목차: FirePOWER Service, FireSIGHT System, AMP에 대한 TAC 문서

목차

FireSIGHT 및 Firepower System에 대한 TAC 문서

소프트웨어 및 보안 업데이트, 리이미지, 마이그레이션 및 설치

- FireSIGHT 시스템에 설치할 수 있는 업데이트 파일 유형
- 4.10.x에서 5.x로 마이그레이션 및 업그레이드한 후 FireSIGHT 시스템의 새로운 용어 이해
- ASA 플랫폼에 FirePOWER Services 모듈 설치 및 설정
- ASA 5585-X 하드웨어 모듈에 FirePOWER(SFR) 서비스 설치
- VMware ESXi에 FireSIGHT Management Center 구축
- Sourcefire Defense Center 및 FirePOWER 어플라이언스 이미지 재설치
- FireSIGHT Management Center에서 자동 다운로드 업데이트 실패
- Firepower Management Center에서 관리되는 디바이스로 데이터를 다운로드하기 위한 지침
- UCS-E 블레이드를 사용하여 ISR 디바이스에서 Firepower Services 구성

라이센스 및 초기 기본 설정

- FireSIGHT 시스템의 기능 라이센스 비교
- FireSIGHT 시스템의 다양한 하드웨어 모델의 지원되는 기능
- FireSIGHT 시스템의 초기 컨피그레이션 단계
- FireSIGHT Management Center에 디바이스 등록
- FireSIGHT 시스템의 가상 라우터 컨피그레이션
- LAN 스위치 없이 VPN 터널을 통해 SFR 모듈 관리
- Firepower 디바이스 및 Firepower Service Module에 대한 라이센스 키 얻기

취약성 및 규칙 커버리지, 이벤트 및 파일 분석

- 웹 사용자 인터페이스를 사용하여 패킷 데이터(PCAP 파일) 다운로드
- Sourcefire FirePOWER 어플라이언스 및 NGIPS 가상 어플라이언스의 패킷 캡처 절차
- 오탐 침입 이벤트를 줄이기 위한 옵션
- FireSIGHT 시스템의 맞춤형 로컬 Snort 규칙

침입 탐지 및 방지(IDS/IPS), Snort 엔진

- 침입 정책에서 Sourcefire 제공 규칙에 대한 기본 상태 결정
- 기본 정책에 대한 기본 규칙을 결정하는 데 사용되는 메트릭
- Defense Center의 SNORT_BPF 변수 컨피그레이션
- Sourcefire FirePOWER 및 가상 어플라이언스의 링크 집계 트래픽 검사
- 인라인 표준화 프리프로세서를 활성화하고 Pre-ACK 및 Post-ACK 검사 이해
- FirePOWER 어플라이언스에서 코어 파일 수집
- FireSIGHT 시스템의 패스 규칙 컨피그레이션
- Firepower 침입 검사에서 EIGRP, OSPF 및 BGP 메시지 제외
- Firepower Services의 단일 스트림 대형 세션(Elephant Flow) 처리

보안 인텔리전스, 지오로케이션 및 URL 필터링

- FireSIGHT 시스템 컨피그레이션의 URL 필터링 예
- 보안 인텔리전스 피드를 다운로드하거나 업데이트할 수 없음
- IP 주소가 FireSIGHT 시스템의 보안 인텔리전스에 의해 차단되거나 블랙리스트에 추가됨
- FireSIGHT 시스템에서 URL 필터링 문제 해결

애플리케이션 제어, VDB, 네트워크 검색

- FireSIGHT에서 호스트를 잘못 식별하거나 이벤트를 Pending 또는 Unknown으로 표시할 수 있습니다.

액세스 제어 규칙/방화벽

- FireSIGHT Management Center에서 연결 이벤트가 사라지는 것 같습니다.

사용자 인터페이스(GUI/CLI), 사용자 액세스 및 인증

- RADIUS 사용자 인증을 위한 ISE와 FireSIGHT System 통합
- RADIUS 사용자 인증을 위해 FireSIGHT System과 ACS 5.x 통합
- FireSIGHT 시스템의 관리자 비밀번호 재설정
- FireSIGHT System에서 SSL/TLS를 통한 Microsoft AD 인증을 위한 인증 객체 확인
- 인증 객체 구성을 위한 Active Directory LDAP 객체 속성 식별
- FireSIGHT 시스템의 LDAP 인증 객체 컨피그레이션
- Ldp.exe를 사용하여 LDAP over SSL/TLS(LDAPS) 및 CA 인증서 확인

CPU 및 메모리 사용률, 네트워크 및 시스템 성능

- FireSIGHT 시스템의 규칙 프로파일링 지침
- "1초 성능 모니터" 옵션을 사용한 성능 통계 수집
- 네트워크에서 지연 문제가 발생할 경우 FireSIGHT 시스템에서 데이터 수집
- 더 높은 MTU(Oversize Packet)로 인한 패킷 삭제 문제 해결

시스템 관리 및 유지 관리

- 재부팅 없이 FireSIGHT 시스템 및 FirePOWER Service에서 프로세스 다시 시작
- Sourcefire 어플라이언스 파일 생성 절차 문제 해결
- FireSIGHT 시스템의 NTP(Network Time Protocol) 문제 해결
- Sourcefire 어플라이언스의 과도한 디스크 사용률 문제 해결
- Cisco Firepower 8000 Series 디바이스의 스택 컨피그레이션
- Cisco FirePOWER 7000 및 8000 Series 디바이스의 클러스터링 구성

