思科网络威胁防御解决方案 1.1 设计和实施指南

上次更新日期：2013 年 7 月 28 日

Cisco Validated Design

作者简介

Matt Robertson

Matt 是思科系统公司安全技术组的一名技术营销工程师，经常与思科的全球最大客户打交道。Matt 致力于开发高级威胁检测和防御解决方案，并且拥有滑铁卢大学计算机工程专业的学士和硕士学位。

Brian MacMahon

Brian McMahon 在过去 25 年中主要忙于担任各种计算机和网络安全角色，包括各类大型和小型机构的培训、测试和技术支持。目前，他是思科系统公司的一名技术营销工程师，从事基于网络行为的威胁检测系统工作。

目 录

思科网络威胁防御解决方案 1.1

简介

威胁格局已经发生演变；政府组织和大型企业充斥着称为高级持续威胁 (APT) 的有针对性的自定义攻击。这些 APT 往往由动机明确且资金充足的攻击者发起，他们能够绕开组织的外围防御来获取网络访问权。为应对这些威胁，许多政府组织和大型企业都开始借助各种工具来帮助识别和研究对其网络造成威胁的攻击。

思科网络威胁防御解决方案 1.1 能够主动检测已在内部网络中运行的威胁。该解决方案使用来自网络设备的遥测数据，在整个网络内部提供无处不在的深入可视性，使安全操作人员能够了解网络流量的相关“人员、内容、时间、位置、原因和方式”，进而发现异常。通过此方法，操作员可以更多地了解接入层和分布层（传统网络安全平台通常不会覆盖到这些层）中可疑活动的性质。思科网络威胁防御解决方案 1.1 所提供的可视性和情景级别可大幅减小漏洞检测所花费的时间，并将控制权交回到安全操作人员手中。

在整个网络中部署思科网络威胁防御解决方案 1.1 可以为安全操作人员提供所需的信息和可视性，支持他们开展各种安全任务，包括（但不限于）：

- 检测数据丢失事件的发生
- 检测内部网络上的网络侦查活动
- 检测和监控整个内部网络中恶意软件的传播
- 检测内部网络上的僵尸网络命令和控制信道

思科网络威胁防御解决方案 1.1 采用了 NetFlow 和基于网络的应用识别 (NBAR) 等思科网络技术，以及思科身份服务引擎 (ISE) 所提供的身份服务、设备分析服务、安全评估服务和用户策略服务。

思科网络威胁防御解决方案 1.1 由思科与 Lancope® 合作开发并提供。Lancope StealthWatch® System（可从思科购买）是现今市场上领先的基于流的安全监控解决方案，在思科网络威胁防御解决方案 1.1 中用作 NetFlow 分析器和管理系统。

本指南介绍有关思科网络威胁防御的设计、部署和实施的详细信息。解决方案 1.1。

公司总部：
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

产品和版本

思科网络威胁防御解决方案 1.1 是经过测试的系统。经证明，在使用表 1 中列出的组件时，该解决方案可以实现所有既定目标。

表 1　思科网络威胁防御解决方案 1.1 组件

组件	硬件	版本	映像类型和许可证
Cisco Catalyst® 3560-X 或 3750-X 系列思科	版本 ID：02 修订版 0x03 10 GE 服务模块	思科 IOS® 软件版本 15.0(1)SE3	通用和 IP Services
Cisco Catalyst 4500E 系列	Supervisor 7E	思科 IOS 软件版本 15.0(2)X0	通用和 IP Base
	Supervisor 7L-E	思科 IOS 软件版本 15.0(2)X0	通用和 IP Base
Cisco Catalyst 6500 系列	Supervisor 2T	思科 IOS 软件版本 15.0(1)SY2	高级企业服务、高级 IP Services 和 IP Base
思科 ISR G2	任意	思科 IOS 软件版本 15.2(4)M2	通用和 IP Base
思科 ASR 1000 系列聚合多业务路由器	思科 ASR 1000 系列路由器处理器 1 或 2 (RP1/RP2)、思科 ASR 1001 路由器、思科 ASR 1002 非模块化路由器、思科 1004、1006 和 1013 路由器并带有 • 速度为 10、20 或 40 Gbps 的嵌入式服务处理器 (ESP) • SPA 接口处理器 (SIP) 10/40	思科 IOS 软件版本 15.2(1)S 或 XE3.5	通用和 IP Base
思科自适应安全设备	任意	思科 ASA 软件版本 8.4(4)1	任意
Cisco NetFlow Generation 设备	3140	思科 NGA 软件版本 1.0	任意
思科身份服务引擎	任意（包括虚拟机）	思科 ISE 软件版本 1.1.1	任意
Lancope StealthWatch Management Console	任意（包括虚拟机）	StealthWatch 6.3	任意
Lancope StealthWatch FlowCollector	任意（包括虚拟机）	StealthWatch 6.3	任意
Lancope StealthWatch FlowSensor	任意（包括虚拟机）	StealthWatch 6.3	任意
Lancope StealthWatch FlowReplicator	任意（包括虚拟机）	StealthWatch 6.3	任意

注意 目前，仅 WS-X6908-10G-2T/2TXL、WS-X6816-10T-2T/2TXL、带有 DFC4/DFC4XL 的 WS-X6716-10G 和带有 DFC4/DFC4XL 的 WS-X6716-10T 线卡可以在基于管理引擎 2T 的系统中执行 NetFlow 记录导出。所有将来的 Cisco Catalyst 6500 系列模块都将支持此功能。

注意 在 Cisco Catalyst 3560-X/3750-X 系列交换机中，只有服务模块的两个 10 千兆以太网端口支持 NetFlow 服务。截至当前版本，这些端口仅支持 10 千兆以太网布线或光纤信道 SFP。

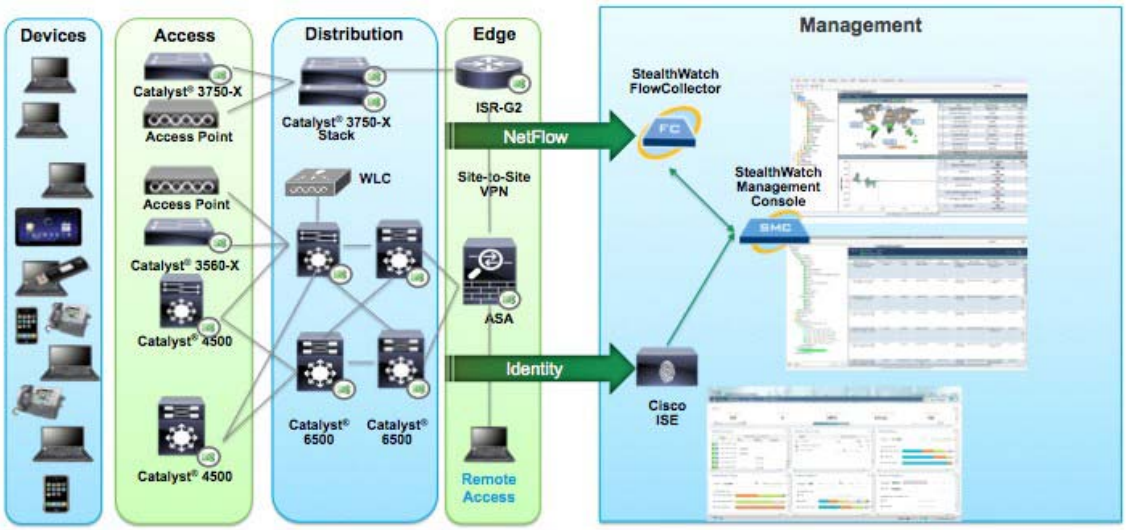
注意 **最佳实践：**在构建整个网络时，可能不会仅使用列出的思科网络设备。要在这些情况下实现解决方案所要求的全面可视性，可能有必要使用 Lancope StealthWatch FlowSensor 来获取对网络的可视性。

解决方案概述

架构

思科网络威胁防御解决方案 1.1 通过使用 Cisco NetFlow 技术提供对所有网络流量的全面可视性。Cisco NetFlow 是所有思科企业级交换机和路由器都支持的一项技术。该技术可在网络的所有层进行全面的遥测，而且不会对性能造成任何影响。通过将此增强的可视性与 Cisco TrustSec® 解决方案所提供的身份和情景信息结合，安全操作员可以更好地了解网络流量。图 1 说明思科网络威胁防御解决方案 1.1 的高级系统架构。

图 1　　网络威胁防御解决方案 1.1. 架构



网络流量的可视性是由思科路由器和交换机的 NetFlow 导出信息提供的。身份服务（包括用户名和配置文件信息）则是由 Cisco TrustSec 解决方案提供。Lancope StealthWatch FlowCollector 提供 NetFlow 收集服务，并执行分析来检测可疑活动。StealthWatch Management Console 提供针对所有 StealthWatch 设备的集中管理功能，以及有关 NetFlow 和身份组合分析的实时数据关联、可视化和整合报告功能。

思科网络威胁防御解决方案 1.1 组件包括用于验证用户身份和生成 NetFlow 数据的网络设备、Lancope StealthWatch System 中的组件和 Cisco TrustSec 中的组件。获取流和行为可视性的最低系统要求是使用由 StealthWatch Management Console 管理的单个 StealthWatch FlowCollector 来部署一个或多个 NetFlow 生成器。获取身份服务的最低要求是在有效的 Cisco TrustSec 监控模式部署中部署思科 ISE 和一个或多个身份验证访问设备。

NetFlow 简介

NetFlow 是一个思科应用，用于在流量穿越思科设备时测量该流量的 IP 网络流量属性（流被识别为指定源和目标之间的单向数据包流）。NetFlow 最初创建旨在测量网络流量特性，例如带宽、应用性能和利用率。NetFlow 在以往一直用于计费和记帐、网络容量规划以及可用性监控。NetFlow 是一种报告技术：在流量穿越设备时，该设备收集有关流量的信息并对流发生后的信息进行报告。NetFlow 报告还具有大量安全应用，包括能够提供不可否认性、异常检测和调查功能。

NetFlow 自首次推出以来历经许多版本，可以在表 2 中进行查看。固定导出格式版本（版本 1、5、7、8）不灵活且无法改编，并且每个新版本都包含与以前版本不兼容的新导出字段。NetFlow 版本 9 将收集和导出过程完全分离，并允许对 NetFlow 收集进行定制。

表 2　NetFlow 版本

版本	状态
1	原始；类似于 v5，但是，没有序列号或 BGP 信息
2	从未发布
3	从未发布
4	从未发布
5	固定格式；在生产中最常见的版本
6	从未发布
7	类似于 v5，但不包括 AS 接口、TCP 标志和 ToS 信息；特定于 Cisco Catalyst 6500 和 7600
8	11 个汇聚机制选项；在企业中从未获得广泛使用
9	灵活、可扩展的导出格式，支持其他字段和技术
IPFIX	类似于 v9，但已标准化，并且具有变量长度字段

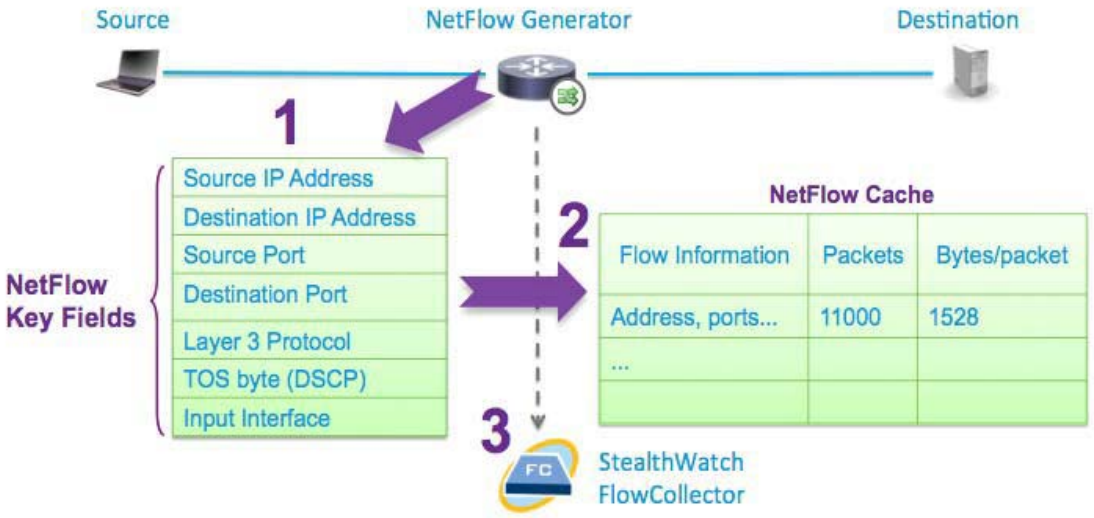
思科网络威胁防御解决方案 1.1 利用 思科 IOS 中 Flexible NetFlow 功能的定制功能，允许使用可定制的 NetFlow v9 记录。使用此方法，思科网络威胁防御解决方案 1.1 为每个解决方案设备定义了 NetFlow 记录，可以通过使用 NBAR 收集诸如 TCP 标志、生存时间 (TTL) 值、协议和应用名称之类的数据包字段来最大化每台设备的安全监控潜力。其中许多字段在 NetFlow 协议的以前版本中不可用；在没有这些字段的情况下，思科网络威胁防御解决方案 1.1 中一些经过调优的检测算法所提供的优势会荡然无存。

注意　**最佳实践：**尽可能使用思科 IOS Flexible NetFlow 功能。

图 2 说明在思科设备上的 NetFlow 操作。

1. 当流量穿越思科设备（NetFlow 生成器）时，会提取 NetFlow 关键字段。
2. 关键字段用于识别 NetFlow 缓存中的流，该缓存是在设备上维护的流的数据库。除关键字段以外，思科设备还收集其他已配置的采集字段（例如 TCP 标志、字节计数器以及开始和结束时间），并且将此信息存储在该流的 NetFlow 缓存条目中。
3. 当流终止或发生超时事件时，将会生成 NetFlow 协议数据单元 (PDU)（称为流记录），并将其发送到流收集器中。

图 2　　思科设备上的 NetFlow 操作



选择监控位置

当在所有网络层的网络设备上启用 NetFlow 时，思科网络威胁防御解决方案 1.1 最有效。通过此级别的可视性，可以记录和分析所有网络流量并识别威胁，例如通过内部网络侧向传播的恶意软件，也就是说，传播到其他主机而不离开 VLAN 和跨越第 3 层边界的恶意软件。可视性跨整个网络并尽量接近流量源，可以提高行为算法的准确性，并确保不会遗漏网络通信。

注意　**最佳实践：**尽可能靠近接入层启用 NetFlow。

思科网络威胁防御解决方案 1.1 实施应完整（非采样）使用 NetFlow。采样的 NetFlow 会遗留盲点，因为只有一定百分比的网络流才具有关联的网络记录。这将难以检测指示恶意活动的单一流量异常。

一些旧思科设备以及思科集成服务路由器 (ISR) 和思科聚合服务路由器 (ASR) 使用功能集的软件实施来支持 NetFlow 服务。部署软件支持的 NetFlow 服务时，请考虑软件路由器的当前利用率，因为启用 NetFlow 会影响设备性能；例如，运行思科 IOS 软件的完全加载的软件路由器可能因启用 NetFlow 而提升大约 15% 的 CPU 利用率。在实现软件支持的 NetFlow 服务时，请查阅位于以下 URL 的 Cisco NetFlow 性能分析白皮书：
http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns562/ns583/net_implementation_white_paper0900aecd80308a66.pdf。

启用 NetFlow 服务后，具有硬件支持的 NetFlow 的思科设备所遭受的性能下降最少。这些设备中最明显的性能限制是受硬件支持的 NetFlow 缓存的大小。表 3 显示在硬件还是软件中支持 CTD 1.1 解决方案组件。

表 3　NetFlow 支持硬件或软件

组件	硬件支持	软件支持
Cisco Catalyst 3560-X 或 3750-X 系列	X	
Cisco Catalyst 4500E 系列	X	
Cisco Catalyst 6500 系列	X	
Cisco NetFlow Generation 设备	X	
思科 ISR G2		X
思科 ASR 1000 系列		X
思科自适应安全设备		X[1]

1. ASA NetFlow 实施称为 NetFlow 安全事件日志记录 (NSEL)，与大多数软件支持的 NetFlow 实施不同。有关详细信息，请参阅本指南中关于 ASA 的小节。

表 4 显示具有硬件支持的 NetFlow 的解决方案设备的缓存大小限制。当设备上的 NetFlow 缓存已满时，该设备不会为通过设备的新流生成 NetFlow 记录。

表 4　思科设备上的 NetFlow 缓存大小限制

组件	硬件	缓存大小（流）
Cisco Catalyst 3500-X	10 GE 服务模块	32,000
Cisco Catalyst 4500E 系列	管理引擎 7E	128,000
	Supervisor 7L-E	128,000
Cisco Catalyst 6500 系列	Supervisor 2T	512,000
	Supervisor 2TXL	1,000,000

注意　具有软件支持的 NetFlow 的设备（例如 ISR）上的 NetFlow 缓存大小受可用内存量的限制。

尽管思科网络威胁防御解决方案 1.1 中的每台 NetFlow 生成设备都支持 Flexible NetFlow 功能，但是可定制的流记录支持因平台而异。这意味着通用流量记录无法捕获所有必要的安全信息，并且无法将其应用于解决方案中的每台设备。表 5 列出跨解决方案设备的流记录支持。鉴于在支持方面存在差异，如果在部署过程中有解决方案组件进行异类混合来填补可视性差距，则可获取最佳结果。

表 5　流记录支持

理想的解决方案流记录	Cisco Catalyst 3560-X/3750-X	Cisco Catalyst 4500 Sup7-E/ Sup7L-E	Cisco Catalyst 6500 Sup2T	思科 ISR	思科 ASR 1000	思科 NGA
match ipv4 tos	是	是	是	是	是	是
match ipv4 protocol	是	是	是	是	是	是
match ipv4 source address	是	是	是	是	是	是
match ipv4 destination address	是	是	是	是	是	是
match ipv4 destination address	是	是	是	是	是	是

