远程办公解决方案部署指南

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

本指南主要面向在企业中承担以下职务的人员：

- 需要解决方案标准实施规程的系统工程师
- 需要获取参考资料以撰写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IBA指南作为工程师之间和各个部署项目的统一指导文件，或利用它更好地规划部署任务的工作范围和成本预算。

版本系列

思科每年对IBA指南进行两次更新和修订。在发布IBA指南系列之前，我们会在IBA实验室对其进行整体评测。为确保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。

您可以通过以下网址查看最新的IBA指南系列：

客户登录：http://www.cisco.com/go/sba

合作伙伴登录：http://www.cisco.com/go/sbachannel

如何阅读命令

许多IBA指南都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

概述 2

AnyConnect PC 和电话 3
- 业务概述 3
- 技术概述 3
- 部署详情 3
- 配置 Cisco ASA 4
- 配置 CUCM 5
- 配置 IP 电话 8

Cisco ASA 5505 11
- 业务概述 11
- 技术概述 11
- 部署详情 11
- 配置用于远程工作人员 VPN 的互联网边缘 ASA 12
- 配置远程工作人员 Cisco ASA 5505 终端 17

OfficeExtend 19
- 业务概述 19
- 技术概述 19
- 部署详情 19
- 配置互联网边缘 20
- 配置局域网 22
- 配置 WLC 23
- 配置 600 系列 OfficeExtend 接入点 27

附录 A：产品列表 29

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**附加部署指南**。思科IBA部署指南包含以下章节：

- **业务概述**——描述了本指南中提出的解决方案的具体功能和应用价值。这一章节的内容对业务决策者尤为重要。
- **技术概述**——描述了支持此企业应用情形的技术解决方案，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**——详细描述各个部署步骤，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，附加部署指南总是紧随基础部署指南之后，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

概述

目前，与远程通信一样，远程办公已不再是一个新概念。早在 2010 年，IDC 就估计全球有超过 3000 万远程工作人员。远程工作人员与移动工作人员的不同之处在于，他们需要一个更像办公室的环境，通常在一个半永久性地点办公，大多数情况是在家中。这些工作人员与主管间可以是非正式的工作关系，也可以有更加规范化的工作安排，遵循书面政策，须注册登记。

如今，远程工作人员效率越来越高，连通性越来越好，这使得公司能够招聘到位于世界各地的优秀人才。同时，远程工作也能帮助员工达成工作与生活间的最佳平衡，在保持出色生产率和业务连续性的同时，提高员工的工作满意度。

支持员工从居住环境访问联网业务服务，给最终用户和 IT 部门带来了巨大的挑战。对于在家中办公的远程工作人员来说，关键是要能够可靠、一致地访问业务服务，获得类似于坐在公司大厦的格子间或办公室的体验。此外，解决方案还必须支持各种不同技能的远程员工，因而能够轻松、简便地部署可接入公司环境的设备至关重要。

IT 部门在部署远程办公解决方案方面，面临着一系列不同的挑战，包括如何从中央站点正确保护、维护和管理远程工作人员环境等。云计算服务的推出，要求 IT 部门在确保员工能够访问这些服务的同时，提供安全的互联网接入，将病毒或攻击风险降至最低。鉴于运营开支始终是一个重要考虑因素，IT 部门必须部署经济高效的解决方案，在不影响质量或功能的情况下提供全面的投资保护。

远程工作人员的需求各不相同，具体取决于他们完成工作所需的信息类型和信息访问频率。而远程办公需要的技术也千差万别，没有一个“万能”的解决方案。为优化公司的远程工作人员解决方案，企业必须了解单个最终用户的独特需求，同时为遍布各地的全体用户提供一个统一、安全的操作环境。

思科提供了一套远程办公解决方案，配以多种选项，适用于所有类型的远程工作人员。思科远程办公解决方案包括：

- Cisco AnyConnect PC 和电话
- 思科自适应安全设备(ASA)系列 5505
- Cisco OfficeExtend
- 思科虚拟办公室(CVO)

本文分为多个部分，每部分介绍一种远程办公解决方案。为帮助您明确哪种远程办公解决方案最适合贵公司，请使用下表确定您的需求和对应的解决方案。

表 1. 远程办公需求和对应的解决方案

您的需求	AnyConnect PC+电话	ASA 5505	OfficeExtend
无线连接	X[1]		X
有线连接	X[1]	X	X[2]
高效的站点内通信[3]		X	
配置复杂度	中等	高	低
永续性	中等	中等	低
此解决方案的建议支持人数	500	50	500

注：

1. 每个设备都必须本地支持 AnyConnect。
2. OfficeExtend 600 系列接入点支持一条物理局域网连接和多达四个 MAC 地址。
3. 是指流量不必离开站点，在设备间通信。

AnyConnect PC 和电话

业务概述

支持员工从居住环境访问联网业务服务，给最终用户和 IT 部门带来了巨大的挑战。对于在家中办公的远程工作人员来说，关键是要能够可靠、一致地访问业务服务，获得类似于坐在公司大厦的格子间或办公室的体验。然而，许多员工已在家中进行了个人网络设置，因为缺少以太网线或会在 2.4GHz 无线频段发生拥堵，并行集成另一网络的作法恐怕不太现实。

IT 部门在部署远程办公解决方案方面，面临一系列挑战，包括如何从中央站点正确保护、维护和管理远程工作人员环境等。鉴于运营开支始终是一个重要考虑因素，IT 部门必须部署经济高效的解决方案，在不影响质量或功能的情况下提供全面的投资保护。

技术概述

适用于 Cisco Unified IP 电话的 Cisco VPN 客户端与适用于 PC 和笔记本电脑的 Cisco AnyConnect 客户端共用，为那些远程工作人员只需要访问数据和语音服务的企业，提供了出色的解决方案。

本解决方案以《IBA 智能业务平台大型企业互联网边缘部署指南》中所介绍的远程接入 VPN 解决方案为基础。该解决方案无需任何修改，就能同时用于支持移动用户和远程工作人员。

因为员工可能全天候远程办公，为了提供与办公室更为接近的环境，本解决方案使用了物理电话，而非在 PC 上运行的软电话。另外，为将电话与员工所属企业相连，本解决方案采用了适用于 Cisco Unified IP 电话的 Cisco VPN 客户端。Cisco VPN 客户端：

