Table des matières : Documents TAC sur le service FirePOWER, le système FireSIGHT et AMP

Contenu

[Documents TAC sur FireSIGHT et Firepower System](#)
[Documents TAC sur Advanced Malware Protection](#)

Documents TAC sur FireSIGHT et Firepower System

Mise à jour, réinstallation, migration et installation des logiciels et de la sécurité

- Types de fichiers de mise à jour pouvant être installés sur un système FireSIGHT
- Comprendre les nouvelles terminologies des systèmes FireSIGHT après une migration et une mise à niveau de 4.10.x vers 5.x
- Installer et configurer d'un module de services FirePOWER sur une plateforme ASA
- Installation des services FirePOWER (SFR) sur le module matériel ASA 5585-X
- Déploiement de FireSIGHT Management Center sur VMware ESXi
- Réinstaller un Sourcefire Defense Center et une appliance FirePOWER
- Échec de la mise à jour automatique du téléchargement sur FireSIGHT Management Center
- Instructions de téléchargement des données depuis Firepower Management Center vers les périphériques gérés
- Configurer les services Firepower sur un périphérique ISR avec une lame UCS-E

Licence et configuration de base initiale

- Comparaison des licences de fonctionnalités sur les systèmes FireSIGHT
- Fonctionnalités prises en charge par les différents modèles matériels de systèmes FireSIGHT
- Étapes de configuration initiale des systèmes FireSIGHT
- Enregistrement d'un périphérique avec FireSIGHT Management Center
- Configuration d'un routeur virtuel sur un système FireSIGHT
- Gestion du module SFR sur un tunnel VPN sans commutateur LAN
- Obtenir la clé de licence pour un périphérique Firepower et un module de service Firepower

Vulnérabilité et couverture des règles, analyse des événements et des fichiers

- Télécharger des données de paquets (fichier PCAP) via l'interface utilisateur Web
- Procédures de capture de paquets sur les appliances Sourcefire FirePOWER et les appliances virtuelles NGIPS
- Options pour réduire les événements d'intrusion de faux positifs
- Règles Snort locales personnalisées sur un système FireSIGHT

Détection et prévention des intrusions (IDS/IPS), moteur Snort

- Détermination de l'état par défaut d'une règle fournie par Sourcefire dans une stratégie d'intrusion
- Mesures utilisées pour déterminer les règles par défaut dans une politique de base
- Configuration de la variable SNORT_BPF sur un centre de défense

- Inspection du trafic agrégé des liaisons par Sourcefire FirePOWER et les appliances virtuelles
- Activer le préprocesseur de normalisation en ligne et comprendre l'inspection pré-ACK et post-ACK
- Collecte de fichiers principaux à partir d'une appliance FirePOWER
- Configuration d'une règle d'acceptation sur un système FireSIGHT
- Exclusion des messages EIGRP, OSPF et BGP de l'inspection des intrusions Firepower
- Traitement d'une session à flux unique important (Elephant Flow) par les services Firepower

Intelligence de sécurité, géolocalisation et filtrage des URL

- Exemple de configuration du filtrage des URL sur un système FireSIGHT
- Impossible de télécharger ou de mettre à jour le flux Security Intelligence
- L'adresse IP est bloquée ou mise sur liste noire par l'intelligence de sécurité d'un système FireSIGHT
- Résolution des problèmes de filtrage des URL sur un système FireSIGHT

Contrôle des applications, VDB, découverte du réseau

- FireSIGHT peut identifier un hôte de manière incorrecte ou marquer un événement comme étant en attente ou inconnu

Règle de contrôle d'accès/Pare-feu

- Les événements de connexion semblent disparaître de FireSIGHT Management Center

Interface utilisateur (GUI/CLI), accès utilisateur et authentification

- Intégration de FireSIGHT System avec ISE pour l'authentification des utilisateurs RADIUS
- Intégration du système FireSIGHT avec ACS 5.x pour l'authentification utilisateur RADIUS
- Réinitialiser le mot de passe de l'administrateur sur les systèmes FireSIGHT
- Vérification de l'objet d'authentification sur FireSIGHT System pour l'authentification Microsoft AD sur SSL/TLS
- Identifier les attributs d'objet LDAP Active Directory pour la configuration des objets d'authentification
- Configuration de l'objet d'authentification LDAP sur le système FireSIGHT
- Vérification du certificat LDAP sur SSL/TLS (LDAPS) et CA à l'aide de Ldp.exe

Utilisation du processeur et de la mémoire, performances du réseau et du système

- Instructions de profilage des règles sur le système FireSIGHT
- Collecte de statistiques de performances à l'aide de l'option Analyseur de performances 1 seconde
- Collecte de données à partir d'un système FireSIGHT lorsqu'un réseau rencontre des problèmes de latence
- Dépannage de la suppression de paquets en raison d'une MTU supérieure (paquet surdimensionné)

Administration et maintenance du système

- Redémarrer les processus sur un système FireSIGHT et un service FirePOWER sans redémarrer
- Dépannage des procédures de génération de fichiers par Sourcefire Appliance
- Résolution des problèmes liés au protocole NTP (Network Time Protocol) sur les systèmes FireSIGHT
- Dépannage de l'utilisation excessive des disques sur les appliances Sourcefire
- Configuration de la pile sur les périphériques Cisco Firepower 8000