表 5　流记录支持（续）

理想的解决方案流记录	Cisco Catalyst 3560-X/3750-X	Cisco Catalyst 4500 Sup7-E/ Sup7L-E	Cisco Catalyst 6500 Sup2T	思科 ISR	思科 ASR 1000	思科 NGA
match transport destination-port	是	是	是	是	是	是
match interface input	是	是	是	是	是	是
match datalink mac source-address	是	否	否	否	否	否
match datalink mac destination-address	是	否	否	否	否	否
collect routing next-hop address ipv4	否	否	否	是	是	是
collect ipv4 dscp	否	是	否	是	是	是
collect ipv4 ttl minimum	match ipv4 ttl	是	否	是	是	是
collect ipv4 ttl maximum	match ipv4 ttl	是	否	是	是	是
collect transport tcp flags	否	是	是	是	是	是
collect interface output	是	是	是	是	是	否
collect counter bytes	是	是	是	是	是	是
collect counter packets	是	是	是	是	是	是
collect timestamp sys-uptime first	是	是	是	是	是	是
collect timestamp sys-uptime last	是	是	是	是	是	是
collect application name	否	否	否	是	是	否

注意　**最佳实践：**虽然并非每台思科网络设备都需要存在于部署过程中以使解决方案发挥作用，但是由于每个平台之间的 NetFlow 支持存在差异，因此思科建议采取异类混合方式，来部署那些所列出的设备。

选择监控位置和 NetFlow 生成设备后，必须在该设备上启用 NetFlow。有关详细信息，请参阅本指南中特定于设备的 NetFlow 配置小节。

确定每秒的流量

确定好监控位置后，下一步是确定并测量该监控位置会生成的每秒流量 (fps)。fps 的数量（量）指示 StealthWatch FlowCollector 必须能够接收和分析的记录数；选择 StealthWatch FlowCollector 型号（在后续小节中进行描述）时，必须考虑此数字。

在部署思科网络威胁防御解决方案 1.1 之前确定 fps 数量需要深思熟虑。许多因素都可能影响网络设备生成的流量，因此，预测确切数值会非常困难。通常，当 1 Gbps 的流量经过 NetFlow 生成器时，该设备生成的 fps 数值会介于 1000 和 5000 之间。但是，这是一般准则，应仅作为起步点。

请注意，流量吞吐量 (Gbps) 与 fps 数量不直接相关；具有直接影响的唯一计量是通过设备的流的数量 （和速率）。例如，可能会有单条高容量 (1 Gbps) 流经过端口，产生的 fps 数值不到 1；相反，也可能有许多小容量流经过端口，虽然总吞吐量很低，但是会产生较高的 fps 数值 （例如，4000 条总吞吐量为 100 Mbps 的流）。 fps 数量主要受以下计量的影响：

- 通过设备的唯一流的数量
- 每秒的新连接数
- 流的生存时间（短期与 长期）

此外，还应考虑 NetFlow 记录可能对网络流量产生的影响（尽管这通常不是一个重要的考虑事项）。一般情况下，NetFlow 在网络中增加的流量微乎其微，因为 NetFlow 记录代表整个流量流的报告。但是，某些流量集可能会生成比其他流量集更多的 NetFlow 记录。可能影响 NetFlow 占用的网络资源的因素包括（但不限于）：

- 每秒流量
- NetFlow 记录大小。网络威胁防御解决方案 1.1 推荐使用 NetFlow v9，该版本的 NetFlow 平均会对每个 1500 字节数据包产生 34 个 NetFlow 记录。
- 流计时器（流的活动和非活动超时）。网络威胁防御解决方案 1.1 建议活动计时器为 60 秒，非活动计时器为 15 秒。

要预测启用 NetFlow 的影响，请使用 Lancope NetFlow 带宽计算器，此工具可在以下 URL 中获取：http://www.lancope.com/resource-center/netflow-bandwidth-calculator-stealthwatch-calculator/

注意 **最佳实践：**如果需要考虑最大限度减少 NetFlow 占用的资源，应尽可能靠近 NetFlow 生成器进行 NetFlow 收集。

注意 **最佳实践：**在非对称路由情况下，非对称路由中的所有设备都应将 NetFlow 记录发送到到同一 FlowCollector。

在确定监控位置并制定设计注意事项后，思科网络威胁防御解决方案 1.1 部署的下一步是选择并部署 Lancope StealthWatch System 组件。

部署 Lancope StealthWatch System

Lancope StealthWatch® System（可从思科购买）是现今市场上领先的基于流的安全监控解决方案，在思科网络威胁防御解决方案 1.1 中用作 NetFlow 分析器和管理系统。表 6 简要介绍和描述 Lancope StealthWatch System 中的各个组件。

表 6　Lancope StealthWatch System 组件

组件	描述
StealthWatch Management Consol	管理、协调和配置所有 StealthWatch 设备，以关联整个企业内的安全性和网络情报。从思科身份服务引擎检索已进行身份验证的会话信息，以关联流和身份。
StealthWatch FlowCollector	作为中央收集器，收集由启用 NetFlow 的设备生成的流数据。StealthWatch FlowCollector 对网络流量进行监控、分类和分析，在网络级别和主机级别创建全面的安全情报。
StealthWatch FlowReplicator	将 NetFlow、系统日志和 SNMP 信息汇聚在单个高速设备中。此高速 UDP 数据包复制器从 FlowReplicator 中的多个位置收集关键的网络优化和安全信息，然后在单条数据流中将这些信息转发到一个或多个 StealthWatch FlowCollector 设备。
StealthWatch FlowSensor	被动监控所有主机和服务器通信及网络流量统计信息，将其转换为会发送到 FlowCollector 的流记录。
StealthWatch FlowSensor VE	专门用于在虚拟服务器内部运行的虚拟设备。FlowSensor VE 被动监控虚拟机内流量，将其转换为会发送到 FlowCollector 的流记录。

设计注意事项

添加 StealthWatch FlowSensor（可选）

在无法从网络设备生成 NetFlow 的情况下，Lancope StealthWatch FlowSensor 和 FlowSensor VE 可用于将通信转换为流记录。通过这种方法，可以在思科网络威胁防御解决方案 1.1 中使用本指南中未指定的网络设备。此外，StealthWatch FlowSensor 还可用于为网络的关键区域添加数据包级应用识别和性能指标。

考虑向思科网络威胁防御解决方案 1.1 部署中添加 StealthWatch FlowSensor 时，请执行以下步骤。

操作步骤

步骤 1　选择 StealthWatch FlowSensor。

选择 StealthWatch FlowSensor 时，应考虑监控点的预期流量配置文件，因为 FlowSensor 必须能够处理发送给它的流量级别。与思科网络威胁防御解决方案 1.1 中的任何其他 NetFlow 生成设备一样，思科建议尽可能靠近接入层部署 FlowSensor。

表 7 列出 StealthWatch FlowSensor 设备型号及其规格。所显示的处理容量是支持的持续速率。FlowSensor 可以处理超过所列容量的短暂突发。与所有 NetFlow 生成器类似，StealthWatch FlowSensor 生成的 NetFlow 流量因受监控的流量配置文件而有所不同。

表 7　StealthWatch FlowSensor 设备规格

型号	处理容量	接口	速度	物理层	外形	功率
250	100 Mbps	2	10/100/100	铜缆	1 RU（短）	非冗余
1000	1 Gbps	6	10/100/1000	铜缆	1 RU（短）	非冗余
2000	60,000	5	10/100/1000	铜缆或光纤	1 RU	冗余
3000	120,000	1 或 2	1GB	光纤	1 RU	冗余

注意　如果达到单个 StealthWatch FlowSensor 的处理容量，则可以使用适当的以太网负载均衡器堆叠多个 FlowSensor。

StealthWatch FlowSensor VE 是一台虚拟设备，可以安装在 vSphere/ESX 主机内部并用于为该主机中虚拟机之间的流量生成 NetFlow 记录。FlowSensor VE 以混合模式连接到虚拟交换机。它从其观察的流量中被动捕获以太网帧，然后创建流记录，其中包含与对话对、比特率和数据包速率相关的有价值的会话统计信息。然后，FlowSensor VE 将这些记录发送到 StealthWatch FlowCollector。表 8 介绍 StealthWatch FlowCollector VE.103 部署的要求。

表 8　StealthWatch FlowSensor VE 规格

磁盘空间要求	流导出格式	最低 CPU 要求	最低内存要求	接口
1.4 GB	NetFlow v9	2 GHz 处理器	512 MB 1024 MB，用于应用检查	最多 16 个 vNIC

步骤 2　将 StealthWatch FlowSensor 集成到网络中。

StealthWatch FlowSensor 必须放在与监控点相邻的第 1 层或第 2 层中。部署模式示例包括使用测试接入端口 (TAP)、交换端口分析器 (SPAN) 端口或网络集线器。有关如何将 StealthWatch FlowSensor 集成到网络中的详细信息，请参阅 Lancope StealthWatch 文档 CD 上的《系统硬件安装指南》。

选择 StealthWatch FlowCollector

StealthWatch FlowCollector 用作思科网络威胁防御解决方案 1.1 中所有 NetFlow 生成器生成的 NetFlow 数据的中央收集和分析点。在解决方案部署中需要选择的 StealthWatch FlowCollector 数量和型号取决于以下因素：

- 以前各节中制定的决策，这些决策影响每秒将到达 StealthWatch FlowCollector 的流量
- StealthWatch FlowCollector 部署策略
- 每个 StealthWatch FlowCollector 的物理容量

操作步骤

步骤 1 确定 StealthWatch FlowCollector 部署策略。

可以通过分布式或集中式方法部署 StealthWatch FlowCollector。在分布式部署中，FlowCollector 部署在多个站点，并且通常放在会产生最高数量的 NetFlow 记录的源附近。此部署的优点是可限制由 NetFlow 引入的开销。在集中式部署中，所有 StealthWatch FlowCollector 都放在单个数据中心（可能在负载均衡器后）中，由此提供的好处是全局使用单个收集位置并可能使用单个 IP 地址进行 NetFlow 收集。此部署在 NetFlow 生成器相隔遥远的环境中提供多个优势。

还可能要考虑站点之间的带宽限制（例如在广域网上）。通常，单个 FlowCollector 应该用于尽可能多的相关流量。当流量不相似时，则集中收集的优势会减少。

当特定 FlowCollector 接收流数据时，它会删除其接收的任何重复流记录，这意味着将为该流创建单个数据库条目。此重复数据删除过程确保 FlowCollector 以最高效的方式存储流数据，同时保留有关每个流导出器的详细信息并消除表明流量增大的报告。

在理想的实施中，导出与特定流相关的数据的每台路由器都将该数据发送到同一 FlowCollector。但是，每个唯一主机对（或对话）会消耗 FlowCollector 上的其他资源。如果同时连接数过高，则会从内存中清除流记录。在部署规划期间请注意，以确保每个 FlowCollector 都有足够的资源来保留所有活动对话中的状态而不清除记录，直至对话已空闲一段时间之后。

注意 **最佳实践：**所有属于流的 NetFlow 记录都应发送到同一 StealthWatch FlowCollector。

步骤 2 性能注意事项。

每个 StealthWatch FlowCollector 可以支持最小保证流量，如表 9 中所示。但是，在为思科网络威胁防御解决方案 1.1 选择 StealthWatch FlowCollector 时，另请考虑以下因素：

- 导出器计数 - 每个 StealthWatch FlowCollector 可以接受的 NetFlow 生成设备的数量。
- 数据速率 - StealthWatch FlowCollector 接收的 fps 的速率。
- 主机计数 - StealthWatch FlowCollector 可以为其维护状态的主机（位于网络内部和外部）的数量。思科建议内部主机数不超过主机计数值的 60%。
- 流存储量 - 网络上特定位置所需的精细流数据量。

注意 如果系统达到导出器的最大数量和特定机箱的最大数据速率，则该系统可能会遭遇性能问题。例如，在达到最大导出器数量时，最大数据速率估计会降低 10% 到 20%。

表 9 StealthWatch FlowCollector 设备规格

型号	每秒流量	导出器数量	主机数	存储器
StealthWatch FlowCollector 1000	最多 30,000	最多 500	最多 250,000	1.0 TB
StealthWatch FlowCollector 2000	最多 60,000	最多 1000	最多 500,000	2.0 TB
StealthWatch FlowCollector 4000	最多 120,000	最多 2000	最多 1,000,000	4.0 TB

表 10 根据虚拟机的保留内存量和 CPU 数量列出对 StealthWatch FlowCollector VE 的支持。

表 10　StealthWatch FlowCollector VE 规格

每秒流量	导出器数量	主机数	保留内存	保留 CPU 数量
最多 4500	最多 250	最多 125,000	4 GB	2
最多 15,000	最多 500	最多 250,000	8 GB	3
最多 22,500	最多 1000	最多 500,000	16 GB	4
最多 30,000	最多 1000	最多 500,000	32 GB	5

选择 StealthWatch Management Console

StealthWatch Management Console (SMC) 管理整个 StealthWatch System 安装，并且按照与其连接的 FlowCollector 的数量和整个系统监控的总流量获取许可。

表 11 显示 SMC 型号及其支持的 StealthWatch FlowCollector 的数量。表 12 列出 SMC VE 可以支持的 FlowCollector 和并发用户的数量（根据保留内存和 CPU 数量而定）。

表 11　SMC 设备规格

SMC 型号	最大 FlowCollector 数量	尺寸	存储器	内存
SMC 1000	5	1 RU	1.0 TB	8 GB
SMC 2000	25	2 RU	2.0 TB	16 GB

表 12　SMC VE 规格

FlowCollector 数量	并发用户数	保留内存	保留 CPU 数量
1	2	4 GB	2
3	5	8 GB	3
5	10	16 GB	4

注意　如果在部署过程中预计有大量主机组和受监控接口，则应考虑高性能 SMC，因为发送到 SMC 的数据量在这些部署过程中会增加。

选择 StealthWatch FlowReplicator（可选）

StealthWatch FlowReplicator 接收或监控 UDP 数据包，并生成这些数据包的副本以发送到一个或多个新目的地，同时在数据包穿越设备时对其进行修改，使其看似来自原始源。每个 FlowReplicator 附带两个活动接口：一个接口分配有用于管理、监控和生成数据包副本的 IP 地址；另一个接口可以置于混合模式下进行监控。

根据每秒的数据包数量 (pps)，将会标定每个 FlowReplicator 具有一定的输入和输出量。每台设备对于每个数据包生成两到三个副本的情况进行测试，但在需要时可以支持更多目标。表 13 列出 StealthWatch FlowReplicator 型号和规格。

表 13　StealthWatch FlowReplicator 设备规格

FlowReplicator 型号	处理容量	物理层	外形	功率	容错
1000	10,000 pps 输入 20,000 pps 输出	铜缆	1 RU（短）	非冗余	否
2000	20,000 pps 输入 60,000 pps 输出	铜缆或光纤	1 RU	冗余	是

注意　如果超过设备的物理限制，并且为链路生成的副本过多，则会丢弃数据包。

部署 Lancope StealthWatch System

本节介绍在 Lancope StealthWatch System 中部署每台设备并准备在思科网络威胁防御解决方案 1.1 中对其进行操作所需的操作步骤。

安装每台设备

要安装每台设备，请执行以下步骤。

操作步骤

步骤 1　安装 StealthWatch Management Console (SMC)。

作为管理设备，SMC 设备应安装在可供所有 StealthWatch System 组件和管理设备访问的网络中的一个位置，并且能够打开与思科身份服务引擎的 HTTPS 连接。如果存在故障转移 SMC，则思科建议将主要 SMC 和辅助 SMC 安装在不同的物理位置。有关详细信息，请参阅 Lancope StealthWatch 文档 CD 上的《*系统硬件安装指南*》。

步骤 2　（可选）安装所有 StealthWatch FlowSensor。

作为被动监控设备，StealthWatch FlowSensor 可以放置在网络中的任何位置，该网络当前不具有本机 NetFlow 支持来观察和记录 IP 活动。与思科网络威胁防御解决方案 1.1 中的任何 NetFlow 配置一样，FlowSensor 在其放置位置可以使其监控接入层流量时最有效。有关 StealthWatch FlowSensor 安装的详细信息，请参阅 Lancope StealthWatch 文档 CD 上的《*系统硬件安装指南*》。

步骤 3　（可选）安装所有 StealthWatch FlowSensor VE。

StealthWatch FlowSensor VE 用于混合监控单个 vSphere/ESX 主机内部的虚拟机间通信。有关详细信息，请参阅 Lancope StealthWatch 文档 CD 上的《*FlowSensor VE 安装和配置指南*》。

步骤 4　安装 StealthWatch FlowCollector

作为收集和监控设备，每台 StealthWatch FlowCollector 设备都应安装在网络中的一个位置，该网络可供将 NetFlow 数据生成并发送到 FlowCollector 的设备访问。FlowCollector 还应该可供任何需要访问管理接口的设备进行访问，包括来自 SMC 的 HTTPS 访问。有关详细信息，请参阅 Lancope StealthWatch 文档 CD 上的《*系统硬件安装指南*》。

步骤 5 （可选）安装 StealthWatch FlowReplicator

对 StealthWatch FlowReplicator 的放置的唯一要求是其具有其余 StealthWatch System 组件的无障碍通信路径。有关详细信息，请参阅下一个操作步骤（配置防火墙）以及 Lancope StealthWatch 文档 CD 上的《*系统硬件安装指南*》。

StealthWatch FlowReplicator 具有两个活动接口：一个接口分配有用于管理、监控和生成数据包副本的 IP 地址；另一个接口可以置于混合模式下进行监控。

配置防火墙

如果在部署中的任意位置存在防火墙，请查阅图 3。该图说明网络威胁防御解决方案 1.1 中的数据流，以确保允许使用适当的端口和服务。表 14 进一步突出显示所需服务。有关详细信息，请参阅 Lancope StealthWatch 文档 CD 上的《*系统硬件安装指南*》。