- **易于部署**——您可通过CUCM管理，完成所有设置。该电话使用ASA上现有的VPN群组配置，建立一条VPN连接，连接到与AnyConnect PC客户端相连的ASA设备对。
- **易于使用**——在大型企业环境中完成电话的配置后，用户可将其带回家，插入宽带路由器中，立即实现连接，无需配置繁杂的菜单。此外，如果企业为远程工作人员提供的是一部Cisco Unified IP电话9971和一台配有无线网卡的笔记本电脑，那么该解决方案无需家庭办公室具备有线连接。
- **易于管理**——电话能够远程进行固件更新和配置更改。
- **安全可靠**——VPN隧道仅适用于来自于电话本身的流量。一台连接到PC端口的电脑负责运行VPN客户端软件，进行身份验证并建立自己的隧道。和AnyConnect PC客户端一样，对电话进行身份验证需要用户提供Active Directory用户名和密码。

这就需要电话预先配置，并在公司网络内部建立初始连接，以检索电话配置。在电话检索到配置后，再使用 VPN 建立后续连接。

目前支持以下电话型号：7942/7962/7945/7965/7975/8900/9900。

部署详情

本部署指南采用了特定的标准设计参数，并参考了多种不属于 CVO 解决方案范畴的网络基础设施服务。这些参数如下表所列。

表 2. 通用设计参数

网络服务	IP 地址
域名	cisco.local
Active Directory、DNS 服务器、DHCP 服务器	10.10.48.10
RADIUS 身份验证系统(Windows Server)	10.10.48.10
网络时间协议(NTP)服务器	10.10.48.17
IP 组播汇聚点(Anycast RP)	10.10.15.252

流程

配置 Cisco ASA

1. 创建身份证书

以下 Cisco ASA 配置假定设备已采用《面向中小企业的 IBA 智能业务平台——无边界网络基础部署指南》远程接入 VPN 章节中的流程进行了预先配置。

程序 1　创建身份证书

为能够从 IP 电话连接至 Cisco ASA，您必须将该设备的一份身份证书导入 Cisco Unified Communications Manager 中。

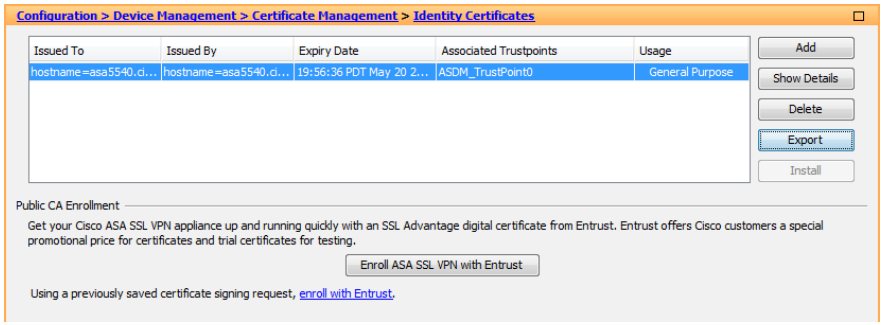
自行签发的身份证书（在基础部署指南中面向 Cisco ASA 的远程接入 VPN 配置流程期间配置）必须导出为 base64 格式文件，然后再导入到 Cisco Unified Communications Manager 中。

步骤 1：启动 ASA 安全设备管理器。

步骤 2：在 **Configuration（配置）> Device Management（设备管理）> Certificate Management（证书管理）**中，点击 **Identity Certificates（身份证书）**。

步骤 3：从身份证书列表中，选择正在使用的身份证书。（例如：ASDM_TrustPoint0）

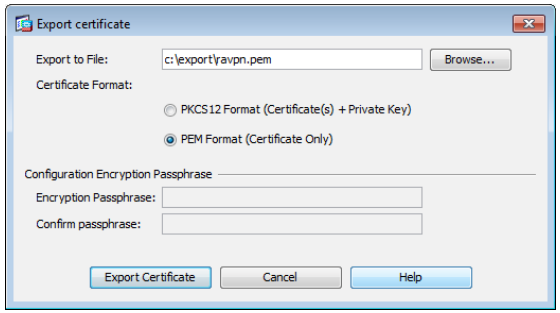
步骤 4：点击 **Export（导出）**。



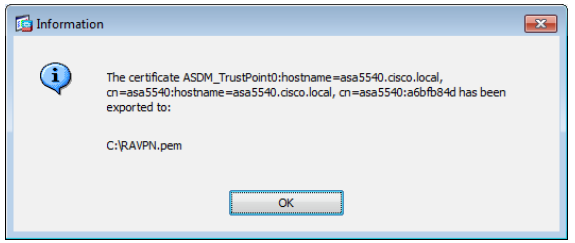
步骤 5：在 Export certificate（导出证书）对话框中，为证书输入一个文件名。（例如：C:\RAVPN.pem)

步骤 6：选择 **PEM Format (Certificate Only)（PEM 格式（仅限证书）。**

步骤 7：点击 **Export Certificate（导出证书）。**



步骤 8：Information（信息）对话框显示证书已导出，点击 **OK。**



步骤 9：点击 **Apply（应用）。**

流程

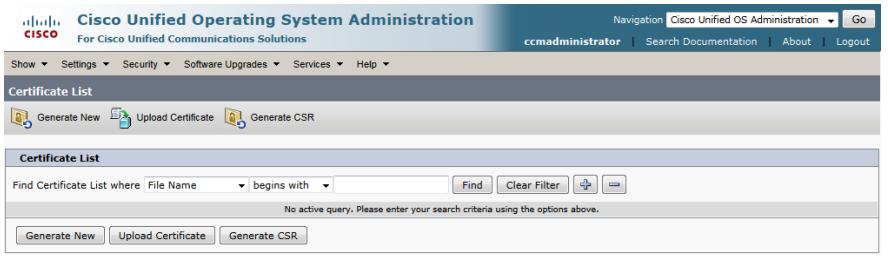
配置 CUCM

1. 导入 ASA 证书
2. 配置 VPN 网关
3. 配置 VPN 群组
4. 设置 VPN 配置文件
5. 配置 VPN 功能
6. 配置通用电话配置文件

程序 1　导入 ASA 证书

步骤 1：转至 Cisco Unified Communications Manager Operating Systems Administration（Cisco Unified Communications Manager 操作系统管理）页面。（例如：https://cucm.cisco.local/cmplatform/）

