

# 可能安装在FireSIGHT系统上的更新文件类型

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[更新类型](#)

[Web界面上的更新页面](#)

[产品更新](#)

[规则更新](#)

[GeoDB更新](#)

[安全情报更新](#)

[URL过滤更新](#)

## 简介

本文档概述了FireSIGHT系统为保持系统最新而安装的各种更新文件类型。某些文件会更新FireSIGHT系统的软件和操作系统，而某些文件会增强安全性。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于下列硬件和软件版本：

- Sourcefire FirePOWER 7000系列设备、8000系列设备和NGIPS虚拟设备
- Sourcefire软件5.0版或更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 更新类型

在FireSIGHT系统上，可以安装以下类型的更新：

	描述	示例
升级	<ul style="list-style-type: none"><li>• 介绍新功能和组件。</li><li>• 包括漏洞修复。</li></ul>	Sourcefire_3D_De 763.sh
补丁程序	<ul style="list-style-type: none"><li>• 解决已知问题。</li><li>• 包括之前修补程序中提供的分辨率。</li></ul>	Sourcefire_3D_De 59.sh
Sourcefire规则更新(SRU)	<ul style="list-style-type: none"><li>• 可安装在软件版本5.0或更高版本上。</li><li>• 更新Snort规则和共享对象规则。</li></ul>	Sourcefire_Rule_
漏洞数据库(VDB)	<ul style="list-style-type: none"><li>• 更新应用和操作系统的指纹、检测器和漏洞信息。</li></ul>	Sourcefire_VDB_E 241.sh
SourceFire GeoLocation数据库更新(GeoDB)	<ul style="list-style-type: none"><li>• 更新与可路由IP地址关联的地理数据。</li></ul>	Sourcefire_Geodb
安全情报源 URL过滤数据	<ul style="list-style-type: none"><li>• 更新用于将IP地址列入黑名单的IP地址列表。</li><li>• 更新用于访问控制规则中URL过滤的数据。</li></ul>	源由FireSIGHT管理中 源由FireSIGHT管理中

## Web界面上的更新页面

要更新FireSIGHT管理中心，您可能必须导航至Web界面的各个页面。它取决于要下载的更新类型。本部分提供到各种更新页面的导航。

### 产品更新

要上载或安装这些组件，请选择“系统”>“更新”，然后选择“产品更新”选项卡：

- 升级
- 补丁程序
- VDB

如果要直接从思科支持站点下载升级、补丁或VDB文件，请单击“下载更新”。该按钮位于页面底部。或者，如果您从思科支持站点手[动下载文件](#)，并且要将其上传到FireSIGHT系统，请点击[上传更新](#)。



### 规则更新

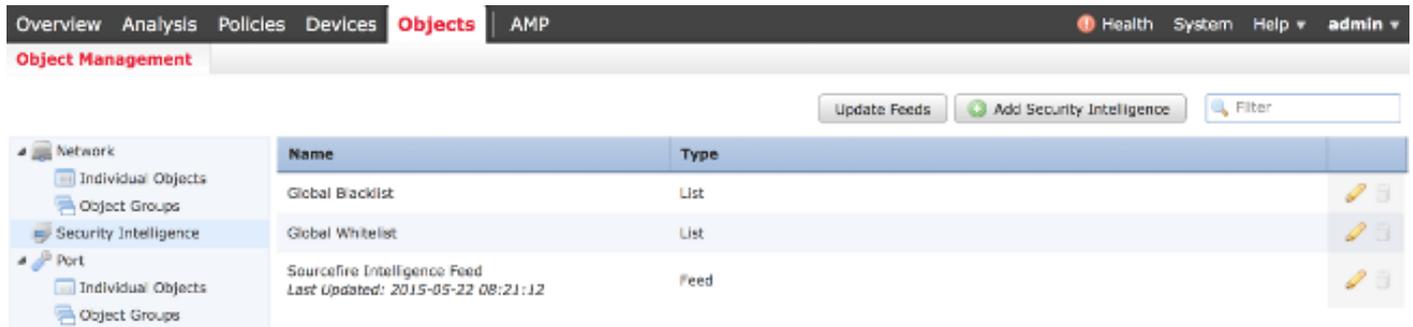
要更新SRU，请选择System > Updates，然后选择Rule Updates选项卡。

### GeoDB更新

要更新GeoDB，请选择System > Updates，然后选择Geolocation Updates选项卡。

## 安全情报更新

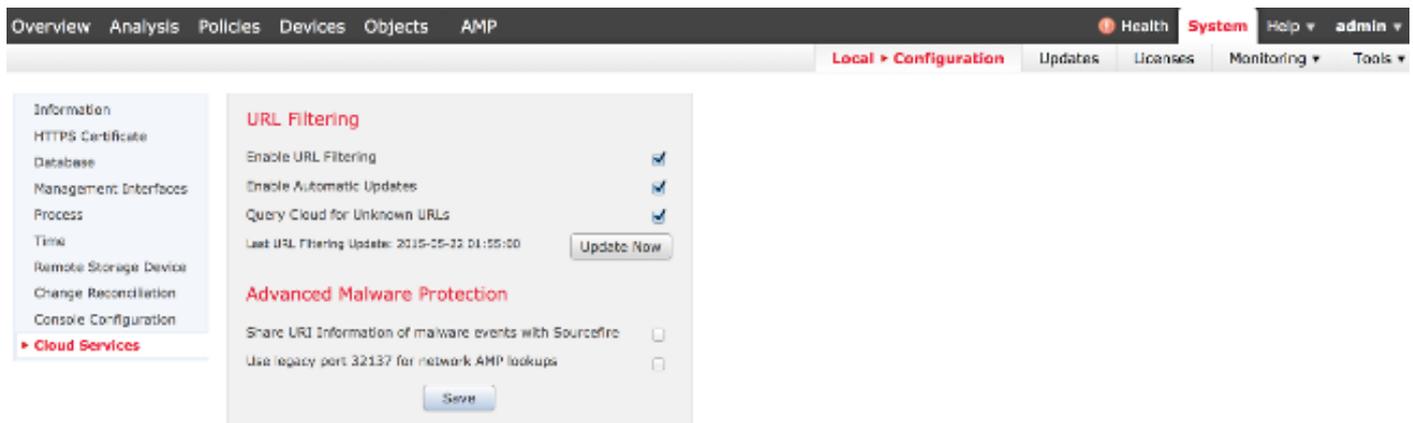
要更新安全情报源，请选择“对象”>“对象管理”。从左侧面板选择“安全情报”选项，然后单击“更新源”。如果要更新自定义源或创建自定义列表，请单击“添加安全情报”。



Name	Type	
Global Blacklist	List	 
Global Whitelist	List	 
Sourcefire Intelligence Feed Last Updated: 2015-05-22 08:21:12	Feed	 

## URL过滤更新

要更新URL过滤数据库，请选择System > Local > Configuration。选择Cloud Services(云服务)，然后单击Update Now。



**URL Filtering**

- Enable URL Filtering
- Enable Automatic Updates
- Query Cloud for Unknown URLs

Last URL Filtering Update: 2015-05-22 01:05:00 [Update Now](#)

**Advanced Malware Protection**

- Share URI Information of malware events with Sourcefire
- Use legacy port 32137 for network AMP lookups

[Save](#)