图 3　　思科网络威胁防御解决方案 1.1 数据流

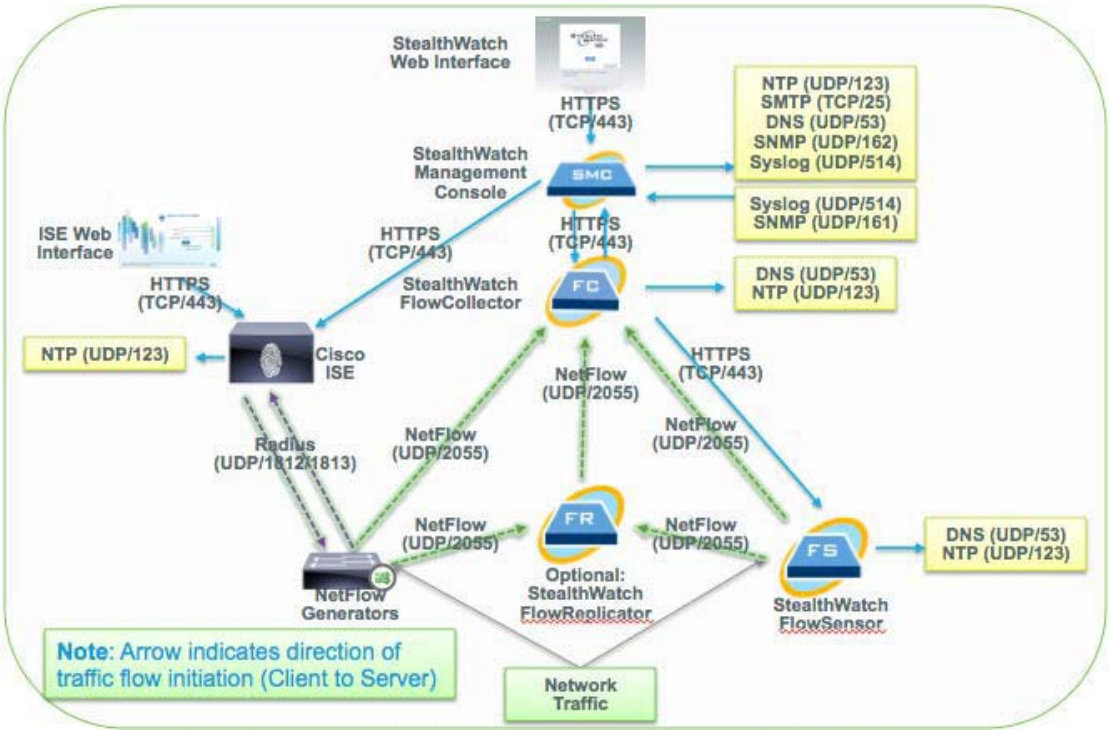


表 14　　所需服务

客户端	服务器	端口	注释
SMC	FlowCollector	TCP/443	HTTPS
SMC	思科身份服务引擎	TCP/443	HTTPS
SMC	导出器	UDP/161	SNMP
SMC	—	UDP/123	NTP
SMC	—	TCP/25	SMTP（可选）
SMC	—	UDP/53	DNS

表 14　所需服务（续）

客户端	服务器	端口	注释
SMC	—	UDP/162	SNMP-TRAP（可选）
SMC	—	UDP/514	SYSLOG（可选）
SMC	身份服务引擎	TCP/443	HTTPS
—	SMC	UDP/514	SYSLOG（可选）
—	SMC	UDP/161	SNMP（可选）
SW 网络界面	SMC	TCP/443	HTTPS
FlowCollector	SMC	TCP/443	HTTPS
FlowCollector	FlowSensor	TCP/443	HTTPS
FlowCollector	—	UDP/123	NTP
FlowCollector	—	UDP/53	DNS
FlowSensor	—	UDP/123	NTP
FlowSensor	—	UDP/53	DNS
FlowSensor	FlowCollector	UDP/2055	NetFlow
导出器	FlowCollector	UDP/2055	NetFlow

在每台设备上运行系统配置

系统配置对话框用于初始化每个 StealthWatch 组件的网络和访问信息。每台 StealthWatch 设备的对话框和配置步骤相同。此配置的详细信息可在 Lancope StealthWatch 文档 CD 上的《系统配置指南》中获取。

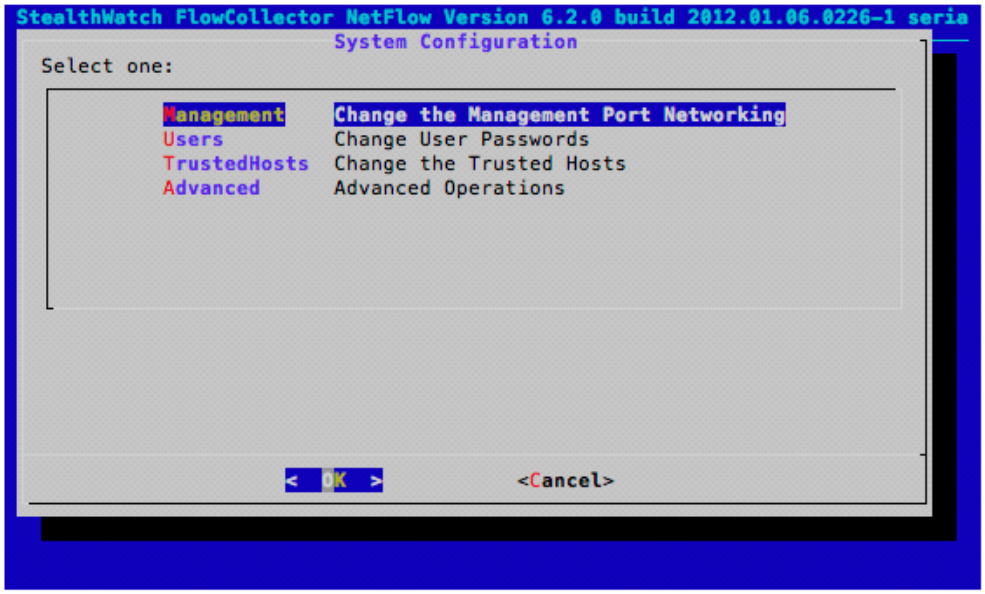
操作步骤

步骤 1　通过控制台界面登录到设备中。

注意　默认控制台用户名为 *sysadmin*，密码为 *lan1cope*。

步骤 2 运行系统配置程序。系统将显示类似于图 4 中的屏幕。

图 4 系统配置屏幕



注意 有关详细信息，请参阅《StealthWatch *系统配置指南*》的第 1 章。

注意 在命令提示符处输入 *SystemConfig* 将进入系统配置。

步骤 3 配置管理端口网络。

这是允许设备连接到网络所必要的 IP 地址和子网信息。这也是用于通过网络界面访问设备的 IP 地址。

注意 有关其他信息，请参阅《StealthWatch *系统配置指南*》的第 2 章。

注意 **最佳实践：**为每个 StealthWatch System 组件配置 DNS 条目。

步骤 4 更改用户密码。

更改用于访问控制台界面的密码。这也是用于对设备命令提示符进行 SSH 访问的密码。

注意 有关详细信息，请参阅《*系统配置指南*》的第 3 章。

注意 SSH 访问在默认情况下已禁用，并且可以通过网络界面启用；这在下一操作步骤中进行了描述。

步骤 5 配置可信主机设置（可选）。

这些设置反映允许访问设备的主机的 IP 地址。有关详细信息，请参阅《*系统配置指南*》的第 4 章。

登录每台设备的网络界面

操作步骤

步骤 1 访问 StealthWatch FlowCollector 的网络界面。

在 **https://sfc.demo.local** 中访问该网络界面，其中 **sfc.demo.local** 是以前操作步骤中配置的 IP 地址的 DNS 条目。

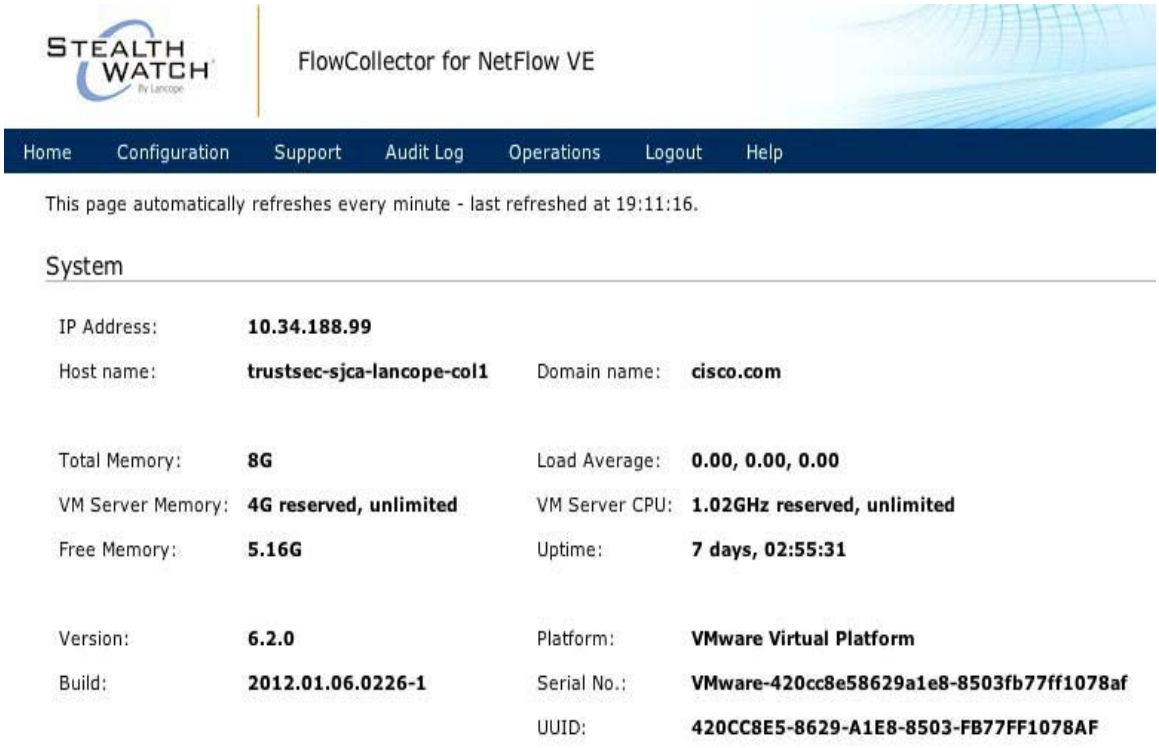
步骤 2 访问 SMC 的网络界面。

在 **https://smc.demo.local/smc/login.html** 中访问该网络界面，其中 smc.demo.local 是以前操作步骤中配置的 IP 地址的 DNS 条目。

注意 网络界面访问凭证与控制台访问凭证不同。默认用户名为 *admin*，密码为 *lan411cope*。

步骤 3 每台设备的网络界面将类似于图 5。

图 5 StealthWatch FlowCollector 网络界面



注意 有关详细信息，请参阅《*系统配置指南*》的第 6 章。

配置主机名和 DNS 设置

操作步骤

步骤 1 从网络界面主页中，点击 **Configuration > Naming and DNS**。

步骤 2 设置设备的主机名和域名。

步骤 3 点击 **Apply**。

步骤 4 将 DNS 服务器的地址输入到文本框中。

步骤 5 点击 **Add**。

步骤 6 点击 **Apply**。

配置时间设置

操作步骤

步骤 1 从网络界面主页中，点击 **Configuration > System Time and NTP**。

步骤 2 确保选择 Enable Network Time Protocol 复选框。

步骤 3 从下拉菜单中选择首选 NTP 服务器，或者在文本框中输入本地 **NTP** 服务器的 **IP** 地址。

注意 **最佳实践：**对于所有思科网络威胁防御解决方案组件（包括 NetFlow 生成器）使用同一时间源。

步骤 4 点击 **Add**。

步骤 5 点击 **Apply**。

步骤 6 将时区设置配置为 StealthWatch 设备所在的时区。

步骤 7 点击 **Apply**。

配置管理员密码

按照此操作步骤更改网络界面管理员帐户的密码。

操作步骤

步骤 1 从网络界面主页中点击 **Configuration > Password**。

步骤 2 使用当前密码和新密码填写文本框。

步骤 3 点击 **Apply**。

配置证书颁发机构证书

注意 在开始此操作步骤之前，必须获取证书颁发机构证书并将其存储在本地磁盘上。

注意 **最佳实践：**此处使用的证书颁发机构证书应该与用于向思科身份服务引擎颁发的身份证书相同。

操作步骤

步骤 1 从网络界面主页中点击 **Configuration > Certificate Authority Certificates**。

步骤 2 点击 **Choose File**，然后浏览本地磁盘以查找 CA 证书。

步骤 3 为证书指定一个名称，以在 SMC 配置中对其进行标识。

步骤 4 点击 Add Certificate。

配置设备身份证书

注意 在开始此操作步骤之前，必须从（上一步中添加的）证书颁发机构获取证书和私钥，并将其存储在本地磁盘上。

操作步骤

步骤 1 从网络界面主页中点击 **Configuration > SSL Certificate**。

步骤 2 点击第一个 **Choose File**，然后浏览本地磁盘以查找设备的身份证书。

步骤 3 （可选）点击第二个 **Choose File**，然后浏览本地磁盘以查找用于颁发身份证书的证书链。

步骤 4 点击第三个 **Choose File**，然后浏览本地磁盘以查找设备的私钥。

步骤 5 点击 **Upload Certificate**。

（可选）配置管理系统

在非 SMC StealthWatch 组件（例如 FlowCollector）上，可以从默认设置修改供 SMC 用于访问设备的凭证。是否执行此步骤完全取决于企业的要求，并不会对思科网络威胁防御解决方案 1.1 的运行造成影响。

注意 要完成此可选设置步骤，必须知道 SMC IP 地址。

操作步骤

步骤 1 从网络界面主页中点击 **Configuration > Management Systems Configuration**。

步骤 2 点击 Add New Management System。

步骤 3 输入 **SMC** 的 IP 地址。

步骤 4 选中 **Is SMC** 复选框。

步骤 5 输入管理员凭证。

步骤 6 输入事件凭证。

步骤 7 点击 **Apply**。

重新启动设备

上述操作步骤会导致设备的主机和时间设置发生更改。思科强烈建议在完成上述步骤后重新启动设备，以确保所有设置都正常运行。

注意 有关网络界面中的每个配置项的详细信息，可在联机帮助中获取，通过点击网络界面中的 **Help** 可以访问联机帮助。

初始化 Lancope StealthWatch System

完成上一节中的操作步骤后，两台必备 Lancope StealthWatch 设备（FlowCollector 和 SMC）应已部署完成，可以开始工作。但是，设备尚未连接在一起，并且 StealthWatch System 未完全初始化。

StealthWatch FlowCollector 已完全部署并可操作，而且现在可以从 NetFlow 导出器接收 NetFlow 记录并开始填充其数据库。如果需要，您可以跳过本文档中的本节内容并在 NetFlow 导出器上配置 NetFlow 导出，从而使其开始生成 NetFlow 并将它发送到 FlowCollector。

本节介绍将 Lancope StealthWatch FlowCollector 集成到 Lancope SMC 中以及为 NetFlow 分析准备 StealthWatch System 的过程。

运行 SMC 客户端软件

操作步骤

步骤 1 访问 SMC 的网络界面。

步骤 2 选择要为客户端计算机上的 SMC 分配的内存量。

步骤 3 如果预计有许多打开的文档或大数据集（例如，超过 100,000 个记录的流查询），请考虑增大内存分配。本地工作站至少应该具有所选内存分配两倍的内存。

步骤 4 点击 **Start** 以下载并安装 SMC 客户端软件。

配置域

首次登录 SMC 客户端时，系统会显示 Default Domain Properties 页面。域定义此部署的相关信息集，包括所有主机和主机组、网络设备、FlowCollector、思科身份服务引擎等等。

注意 **最佳实践：**为整个企业的思科网络威胁防御解决方案 1.1 部署使用单个域。

操作步骤

步骤 1 在 Name 字段中，输入域的名称。

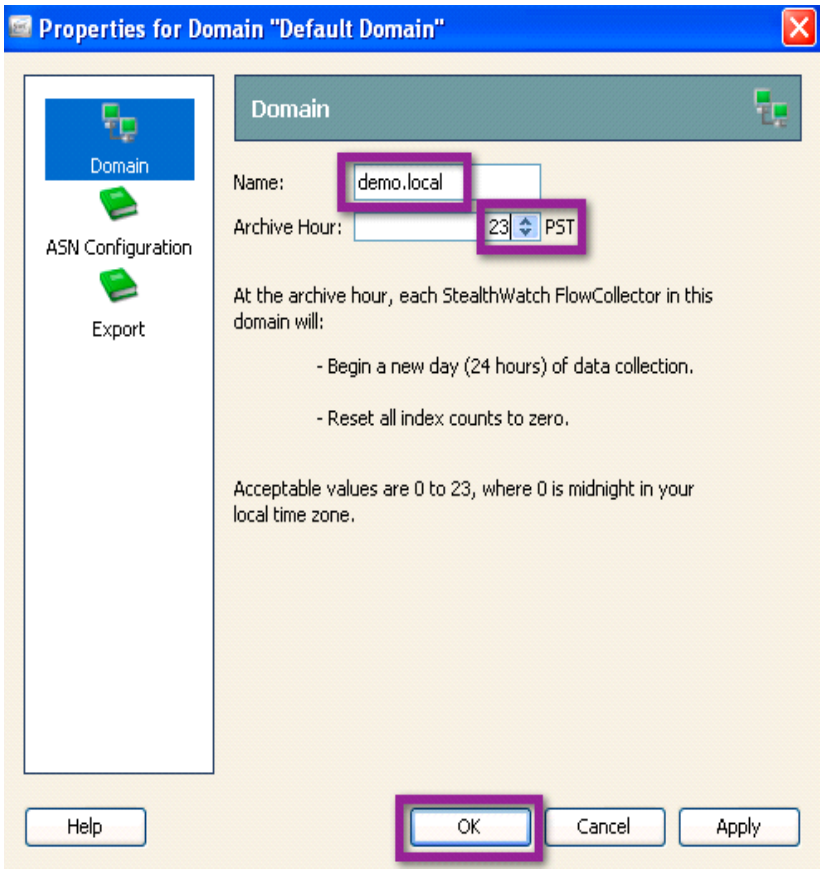
步骤 2 在 Archive Hour 字段中，指定存档时间。

存档时间是相关域中的所有 StealthWatch FlowCollector 开始新一天（24 小时）数据收集并将所有索引计数器重置为零的时刻。前 24 小时内接收的所有数据都将在数据库中存档。

