IPv6互联网边缘部署指南

智能业务平台

修订版：2011年下半年

前言

本指南是一份思科®智能业务平台（IBA）指南。

本指南的目标受众

本指南主要面向承担以下职务的人员：

- 需要实施解决方案时的标准规范的系统工程师
- 需要获取参考资料以撰写思科IBA实施项目工作说明书的项目经理
- 需要借助产品指南销售新技术或撰写自己的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指南作为工程师之间技术交流、项目实施经验分享的统一指导文件，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

思科每年对IBA指南进行两次更新和修订。在发布思科IBA指南系列之前，我们将在IBA实验室对其进行整体评测。为确保思科IBA指南中各个设计之间的兼容性，您应使用同一IBA系列中的设计指南文档。

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。指南系列的命名方式如下：

- 年2月指南系列
- 年8月指南系列

其中的年表示发布该指南系列的公历年度。

您可以在以下网址查看最新的思科IBA指南系列：
客户访问：http://www.cisco.com/go/cn/iba
合作伙伴访问：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
```

问题和评论

如需要了解更多有关思科IBA智能业务平台的信息，请访问
http://www.cisco.com/go/cn/iba

如需要注册快速报价工具（QPT），请访问
http://www.cisco.com/go/qpt

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

本IBA指南的内容 1
- 关于IBA 1
- 关于本指南 1

简介 2
- 业务概述 2
- 技术概述 2

部署详情 4
- 配置Cisco ASA，提供到ISP的IPv6连接 5
- 将Cisco ASA配置为允许访问IPv6 Web服务器 10
- 配置ASA将IPv6流量传送至IPS 15
- 为IPv6配置主机 19
- 域名服务 21

附录A：产品列表 23

附录B：CLI配置 24
- ASA 24
- IPS 27

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。

© 2011 思科系统公司。保留所有权利。

本IBA指南的内容

关于IBA

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。

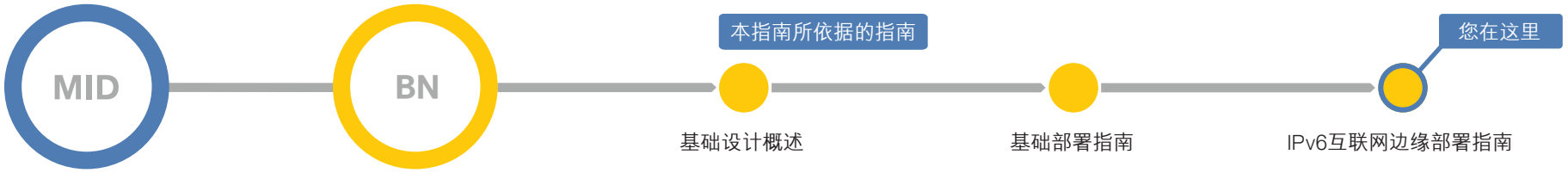
思科IBA在一个综合解决方案中集成了局域网、广域网、无线、安全、数据中心、应用优化和统一通信技术，并对其进行了严格测试，确保能够实现无缝协作。IBA采用的组件式方法简化了在采用多种技术时通常需要进行的系统集成工作，使您可以随意选择能够满足组织需求的解决方案，而不必担心技术复杂性方面的问题。

关于本指南

本指南是一份附加设计概述，包含如下内容：

- **业务概述** —— 描述了本指南中提出的解决方案的应用案例和应用价值。这一章节的内容对业务决策者尤为重要。
- **技术概述** —— 描述了支持该应用案例的技术解决方案，包括对构成此解决方案的思科产品的介绍。技术决策者可以利用此章节的内容了解解决方案的工作原理。
- **部署详情** —— 详细描述具体的部署步骤，指导您部署和配置思科IBA解决方案。系统工程师可以在这些步骤的指导下快速、可靠地配置和启用解决方案。

在成功部署路线图上，附加设计概述总是紧随基础设计概述之后，如下所示。



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——即上面路线图中本指南左侧的所有指南。所有以本指南为依据的指南都在右侧。

如需要了解更多有关思科IBA智能业务平台的信息，请访问：
http://www.cisco.com/go/cn/iba
如需要注册快速报价工具（QPT），请访问：
http://www.cisco.com/go/qpt

简介

业务概述

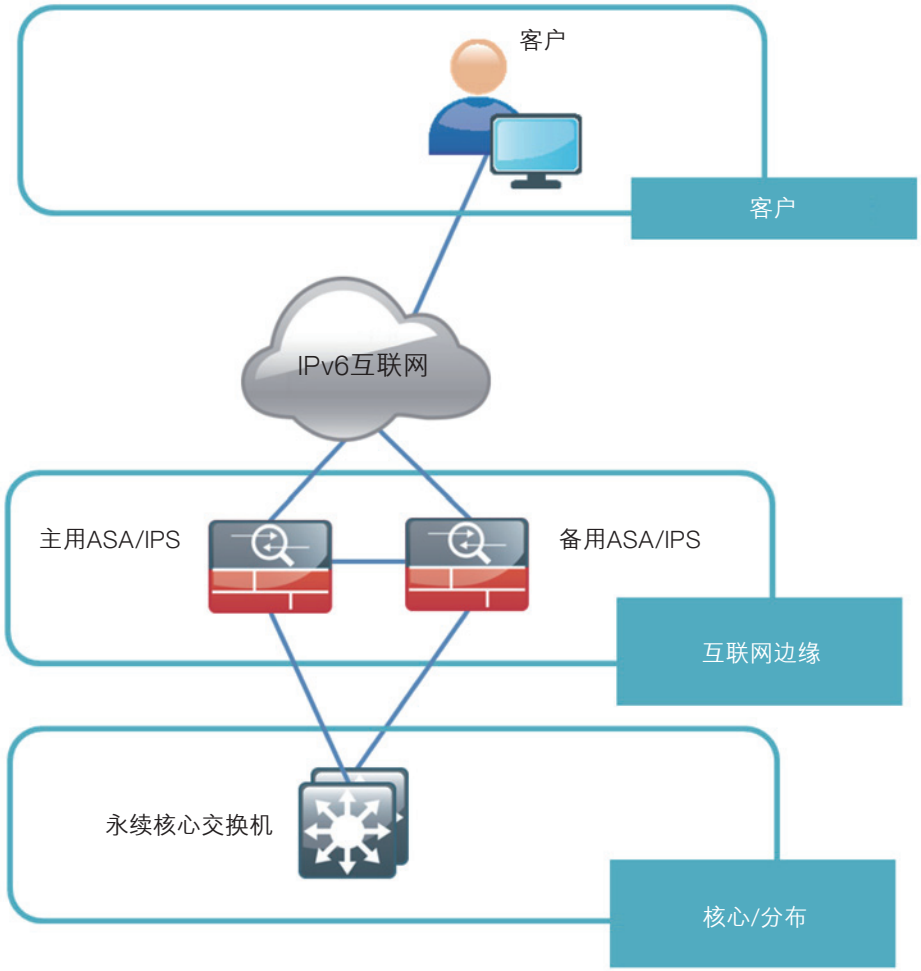
现在，IPv4地址在几乎一切事物中得到了史无前例的广泛应用，包括智能电话、平板电脑、电脑、摄像机和智能电表等。IPv4地址分配目前已几乎达到极限，新的地址很难找到，并且在未来几年内将不再可用。IPv4地址的耗尽成为大多数IPv6部署的主要推动力。相比之下，IPv6能够提供大得多的地址空间。

企业必须为最终迁移到IPv6互联网做好准备。尽管IPv4目前可能一切良好，并且仍然统治着互联网，但它无疑无法在未来保持这一趋势。虽然如今大多数客户交互都是通过IPv4实现的，但世界的某些地区已经开始向IPv6迁移，并且这一现象将很快扩展到全球。许多政府强制规定在政府、教育和公共互联网部署中使用IPv6。企业也不希望错过与采用全新IPv6互联网的客户和合作伙伴进行交流的机会。在继续使用现有IPv4网络的同时规划和实施IPv6，将能够帮助避免在这一迁移过程中错失市场机遇。这意味着企业的互联网边缘不仅要能够支持现有的IPv4客户，同时还要能够支持全新的IPv6客户。

技术概述

思科IBA智能业务平台能够轻松支持贵企业的IPv6互联网边缘客户端。本指南描述了贵企业如何能够立足于技术发展的前沿，在IPv6的基础上构建企业网络的同时，仍继续为您的IPv4客户提供接入支持。双堆栈设计将能够支持IPv4与IPv6在迁移过程中实现共存。

图1. 逻辑架构



本指南描述了如何使用现有的硬件（详细介绍见《基础部署指南》）来提供新的配置，支持IPv6。

您可以通过渐进式配置变更，在思科IBA智能业务平台无边界互联网基础上添加IPv6互联网边缘。在这一过程中需要进行额外配置，同时用于现有IPv4基础的现有软件也要能够支持IPv6配置。IPv4和IPv6网络将共存于同一设备上，但在逻辑上相互独立。

IPv4在未来多年内将会继续使用。在迁移到IPv6的过程中，同时支持这两种地址空间对于企业的发展至关重要。此处介绍的配置在预先存在的IPv4配置上构建了一个IPv6基础

设施。这一配置将无法作为一个独立的设置进行工作。

