Inhalt: TAC-Dokumente zu FirePOWER Service, FireSIGHT System und AMP

Inhalt

[TAC-Dokumente zu FireSIGHT und FirePOWER System](#)
[TAC-Dokumente zu Advanced Malware Protection](#)

TAC-Dokumente zu FireSIGHT und FirePOWER System

Software- und Sicherheitsupdates, Neuzuordnung, Migration und Installation

- Arten von Aktualisierungsdateien, die auf einem FireSIGHT-System installiert werden können
- Kenntnis der neuen Terminologien von FireSIGHT-Systemen nach der Migration und dem Upgrade von 4.10.x auf 5.x
- Installieren und Konfigurieren eines FirePOWER-Servicemoduls auf einer ASA-Plattform
- Installation von FirePOWER (SFR) Services auf ASA 5585-X-Hardwaremodul
- Bereitstellung von FireSIGHT Management Center auf VMware ESXi
- Erneute Image-Erstellung Sourcefire Defense Center und eine FirePOWER-Appliance
- Fehler beim automatischen Herunterladen von Updates in einem FireSIGHT Management Center
- Richtlinien für den Download von Daten vom FirePOWER Management Center auf verwaltete Geräte
- Konfigurieren von FirePOWER Services auf einem ISR-Gerät mit einem UCS-E-Blade

Lizenz und anfängliches grundlegendes Setup

- Vergleich der Funktionslizenzen bei FireSIGHT-Systemen
- Unterstützte Funktionen und Leistungsmerkmale verschiedener Hardwaremodelle des FireSIGHT-Systems
- Schritte zur Erstkonfiguration von FireSIGHT-Systemen
- Registrieren eines Geräts bei einem FireSIGHT Management Center
- Konfiguration eines virtuellen Routers auf einem FireSIGHT-System
- Management des SFR-Moduls über VPN-Tunnel ohne LAN-Switch
- Erwerben Sie den Lizenzschlüssel für ein FirePOWER-Gerät und ein FirePOWER-Servicemodul.

Schwachstellen- und Regelabdeckung, Ereignis- und Dateianalyse

- Herunterladen von Paketdaten (PCAP-Datei) über die Web-Benutzeroberfläche
- Verfahren zur Paketerfassung für Sourcefire FirePOWER-Appliances und virtuelle NGIPS-Appliances
- Optionen zur Reduzierung falsch positiver Angriffsereignisse
- Benutzerdefinierte lokale Snort-Regeln auf einem FireSIGHT-System

Intrusion Detection and Prevention (IDS/IPS), Snort Engine

- Bestimmung des Standardstatus für eine von Sourcefire bereitgestellte Regel in einer Richtlinie für Sicherheitsrisiken
- Kennzahlen zur Bestimmung der Standardregeln in einer Basisrichtlinie

- Konfiguration der SNORT_BPF-Variablen in einem Defense Center
- Überprüfung des Link-aggregierten Datenverkehrs durch Sourcefire FirePOWER und virtuelle Appliances
- Aktivieren des Inline-Normalisierungspräprozessors und Verstehen der Pre-ACK- und Post-ACK-Inspektion
- Sammlung von Kerndateien einer FirePOWER-Appliance
- Konfiguration einer Pass-Regel auf einem FireSIGHT-System
- Ausschluss von EIGRP-, OSPF- und BGP-Nachrichten von der FirePOWER Intrusion Inspection
- Verarbeitung einer großen Single-Stream-Sitzung (Elephant Flow) durch die FirePOWER Services

Sicherheitsinformationen, Geolokalisierung und URL-Filterung

- URL-Filterung in einem FireSIGHT-System - Konfigurationsbeispiel
- Sicherheitsinformations-Feed kann nicht heruntergeladen oder aktualisiert werden
- IP-Adresse wird von der Sicherheitsintelligenz eines FireSIGHT-Systems blockiert oder auf Blacklist gesetzt
- Fehlerbehebung bei Problemen mit der URL-Filterung auf einem FireSIGHT-System

Anwendungskontrolle, VDB, Netzwerkerkennung

- FireSIGHT kann einen Host falsch identifizieren oder ein Ereignis als ausstehend oder unbekannt markieren.