注意 **最佳实践：**将存档时间设置为网络流量处于最小值时的时刻。

步骤 3 点击 **OK**，如图 6 所示。

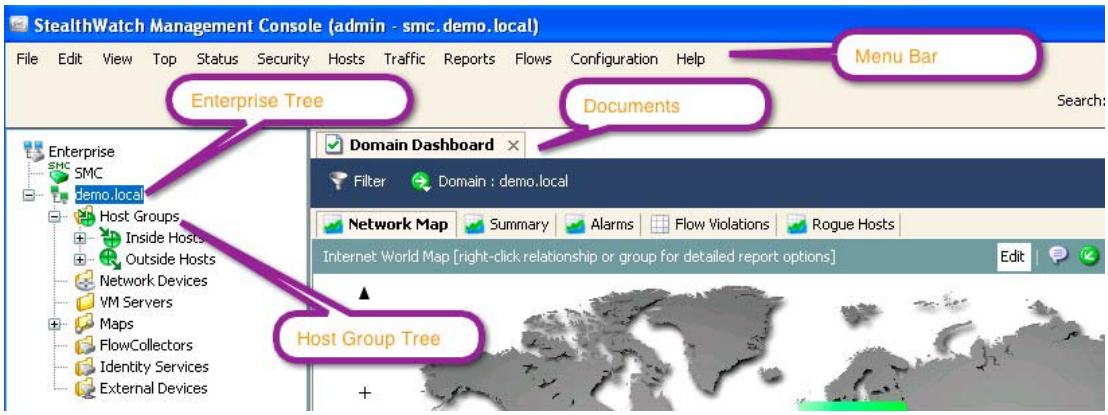
图 6　　设置存档时间



步骤 4 熟悉 SMC 显示（请参阅图 7）。

顶部菜单栏显示菜单选项。左侧显示 Enterprise 树，其中还包含主机组树。右侧是文档显示的位置。

图 7　　设置存档时间



添加 StealthWatch FlowCollector

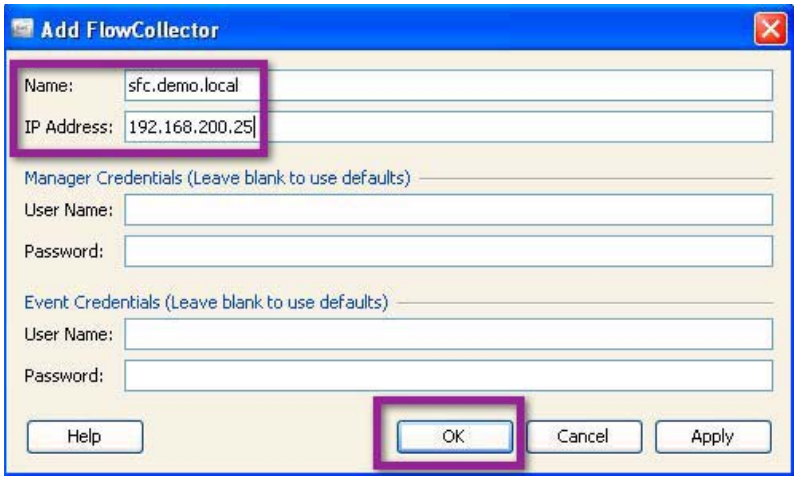
操作步骤

步骤 1　突出显示 Enterprise 树中的域。

步骤 2　点击 **Configuration > Add FlowCollector**。

步骤 3　输入 StealthWatch FlowCollector 的名称和 IP 地址（请参阅图 8）。

图 8　　添加 FlowCollector



步骤 4 输入管理员凭证和事件凭证（可选）。只有在 FlowCollector 部署时更改了默认凭证的情况下，才需要执行此步骤。

步骤 5 点击 **OK**。

步骤 6 系统将打开 Properties for FlowCollector 对话框。使用表 15 验证默认配置。

表 15 默认详细配置信息

配置项	选项	设置
FlowCollector	Name	sfc.demo.local
Advanced	Ignore flows between inside hosts	未选择
	Ignore flows between outside hosts	未选择
	Ignore flow to and from non-routable addresses	未选择
	Ignore flows between inside hosts when calculating File Sharing Index	已选择
	Ignore null0 flows	未选择
	Seconds required to qualify a flow as long duration	32.4k
	Suspect long duration flow trust threshold	6
	Minimum number of asymmetric flows per 5-minute period to trigger Asymmetric_Route alert	50
	Minimum number of Class C subnets an infected host must contact before a worm alarm is triggered	8
	Store flow interface data	尽可能多
Watch List	空	
Broadcast List	空	
Ignore List	空	
Mitigation White List	IP ranges	SMC IP 地址
	Domain names	空
Monitor Port	Port	2055
Exporters & Interfaces	Accept flows from any exporter	已选择
System Alarms	FlowCollector Data Deleted	未选择
	FlowCollector Flow Data Lost	已选择
	FlowCollector Log Retention Reduced	已选择
	FlowCollector Management Channel Down	已选择
	FlowSensor Time Mismatch	已选择
	FlowSensor Traffic Lost	已选择
	FlowSensor VE Configuration Error	已选择
	Interface Utilization Exceeded Inbound	已选择
	Interface Utilization exceeded Outbound	已选择

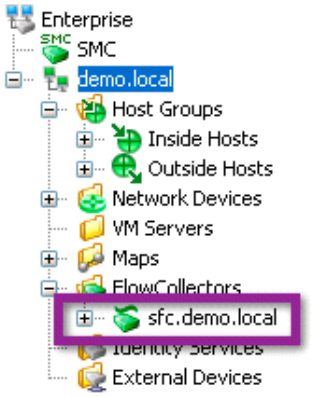
表 15　默认详细配置信息（续）

配置项	选项	设置
	New VM	已选择
	V-Motion	已选择

步骤 7　点击 **Synchronize > Synchronize**，然后点击 **Close**。

步骤 8　展开 Enterprise 树以查看 FlowCollector（请参阅图 9）。

图 9　　查看 FlowCollector



部署过程进行到现在，StealthWatch System 应已完成部署，并准备开始接收和分析 NetFlow 记录。

在思科设备上配置 Flexible NetFlow

如前所述，思科网络威胁防御解决方案 1.1 使用特定思科平台的 Flexible NetFlow 功能。本节简要概述在思科 IOS 上配置 Flexible NetFlow 所需的概念和步骤，然后为作为思科网络威胁防御解决方案 1.1 版本组件的思科设备提供详细的配置与故障排除指南。

Flexible NetFlow 配置概述

在 Cisco IOS 设备上配置 Flexible NetFlow 包括 4 个步骤，具体如下：

- 配置流记录
- 配置流导出器
- 创建流监控器
- 将流监控器应用于一个或多个接口

配置流记录

流记录定义 NetFlow 进程将要收集的信息，例如流中的数据包数量和每条流收集的计数器的类型。自定义 NetFlow 记录指定一系列 match 和 collect 命令，这些命令告知思科设备要在传出 NetFlow 记录中包含哪些字段。思科网络威胁防御解决方案 1.1 定义每个受支持设备的特定流记录；思科强烈建议使用这些流记录获取尽可能最佳的部署结果。

match 字段是关键字段，表示其用于确定流的唯一性。*collect* 字段是记录中包含的额外信息，用于向收集器提供更多详细信息以进行报告和分析。

配置流导出器

流导出器定义 NetFlow 记录的发送位置和发送方式。流导出器的配置在网络威胁防御解决方案 1.1 中使用的所有思科 IOS 设备之间都相同。请注意，此配置可能与旧思科 IOS 和平台版本中的 NetFlow 配置不同。

创建流监控器

流监控器描述 NetFlow 缓存或该缓存中存储的信息。此外，流监控器还会链接流记录和流导出器。流监控器包括各种缓存特性，例如用于导出的计时器、缓存的大小以及数据包采样率（如果需要）。

由于网络流量会穿越思科设备，因此将持续创建和跟踪流。当流到期时，将其从 NetFlow 缓存导出到 StealthWatch FlowCollector。如果流在特定时间段处于非活动状态（例如，流未接收新数据包），或者如果流长期生存（活动）且持续时间超过活动计时器（例如，长时间 FTP 下载），则表明该流准备就绪进行导出。有些计时器用于确定流处于非活动状态还是长期生存。

注意 **最佳实践：**思科网络威胁防御解决方案 1.1 建议活动超时时间为 60 秒，非活动超时时间为 15 秒。

将流监控器应用于接口

在流监控器应用于接口之前，思科设备不生成任何 NetFlow 记录。当应用于接口时，流监控器会激活，并且仅为监控器应用于的接口生成 NetFlow 记录。

注意 **最佳实践：**思科网络威胁防御解决方案 1.1 建议将流监控器应用于所有需要流的安全可视性的接口。

Cisco Catalyst 3560-X 和 3750-X 系列

在 10GE 服务模块的 Cisco Catalyst 3560-X 和 3750-X (Cat3k-X) 系列交换机中支持 Flexible NetFlow。该服务模块以前在平台上不受支持，但是可以在穿越该模块的所有流量上启用硬件支持的线速 NetFlow。

能够在接入层生成 NetFlow 并获取流可视性是思科网络威胁防御解决方案 1.1 的一个关键组成部分。以前，NetFlow 提供的可视性仅在第 3 层边界可用，屏蔽 LAN 内的攻击。随着 NetFlow 如今在接入层可用，可以检测 LAN 中存在的可疑行为。

设计注意事项

仅在具有 10GE 服务模块的 Cisco Catalyst 3500-X 系列（3560-X 和 3750-X）平台上支持 Cisco Catalyst 3500 系列上的 NetFlow 服务。请注意，由服务模块启用 NetFlow 功能：仅为穿越该模块的流量生成 NetFlow 数据。因此，服务模块成为思科网络威胁防御解决方案 1.1 中至关重要的组件。

10GE 服务模块支持所谓的 “南-北” NetFlow，意味着它会为穿越交换机的流（例如，进入或离开中继端口的流）生成 NetFlow 记录。服务模块不支持 “东-西” NetFlow；这意味着不会为没有穿越服务模块的流量（例如，在本地交换的流量）生成 NetFlow。由于思科网络威胁防御解决方案 1.1 的目标之一是获取对本地交换的流量的可视性，因此请仔细考虑部署选项。

在服务模块上的硬件中支持 NetFlow。硬件能够在其常驻缓存中支持 32,000 条流。请注意，此数字在 Cisco Catalyst 3750-X 交换机堆栈中会进行调整。例如，具有四个服务模块的四台交换机组成的堆栈可以支持 128,000 条流。在服务模块上启用 NetFlow 时，交换机的性能没有降低。

启用服务模块

要正常运行，服务模块必须安装在支持硬件平台中，并且具有正确的思科 IOS 软件映像和许可证。表 16 列出在服务模块上启用 Flexible NetFlow 的最低要求。

表 16　Cisco Catalyst 3500-X 系列服务模块要求

组件	要求
最低硬件	版本 ID：02 修订版：0x03
思科 IOS 软件	15.0(1)SE3
许可证	IP Services

注意 服务模块具有自己的操作系统。要正常运作，服务模块上的操作系统必须与交换机自身上的操作系统匹配。

注意 以下操作步骤假设您符合硬件要求并已获取 IP Services 许可证和适当的思科 IOS 软件包。

操作步骤

步骤 1 安装服务模块并打开交换机。

步骤 2 将交换机升级到正确的软件映像。

```
3560X# archive download-sw /overwrite /reload image-name
```

步骤 3 安装 IP Services 许可证。

```
3560X# license install license-name
```

注意 交换机可能需要重新启动以激活许可证。

步骤 4 确保许可证处于活动状态。

```
3560X# show license detail
Index: 1        Feature: ipservices                     Version: 1.0
       License Type: Permanent
       License State: Active, In Use
       License Priority: Medium
       License Count: Non-Counted
       Store Index: 1
       Store Name: Primary License Storage
```

步骤 5 将服务模块升级到正确的软件映像。

```
3560X# archive download-sw service-module-image-name
```

步骤 6 确保服务模块正常运行。

```
3560X#show switch service-modules
Switch/Stack supports service module CPU version: 03.00.41
                           Temperature                                  CPU
Switch#  H/W Status        (CPU/FPGA)             CPU Link              Version
-------------------------------------------------------------------------------------------------------
 1       OK                67C/74C                connected             03.00.41
```

如果配置不正确，则会显示类似于以下的消息：

```
3560X#show switch service-modules
Switch/Stack supports service module CPU version: 03.00.41
                           Temperature                                  CPU
Switch#  H/W Status        (CPU/FPGA)             CPU Link              Version
-------------------------------------------------------------------------------------------------------
 1       LB-PASS-THRU *    71C/87C                notconnected          N/A
 *    Module services not supported on a Lanbase license
```

如果硬件状态处于 PASS-THRU 模式，则表明发生配置错误。错误消息提供有关错误原因的详细信息，即硬件、软件映像或许可证不符合要求。审核检查表和以上步骤以进行修复。

布线

10GE 服务模块有两个双速度 10 千兆以太网 SFP+ 端口。截至当前版本 (15.01)，这些端口不支持铜缆 1000BASE-T。将服务模块布线到铜缆网络中时，必须制定特殊注意事项。

注意 **最佳实践：**使用标准 10GbE 铜缆（要求聚合/核心交换机具有可用的 10GbE 端口）。

注意 **最佳实践：**将多模千兆以太网光纤 SFP (GLC-SX-MM) 与介质转换器配合使用。

Flexible NetFlow 配置

Cisco Catalyst 3500-X 系列交换机通常部署在接入层。本节介绍如何实施将 Cisco Catalyst 3500-X 系列的 Flexible NetFlow 功能充分用作接入层交换机所需的流可视性级别。

配置流记录

操作步骤

步骤 1 使用以下命令创建流记录：

```
3560X(config)#flow record CYBER_3KX_RECORD
3560X(config-flow-record)#match datalink mac source-address
3560X(config-flow-record)#match datalink mac destination-address
3560X(config-flow-record)#match ipv4 tos
3560X(config-flow-record)#match ipv4 ttl
3560X(config-flow-record)#match ipv4 protocol
3560X(config-flow-record)#match ipv4 source address
3560X(config-flow-record)#match ipv4 destination address
3560X(config-flow-record)#match transport source-port
3560X(config-flow-record)#match transport destination-port
3560X(config-flow-record)#collect interface input snmp
3560X(config-flow-record)#collect interface output snmp
3560X(config-flow-record)#collect counter bytes
3560X(config-flow-record)#collect counter packets
3560X(config-flow-record)#collect timestamp sys-uptime first
3560X(config-flow-record)#collect timestamp sys-uptime last
```

上述示例记录利用以下事实，即，作为接入层交换机，它可以唯一地标识最终用户设备和流量集。

数据链路源/目标 MAC 地址提供将流量接收/发送到交换机的用户设备的唯一标识符，以及有关可从该设备的组织唯一标识符 (OUI) 获取的设备供应商的信息。

输入/输出接口值报告流量进入/退出交换机所通过的物理接口的简单网络管理协议 (SNMP) 接口索引值。例如，对于下游流，输入接口值指服务模块上的端口，而输出接口值指下行链路端口。后者在与来自有线位置数据库的信息集成时，可用于跟踪用户设备的位置。

配置流导出器

流导出器描述 FlowCollector，包括目标 IP 地址和端口。

操作步骤

步骤 1 定义导出器。

```
3560X(config)#flow exporter CYBER_EXPORTER
```

步骤 2 （可选）添加描述。

```
3560X(config-flow-exporter)#description Lancope StealthWatch FlowCollector for the
Cisco Cyber Threat Defense Solution
```

步骤 3 定义源。

```
3560X(config-flow-exporter)#source <SVI Interface>
```

此设置是交换机发出 NetFlow 记录所在的 IP 地址。最佳实践是使用管理 VLAN 上的 IP 地址定义环回接口或 SVI 接口，并且使用该接口作为源。

步骤 4 定义目标 IP 地址。

```
3560X(config-flow-exporter)#destination <ip-address>
```

步骤 5 定义传输协议。

```
3560X(config-flow-exporter)#transport udp 2055
```

注意 **最佳实践：**NetFlow 通常通过 UDP 端口 2055 进行发送。

创建流监控器

流监控器表示设备的 NetFlow 数据库，并将流记录和流监控器链接在一起。

操作步骤

步骤 1 定义流监控器。

```
3560X(config)#flow monitor CYBER_MONITOR
```

步骤 2 （可选）添加描述。

```
3560X(config-flow-monitor)#description Main NetFlow Cache for the Cisco Cyber
Threat Defense Solution
```

步骤 3 配置流记录。

```
3560X(config-flow-monitor)#record CYBER_3KX_RECORD
```

步骤 4 配置导出器。

```
3560X(config-flow-monitor)#exporter CYBER_EXPORTER
```

步骤 5 定义活动超时时间。

活动超时时间是指为仍处于活动状态的流生成 NetFlow 记录的频率。思科建议使用的值为 60 秒。

```
3560X(config-flow-monitor)#cache timeout active 60
```

步骤 6 定义非活动超时时间。

非活动超时时间是指处于非活动状态（不传输数据）但仍常驻在缓存中的流因超时而在缓存中被清除的时间段。思科建议使用的值为 15 秒。

```
3560X(config-flow-monitor)#cache timeout inactive 15
```

将流监控器应用于接口

操作步骤

步骤 1 进入接口配置模式。

```
3560X(config)#interface range tenGigabitEthernet 1/1-2
```

步骤 2 对入口流量应用流监控器。

```
3560X(config-if-range)#ip flow monitor CYBER_MONITOR input
```

步骤 3 对出口流量应用流监控器。

```
3560X(config-if-range)#ip flow monitor CYBER_MONITOR output
```

验证

操作步骤

步骤 1 使用 show 命令验证配置。

```
3560X#show run flow [exporter|monitor|record]
```

验证 NetFlow 记录是否从设备导出并由 FlowCollector 接收。（在以下的 “Flexible NetFlow 导出验证” 一节中提供了详细信息。）

