Table of Contents: TAC Documents on FirePOWER Service, FireSIGHT System, and AMP

Contents

TAC Documents on FireSIGHT and Firepower System

Software and Security Update, Reimage, Migration and Installation

License and Initial Basic Setup

Vulnerability and Rule Coverage, Event and File Analysis

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

- Enable the Inline Normalization Preprocessor and Understand Pre-ACK and Post-ACK Inspection
- Collection of Core Files From a FirePOWER Appliance
- Configuration of a Pass Rule on a FireSIGHT System
- Exclusion of EIGRP, OSPF and BGP Messages from the Firepower Intrusion Inspection
- Processing of Single Stream Large Session (Elephant Flow) by the Firepower Services

Security Intelligence, Geolocation and URL Filtering

- URL Filtering on a FireSIGHT System Configuration Example
- Unable to Download or Update the Security Intelligence Feed
- IP Address is Blocked or Blacklisted by the Security Intellegence of a FireSIGHT System
- Troubleshoot Issues with URL Filtering on a FireSIGHT System

Application Control, VDB, Network Discovery

- FireSIGHT May Identify a Host Incorrectly, or Mark an Event as Pending or Unknown

Access Control Rule/Firewall

- Connection Events Appear to Disappear from the FireSIGHT Management Center

User Interface (GUI/CLI), User Access and Authentication

- Integration of FireSIGHT System with ISE for RADIUS User Authentication
- Integration of FireSIGHT System with ACS 5.x for RADIUS User Authentication
- Reset the Password of Admin User on FireSIGHT Systems
- Verification of Authentication Object on FireSIGHT System for Microsoft AD Authentication Over SSL/TLS
- Identify Active Directory LDAP Object Attributes for Authentication Object Configuration
- Configuration of LDAP Authentication Object on FireSIGHT System
- Verify LDAP over SSL/TLS (LDAPS) and CA Certificate Using Ldp.exe

CPU and Memory Utilization, Network and System Performance

- Rule Profiling Instructions on FireSIGHT System
- Collection of Performance Statistics Using "1-Second Performance Monitor" Option
- Collection of Data from a FireSIGHT System When a Network Experiences Latency Issues
- Troubleshoot Dropping of Packets Due to Higher MTU (Oversize Packet)

System Administration and Maintenance

- Restart the Processes on a FireSIGHT System and a FirePOWER Service without a Reboot
- Sourcefire Appliance Troubleshoot File Generation Procedures
- Troubleshoot Issues with Network Time Protocol (NTP) on FireSIGHT Systems
- Troubleshoot Excessive Disk Utilization on Sourcefire Appliances
- Configuration of Stack on the Cisco Firepower 8000 Series Devices
- Configuration of Clustering on Cisco FirePOWER 7000 and 8000 Series Devices

Hardware Operation

- Health Alerts from Power Supply Unit of FireSIGHT System
- Troubleshoot an Issue with Lights-Out Management (LOM) on a FireSIGHT Management Center or a FirePOWER Appliance
- FireSIGHT System Returns "Input/Output Error" Message
- A FirePOWER Appliance becomes frozen after attempting to boot it into single user mode
- Troubleshoot Issues with Fans on a FireSIGHT System
- Perform Diagnostic Tests from the LCD Panel of a FirePOWER Appliance

- Insert and Remove a Network Module (NetMod) on an 8000 Series FirePOWER Appliance
- Identify Issues with Network Flow Engine Cards in Sourcefire FirePOWER 7000 and 8000 Series Appliances
- Common Concerns About FirePOWER 8000 Series Appliance Rail Kit
- Firepower 7000 Series Appliance Rail Kit Installation Instruction
- A FireSIGHT Management Center FS4000 Model May Trigger "Disk Degraded" Health Alert
- SSD/RAID Reconfiguration Procedures for FireSIGHT Management Center Models FS2000 and FS4000

SSL Decryption

- Reimage a Sourcefire SSL Appliance 1500/2000 to Version 3.6 or Greater
- Obtain a BIOS Password for an SSL Appliance
- Packet Capture Procedures on an SSL Appliance
- Configuration of SNMP on an SSL Appliance
- Configuration of Basic Ruleset on an SSL Appliance
- Configuration of an SSL Inspection Policy on the Cisco FireSIGHT System

Integration with ISE, Estreamer, SIEM, User Agent, API, and Connector

- Login to a remote desktop using RDP changes the user associated to an IP address
- Troubleshoot Issues Between FireSIGHT System and eStreamer Client (SIEM)
- Installation and Uninstallation of Sourcefire User Agent
- Troubleshoot Connectivity Issues with Sourcefire User Agent
- Configure a FireSIGHT System to Send Alerts to an External Syslog Server
- Grant Minimum Permission to an Active Directory User Account Used by the Sourcefire User Agent
- The Real-Time Status of User Agent is Shown as Unknown
- Generate Troubleshoot Data for Sourcefire Software Running on BlueCoat X-Series Platform
- Understanding TrustSec-Based Access Control with Firepower and ISE
- Cisco Firepower User Agent Database Service Does not Restart after a Stop

TAC Documents on Advanced Malware Protection

AMP For Endpoints, FireAMP Connector

- Collection of Diagnostic Data from a FireAMP Connector Running on Windows
- Collection of Diagnostic Data from a FireAMP Connector Running on Mac OSX
- Collection of Diagnostic Data from a FireAMP Connector Running on Linux
- Image or Clone a Computer with FireAMP Connector Installed
- Configure and Manage Exclusions in FireAMP
- Removal of the FireAMP Cache and History Files on Windows
- Command Line Switches for FireAMP Connector Installer
- Disable and Enable the FireAMP Connector Client Service
- Run the FireAMP Connector Client Service in the Background and Hide the User Interface
- Upgrade a FireAMP Connector on Windows Operating Systems
- FireAMP Connector Service Fails to Stop due to Connector Protection
- File Types That are Scanned by FireAMP Connector
- FireAMP Guide to Exclusions on Windows
- Obtain Troubleshoot Data on an Android Device for FireAMP Mobile Connector Issues

- Initiate Scheduled Scans on FireAMP / AMP for Endpoints
- Perform Endpoint Indication of Compromise (IOC) Scans with AMP for Endpoints or FireAMP
- Installation and Configuration of AMP Module Through AnyConnect 4.x and AMP Enabler
- Deployment of Cisco AMP for Endpoints with Identity Persistence
- Work with the Advanced Malware Protection (AMP) False Positive or False Negative Events
- Overview of the Cisco AMP for Endpoint API

AMP for Network

- Required Servers for Advanced Malware Protection (AMP) Operations
- Troubleshoot Connectivity and Registration Issues with AMP on FireSIGHT Management Center
- Process to Remove Connections Between a FireSIGHT Management Center and FireAMP Cloud Console

Cloud

- Installation and Configuration of FireAMP Private Cloud
- Generate a Support Snapshot File on a FireAMP Private Cloud
- Upload a File to FireAMP Cloud Console to View Recent File Analysis

Threat Grid

- Generate a Support Snapshot on an AMP Threat Grid Appliance