IBA

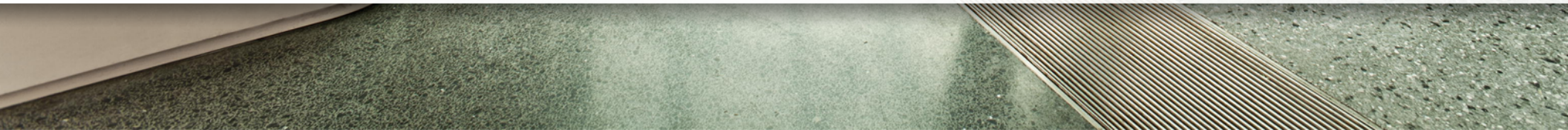
无边界网络

部署指南

基于NetFlow的应用监控部署指南

智能业务平台IBA

2012年8月系列



前言

本指南的目标受众

Cisco®智能业务平台(IBA)指南主要面向承担以下职务的读者:

- 需要用标准程序来实施方案时的系统工程师
- 需要撰写思科IBA实施项目工作说明书的项目经理
- 需要销售新技术或撰写实施文档的销售合作伙伴
- 需要课堂讲授或在职培训材料的培训人员

一般来说,您也可以将思科IBA指南作为增加工程师和项目实施统一性的指导文件,或利用它更好地规划项目成本预算和项目工作范围。

版本系列

思科将定期对IBA指南进行更新和修订。在开发新的思科IBA指南系列时,我们将会对 其进行整体评测。为确保思科IBA指南中各个设计之间的兼容性,您应当使用同一系列 中的设计指南文档。

每一个系列的Release Notes (版本说明) 提供了增加和更改内容的总结。

所有思科IBA指南的封面和每页的左下角均标有指南系列的名称。我们以某系列指南发 布时的年份和月份来对该系列命名,如下所示:

年 月 系列

例如,我们把于2011年8月发布的系列指南命名为:
"2012年8月系列"

您可以在以下网址查看最新的IBA指南系列:

http://www.cisco.com/go/cn/iba

如何阅读命令

许多思科IBA指南详细说明了思科网络设备的配置步骤,这些设备运行着Cisco IOS、 Cisco NX-OS或其他需要通过命令行界面(CLI)进行配置的操作系统。下面描述了系 统命令的指定规则,您需要按照这些规则来输入命令:

在CLI中输入的命令如下所示:

```
configure terminal
```

为某个变量指定一个值的命令如下所示:

```
ntp server 10.10.48.17
```

包含您必须定义的变量的命令如下所示:

```
class-map [highest class name]
```

以交互示例形式显示的命令(如脚本和包含提示的命令)如下所示:

```
Router# enable
```

包含自动换行的长命令以下划线表示。应将其作为一个命令进行输入:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

系统输出或设备配置文件中值得注意的部分以高亮方式显示,如下所示:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

问题和评论

如果您需要评论一个指南或者提出问题, 请使用 IBA反馈表。

如果您希望在出现新评论时获得通知,我们可以发送RSS信息。

目录

基于NetFlow的应用监控部署指南 1

前言 5

业务概述 5

技术概述 5

部署详情 14

配置设备以导出NetFlow信息 15

监控NetFlow数据 20

附录A: 产品列表 25

WAN 汇聚 25

WAN远端站点 25

附录B: Show-Flow监控器完整输出 27

附录C: 支持NetFlow的设备配置 29

支持NetFlow的ASR1000系列路由器 (TNF和FNF) 29

支持NetFlow的ISR-G2系列路由器 (TNF和FNF) 33

附录D: 变更 47

本IBA指南的内容

关于IBA无边界网络

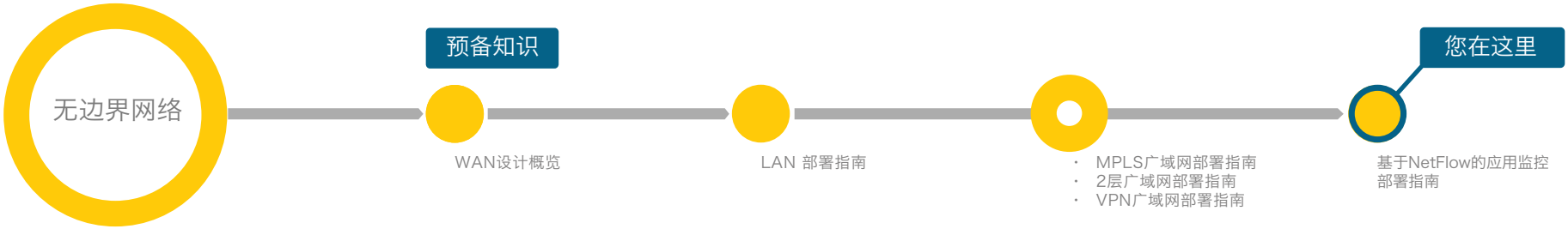
思科IBA能帮助您设计和快速部署一个全服务企业网络。IBA系统是一种规范式设计，即购即用，而且具备出色的可扩展性和灵活性。

思科IBA在一个综合的解决方案中集成了局域网、广域网、无线、安全、数据中心、应用优化和统一通信技术，并对其进行了严格测试，确保能实现无缝协作。IBA采用的模块化分类简化了多技术系统集成的复杂度，使您能够根据需要解决企业需求，而无需担心技术复杂性。

思科IBA无边界网络是一个稳固的网络基础架构，为拥有250至10,000名用户的企业网络设计。IBA无边界网络架构集成了有线和无线局域网接入、广域网连接、广域网应用加速以及互联网边缘的安全架构。

成功部署路线图

为确保您能够按照本指南中的设计成功完成部署，您应当阅读本指南所依据的所有相关指南——即如下路线中本指南之前的所有指南。



关于本指南

本部署指南包括一个或多个部署章节，其中包含如下内容：

- **业务概述**——描述本设计的商业用例，业务决策者可通过本章内容来了解解决方案与企业运营的相关性。
- **技术概述**——描述该商业用例的技术设计，包含思科产品如何应对业务挑战。技术决策者可利用本章节理解该设计如何实现。
- **部署详情**——提供解决方案的逐步实施和配置的指导。系统工程师可以在这些步骤的指导下快速和可靠的设计和部署网络。

您可以在以下网址查看最新的IBA指南系列：

http://www.cisco.com/go/cn/iba

前言

业务概述

广域网是重要基础设施，支持着企业所有职能部门的业务流程。对于负责规划、运营和维护网络及网络服务的员工来说，全面监控网络的最新状态是必不可少的。同时他们还需要收集短期和长期的信息，以全面了解网络的性能情况以及网络上活跃的应用。来自网络的NetFlow数据与来自语音和视频电话控制系统的呼叫详情记录同等重要。

企业最关注的方面包括：

- 当前在使用哪些应用及其对网络的影响。
- 网络流量的具体情况—谁、什么、何时、何地、以何种方式。
- 网络资源的效率和利用率。
- 变化对网络的影响。
- 可能预兆安全事件的网络异常情况。

容量规划是企业在管理其网络时所面临的最重要的问题之一。网络容量规划工作与其说是一门科学，还不如说是一门艺术。这一工作旨在平衡需求，以在不超出资本预算的情况下满足用户的性能期望。

广域网带宽非常昂贵。许多公司试图通过购买处理网络流量所需的最低带宽，来控制成本。但这一战略会导致堵塞，造成应用性能降低。

对网络的可视能力可支持进行资源调整，确保适当使用资源来支持企业目标。同时它还能够帮助IT人员验证服务质量（QoS）是否正确实施，以便语音或视频等延迟敏感型流量能够获得较高优先级。监控在网络安全性方面也起着关键作用，因为不间断的流量监控可以检测出拒绝服务（DoS）攻击、网络传播的蠕虫和其他不良的网络事件。

本指南主要侧重于探讨网络内的应用监控。

技术概述

NetFlow是运行在路由器和交换机上的思科IOS软件的一种嵌入功能。它允许企业收集流量流信息。

一般情况下，NetFlow数据的主要使用情况包括：

- 网络规划和容量规划。
- 实时网络监控。
- 应用和用户剖析(profiling)。
- 安全事件检测和分类。
- 记帐和计费。
- 网络数据仓储、取证和数据采掘。
- 故障排除.

NetFlow可为企业带来诸多优势，能够使企业：

- 通过识别已知基准的变化，分析新应用及其网络影响。
- 通过使用NetFlow统计数据来测量与不同应用策略相关的广域网流量变化，减少峰值广域网流量，并了解谁在使用网络以及谁是最大网络流量生成者（top-talker）。
- 利用命令行界面（CLI）或报告工具，实时诊断网络性能缓慢现象、带宽占用大户以及带宽利用率。
- 通过识别引起堵塞的应用，检测未授权的广域网流量并避免代价高昂的升级。
- 检测并监控安全异常以及其它网络中断情况及其相关来源。
- 验证是否正确实施了服务质量(QoS)，并确保已为每个服务类别（CoS）分配了适当的带宽，以及没有CoS超额预订或预订不足。

传统NetFlow（TNF）

思科NetFlow使转发流量的网络设备能够收集有关各流量流的数据。传统NetFlow（TNF）指NetFlow的原始实施，可将一个流作为以下七个关键字段的独特组合：

- IPv4源IP地址
- IPv4目的地IP地址
- 源端口编号
- 目的地端口编号
- 第3层协议类型
- 服务类型（ToS）字节

・输入逻辑接口

这些关键字段定义一个独特的流。如果一个流与其他流相比具有一个不同的字段，那么它将被视为一个新的流。

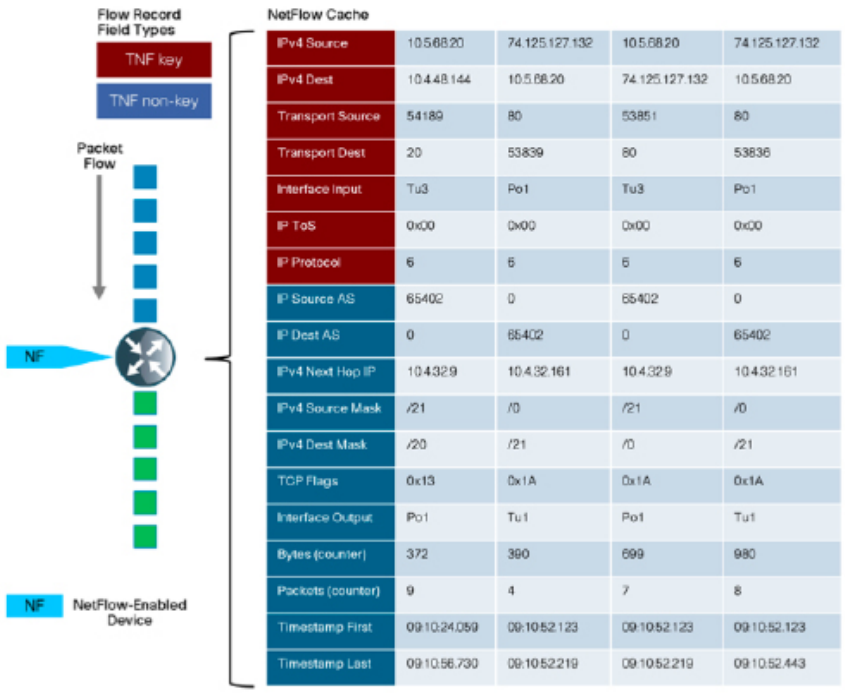
NetFlow通过创建NetFlow高速缓存项来运行，此高速缓存项包含了支持NetFlow的设备上的所有活动流的信息。NetFlow通过标准交换路径处理第一个流数据包，来构建其高速缓存。它在NetFlow高速缓存内保留所有活动流的流记录。NetFlow高速缓存中的每个流记录包含关键字段，以及其他非关键字段，这些信息随后可在将导出数据至收集设备时使用。每个流记录均通过识别带有相似流特征的数据包来创建，并统计或跟踪每个流的数据包和字节数。