하드웨어 운영

- FireSIGHT 시스템 전원 공급 장치의 상태 알림
- FireSIGHT Management Center 또는 FirePOWER Appliance의 LOM(Lights-Out Management) 문제 해결
- FireSIGHT 시스템에서 "Input/Output Error" 메시지 반환
- FirePOWER Appliance는 단일 사용자 모드로 부팅을 시도한 후 정지됩니다
- FireSIGHT 시스템에서 팬 문제 해결
- FirePOWER 어플라이언스의 LCD 패널에서 진단 테스트 수행
- 8000 Series FirePOWER Appliance에서 네트워크 모듈(NetMod) 삽입 및 제거
- Sourcefire FirePOWER 7000 및 8000 Series 어플라이언스의 Network Flow Engine 카드 문제 파악
- FirePOWER 8000 Series 어플라이언스 레일 키트에 대한 일반적인 우려 사항
- Firepower 7000 Series Appliance 레일 키트 설치 지침
- FireSIGHT Management Center FS4000 모델이 "Disk Degraded" 상태 알림을 트리거할 수 있

음
- FireSIGHT Management Center 모델 FS2000 및 FS4000의 SSD/RAID 재구성 절차

SSL 암호 해독

- Sourcefire SSL Appliance 1500/2000을 버전 3.6 이상으로 리이미징합니다.
- SSL 어플라이언스에 대한 BIOS 비밀번호 얻기
- SSL 어플라이언스의 패킷 캡처 절차
- SSL 어플라이언스에서 SNMP 컨피그레이션
- SSL 어플라이언스에서 기본 규칙 세트 구성
- Cisco FireSIGHT 시스템에 대한 SSL 검사 정책 컨피그레이션

ISE, Estreamer, SIEM, 사용자 에이전트, API, 커넥터와 통합

- RDP를 사용하여 원격 데스크톱에 로그인하면 IP 주소와 연결된 사용자가 변경됩니다
- FireSIGHT System과 eStreamer Client(SIEM) 간의 문제 해결
- Sourcefire 사용자 에이전트 설치 및 제거
- Sourcefire User Agent로 연결 문제 해결
- 외부 Syslog 서버에 경고를 전송하도록 FireSIGHT 시스템 구성
- Sourcefire 사용자 에이전트가 사용하는 Active Directory 사용자 계정에 최소 권한 부여
- 사용자 에이전트의 실시간 상태가 알 수 없음으로 표시됩니다
- BlueCoat X-Series 플랫폼에서 실행되는 Sourcefire 소프트웨어의 문제 해결 데이터 생성
- Firepower 및 ISE를 통한 TrustSec 기반 액세스 제어 이해
- Cisco Firepower User Agent 데이터베이스 서비스가 중지 후 다시 시작되지 않음

AMP에 대한 TAC 문서

AMP For Endpoints, FireAMP Connector

- Windows에서 실행되는 FireAMP Connector에서 진단 데이터 수집
- Mac OSX에서 실행 중인 FireAMP Connector에서 진단 데이터 수집
- Linux에서 실행되는 FireAMP Connector에서 진단 데이터 수집
- FireAMP Connector가 설치된 컴퓨터 이미지 또는 복제
- FireAMP에서 제외 구성 및 관리
- Windows에서 FireAMP 캐시 및 기록 파일 제거
- FireAMP Connector Installer용 명령줄 스위치
- FireAMP Connector 클라이언트 서비스 비활성화 및 활성화
- 백그라운드에서 FireAMP Connector 클라이언트 서비스를 실행하고 사용자 인터페이스 숨기기
- Windows 운영 체제에서 FireAMP Connector 업그레이드
- 커넥터 보호 때문에 FireAMP Connector Service를 중지하지 못함
- FireAMP Connector에서 스캔되는 파일 유형
- Windows에서 제외에 대한 FireAMP 가이드
- FireAMP Mobile Connector 문제용 Android 디바이스의 문제 해결 데이터 얻기
- FireAMP/AMP for Endpoints에서 예약된 스캔 시작
- AMP for Endpoints 또는 FireAMP로 엔드포인트 IOC(Indication of Compromise) 스캔 수행
- AnyConnect 4.x 및 AMP Enabler를 통한 AMP 모듈 설치 및 구성
- ID 지속성을 갖춘 Cisco AMP for Endpoints 구축
- AMP(Advanced Malware Protection) 오탐 또는 오탐 이벤트 작업
- Cisco AMP for Endpoint API 개요

AMP for Network

- AMP(Advanced Malware Protection) 운영에 필요한 서버
- AMP on FireSIGHT Management Center로 연결 및 등록 문제 해결
- FireSIGHT Management Center와 FireAMP Cloud Console 간 연결 제거 프로세스

클라우드

- FireAMP Private Cloud 설치 및 구성
- FireAMP Private Cloud에서 지원 스냅샷 파일 생성
- FireAMP Cloud Console에 파일을 업로드하여 최근 파일 분석 보기

Threat Grid

- AMP Threat Grid Appliance에서 지원 스냅샷 생성