最终 Cisco Catalyst 3500-X 系列 NetFlow 配置

```
!
flow record CYBER_3KX_RECORD
 match datalink mac source-address
 match datalink mac destination-address match ipv4 tos
 match ipv4 ttl
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect interface input snmp
 collect interface output snmp
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
!
flow exporter CYBER_EXPORTER
 description Lancope StealthWatch FlowCollector for the Cisco Cyber Threat Defense
Solution
```

```
 destination <ip-address>
 source <SVI-interface>
 transport udp 2055
!
!
flow monitor CYBER_MONITOR
 description Main NetFlow Cache for the Cisco Cyber Threat Defense Solution
 record CYBER_3KX_RECORD
 exporter CYBER_EXPORTER
 cache timeout active 60
 cache timeout inactive 15
!
!
interface TenGigabitEthernet1/1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip flow monitor CYBER_MONITOR input
 ip flow monitor CYBER_MONITOR output
!
interface TenGigabitEthernet1/1/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip flow monitor CYBER_MONITOR input
 ip flow monitor CYBER_MONITOR output?
!
```

注意 有关详细信息，请参阅位于以下 URL 的《Cisco Catalyst 3K-X 服务模块》在访问过程中启用 Flexible NetFlow：
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps10745/white_paper_c11-691508_ps10744_Products_White_Paper.html

Cisco Catalyst 4500 系列 Supervisor Engine 7-E/7-LE

随着 Supervisor Engine 7-E 和 7-LE 的发行，向 Cisco Catalyst 4500 系列中引入了本机 Flexible NetFlow 支持；以前，Cisco Catalyst 4500 系列使用可选 NetFlow 服务卡支持 NetFlow。

模块化 Cisco Catalyst 4500 系列在接入层和汇聚层均存在，并在 IP-base 映像和许可证中包含 NetFlow 服务。

设计注意事项

思科网络威胁防御解决方案 1.1 建议将 Cisco Catalyst 4500 Supervisor 7-E/7-LE 部署为既是接入层交换机又是聚合层交换机。Supervisor 7-E 和 7-LE 支持一个跨所有流监控器共享的包含 128,000 个条目的硬件流表。虽然可以在流监控器中限制缓存条目数（使用流监控器配置中的 **cache entries** *numbers* 命令），但是本部署指南假设对整台交换机使用单个流监控器，并向思科网络威胁防御解决方案 1.1 分配完整的流缓存。

Cisco Catalyst 4500 系列不支持在单个流记录中同时选择第 2 层和第 3 层字段。这与解决方案中的其他接入层交换机不同（Cisco Catalyst 3500-X 系列）。

Flexible NetFlow 配置

如前所述，Supervisor 7-E 和 7-LE 支持范围广泛的 NetFlow 服务，并且在接入层和汇聚层均可有效使用。本节介绍用于在 Supervisor 7-E/7-LE 上实施建议级别的必要流可视性的操作步骤。

由于 Cisco Catalyst 4500 系列交换机可以同时充当接入层和聚合层交换机，因此可以为接入端口和中继端口定义不同的流记录和流监控器。但是，思科网络威胁防御解决方案 1.1 建议对二者使用相同的配置，以使配置尽可能简单，同时保留完整的功能。

配置流记录

操作步骤

步骤 1 使用以下命令创建流记录：

```
4500sup7e(config)#flow record CYBER_4K_RECORD
4500sup7e(config-flow-record)#match ipv4 tos
4500sup7e(config-flow-record)#match ipv4 protocol
4500sup7e(config-flow-record)#match ipv4 source address
4500sup7e(config-flow-record)#match ipv4 destination address
4500sup7e(config-flow-record)#match transport source-port
4500sup7e(config-flow-record)#match transport destination-port
4500sup7e(config-flow-record)#collect ipv4 dscp
4500sup7e(config-flow-record)#collect ipv4 ttl minimum
4500sup7e(config-flow-record)#collect ipv4 ttl maximum
4500sup7e(config-flow-record)#collect transport tcp flags
4500sup7e(config-flow-record)#collect interface output
4500sup7e(config-flow-record)#collect counter bytes
4500sup7e(config-flow-record)#collect counter packets
4500sup7e(config-flow-record)#collect timestamp sys-uptime first
4500sup7e(config-flow-record)#collect timestamp sys-uptime last
```

注意 Cisco Catalyst 4500 系列不允许在单个流记录中同时选择第 2 层和第 3 层字段。

配置流导出器

流导出器描述 FlowCollector，包括目标 IP 地址和端口。

操作步骤

步骤 1 定义导出器。

```
4500sup7e(config)#flow exporter CYBER_EXPORTER
```

步骤 2 （可选）添加描述。

```
4500sup7e(config-flow-exporter)#description Lancope StealthWatch FlowCollector for
Cisco Cyber Threat Defense Solution
```

步骤 3 定义源。

```
4500sup7e(config-flow-exporter)#source <SVI Interface>
```

此设置是交换机发出 NetFlow 记录所在的 IP 地址。最佳实践是使用管理 VLAN 上的 IP 地址定义环回接口或 SVI 接口，并且使用该接口作为源。

步骤 4 定义目标 IP 地址。

```
4500sup7e(config-flow-exporter)#destination <ip-address>
```

步骤 5 定义传输协议。

```
4500sup7e(config-flow-exporter)#transport udp 2055
```

注意 **最佳实践：**NetFlow 通常通过 UDP 端口 2055 进行发送。

创建流监控器

流监控器表示设备的 NetFlow 数据库，并将流记录和流监控器链接在一起。

操作步骤

步骤 1 定义流监控器。

```
4500sup7e(config)#flow monitor CYBER_MONITOR
```

步骤 2 （可选）添加描述。

```
4500sup7e(config-flow-monitor)#description Main NetFlow Cache for the Cisco Cyber
Threat Defense Solution
```

步骤 3 配置流记录。

```
4500sup7e(config-flow-monitor)#record CYBER_4K_RECORD
```

步骤 4 配置导出器。

```
4500sup7e(config-flow-monitor)#exporter CYBER_EXPORTER
```

步骤 5 定义活动超时时间。

活动超时时间是指为仍处于活动状态的流生成 NetFlow 记录的频率。思科建议使用的值为 60 秒。

```
4500sup7e(config-flow-monitor)#cache timeout active 60
```

步骤 6 定义非活动超时

非活动超时时间是指处于非活动状态（不传输数据）但仍常驻在缓存中的流因超时而在缓存中被清除的时间段。思科建议使用的值为 15 秒。

```
4500sup7e(config-flow-monitor)#cache timeout inactive 15
```

将流监控器应用于接口

操作步骤

步骤 1 进入接口配置模式。

```
4500sup7e(config)#interface GigabitEthernet 1/1
```

步骤 2 对第 2 层交换输入流量应用流监控器。

```
4500sup7e(config-if)#ip flow monitor CYBER_MONITOR layer2-switched input
```

验证

步骤 1 使用 show 命令检查配置。

```
4500sup7e#show run flow [exporter|monitor|record]
```

验证 NetFlow 记录是否从设备导出并由 FlowCollector 接收。（在以下的 “Flexible NetFlow 导出验证” 一节中提供了详细信息。）

最终 Cisco Catalyst 4500 系列 Supervisor 7-E/7-LE NetFlow 配置

```
!
flow record CYBER_4K_RECORD
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address match transport source-port
 match transport destination-port match interface input
 collect ipv4 dscp
 collect ipv4 ttl minimum collect ipv4 ttl maximum
 collect transport tcp flags collect interface output collect counter bytes collect
counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
!
flow exporter CYBER_EXPORTER
?description Lancope StealthWatch FlowCollector for the Cisco Cyber Threat Defense
Solution
 ?destination <ip-address>
 source <SVI-interface>
 transport udp 2055
!
!
flow monitor CYBER_MONITOR
 description Main NetFlow Cache for the Cisco Cyber Threat Defense Solution 1
 record CYBER_4K_RECORD
 exporter CYBER_EXPORTER
 cache timeout active 60
 cache timeout inactive 15
!
interface GigabitEthernet1/1
 ip flow monitor CYBER_MONITOR input
!
```

注意 有关详细信息，请参阅位于以下 URL 的《*Cisco Catalyst 4500 系列交换机软件配置指南，IOS-XE 3.1.0 版本 SG：配置 Flexible NetFlow*》：
http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/01xo/configuration/guide/fnf.html

Cisco Catalyst 6500 系列管理引擎 SUP2T

自从 Cisco Catalyst 6500 系列推出以来，NetFlow 服务便在平台上可用。Cisco Catalyst 6500 系列的管理引擎 SUP2T 的推出继续推进 NetFlow 服务，包括引入 Flexible NetFlow 支持和 NetFlow 功能集的完整硬件支持。

设计注意事项

Cisco Catalyst 6500 系列的管理引擎 SUP2T 支持单一系统以前所未有的级别收集 NetFlow 数据：可以将部署扩展为支持 1300 万个流条目。表 17 突出显示管理引擎 SUP2T 的改进的 NetFlow 功能集。

表 17　Cisco Catalyst 6500 系列交换机管理引擎 SUP2T NetFlow 支持

特性	管理引擎 SUP2T/SUP2TXL
NetFlow 表大小	512,000/1,000,000
NetFlow 哈希效率	99%
最大流条目数 (6513-E)	1300 万
出口 NetFlow	是
TCP 标志	是

注意 目前，仅 WS-X6908-10G-2T/2TXL、WS-X6816-10T-2T/2TXL、带有 DFC4/DFC4XL 的 WS-X6716-10G 和带有 DFC4/DFC4XL 的 WS-X6716-10T 线卡可以在基于管理引擎 2T 的系统中执行 NetFlow 记录导出。所有将来的 6500 系列模块都将支持此功能。

Flexible NetFlow 配置

本节介绍用于在管理引擎 SUP2T 上实施对于思科网络威胁防御解决方案 1.1 必要的推荐级别的流可视性的步骤。

由于 Cisco Catalyst 6500 系列交换机可以充当接入层、汇聚层或分发层交换机，因此可以为接入端口和中继端口定义不同的流记录和流监控器。但是，本指南建议对二者使用相同的配置，以保持配置尽可能简单，同时保留完整的功能。

配置流记录

操作步骤

步骤 1 使用以下关键字段和非关键字段创建流记录。

```
6500sup2T(config)#flow record CYBER_6K_RECORD
6500sup2T(config-flow-record)#match ipv4 tos
6500sup2T(config-flow-record)#match ipv4 protocol
6500sup2T(config-flow-record)#match ipv4 source address
6500sup2T(config-flow-record)#match ipv4 destination address
6500sup2T(config-flow-record)#match transport source-port
6500sup2T(config-flow-record)#match transport destination-port
6500sup2T(config-flow-record)#match interface input
6500sup2T(config-flow-record)#collect transport tcp flags
6500sup2T(config-flow-record)#collect interface output
6500sup2T(config-flow-record)#collect counter bytes
6500sup2T(config-flow-record)#collect counter packets
6500sup2T(config-flow-record)#collect timestamp sys-uptime first
6500sup2T(config-flow-record)#collect timestamp sys-uptime last
```

注意 管理引擎 SUP2T 支持收集 TCP 标志；但是，它不支持在 ipv4 报头中收集 TTL 字段。

配置流导出器

流导出器描述 FlowCollector，包括目标 IP 地址和端口。

操作步骤

步骤 1 定义导出器。

```
6500sup2T(config)#flow exporter CYBER_EXPORTER
```

步骤 2 （可选）添加描述。

```
6500sup2T(config-flow-exporter)#description Lancope StealthWatch FlowCollector for
the Cisco Cyber Threat Defense Solution
```

步骤 3 定义源。

```
6500sup2T(config-flow-exporter)#source <SVI-interface>
```

此设置是交换机发出 NetFlow 记录所在的 IP 地址。最佳实践是使用管理 VLAN 上的 IP 地址定义环回接口或 SVI 接口，并且使用该接口作为源。

步骤 4 定义目标 IP 地址。

```
6500sup2T(config-flow-exporter)#destination <ip-address>
```

步骤 5 定义传输协议。

```
6500sup2T(config-flow-exporter)#transport udp 2055
```

注意 **最佳实践：**NetFlow 通常通过 UDP 端口 2055 进行发送。

创建流监控器

流监控器表示设备的 NetFlow 数据库，并将流记录和流监控器链接在一起。

操作步骤

步骤 1 定义流监控器。

```
6500sup2T(config)#flow monitor CYBER_MONITOR
```

步骤 2 （可选）添加描述。

```
6500sup2T(config-flow-monitor)#description Main NetFlow Cache for the Cisco Cyber
Threat Defense Solution
```

步骤 3 配置流记录。

```
6500sup2T(config-flow-monitor)#record CYBER_6K_RECORD
```

步骤 4 配置导出器。

```
6500sup2T(config-flow-monitor)#exporter CYBER_EXPORTER
```

步骤 5 定义活动超时时间。

活动超时时间是指为仍处于活动状态的流生成 NetFlow 记录的频率。思科建议使用的值为 60 秒。

```
6500sup2T(config-flow-monitor)#cache timeout active 60
```

步骤 6 定义非活动超时时间。

非活动超时时间是指处于非活动状态（不传输数据）但仍常驻在缓存中的流超时退出缓存的时间段。思科建议使用的值为 15 秒。

```
6500sup2T(config-flow-monitor)#cache timeout inactive 15
```

将流监控器应用于接口

在 Cisco Catalyst 6500 系列交换机上，流监控器只能应用于路由（第 3 层）端口。但是，如果应用于路由端口，则仅为跨越第 3 层边界且不在 VLAN 内部的流量生成 NetFlow 记录。

要监控 VLAN 内部流量，必须在 VLAN 接口上应用流监控器。

操作步骤

步骤 1 进入 VLAN 接口配置模式。

```
6500sup2T(config)#interface vlan 100
```

步骤 2 对入口流量应用流监控器。

```
6500sup2T(config-if)#ip flow monitor CYBER_MONITOR input
```

步骤 3 对出口流量应用流监控器。

```
6500sup2T(config-if)#ip flow monitor CYBER_MONITOR output
```

验证

操作步骤

步骤 1 使用 show 命令检查配置。

```
6500sup2T#show run flow [exporter|monitor|record]
```

验证 NetFlow 记录是否从设备导出并由 FlowCollector 接收。（在以下的 “Flexible NetFlow 导出验证” 一节中提供了详细信息。）

最终 Cisco Catalyst 6500 系列 Supervisor 2T NetFlow 配置

```
!
flow record CYBER_6K_RECORD
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 collect transport tcp flags
 collect interface output collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
!
```

```
flow exporter CYBER_EXPORTER
 description Lancope StealthWatch FlowCollector for the Cisco Cyber Threat Defense
Solution
 destination <ip-address>
 source <SVI-interface>
 transport udp 2055
!
!
flow monitor CYBER_MONITOR
 description Main NetFlow Cache for the Cisco Cyber Threat Defense Solution
 record CYBER_6K_RECORD
 exporter CYBER_EXPORTER
 cache timeout active 60
 cache timeout inactive 15
!
!
interface Vlan 200
 ip flow monitor CYBER_MONITOR input
 ip flow monitor CYBER_MONITOR output
!
```

注意 有关详细信息，请参阅位于以下 URL 的《Cisco Catalyst 6500 管理引擎 SUP2T：NetFlow 增强功能》：
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-652021.html

第二代思科集成多业务路由器

Cisco ISR G2 路由器上的 Flexible NetFlow 支持遵守思科 IOS 软件指南中所记录的 NetFlow 的平台独立的实施。在 ISR 上，NetFlow 服务支持采用传统的 NetFlow 方法收集信息，以及为跨越第 3 层边界的流生成 NetFlow 记录。在提供对穿越不同网络区域的流的可视性方面，Cisco ISR 借此成为一个关键组件。

此外，ISR G2 还包含与 NetFlow 服务完全集成的软件支持的基于网络的应用识别 (NBAR)。如果启用，则 NBAR 可以对穿越接口的数据包执行深入的数据包检测，从而对生成流量的应用进行识别和分类（适用于受支持协议）。可以在 NetFlow 记录中导出流量集的应用分类。

设计注意事项

Cisco ISR G2 平台使用功能集的软件实施来支持 NetFlow 和 NBAR 服务。在部署软件支持的 NetFlow 服务时请注意，因为此功能会影响设备性能；例如，运行 Cisco IOS 软件的完全加载的 ISR 会因 NetFlow 支持而提升大约 15% 的 CPU 利用率。

在实施软件支持的 NetFlow 服务时，请参阅位于以下 URL 的 Cisco NetFlow 性能分析白皮书：
http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns562/ns583/net_implementation_white_paper0900aecd80308a66.pdf

Flexible NetFlow 配置

思科 ISR G2 平台通常部署为 VLAN 之间的第 3 层边界，并且往往位于分支网络的边缘。本节介绍用于实施建议级别的流可视性以充分使用思科 ISR G2 的 Flexible NetFlow 和 NBAR 功能的步骤。

配置流记录

操作步骤

步骤 1 使用以下关键字段和非关键字段创建流记录。

```
ISR(config)#flow record CYBER_ISR_RECORD
ISR(config-flow-record)#match ipv4 tos
ISR(config-flow-record)#match ipv4 protocol
ISR(config-flow-record)#match ipv4 source address
ISR(config-flow-record)#match ipv4 destination address
ISR(config-flow-record)#match transport source-port
ISR(config-flow-record)#match transport destination-port
ISR(config-flow-record)#match interface input
ISR(config-flow-record)#collect routing next-hop address ipv4
ISR(config-flow-record)#collect ipv4 dscp
ISR(config-flow-record)#collect ipv4 ttl minimum
ISR(config-flow-record)#collect ipv4 ttl maximum
ISR(config-flow-record)#collect transport tcp flags
ISR(config-flow-record)#collect interface output
ISR(config-flow-record)#collect counter bytes
ISR(config-flow-record)#collect counter packets
ISR(config-flow-record)#collect timestamp sys-uptime first
ISR(config-flow-record)#collect timestamp sys-uptime last
ISR(config-flow-record)#collect application name
```

上述流记录利用 NetFlow 版本 9 格式设置和 ISR 位置作为第 3 层边界，并收集许多在 NetFlow 的所有基于交换机的实施过程中都不可用的第 3 层和第 4 层字段，例如 Time To Live 字段、TCP 标志和下一跳地址。

ISR 是思科网络威胁防御解决方案 1.1 中唯一支持 NBAR 的设备。上述流记录允许使用 *collect application name 选项*收集创建流的应用的名称。

