion de Policy Manager

- Etablissement de divers niveaux de contrôle d'accès
- Gestion d'administrateurs de domaines
- Définition de droits et privilèges d'accès
- Affectation et test des droits et privilèges d'accès

Configuration de composants du côté serveur

- Gestion de sites uniques ou multiples
- Synchronisation avec les serveurs de répertoire
- Configuration de HTTPS
- Gestion de la base de données
- Gestion d'Enforcers et réplique

Gestion de Client Manager

- Administration des utilisateurs, ordinateurs, groupes et agents
- Réalisation de mises à jour de logiciels
- Exportation de paquets de logiciels

Gestion des politiques

- Application de la gestion des politiques
- Définition des emplacements
- Gestion des politiques de protection des pare-feu, HIP, et système d'exploitation

Interprétation des notifications d'événements

- Différenciation entre types de notifications
- Configuration et dépannage de notifications d'événements de serveurs
- Personnalisation de la structure de notification
- Configuration de paramètres complémentaires

Description de Symantec Protection Agent

- Identification des composants de Symantec Protection Agent
- Définition des fonctions principales
- Définition des conditions d'installation
- Examen des communications entre le serveur et les agents
- Définition de l'impact du système

Installation de Symantec Protection Agent

- Récupération et création de paquets de logiciels
- Examen des conditions d'installation
- Installation de Protection Agent
- Définition des paramètres de Protection Agent
- Analyse des journaux des agents

Définition des modes de Protection Agent

- Capacité des utilisateurs à personnaliser leurs paramètres de sécurité
- Configuration de tous les paramètres afin qu'ils soient contrôlés par Policy Manager
- Configuration des paramètres afin qu'ils soient partagés par l'utilisateur et Policy Manager

Contrôle de l'expérience utilisateur

- Définition du niveau d'exposition
- Configuration des éléments de protection
- Configuration des notifications

Dépannage de Protection Agent

- Vérification des fonctions du système d'exploitation et de l'agent
- Analyse des journaux
- Identification des applications bloquées
- Importation et exportation de profils
- Validation de la connectivité de Policy Manager

Dépannage de Policy Manager

- Analyse des journaux
- Confirmation des fonctionnalités de Policy Manager
- Vérification de l'exécution correcte des règles
- Contacter le support

Contrôle des rapports et journaux

- Identification et analyse des rapports
- Utilisation de l'outil de requête de données
- Analyse des journaux des serveur, agent et Enforcer

Déploiement de Symantec Sygate Enterprise Protection

- Réalisation d'une évaluation

- Développement d'une architecture
- Réalisation d'un test de fonctionnement
- Réalisation d'un test utilisateur de pré-production
- Exécution du déploiement de production
- Réalisation de l'administration courante et tuning

Gestion de groupes

- Visualisation de concepts de groupes
- Affectation d'agents à un groupe temporaire
- Héritage et recommandations

Configuration d'emplacements

- Description des concepts d'emplacements
- Examen des applications et héritage courants
- Travail avec les emplacements et les groupes
- Affectation de déclencheurs aux emplacements
- Configuration de l'intégrité de l'hôte
- Identification des emplacements et configurations recommandés

Création de politiques de pare-feu avancées

- Définition de la sévérité des règles
- Déplacement des règles
- Importation et exportation de politiques
- Configuration de paramètres généraux et avancés

Configuration de la prévention d'intrusion

- Description des concepts de prévention d'intrusion
- Activation de la prévention d'intrusion
- Configuration de la prévention d'intrusion pour les groupes
- Gestion des bibliothèques de signatures et détails

Présentation de Host Intrusion Prevention (HIPS)

- Description des concepts Host IP
- Examen de la protection du système d'exploitation
- Application du verrouillage du système
- Restriction des applications avec des empreintes de fichiers
- Empêchement de l'exécution de programme

Création de politiques d'intégrité de l'hôte

- Description des fonctionnalités et concepts clés
- Ajout et gestion de politiques
- Définition des conditions des politiques
- Utilisation de conditions prédéfinies

Application de la sécurité avec Symantec Network Access Control

- Description des concepts et approche
- Application de la conformité aux politiques de sécurité via l'auto-application
- Installation et gestion de Gateway Enforcer
- Installation et gestion de LAN Enforcer (802.1x)
- Installation et gestion de DHCP Enforcer

Distribution du logiciel agent

- Planification de la distribution d'agents
- Déploiement d'agents



- Mise à jour d'agents
- Personnalisation de builds d'agents