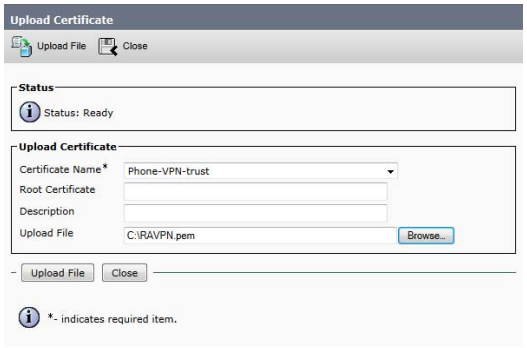
步骤 2：在 Security（安全）> Certificate Management（证书管理）中，点击 Upload Certificate（上传证书）。



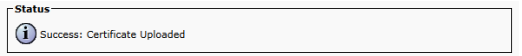
步骤 3：在 Upload Certificate（上传证书）页，Certificate Name（证书名称）选择 Phone-VPN-trust。

步骤 4：在 Upload File（上传文件）框中，输入程序 1 步骤 5 中获得的证书文件名称。

步骤 5：点击 Upload File（上传文件）。

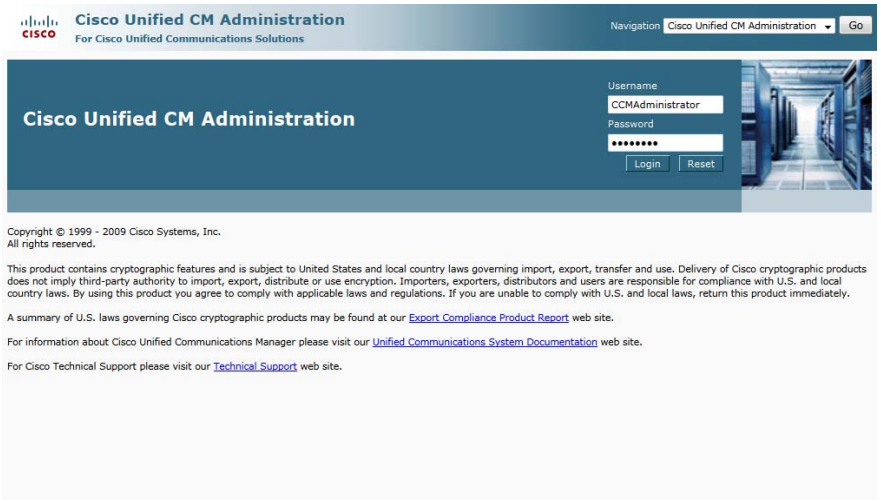


步骤 6：上传完成后，Status（状态）窗格显示 Success: Certificate Uploaded（成功：证书已上传）。

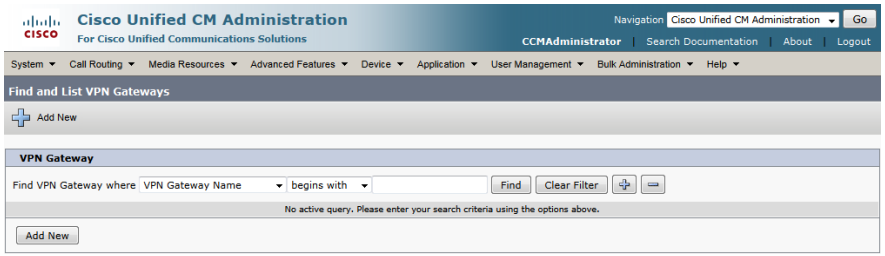


程序 2　配置 VPN 网关

步骤 1：在 Navigation（导航）中选择 **Cisco Unified CM Administration（Cisco Unified CM 管理）**，然后点击 **Go（开始）**。



步骤 2：在 **Advanced Features（高级功能）> VPN > VPN Gateway（VPN 网关）**中，点击 **Add New（添加新网关）**。

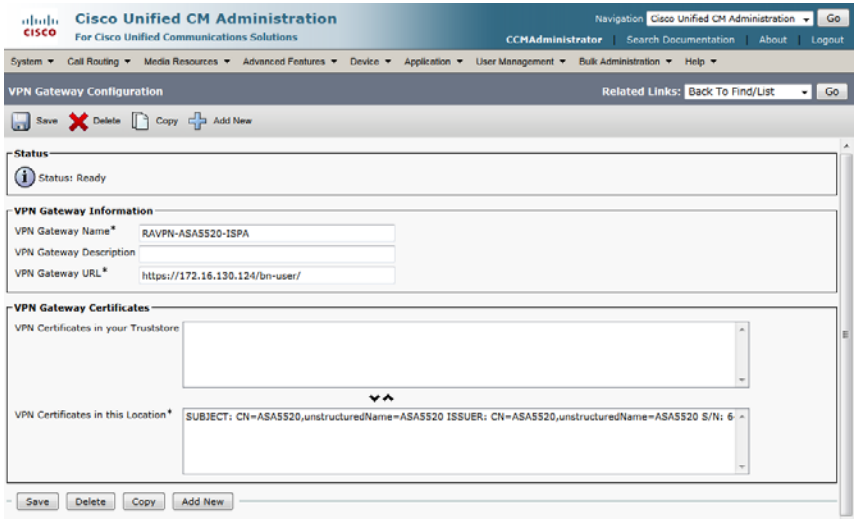


步骤 3：在 VPN Gateway Configuration（VPN 网关配置）页面，输入一个 VPN 网关名称。（例如：IE-ASA5520)

步骤 4：在 **VPN Gateway URL（VPN 网关 URL）**框中，输入 Cisco ASA 主互联网链接上 VPN 群组的 URL。（例如：https://172.17.30.2/anyconnect/)

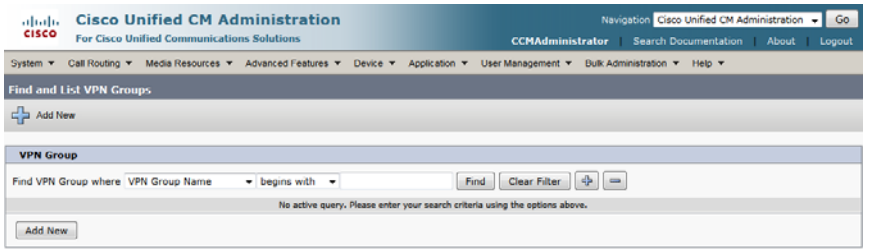
步骤 5：在 VPN Gateway Certificates（VPN 网关证书）窗格，通过选中证书并点击**下箭头**，将证书从可信库移动到该位置。

