

在FirePOWER模块中配置基于域的安全情报 (DNS策略) 和ASDM (机上管理)

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[域列表和源概述](#)

[Cisco TALOS提供的域列表和源](#)

[自定义域列表和源](#)

[配置DNS安全情报](#)

[步骤1.配置自定义DNS源/列表 \(可选 \)。](#)

[手动将IP地址添加到全局黑名单和全局白名单](#)

[创建黑名单域的自定义列表](#)

[步骤2.配置Sinkhole对象 \(可选 \)。](#)

[步骤3.配置DNS策略。](#)

[步骤4.配置访问控制策略。](#)

[步骤5.部署访问控制策略。](#)

[验证](#)

[DNS安全情报事件监控](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何使用自适应安全设备管理器(ASDM)在带FirePOWER模块的ASA上配置基于域的安全情报(SI)。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA (自适应安全设备) 防火墙知识
- ASDM (自适应安全设备管理器)
- FirePOWER模块知识

注意：安全情报过滤器需要保护许可证。

使用的组件

本文档中的信息基于以下软件版本：

- ASA FirePOWER模块(ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)，软件版本为6.0.0及更高
- ASA FirePOWER模块(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X)，软件版本为6.0.0及更高版本

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。

背景信息

Firepower系统能够拦截DNS流量请求并查找恶意域名。如果Firepower模块发现恶意域，Firepower会根据DNS策略的配置采取适当措施来缓解请求。

新的攻击方法旨在破坏基于IP的情报，滥用DNS负载均衡功能，以隐藏恶意服务器的实际IP地址。虽然与攻击相关的IP地址经常交换进出，但域名很少更改。

Firepower能够将恶意请求重定向到Sinkhole服务器，该服务器可以是蜜罐服务器，以检测、转移或研究尝试，以更深入地了解攻击流量。

域列表和源概述

域列表和源包含恶意域名列表，根据攻击类型进一步分类为不同类别。通常，您可以将源分为两种类型。

Cisco TALOS提供的域列表和源

DNS攻击者：不断扫描漏洞或尝试利用其他系统的域名的集合。

DNS Bogon:不分配但重新发送流量的域名集合，也称为假IP。

DNS Bot:作为僵尸网络的一部分主动参与并由已知僵尸网络控制器控制的域名集合。

DNS CnC:被标识为已知僵尸网络的控制服务器的域名的集合。

DNS漏洞攻击包：尝试利用其他系统的域名的集合。

DNS恶意软件：尝试传播恶意软件或主动攻击任何访问它们的人的域名的集合。

DNS Open_proxy : 运行开放Web代理并提供匿名Web浏览服务的域名集合。

DNS Open_relay : 提供垃圾邮件和网络钓鱼攻击者使用的匿名邮件中继服务的域名集合。

DNS网络钓鱼 : 主动试图欺骗最终用户输入其机密信息 (如用户名和密码) 的域名集合。

DNS响应 : 重复观察到参与可疑或恶意行为的域名的集合。

DNS垃圾邮件 : 被标识为发送垃圾邮件源的域名的集合。

DNS可疑 : 显示可疑活动且正在进行活动调查的域名的集合。

DNS Tor_exit_node : 为Tor匿名器网络提供退出节点服务的域名集合。

自定义域列表和源

DNS全局黑名单 : 管理员识别为恶意的自定义域名列表的集合。

DNS全局白名单 : 管理员识别为正版的自定义域名列表的集合。

配置DNS安全情报

配置基于域名的安全情报有多个步骤。

1. 配置自定义DNS源/列表 (可选)
2. 配置Sinkhole对象 (可选)
3. 配置DNS策略
4. 配置访问控制策略
5. 部署访问控制策略

步骤1.配置自定义DNS源/列表 (可选)。

有两个预定义的列表允许您向其添加域。为要阻止的域创建您自己的列表和源。

- DNS全局黑名单
- DNS全局白名单

手动将IP地址添加到全局黑名单和全局白名单

Firepower模块允许您在知道某些域是某些恶意活动的一部分时将其添加到全局黑名单。如果您希望允许流量到某些被黑名单域阻止的域，也可以将域添加到全局白名单。如果将任何域添加到全局黑名单/全局白名单，则该域将立即生效，无需应用策略。