技术提示

NetFlow关键字段独特地确定一个流。

NetFlow非关键字段包含每个流的其他信息，并与关键字段信息一起存储。

图 1 - TNF高速缓存



最初TNF使用入口和出口NetFlow记帐特性，如今这已被认为是一种过时的功能。支持NetFlow的设备能够后向兼容这些在新配置框架内实施的记帐特性。具体信息在下文中进行了详细介绍。

Flexible NetFlow (FNF)

Flexible NetFlow (FNF) 不同于TNF，它允许您定制和关注特定的网络信息。您可以使用传统的七个关键字段的子集或超集，来定义一个流。FNF还拥有多个额外字段（关键和非关键）。这允许企业获得更具体的信息，以便减少导出的信息量总和流数量，从而增强可扩展性和聚合。

可用的关键字段如表1中所列。如果需要，这些关键字段还可用作非关键字段。

表 1 - 所有FNF关键字段

关键字段类型	关键字段值
应用	name
数据链路	dot1q vlan input dot1q vlan output dot1q mac destination address input dot1q mac destination address output dot1q mac source address input dot1q mac source address output
流	direction sampler
接口	input output
IPv4	destination address destination mask destination prefix dscp fragmentationflags fragmentation offset header-length id length header length payload length total option map precedence protocol section header size [value] section payload size [value] source address source mask source prefix tos total-length ttl version
路由	destination as destination traffic-index forwarding-status is-multicast multicast replication-factor next-hop address source as source traffic-index vrf input

传输	destination-port icmp code icmp type igmp type source-port tcp acknowledgement-number tcp destination-port tcp flags tcp header-length tcp sequence-number tcp source-port tcp urgent-pointer tcp window-size udp destination-port udp message-length udp source-port

可针对每个独特流收集的非关键字段如表2中所示。

表 2 - 额外非关键字段

非关键字段类型	非关键字段值
计数器	bytes packets
时间戳	sys-uptime first sys-uptime last
IPv4	total-length maximum total-length minimum ttl maximum ttl minimum

从TNF迁移至FNF

在网络设备上引入FNF支持需要新的配置方法来提供额外能力。您也可使用这一新配置CLI来配置传统TNF，而不必使用原始配置CLI（现在被称为经典CLI）。

FNF包括多个预定义的记录，可供您用来启动网络中的监控流量。预定义的记录可确保后向兼容可能不包括FNF支持的NetFlow收集器配置。它们拥有独特的关键和非关键字段组合，后向兼容传统TNF配置。

在我们的部署中所使用的预定义记录**netflow ipv4 original input**在功能上等同于在使用流记录之前所用的原始TNF入口和出口NetFlow记帐特性。经典与新配置方法的对比如下。

传统NetFlow—经典CLI

```
interface GigabitEthernet0/0
ip flow [ingress|egress]
!
ip flow-export destination 10.4.48.171 2055
ip flow-export source Loopback0
ip flow-export version 9
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
```

新配置CLI示例使用了预定义的**record ipv4 original-input**，其中包括了在图1中所列的TNF关键和非关键字段。

该示例应被用于将传统TNF部署迁移至新的CLI，而无需更改设备行为。

技术提示

仅思科汇聚多业务路由器1000（ASR1000）和思科第二代集成多业务路由器（ISR-G2）支持预定义的流记录。

传统NetFlow—新配置CLI

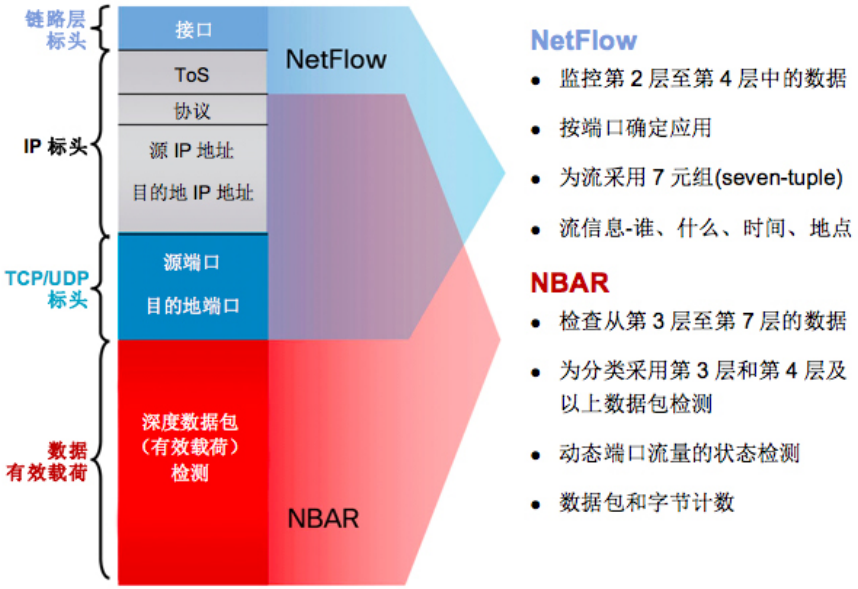
```
interface GigabitEthernet0/0
 ip flow monitor Monitor-NF [input|output]
!
```

```
flow exporter Export-NF-1
 destination 10.4.48.171
 source Loopback0
 transport udp2055
 export-protocol netflow-v9
 !
flow monitor Monitor-NF
 record netflow ipv4 original-input
 exporter Export-NF-1
 cache timeout active 1
 cache timeout inactive 15
```

基于网络的应用识别(NBAR)

基于网络的应用识别 (NBAR) 是思科IOS软件中的智能分类引擎，能够识别广泛的应用，包括基于Web的应用和客户端/服务器应用。NBAR使用深度包检测来查看传输层有效载荷，以确定相关的应用，如图2中所示。

图 2 - NetFlow和NBAR集成



NBAR能够对应用进行分类，这些应用使用：

- 静态分配的传输控制协议 (TCP) 和用户数据报协议 (UDP) 端口编号。
- 非UDP和非TCP IP协议。
- 建立连接的过程中协商的动态分配的TCP和UCP端口编号；应用和协议分类需要状态检测。这种能力可以通过在进行了分配的数据连接端口上传送控制连接，发现将被分类的数据连接。
- 子端口分类；HTTP分类 (URL、mime (多用途互联网邮件扩展) 或主机名) 和思杰应用独立计算架构 (ICA) 流量分类 — 基于公布的应用名称。
- 基于深度包检测的分类和多应用特定属性。实时传输协议 (RTP) 有效载荷分类基于这一算法，其数据包基于RTP报头中的多个属性被归为RTP类别。

FNF可与NBAR无缝集成，并能够使用**application name**作为FNF流记录中的关键字段或非关键字段来收集数据。NBAR提供的应用识别比使用TCP/UDP已知端口映射更有效。

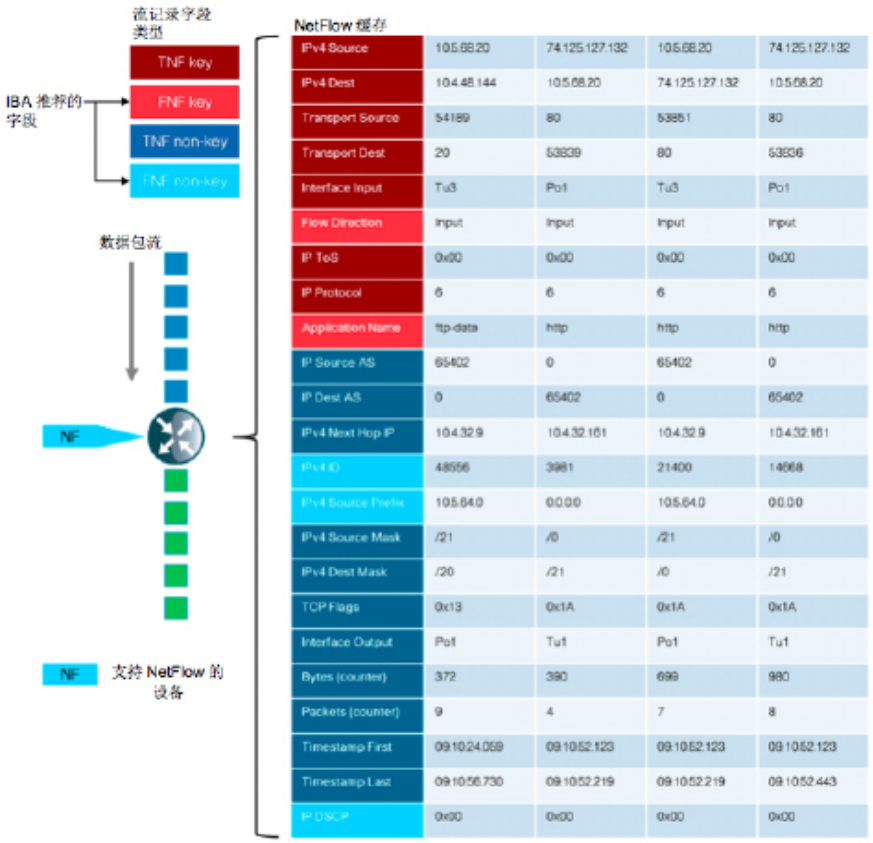
技术提示

采用NBAR的应用识别是从TNF迁移到FNF的主要原因之一。

注意，思科ASR1000当前在端口通道接口上不支持NBAR。

思科IBA智能业务平台的FNF实施选择了额外字段，它们在所部署的架构中提供了改进的应用可见性。这些额外字段列在图3中。

图 3 - FNF缓存



NetFlow与加密的交互

配置NetFlow时，了解当在接口上发送和接收网络流量时思科IOS如何处理流量将非常有帮助。这可以通过一个按顺序排列的列表清晰地显示出来，如图4中所示。

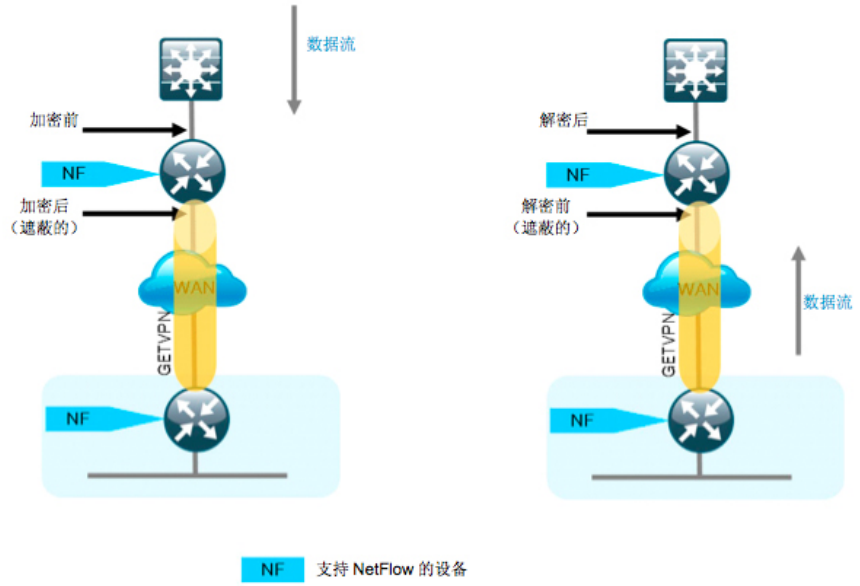
图 4 - IOS操作顺序

根据操作顺序，为了正确进行流量分类，NetFlow必须在发送时进行加密前监控，并在接收时进行解密后监控。否则，使用的实际协议仍很模糊，所有流量显示为IPSec，而没有提供其他详细信息。来自广域网的加密流量由NetFlow采用相应局域网接口上的出站监视器进行适当分类。同样，到广域网的流量由NetFlow采用相应局域网接口上的入站监视器进行适当分类。这在图5中进行了阐述。