本指南描述的解决方案能够支持IPv6 Web流量，特别是进出互联网边缘的HTTP/HTTPS Web流量。此解决方案假定：

- 互联网服务提供商（ISP）配置了一个以太网切换(handoff)，具有到隔离区（DMZ）中思科系统以太网交换机的IPv6连接。
- 互联网边缘路由器位于提供商网络中，不属于此配置的一部分。
- 互联网边缘路由器将拥有一个静态路由，将IPv6流量导向企业的ASA。
- 来自ISP边界路由器的IPv6连接将在一对稳定可靠的Cisco ASA防火墙上终止。

Cisco ASA设备提供了以下功能：

- 端接ISP IPv6连接
- 到提供商网络的静态IPv6缺省路由
- 基于IPv6访问列表的安全性
- 为IPv6 DMZ中的服务器提供IPv6入侵防御支持

您还必须将贵企业针对IPv6的安全策略考虑在内。在边界安全方面，IPv6与IPv4并无不同。您在部署前必须制定安全策略和计划。在《基础部署指南》中介绍的有效IPv4安全策略可沿用至IPv6网络。这一设计配置了支持HTTP和HTTPS的访问控制列表。针对ICMP的配置仅用于初始故障排除，应在配置完成后移除。

如需了解有关IPv6的更多信息，我们建议阅读以下出版物：

- 《IPv6安全性》(IPv6 Security)，思科出版物，2008年出版
- 《面向企业网络的IPv6》(IPv6 for Enterprise Networks)，思科出版物，2011年出版

备注

部署详情

当前在基础架构中配置的Cisco ASA设备采用IPv4进行配置和管理。这一点在本配置中将保持不变。针对IPv4的IPv4管理和故障切换配置将保持不变。本部署并非一个独立设置。现有的IPv4基础架构提供了IPv4连接、高可用性和管理功能。

IPv6编址基础知识

IPv6编址设计考虑事项在《思科IBA智能业务平台IPv6地址指南》中有相关介绍。下文是一个简要概述，介绍了可在本文中找到的IPv6编址上下文环境。

IPv6使用以冒号(:)分隔的16字节16进制地址段，来表示128位地址格式，使地址表达更简化、更不易于出错。以下是一个有效IPv6地址的示例：2001:db8:130F:0000:0000:09C0:876A:130B。

地址字段中的前导零位可选，且能够压缩。例如：以下16进制地址能以压缩格式表达：

示例1：2001:db8:130F:0000:0000:09C0:876A:130B =2001:db8:130F:0:0:9C0:876A:130B (压缩格式)

一对冒号（::）能够表示相连的0字段。但是，在一个有效的IPv6地址中，只允许使用一次冒号对。

示例1：2001:db8:130F:0:0:9C0:876A:130B =2001:db8:130F::9C0:876A:130B (压缩格式)

/前缀长度变量是一个十进制数值，表示构成前缀的地址高阶连续位的数目，是地址的网络部分。例如：2001:db8:8086:6502::/64是一个正确的IPv6前缀。本设计中的所有前缀均为64位。

服务提供商指派给企业的前缀通常为48位。这使得企业可以为网络指派65,536个64位前缀。针对本部署，我们建议所有网络均使用64位前缀，包括互联网服务提供商连接和DMZ服务器子网。

推荐的IPv6互联网边缘部署设置

IPv6配置要求您的ISP提供地址空间。本示例使用了2001:0DB8::/32，这是一个不可路由的地址范围，仅用于文档目的[RFC3849]。

对于本文中提及的配置参考，您可以使用下图。您可以将下一页打印出来以便参考。

图2. IPv6互联网边缘部署架构

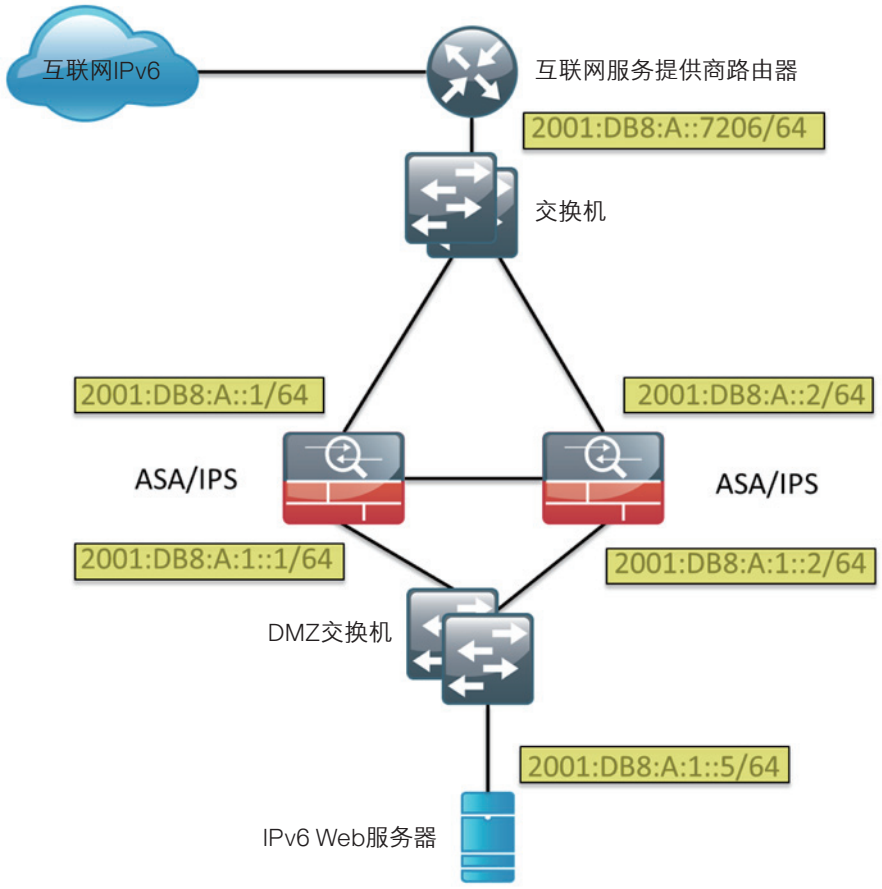


表1. 针对本配置的IPv6地址

端点	IPv6地址
客户点到点链路的ISP端	2001:DB8:A::7206/64
点到点链接的客户终端，主用Cisco ASA	2001:DB8:A::1/64
点到点链接的客户终端，备用Cisco ASA	2001:DB8:A::2/64
Cisco ASA Web DMZ地址，主用Cisco ASA	2001:DB 8: A :1::1/64
Cisco ASA Web DMZ地址，备用Cisco ASA	2001:DB8:A:1::2/64
DMZ中的Web服务器	2001:DB8:A:1::5/64

流程

配置Cisco ASA，提供到ISP的IPv6连接

1. 为IPv6配置外部接口
2. 为IPv6配置高可用性
3. 配置IPv6静态路由

程序1　为IPv6配置外部接口

Cisco ASA根据基础架构中的配置规程进行配置和传输IPv4流量。在进行配置变更时必须格外谨慎，以免中断IPv4流量。了解并确认您在ASDM中的位置。此处我们将对活动的接口进行变更。注意不要改变IPv4配置。

步骤1：使用在针对IPv4的基础设置中曾使用的用户名和密码，登录Cisco ASA设备管理器（ASDM）。

技术提示

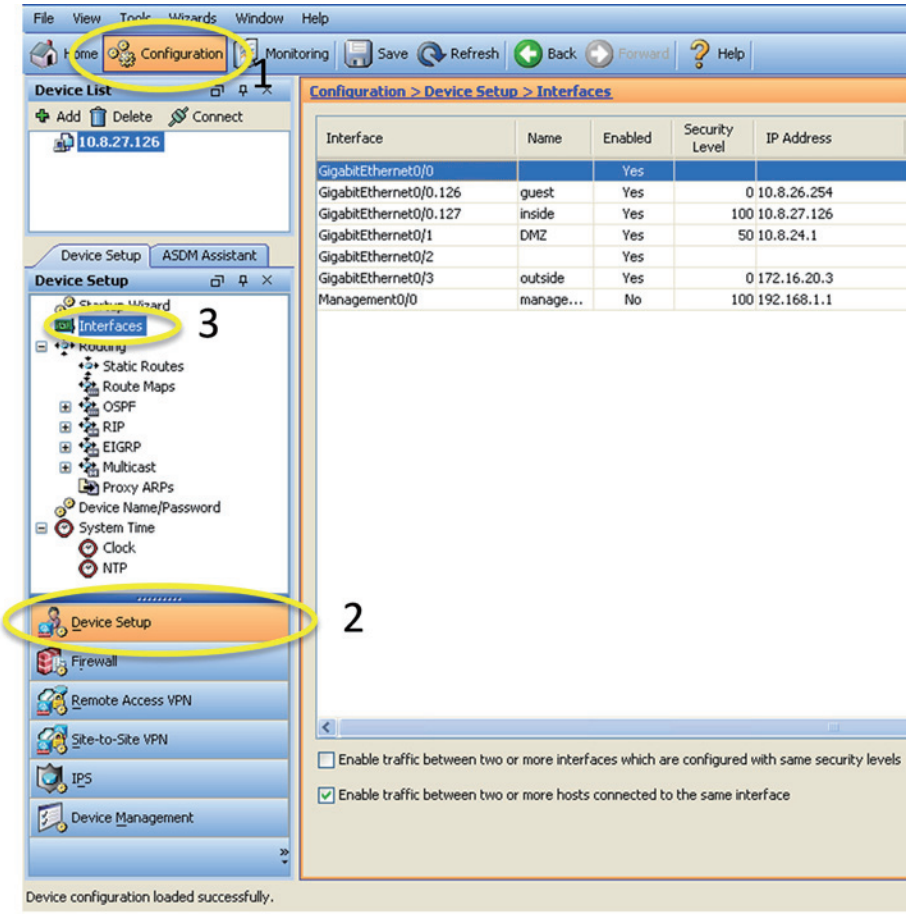
如果您未使用过ASDM，请在Web浏览器中打开https://<ASA-Management-IP-Address>。

ASDM采用了Java语言，将会下载一个小程序到您的电脑。

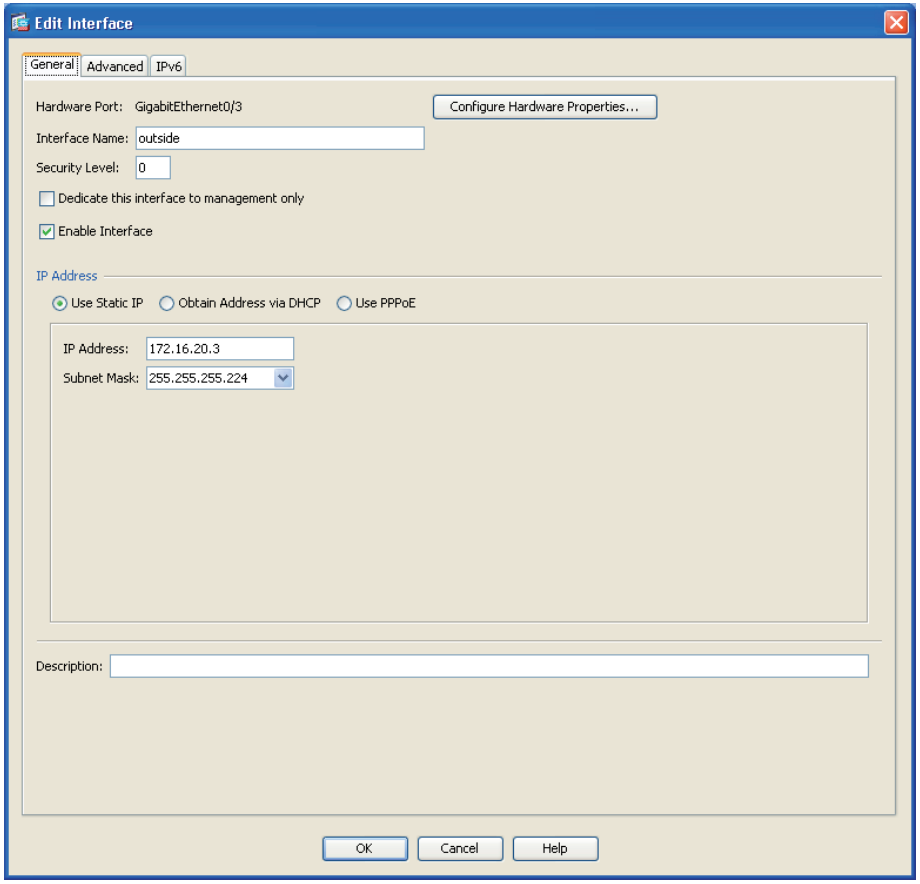
ASDM 6.3支持Windows 7、XP、Vista和Server 2008、Mac OS 10.4、10.5和10.6，以及Red Hat Enterprise Linux 5。支持的Web浏览器包括Internet Explorer 6.0或更高版本、以及Firefox 1.5或更高版本。

步骤2：转至：

1. Configuration（配置）
2. Device Setup（设备设置）
3. Interfaces（接口）

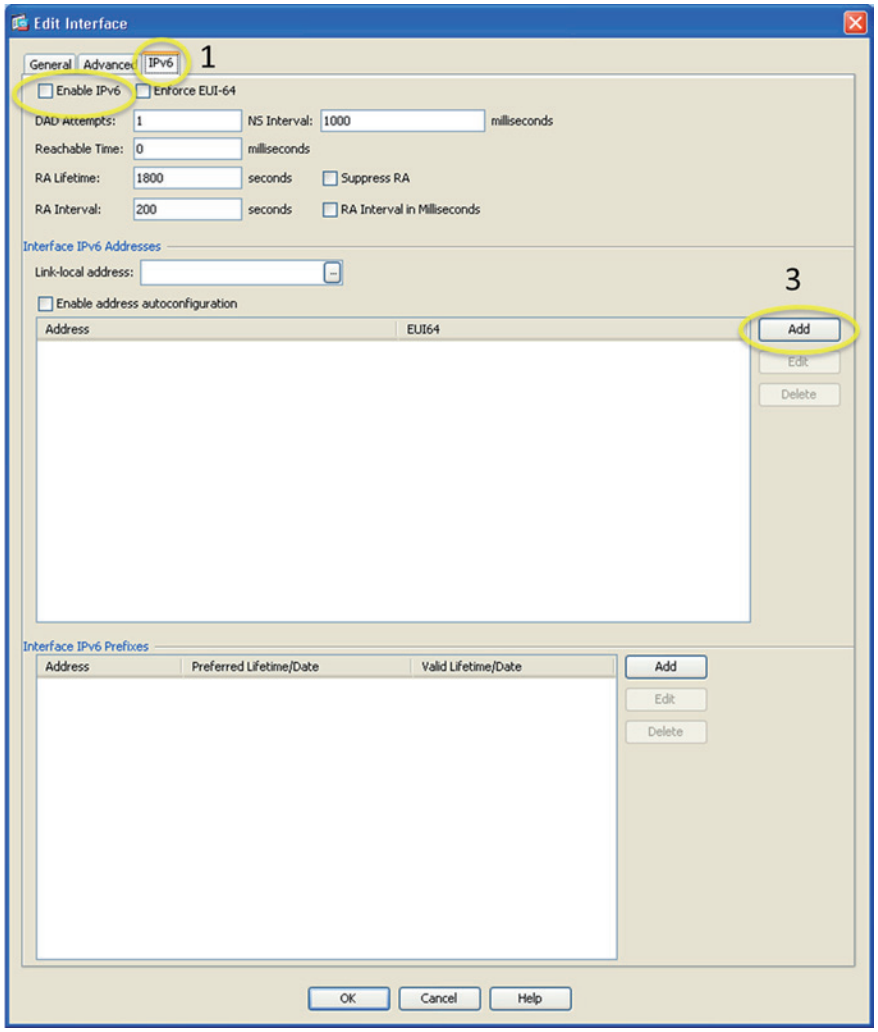


步骤3：选择外部接口并单击Edit（编辑）。Edit Interface（编辑接口）对话框出现。

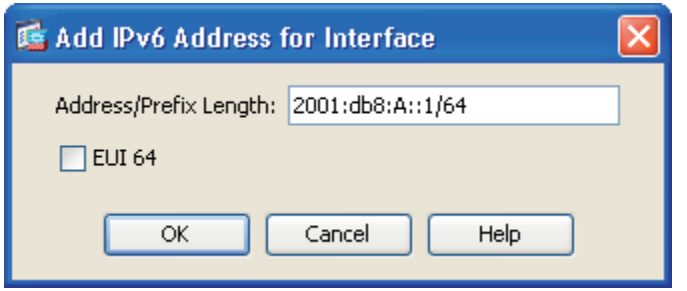


步骤4：为接口配置IPv6:

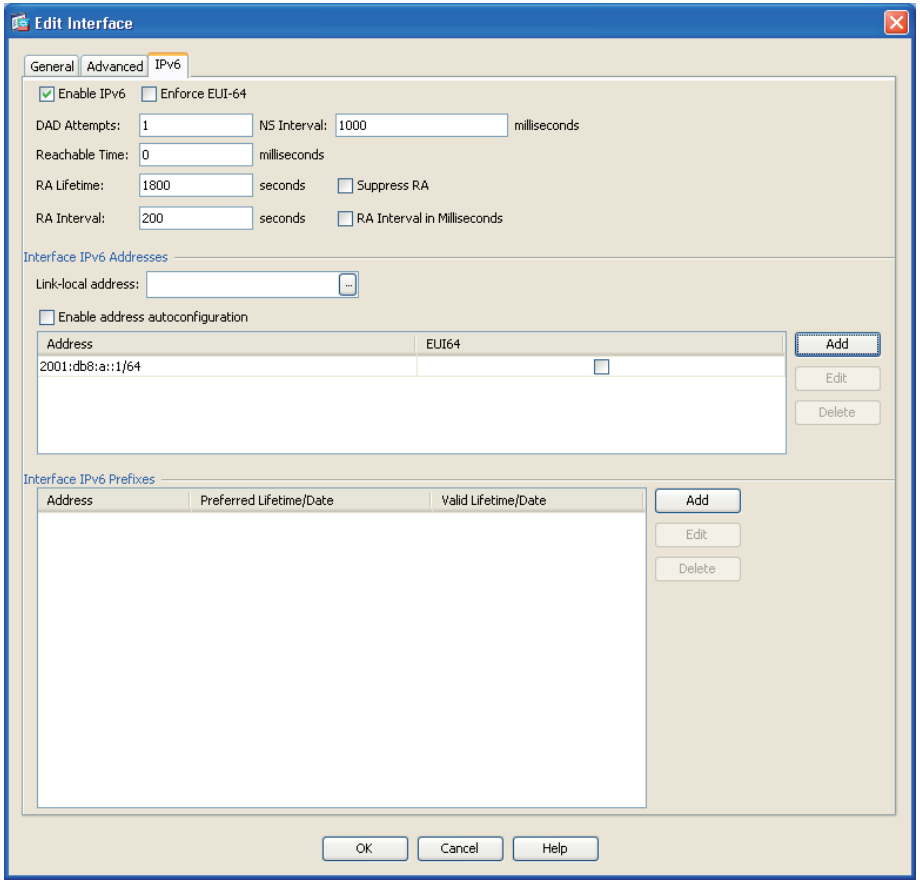
1. 选择IPv6选项卡。
2. 选中Enable IPv6（启用IPv6）复选框。
3. 点击Add（添加）。



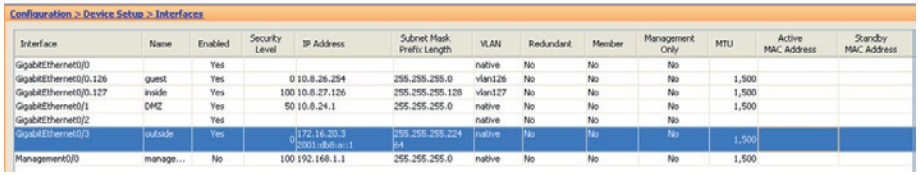