要将IP地址添加到全局黑名单/全局白名单，请导航到**Monitoring > ASA FirePOWER Monitoring > Real Time Eventing**，将鼠标悬停在连接事件上并选择**View Details**。

您可以将域添加到全局黑名单/全局白名单。单击**Edit on DNS** (在DNS上编辑) 部分，然后选择**Whitelist DNS Requests to Domain Now/Blacklist DNS Requests to Domain Now** (立即将DNS请求列入黑名单)，将域添加到相应的列表，如图所示。

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

Connection Event ---- Allow Time: Fri 15/7/16 9:48:39 AM (IST) (start of the flow) [Close](#)

ASA FirePOWER firewall connection event

Reason:

Event Details

Initiator		Responder		Traffic	
Initiator IP	192.168.20.50	Responder IP	10.76.77.50	Ingress Security Zone	inside
Initiator Country and Continent	not available	Responder Country and Continent	not available	Egress Security Zone	outside
Source Port/ICMP Type	57317	Destination Port/ICMP Code	53	Ingress Interface	inside
User	Special Identities/No Authentication Required	URL	not available	Egress Interface	outside
Transaction		URL Category	not available	TCP Flags	0
Initiator Packets	1.0	URL Reputation	Risk unknown	NetBIOS Domain	not available
Responder Packets	0.0	HTTP Response	0	DNS	
Total Packets	1.0	Application		DNS Query	malicious.com
Initiator Bytes	73.0	Application	not available	Sinkhole	Whitelist DNS Requests to Domain Now Blacklist DNS Requests to Domain Now
Responder Bytes	0.0	Application Categories	not available	View more	
Connection Bytes	73.0	Application Tag	not available	SSL	
Policy		Client Application	DNS	SSL Status	Unknown (Unknown)
Policy	Default Allow All Traffic	Client Version	not available	SSL Policy	not available
Firewall Policy Rule/SI Category	intrusion_detection	Client Categories	network protocols/services	SSL Rule	not available
Monitor Rules	not available	Client Tag	opens port	SSL Version	Unknown
ISE Attributes		Web Application	not available	SSL Cipher Suite	TLS_NULL_WITH_NULL_NULL
End Point Profile Name	not available	Web App Categories	not available	SSL Certificate Status	Not Checked
Security Group Tag Name	not available	Web App Tag	not available	View more	
Location IP	::	Application Risk	not available		
		Application Business Relevance	not available		

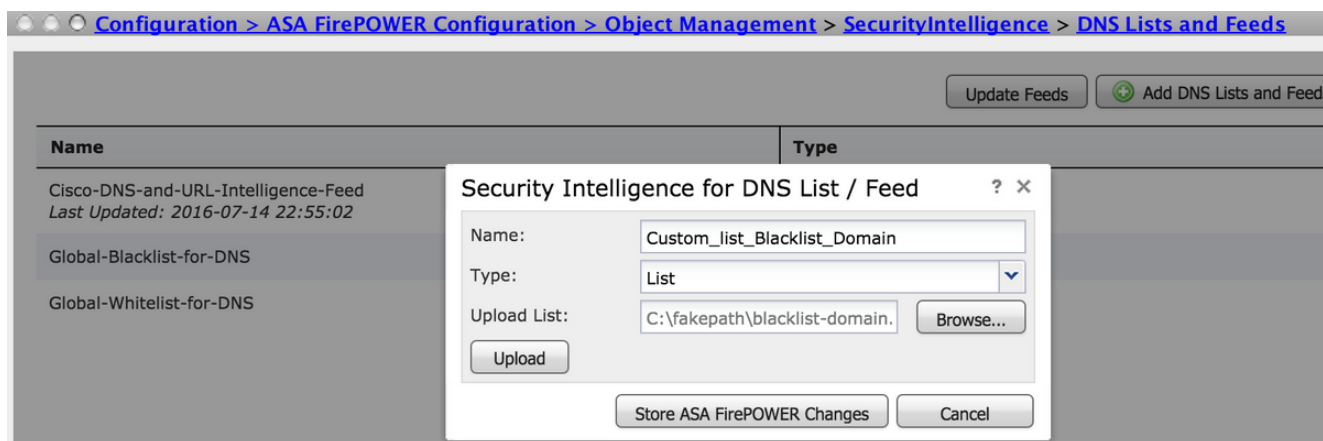
要验证域是否已添加到全局黑名单/全局白名单，请导航至Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > DNS Lists and Feeds，并编辑 Global-Blacklist for DNS / Global Whitelist for DNS。您还可以使用删除按钮从列表中删除任何域。

