目录：有关FirePOWER服务、FireSIGHT系统和AMP的TAC文档

目录

FireSIGHT和Firepower系统上的TAC文档
有关高级恶意软件防护的TAC文档

FireSIGHT和Firepower系统上的TAC文档

软件和安全更新、重新映像、迁移和安装

- FireSIGHT系统上可能安装的更新文件类型
- 在从4.10.x迁移并升级到5.x之后，了解FireSIGHT系统的新术语
- 在ASA平台上安装和配置FirePOWER服务模块
- 在ASA 5585-X硬件模块上安装FirePOWER(SFR)服务
- 在VMware ESXi上部署FireSIGHT管理中心
- 重新映像Sourcefire防御中心和FirePOWER设备
- FireSIGHT管理中心上的自动下载更新失败
- 将数据从Firepower管理中心下载到受管设备的准则
- 使用UCS-E刀片在ISR设备上配置Firepower服务

许可证和初始基本设置

- FireSIGHT系统功能许可证比较
- FireSIGHT系统各种硬件型号的支持特性和功能
- FireSIGHT系统的初始配置步骤
- 向FireSIGHT管理中心注册设备
- 在FireSIGHT系统上配置虚拟路由器
- 通过没有LAN交换机的VPN隧道管理SFR模块
- 获取Firepower设备和Firepower服务模块的许可证密钥

漏洞和规则覆盖、事件和文件分析

- 使用Web用户界面下载数据包数据（PCAP文件）
- Sourcefire FirePOWER设备和NGIPS虚拟设备上的数据包捕获过程
- 减少误报入侵事件的选项
- FireSIGHT系统上的自定义本地Snort规则

入侵检测和防御(IDS/IPS)、Snort引擎

- 确定入侵策略中Sourcefire提供的规则的默认状态
- 用于确定基本策略中的默认规则的度量
- 在防御中心上配置SNORT_BPF变量
- Sourcefire FirePOWER和虚拟设备对链路聚合流量的检测
- 启用内联规范化预处理器并了解Pre-ACK和Post-ACK检测
- 从FirePOWER设备收集核心文件
- 在FireSIGHT系统上配置通过规则
- 从Firepower入侵检测排除EIGRP、OSPF和BGP消息
- Firepower服务处理单流大会话（大象流）

安全情报、地理位置和URL过滤

- FireSIGHT系统上的URL过滤配置示例
- 无法下载或更新安全情报源
- IP地址被FireSIGHT系统的安全情报阻止或列入黑名单
- 排除FireSIGHT系统上的URL过滤问题

应用控制、VDB、网络发现

- FireSIGHT可能错误地识别主机，或者将事件标记为待定或未知

访问控制规则/防火墙

- 连接事件似乎从FireSIGHT管理中心消失

用户界面(GUI/CLI)、用户访问和身份验证

- FireSIGHT系统与ISE的集成，用于RADIUS用户身份验证
- FireSIGHT系统与ACS 5.x的集成，用于RADIUS用户身份验证
- 重置FireSIGHT系统上管理员用户的密码
- 在FireSIGHT系统上验证身份验证对象以通过SSL/TLS进行Microsoft AD身份验证
- 识别身份验证对象配置的Active Directory LDAP对象属性
- 在FireSIGHT系统上配置LDAP身份验证对象
- 使用Ldp.exe验证基于SSL/TLS的LDAP(LDAPS)和CA证书

CPU和内存利用率、网络和系统性能

- FireSIGHT系统上的规则分析说明
- 使用“1秒性能监控器”选项收集性能统计信息
- 当网络遇到延迟问题时从FireSIGHT系统收集数据
- 排除由于MTU较大而丢弃数据包的故障（数据包过大）

系统管理和维护

- 重新启动FireSIGHT系统和FirePOWER服务上的进程，而无需重新启动
- Sourcefire设备文件生成故障排除过程
- 排除FireSIGHT系统上的网络时间协议(NTP)问题
- 对Sourcefire设备上的磁盘过度使用问题进行故障排除
- 在Cisco Firepower 8000系列设备上配置堆栈
- 在Cisco FirePOWER 7000和8000系列设备上配置集群