步骤 6：点击 **Save（保存）**。



程序 3　配置 VPN 群组

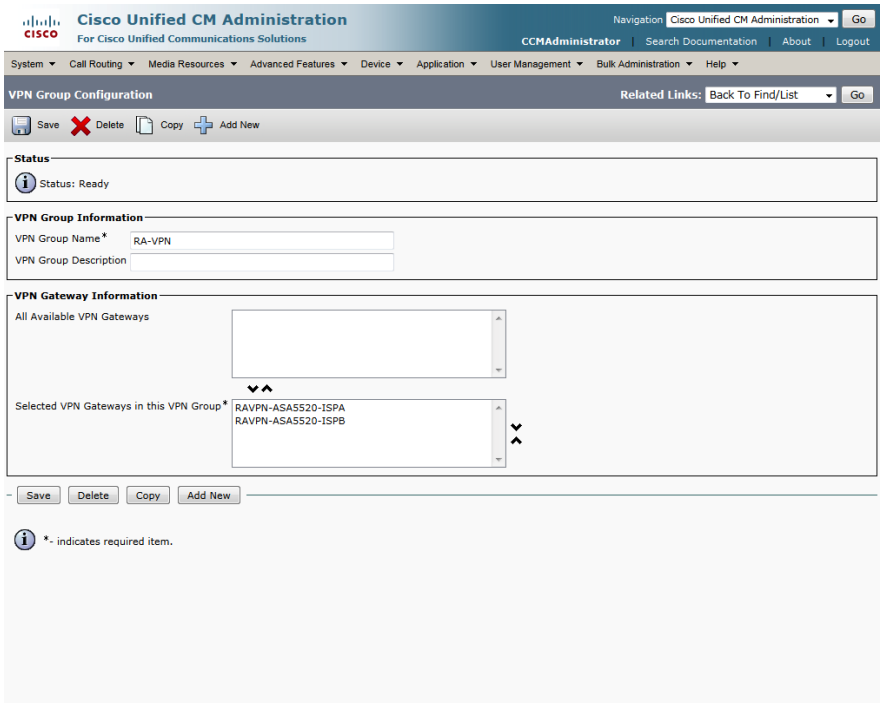
步骤 1：在 **Advanced Features（高级功能）> VPN > VPN Group（VPN 群组）**中，点击 **Add New（添加新群组）**。



步骤 2：在 VPN Group Configuration（VPN 群组配置）页面，输入一个 **VPN 群组名称。**（例如 RA-VPN）

步骤 3：通过选中网关并点击**下箭头**，将主 VPN 网关从 **Available VPN Gateway list（可用 VPN 网关列表）**移动到 **Selected VPN Gateway list（所选 VPN 网关列表）**。

步骤 4：点击 Save（保存）。



程序 4　设置 VPN 配置文件

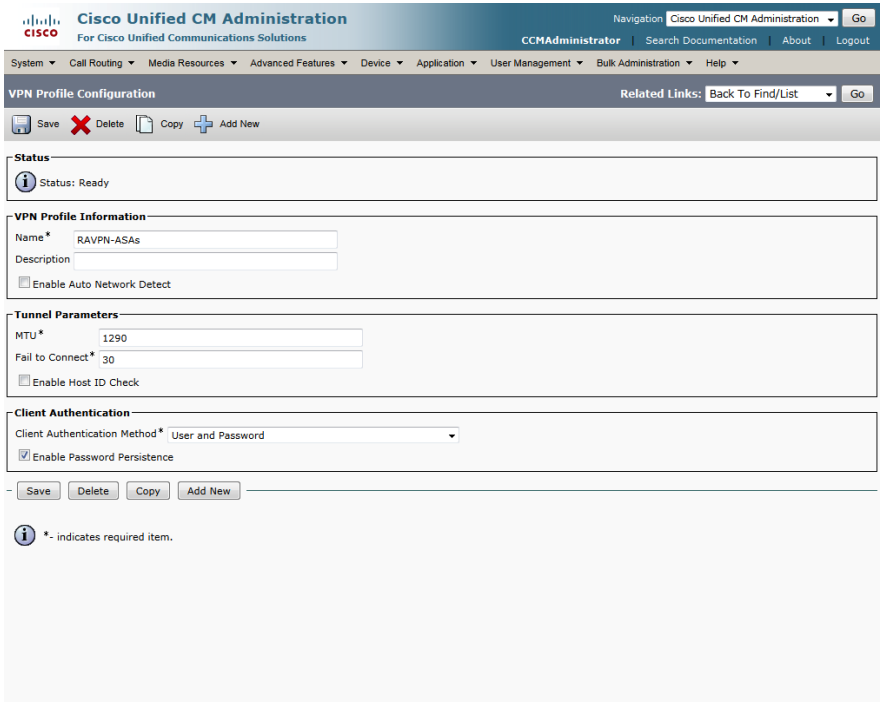
步骤 1：在 Advanced Features（高级功能）> VPN > VPN Profile（VPN 配置文件）中，点击 Add New（添加新 VPN 配置文件）。

步骤 2：在 VPN Profile Configuration（VPN 配置文件配置）页面，输入一个 Name（名称）。（例如：RAVPN-ASAs)