创建黑名单域的自定义列表

Firepower允许您创建自定义域列表，该列表可通过两种不同的方法用于黑名单（阻止）。

1. 您可以将域名写入文本文件（每行一个域），并将文件上传到FirePOWER模块。

要上传文件，请导航至Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > DNS Lists and Feeds，然后选择Add DNS Lists and Feeds（添加DNS列表和源）
名称：指定自定义列表的名称。
type：从下拉列表中选择“列表”。
上传列表：选择Browse以在系统中查找文本文件。选择Upload以上载文件。



单击Store ASA FirePOWER Changes(存储ASA FirePOWER更改)以保存更改。

2. 您可以将任何第三方域用于Firepower模块可以连接第三方服务器以获取域列表的自定义列表。

要进行此配置，请导航至Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > DNS Lists and Feeds，然后选择Add DNS Lists and Feeds

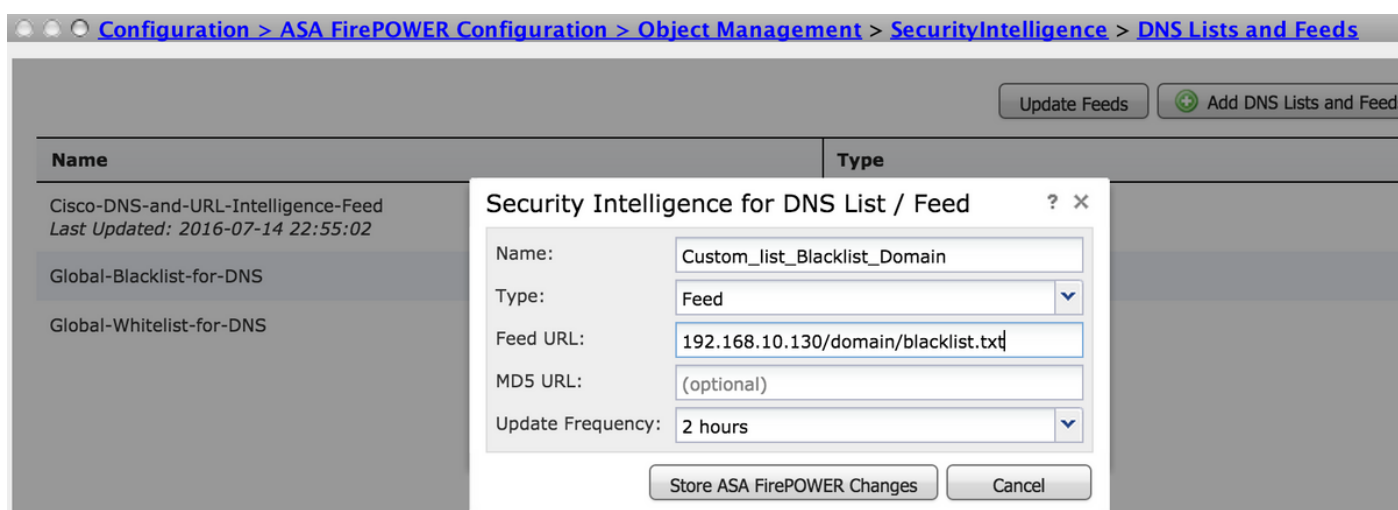
名称：指定自定义源的名称。

type：从下拉列表中选择Feed。

源URL:指定FirePOWER模块可以连接和下载源的服务器URL。

MD5 URL:指定哈希值以验证源URL路径。

更新频率：指定模块连接到URL源服务器的时间间隔。



选择Store ASA FirePOWER Changes以保存更改。