Zugriffskontrollregel/Firewall

- Anscheinend verschwinden Verbindungsereignisse aus dem FireSIGHT Management Center

Benutzeroberfläche (GUI/CLI), Benutzerzugriff und Authentifizierung

- Integration von FireSIGHT-System mit ISE für RADIUS-Benutzerauthentifizierung
- Integration von FireSIGHT System mit ACS 5.x für RADIUS-Benutzerauthentifizierung
- Zurücksetzen des Passworts des Admin-Benutzers auf FireSIGHT-Systemen
- Verifizierung des Authentifizierungsobjekts auf dem FireSIGHT-System für die Microsoft AD-Authentifizierung über SSL/TLS
- Identifizieren von Active Directory-LDAP-Objektattributen für die Authentifizierungsobjektkonfiguration
- Konfiguration des LDAP-Authentifizierungsobjekts auf dem FireSIGHT-System
- Überprüfen Sie LDAP über SSL/TLS (LDAPS) und das CA-Zertifikat mit Ldp.exe

CPU- und Speichernutzung, Netzwerk- und Systemleistung

- Anweisungen zur Regelprofilierung auf FireSIGHT-Systemen
- Erfassung von Leistungsstatistiken mit der Option "Leistungsüberwachung in 1 Sekunde"
- Erfassen von Daten aus einem FireSIGHT-System bei Netzwerkproblemen
- Fehlerbehebung beim Verwerfen von Paketen aufgrund höherer MTU (Oversize Packet)

Systemverwaltung und -wartung

- Starten Sie die Prozesse auf einem FireSIGHT-System und einem FirePOWER-Service ohne Neustart neu.
- Fehlerbehebung bei Sourcefire Appliances - Verfahren zur Dateigenerierung
- Fehlerbehebung bei Problemen mit Network Time Protocol (NTP) auf FireSIGHT-Systemen
- Fehlerbehebung bei übermäßiger Festplattenauslastung auf Sourcefire-Appliances
- Konfiguration von Stack auf Cisco FirePOWER-Geräten der Serie 8000

- Konfiguration von Clustering auf Cisco FirePOWER-Geräten der Serien 7000 und 8000

Hardwarebetrieb

- Statuswarnungen von der Stromversorgungseinheit des FireSIGHT-Systems
- Fehlerbehebung bei einem Problem mit Lights-Out Management (LOM) in einem FireSIGHT Management Center oder einer FirePOWER-Appliance
- FireSIGHT-System gibt Meldung "Input/Output Error" (Eingabe/Ausgabe-Fehler) zurück
- Eine FirePOWER-Appliance wird eingefroren, nachdem versucht wurde, sie im Einzelbenutzermodus zu starten.
- Fehlerbehebung bei Lüfterproblemen in einem FireSIGHT-System
- Durchführen von Diagnosetests über die LCD-Anzeige einer FirePOWER-Appliance
- Einsetzen und Entfernen eines Netzwerkmoduls (NetMod) in einer FirePOWER Appliance der Serie 8000
- Identifizieren von Problemen mit Network Flow Engine-Karten in Sourcefire FirePOWER-Appliances der Serien 7000 und 8000
- Häufige Bedenken hinsichtlich der Schienen-Kits der FirePOWER Appliance der Serie 8000
- Installationsanleitung für das FirePOWER Appliance Rail Kit der Serie 7000
- Ein FireSIGHT Management Center FS4000-Modell löst möglicherweise einen Integritätsalarm "Datenträger heruntergestuft" aus.
- SSD/RAID-Neukonfigurationsverfahren für die FireSIGHT Management Center-Modelle FS2000 und FS4000