技术提示

当使用连接局域网分发层及其广域网接口上的GETVPN加密的端口通道接口时，思科ASR1000路由器不能使用NBAR对数据进行分类。

图 5 - 加密和NetFlow



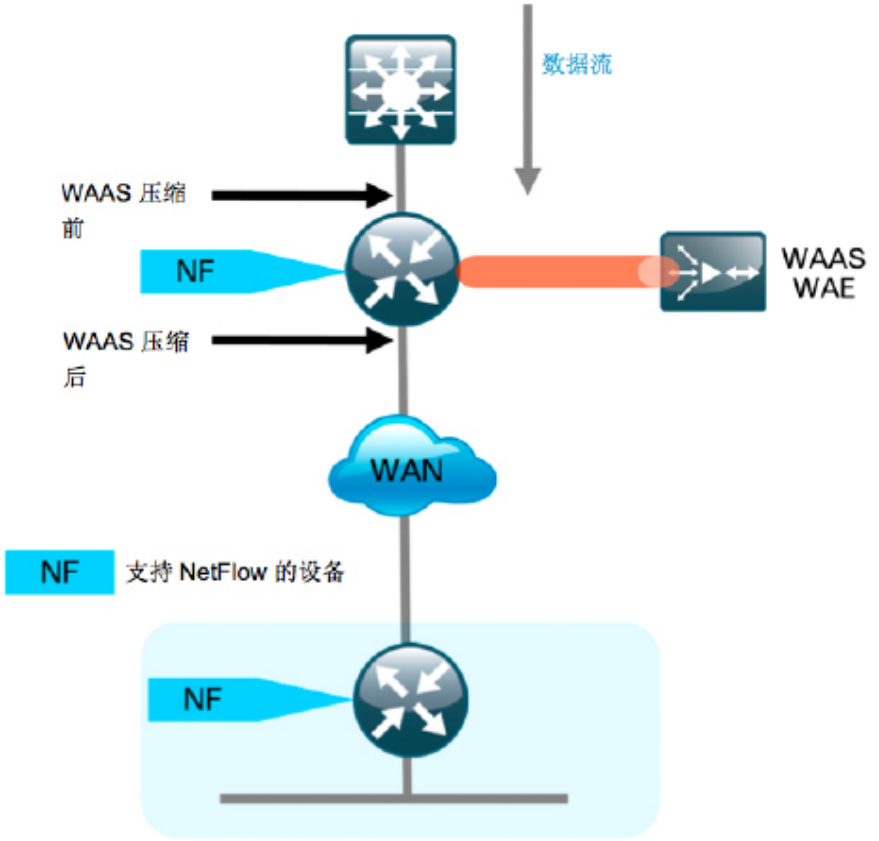
NetFlow与应用优化的交互

思科IBA智能业务平台架构包括了使用思科广域应用服务（WAAS）的应用优化，以加速和优化广域网中的数据。关于部署的全部详情在《思科IBA智能业务平台——无边界网络应用优化部署指南》中提供。

您可以配置NetFlow，以便能够在源地址和目的地之间的路径上的多个点收集信息。当您使用应用优化时，您选择监控的接口和被监控的方向会影响网络设备缓存的数据。图6中的拓扑图显示了潜在的复杂性。

您可以在两个地点监控通过广域网前往远程站点的流量。在面向局域网的接口中入站方向缓存的流反映在经过思科WAAS优化之前的未压缩数据。在面向广域网的接口中出站方向缓存的相同流反映经过思科WAAS优化的压缩数据。

图 6 - 应用优化和NetFlow



对于具有应用优化的NetFlow，思科IBA智能业务平台建议在面向局域网和面向广域网的接口中都配置入站和出站流监控。这可确保可捕获所有流信息。在面向局域网的接口上收集的流数据可提供正在使用的应用及其实际网络使用情况的准确视图。在面向广域网的接口中收集的流数据可准确反映从广域网发送和接收的网络流量总量。

技术提示

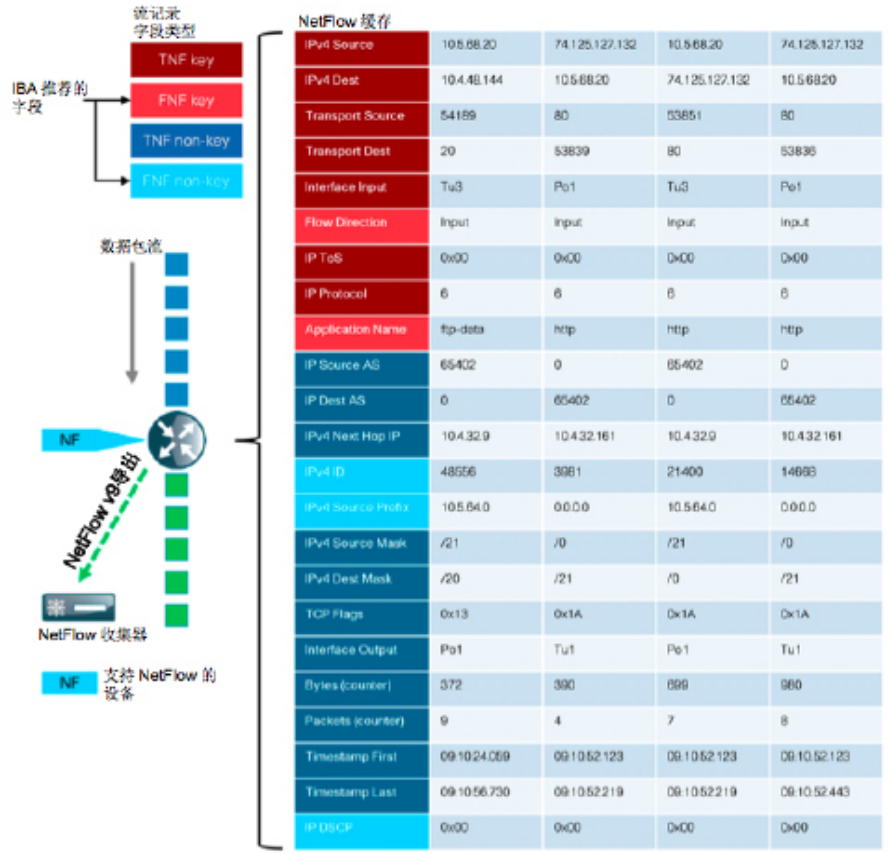
在分析过程中，有必要根据是否需要面向局域网或面向广域网的分析，而过滤数据。

监控

通过使用CLI show命令，可以直接从支持NetFlow的设备中查看NetFlow数据，但是该方法有些繁琐，而且难以在多个设备间关联数据。

流详细信息被导出到运行流收集器服务的外部设备，如图7中所示。缓存的流数据基于可配置的定时器定期被发送。对于在NetFlow设备中交换的流信息，收集器能够存储范围广泛的历史记录。NetFlow非常高效；导出的数据量仅占路由器或交换机中实际流量的很小比例。NetFlow对每个数据包进行记账（当在非采样模式中时），并能够为进入路由器或交换机的所有网络流量提供一个高度精简的详细视图。NetFlow收集器应位于服务器机房或数据中心。

图 7 - NetFlow导出至收集器



查看NetFlow数据的最有效方式是通过专门的分析应用，通常与流收集器服务搭配使用。各种应用通常侧重于流量分析、安全性（异常检测和拒绝服务）或计费。TNF监控应用预期将导出一个标准字段集。每个特定的FNF监控应用将可能拥有一个定制的NetFlow属性集和一种特殊的导出格式，必须在将数据发送至收集器之前，在支持NetFlow的设备上进行配置。

实施FNF的要求在很大程度上取决于您所使用的收集器/分析应用。在本指南“部署详情”部分，针对以下应用的TNF和FNF提供了示例部署指导。

仅传统NetFlow:

- SolarWindsOrion NetFlow Traffic Analyzer (NTA)

Flexible NetFlow:

- ActionPacked! LiveAction
- LancopeStealthWatch
- Plixer Scrutinizer
- SevOne Network Management System (NMS)

本指南使用这些应用的原因如下:

- 在典型的思科IBA智能业务平台企业中大量使用
- 专门致力于NetFlow分析
- 易于使用
- 凭借FNF支持居于行业领先地位

本指南侧重于在思科IBA智能业务平台支持的网络拓扑中配置TNF和FNF, 在所有支持FNF和NBAR并采用业经测试的软硬件组合的设备上实现NetFlow。这包括总部的广域网路由器和远程站点路由器。

备注

部署详情

思科路由器支持两种NetFlow配置方法：一种新方法，用于FNF部署；以及一种老方法，仅限于TNF部署使用。本指南侧重于探讨可用于同时支持FNF和TNF部署的新方法。

在思科IBA智能业务平台架构中使用的广域网路由器能够支持FNF和TNF。广域网聚合路由器应监控面向局域网和面向广域网的接口，但思科ASR1000系列上的端口通道接口例外，如图8中所示。远程站点路由器应监控面向广域网的接口和面向接入层或分布层的接口，如图9中所示。收集的具体数据字段，以及启用了NetFlow的设备上使用的适当定时器值，记录在以下程序中。