注意 在路由器上使用 NBAR 服务会影响路由器的性能。虽然应用名称的收集对于思科网络威胁防御解决方案 1.1 意义重大，但是必须谨慎启用 NBAR 服务。

配置流导出器

流导出器描述 FlowCollector，包括目标 IP 地址和端口。

操作步骤

步骤 1 定义导出器。

```
ISR(config)#flow exporter CYBER_EXPORTER
```

步骤 2 （可选）添加描述。

```
ISR(config-flow-exporter)#description Lancope StealthWatch FlowCollector for the
Cisco Cyber Threat Defense Solution
```

步骤 3 定义源。

```
ISR(config-flow-exporter)#source loopback 1
```

此设置是交换机发出 NetFlow 记录所在的 IP 地址。最佳实践是使用管理 VLAN 上的 IP 地址定义环回接口，并且使用该接口作为源。

步骤 4 定义目标 IP 地址。

```
ISR(config-flow-exporter)#destination <ip-address>
```

步骤 5 定义传输协议。

```
ISR(config-flow-exporter)#transport udp 2055
```

注意 **最佳实践：**NetFlow 通常通过 UDP 端口 2055 进行发送。

创建流监控器

流监控器表示设备的 NetFlow 数据库，并将流记录和流监控器链接在一起。

操作步骤

步骤 1 定义流监控器。

```
ISR(config)#flow monitor CYBER_MONITOR
```

步骤 2 （可选）添加描述。

```
ISR(config-flow-monitor)#description Main NetFlow Cache for the Cisco Cyber Threat
Defense Solution
```

步骤 3 配置流记录。

```
ISR(config-flow-monitor)#record CYBER_ISR_RECORD
```

步骤 4 配置导出器。

```
ISR(config-flow-monitor)#exporter CYBER_EXPORTER
```

步骤 5 定义活动超时时间。

活动超时时间是指为仍处于活动状态的流生成 NetFlow 记录的频率。思科建议使用的值为 60 秒。

```
ISR(config-flow-monitor)#cache timeout active 60
```

步骤 6 定义非活动超时时间。

非活动超时时间是指处于非活动状态（不传输数据）但仍常驻在缓存中的流因超时而在缓存中被清除的时间段。思科建议使用的值为 15 秒。

```
ISR(config-flow-monitor)#cache timeout inactive 15
```

将流监控器应用于接口

应将流监控器应用于所有路由接口和子接口。

操作步骤

步骤 1 进入接口配置模式。

```
ISR(config)#interface GigabitEthernet 0/0
```

步骤 2 对入口流量应用流监控器。

```
ISR(config-if)#ip flow monitor CYBER_MONITOR input
```

验证

操作步骤

步骤 1 使用 show 命令检查配置。

```
ISR#show run flow [exporter|monitor|record]
```

验证 NetFlow 记录是否从设备导出并由 FlowCollector 接收。（在以下的 “Flexible NetFlow 导出验证” 一节中提供了详细信息。）

最终配置

```
!
flow record CYBER_ISR_RECORD
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 ttl minimum
 collect ipv4 ttl maximum
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect application name
!
!
flow exporter CYBER_EXPORTER
 description Lancope StealthWatch FlowCollector for the Cisco Cyber Threat Defense
Solution
 destination <ip-address>
 source loopback 1
 transport udp 2055
!
!
```

```
flow monitor CYBER_MONITOR
 description Main NetFlow Cache for the Cisco Cyber Threat Defense Solution
 record CYBER_ISR_RECORD
 exporter CYBER_EXPORTER
 cache timeout active 60
 cache timeout inactive 15
!
!
interface GigabitEthernet0/0
 ip address <ip-address> <net-mask>
 ip flow monitor CYBER_MONITOR input
!
```

注意 有关详细信息，请参阅位于以下 URL 的《*NetFlow 配置指南，思科 IOS 软件版本 15.2 M&T*》：http://www.cisco.com/en/US/partner/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book.html

思科 ASR 1000 系列

思科 ASR 1000 系列路由器上的 Flexible NetFlow 支持遵守思科 IOS 指南中所记录的 NetFlow 的独立于平台的实施。ASR 上的 NetFlow 支持采用传统的 NetFlow 方法收集信息，以及为跨越第 3 层边界的流生成 NetFlow 记录。在提供对穿越不同网络区域的流的可视性方面，ASR 借此成为一个关键组件。

设计注意事项

思科 ASR 1000 包含与 NetFlow 服务完全集成的软件支持的 NBAR。如果启用，则 NBAR 可以对穿越接口的数据包执行深入的数据包检测，从而对生成流量的应用进行识别和分类（适用于受支持协议）。可以在 NetFlow 记录中导出流量集的应用分类。

由于 NetFlow 和 NBAR 作为软件服务在 ASR 1000 系列上实现，因此在部署这些功能时应注意，因为它们对设备性能造成影响。

配置 NetFlow 导出

配置流记录

流记录配置定义为每条流收集哪些数据字段。

操作步骤

步骤 1 使用以下关键字段和非关键字段创建流记录。

```
ASR(config)#flow record CYBER_ASR_RECORD
ASR(config-flow-record)#match ipv4 tos
ASR(config-flow-record)#match ipv4 protocol
ASR(config-flow-record)#match ipv4 source address
ASR(config-flow-record)#match ipv4 destination address
ASR(config-flow-record)#match transport source-port
ASR(config-flow-record)#match transport destination-port
ASR(config-flow-record)#match interface input
ASR(config-flow-record)#collect routing next-hop address ipv4
ASR(config-flow-record)#collect ipv4 dscp
ASR(config-flow-record)#collect ipv4 ttl minimum
```

```
ASR(config-flow-record)#collect ipv4 ttl maximum
ASR(config-flow-record)#collect transport tcp flags
ASR(config-flow-record)#collect interface output
ASR(config-flow-record)#collect counter bytes
ASR(config-flow-record)#collect counter packets
ASR(config-flow-record)#collect timestamp sys-uptime first
ASR(config-flow-record)#collect timestamp sys-uptime last
ASR(config-flow-record)#collect application name
```

通过利用 NetFlow 版本 9 格式设置和 ASR 的角色作为第 3 层边界，可以收集许多并非始终在 NetFlow 的基于交换机的实施过程中可用的第 3 层和第 4 层字段，例如生存时间值、TCP 标志和下一跳地址。

请注意，上述流记录能够使用 *collect application name* 选项从 NBAR 收集应用的名称。如果未运行 NBAR，则可以省略该行。

注意 NBAR 服务能够影响路由器的性能；虽然应用名称的收集对于思科网络威胁防御解决方案意义重大，但是必须谨慎启用 NBAR 服务。

配置流导出器

流导出器配置定义流记录的发送位置 (FlowCollector)，包括目标 IP 地址和端口。

操作步骤

步骤 1 定义导出器。

```
ASR(config)#flow exporter CYBER_EXPORTER
```

步骤 2 （可选）添加描述。

```
ASR(config-flow-exporter)#description Lancope StealthWatch FlowCollector for the
Cisco Cyber Threat Defense Solution
```

步骤 3 定义源。

```
ASR(config-flow-exporter)#source Loopback 1
```

此设置是交换机将用作 NetFlow 导出记录的源的 IP 地址。最佳实践是使用管理 VLAN 上的 IP 地址定义环回接口（所示示例中的 Loopback 1），并且使用该接口作为源。请注意，必须先配置环回接口，然后才能将其用作流导出源。

步骤 4 定义目标 IP 地址。

```
ASR(config-flow-exporter)#destination ip-address-of-FlowCollector
```

步骤 5 定义传输协议。

```
ASR(config-flow-exporter)#transport udp 2055
```

注意 **最佳实践：**NetFlow 通常通过 UDP 端口 2055 进行发送。

创建流监控器

流监控器表示设备的内存常驻 NetFlow 数据库，并且将流记录和流导出器配置链接在一起。

操作步骤

步骤 1 定义流监控器。

```
ASR(config)#flow monitor CYBER_MONITOR
```

步骤 2 （可选）添加描述。

```
ASR(config-flow-monitor)#description Main NetFlow Cache for the Cisco Cyber Threat
Defense Solution
```

步骤 3 配置流记录。

```
ASR(config-flow-monitor)#record CYBER_ASR_RECORD
```

步骤 4 配置导出器。

```
ASR(config-flow-monitor)#exporter CYBER_EXPORTER
```

步骤 5 定义活动超时时间。

活动超时时间是指为仍处于活动状态的流生成 NetFlow 记录的频率。建议使用的值为 60 秒。

```
ASR(config-flow-monitor)#cache timeout active 60
```

步骤 6 定义非活动超时时间。

非活动超时时间是指处于非活动状态（不传输数据）但仍常驻在缓存中的流超时退出缓存的时间段。思科建议使用的值为 15 秒。

```
ASR(config-flow-monitor)#cache timeout inactive 15
```

将流监控器应用于接口

应将流监控器应用于所有路由接口和子接口。

操作步骤

步骤 1 进入接口配置模式。

```
ASR(config)#interface GigabitEthernet 0/0/0
```

步骤 2 对入口流量应用流监控器。

```
ASR(config-if)#ip flow monitor CYBER_MONITOR input
```

验证

操作步骤

步骤 1 使用 show 命令检查配置。

```
ASR#show run flow [exporter|monitor|record]
```

步骤 2 验证 NetFlow 记录是否从设备导出并由 FlowCollector 接收。（有关详细信息，请参阅《设计和实施指南》。）

最终配置

```
!
flow record CYBER_ASR_RECORD
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 ttl minimum
 collect ipv4 ttl maximum
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect application name
!
!
flow exporter CYBER_EXPORTER
?description Lancope StealthWatch FlowCollector for the Cisco Cyber Threat Defense
Solution
?destination <ip-address>
 source loopback 1
 transport udp 2055
!
!
flow monitor CYBER_MONITOR
description Main NetFlow Cache for the Cisco Cyber Threat Defense Solution
 record CYBER_ASR_RECORD
 exporter CYBER_EXPORTER
 cache timeout active 60
?cache timeout inactive 15
!
!
interface GigabitEthernet0/0/0
 ip address <ip-address> <net-mask>
 ip flow monitor CYBER_MONITOR input
!
```

注意 有关详细信息，请参阅位于以下 URL 的《NetFlow 配置指南，思科 IOS XE 版本 3S (ASR 1000)》：http://www.cisco.com/en/US/docs/ios-xml/ios/netflow/configuration/xe-3s/asr1000/nf-xe-3s-asr1000-book.pdf

Cisco NetFlow Generation 设备

在大型数据中心内，高速生成 NetFlow 可能困难重重。Cisco NetFlow Generation 设备 (NGA) 是专用于在千兆级数据中心内提供流可视性的高性能解决方案，可以作为思科网络威胁防御解决方案的一部分，通过可扩展且价格合理的方式恢复这些环境中的流可视性。

设计注意事项

思科 NGA 具有四个 10G 监控接口和最多四个独立的流缓存和流监控器。这意味着思科 NGA 最多可以接收 40 千兆 数据，并且支持数据端口、记录模板和导出参数的各种组合。将 NGA 放在数据中心内时，务必对此加以考虑。

NGA 可用于从物理接入层、汇聚层和核心层接收数据， 目标是确保数据中心内所有流量以及离开数据中心的流量的完整可视性。虚拟环境内的流量（虚拟机间流量）可以通过 StealthWatch FlowSensor VE 进行监控，而进入和离开数据中心的流量则可以通过 ASA 或其他类似的边缘设备进行监控。并提供更多有关数据中心出站流量的统计信息。思科 NGA 具有极强的可扩展性，能够支持最多 6400 万条活动流。有关安装的更多详细信息，请参阅《*Cisco NetFlow Generation 设备 3140 快速入门指南*》。

注意 **最佳实践：**NGA 监控接口应放在堵塞点，以确保提供对数据中心内部流量的完整可视性。

在 NGA 上配置 NetFlow 时，请记住有关受支持设备的以下限制：

- 最多 10 个过滤器 - 这些过滤器定义哪些流将发送到特定收集器。这样做可以使用收集器的分析应用并且跨收集器对 NetFlow 数据进行负载均衡。
- 最多 4 个受管设备 - 如前所述，通过受管设备设置可以从流量源收集接口信息。
- 最多 6 个收集器 - NetFlow 导出最多支持 6 个不同的 NetFlow 收集器，以便您可以对 NetFlow 数据导出进行负载均衡，并监控数据中心内的特定应用。
- 最多 4 个监控器 - 最多可以有 4 个独立流监控器（流缓存）同时处于活动状态。每个监控器支持最多三条记录。在这三条记录中，仅支持 IPv4、IPv6 和第 2 层记录类型分别只能有一个。

Flexible NetFlow 配置

当 Cisco NGA 已完成部署并开始接收网络流量副本后（有关详细信息，请参阅《思科网络威胁防御解决方案 1.1 方法指南：*使用 Cisco NetFlow Generation 设备获得数据中心可视性*》），下一步必须配置 Flexible NetFlow 导出。可以通过网络界面或直接从 CLI 在思科 NGA 上配置 Flexible NetFlow；介绍使用思科 NGA 网络界面进行验证配置的方法。

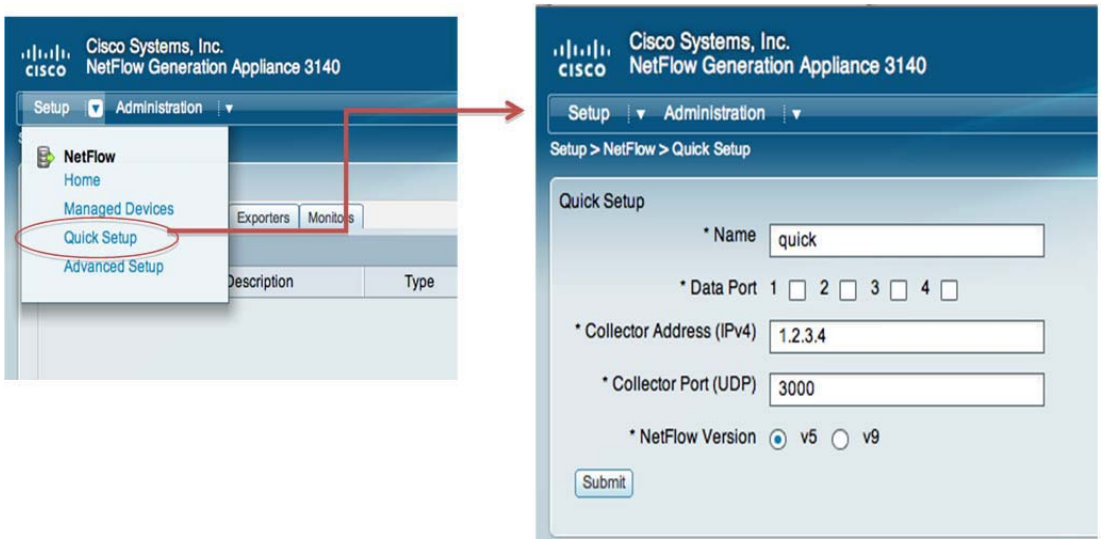
执行快速设置 NetFlow 配置

这是用于将 v5 或 v9 NetFlow 数据包导出到收集器的最轻松最简单的配置。

操作步骤

步骤 1 点击 **Setup > Quick Setup**，如图 10 中所示。

图 10　　快速设置



步骤 2 定义名称。

输入唯一名称以标识此配置。

步骤 3 定义一个或多个数据端口。

确定要接收传入数据包的各个设备数据端口，选中相应的复选框。

步骤 4 定义收集器地址。

在 Collector Address 字段中输入收集器的 IP 地址。

步骤 5 定义 UDP 收集器端口。

输入收集器设备正在监听的端口。通常，这在收集器设备上是可配置项。StealthWatch 默认 NetFlow 在 UDP 端口 2055 上进行监听。

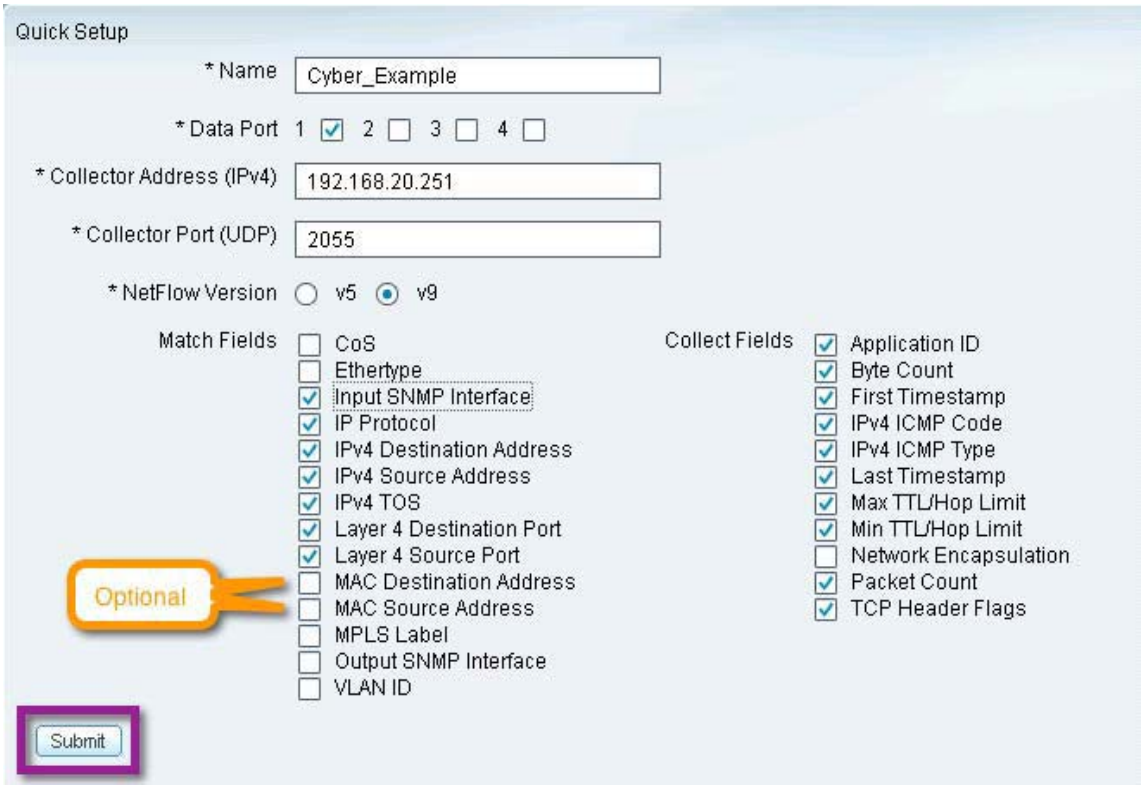
步骤 6 定义 NetFlow 版本。

选择版本 5 以将设备配置为执行标准 NetFlow 版本 5 监控和导出。无需选择单个记录字段，因为 NetFlow 版本 5 标准已预先确定这些字段。

选择要在监控/收集中包含哪些版本 9 字段。

注意 **最佳实践：**使用版本 9 并选择字段，如图 11 中所示。

图 11　　快速设置窗口



注意　根据受管设备设置是否已配置，MAC 字段可选。如果受管设备设置已配置，则应选择 MAC 字段；如果受管设备设置未配置，则不应选择 MAC 字段。

步骤 7　点击 **Submit**。系统将创建以下组件：

- 对于 V5：
  - 名为 *Cyber_Example_collector* 的收集器
  - 名为 *Cyber_Example_exporter* 的导出器
  - 名为 *Cyber_Example _monitor* 的监控器
- 对于 V9：
  - 名为 *Cyber_Example_collector* 的收集器
  - 名为 *Cyber_Example_exporter* 的导出器
  - 名为 *Cyber_Example_monitor* 的监控器
  - 名为 *Cyber_Example_record* 的记录

