

# Índice: Documentos TAC no serviço de FirePOWER, no sistema de FireSIGHT, e no AMP

## Índice

[Documentos TAC em FireSIGHT e no sistema de FirePOWER](#)

[Documentos TAC em proteção avançada do malware](#)

## Documentos TAC em FireSIGHT e no sistema de FirePOWER

Software e atualização da Segurança, nova imagem, migração e instalação

- [Tipos de arquivos da atualização que puderam ser instalados em um sistema de FireSIGHT](#)
- [Compreenda as terminologias novas de sistemas de FireSIGHT após uma migração e promova-as de 4.10.x a 5.x](#)
- [Instale e configure um Módulo de serviços de FirePOWER em uma plataforma ASA](#)
- [A instalação de serviços de FirePOWER \(SFR\) no módulo de hardware ASA 5585-X](#)
- [Desenvolvimento do centro de gerenciamento de FireSIGHT em VMware ESXi](#)
- [Nova imagem um centro da defesa de Sourcefire e um dispositivo de FirePOWER](#)
- [Falha automática da atualização da transferência em um centro de gerenciamento de FireSIGHT](#)
- [Diretrizes para transferir dados do centro de gerenciamento de FirePOWER aos dispositivos gerenciado](#)
- [Configurar serviços de FirePOWER em um dispositivo ISR com uma lâmina UCS-E](#)

Licença e instalação básica inicial

- [Comparação das licenças de recurso em sistemas de FireSIGHT](#)
- [Características suportadas e capacidades de vários modelos de hardware do sistema de FireSIGHT](#)
- [Etapas da configuração inicial de sistemas de FireSIGHT](#)
- [Registrar um dispositivo com um centro de gerenciamento de FireSIGHT](#)
- [Configuração de um roteador virtual em um sistema de FireSIGHT](#)
- [Gerenciamento do módulo SFR sobre o túnel VPN sem switch LAN](#)
- [Obtenha a chave de licença para um dispositivo de FirePOWER e um módulo de serviço de FirePOWER](#)

Vulnerabilidade e de cobertura, de evento e de arquivo da regra análise

- [Dados do pacote da transferência \(arquivo PCAP\) que usam a relação de usuário de web](#)
- [Procedimentos da captura de pacote de informação em dispositivos de Sourcefire FirePOWER e em dispositivos virtuais NGIPS](#)
- [Opções para reduzir eventos da intrusão do falso positivo](#)
- [Regras locais do Snort do costume em um sistema de FireSIGHT](#)

Intrusion detection e prevenção (IDS/IPS), motor do Snort

- [A determinação do estado padrão para um Sourcefire forneceu a regra em uma política da](#)

## intrusão

- Medidor usado para determinar as regras de padrão em uma política baixa
- Configuração da variável SNORT BPF em um centro da defesa
- A inspeção do link agregou o tráfego por Sourcefire FirePOWER e dispositivos virtuais
- Permita o Preprocessor Inline da normalização e compreenda a inspeção PRE-ACK e Cargo-ACK
- Coleção dos arquivos principais de um dispositivo de FirePOWER
- Configuração de uma regra da passagem em um sistema de FireSIGHT
- Exclusão do EIGRP, do OSPF e dos mensagens BGP da inspeção da intrusão de FirePOWER
- Processamento da grande sessão do único córrego (fluxo do elefante) pelos serviços de FirePOWER

### Inteligência de Segurança, Geolocation e Filtragem URL

- Filtragem URL em um exemplo da configuração de sistema de FireSIGHT
- Incapaz de transferir ou atualizar a alimentação da inteligência de Segurança
- O endereço IP de Um ou Mais Servidores Cisco ICM NT é obstruído ou pãr pela Segurança Intellegence de um sistema de FireSIGHT
- Pesquise defeitos edições com Filtragem URL em um sistema de FireSIGHT

### Controle de aplicativo, VDB, descoberta da rede

- FireSIGHT pode identificar um host incorretamente, ou marque um evento como durante ou o desconhecido