- Configuration du clustering sur les périphériques des gammes Cisco FirePOWER 7000 et 8000

Fonctionnement du matériel

- Alertes de santé provenant de l'unité d'alimentation du système FireSIGHT
- Dépannage d'un problème de gestion des pannes de courant (LOM) sur un appareil FireSIGHT Management Center ou FirePOWER
- Le système FireSIGHT renvoie le message « Input/Output Error »
- Une appliance FirePOWER se fige après une tentative de démarrage en mode utilisateur unique
- Résolution des problèmes de ventilateurs sur un système FireSIGHT
- Tests de diagnostic à partir de l'écran LCD d'un appareil FirePOWER
- Insertion et retrait d'un module réseau (NetMod) sur un appareil FirePOWER de la gamme 8000
- Identification des problèmes liés aux cartes Network Flow Engine dans les appliances Sourcefire FirePOWER 7000 et 8000
- Préoccupations courantes concernant le kit de rail des appliances FirePOWER 8000
- Instructions d'installation du kit de rail du matériel Firepower 7000
- Un modèle FireSIGHT Management Center FS4000 peut déclencher une alerte d'intégrité « Disque endommagé »
- Procédures de reconfiguration SSD/RAID pour les modèles FireSIGHT Management Center FS2000 et FS4000

Déchiffrement SSL

- Réinstaller une appliance Sourcefire SSL 1500/2000 à la version 3.6 ou ultérieure
- Obtenir un mot de passe BIOS pour un appareil SSL
- Procédures de capture de paquets sur un appareil SSL
- Configuration de SNMP sur un appareil SSL
- Configuration d'un ensemble de règles de base sur un appareil SSL
- Configuration d'une stratégie d'inspection SSL sur le système Cisco FireSIGHT

Intégration avec ISE, Estreamer, SIEM, User Agent, API et Connector

- La connexion à un bureau distant à l'aide du protocole RDP modifie l'utilisateur associé à une adresse IP
- Résolution des problèmes entre le système FireSIGHT et le client eStreamer (SIEM)
- Installation et désinstallation de Sourcefire User Agent
- Résolution des problèmes de connectivité avec Sourcefire User Agent
- Configurer un système FireSIGHT pour envoyer des alertes à un serveur Syslog externe
- Accorder une autorisation minimale à un compte d'utilisateur Active Directory utilisé par l'agent utilisateur Sourcefire
- L'état en temps réel de l'agent utilisateur est affiché comme Inconnu
- Générer des données de dépannage pour le logiciel Sourcefire exécuté sur la plate-forme BlueCoat série X
- Présentation du contrôle d'accès basé sur TrustSec avec Firepower et ISE
- Le service de base de données de Cisco Firepower User Agent ne redémarre pas après un arrêt

Documents TAC sur Advanced Malware Protection

AMP pour terminaux, connecteur FireAMP

- Collecte de données de diagnostic à partir d'un connecteur FireAMP sous Windows
- Collecte de données de diagnostic à partir d'un connecteur FireAMP exécuté sur Mac OSX
- Collecte de données de diagnostic à partir d'un connecteur FireAMP sous Linux
- Image ou clonage d'un ordinateur équipé d'un connecteur FireAMP
- Configuration et gestion des exclusions dans FireAMP
- Suppression des fichiers de cache et d'historique FireAMP sous Windows
- Commutateurs de ligne de commande pour l'installation du connecteur FireAMP
- Désactiver et activer le service client du connecteur FireAMP
- Exécuter le service client Connecteur FireAMP en arrière-plan et masquer l'interface utilisateur
- Mise à niveau d'un connecteur FireAMP sur les systèmes d'exploitation Windows
- Échec de l'arrêt du service de connecteur FireAMP en raison de la protection du connecteur
- Types de fichiers analysés par le connecteur FireAMP
- Guide des exclusions FireAMP sous Windows
- Obtention de données de dépannage sur un appareil Android pour les problèmes de connecteur FireAMP Mobile
- Lancer des analyses planifiées sur FireAMP / AMP for Endpoints
- Analyser les indicateurs de compromission des terminaux avec AMP for Endpoints ou FireAMP
- Installation et configuration du module AMP via AnyConnect 4.x et AMP Enabler
- Déploiement de Cisco AMP for Endpoints avec persistance de l'identité
- Utilisation des événements faux positifs ou faux négatifs d'AMP (Advanced Malware Protection)
- Présentation de l'API Cisco AMP for Endpoint

AMP pour réseau

- Serveurs requis pour les opérations AMP (Advanced Malware Protection)
- Résolution des problèmes de connectivité et d'enregistrement avec AMP sur FireSIGHT Management Center
- Procédure de suppression des connexions entre FireSIGHT Management Center et FireAMP Cloud Console

Nuage

- Installation et configuration du cloud privé FireAMP
- Générer un fichier de snapshot de prise en charge sur un cloud privé FireAMP
- Télécharger un fichier sur la console FireAMP Cloud pour afficher une analyse de fichier récente

Grille contre les menaces (Threat Grid)

- Générer un instantané de prise en charge sur un appareil AMP Threat Grid

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.