步骤5：输入带有正确前缀长度的IPv6地址，单击OK。针对本配置的IPv6地址为2001:dba:a::1/64



这一新IPv6地址显示在IPv6接口配置中。

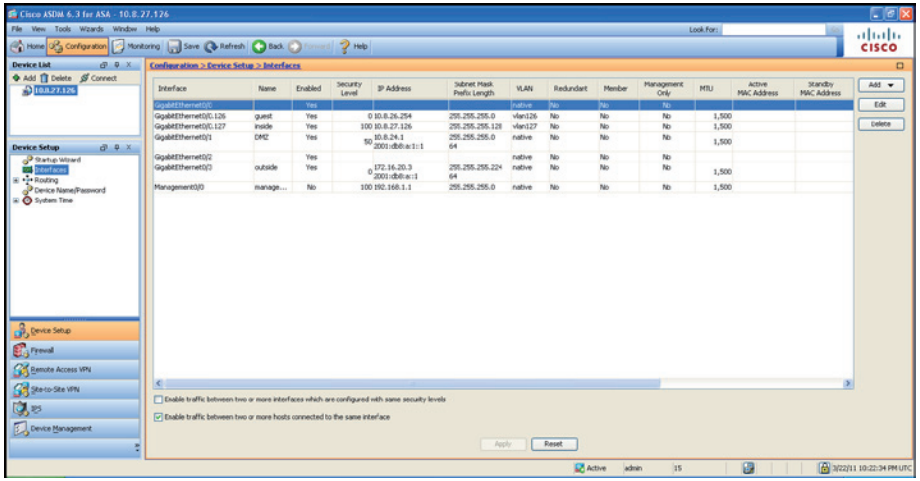


步骤6：单击OK返回到接口配置屏幕。单击屏幕底部的Apply（应用），使配置变更生效。



步骤7：重复前述步骤，使用用于DMZ的接口IPv6地址配置DMZ接口。

DMZ IPv6配置显示新值。



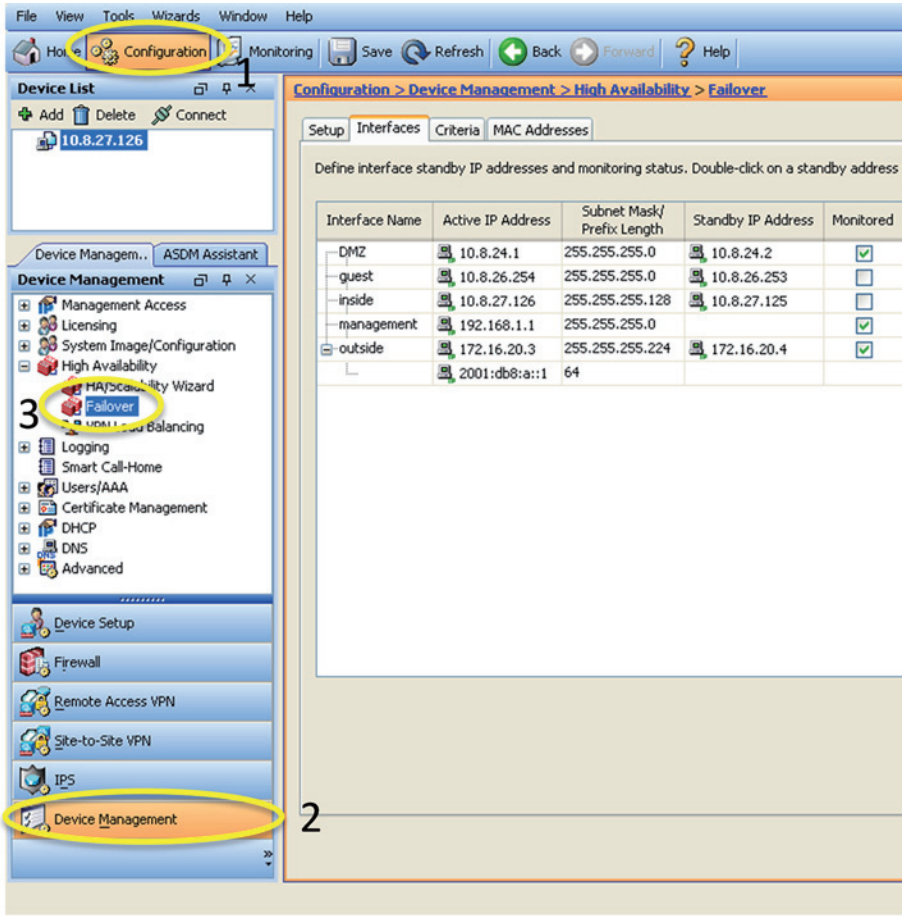
程序2　为IPv6配置高可用性

接下来，您需要为新创建的IPv6接口配置高可用性（HA），以便在主用和备用Cisco ASA设备之间进行接口故障切换。对于为IPv6配置的每一个接口，您必须配置HA IPv6地址，以支持故障切换到备用Cisco ASA设备。

Cisco ASA上已经为IPv4配置了HA特性，支持机箱到机箱故障切换。这一针对IPv4的配置将保持不变。

步骤1：转至：

1. Configuration（配置）
2. Device Management（设备管理）
3. High Availability（高可用性）> Failover（故障切换）
4. 在Interfaces（接口）选项卡上，显示了为IPv4和IPv6配置的接口。



步骤2：选择IPv6外部接口。

步骤3：单击为空的备用IP地址字段，输入故障切换IPv6地址，按Enter键。

outside	172.16.20.3	255.255.255.224	172.16.20.4	☑
	2001:db8:a::1	64	2001:db8:a::2	

步骤4：重复步骤2-3为DMZ配置接口故障切换IPv6地址。

故障切换地址显示新地址。

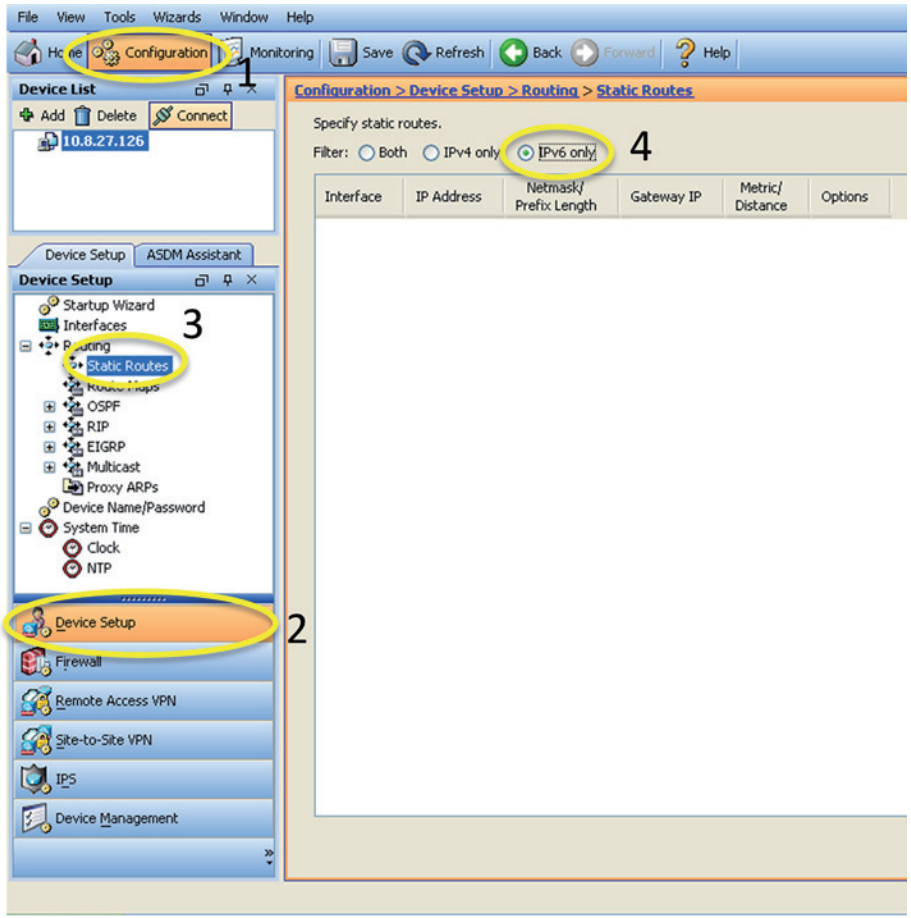
DMZ	10.8.24.1	255.255.255.0	10.8.24.2	☑
	2001:db8:a:1::1	64	2001:db8:a:1::2	

程序3　配置IPv6静态路由

接下来，您需要在Cisco ASA上为IPv6互联网接入配置静态路由。IPv6必须配置IPv6路由。这一设置使用了到服务提供商的静态路由。

步骤1：转至：

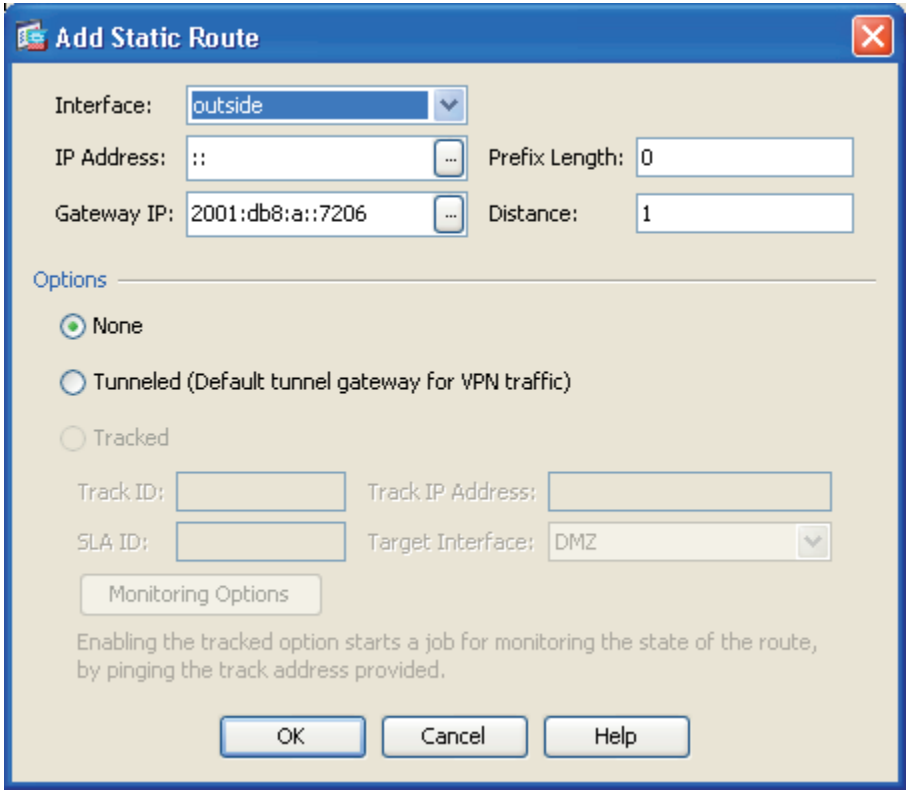
1. Configuration（配置）
2. Device Setup（设备设置）
3. Routing（路由）
4. Static Routes（静态路由），选择IPv6 only（仅IPv6）



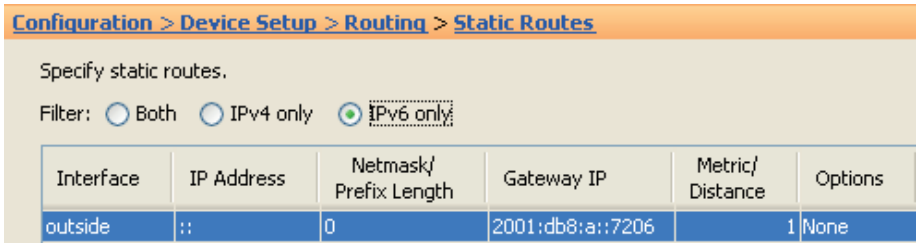
步骤2：单击Add（添加）。Add Static Route（添加静态路由）对话框出现。您将在这里添加到服务提供商的静态路由。这一全新缺省路由将适用于所有未在Cisco ASA上配置的IPv6流量。所有这些流量将被引导至服务提供商。

步骤3：输入以下值，单击OK，将所有其他字段保留为缺省值：

- 选择Interface（接口:： outside
- IP地址: ::
- Prefix Length（前缀长度:： 0
- Gateway IP（网关IP: :（Service Provider IPv6地址）



静态路由表显示新值。



流程

将Cisco ASA配置为允许访问IPv6 Web服务器

1. Add IPv6 Network Objects
2. 添加针对HTTP/HTTPs的IPv6规则
3. 添加针对IPv6 Ping的ICMP IPv6规则

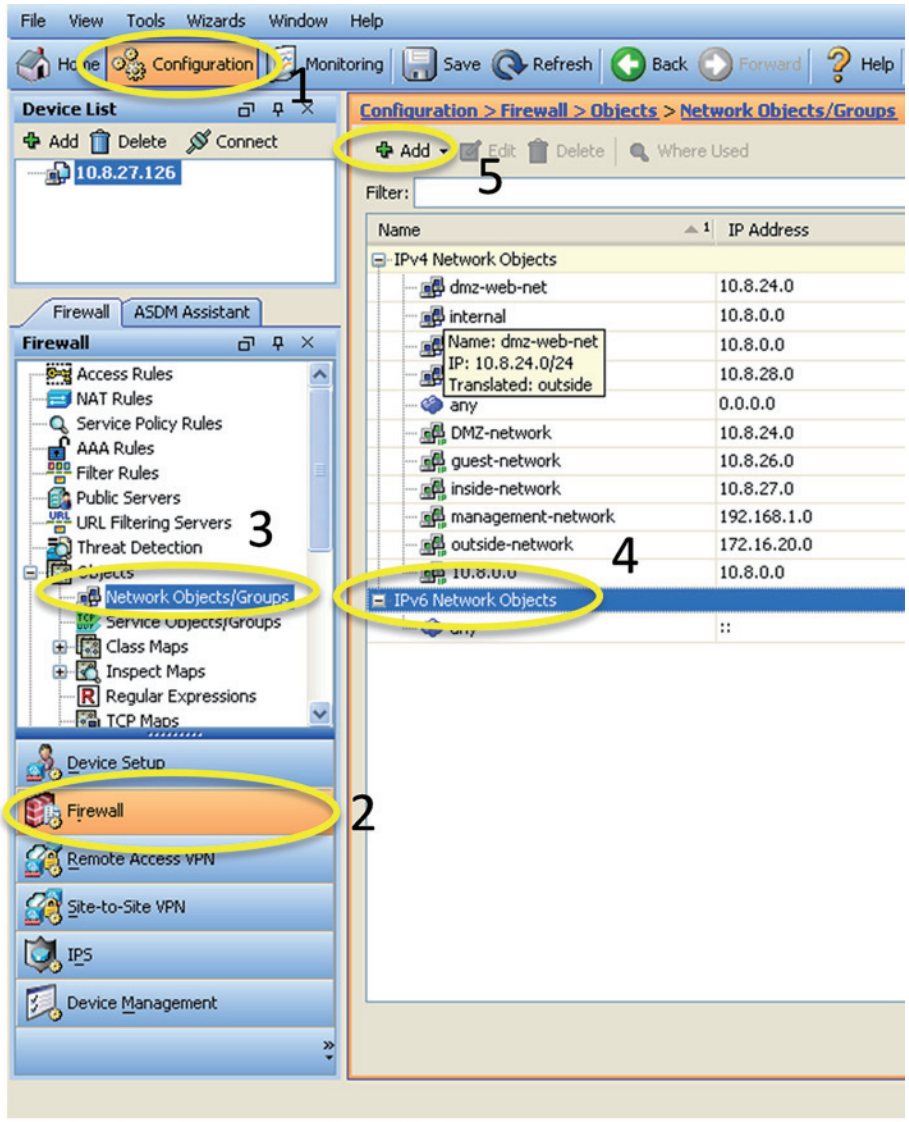
程序1　添加IPv6网络对象

为简化防火墙规则的添加，您将创建一个网络对象，涵盖适用于DMZ前缀的IPv6前缀。如果企业安全策略需要，您可以通过将前缀长度变更为128位，并指定整个服务器IPv6地址，为每一台特定的服务器添加对象。

步骤1：转至：

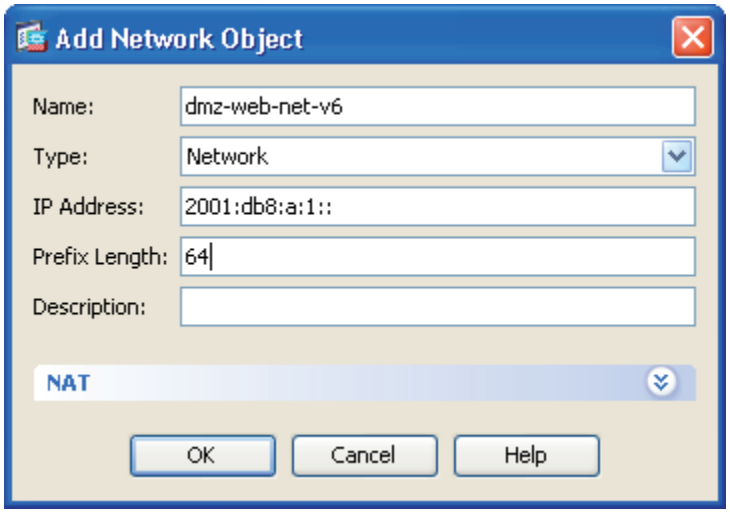
1. Configuration（配置）
2. 防火墙
3. Objects（对象）> Network Objects/Groups（网络对象/组）

步骤2：选择IPv6 Network Objects（IPv6网络对象），单击Add（添加），之后选择Add Network Object from the list（从列表中添加网络对象）。Add Network Object（添加网络对象）窗口将会出现。

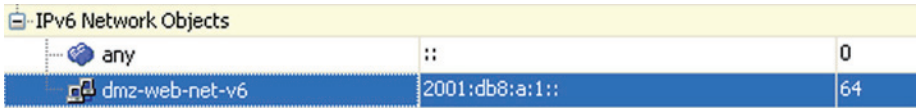


步骤3：输入以下值，单击OK:

- 对象名称:
- 类型：网络
- IPv6 DMZ网络的前缀长度



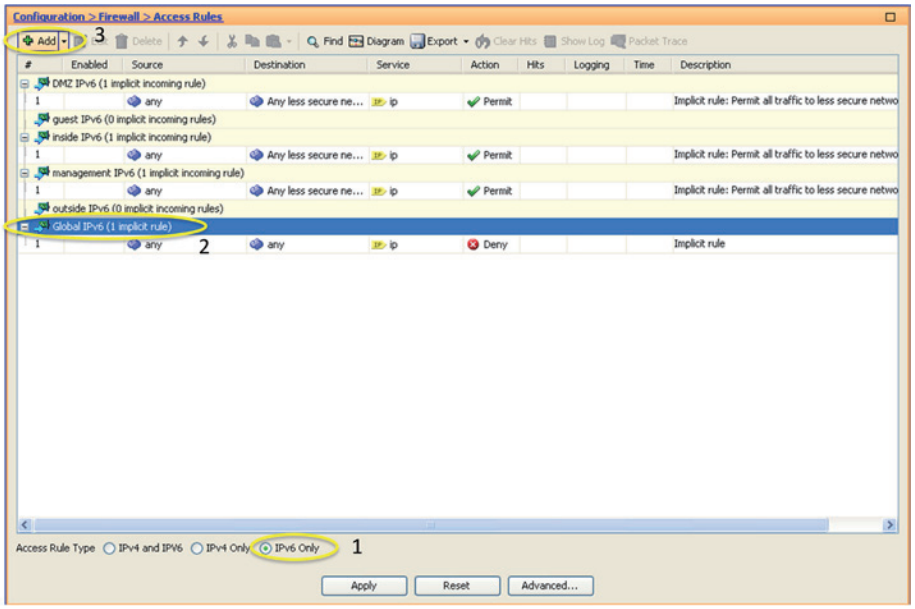
全新IPv6网络对象出现。



程序2　添加针对HTTP/HTTPs的IPv6规则

步骤1：要确保Web服务器安全可靠，必须将Cisco ASA配置为仅允许发送HTTP和HTTPs流量到Web服务器。要实现此目标，需要为IPv6创建一个访问控制列表（ACL）。下方的ACL允许将HTTP和HTTPs流量发送到DMZ Web服务器前缀。

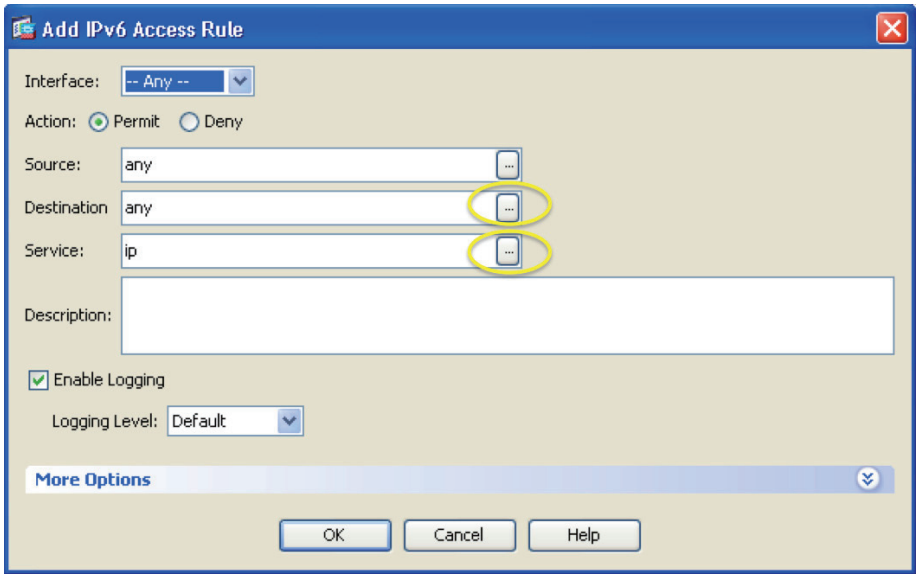
步骤2：请参阅程序1步骤1作为参考，转至Configuration（配置），之后转至Firewall（防火墙）> Access Rules（访问规则）。



步骤3：选择以下选项：

1. 在对话框的底部，选择IPv6 Only（仅IPv6）。列表显示了缺省指派的隐含规则
2. 选择Global IPv6（全局IPv6）
3. 单击Add（添加）激活规则配置，并选择Add IPV6 Access Rule（添加IPv6访问规则）。

步骤4：在Add IPv6 Access Rule（添加IPv6访问规则）对话框中，在Interface（接口）列表中，选择Any（任意）。其他字段将在以下步骤中进行填充。

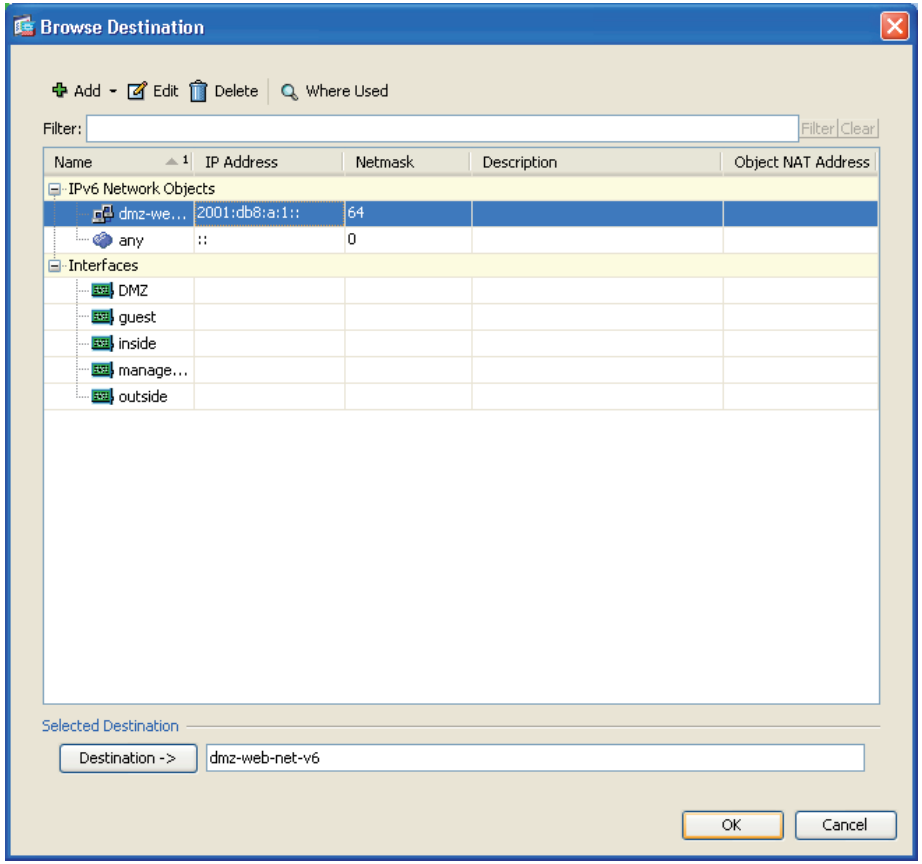


步骤5：选择Permit（允许）。

步骤6：在Source（来源）框中，输入any（任意）。

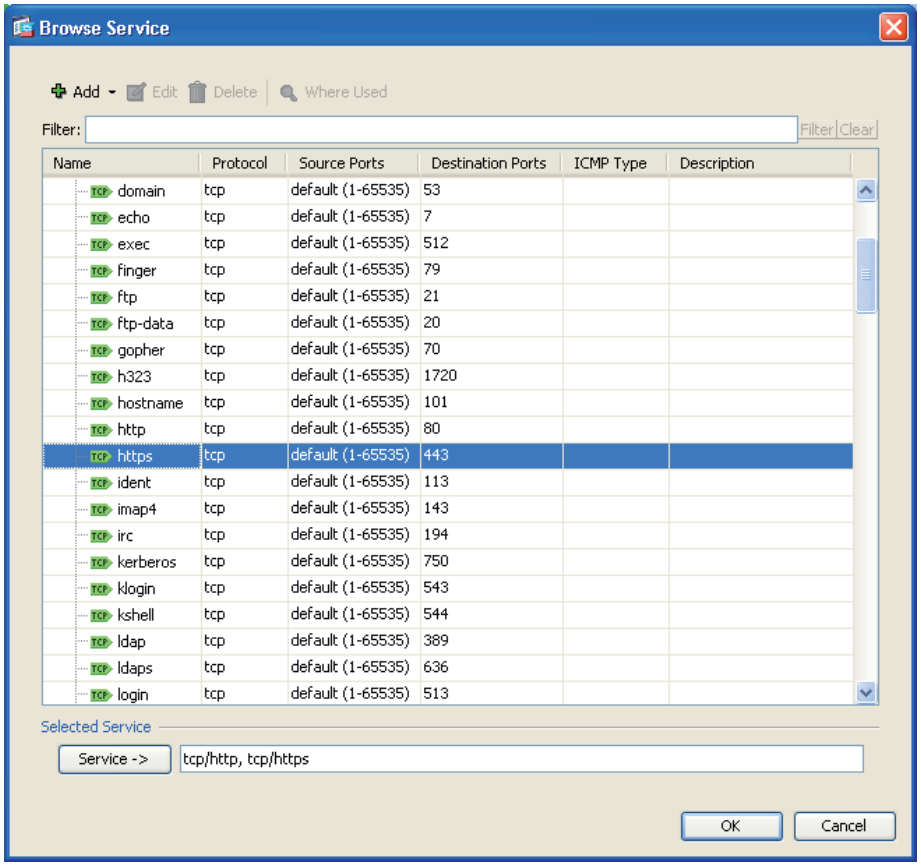