步骤2.配置Sinkhole对象（可选）。

Sinkhole IP地址可用作对恶意DNS请求的响应。客户端计算机获取用于恶意域名查找的Sinkhole服务器IP地址，并且，n终端计算机尝试连接到Sinkhole服务器。因此，Sinkhole可以充当蜜罐来调查攻击流量。Sinkhole可配置为触发危害指示器(IOC)。

要添加Sinkhole服务器，请依次选择Configuration > ASA FirePOWER Configuration > Object Management > Sinkhole，然后单击Add Sinkhole选项。

名称：指定Sinkhole服务器的名称。

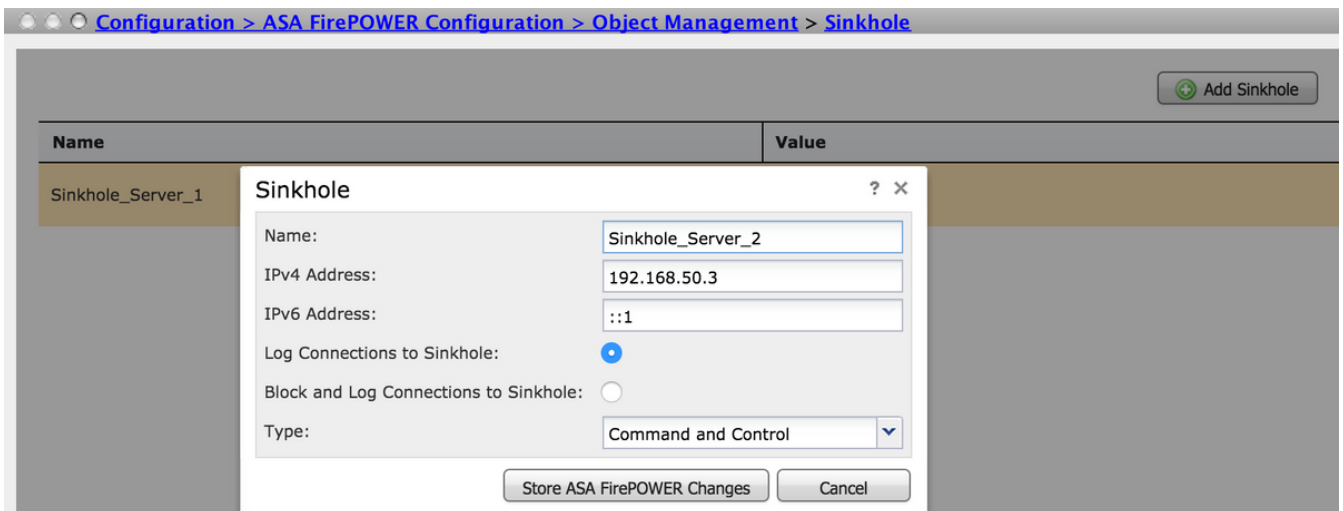
IP 地址：指定Sinkhole服务器的IP地址。

记录与Sinkhole的连接：启用此选项可记录终端和Sinkhole服务器之间的所有连接。

阻止和记录与Sinkhole的连接：启用此选项可阻止连接，并仅在流连接开始时记录。如果没有物理Sinkhole服务器，可以指定任何IP地址，并且可以看到连接事件和IOC触发器。

type：从下拉列表中选择要为其选择与Sinkhole事件关联的IOC（危害表现）类型的Feed。有三种类型的Sinkhole IOC可以标记。

- 恶意软件
- 命令和控制
- 网络钓鱼



步骤3.配置DNS策略。

需要配置DNS策略，以决定DNS源/列表的操作。导航至Configuration > ASA FirePOWER Configuration > Policies > DNS Policy。

