



Cisco : Formation Réseaux, Infrastructure et Collaboration

Sécurité

5- Mettre en oeuvre Cisco Intrusion Prevention System v7

Durée: 5 Jours

Réf de cours: IPS

Version: 7

Résumé

Cette formation permet aux stagiaires d'acquérir les connaissances et compétences nécessaires pour déployer IPS (Cisco Intrusion Prevention System). Ils seront ainsi capables de limiter les risques sur les applications et infrastructures utilisant les fonctionnalités Cisco IPS.

Pré-requis

Avoir suivi les formations Cisco ICND1, ICND2 et IINS ou posséder les connaissances équivalentes. La connaissance de Windows est conseillée.

Public visé

Cette formation est conçue pour les ingénieurs sécurité réseau qui mettent en œuvre les solutions Cisco IPS ainsi que les personnes qui cherchent à obtenir la certification CCNP Sécurité.

Certification

- Cette formation, dans sa version 6.0, prépare au passage de l'examen de certification Cisco 642-533, lequel permet d'obtenir en partie le titre de **certification CCSP - Cisco Certified Security Professional**. Cet examen disparaît au 31/05/2011.
- Dans sa version 7, l'examen de certification correspondant est le **642-627**, préparant au titre de certification Cisco **CCNP Sécurité**.

Objectifs

A l'issue de cette formation, les stagiaires seront capables de :

- Evaluer les produits et les architectures de déploiement pour la ligne de produits Cisco IPS
- Choisir l'emplacement idéal pour la sonde Cisco IPS
- Mettre en œuvre une stratégie de sécurité à l'aide des sondes Cisco IPS en concordance avec les stratégies locales et les besoins de l'entreprise
- Déployer des stratégies personnalisées pour adapter l'analyse et les réponses de l'IPS au trafic de l'environnement de l'entreprise
- Gestion et analyse de la base de données du Cisco IPS
- Mettre en œuvre la virtualisation d'une stratégie complexe Cisco IPS, la haute disponibilité et les solutions de haute performance en accord avec les stratégies locales et les besoins de l'entreprise
- Effectuer la configuration initiale et la maintenance spécifique de l'IPS Cisco

Contenu

Introduction à la prévention et la détection d'intrusion, le logiciel Cisco IPS et les périphériques supportés

- Evaluer la prévention d'intrusion et les systèmes de détection d'intrusion
- Choisir les logiciels et matériel IPS ainsi que les applications supportées
- Evaluer l'analyse du trafic réseau IPS, les méthodes, les possibilités «d'évasion» et «anti-évasive contremesures»
- Choisir l'architecture de déploiement de réseaux IPS et IDS

Installation et maintenance des sondes Cisco IPS

- Intégrer la sonde Cisco IPS dans un réseau
- Améliorer la configuration initiale des sondes Cisco IPS
- Gérer les périphériques Cisco IPS

Appliquer les stratégies de sécurité Cisco IPS

- Configurer l'analyse de base du trafic
- Mettre en œuvre les signatures Cisco IPS et les réponses*
- Configurer la «signature Engine» et la base de données signatures de Cisco IPS
- Déployer l'opération «anomalie»

Adaptation de l'analyse du trafic et des réponses à l'environnement

Gestion et analyse des événements

- Installer et intégrer Cisco IPS Manager Express avec les sondes Cisco IPS
- Gérer les événements à l'aide de Cisco IPS Manager Express
- Utiliser Cisco IME Rapports et notifications
- Intégrer Cisco IPS avec Cisco Security Manager et Cisco Security MARS
- Utiliser la base de données et les services IntelliShield

Déploiement de la virtualisation, de la haute disponibilité et les solutions de Haute Performance

- Utiliser les sondes virtuels Cisco IPS
- Déployer Cisco IPS pour la haute disponibilité et la haute performance

Configurer et maintenir le matériel spécifique Cisco IPS

- Configurer et maintenir Cisco ASA AIP SSM et les modules AIP SSC
- Configurer et maintenir Cisco ISR IPS AIM et les modules IPS NME
- Configurer et maintenir le module Cisco IDSM-2

- Personnaliser l'analyse du trafic
- Gérer les faux positifs et négatifs
- Améliorer la qualité des alarmes et des réponses