### Regra/Firewall do controle de acesso

- Os eventos de conexão parecem desaparecer do centro de gerenciamento de FireSIGHT

### Interface do utilizador (GUI/CLI), acesso de usuário e autenticação

- Integração do sistema de FireSIGHT com o ISE para a autenticação de usuário RADIUS
- Integração do sistema de FireSIGHT com ACS 5.x para a autenticação de usuário RADIUS
- Restaure a senha do usuário admin em sistemas de FireSIGHT
- Objeto da verificação de autenticação no sistema de FireSIGHT para a autenticação de Microsoft AD sobre o SSL/TLS
- Identifique atributos de objeto do diretório ativo LDAP para a configuração do objeto da autenticação
- Configuração do objeto da autenticação LDAP no sistema de FireSIGHT
- Verifique o LDAP sobre SSL/TLS (LDAP) e o certificado de CA usando Ldp.exe

### CPU e utilização de memória, rede e desempenho de sistema

- Regra que perfila instruções no sistema de FireSIGHT
- Coleção das estatísticas de desempenho usando opção do monitoramento de desempenho "1-Second"
- Levantamento de dados de um sistema de FireSIGHT quando uma rede experimentar edições da latência
- Pesquise defeitos deixar cair de pacotes devido a um MTU mais alto (o pacote de tamanho grande)

### A administração do sistema e manutenção

- Reinicie os processos em um sistema de FireSIGHT e em um serviço de FirePOWER sem uma repartição

- [O dispositivo de Sourcefire pesquisa defeitos procedimentos de geração do arquivo](#)
- [Pesquise defeitos edições com o Network Time Protocol \(NTP\) em sistemas de FireSIGHT](#)
- [Pesquise defeitos a utilização excessiva do disco em dispositivos de Sourcefire](#)
- [Configuração da pilha nos dispositivos do 8000 Series de Cisco FirePOWER](#)
- [Configuração da aglomeração em dispositivos do 7000 e 8000 Series de Cisco FirePOWER](#)

#### Operação de hardware

- [Alertas da saúde da unidade de fonte de alimentação de sistema de FireSIGHT](#)
- [Pesquise defeitos uma edição com Gerenciamento das luzes-Para fora \(LOM\) em um centro de gerenciamento de FireSIGHT ou em um dispositivo de FirePOWER](#)
- [Mensagem do erro entrada/saída” dos retornos do sistema do “de FireSIGHT](#)
- [Um dispositivo de FirePOWER torna-se congelado após a tentativa carreg a no modo do usuário único](#)
- [Pesquise defeitos edições com fãs em um sistema de FireSIGHT](#)
- [Execute testes diagnósticos do painel LCD de um dispositivo de FirePOWER](#)
- [Introduza e remova um módulo de rede \(NetMod\) em um dispositivo de FirePOWER do 8000 Series](#)
- [Identifique edições com as placas de Engine do fluxo de rede em dispositivos do 7000 e 8000 Series de Sourcefire FirePOWER](#)
- [Os interesses da terra comum sobre o dispositivo do 8000 Series de FirePOWER cercam o jogo](#)
- [Instrução de instalação do jogo do trilho do dispositivo do 7000 Series de FirePOWER](#)
- [Um modelo do centro de gerenciamento FS4000 de FireSIGHT pode provocar o alerta degradado “disco” da saúde](#)
- [Os procedimentos de reconfiguração SSD/RAID para o centro de gerenciamento de FireSIGHT modelam FS2000 e FS4000](#)

#### Descriptografia de SSL

- [Nova imagem um dispositivo 1500/2000 de Sourcefire SSL à versão 3.6 ou mais recente](#)
- [Obtenha uma senha BIOS para um dispositivo SSL](#)
- [Procedimentos da captura de pacote de informação em um dispositivo SSL](#)
- [Configuração do SNMP em um dispositivo SSL](#)
- [Configuração de Ruleset básico em um dispositivo SSL](#)
- [Configuração de uma política da inspeção SSL no sistema de Cisco FireSIGHT](#)