图 8 - 在哪里监控NetFlow—广域网聚合

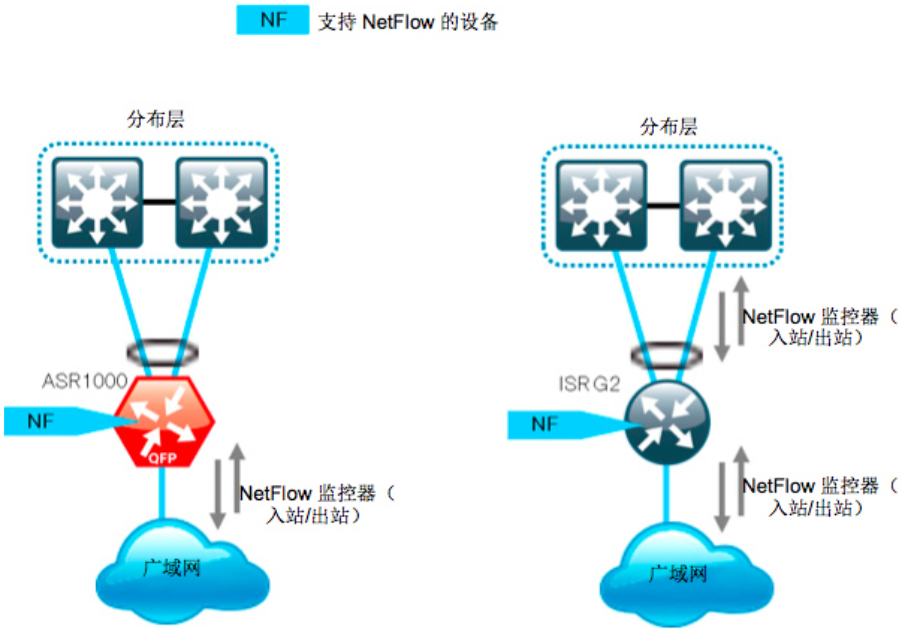
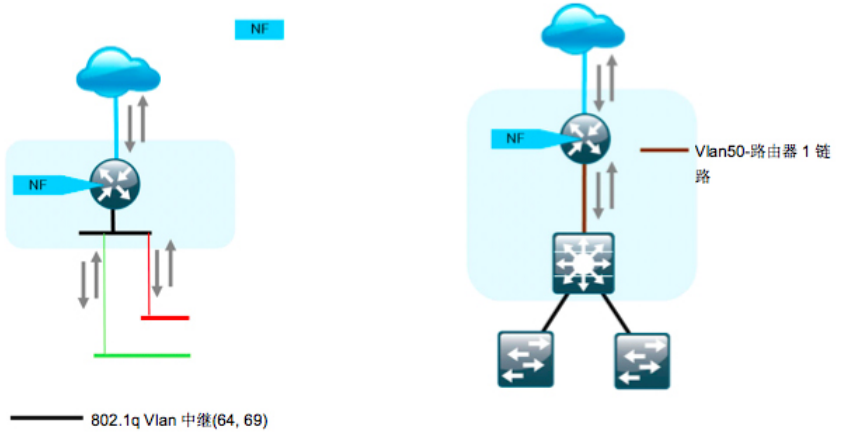


图 9 - 在哪里监控NetFlow—广域网远程站点



必须完成以下流程，才能实现NetFlow数据收集和可选数据导出。

- 创建一个FNF流记录或选择一个内建的流记录，以与TNF一起使用。
- 为每个外部NetFlow收集器创建一个流导出器。
- 创建一个流监控器，并将它与定制或内建的流记录相关联。如果您想在外部收集器上分析数据，您还必须分配一个或多个流导出器。
- 向网络设备上的接口分配流监控器。

接下来的程序包括有关需要收集哪些关键字段和非关键字段来对您的网络进行有效的应用监控的最佳实践建议。本指南在程序中提供了两组示例。这些示例阐述了如何与仅支持TNF的NetFlow收集器以及支持FNF的NetFlow收集器进行集成。

流程

配置设备以导出NetFlow信息

1、创建Flexible NetFlow流记录

2、创建流导出器

3、创建流监控器

4、将流监控器应用于广域网和局域网

程序 1　创建Flexible NetFlow流记录

Flexible NetFlow (FNF) 要求明确配置同时包含关键字段和非关键字段的流记录。此程序提供了有关如何配置用户定义的流记录的指导，该流记录包含所有TNF字段 (关键和非关键)，以及额外FNF字段 (关键和非关键)。所产生的流记录包括经典NetFlow部署中使用的全部TNF字段子集。

步骤 1: 指定关键字段。这决定了独特的流。确保包括针对各关键字段的单独匹配语句。

技术提示

建议您使用表3中所列的TNF关键字段，以及表4中所列的额外FNF关键字段。

```
flow record[record name]
 description [recorddescription]
match [key field type] [key field value]
```

表 3 - 建议的TNF关键字段 (TNF和FNF)

关键字段类型	关键字段值
ipv4	tos protocol source address destination address
传输	source port destination port
接口	input
流	sampler

表 4 - 建议的额外FNF关键字段(仅FNF)

关键字段类型	关键字段值	注释
流	direction	允许在同一接口进行入口/出口流收集
应用	name	支持收集各流的NBAR信息

技术提示

思科ASR1000当前在端口通道接口上不支持NBAR，当使用**application name**作为流记录中的关键字段时，您不能将流监控器应用于此平台上的端口通道接口。

步骤 2: 指定针对各独特流要收集的非关键字段。确保包括针对各非关键字段的单独收集语句。

Flexible NetFlow允许使用额外的、用户指定的非关键字段。建议您使用表5中所列的额外TNF非关键字段，以及表6中所列的额外FNF非关键字段。

```
flow record[record name]
collect [non-key field type] [non-key field value]
```

表 5 - 建议的TNF非关键字段(TNF和FNF)

非关键字段类型	非关键字段值
路由	source as destination as next-hop address ipv4
ipv4	source mask destination mask
传输	tcp flags
接口	output
计数器	bytes packets
时间戳	sys-uptime first sys-uptime last

表 6 - 建议的额外FNF非关键字段(仅FNF)

非关键字段类型	关键字段值	注释
ipv4	dscp id source prefix source mask	针对各流的额外IPv4信息

示例

```
flow record Record-FNF
 description Flexible NetFlow with NBAR Flow 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
 match flow direction
 match application name
collect routing source as
 collect routing destination as
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 id
 collect ipv4 source prefix
 collect ipv4 source mask
 collect ipv4 destination mask
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
```

程序 2　创建流导出器

存储在网络设备高速缓存中的NetFlow数据在导出到外部收集器时，能够被更有效地进行分析。

当把数据导出至一个外部收集器时，只需创建一个流导出器。如果仅在网络设备上分析数据，则可以略过此程序。

读者提示

大部分外部收集器使用SNMP来从网络设备检索接口表。确保您已完成您平台的相关SNMP程序。

广域网路由器程序在《思科IBA智能业务平台——无边界网络MPLS广域网部署指南》、《第二层广域网部署指南》或《VPN广域网部署指南》中列出。

不同的NetFlow收集器应用支持不同的导出版本格式（v5和v9），并有望在特定UDP或TCP端口上接收导出的数据。在此部署中，用于测试的收集器应用使用了表7中指定的参数。

表 7 - 经过测试的NetFlow收集器参数

供应商	应用	版本	功能	导出协议	目的地端口
ActionPacked!	LiveAction	2.42	Flexible NetFlow	netflow-v9	UDP 2055
Cisco	Prime Assurance Manager	1.1	Flexible NetFlow	netflow-v9	UDP 9991
Plixer	Scrutinizer	9.01	Flexible NetFlow	netflow-v9	UDP 2055
SevOne	Network Management System	4.1.3.74	Flexible NetFlow	netflow-v9	UDP 9996
SolarWinds	NetFlow Traffic Analyzer	3.9.0	Traditional NetFlow	netflow-v9	UDP 2055

步骤 1: 配置一个基本流导出器。

```
flow exporter [exporter name]
 description [exporter description]
 destination [NetFlow collector IP address]
 source Loopback0
 transport [UDP or TCP] [port number]
export-protocol [export protocol]
```

步骤 2: 如果您以NetFlow v9格式导出FNF记录，则导出FNF的接口表。

```
flow exporter [exporter name]
 option interface-table
```

步骤 3: 如果您在使用NBAR流记录，则导出NBAR应用表。

```
flow exporter [exporter name]
 option application-table
```

步骤 4: 如果您正在使用思科ISR-G2系列路由器，启用**output-features**。否则，源自广域网远程站点路由器的NetFlow流量将不会被加密或使用QoS进行标记。

```
flow exporter [exporter name]
output-features
```

示例 (带Plixer的FNF)

```
flow exporter Export-FNF-Plixer
 description FNF v9
 destination 10.4.48.171
 source Loopback0
output-features    ! this command is not required on ASR1000
routers
 transport udp 2055
export-protocol netflow-v9
option interface-table
 option application-table
```

示例 (带SolarWinds的TNF)

```
flow exporter Export-TNF-Solarwinds
 description TNF v9
 destination 10.4.48.173
output-features    ! this command is not required on ASR1000
routers
source Loopback0
 transport udp 2055
export-protocol netflow-v9
```

程序 3　创建流监控器

必须对网络设备进行配置，来监控每个接口上流经设备的流。流监控器必须包括一个流记录，如果要收集和分析数据，可选择包括一个或多个流导出器。流监控器创建后，它可应用于设备接口。流监控器可在高速缓存中存储流信息，同时针对此高速缓存的定时器值可在流监控器配置中进行修改。建议您将超时活动定时器设定为60秒，以导出现有长寿命流上的流数据。

步骤 1: 创建流监控器，然后设定高速缓存定时器。

```
flow monitor[monitor name]
 description [monitor description]
cache timeout active 60
```

步骤 2: 将流记录关联到流监控器。您可以使用一个定制或内建的流记录。

```
flow monitor[monitor name]
record [record name]
```

步骤 3: 如果您在使用外部NetFlow收集器，请将导出器与流监控器相关联。如果您在使用多个导出器，则添加额外行。

```
flow monitor[monitor name]
exporter [exporter name]
```

示例(带Plixer的FNF)

```
flow monitorMonitor-FNF
description FNF/NBAR Application Traffic Analysis
 record Record-FNF
 exporter Export-FNF-Plixer
 cache timeout active 60
```

示例 (使用预定义记录和SolarWinds的TNF)

技术提示

netflow ipv4 original-input是一个预定义的内建记录，可模拟针对TNF的经典CLI。

```
flow monitor Monitor-TNF
description TNF Traffic Analysis
 record netflow ipv4 original-input
 exporter Export-TNF-Solarwinds
 cache timeout active 60
```

```
ip flow monitor Monitor-TNF output
```

程序 4　将流监控器应用于广域网和局域网

针对NetFlow的最佳实践是监控到网络设备的所有入站和出站流量。此方法涵盖所有流量，与加密或应用优化无关。

技术提示

确保将流监控器应用于所有设备接口。

思科ASR1000系列路由器当前不支持端口通道接口上的NBAR。

步骤 1: 将流监控器应用于设备接口。

```
interface[name]
ip flow monitor [monitor name]input
 ip flow monitor [monitor name]output
```

示例- FNF

```
interface GigabitEthernet0/0
 description MPLS WAN Uplink
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-FNF output
interface GigabitEthernet0/2.64
 description Wired Data
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-FNF output
```

示例 - TNF

```
interface GigabitEthernet0/0
 description MPLS WAN Uplink
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-TNF output
interface GigabitEthernet0/2.64
 description Wired Data
 ip flow monitor Monitor-TNF input
```

流程

监控NetFlow数据

1、查看未过滤的原始流数据

2、过滤和查看流数据

3、查看来自NetFlow收集器的报告

存储在网络设备高速缓存中的数据能够以多种不同的方法进行查看，以支持常见使用情况。本文简要介绍了这些方法，提供了如何访问流数据的示例。

程序 1　查看未过滤的原始流数据

查看NetFlow高速缓存的最简单方法是通过以下命令，这可以提供高速缓存状态概要及后续的一系列独立高速缓存项。

步骤 1： 显示NetFlow高速缓存。

```
show flow monitor[monitor name]cache
```

示例

```
Router#show flow monitor Monitor-FNF cache
 Cache type:                               Normal
Cache size:                                 4096
Current entries:                              55
High Watermark:                             4096
Flows added:                             2188410
Flows aged:                              2188355
  - Active timeout      (    60 secs)      153722
  - Inactive timeout    (    15 secs)     1984047
  - Event aged                                 0
  - Watermark aged                         37846
  - Emergency aged                         12740
  IPV4 SOURCE ADDRESS:        10.11.4.10
  IPV4 DESTINATION ADDRESS:   172.16.50.80
  TRNS SOURCE PORT:           52790
  TRNS DESTINATION PORT:      80
  INTERFACE INPUT:            Po1.64
  FLOW DIRECTION:             Input
  IP TOS:                     0x00
  IP PROTOCOL:                6
  APPLICATION NAME:           nbar http
  ipv4 next hop address:      192.168.6.134
  ipv4 id:                    355
  ipv4 source prefix:         10.11.4.0
  ipv4 source mask:           /24
  ipv4 destination mask:      /0
  tcp flags:                  0x18
  interface output:           Gi0/0
  counter bytes:              2834
  counter packets:            38
  timestamp first:            14:30:03.102
  timestamp last:             14:30:03.734
  ip dscp:                    0x00
```