步骤7：单击Destination（目的地）框中的省略号（...）按钮。

步骤8：在Browse Destination（浏览目的地）对话框中，在IPv6 Network Objects（IPv6网络对象）下，双击dmz-web-net-v6，它将显示在目的地框中。单击OK关闭窗口。



步骤9：单击Service（服务）框中的省略号(...）按钮。

步骤10：在Browse Service（浏览服务）对话框中，向下滚动鼠标，双击http和https。这两个值将显示在下方的Selected Service（选中的服务）字段中。



步骤11：单击OK，之后在Firewall Rules（防火墙规则）窗口中，单击Apply（应用）。

程序3　添加针对IPv6 Ping的ICMP IPv6规则

（可选）

这一可选程序允许对DMZ上的服务器进行IPv6 ping操作。该操作将在后面的IPS部分的程序中使用，以展示面向IPv6的入侵防御系统（IPS）的警告功能。这一规则应在测试完成后移除。在配置前检查您的安全策略。

读者提示

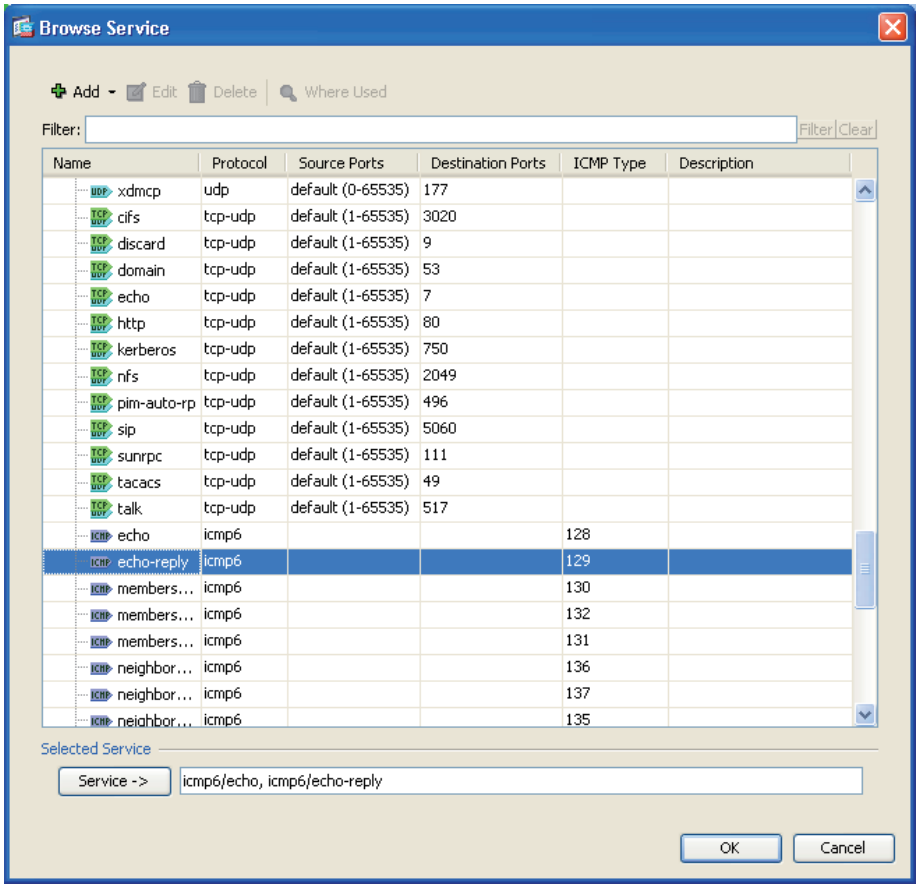
路径MTU发现（PMTUD）需要使用ICMP。这一点至关重要，因为部分IPv6可能将穿过降低了MTU值的隧道。在安全规划中，为使MTU发现能够在IPv6中使用，需要考虑允许ICMPv6 type 2 Packet Too Big数据包。

步骤1：重复上一程序中的步骤1-7。

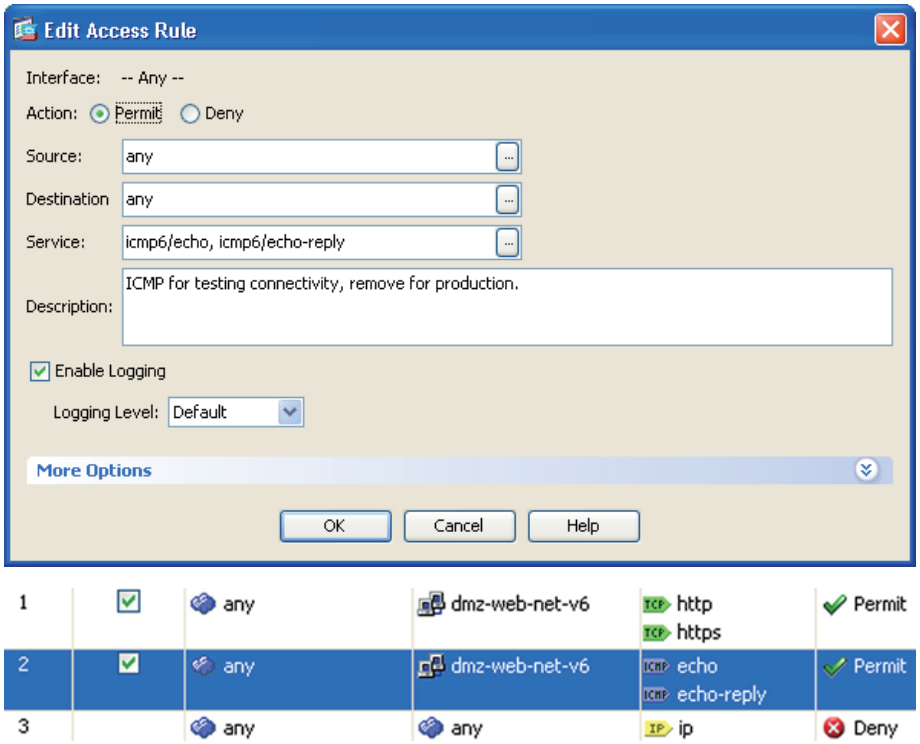
步骤2：在Destination（目的地）框中，输入Any（任意）。

步骤3：单击Service（服务）框中的省略号(...）按钮。

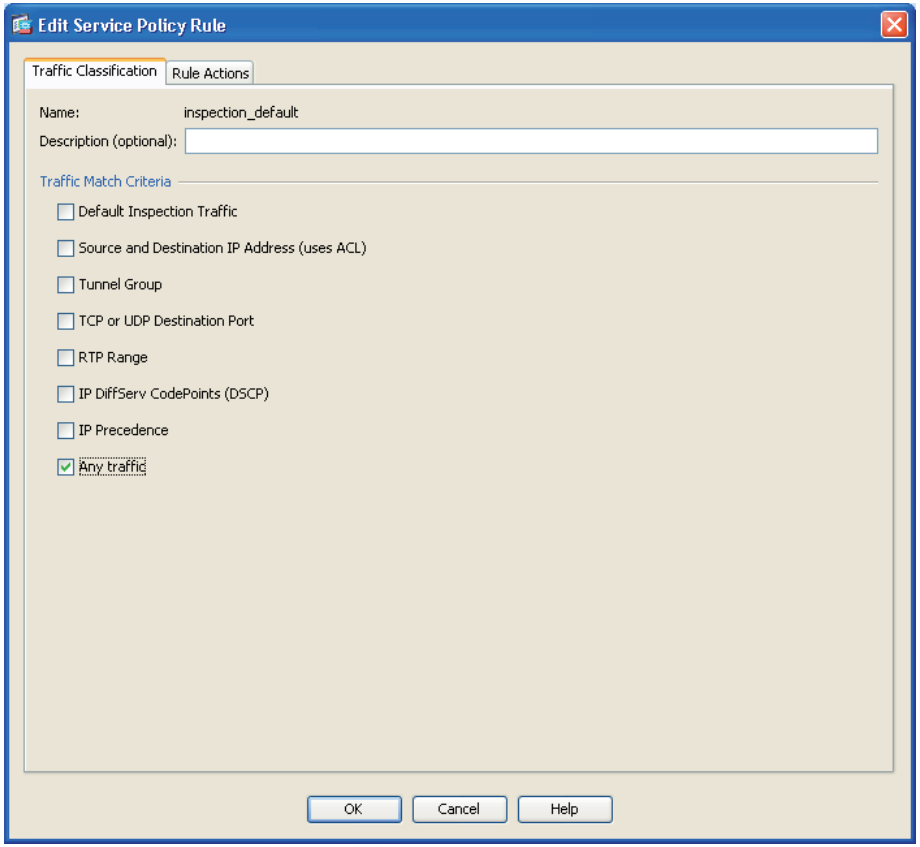
步骤4：在Browse Service（浏览服务）对话框中，双击Echo和Echo Reply。这两个值将显示在下方的Selected Service（选中的服务）字段中。



步骤5：单击OK（确定）。IPv6 ICMP规则已添加。



步骤2：在Traffic Classification（流量分类）选项卡上，清除Default Inspection Traffic（缺省检查流量）复选框，选择Any Traffic（任意流量）：



流程

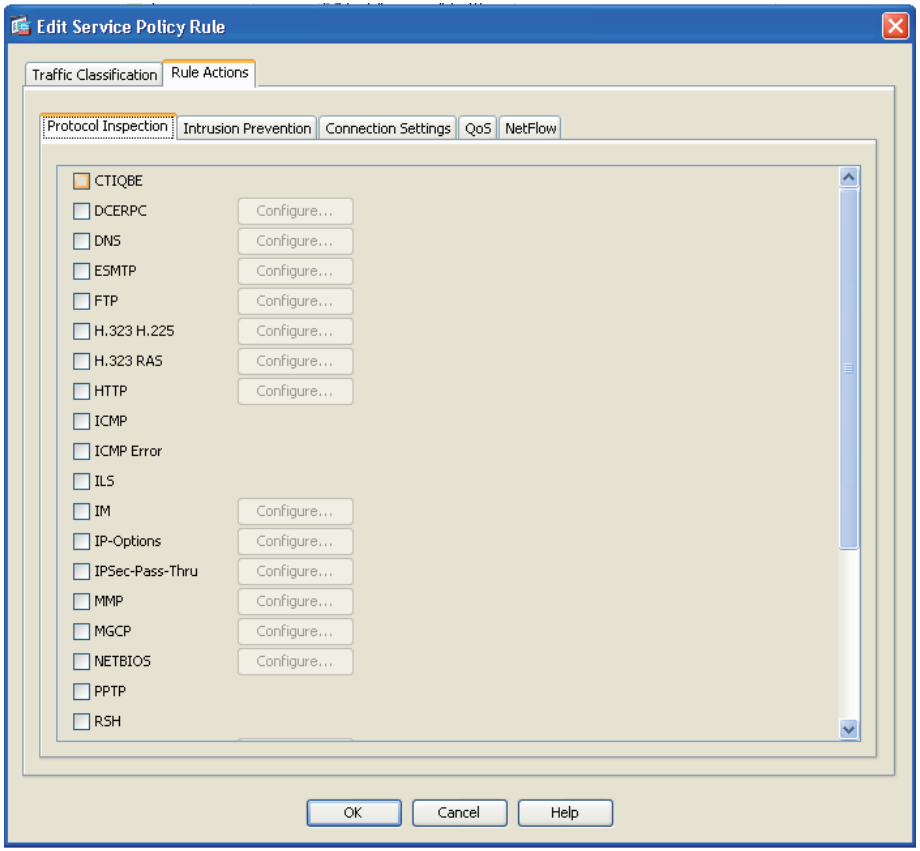
配置ASA将IPv6流量传送至IPS

1. 连接至IPS

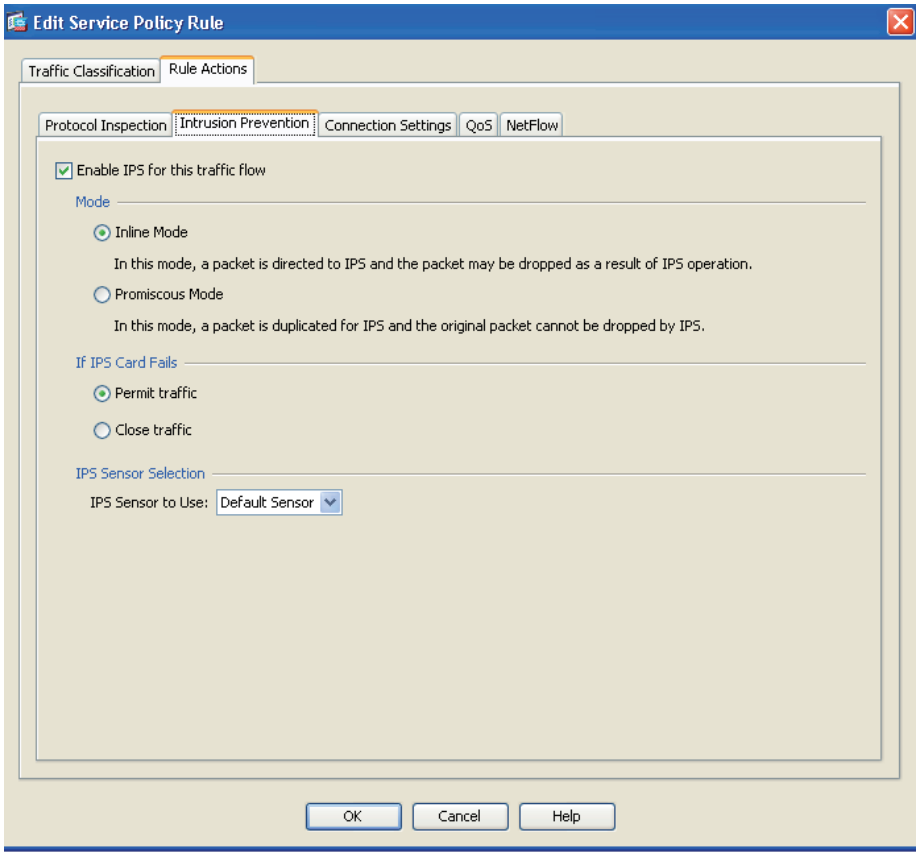
程序1　连接至IPS

步骤1：转至Configuration（配置）> Firewall（防火墙）> Service Policy Rules（服务策略规则），选择全局策略，之后单击Edit（编辑）。

步骤3：在Rule Actions（规则动作）选项卡上，在Protocol Inspection（协议检测）子选项卡上，取消选择所有选项：

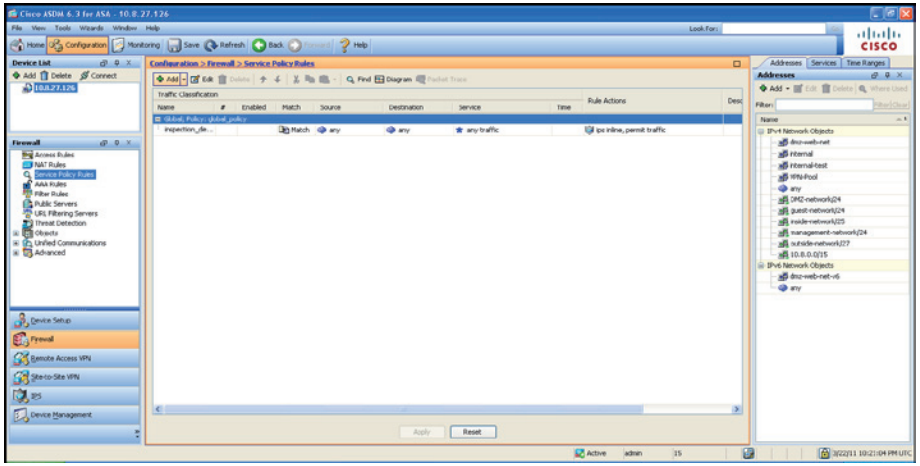


步骤4：在Rule Actions（规则动作）选项卡上，在Intrusion Prevention（入侵防御）子选项卡上，选择Enable IPS for this traffic flow（针对此流量启用IPS），它应用了Inline Mode（内嵌模式）和Permit Traffic（允许流量）。

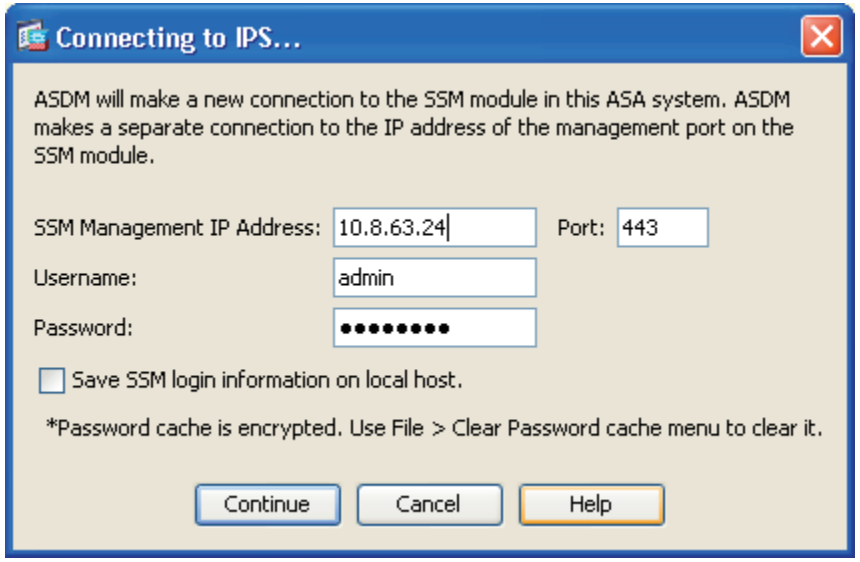


步骤5：点击OK退出Edit Service Policy Rule（编辑服务策略规则）窗口。

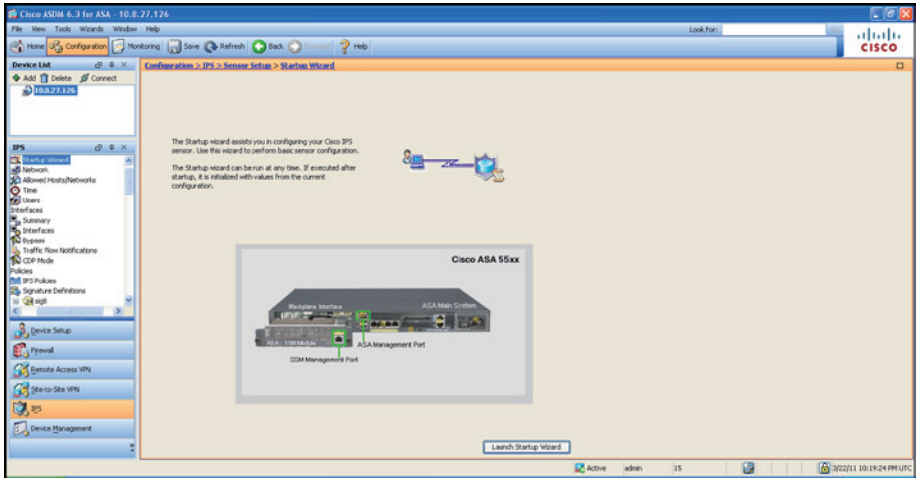
步骤6：验证IPS的全局服务策略设置允许任意流量，之后单击Apply（应用）应用该配置。



步骤7：转至Configuration（配置）> IPS。ASDM提示登录到IPS模块。输入相应的登录凭证，单击Continue（继续）。单击Yes（是）继续。



步骤8：在IPS的主配置窗口，在左侧面板，选择Signature Definitions（签名定义）。

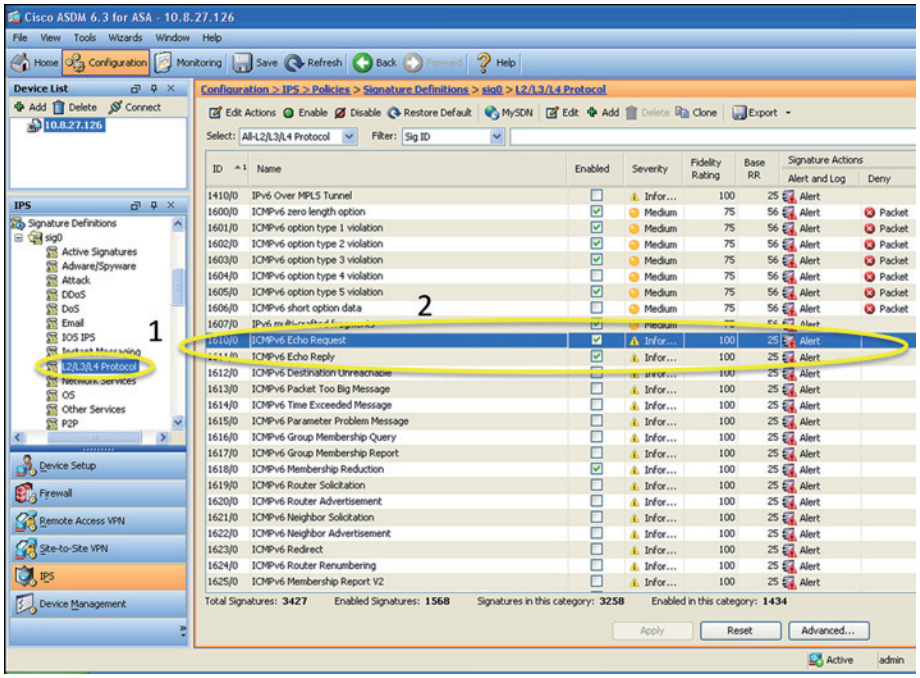


步骤9：选择Signature Definitions（签名定义）> Sig0 > L2/L3/L4 Protocol（L2/L3/L4协议）。本示例使用了ICMPv6 Echo Request和Echo Reply以显示IPS的功能，并在之前的防火墙规则中设置了IPv6 ping。为ICMPv6 Echo Request和Echo Reply选择Enabled（启用），之后单击Apply（应用）。

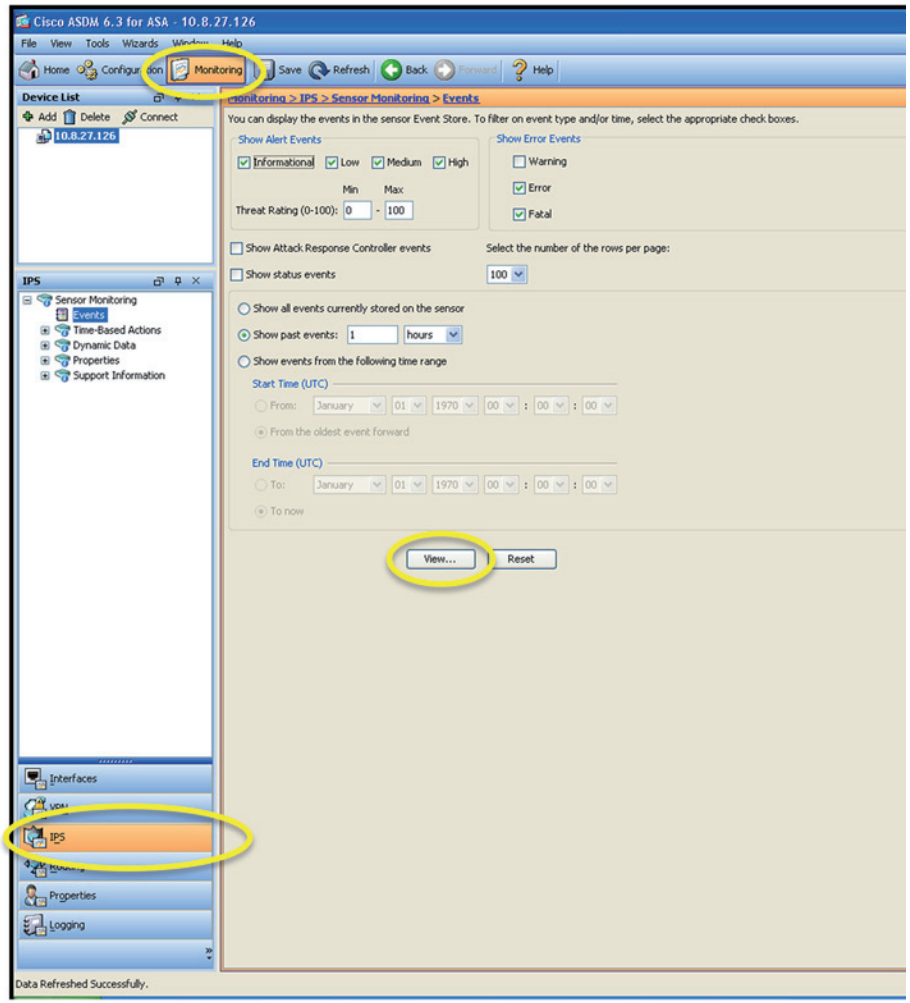
技术提示

此处的这一配置显示了IPS针对IPv6流量的报告功能。ICMP IPv6 ping可轻松生成，用于测试IPS报告功能。在测试完成后取消选中Enabled（启用）框，并进行应用。

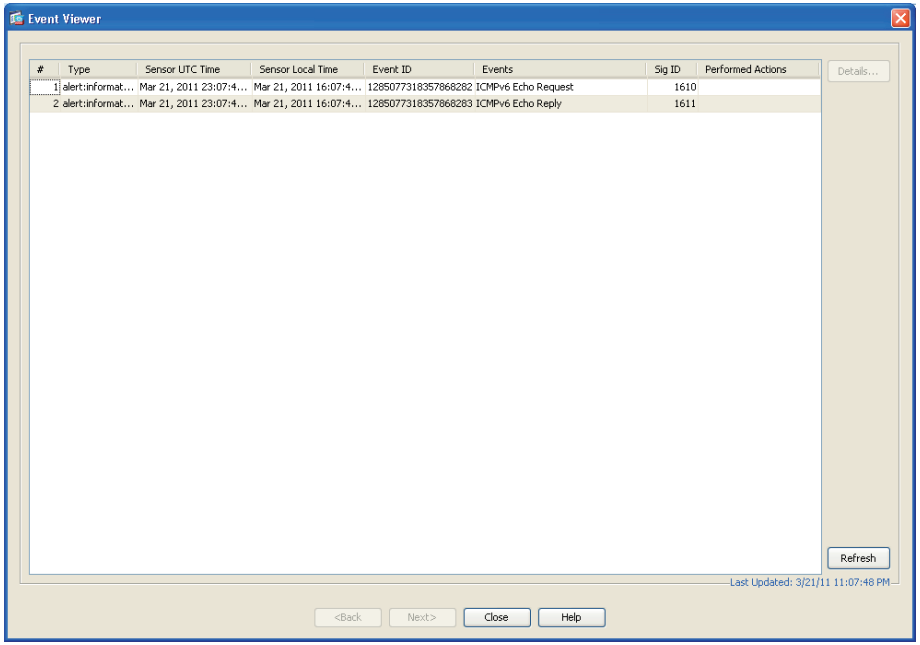
此处有多个其他选项可用，应针对IPv6入侵防御进行仔细查看。



步骤10：如果您希望监控事件，转至Monitoring（监控）> IPS。左侧显示了几个查看事件的选项。系统将显示针对ICMP Echo和Echo Request的IPv6配置事件，以供参考。要在杂乱的事件窗口中向下钻取，在Show Alert Events（显示告警事件）下仅选择Informational（信息）。使用DMZ外部的主机，对DMZ中的主机进行ping操作。单击View（查看）。



步骤11：检查IPS是否记录了IPv6 ICMP Echo Reply和Echo Request。



步骤12：将备用ASA的状态从备用改为主用

技术提示

到达第二个IPS的另一种方法是通过IPS Device Manager GUI。要直接访问传感器，连接至https://<IP-ADDRESS-IPS>。您可以安装IDM Launcher（如尚未安装）。这一步骤不要求将ASA从Standby（备用）故障切换到Active（主用）。

输入failover active命令，将ASA的状态改为主用。设备交换IP地址，形成一个防火墙故障切换事件。