默认DNS策略包含两个默认规则。第一条规则Global Whitelist for DNS包含允许的域的自定义列表(Global-Whitelist-for-DNS)。在系统尝试匹配任何黑名单域之前，此规则位于顶部以首先匹配。第二条规则Global Blacklist for DNS包含阻止域的自定义列表(Global-Blacklist-for-DNS)。

您可以添加更多规则，以定义Cisco TALOS提供的域列表和源的各种操作。要添加新规则，请选择Add DNS Rule。

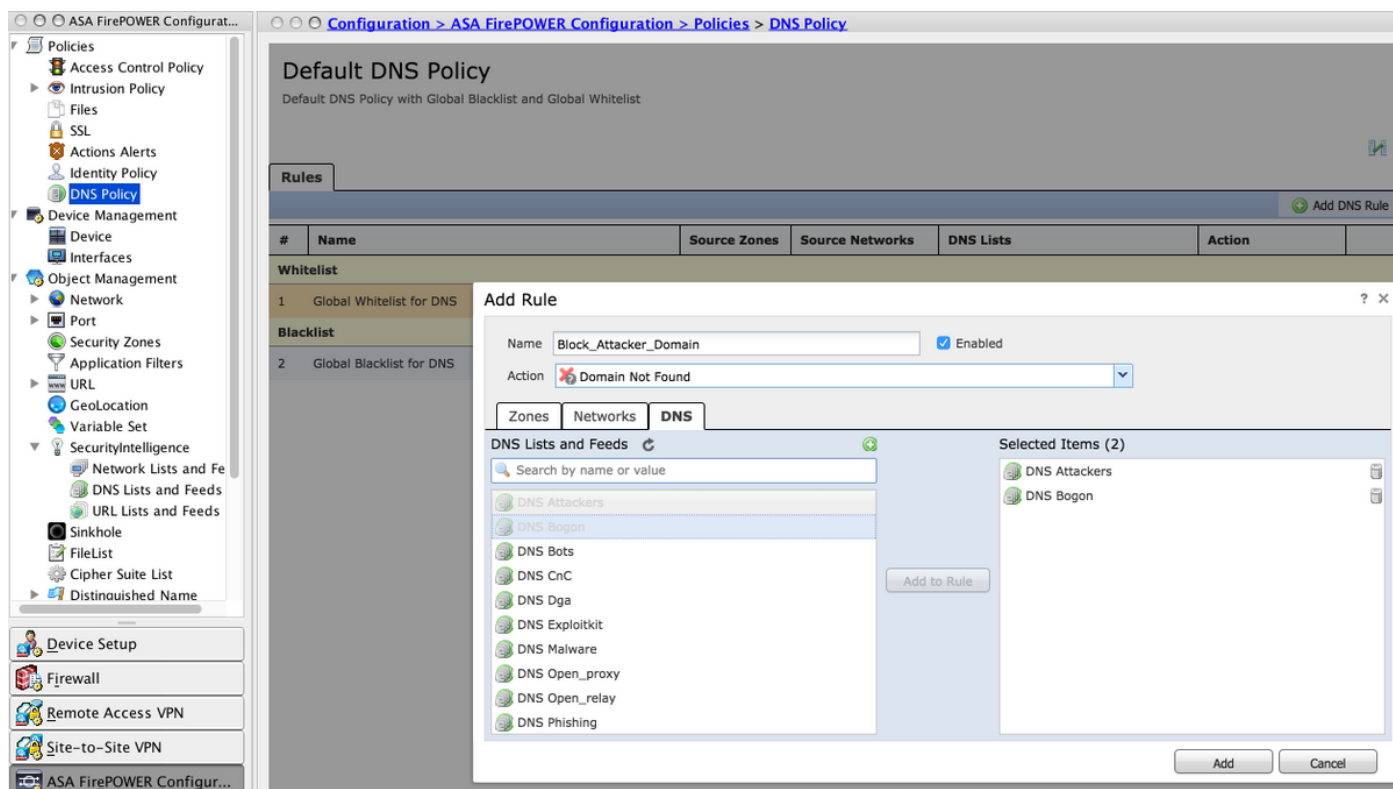
名称：指定规则名称。

操作：指定此规则匹配时要触发的操作。

- **白名单**：这允许DNS查询。
- **监控**:此操作会为DNS查询生成事件，并且流量继续匹配后续规则。
- **找不到域**：此操作将DNS响应作为未找到域（不存在域）发送。
- **丢弃**：此操作会以静默方式阻止和丢弃DNS查询。
- **Sinkhole**:此操作将Sinkhole服务器的IP地址作为对DNS请求的响应发送。