#### Integração com ISE, Estreamer, SIEM, agente de usuário, API, e conector

- [O início de uma sessão a um desktop remoto que usa o RDP muda o usuário associado a um endereço IP de Um ou Mais Servidores Cisco ICM NT](#)
- [Pesquise defeitos edições entre o sistema de FireSIGHT e o cliente do eStreamer \(SIEM\)](#)
- [A instalação e desinstalação do agente de usuário de Sourcefire](#)
- [Pesquise defeitos problemas de conectividade com agente de usuário de Sourcefire](#)
- [Configurar um sistema de FireSIGHT para enviar alertas a um servidor syslog externo](#)
- [Permissão mínima de Grant a uma conta de usuário do diretório ativo usada pelo agente de usuário de Sourcefire](#)
- [O estado do tempo real do agente de usuário é mostrado como o desconhecido](#)
- [Gerencia pesquisam defeitos dados para o software de Sourcefire que é executado na plataforma das X-séries de BlueCoat](#)
- [Compreendendo o controle de acesso TrustSec-baseado com FirePOWER e o ISE](#)
- [O serviço de base de dados do agente de usuário de Cisco FirePOWER não reinicia após](#)

[uma parada](#)

## Documentos TAC em proteção avançada do malware

### AMP para valores-limite, conector de FireAMP

- [Coleção de dados de diagnóstico de um conector de FireAMP que é executado em Windows](#)
- [Coleção de dados de diagnóstico de um conector de FireAMP que é executado no Mac OSX](#)
- [Coleção de dados de diagnóstico de um conector de FireAMP que é executado em Linux](#)
- [A imagem ou clona um computador com o conector de FireAMP instalado](#)
- [Configurar e controle exclusões em FireAMP](#)
- [Remoção do esconderijo e dos arquivos históricos de FireAMP em Windows](#)
- [Switches da linha de comando para o instalador do conector de FireAMP](#)
- [Desabilite e permita o serviço do cliente de conector de FireAMP](#)
- [Execute o serviço do cliente de conector de FireAMP no fundo e esconda a interface do utilizador](#)
- [Promova um conector de FireAMP em sistemas operacionais de Windows](#)
- [O serviço do conector de FireAMP não para devido à proteção do conector](#)
- [Tipos de arquivo que são feitos a varredura pelo conector de FireAMP](#)
- [Guia de FireAMP às exclusões em Windows](#)
- [Obtenha pesquisam defeitos dados em um dispositivo de Android para edições móveis do conector de FireAMP](#)
- [Inicie varreduras programadas em FireAMP/AMP para valores-limite](#)
- [Execute a indicação do valor-limite de varreduras do acordo \(IOC\) com o AMP para valores-limite ou FireAMP](#)
- [A instalação e configuração do módulo AMP com AnyConnect 4.x e AMP Habilitador](#)
- [Desenvolvimento de Cisco AMP para valores-limite com persistência da identidade](#)
- [Trabalho com os eventos avançados do falso positivo ou do falso negativo da proteção do malware \(AMP\)](#)
- [Vista geral de Cisco AMP para o valor-limite API](#)

### AMP para a rede

- [Servidores obrigatórios para operações avançadas da proteção do malware \(AMP\)](#)
- [Pesquise defeitos edições da Conectividade e do registro com o AMP no centro de gerenciamento de FireSIGHT](#)
- [Processo para remover as conexões entre um centro de gerenciamento de FireSIGHT e um console da nuvem de FireAMP](#)

### Nuvem

- [A instalação e configuração da nuvem privada de FireAMP](#)
- [Gerencia um arquivo de instantâneo do apoio em uma nuvem privada de FireAMP](#)
- [Transfira arquivos pela rede um arquivo ao console da nuvem de FireAMP para ver a análise do arquivo recente](#)

### Grade da ameaça

- [Gerencia um instantâneo do apoio em um dispositivo da grade da ameaça AMP](#)