```
# failover active
Switching to Active # show failover
[Output removed for brevity....]
This host: Secondary - Active
```

步骤13：在备用ASA中配置IPS

利用ASDM重新连接到ASA（现在使用的是备用转为主用的防火墙）的主IP地址。遵循以上程序和步骤，对第二个IPS进行与第一个IPS相同的配置。

流程

为IPv6配置主机

1. 在Windows 2008 Server上配置IPv6

构建主机有多种方案：

- 方案1 —— 为IPv6 Web内容创建一个新主机
  - 这需要更多工作，但可以建立一个纯粹的IPv6设置，不包含当前的嵌入式IPv4地址。
  - 其劣势是需要维护两个内容主机。
- 方案2 —— 使用现有的提供IPv4的主机
  - 这一方案的优势是无需建立两台包含重复内容的服务器。
  - 可能的不利方面是现有Web内容中嵌入的IPv4地址。

主机配置

- 选项1 —— 仅IPv6
- 选项2 —— IPv4和IPv6（双堆栈）
  - IPv6在互联网边缘架构中被启用。主机上需要IPv4来访问内部网络。这一设置要求主机采用同时支持IPv4和IPv6的双堆栈设计。这种双堆栈设置依赖于IPv4来进行DNS和后端服务器访问，以及提供IPv4 Web服务。

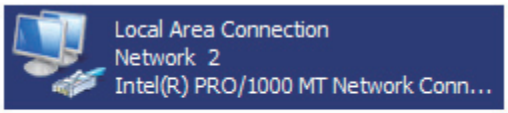
这一配置在新的Web服务器上使用IPv4/IPv6双堆栈配置建立。在现有服务器上进行配置要求对用于静态或非相关IPv4引用的Web内容进行全面的检查。

程序1　在Windows 2008 Server上配置IPv6

步骤1：登录至相应的Windows 2008 Server

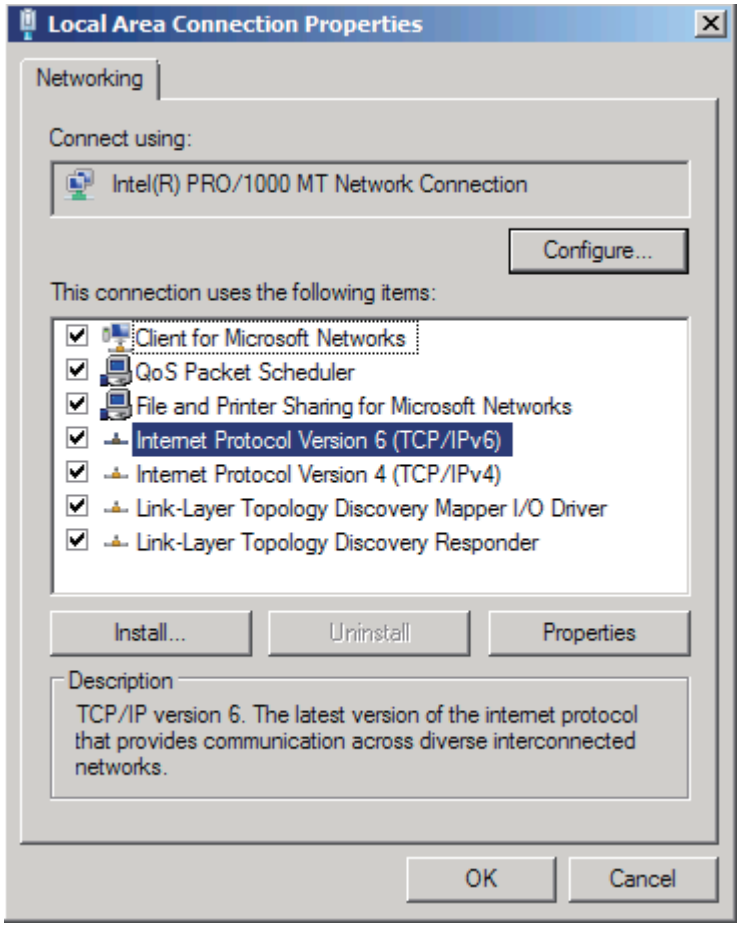
步骤2：右击以太网接口，单击Properties（属性）。

图3. Windows 2008以太网接口

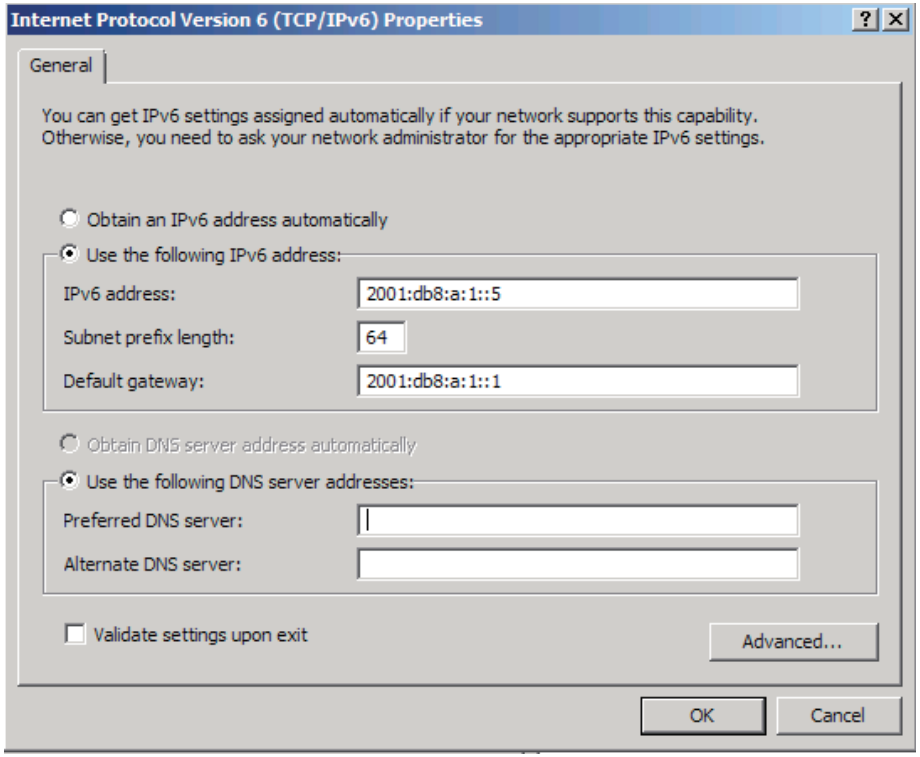


步骤3：如果IPv6未被选中，请将其选中，之后单击OK关闭Properties（属性）页面。重新打开Properties（属性）页面，继续配置。如果您不关闭而重新打开，Windows将不允许您添加IPv6地址。

步骤4：选择IPv6，之后单击Properties（属性）。



步骤5：选择Use the following IPv6 address（使用以下IPv6地址）。输入IPv6地址、前缀长度和缺省网关。

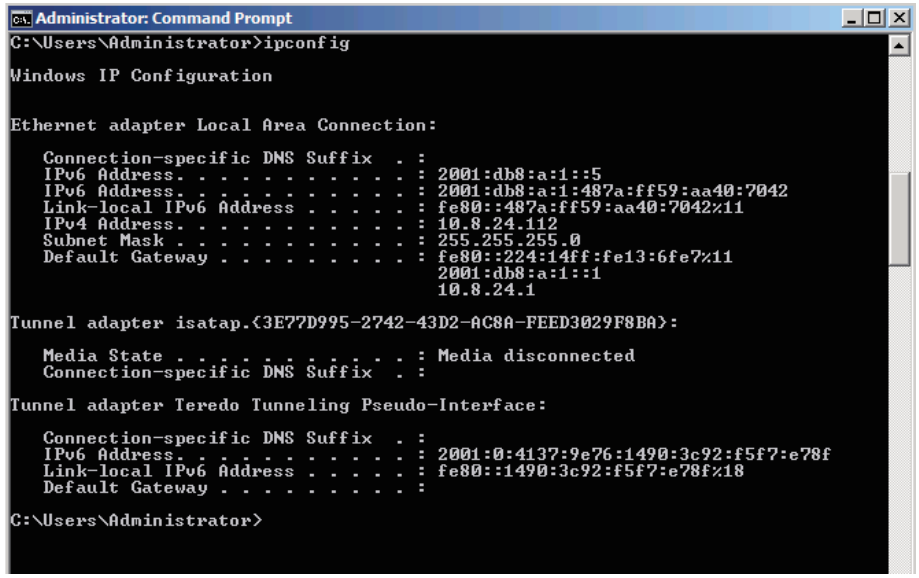


步骤6：单击OK退出。在以太网接口上单击OK完成配置。

技术提示

如果此主机上未定义DNS，它将缺省采用IPv4接口上的IPv4 DNS。该主机将接收Web请求，它并非一个需要IPv6 DNS的客户端。如果它是一个需要IPv6 DNS的客户端，需要输入一个IPv6 DNS条目。

步骤7：在命令行窗口中输入ipconfig，检查IPv6配置是否正确无误。



域名服务

针对IPv6互联网边缘的域名服务（DNS）由服务提供商处理。IPv6引入了AAAA记录，该记录可将IPv6地址映射到主机。这一点类似于将IPv4地址映射到主机的记录。本配置中的Web服务器采用双堆栈设计，其DNS针对IPv4进行了配置。在此设置中服务主机并不一定需要IPv6 DNS。服务提供商需要一个IPv6 DNS条目，以在互联网上传播Web服务器主机地址。仅包含IPv6地址的客户端将在查询地址时收到正确的地址。同时配置有IPv4和IPv6 DNS服务器的客户端将根据操作系统算法进行查询。

在从IPv4进行迁移的过程中，面向IPv6的DNS为您的DNS条目提供了两个选项：

- 选项1 —— 完整的纯IPv6 DNS名称，例如：web.ipv6.organzation. com
- 选项2 —— 针对IPv4地址的额外AAAA IPv6记录，解析到一个DNS名称，例如：web. organzation.com

支持这两个选项的DNS和双堆栈带来了几大挑战。选项1最简洁，但它无法使用统一的IPv4和IPv6基础设施。这一选项能够正常工作，但用户必须现在就知道IPv6 Web地址。

选项2允许IPv4和IPv6主机使用相同的地址。如果双堆栈设置在客户端进行了正确配置，这一选项将能够正常工作。要使此选项发挥作用且不出现超时，DNS必须能够完全支持IPv4和IPv6。如果客户端配置了IPv6，但IPv6 DNS未连接到互联网，DNS在切换到IPv4之前将会出现超时问题。请注意：许多操作系统都已经安装了IPv6，并在安装时设置为自动配置。这意味着尽管企业未配置IPv6，但IPv6可能会在客户端上自动设置。每种操作系统均有其各自的算法，用于在双堆栈设置中处理DNS查找问题。如果DNS服务器上配置了AAAA记录，IPv4可成功用于IPv6 DNS查找。

备注

附录A：产品列表

以下产品和软件版本已经过验证，可用于思科智能业务平台。

Functional Area	Product	Part Numbers	Software Version
Internet Edge Firewall	Adaptive Security Appliance		ASA 8.4.1
	Cisco ASA 5540 with the SSM-40 IPS Module	ASA5540-AIP40-K9	7.0(5a)E4
	Cisco ASA 5520 with the SSM-20 IPS Module	ASA5520-AIP20-K9	
	Cisco ASA 5510 with the SSM-10 IPS Module	ASA5510-AIP10-K9	

附录B：CLI配置

ASA