程序 2　过滤和查看流数据

(可选)

如果您知道特定字段，如源IP地址或目的地IP地址或者TCP/UDP端口编号，那么您可以搜索准确匹配的高速缓存，或者使用支持更广泛匹配标准的正则表达式。

步骤 1： 显示过滤的NetFlow高速缓存。

```
show flow monitor[monitor name]cache filter [filter
parameters]
```

表 8 - NetFlow 高速缓存过滤器参数

字段类型	可用参数
应用	name **[value]**
计数器	bytes **[value]** flows **[value]** packets **[value]**
流	direction input direction output
接口	input **[interface type][number]** output **[interface type][number]**
IPv4	destination address **[value]** destination mask **[value]** dscp **[value]** id **[value]** protocol **[value]** source address **[value]** source mask **[value]** tos**[value]**
路由	next-hop address ipv4 **[value]**
时间戳	sys-uptime first **[value]** sys-uptime last **[value]**
传输	destination-port **[value]** source-port **[value]** tcp flags **[value]**

示例

以下命令显示了如何验证RTP流拥有适当的QoS差分服务代码点 (DSCP) 设置。

技术提示

交互式视频配置用于使用DSCP cs4和af41。

cs4 = 0x20
af41 = 0x22

```
Router#show flow monitor Monitor-FNF cache filter application
name regexp rtp
    IPV4 SOURCE ADDRESS:       10.11.4.40
    IPV4 DESTINATION ADDRESS:  10.10.48.27
    TRNS SOURCE PORT:          2454
    TRNS DESTINATION PORT:     51124
    INTERFACE INPUT:           Gi0/0
    FLOW DIRECTION:            Input
    IP TOS:                    0x88
    IP PROTOCOL:               17
    APPLICATION NAME:          nbarrtp
    ipv4 next hop address:     10.10.32.1
    ipv4 id:                   0
    ipv4 source prefix:        10.11.0.0
    ipv4 source mask:          /16
    ipv4 destination mask:     /24
    tcp flags:                 0x00
    interface output:          Po32
    counter bytes:             875384
    counter packets:           2391
    timestamp first:           15:32:52.027
    timestamp last:            15:33:39.827
    ip dscp:                   0x22
```

步骤 2: 分类和格式化流数据。

可用于搜索NetFlow高速缓存的同一字段还可用作简单分类字段。您可从表9中选择任意参数，并按最高到最低或最低到最高进行排序。此外，您还能够以多种

方式格式化命令输出，如表10中所列。此表输出最适合确定最大流量来源或目的地。

```
show flow monitor [monitor name] cache sort [filter parameters]
```

表 9 - NetFlow缓存分类参数

字段类型	可用参数
应用	name
计数器	bytes flows packets
流	direction input direction output
最高（缺省）	—
接口	input **[interface type][number]** output **[interface type][number]**
IPv4	destination address **[value]** destination mask **[value]** dscp**[value]** id **[value]** protocol **[value]** source address **[value]** source mask **[value]** tos**[value]**
最低	—
路由	next-hop address ipv4 **[value]**
时间戳	sys-uptime first **[value]** sys-uptime last **[value]**
传输	destination-port **[value]** source-port **[value]** tcp flags **[value]**

表 10 - NetFlow缓存输出格式

格式类型	可用参数
csv	适用于剪切/粘贴导出
记录（缺省）	最适用于查看各高速缓存项
表	适用于非屏幕显示（要求316字符宽）

示例

以下命令显示了如何查看按**counter bytes（计数字节）**分类并针对屏幕浏览格式为表的高速缓存。

```
Router#show flow monitor Monitor-FNF cache sort  counter bytes format table
```

以下是使用**show flow monitor（显示流监控器）**命令后的部分输出结果。如欲了解完整输出示例，请查看附录B。

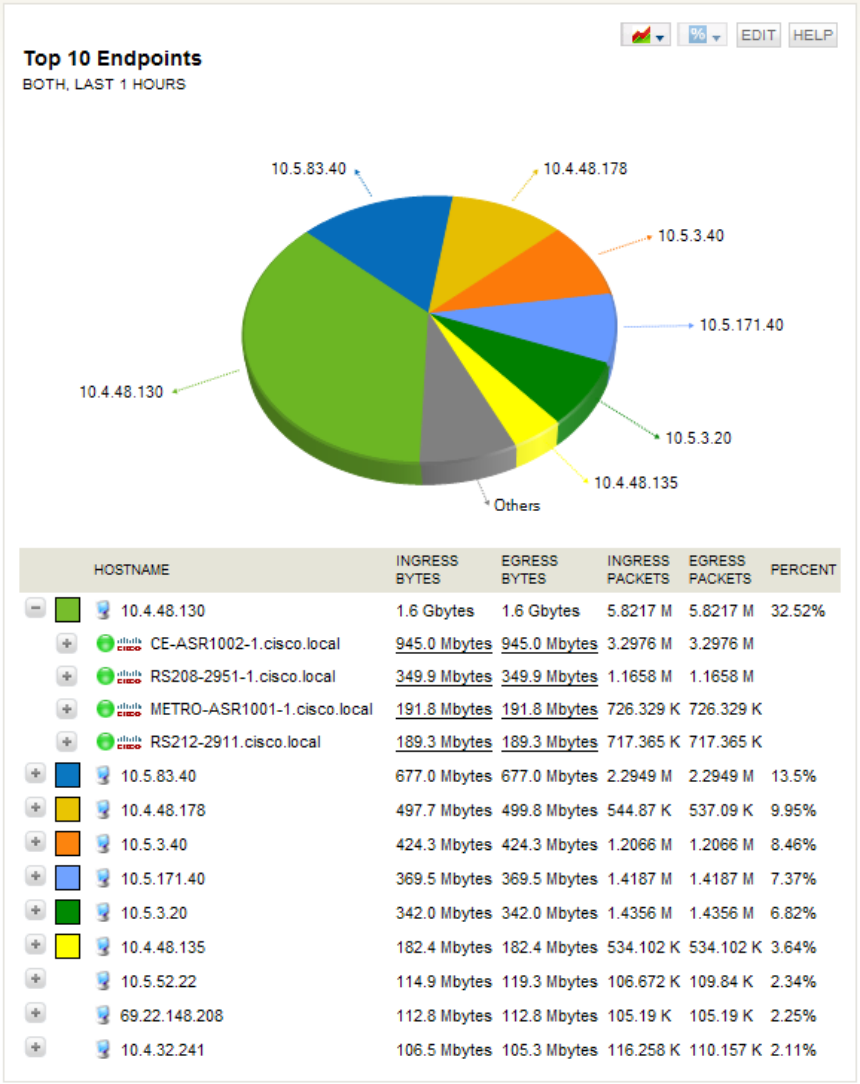
```
Router#show flow monitor Monitor-FNF cache sort counter bytes format table
Processed 57 flows
Aggregated to 57 flows
Showing the top 20 flows

IPV4 SRC ADDR    IPV4 DST ADDR    TRNS SRC PORT  TRNS DST PORT...
===============  ===============  =============  =============...
10.10.48.27      10.11.4.40             51128           2456...
10.11.4.40       10.10.48.27             2456          51128...
10.10.48.27      10.11.4.40             51124           2454...
10.11.4.40       10.10.48.27             2454          51124...
10.11.4.40       10.10.48.27             2457          51129...
.                .                          .              .
.                .                          .              .
.                .                          .              .
```

程序 3　查看来自NetFlow收集器的报告

本程序重点介绍了Plixer Scrutinizer和SolarWinds NTA提供的报告类型。

使用外部收集器的一个主要优势是能够汇聚从多个网络设备中收集的信息。一个出色的收集器能够查看从特定设备和接口收集的数据，并将从网络上多个设备和接口收集的数据进行关联。

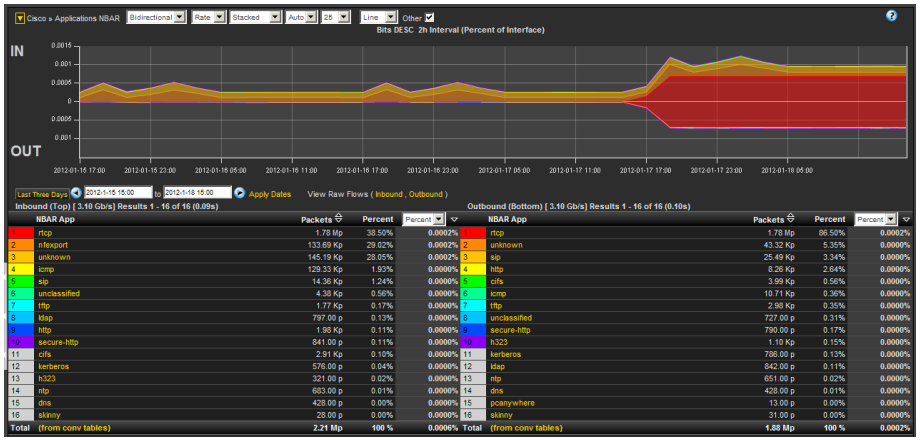
图 10 - SolarWinds NTA终端汇总



HOSTNAME	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
10.4.48.130	1.6 Gbytes	1.6 Gbytes	5.8217 M	5.8217 M	32.52%
CE-ASR1002-1.cisco.local	945.0 Mbytes	945.0 Mbytes	3.2976 M	3.2976 M	
RS208-2951-1.cisco.local	349.9 Mbytes	349.9 Mbytes	1.1658 M	1.1658 M	
METRO-ASR1001-1.cisco.local	191.8 Mbytes	191.8 Mbytes	726.329 K	726.329 K	
RS212-2911.cisco.local	189.3 Mbytes	189.3 Mbytes	717.365 K	717.365 K	
10.5.83.40	677.0 Mbytes	677.0 Mbytes	2.2949 M	2.2949 M	13.5%
10.4.48.178	497.7 Mbytes	499.8 Mbytes	544.87 K	537.09 K	9.95%
10.5.3.40	424.3 Mbytes	424.3 Mbytes	1.2066 M	1.2066 M	8.46%
10.5.171.40	369.5 Mbytes	369.5 Mbytes	1.4187 M	1.4187 M	7.37%
10.5.3.20	342.0 Mbytes	342.0 Mbytes	1.4356 M	1.4356 M	6.82%
10.4.48.135	182.4 Mbytes	182.4 Mbytes	534.102 K	534.102 K	3.64%
10.5.52.22	114.9 Mbytes	119.3 Mbytes	106.672 K	109.84 K	2.34%
69.22.148.208	112.8 Mbytes	112.8 Mbytes	105.19 K	105.19 K	2.25%
10.4.32.241	106.5 Mbytes	105.3 Mbytes	116.258 K	110.157 K	2.11%