硬件操作

- 来自FireSIGHT系统电源设备的运行状况警报
- 对FireSIGHT管理中心或FirePOWER设备上的无人值守管理(LOM)问题进行故障排除
- FireSIGHT系统返回“输入/输出错误”消息
- FirePOWER设备在尝试引导至单用户模式后会冻结
- 排除FireSIGHT系统风扇问题
- 从FirePOWER设备的LCD面板执行诊断测试
- 在8000系列FirePOWER设备上插入和移除网络模块(NetMod)
- 确定Sourcefire FirePOWER 7000和8000系列设备中的网络流引擎卡问题
- FirePOWER 8000系列设备滑轨套件的常见问题
- Firepower 7000系列设备滑轨套件安装说明
- FireSIGHT管理中心FS4000型号可能会触发“磁盘降级”运行状况警报
- FireSIGHT管理中心型号FS2000和FS4000的SSD/RAID重新配置过程

SSL解密

- 将Sourcefire SSL设备1500/2000重新映像到3.6或更高版本
- 获取SSL设备的BIOS密码
- SSL设备上的数据包捕获过程
- 在SSL设备上配置SNMP
- 在SSL设备上配置基本规则集
- 在Cisco FireSIGHT系统上配置SSL检查策略

与ISE、Estreamer、SIEM、用户代理、API和连接器集成

- 使用RDP登录远程桌面会更改与IP地址关联的用户
- 排除FireSIGHT系统和eStreamer客户端(SIEM)之间的问题
- 安装和卸载Sourcefire用户代理
- 排除Sourcefire用户代理的连接问题
- 配置FireSIGHT系统以将警报发送到外部系统日志服务器
- 向Sourcefire用户代理使用的Active Directory用户帐户授予最低权限
- 用户代理的实时状态显示为未知
- 为在BlueCoat X系列平台上运行的Sourcefire软件生成故障排除数据
- 通过Firepower和ISE了解基于TrustSec的访问控制
- Cisco Firepower用户代理数据库服务在停止后不重新启动

有关高级恶意软件防护的TAC文档

面向终端的AMP、FireAMP连接器

- 从Windows上运行的FireAMP连接器收集诊断数据
- 从Mac OSX上运行的FireAMP连接器收集诊断数据
- 从Linux上运行的FireAMP连接器收集诊断数据
- 映像或克隆安装了FireAMP连接器的计算机
- 配置和管理FireAMP中的例外项
- 删除Windows上的FireAMP缓存和历史记录文件
- FireAMP连接器安装程序的命令行开关
- 禁用和启用FireAMP连接器客户端服务
- 在后台运行FireAMP连接器客户端服务并隐藏用户界面
- 升级Windows操作系统上的FireAMP连接器
- FireAMP连接器服务因连接器保护而无法停止
- FireAMP连接器扫描的文件类型
- FireAMP Windows排除项指南
- 获取Android设备上有关FireAMP移动连接器问题的故障排除数据
- 在面向终端的FireAMP/AMP上启动计划扫描
- 使用面向终端的AMP或FireAMP执行终端危害表现(IOC)扫描
- 通过AnyConnect 4.x和AMP Enabler安装和配置AMP模块
- 面向具有身份持久性的终端的思科AMP的部署
- 使用高级恶意软件防护(AMP)误报或漏报事件
- 面向终端API的思科AMP概述

面向网络的AMP

- 高级恶意软件防护(AMP)操作所需的服务器
- 排除AMP on FireSIGHT管理中心的连接和注册问题
- 删除FireSIGHT管理中心与FireAMP云控制台之间的连接的流程

云

- 安装和配置FireAMP私有云
- 在FireAMP私有云上生成支持快照文件
- 将文件上传到FireAMP云控制台以查看最新的文件分析

Threat Grid

- 在AMP Threat Grid设备上生成支持快照

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。