```
ASA Version 8.4(1)
!
hostname IE5520a
domain-name cisco.local
enable password 2y4FIGBVVyBLau0Q encrypted
passwd 2y4FIGBVVyBLau0Q encrypted
names
!
interface GigabitEthernet0/0
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/0.126
 vlan 126
 nameif guest
 security-level 0
 ip address 10.8.26.254 255.255.255.0 standby 10.8.26.253
!
interface GigabitEthernet0/0.127
 vlan 127
 nameif inside
 security-level 100
 ip address 10.8.27.126 255.255.255.128 standby 10.8.27.125
!
interface GigabitEthernet0/1
 nameif DMZ
 security-level 50
 ip address 10.8.24.1 255.255.255.0 standby 10.8.24.2
 ipv6 address 2001:db8:a:1::1/64 standby 2001:db8:a:1::2
 ipv6 enable
!
interface GigabitEthernet0/2
 description LAN/STATE Failover Interface
!
interface GigabitEthernet0/3
 nameif outside
 security-level 0
 ip address 172.16.20.3 255.255.255.224 standby 172.16.20.4
 ipv6 address 2001:db8:a::1/64 standby 2001:db8:a::2
 ipv6 enable
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
boot system disk0:/asa841-k8.bin
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.local
object network internal
 subnet 10.8.0.0 255.254.0.0
object network VPN-Pool
 subnet 10.8.28.0 255.255.254.0
object network internal-test
 subnet 10.8.0.0 255.254.0.0
object network dmz-web-net-v6
 subnet 2001:db8:a:1::/64
object-group service DM_INLINE_TCP_1 tcp
 port-object eq www
 port-object eq https
object-group service DM_INLINE_SERVICE_1
 service-object icmp6 echo
```