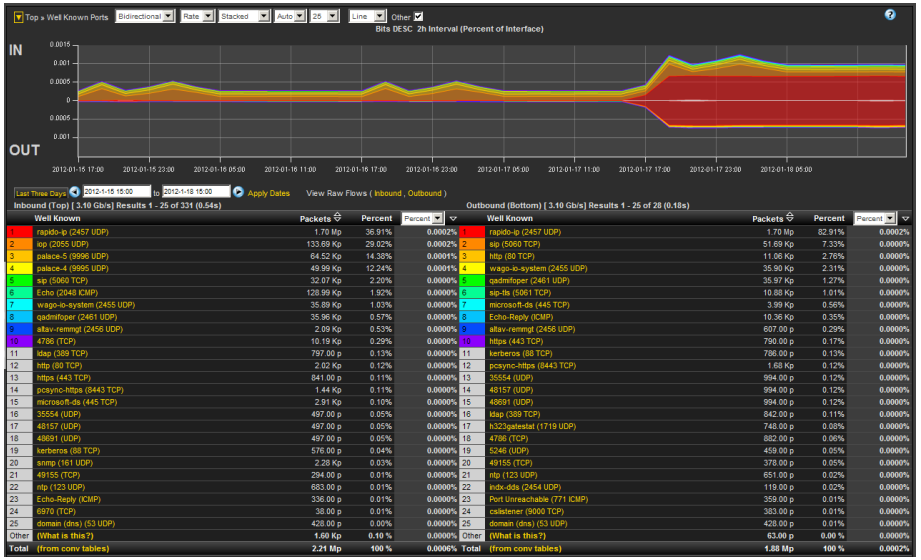
在网络设备本地缓存的NetFlow数据存在时间相对较短，通常在几分钟内就会被新的流代替。外部收集器是保留网络流量模式长期视图的关键。所使用的应用可以通过利用FNF和NBAR最准确地予以确定。

图 11 - Plixer Scrutinizer—应用NBAR报告 (72小时时间跨度)



要全面阐述NBAR值，以识别需要比较的应用，因为TNF只能通过使用TCP或UDP已知端口 (WKP) 来识别应用。由于Plixer支持FNF和NBAR以及TNF，您可以使用WKP生成相同的报告。

图 12 - Plixer Scrutinizer WKP报告 (72小时时间跨度)



主要区别在于，目前包括视频会议在内的许多应用都倾向于使用广泛的TCP或UDP端口，这些端口可在较大的已知范围内动态选择。各种WKP可能属于这些范围，但如果没有NBAR提供的额外应用认知，NetFlow收集器会错误地识别应

用。

NetFlow非常适用于识别、隔离和纠正网络问题，尤其是多台设备上所体现的配置问题，例如错误配置的QoS策略。您可以生成一份报告，过滤两个端点之间的各个对话。此类对话应使用特定的DSCP值进行双向标记，如RTP视频流。如果终端间路径上的任何中间设备不能一致地显示要正确标记的数据，则可能存在错误配置的设备。

图 13 - PlixerScrutinizer DSCP报告 (解决QoS信任边界问题的前/后)

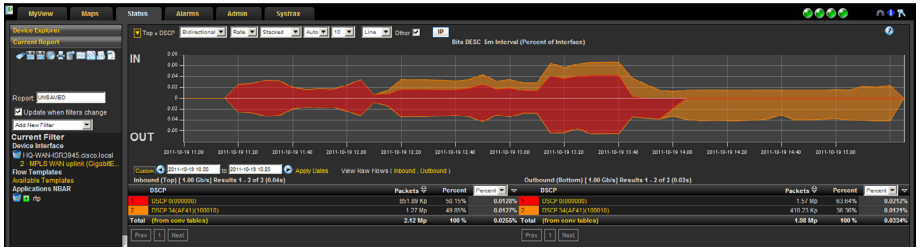


图13中显示的报告通过为总部广域网路由器选择DSCP报告而生成，并可过滤以仅显示RTP流量。该报告显示了采用DSCP 0进行错误标记的RTP。

这一问题可通过检查连接路由器与视频终端的局域网交换机之间的QoS信任边界来解决。发送并纠正这一问题后，报告会重新生成，以验证配置变更是否工作正常。此报告现在显示，RTP被正确标记为AF41 (DSCP 34) 。

备注

附录A: 产品列表

WAN 汇聚

功能区域	产品描述	产品编号	软件版本
WAN-汇聚路由器	Aggregation Services 1002 Router	ASR1002-5G-VPN/K9	IOS-XE 15.2(2)S Advanced Enterprise
	Aggregation Services 1001 Router	ASR1001-2.5G-VPNK9	
WAN-汇聚路由器	Cisco 3945 Security Bundle w/SEC license PAK	CISCO3945-SEC/K9	15.1(4)M4 securityk9, datak9
	Cisco 3925 Security Bundle w/SEC license PAK	CISCO3925-SEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	

WAN远端站点

功能区域	产品描述	产品编号	软件版本
模块化WAN远端站点路由器	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.1(4)M4 securityk9, datak9
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	
模块化WAN远端站点路由器	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9	15.1(4)M4 securityk9, datak9
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9	
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-K9	

功能区域	产品描述	产品编号	软件版本
模块化WAN远端站点路由器	1941 WAAS Express only Bundle	C1941-WAASX-SEC/K9	15.1(4)M4 securityk9, datak9
	Data Paper PAK for Cisco 1900 series	SL-19-DATA-K9	
固定端口WAN远端站点路由器	Cisco 881 SRST Ethernet Security Router with FXS FXO 802.11n FCC Compliant	C881SRST-K9	15.1(4)M4 securityk9, datak9

附录B: Show-Flow监控器完整输出

以下是**show flow monitor (显示流监控器)** 命令完整输出结果的示例。

```
HQ-WAN-ISR3945#show flow monitor Monitor-FNF-Basic cache sort counter bytes form table
Processed 57 flows
Aggregated to 57 flows
Showing the top 20 flows
```

IPV4 SRC ADDR	IPV4 DST ADDR	TRNS SRC PORT	TRNS DST PORT	INTF INPUT	FLOW DIRN	IP TOS	IP PROT	APP NAME	IPV4 NEXT HOP ADDR	IPV4 ID	IPV4 SRC PREFIX	IPV4 SRC MASK	IPV4 DST MASK	TCP FLAGS	INTF OUTPUT	BYTES	PKTS	TIME FIRST	TIME LAST	IP DSCP
10.10.48.27	10.11.4.40	51128	2456	FO32	INPUT	0x88	17	NBAR RTP	192.168.6.130	0	10.10.48.0	/24	/16	0x00	GI0/0	9295512	7407	11:50:25.751	11:51:20.119	0x22
10.11.4.40	10.10.48.27	2456	51128	GI0/0	INPUT	0x88	17	NBAR RTP	10.10.32.1	0	10.11.0.0	/16	/24	0x00	FO32	984272	816	11:51:14.731	11:51:20.103	0x22
10.10.48.27	10.11.4.40	51124	2454	FO32	INPUT	0x88	17	NBAR RTP	192.168.6.130	0	10.10.48.0	/24	/16	0x00	GI0/0	848448	2320	11:50:33.739	11:51:20.119	0x22
10.11.4.40	10.10.48.27	2454	51124	GI0/0	INPUT	0x88	17	NBAR RTP	10.10.32.1	0	10.11.0.0	/16	/24	0x00	FO32	336816	920	11:51:01.735	11:51:20.115	0x22
10.11.4.40	10.10.48.27	2457	51129	GI0/0	INPUT	0x88	17	NBAR RTCP	10.10.32.1	0	10.11.0.0	/16	/24	0x00	FO32	23280	193	11:51:01.811	11:51:20.111	0x22
10.10.48.27	10.11.4.40	51129	2457	FO32	INPUT	0x88	17	NBAR RTCP	192.168.6.130	0	10.10.48.0	/24	/16	0x00	GI0/0	8080	67	11:51:13.759	11:51:20.059	0x22
10.11.8.1	10.10.48.171	58822	2055	GI0/0	INPUT	0x00	17	NBAR NETFLOW V9	10.10.32.1	40417	10.11.0.0	/16	/24	0x00	FO32	7934	18	11:50:42.791	11:51:19.791	0x00
10.10.32.10	10.10.32.126	2048	2048	FO32	INPUT	0x00	17	NBAR UNKNOWN	0.0.0.0	24404	10.10.32.0	/25	/0	0x00	NULL	5952	31	11:50:49.787	11:51:19.779	0x00
10.11.0.1	10.10.48.170	59003	2055	GI0/0	INPUT	0x00	17	NBAR NETFLOW V9	10.10.32.1	29145	10.11.0.0	/16	/24	0x00	FO32	5416	22	11:50:22.995	11:51:16.003	0x00
10.11.4.40	10.10.48.27	2455	51125	GI0/0	INPUT	0x88	17	NBAR RTCP	10.10.32.1	0	10.11.0.0	/16	/24	0x00	FO32	1440	9	11:50:38.207	11:51:17.207	0x22
10.11.8.1	10.10.48.170	62188	2055	GI0/0	INPUT	0x00	17	NBAR NETFLOW V9	10.10.32.1	28853	10.11.0.0	/16	/24	0x00	FO32	1424	8	11:50:56.671	11:51:19.671	0x00
10.10.48.27	10.11.4.40	51128	2456	FO32	INPUT	0x88	17	NBAR UNCLASSIFIED	192.168.6.130	0	10.10.48.0	/24	/16	0x00	GI0/0	1416	1	11:51:14.787	11:51:14.787	0x22
10.10.48.27	10.11.4.40	51125	2455	FO32	INPUT	0x88	17	NBAR RTCP	192.168.6.130	0	10.10.48.0	/24	/16	0x00	GI0/0	1120	7	11:50:51.859	11:51:18.859	0x22
10.11.5.12	10.10.48.20	51241	5060	GI0/0	INPUT	0x60	6	NBAR SIP	10.10.32.1	28464	10.11.0.0	/16	/24	0x18	FO32	1029	3	11:51:10.103	11:51:10.107	0x18
10.11.13.51	10.10.48.20	52603	5060	GI0/0	INPUT	0x60	6	NBAR SIP	10.10.32.1	2678	10.11.0.0	/16	/24	0x18	FO32	962	2	11:51:15.003	11:51:15.007	0x18
10.11.13.50	10.10.48.20	44932	5060	GI0/0	INPUT	0x60	6	NBAR SIP	10.10.32.1	63844	10.11.0.0	/16	/24	0x18	FO32	919	3	11:51:05.323	11:51:05.331	0x18
10.10.48.147	10.10.32.254	54629	22	FO32	INPUT	0x00	6	PORT SSH	0.0.0.0	825	10.10.48.0	/24	/0	0x18	NULL	800	9	11:51:16.431	11:51:20.115	0x00
10.11.12.41	10.10.48.27	58388	5061	GI0/0	INPUT	0x00	6	NBAR 5061SIPTLS	10.10.32.1	29257	10.11.0.0	/16	/24	0x18	FO32	765	2	11:51:15.987	11:51:15.999	0x00
10.10.48.20	10.11.13.50	5060	44932	FO32	INPUT	0x60	6	NBAR SIP	192.168.6.130	40962	10.10.48.0	/24	/16	0x18	GI0/0	749	2	11:51:05.327	11:51:05.331	0x18
10.10.48.20	10.11.5.12	5060	51241	FO32	INPUT	0x60	6	NBAR SIP	192.168.6.130	28554	10.10.48.0	/24	/16	0x18	GI0/0	746	2	11:51:10.103	11:51:10.103	0x18

附录C: 支持NetFlow的设备配置

支持NetFlow的ASR1000系列路由器 (TNF和FNF)