步骤 3：因为 ASA 身份证书是自行签发的，请不要勾选 Enable Host ID Check（启用主机 ID 检查）。

步骤 4：选择 Enable Password Persistence（启用永久密码）。

步骤 5：点击 Save（保存）。

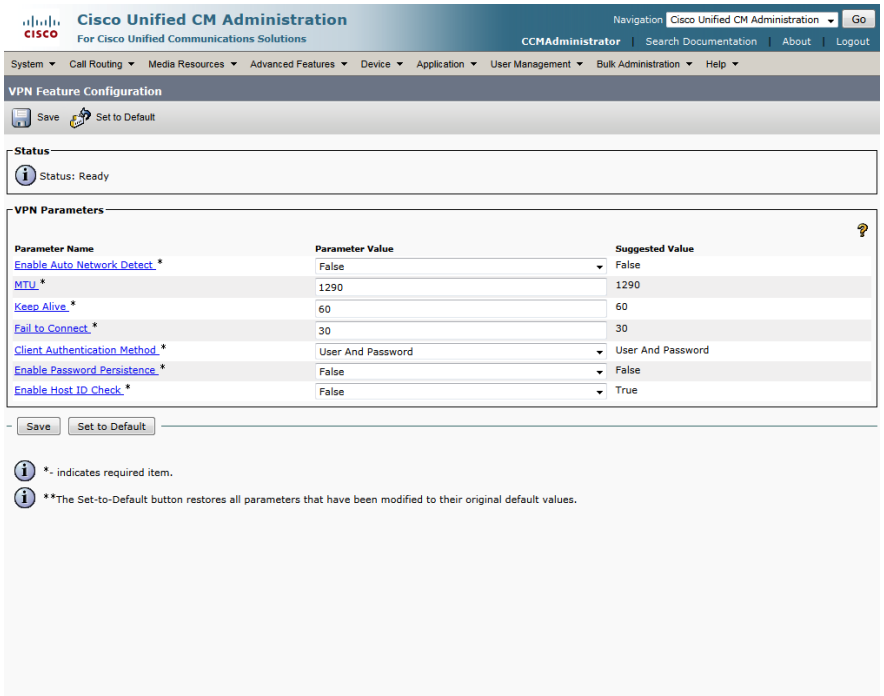


程序 5　配置 VPN 功能

步骤 1：在 Advanced（高级）>VPN 中，点击 VPN Feature Configuration（VPN 功能配置）。

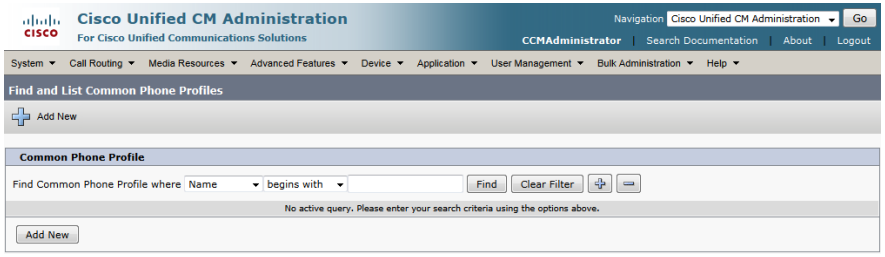
步骤 2：因为 ASA 身份证书是自行签发的，所以应在 Enable Host ID Check（启用主机 ID 检查）字段中选择 False（不适用）。

步骤 3：点击 Save（保存）。



程序 6　配置通用电话配置文件

步骤 1：在 Device（设备）> Device Settings（设备设置）> Common Phone Profile（通用电话配置文件）中，点击 Add New（添加新配置文件）。



步骤 2：在 Common Phone Profile Configuration（通用电话配置文件设置）页面，输入 Name（名称）。（例如：VPN Common Phone Profile)

步骤 3：在 VPN information (VPN 信息) 窗格中，选择程序 3 中创建的 VPN Group (VPN 群组）。（例如：RA-VPN)

步骤 4：在 VPN information (VPN 信息) 窗格中，选择程序 4 中创建的 VPN Profile (VPN 配置文件）。（例如：RAVPN-ASAs)

步骤 5：点击 Save（保存）。

流程

配置 IP 电话

1. 注册和配置设备
2. 连接 IP 电话

在使用 VPN 前，电话必须从机构网络内部，在 Cisco Unified Communications Manager 上注册。注册流程将更新电话固件并下载电话配置，包括 VPN 设置。

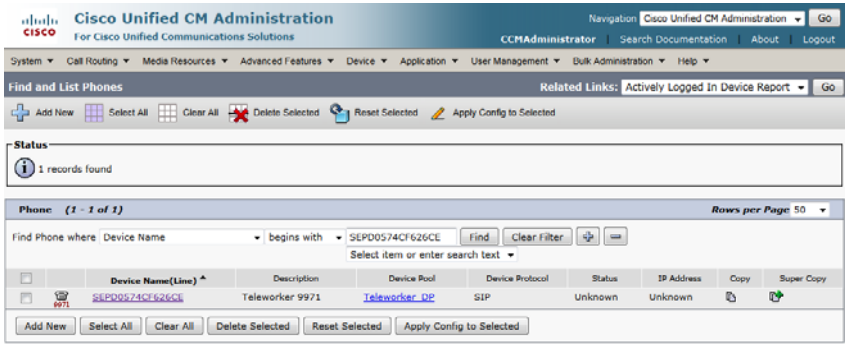
以下流程为注册设备配置了 VPN 信息，以便它能在企业网络之外部署。

程序 1　注册和配置设备

步骤 1：在 Device（设备）> Phone（电话）中，在搜索文本框中输入设备名称。

步骤 2：点击 Find（搜索）。

步骤 3：如需打开 Phone Configuration（电话配置）页面，点击 **Device Name（设备名称）。**

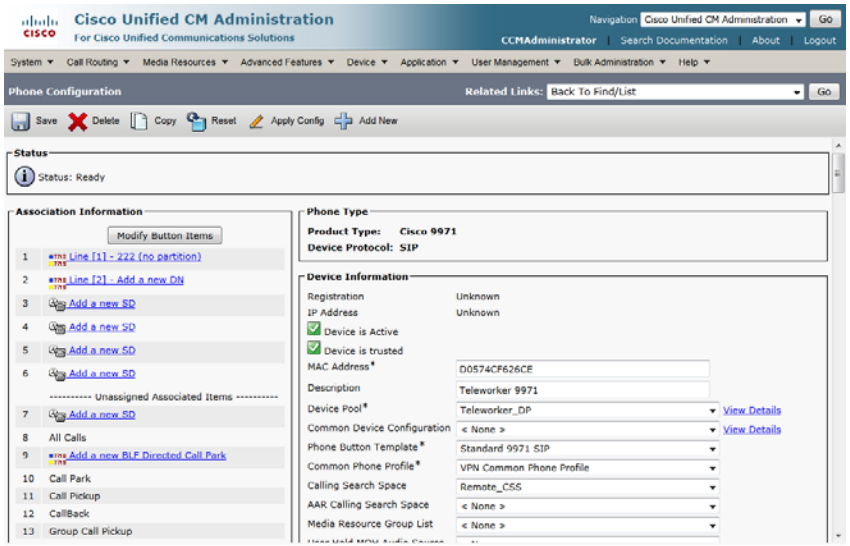


步骤 4：在 Phone Configuration（电话配置）页，选择 **Device Pool（设备池）。**（例如：Teleworker_DP)