SSL-Verschlüsselung

- Erstellen Sie ein neues Image einer Sourcefire SSL-Appliance 1500/2000 auf Version 3.6 oder höher
- BIOS-Kennwort für eine SSL-Appliance abrufen
- Verfahren zur Paketerfassung auf einer SSL-Appliance
- Konfiguration von SNMP auf einer SSL-Appliance
- Konfiguration des grundlegenden Regelsatzes auf einer SSL-Appliance
- Konfiguration einer SSL-Inspektionsrichtlinie auf dem Cisco FireSIGHT-System

Integration mit ISE, Estreamer, SIEM, User Agent, API und Connector

- Anmeldung bei einem Remote-Desktop mit RDP zum Ändern des einer IP-Adresse zugeordneten Benutzers
- Fehlerbehebung bei Problemen zwischen dem FireSIGHT-System und dem eStreamer-Client (SIEM)
- Installation und Deinstallation von Sourcefire User Agent
- Behebung von Verbindungsproblemen mit dem Sourcefire Benutzer-Agent
- Konfigurieren eines FireSIGHT-Systems zum Senden von Warnmeldungen an einen externen Syslog-Server
- Mindestberechtigungen für ein Active Directory-Benutzerkonto gewähren, das vom Sourcefire-Benutzer-Agent verwendet wird
- Der Echtzeitstatus des Benutzer-Agents wird als "Unbekannt" angezeigt.
- Generieren von Fehlerbehebungsdaten für Sourcefire Software auf BlueCoat X-Series-Plattform
- TrustSec-basierte Zugriffskontrolle mit FirePOWER und ISE
- Der Datenbankdienst des Cisco FirePOWER-Benutzeragenten wird nach einem Stopp nicht neu gestartet.

TAC-Dokumente zu Advanced Malware Protection

AMP für Endgeräte, FireAMP-Connector

- Erfassung von Diagnosedaten eines FireAMP Connectors unter Windows
- Sammlung von Diagnosedaten aus einem FireAMP-Connector unter Mac OSX
- Sammlung von Diagnosedaten aus einem FireAMP Connector unter Linux
- Abbild oder Klonen eines Computers mit installiertem FireAMP-Anschluss
- Konfigurieren und Verwalten von Ausschlüssen in FireAMP
- Entfernen des FireAMP-Cache und der Verlaufsdateien unter Windows
- Befehlszeilenschalter für FireAMP Connector Installer
- Deaktivieren und Aktivieren des FireAMP Connector-Client-Service
- Führen Sie den FireAMP Connector Client Service im Hintergrund aus, und blenden Sie die Benutzeroberfläche aus.
- Upgrade eines FireAMP-Connectors unter Windows-Betriebssystemen
- FireAMP Connector-Service wegen Connector-Schutz nicht angehalten
- Dateitypen, die von FireAMP Connector gescannt werden
- FireAMP-Leitfaden für Ausschlüsse unter Windows
- Abrufen von Fehlerbehebungsdaten auf einem Android-Gerät für FireAMP Mobile Connector-Probleme
- Zeitgesteuerte Suche in FireAMP/AMP für Endgeräte
- IOC-Scans (Indication of Compromise) für Endgeräte mit AMP für Endgeräte oder FireAMP
- Installation und Konfiguration des AMP-Moduls über AnyConnect 4.x und AMP Enabler
- Bereitstellung von Cisco AMP für Endgeräte mit Identitätssicherung
- Arbeiten Sie mit AMP (Advanced Malware Protection) bei Fehlalarmen oder Fehlalarmen
- Überblick über die API von Cisco AMP für Endgeräte

AMP für Netzwerke

- Erforderliche Server für Advanced Malware Protection (AMP)
- Behebung von Verbindungs- und Registrierungsproblemen mit AMP in FireSIGHT Management Center
- Prozess zum Entfernen von Verbindungen zwischen einem FireSIGHT Management Center und der FireAMP Cloud-Konsole

Cloud

- Installation und Konfiguration der FireAMP Private Cloud
- Erstellen einer Support-Snapshot-Datei in einer FireAMP Private Cloud
- Datei in FireAMP-Cloud-Konsole hochladen, um aktuelle Dateianalysen anzuzeigen

Threat Grid

- Erstellen eines Support-Snapshots auf einer AMP Threat Grid Appliance