广域网汇聚—MPLS CE路由器

```
version 15.2
service timestamps debug datetimemseclocaltime
service timestamps log datetimemseclocaltime
service password-encryption
no platform punt-keepalive disable-kernel-core
!
hostname CE-ASR1002-1
!
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
flow record Record-FNF
 description Flexible NetFlow with NBAR Flow 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
 match flow direction
 match application name
 collect routing source as
 collect routing destination as
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 id
 collect ipv4 source prefix
 collect ipv4 source mask
 collect ipv4 destination mask
 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 Export-FNF-Plixer
 description FNF v9
 destination 10.4.48.171
 source Loopback0
 transport udp 2055
 option interface-table
 option application-table
!
!
flow exporter Export-FNF-PrimeAM
 description FNF v9
 destination 10.4.48.180
 source Loopback0
 transport udp 9991
 option interface-table
 option application-table
!
!
flow exporter Export-FNF-LiveAction
 description FNF v9
 destination 10.4.48.178
 source Loopback0
 transport udp 2055
 option interface-table
 option application-table
!
!
flow exporter Export-FNF-SevOne
 description FNF v9
 destination 10.4.48.172
 source Loopback0
 transport udp 9996
 option interface-table
 option application-table
!
!
flow exporter Export-FNF-Lancope
 description FNF v9
 destination 10.4.48.174
 source Loopback0
 transport udp 2055
 option interface-table
 option application-table
!
!
flow exporter Export-TNF-Solarwinds
 description TNF v9
 destination 10.4.48.173
 source Loopback0
 transport udp 2055
!
!
flow monitor Monitor-FNF
 description FNF Traffic Analysis
 exporter Export-FNF-Plixer
 exporter Export-FNF-PrimeAM
 exporter Export-FNF-LiveAction
 exporter Export-FNF-Lancope
 exporter Export-FNF-SevOne
 cache timeout active 60
 cache entries 200000
 record Record-FNF
!
!
flow monitor Monitor-TNF
 description TNF Traffic Analysis
 exporter Export-TNF-Solarwinds
 cache timeout active 60
 cache entries 200000
 record netflow ipv4 original-input
!
!
!
```

```
!
ip domain name cisco.local
ip multicast-routing distributed
!
!
!
ipwccp source-interface Loopback0
ipwccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAE
password 7 141443180F0B7B7977
ipwccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAE
password 7 104D580A061843595F
!
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
username admin password 7 0205554808095E731F
!
redundancy
 mode none
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
 match dscp af21
class-map match-any BGP-ROUTING
 match protocol bgp
class-map match-any INTERACTIVE-VIDEO
 match dscp cs4  af41
class-map match-any CRITICAL-DATA
 match dscp cs3  af31
class-map match-any VOICE
 match dscpef
class-map match-any SCAVENGER
 match dscp cs1  af11
class-map match-any NETWORK-CRITICAL
 match dscp cs2  cs6
!
policy-map MARK-BGP
 class BGP-ROUTING
  set dscp cs6
policy-map WAN
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
   service-policy MARK-BGP
 class class-default
  bandwidth percent 25
  random-detect
policy-map WAN-INTERFACE-G0/0/3
```

```
 class class-default
  shape average 300000000
   service-policy WAN
!
!
!
interface Loopback0
 ip address 10.4.32.241 255.255.255.255
ippim sparse-mode
!
interface Port-channel1
 ip address 10.4.32.2 255.255.255.252
ipwccp 61 redirect in
ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-TNF output
ippim sparse-mode
 no negotiation auto
 !
interface GigabitEthernet0/0/0
 description WAN-D3750X Gig1/0/1
 no ip address
 negotiation auto
cdp enable
 channel-group 1 mode active
!
interface GigabitEthernet0/0/1
 description WAN-D3750X Gig2/0/1
 no ip address
 negotiation auto
 channel-group 1 mode active
!
interface GigabitEthernet0/0/2
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/3
 description MPLS PE router
 bandwidth 300000
 ip address 192.168.3.1 255.255.255.252
ipwccp 62 redirect in
ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF output
 ip flow monitor Monitor-TNF output
 negotiation auto
 !
interface GigabitEthernet0
vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
!
router eigrp 100
 distribute-list route-map BLOCK-TAGGED-ROUTES in
 default-metric 300000 100 255 1 1500
 network 10.4.0.0 0.1.255.255
 redistribute bgp 65511
 passive-interface default
 no passive-interface Port-channel1
eigrp router-id 10.4.32.241
!
router bgp 65511
bgp router-id 10.4.32.241
bgp log-neighbor-changes
 network 0.0.0.0
 network 192.168.3.0 mask 255.255.255.252
 redistribute eigrp 100
 neighbor 10.4.32.242 remote-as 65511
 neighbor 10.4.32.242 update-source Loopback0
 neighbor 10.4.32.242 next-hop-self
 neighbor 192.168.3.2 remote-as 65401
!
```

```
ip forward-protocol nd
!
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ippimautorp listener
ippim register-source Loopback0
ip tacacs source-interface Loopback0
!
ip access-list standard WAE
 permit 10.4.32.162
 permit 10.4.32.161
!
ip access-list extended WAAS-REDIRECT-LIST
 deny   tcp any anyeq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any anyeq telnet
 deny   tcp any eqtacacs any
 deny   tcp any anyeq tacacs
 deny   tcp any eqbgp any
 deny   tcp any anyeqbgp
 deny   tcp any anyeq 123
 deny   tcp any eq 123 any
 permit tcp any any
!
ip sla responder
logging 10.4.48.35
access-list 55 permit 10.4.48.0 0.0.0.255
!
route-map BLOCK-TAGGED-ROUTES deny 10
 match tag 65401 65402 65512
!
route-map BLOCK-TAGGED-ROUTES permit 20
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
snmp-server trap-source Loopback0
!
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 01200307490E12242455
!
!
control-plane
!
!
line con 0
 logging synchronous
stopbits 1
line aux 0
stopbits 1
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
ntp source Loopback0
ntp server 10.4.48.17
!
end
```

支持NetFlow的ISR-G2系列路由器 (TNF和FNF)

带接入层的远程站点(RS201)

```
version 15.1
service timestamps debug datetimemseclocaltime
service timestamps log datetimemseclocaltime
service password-encryption
!
hostname RS201-2911
!
```

```
boot-start-marker
boot system flash:c2900-universalk9-mz.SPA.151-4.M4.bin
boot-end-marker
!
!
enable secret 5 $1$Rmfp$Btut/0xCUYDOmlruhEsPt1
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authentication login MODULE none
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
ipv6 spd queue min-threshold 62
ipv6 spd queue max-threshold 63
!
flow record Record-FNF
 description Flexible NetFlow with NBAR Flow 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
 match flow direction
 match application name
 collect routing source as
 collect routing destination as
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 id
 collect ipv4 source prefix
 collect ipv4 source mask
 collect ipv4 destination mask
 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 Export-TNF-Solarwinds
 description TNF v9
 destination 10.4.48.173
 source Loopback0
 output-features
 transport udp 2055
!
!
flow exporter Export-FNF-Plixer
 description FNF v9
 destination 10.4.48.171
 source Loopback0
 output-features
 transport udp 2055
 option interface-table
 option application-table
```

```
!
!
flow exporter Export-FNF-PrimeAM
 description FNF v9
 destination 10.4.48.180
 source Loopback0
 output-features
 transport udp 9991
 option interface-table
 option application-table
!
!
flow exporter Export-FNF-LiveAction
 description FNF v9
 destination 10.4.48.178
 source Loopback0
 output-features
 transport udp 2055
 option interface-table
 option application-table
!
!
flow exporter Export-FNF-SevOne
 description FNF v9
 destination 10.4.48.172
 source Loopback0
 output-features
 transport udp 9996
 option interface-table
 option application-table
!
!
flow exporter Export-FNF-Lancope
 description FNF v9
 destination 10.4.48.174
 source Loopback0
 output-features
 transport udp 2055
 option interface-table
 option application-table
!
!
flow monitor Monitor-TNF
 description TNF Traffic Analysis
 record netflow ipv4 original-input
 exporter Export-TNF-Solarwinds
 cache timeout active 60
!
!
flow monitor Monitor-FNF
 description FNF Traffic Analysis
 record Record-FNF
 exporter Export-FNF-SevOne
 exporter Export-FNF-Lancope
 exporter Export-FNF-LiveAction
 exporter Export-FNF-PrimeAM
 exporter Export-FNF-Plixer
 cache timeout active 60
!
ip source-route
ipauth-proxy max-login-attempts 5
ip admission max-login-attempts 5
ipcef
!
!
!
ipvrf INET-PUBLIC1
rd 65512:1
!
ip multicast-routing
!
!
ip domain name cisco.local
ip name-server 10.4.48.10
```

```
ipwccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAE
password 7 110A4816141D5A5E57
ipwccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAE
password 7 130646010803557878
!
multilink bundle-name authenticated
!
!
!
!
voice-card 0
!
!
!
!
!
!
!
license udipid CISCO2911/K9 sn FTX1347A1TN
license boot module c2900 technology-package datak9
hw-module sm 1
!
!
!
username admin password 7 04585A150C2E1D1C5A
!
redundancy
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
 match  dscp af21
class-map match-any BGP-ROUTING
 match protocol bgp
class-map match-any INTERACTIVE-VIDEO
 match  dscp cs4  af41
class-map match-any CRITICAL-DATA
 match  dscp cs3  af31
class-map match-any VOICE
 match  dscpef
class-map match-any SCAVENGER
 match  dscp cs1  af11
class-map match-any NETWORK-CRITICAL
 match  dscp cs2  cs6
!
!
policy-map MARK-BGP
 class BGP-ROUTING
  set dscp cs6
policy-map WAN
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
  service-policy MARK-BGP
 class class-default
  bandwidth percent 25
  random-detect
policy-map WAN-INTERFACE-G0/0/0
 class class-default
```

```
  shape average 10000000
  service-policy WAN
policy-map WAN-INTERFACE-G0/0
 class class-default
  shape average 10000000
  service-policy WAN
!
!
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
encraes 256
 authentication pre-share
 group 2
!
crypto isakmpkeepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
keyring DMVPN-KEYRING1
   match identity address 0.0.0.0 INET-PUBLIC1
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE1
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
!
!
!
interface Loopback0
 ip address 10.255.251.201 255.255.255.255
ippim sparse-mode
!
interface Tunnel10
 bandwidth 10000
 ip address 10.4.34.201 255.255.254.0
 no ip redirects
ipmtu 1400
ipwccp 62 redirect in
ippimdr-priority 0
ippimnbma-mode
ippim sparse-mode
ip hello-interval eigrp 200 20
ip hold-time eigrp 200 60
ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-TNF output
 ip flow monitor Monitor-FNF output
ipnhrp authentication cisco123
ipnhrp map multicast 172.16.130.1
ipnhrp map 10.4.34.1 172.16.130.1
ipnhrp network-id 101
ipnhrpholdtime 600
ipnhrpnhs 10.4.34.1
ipnhrp registration no-unique
ipnhrp shortcut
ipnhrp redirect
iptcp adjust-mss 1360
ip summary-address eigrp 200 10.5.40.0 255.255.248.0
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC1
 tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Port-channel1
 description EtherChannel link to RS201-A2960S
 no ip address
 hold-queue 150 in
!
interface Port-channel1.64
 description Wired Data
```

```
 encapsulation dot1Q 64
 ip address 10.5.44.1 255.255.255.0
 ip helper-address 10.4.48.10
ipwccp 61 redirect in
ippim sparse-mode
ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-TNF output
 ip flow monitor Monitor-FNF output
!
interface Port-channel1.65
 description Wireless Data
 encapsulation dot1Q 65
 ip address 10.5.42.1 255.255.255.0
 ip helper-address 10.4.48.10
ipwccp 61 redirect in
ippim sparse-mode
!
interface Port-channel1.69
 description Wired Voice
 encapsulation dot1Q 69
 ip address 10.5.45.1 255.255.255.0
 ip helper-address 10.4.48.10
ippim sparse-mode
ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-TNF output
 ip flow monitor Monitor-FNF output
!
interface Port-channel1.70
 description Wireless Voice
 encapsulation dot1Q 70
 ip address 10.5.43.1 255.255.255.0
 ip helper-address 10.4.48.10
ippim sparse-mode
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 bandwidth 10000
 ip address 192.168.3.21 255.255.255.252
ipwccp 62 redirect in
ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-TNF output
 ip flow monitor Monitor-FNF output
iptcp adjust-mss 1360
 duplex auto
 speed auto
 no cdp enable
 service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
 description RS201-A2960S Gig2/0/24
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface GigabitEthernet0/2
 description RS201-A2960S Gig1/0/24
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface GigabitEthernet0/0/0
ipvrf forwarding INET-PUBLIC1
 ip address dhcp
 ip access-group ACL-INET-PUBLIC in
 duplex auto
 speed auto
```

```
 no cdp enable
 service-policy output WAN-INTERFACE-G0/0/0
!
interface SM1/0
 ip address 192.0.2.2 255.255.255.252
 service-module external ip address 10.5.44.8 255.255.255.0
 !Application: Restarted at Wed Jun  6 21:07:33 2012
 service-module ip default-gateway 10.5.44.1
!
interface SM1/1
 description Internal switch interface connected to Service
Module
 no ip address
 shutdown
!
interface Vlan1
 no ip address
!
!
!
router eigrp 200
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
eigrp router-id 10.255.251.201
eigrp stub connected summary
!
router bgp 65511
bgp router-id 10.255.251.201
bgp log-neighbor-changes
 network 10.5.44.0 mask 255.255.255.0
 network 10.5.45.0 mask 255.255.255.0
 network 10.255.251.201 mask 255.255.255.255
 network 192.168.3.20 mask 255.255.255.252
 aggregate-address 10.5.40.0 255.255.248.0 summary-only
 neighbor 192.168.3.22 remote-as 65401
!
ip forward-protocol nd
!
ippimautorp listener
ippim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
ip access-list standard WAE
 permit 10.5.44.8
!
ip access-list extended ACL-INET-PUBLIC
 permit udp any anyeq non500-isakmp
 permit udp any anyeqisakmp
 permit esp any any
 permit udp any anyeqbootpc
 permit icmp any any echo
 permit icmp any any echo-reply
 permit icmp any anyttl-exceeded
 permit icmp any any port-unreachable
 permit udp any anygt 1023 ttleq 1
ip access-list extended WAAS-REDIRECT-LIST
 deny   tcp any anyeq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any anyeq telnet
 deny   tcp any eqtacacs any
 deny   tcp any anyeq tacacs
 deny   tcp any eqbgp any
 deny   tcp any anyeqbgp
 deny   tcp any anyeq 123
 deny   tcp any eq 123 any
```

```
 permit tcp any any
!
ip sla responder
logging 10.4.48.35
access-list 55 permit 10.4.48.0 0.0.0.255
access-list 67 permit 192.0.2.2
!
!
!
!
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 0538030C33495A221C1C
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
 shutdown
!
!
!
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line 67
 access-class 67 in
 login authentication MODULE
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
 access-class 55 in
 transport preferred none
 transport input ssh
line vty 5 15
 access-class 55 in
 transport preferred none
 transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
end
```