步骤 5：选择程序 6 中创建的 **Common Phone Profile（通用电话配置文件）。**（例如：VPN Common Phone Profile)

步骤 6：选择 **Calling Search Space（呼叫搜索空间）**，点击 **Save（保存）。**（例如：Remote_CSS)

步骤 7：点击 **Apply Config（应用配置）。**



程序 2　连接 IP 电话

步骤 1：将电话与用户的家庭网络相连。

步骤 2：为通过 VPN 将电话与企业相连，选择 **Applications（应用）> VPN。**

步骤 3：对于 **VPN Enabled（启用 VPN）**项，选择 **On（打开）。**

步骤 4：输入用户 ID 和密码。

步骤 5：按 **Sign In（登入）**，VPN Status（VPN 状态）显示为 **Connected（连接）**。

备注

Cisco ASA 5505

业务概述

目前，许多企业都日益需要为员工提供远程办公解决方案。员工们普遍认为上下班路上和办公室闲聊的时间都属于“工作”时间，而企业需要租用或购买办公室场地和办公家具，甚至部署用于为员工提供支持的网络基础设施，这些加起来是巨大的投资和运营开支。

在远程工作人员家中提供类似办公室的工作环境，需要：

- 一部能作为企业电话系统分机的电话。
- 一个运行安静、平稳的低功率解决方案，为一部或多部 IP 电话或其它桌面协作资源提供多条以太网连接。
- 一条或多条供计算机接入企业网络的以太网连接，以及用于其它联网设备，如打印机和 IP 视频监视设备等的以太网连接。

在远程办公地点，无需无线连接，因为所有远程办公资源都使用有线以太网。

技术概述

Cisco ASA 5505 是远程工作人员连接企业总部的低成本选择。Cisco ASA 5505 在一个紧凑、无风扇的机型中，为数据和协作终端提供了安全连接，最大程度降低了噪音级别和空间需求。

Cisco ASA 5505 远程办公解决方案可以与思科 IBA 智能业务平台中小企业或大型企业设计的互联网边缘部分相集成。远程工作人员连接在总部或是备用站点，如地区办公室或业务连续性站点处的永续 Cisco ASA 防火墙上端接。尽管某些配置可以完全不使用远程接入虚拟专用网(RAVPN)资源，但也可以重复利用其中的一些配置。对于 Cisco ASA 5505 远程工作人员终端的支持不会影响到 RAVPN 的连接，配置的应用不会造成服务的中断。

Cisco ASA 5505 远程工作人员解决方案为终端设备，如笔记本电脑和台式机、IP 电话、打印机，以及其它通过有线以太网与网络相连的设备等，提供了网络接入功能。Cisco ASA 5505 的两个端口提供有以太网供电，可支持 IP 电话、IP 视频监视和其它终端，而不必在远程工作人员的办公室布置大量线缆和“墙壁”电源。

ASA 5505 远程工作人员解决方案提供：

- **低廉的成本**——完美结合了 Cisco ASA 5505、思科 IP 电话，以及总部互联网边缘 ASA 上的必要许可证。
- **灵活的连接**——Cisco ASA 5505 的集成以太网交换机能支持多种终端设备，包括两个可提供 PoE 的接口。
- **简单的部署**——Cisco ASA 5505 能使用简要文本文件配置，快速完成配置工作。
- **安全可靠**——远程工作人员的连接可通过取消激活总部设备上的远程办公站点证书而终止。

在理想状态下，Cisco ASA 5505 远程工作人员的设备将在预配置后，送回到他们的家中。此外，他们还可将新配置的桌面 IP 电话或已有桌面 IP 电话带回家，并通过 VPN 在 Call Manager 服务器上注册。

部署详情

远程接入连接的配置分两个阶段。在第一阶段，您将在总部配置永续的互联网边缘设备对，以接收来自远程工作人员 5505 设备的 VPN 连接。在第二阶段，您将进行远程工作人员 5505 硬件客户端上的配置。

流程

配置用于远程工作人员 VPN 的互联网边缘 ASA

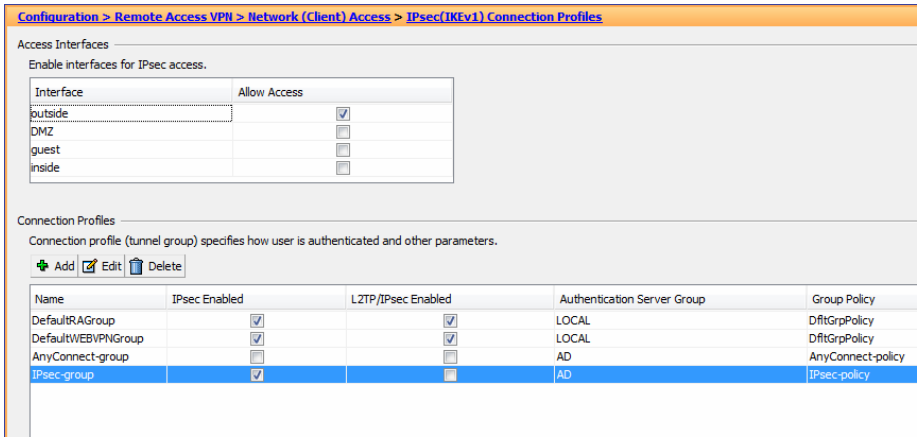
1. 配置 IPsec(IKEv1)连接配置文件
2. 配置 NAT 豁免策略

按照规定，针对 Cisco ASA 5505 远程工作人员 VPN 的总部互联网边缘 Cisco ASA 配置是独立的。但有几个特性取决于互联网边缘基础的配置，因此您需要遵循《面向中小企业的 IBA 智能业务平台——无边界网络基础部署指南》中关于 Cisco ASA 远程接入 VPN 的配置步骤。

程序 1　配置 IPsec(IKEv1)连接配置文件

IPsec 连接配置文件中包括大量设定 VPN 客户端连接行为的配置，因此在这一流程中，您必须执行多个步骤，来完成中央配置。

步骤 1：转至 **Configuration（配置）** > **Remote Access VPN（远程接入 VPN）** > **Network (Client) Access（网络（客户端）接入）** > **IPsec(IKEv1)Connection Profiles（IPsec(IKEv1)连接配置文件）**选项卡，在 **Connection Profiles（连接配置文件）**下方右边的面板中，点击 **Add（添加）**按钮。