```
 service-object icmp6 echo-reply
access-list inside_mpc extended permit ip 10.8.0.0 255.254.0.0
any
access-list outside_mpc extended permit ip any 10.8.0.0
255.254.0.0
access-list RA_SplitTunnelACL standard permit 10.8.0.0
255.254.0.0
pager lines 24
logging enable
logging asdm informational
mtu guest 1500
mtu inside 1500
mtu DMZ 1500
mtu outside 1500
mtu management 1500
ip local pool RAPool 10.8.28.0-10.8.29.254 mask 255.255.254.0
ipv6 route outside ::/0 2001:db8:a::7206
ipv6 access-list global_access_ipv6 permit tcp any object dmz-
web-net-v6 object-group DM_INLINE_TCP_1
ipv6 access-list global_access_ipv6 permit object-group DM_
INLINE_SERVICE_1 any any
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/2
failover polltime unit 1 holdtime 3
failover polltime interface 1 holdtime 5
failover key *****
failover replication http
failover link failover GigabitEthernet0/2
failover interface ip failover 10.8.27.130 255.255.255.252
standby 10.8.27.129
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-643.bin
asdm history enable
arp timeout 14400
nat (inside,any) source static internal internal destination
static VPN-Pool VPN-Pool
!
object network internal-test
 nat (inside,outside) dynamic interface
access-group global_access_ipv6 global
!
router eigrp 1
 network 10.8.0.0 255.254.0.0
 passive-interface guest
 passive-interface DMZ
 passive-interface outside
 redistribute static
!
route outside 0.0.0.0 0.0.0.0 172.16.20.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server cisco.local protocol nt
aaa-server cisco.local (inside) host 10.8.48.10
 nt-auth-domain-controller 10.8.48.10
http server enable
http 192.168.1.0 255.255.255.0 management
http 10.8.0.0 255.254.0.0 inside
http redirect outside 80
no snmp-server location
no snmp-server contact
service resetoutside
crypto dynamic-map 5505DYN-MAP 5 set security-association
lifetime seconds 28800
crypto dynamic-map 5505DYN-MAP 5 set security-association
lifetime kilobytes 46080000
crypto dynamic-map 5505DYN-MAP 5 set reverse-route
```