步骤 8　选择 Monitor 选项卡中的 **Cyber_Example_monitor**，然后点击 **Activate/Inactivate**。

这使新创建的流监控器能够为输入流量生成 NetFlow 信息并将其发送到 StealthWatch FlowCollector。

有关创建过滤器，设置多个收集器、记录、导出器和监控器的高级信息，请参阅“ *设置多个 NetFlow 监控器实例*”一节下的 《*Cisco NetFlow Generation 设备 (NGA) 3140 用户指南*》。

思科 ASA 5500 系列自适应安全设备

关于 NetFlow 安全事件日志记录

NetFlow 的思科 ASA 实施称为 NetFlow 安全事件日志记录 (NSEL)。NSEL 首先在思科 ASA 软件版本 8.2(1) 中引入，与标准系统日志记录所提供的相比，可以通过更高效且扩展性更强的方式从安全设备导出特定、大量、与流量相关的事件。

NSEL 在 NetFlow v9 协议基础上构建；但是，NetFlow v9 记录中的字段的使用方式与在标准 NetFlow 报告中不同。

标准 NetFlow 和 NSEL 之间的主要区别在于，NSEL 是一种状态流跟踪机制，仅导出那些在 IP 流中指示重大事件的记录。NSEL 事件用于导出有关流状态的数据，并且由导致状态更改的事件触发，而不是由如同标准 NetFlow 的活动计时器触发。ASA 当前对三种事件类型进行报告：

- 流创建
- 流拆解
- 流被拒绝

此外，还应注意 NSEL 和标准 NetFlow 版本 9 实施之间的一些其他差异。

- NSEL 是双向的。通过思科 IOS 设备进行的连接会生成两条流，每个方向一条，而 NSEL 每个连接发送单条流。
- NSEL 报告双向流的总字节计数，而不是每个方向的字节计数。
- NSEL 不报告数据包计数。
- NSEL 已为三种事件类型预定义模板。这些模板通常在所有 NSEL 数据记录之前导出。

在基于接口的策略中不支持 NSEL 流导出操作；只能在全局服务策略中应用这些操作。

NSEL 提供独特优势，并且，如果 NSEL 记录和数据相应地进行了处理，则可以提供对通过网络边缘的流量的更好的洞察和可视性。作为思科网络威胁防御解决方案的组件，Lancope StealthWatch System 了解并利用特有字段来提供可视性和情景，从而协助安全分析师检测网络威胁。

注意 **最佳实践：**为将 ASA 数据的优势最大化，建议使用其他设备将相同的流数据从传统 NetFlow 导出到 StealthWatch，以填写缺失的超时、数据包和字节计数数据。这确保完整的流可视性，同时维持通过 NSEL 提供的独特情景优势。

配置 NSEL

使用模块化策略框架 (MPF) 在 ASA 设备上配置 NSEL。对所有流启用 NSEL 的最简单方法是将其配置为全局策略的一部分，如以下操作步骤中所述。

配置 NSEL 收集器

操作步骤

步骤 1 配置 NSEL 收集器。

此步骤定义将由 ASA 将 NetFlow 记录发送到的 NetFlow 收集器。

```
ASA(config)# flow-export destination interface-name collector-ip-address port
```

其中 *interface-name* 是指 ASA 设备上的可以到达收集器（位于 *collector-ip-address* 和 *port*）的接口。例如：

```
ASA(config)# flow-export destination inside 192.168.200.25 2055
```

在全局策略中配置 NSEL

操作步骤

步骤 1 输入 global_policy 配置。

```
ASA(config)# policy-map global_policy
```

步骤 2 输入 class-default 配置。

```
ASA(config-pmap)# class class-default
```

步骤 3 定义所有流量的流输出操作。

```
ASA(config-pmap-c)# flow-export event-type all destination collector-ip-address
```

其中 collector-ip-address 是提供给先前创建的收集器的同一 IP 地址。

（可选）调整模板超时间隔

操作步骤

步骤 1 修改模板记录的发送间隔。

```
ASA(config)# flow-export template timeout-rate 2
```

注意 **最佳实践：**使用间隔速率 2 分钟，如此处所示。

（可选）禁用冗余系统日志消息

由于 NSEL 的目的是创建更高性能的记录基于流的事件的方法，因此启用 NSEL 会创建若干冗余系统日志消息。在高性能部署中，禁用这些冗余消息有益。

操作步骤

步骤 1 禁用冗余系统日志消息。

```
ASA(config)# logging flow-export-syslogs disable
```

步骤 2 显示冗余系统日志消息的状态。

```
ASA# show logging flow-export-syslogs
```

验证

操作步骤

步骤 1 使用 **show** 命令验证配置。

步骤 2 检查运行时计数器以查看 NSEL 统计数据和错误数据。

```
ASA# show flow-export counters
destination: management 192.168.200.25 2055
  Statistics:
    packets sent                                        2896
  Errors:
    block allocation failure                               0
    invalid interface                                      0
    template send failure                                  0
    no route to collector                                  0
```

如果配置正确，则命令的输出应显示：

- 将是 StealthWatch FlowCollector 的 IP 地址的目标
- 发送的大于零的数据包数量（假设流正在穿越设备）
- 零个错误

步骤 3 验证 ASA 是否位于 SMC 中 StealthWatch FlowCollector 的导出器树中。

步骤 4 通过右键单击 ASA，然后选择 **Flows > Flow Table** 来打开流表。

最终配置

```
!
flow-export destination management <ip-address> 2055
!
policy-map global_policy
 class class-default
  flow-export event-type all destination <ip-address>
!
flow-export template timeout-rate 2
logging flow-export syslogs disable
!
```

注意 有关更多详细信息，请参阅《*配置网络安全事件系统日志*》(http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/monitor_nsel.html) 和《适用于 NetFlow 收集器的思科 ASA 5500 系列实施指南，版本 8.4、8.5 和 8.6》(http://www.cisco.com/en/US/docs/security/asa/asa84/system/netflow/netflow.html)

Flexible NetFlow 导出验证

当在解决方案中的每台设备上配置了 NetFlow 时，有必要验证流监控器是否正常运行并且是将 NetFlow 记录导出到 StealthWatch FlowCollector。在前面各节中，设备配置有 Flexible NetFlow，并且配置经过验证与思科网络威胁防御解决方案 1.1 建议的 Flexible NetFlow 配置一致。使用以下操作步骤验证 NetFlow 配置是否正常运行。

在基于思科 IOS 软件的设备上验证 NetFlow 导出

操作步骤

步骤 1 显示缓存中存在的流记录。

```
Cisco-IOS#show flow monitor CYBER_MONITOR cache
```

此命令显示当前在 CYBER_MONITOR 的内存中的所有流记录。假设流正在通过已配置的接口，则应该显示记录。否则，请确保流监控器按正确的方向应用于正确的接口，并且该接口上存在流量。

步骤 2 显示流监控器的历史统计信息。

```
Cisco-IOS#show flow monitor CYBER_MONITOR statistics
  Cache type:                               Normal
  Cache size:                                  128
  Current entries:                               0
  High Watermark:                                0

  Flows added:                                   0
  Flows aged:                                    0
    - Active timeout      (   60 secs)           0
    - Inactive timeout    (   15 secs)           0
    - Event aged                                 0
    - Watermark aged                             0
    - Emergency aged                             0

  Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                              19

  Flows added:                                   0
  Flows aged:                               171593
    - Active timeout      (   60 secs)       171593
```

此命令显示 CYBER_MONITOR 的历史统计信息，包括当前在缓存中的流的数量和缓存中因过期而已清除的流的数量。此处还可验证缓存大小以及活动和非活动超时时间的长短。

步骤 3 确保流记录是从设备导出。

```
Cisco-IOS#show flow exporter CYBER_EXPORTER statistics
Flow Exporter CYBER_EXPORTER:
   Packet send statistics (last cleared 8w4d ago):
     Successfully sent:         702414                 (147362340 bytes)

Client send statistics:
   Client: Flow Monitor EXAMPLE_MONITOR
     Records added:             0
       - sent:                  1404828
     Bytes added:               0
       - sent:                  147362340
```

此命令显示从流导出器导出的数据包和字节的历史计数。发送的数据包数量（和发送的记录数）应大于零并在增加。否则，请确保将流导出器适当应用于流监控器。

注意 NetFlow 允许在单个数据包中发送多条流记录，因此上述输出中的记录计数和数据包计数可能不同。

在思科 ASA 设备上验证 NetFlow 导出

操作步骤

步骤 1 检查运行时计数器以查看 NSEL 统计数据和错误数据。

```
ASA# show flow-export counters
destination: management 192.168.200.25 2055
  Statistics:
    packets sent                                        2896
  Errors:
    block allocation failure                               0
    invalid interface                                      0
    template send failure                                  0
    no route to collector                                  0
```

如果配置正确，则命令的输出应显示：

- 将是 StealthWatch FlowCollector 的 IP 地址的目标
- 发送的将大于零的数据包数量（假设流正在穿越设备）
- 零个错误

验证 NetFlow 记录是否由 FlowCollector 接收

确保配置正常运行的最终步骤是确保每个导出器的流记录由 FlowCollector 接收。

注意 此操作步骤假设以前的步骤成功，并且 NetFlow 是从 NetFlow 生成设备导出。

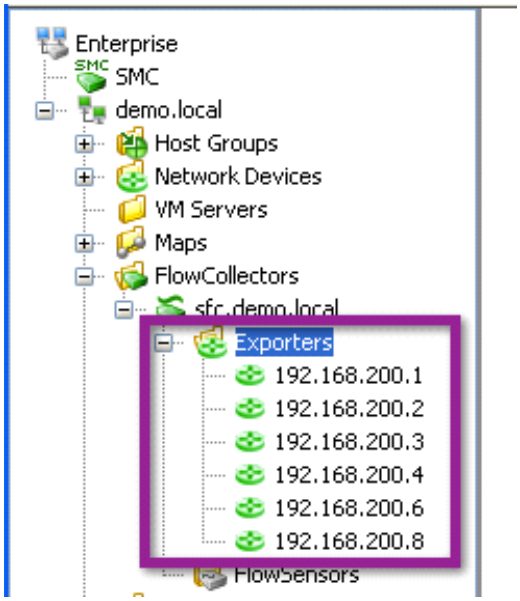
操作步骤

步骤 1 登录 SMC 控制台。

步骤 2 展开 Enterprise 树中的 FlowCollector。

步骤 3 验证已配置的流导出器是否显示在展开的树中，如图 12 中所示。

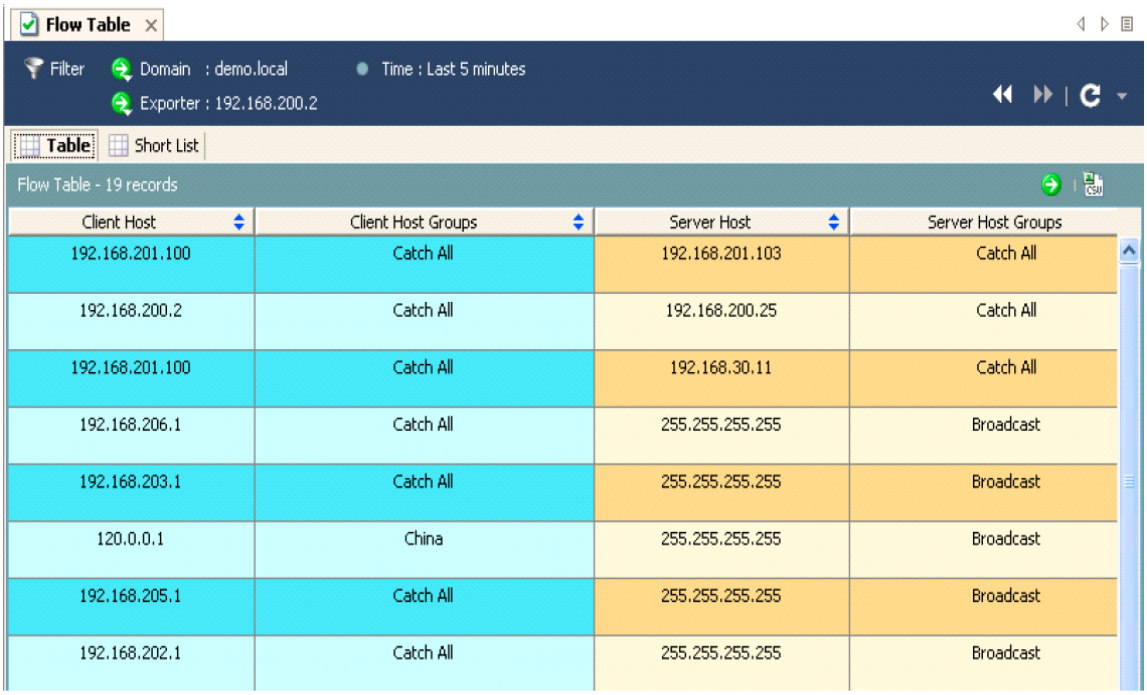
图 12　展开的树



步骤 4　右键单击流导出器，然后点击 **Flows > Flow Table**。

步骤 5　确保表中显示的是（预期）流记录，如图 13 中所示。

图 13　流表



将 NetFlow 分析与身份、设备分析和用户服务集成

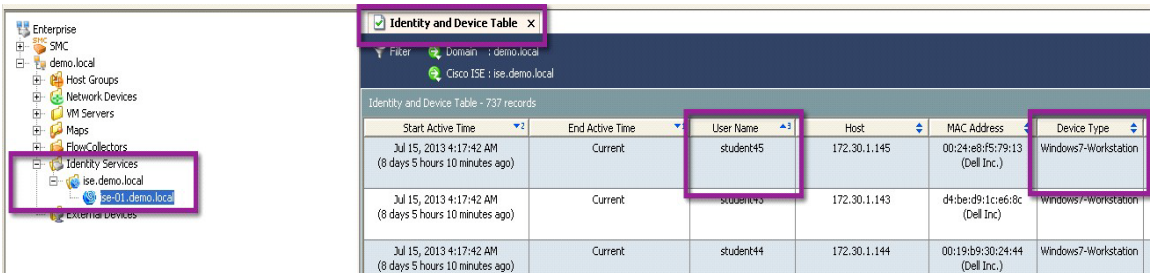
概述

思科网络威胁防御解决方案 1.1 专门用于与 Cisco TrustSec 解决方案一起协调运行，意味着两种解决方案可以同时部署，并且共同为管理员提供对其网络的增强可视性与可控性。

注意 假设读者熟悉 Cisco TrustSec 解决方案 2.0 或更高版本并已将其至少部署为监控器模式或进行更好的部署。有关 TrustSec 的详细信息，请参阅以下 URL：http://www.cisco.com/go/trustsec

通过在 Lancope StealthWatch Management Console (SMC) 和思科身份服务引擎 (ISE) 之间进行集成，管理员可以从 SMC 控制台中快速将用户和设备身份与一条流或一组流关联。图 14 显示此增强功能，其中用户名、设备类型和所有其他会话信息连同所有具有 IP 地址的关联流都可用。本节介绍将 Lancope SMC 与 Cisco TrustSec 解决方案或思科 ISE 部署集成以增强思科网络威胁防御解决方案的功能的过程。

图 14　　身份和设备表



将 Lancope SMC 与思科身份服务引擎集成

StealthWatch 6.3 使用具象状态传输 (REST) API 从思科 ISE 监控 (MNT) 节点收集身份信息。REST API 通过安全并已进行身份验证的 HTTPS 会话来传递。

验证身份服务引擎监控节点部署

要在思科 ISE 节点上成功调用 API 调用，必须将该节点部署为有效的 MNT 节点。可以通过检查 ISE 控制面板中的 ISE 部署配置来验证此部署。

操作步骤

步骤 1 登录思科 ISE 控制面板。

步骤 2 转至 **Administration > System > Deployment**。

系统将显示 Deployment Nodes 页面，其中列出所部署的所有已配置的节点。

步骤 3 在 Deployment Nodes 页面的 Role(s) 列中，验证要监控的目标节点的角色是否将该节点的类型显示为思科监控 ISE 节点，如图 15 中所示。（注：Standalone 角色包含 MNT 功能。）

图 15 Deployment Nodes 屏幕

在 ISE 上创建管理员用户以监控访问

注意 **最佳实践：**对于思科网络威胁防御解决方案和所有利用 ISE REST API 的部署，建议的做法是在 ISE 上创建单独的用户帐户以验证 API 使用。