步骤 2：在 **Add IPsec Remote Access Connection Profile（添加 IPsec 远程接入连接配置文件）**面板中，输入以下详细信息。该配置会影响 5505 远程工作人员设备的行为，如下所述：

- 名称：Teleworker5505

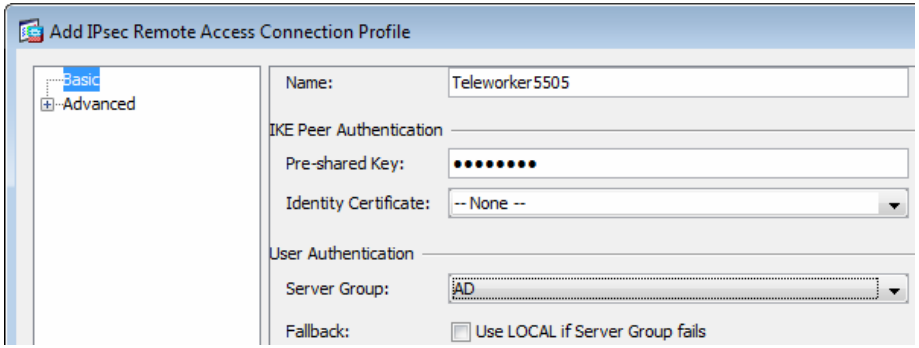
  这是 5505 Easy VPN 客户端配置中将用到的 VPN 群组的名称。

- IKE 设备对身份验证预共享密钥：[IKE Group Key]

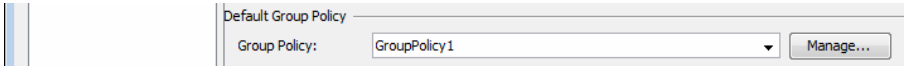
  这是必须在 5505 Easy VPN 客户端配置中重复输入的群组密钥。

- 服务器组：选择 AD

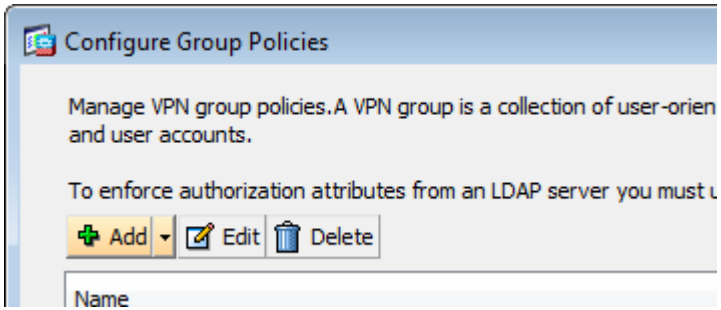
  通过选择网络的 Windows 域控制器，用于验证为打开 Easy VPN 客户端隧道而提交的用户名和密码。



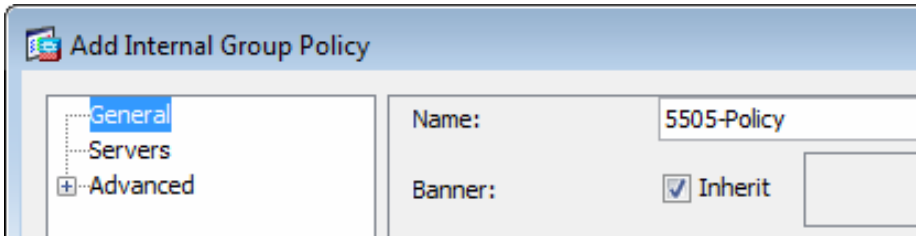
步骤 3：在 **Group Policy（群组策略）**列表的右侧，点击 **Manage（管理）**。



步骤 4：在 Configure Group Policies（配置群组策略）面板中（通过点击 Manage（管理）打开，如上所示），点击 **Add（添加）**。

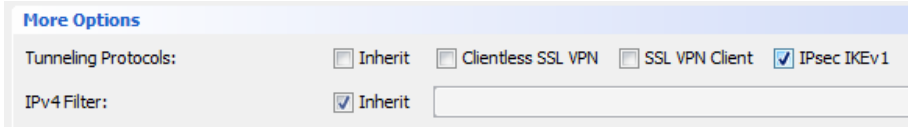


步骤 5：在 Add Internal Group Policy（添加内部群组策略）窗口，选择 **General（常规）**，然后在 **Name（名称）**框中输入 5505-Policy。

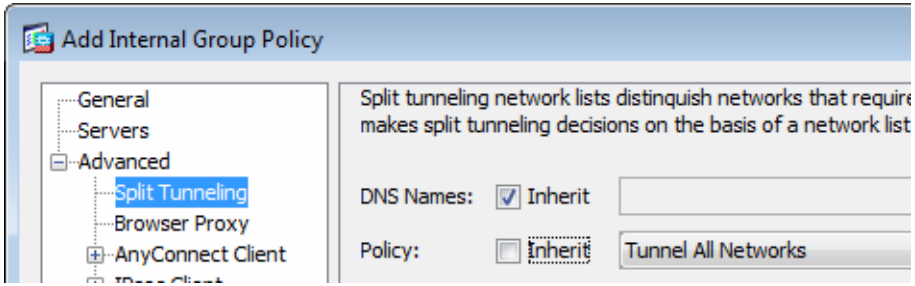


步骤 6：点击 **More Options（更多选项）**，展开选项面板。

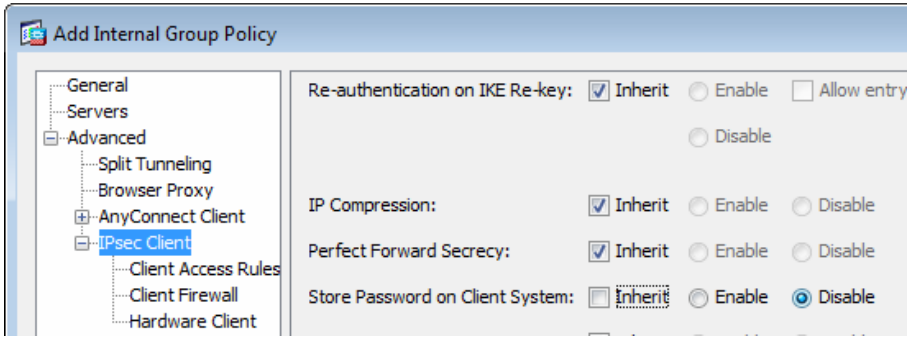
步骤 7：在 Tunneling Protocols（隧道协议）旁，取消勾选 **Inherit（继承）**，然后选择 **IPsec IKEv1**。