带分布层的远程站点(RS200)

```
version 15.1
service timestamps debug datetimemseclocaltime
service timestamps log datetimemseclocaltime
service password-encryption
```

```
!
hostname RS200-3925-1
!
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
crypto pki token default removal timeout 0
!
no ipv6 cef
ipv6 spd queue min-threshold 62
ipv6 spd queue max-threshold 63
!
flow record Record-FNF
 description Flexible NetFlow with NBAR Flow 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
 match flow direction
 match application name
 collect routing source as
 collect routing destination as
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 id
 collect ipv4 source prefix
 collect ipv4 source mask
 collect ipv4 destination mask
 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 Export-FNF-Plixer
 description FNF v9
 destination 10.4.48.171
 source Loopback0
 output-features
 transport udp 2055
 option interface-table
 option application-table
!
!
flow exporter Export-FNF-PrimeAM
 description FNF v9
 destination 10.4.48.180
 source Loopback0
 output-features
 transport udp 9991
```

```
 option interface-table
 option application-table
!
!
flow exporter Export-FNF-LiveAction
 description FNF v9
 destination 10.4.48.178
 source Loopback0
 output-features
 transport udp 2055
 option interface-table
 option application-table
!
!
flow exporter Export-FNF-SevOne
 description FNF v9
 destination 10.4.48.172
 source Loopback0
 output-features
 transport udp 9996
 option interface-table
 option application-table
!
!
flow exporter Export-FNF-Lancope
 description FNF v9
 destination 10.4.48.174
 source Loopback0
output-features
 transport udp 2055
 option interface-table
 option application-table
!
!
flow monitor Monitor-FNF
 description FNF Traffic Analysis
 record Record-FNF
 exporter Export-FNF-SevOne
 exporter Export-FNF-Lancope
 exporter Export-FNF-LiveAction
 exporter Export-FNF-PrimeAM
 exporter Export-FNF-Plixer
 cache timeout active 60
!
ip source-route
ipcef
!
!
!
ip multicast-routing
!
!
ip domain name cisco.local
ipwccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAE
password 7 0508571C22431F5B4A
ipwccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAE
password 7 130646010803557878
!
multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
!
!
!
!
!
license udipid C3900-SPE100/K9 sn FOC14415C5Q
hw-module sm 2
```

```
!
!
!
username admin password 7 070C705F4D06485744
!
redundancy
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
 match  dscp af21
class-map match-any BGP-ROUTING
 match protocol bgp
class-map match-any INTERACTIVE-VIDEO
 match  dscp cs4  af41
class-map match-any CRITICAL-DATA
 match  dscp cs3  af31
class-map match-any VOICE
 match  dscpef
class-map match-any SCAVENGER
 match  dscp cs1  af11
class-map match-any NETWORK-CRITICAL
 match  dscp cs2  cs6
!
!
policy-map MARK-BGP
 class BGP-ROUTING
  set dscp cs6
policy-map WAN
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
  service-policy MARK-BGP
 class class-default
  bandwidth percent 25
  random-detect
policy-map WAN-INTERFACE-G0/0
 class class-default
  shape average 25000000
  service-policy WAN
!
!
!
interface Loopback0
 ip address 10.255.251.200 255.255.255.255
ippim sparse-mode
!
interface Port-channel1
 description EtherChannel link to RS200-D3750X
 no ip address
 hold-queue 150 in
!
interface Port-channel1.50
 description R1 routed link to distribution layer
 encapsulation dot1Q 50
 ip address 10.5.0.1 255.255.255.252
ipwccp 61 redirect in
ippim sparse-mode
ip flow monitor Monitor-FNF input
```

```
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF output
 ip flow monitor Monitor-TNF output
 !
interface Port-channel1.99
 description Transit net
 encapsulation dot1Q 99
 ip address 10.5.0.9 255.255.255.252
ippim sparse-mode
ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF output
 ip flow monitor Monitor-TNF output
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 bandwidth 50000
 ip address 192.168.3.17 255.255.255.252
ipwccp 62 redirect in
ip flow monitor Monitor-FNF input
 ip flow monitor Monitor-TNF input
 ip flow monitor Monitor-FNF output
 ip flow monitor Monitor-TNF output
 duplex auto
 speed auto
 no cdp enable
 service-policy output WAN-INTERFACE-G0/0
 !
interface GigabitEthernet0/1
 description RS200-D3750X Gig2/0/23
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface GigabitEthernet0/2
 description RS200-D3750X Gig1/0/23
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface SM2/0
 ip address 10.5.0.17 255.255.255.252
 service-module ip address 10.5.0.18 255.255.255.252
 !Application: running
 service-module ip default-gateway 10.5.0.17
!
interface SM2/1
 description Internal switch interface connected to Service
Module
 no ip address
!
interface Vlan1
 no ip address
!
!
router eigrp 100
 default-metric 25000 100 255 1 1500
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute bgp 65511
 passive-interface default
 no passive-interface Port-channel1.50
 no passive-interface Port-channel1.99
eigrp router-id 10.255.251.200
!
router bgp 65511
bgp router-id 10.255.251.200
bgp log-neighbor-changes
 network 10.5.1.0 mask 255.255.255.0
```

```
 network 10.5.2.0 mask 255.255.255.0
 network 10.5.3.0 mask 255.255.255.0
 network 10.5.4.0 mask 255.255.255.0
 network 10.255.251.200 mask 255.255.255.255
 network 192.168.3.16 mask 255.255.255.252
 network 192.168.3.17 mask 255.255.255.255
 aggregate-address 10.5.0.0 255.255.248.0 summary-only
 neighbor 192.168.3.18 remote-as 65401
!
ip forward-protocol nd
!
ippimautorp listener
ippim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Loopback0
!
ip access-list standard WAE
 permit 10.5.7.8
 permit 10.5.7.9
!
ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Redirect List
 deny   tcp any anyeq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any anyeq telnet
 deny   tcp any eqtacacs any
 deny   tcp any anyeq tacacs
 deny   tcp any eqbgp any
 deny   tcp any anyeqbgp
 deny   tcp any anyeq 123
 deny   tcp any eq 123 any
 permit tcp any any
!
ip sla responder
logging 10.4.48.35
!
!
!
!
nlsresp-timeout 1
cpdcr-id 1
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 04680E051D2458650C00
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
 shutdown
!
!
!
line con 0
 logging synchronous
line aux 0
```

```
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line 131
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
end
```

备注

附录D: 变更

本附录总结了相比先前的思科IBA智能业务平台系列，本指南所做的变更。

- 我们增添了思科ASR1000系列路由器作为广域网汇聚路由器。
- 我们增添了额外的NetFlow收集器应用。

备注

反馈

点击 这里 提供反馈到IBA

本手册中的所有设计、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,或与交易过程、使用或贸易惯例相 关的保证。在任何情况下,思科及其供应商对任何间接的、特殊的、继发的或偶然性的损害均不承担责任,包括但不限于由于使用或未能使用本手册所造成的利润损失或数据丢失或损害,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。用户对于这些设计的使用负有全部责任。这些设计不属于思科、供应商或合作伙伴的技术建议或其它专业建议。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。

文中使用的任何互联网协议(IP)地址均非真实地址。文中的任何举例、命令显示输出和图示仅供说明之用。在图示中使用任何真实IP 地址均属无意和巧合。

© 2012 思科系统公司。保留所有权利。

美国总部
Cisco Systems, Inc.
San Jose, CA

亚太总部
Cisco Systems (USA) Pte. Ltd.
Singapore

欧洲总部
Cisco Systems International BV Amsterdam,
The Netherlands

思科在全球拥有超过200家办公室。地址，电话号码和传真在思科网站中列出： www.cisco.com/go/offices。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)