```
crypto map 5505MAP 60 ipsec-isakmp dynamic 5505DYN-MAP
crypto map 5505MAP interface outside
telnet timeout 5
ssh 10.8.0.0 255.254.0.0 inside
ssh timeout 5
ssh version 2
console timeout 0
dhcpd ping_timeout 750
!
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
!
tls-proxy maximum-session 1000
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 enable outside
group-policy 5505Group internal
group-policy 5505Group attributes
 ip-comp enable
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value RA_SplitTunnelACL
 user-authentication-idle-timeout 480
 nem enable
group-policy DfltGrpPolicy attributes
 dns-server value 10.8.48.10
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value RA_SplitTunnelACL
 default-domain value cisco.local
 address-pools value RAPool
username 5505site1 password OxCSnUHMIWqoYx3T encrypted
username 5505site1 attributes
 vpn-group-policy 5505Group
username admin password w2Y.6Op4j7clVDk2 encrypted privilege 15
tunnel-group DefaultRAGroup general-attributes
 address-pool RAPool
 authentication-server-group cisco.local LOCAL
tunnel-group DefaultWEBVPNGroup general-attributes
 address-pool RAPool
 authentication-server-group cisco.local LOCAL
tunnel-group RA5505 type remote-access
tunnel-group RA5505 general-attributes
 default-group-policy 5505Group
!
class-map inside-class
 match access-list inside_mpc
class-map inspection_default
class-map outside-class
 match access-list outside_mpc
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  ips inline fail-open
policy-map IPS-Inside
 class inside-class
  ips inline fail-open sensor vs0
policy-map IPS-Outside
 class outside-class
  ips inline fail-open sensor vs0
!
service-policy global_policy global
service-policy IPS-Inside interface inside
service-policy IPS-Outside interface outside
prompt hostname context
call-home
 profile CiscoTAC-1
```

```
  no active
  destination address http https://tools.cisco.com/its/service/
oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:847cd64b81a5aaedff141358ba96c527
: end
```

IPS

```
! ------------------------------
! Current configuration last modified Fri Apr 15 12:16:18 2011
! ------------------------------
! Version 7.0(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S479.0   2010-03-19
!     Virus Update        V1.4     2007-03-02
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.8.63.24/24,10.8.63.1
host-name p2-ie-aip-10b
telnet-option disabled
access-list 10.0.0.0/8
dns-primary-server enabled
address 10.8.48.10
exit
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset -480
standard-time-zone-name PST
exit
ntp-option enabled-ntp-unauthenticated
ntp-server 10.8.48.17
exit
summertime-option recurring
offset 60
summertime-zone-name PDT
exit
auto-upgrade
cisco-server disabled
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
```

```
service signature-definition sig0
signatures 1610 0
status
enabled true
exit
exit
signatures 1611 0
status
enabled true?
exit
exit
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/1
exit
exit
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

B-56000019-1 8/11