指定Zones/ Network以定义规则条件。在DNS选项卡中，选择DNS列表和源，然后移至Selected Items选项，您可以在其中应用配置的操作。

您可以根据组织需求，使用不同的操作为不同的DNS列表和源配置多个DNS规则。

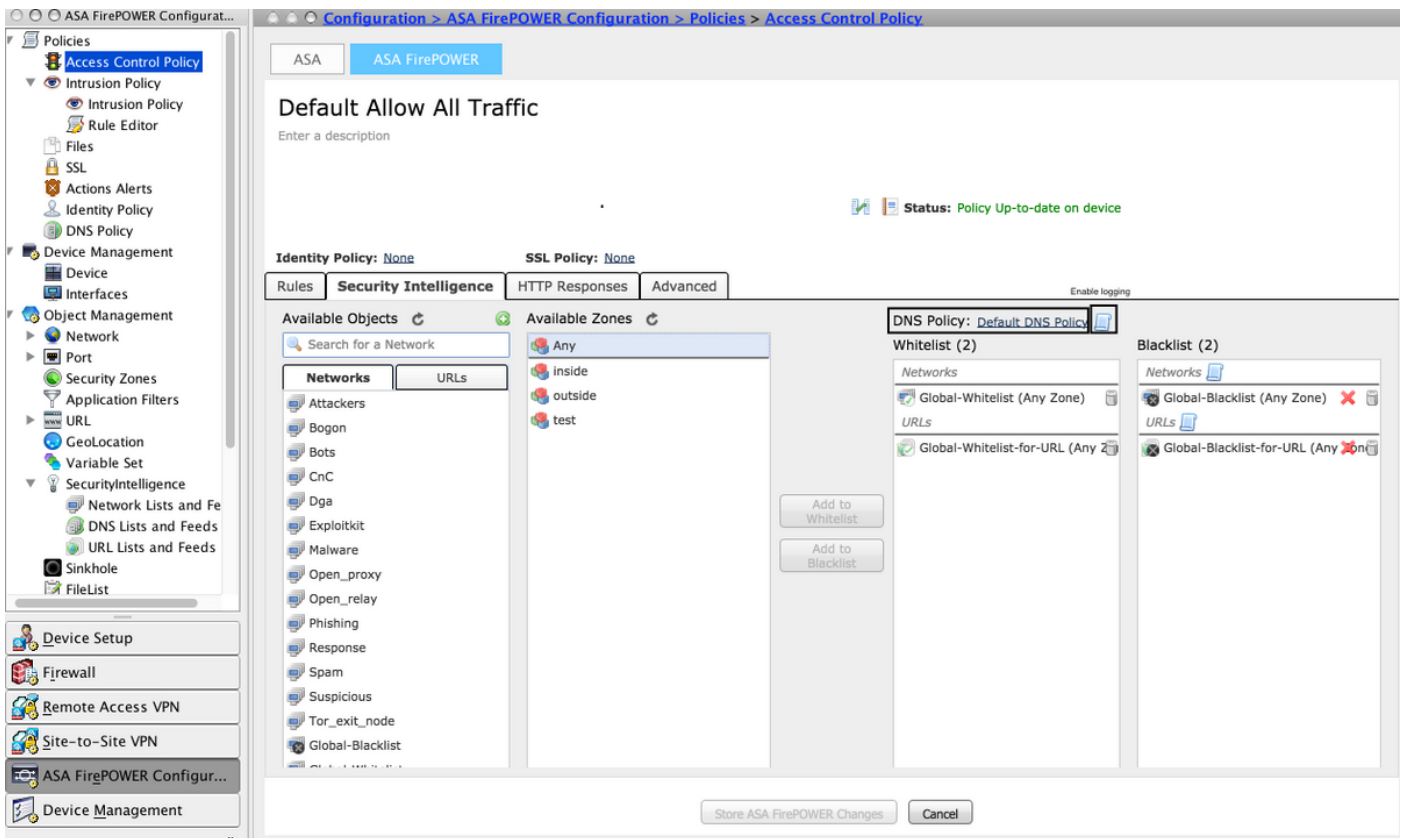


单击“添加”选项以添加规则。

步骤4.配置访问控制策略。

要配置基于DNS的安全情报，请导航至Configuration > ASA Firepower Configuration > Policies > Access Control Policy，选择Security Intelligence选项卡。

确保已配置DNS策略，或者，您可以在点击日志图标时启用日志，如图所示。



选择“Store ASA Firepower Changes”(存储ASA Firepower更改)选项以保存AC策略更改。

步骤5.部署访问控制策略。

要使更改生效，必须部署访问控制策略。在应用策略之前，请参阅指示设备上的访问控制策略是否已过期。

要将更改部署到传感器，请单击Deploy，然后选择Deploy FirePOWER Changes，然后在弹出窗口中选择Deploy以部署更改。

注意：在版本5.4.x中，要将访问策略应用于传感器，您需要单击“应用ASA FirePOWER更改”(Apply ASA FirePOWER Changes)。

注意：导航至监控> ASA Firepower监控>任务状态。确保任务已完成以确认配置更改。**验证**仅当触发事件时，才能验证配置。为此，您可以强制在计算机上执行DNS查询。但是，当已知恶意服务器被攻击时，请谨慎注意其影响。生成此查询后，可以在“实时事件”部分中看到该事件。**DNS安全情报事件监控**要通过Firepower模块查看安全情报，请导航至Monitoring > ASA Firepower Monitoring > Real Time Eventing。选择Security Intelligence选项卡。这将显示如图所示的事件

:

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