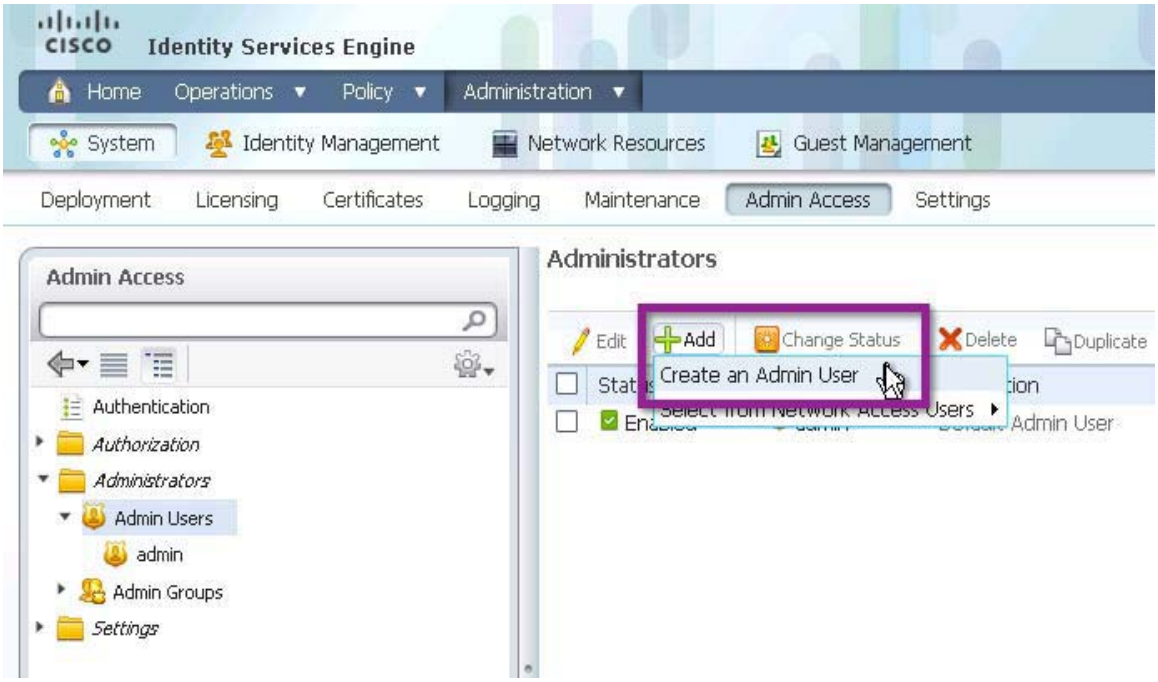
操作步骤

步骤 1 登录 ISE 控制面板。

步骤 2 转至 **Administration > System > Admin Access > Administrators**。

步骤 3 选择 **Admin Users**。点击 **Add**，然后选择 **Create an Admin User**，如图 16 中所示。

图 16　创建管理员用户



步骤 4　填写 Admin User、Password、User Information、Account Options 和 Admin Groups 部分（请参阅表 18）。

表 18　管理员用户信息

配置项	设置
Admin User	使用易于区分的内容对管理员用户进行命名。 确保帐户状态设置为 Enabled。
Password	创建用户的密码。
User Information	可选：添加用于描述用户的信息。
Account Options	可选：添加有意义的描述，例如： *Account used the StealthWatch Management Console to access ISE Session information for the Cisco Cyber Threat Defense Solution*。
Admin Groups	将用户放在预定义的 *Helpdesk Admin 组中*。

步骤 5　点击 Submit。

确保 ISE 中有活动会话

操作步骤

步骤 1 登录 ISE 控制面板。

步骤 2 点击 **Operations > Authentications**。

步骤 3 确保 Live Authentications 表不为空。

使用网络浏览器验证 ISE API

思科 ISE 和 Lancope SMC 之间的集成利用 Cisco ISE 所支持的两个 API 调用：

- Authenticated Sessions List - 检索所有当前活动的已进行身份验证的会话的列表。
- Endpoint by IP Address - 按 IP 地址检索主机的已进行身份验证的会话信息。

在继续集成之前，思科建议使用网络浏览器验证 Admin 凭证和 API 操作。

操作步骤

步骤 1 打开网络浏览器（建议使用 Mozilla Firefox）。

步骤 2 使用以下 URL 调用 *AuthList* API：

https://ise.demo.local/ise/mnt/api/Session/AuthList/null/null

注意 在此示例中，*ise.demo.local* 是 ISE 节点的 DNS 名称。请替换为您的环境中 ISE MNT 节点的正确 DNS 名称或 IP 地址。

步骤 3 使用操作步骤 2 中的监控凭证登录。

步骤 4 验证是否显示了身份验证列表。

注意 如果在 ISE 中未保留任何活动的已进行身份验证的会话，则身份验证列表为空。如果未从 API 返回任何会话，请转至 ISE 控制面板以验证是否存在活动会话。

步骤 5 使用 ISE 中活动会话内的 IP 地址，在以下 URL 调用 *Endpoint by IP Address API*：

https://ise.demo.local/ise/mnt/api/Session/EndPointIPAddress/<ip-address>

步骤 6 使用操作步骤 2 中的监控凭证登录。

步骤 7 验证是否检索到身份验证会话信息。

配置证书颁发机构证书

必须将 SMC 配置为信任颁发思科 ISE 的身份证书的证书颁发机构。如果在 StealthWatch System 的部署中跟随最佳实践，则表明此操作步骤已经完成，否则，必须获取证书颁发机构的证书并将其安装在 SMC 上。

操作步骤

步骤 1 登录 SMC（管理）网络界面。

步骤 2 从主页中点击 **Configuration > Certificate Authority Certificates**。

步骤 3 点击 **Choose File**，然后浏览本地磁盘以查找 CA 证书。

步骤 4 为证书指定一个名称，以在 SMC 配置中对其进行标识。

步骤 5 点击 **Add Certificate**。

向 Lancope SMC 注册思科 ISE。

此时在部署中，经过验证表明思科 ISE 中存在活动的身份验证会话，并且可由外部实体使用已配置的用户名和密码检索这些会话。

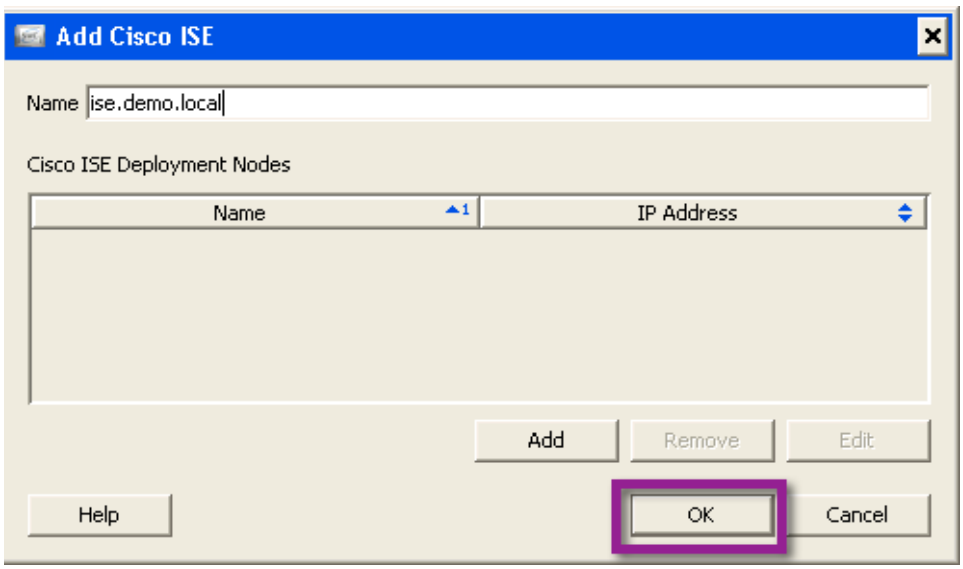
操作步骤

步骤 1 登录 SMC 客户端软件。

步骤 2 突出显示域，然后点击 **Configuration > Add Cisco ISE …**

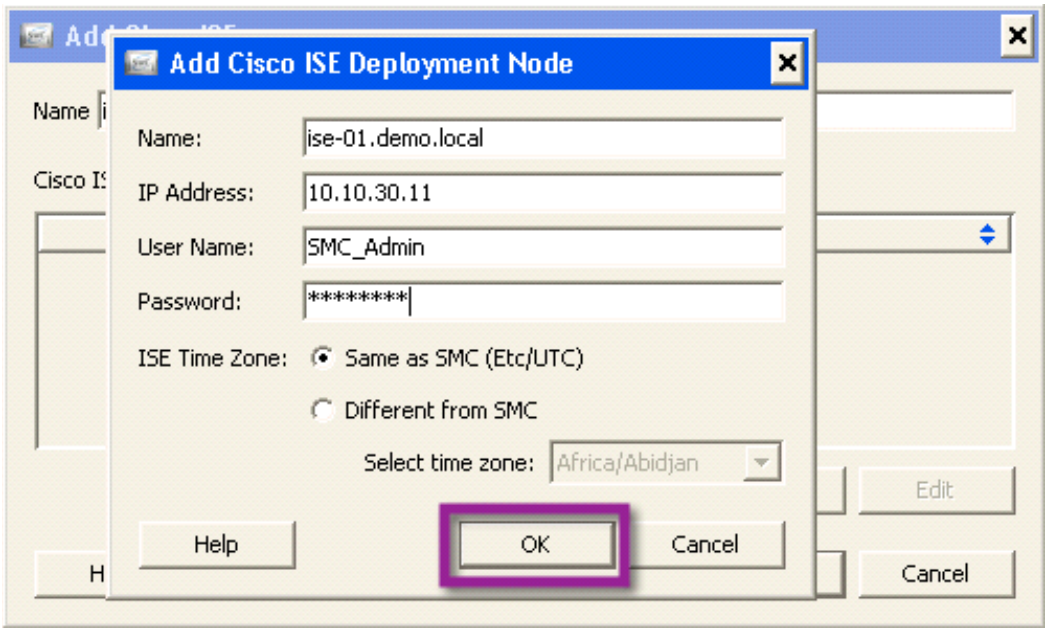
步骤 3 输入 ISE 部署的名称，如图 17 中所示。

图 17　　添加思科 ISE



步骤 4 点击 Add，并且输入 Name、IP Address、User Name 和 Password，标识思科身份服务引擎所在的时区，然后点击 **OK**。（请参阅图 18。）

图 18　添加思科 ISE 部署节点

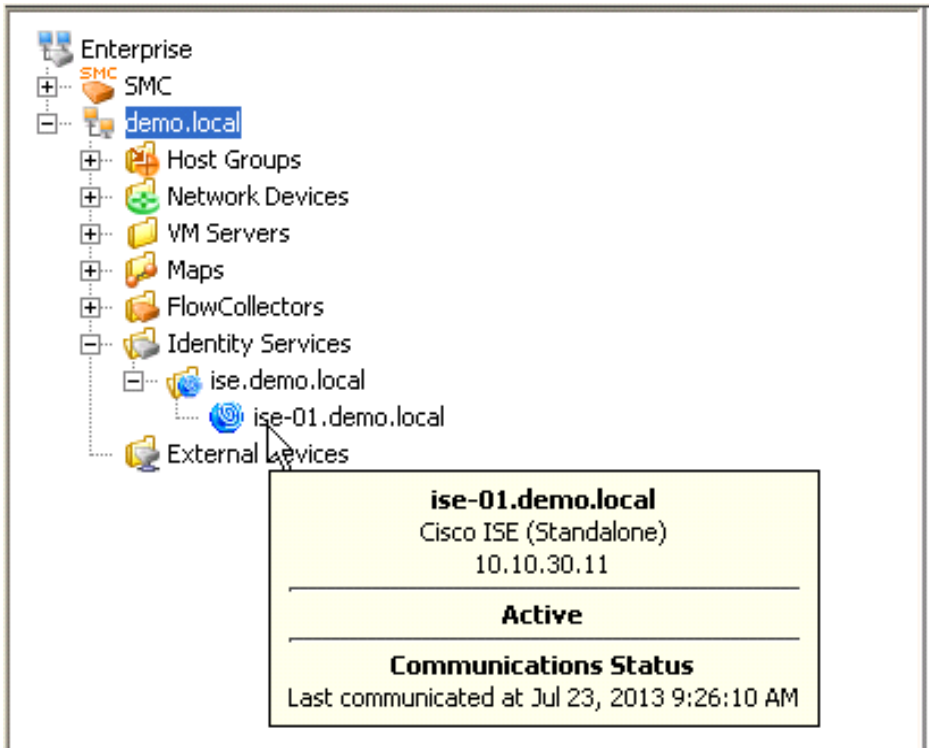


步骤 5 要输入第二个 ISE MNT 节点以实现冗余，请对第二个节点重复上一步骤。

步骤 6 检查与思科身份服务引擎的通信状态。

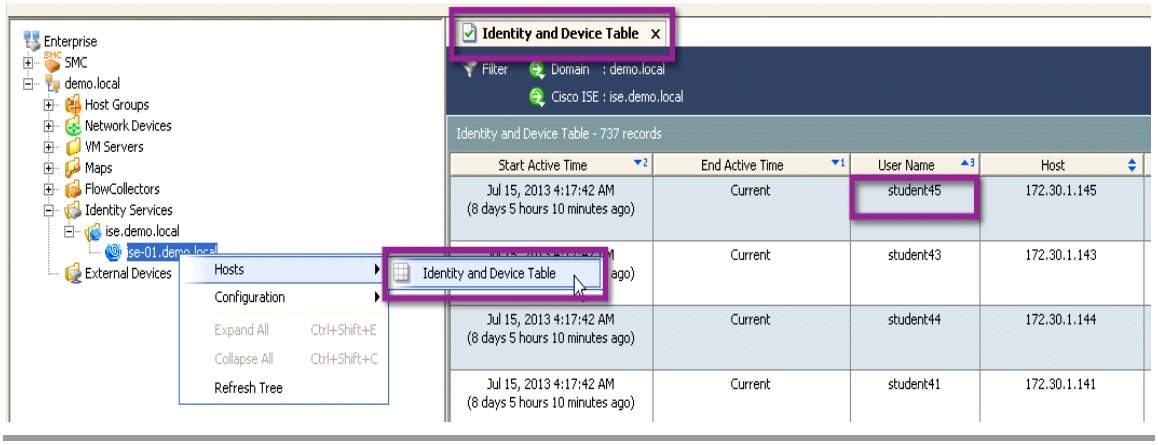
展开 Identity Services 菜单并将鼠标悬停在身份服务引擎图标上以查看通信状态，如图 19 中所示。

图 19　　检查通信状态



步骤 7　右键单击身份服务引擎图标，然后转至 **Hosts > Identity and Device Table**。这将打开 Identity and Device Table，如图 20 中所示。验证已进行身份认证的用户名在表中是否存在。

图 20　　身份和设备表



总结

本指南描述思科网络威胁防御解决方案 1.1 的设计、部署和实施详细信息。现在，可行的解决方案在网络上应该存在，并且准备帮助进行高级威胁防御检测和加速事件响应。请参考思科网络威胁防御指南系列中的其他指南，以了解如何将此解决方案充分利用于网络威胁防御。

附录 A：参考

安全网络服务

- 《Cisco TrustSec 解决方案 2.0 设计和实施指南》— http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_2.0/trustsec_2.0_dig.pdf

NetFlow

- 《Lancope NetFlow 带宽计算器》— http://www.lancope.com/resource-center/netflow-bandwidth-calculator-stealthwatch-calculator/
- 《NetFlow 性能分析》— http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns562/ns583/net_implementation_white_paper0900aecd80308a66.pdf
- 《Cisco Catalyst 3K-X 服务模块：在访问过程中启用 Flexible NetFlow》— http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps10745/white_paper_c11-691508_ps10744_Products_White_Paper.html
- 《Cisco Catalyst 4500 系列交换机软件配置指南，Cisco IOS-XE 软件版本
- 3.1.0 SG：配置 Flexible NetFlow》— http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/01xo/configuration/guide/fnf.html
- 《Cisco Catalyst 6500 系列管理引擎 SUP2T：NetFlow 增强功能》— http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-652021.html
- 《NetFlow 配置指南，思科 IOS 软件版本 15.2 M&T》— http://www.cisco.com/en/US/partner/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book.html
- 《配置网络安全事件记录日志 (NSEL)》— http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/monitor_nsel.html
- 《适用于 NetFlow 收集器的思科 ASA 5500 系列实施指南，版本 8.4、8.5 和 8.6》- http://www.cisco.com/en/US/docs/security/asa/asa84/system/netflow/netflow.html

身份服务引擎

- 《思科身份服务引擎 API 参考指南，版本 1.0.4》— http://www.cisco.com/en/US/docs/security/ise/1.0/api_ref_guide/ise10_api_ref_guide.html

关于思科验证设计计划

CVD 计划由一些经过设计、测试和记录的系统和解决方案组成，旨在提高客户部署的速度、可靠性和可预测性。有关详细信息，请访问 http://www.cisco.com/go/designzone。

本手册中所有设计、规格、陈述、信息和建议（统称为“设计”）均按“原样”提供，可能包含错误信息。思科及其供应商不提供任何保证，包括（但不限于）适销性、适合特定用途和非侵权保证，或因交易习惯或贸易惯例而产生的保证。任何情况下，思科或其供应商均不对任何间接性、特殊性、后果性或附带性损害承担责任，包括（但不限于）因使用或未使用这些设计而导致的利润损失或数据丢失或损坏，即使思科或其供应商已被告知存在此类损害的可能性。这些设计如有更改，恕不另行通知。用户对这些设计的使用负有全部责任。这些设计并不构成思科及其供应商或合作伙伴的技术建议或其他专业建议。用户在采用这些设计之前应咨询他们的技术顾问。思科未测试的一些因素可能导致结果有所不同。

思科所采用的 TCP 报头压缩是加州大学伯克莱分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。版权所有。© 1981，加利福尼亚州大学董事。思科和思科徽标是思科系统公司和/或其附属公司在美国和其他国家/地区的 商标。如需思科商标的列表，请访问 http://www.cisco.com/go/trademarks。本文提及的第三方商标均归属其各自所有者。使用“合作伙伴”一词并不暗示思科和任何其他公司存在合伙关系。(1005R) 本文档中使用的任何互联网协议 (IP) 地址和电话号码并不代表实际地址和电话号码。本文档中包括的任何示例、命令显示输出、网络拓扑图和其他图形仅用于说明目的。在图示内容中使用的任何实际 IP 地址或电话号码纯属虚构，如有雷同，纯属巧合。