All ASA FirePOWER Events | Connection | Intrusion | File | Malware File | Security Intelligence

Filter: protocol=udp

Filter







Pause Refresh Rate: 5 seconds 15/7/16 12:20:21 PM (IST)

Receive Times	Action	First Packet	Last Packet	Reason	Initiator IP	Responder IP	Source Port
15/7/16 12:20:04 PM	Domain Not Found	15/7/16 12:20:03 PM		DNS Block	192.168.20.50	10.76.77.50	65296
15/7/16 12:20:04 PM	Domain Not Found	15/7/16 12:20:03 PM		DNS Block	192.168.20.50	10.76.77.50	65295

故障排除 本节提供可用于排除配置故障的信息。为确保安全情报源是最新的，请导航至 Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > DNS Lists and Feeds，并检查上次更新源的时间。可以选择“编辑”以设置源更新的频率。

Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > DNS Lists and Feeds

Update Feeds Add DNS Lists and Feeds Filter

Name	Type	
Cisco-DNS-and-URL-Intelligence-Feed <i>Last Updated: 2016-07-15 00:55:03</i>	Feed	 
Global-Blacklist-for-DNS	List	 
Global-Whitelist-for-DNS	List	 

确保访问控制策略部署已成功完成。 监控安全情报实时事件选项卡以查看流量是否被阻止。 **相关信息**

- [Cisco ASA FirePOWER模块快速入门指南](#)
- [技术支持和文档 - Cisco Systems](#)