步骤 8：转至 **Advanced（高级）> Split Tunneling（分离隧道）**，在右侧面板中，取消勾选 Policy（策略）旁的 **Inherit（继承）**。在“Policy”（策略）行，确保选择 **Tunnel All Networks（隧道连接所有网络）**。

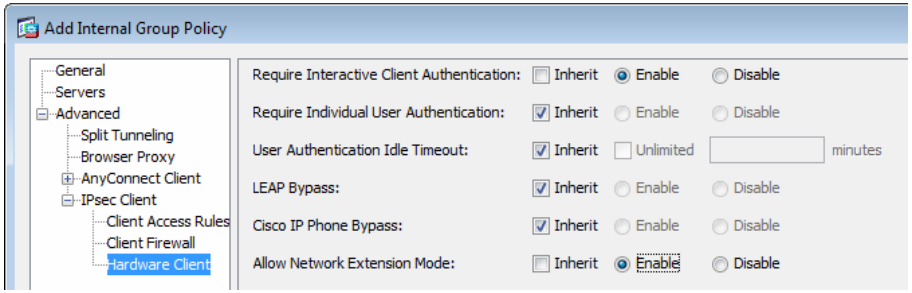


步骤 9：转至 **Advanced（高级）> IPsec Client（IPsec 客户端）**，取消勾选位于 Store Password On Client System（将密码存储在客户端系统中）旁边的 **Inherit（继承）**。确保选择 **Disable（禁用）**。



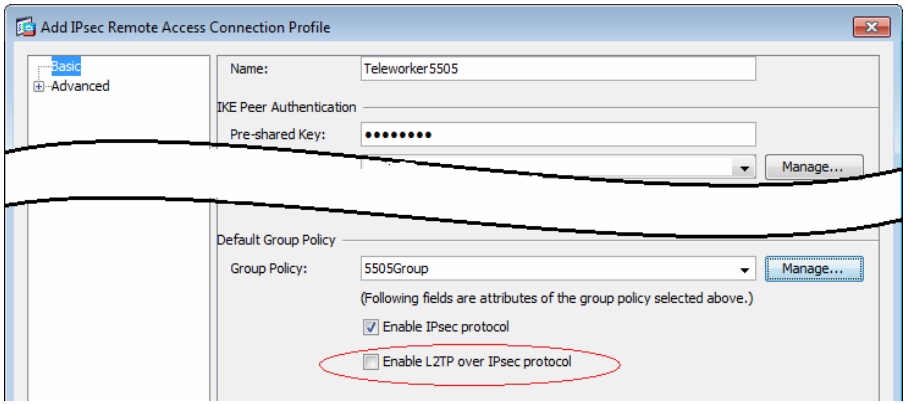
步骤 10：转至 Advanced（高级）> IPsec Client（IPsec 客户端）> Hardware Client（硬件客户端），完成以下任务：

- 取消勾选位于 Require Interactive Client Authentication（需要交互式客户端身份验证）旁边的 Inherit（继承），确保选择 Enable（启用）。
- 取消勾选位于 Allow Network Extension Mode（许可网络扩展模式）旁边的 Inherit（继承），确保选择 Enable（启用）。
- 点击 OK。

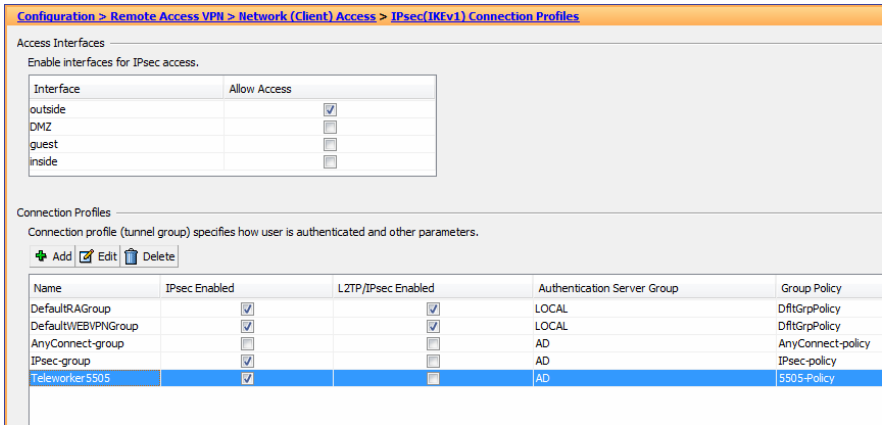


步骤 11：在 Configure Group Policies（配置群组策略）窗口中，点击 OK。

步骤 12：在 Add IPsec Remote Access Connection Profile（添加 IPsec 远程接入连接配置文件）窗口，取消勾选 Enable L2TP over IPsec protocol（启用 L2TP over IPsec 协议），然后点击 OK。



步骤 13：在 Access Interfaces（接入接口）下，设备的外部接口旁边，确保勾选 Allow Access（允许接入）复选框。



步骤 14：在 Connection Profiles（连接配置文件）下，确认新的 Teleworker5505 配置文件已出现，然后点击 Apply（应用）。

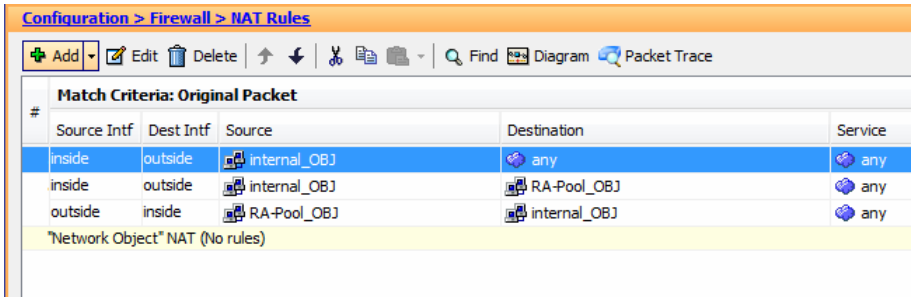
通过完成以上步骤，将应用下面的配置。

```
group-policy 5505-Policy internal
group-policy 5505-Policy attributes
 password-storage disable
 vpn-tunnel-protocol ikev1
 split-tunnel-policy tunnelall
 secure-unit-authentication enable
 nem enable
exit
tunnel-group Teleworker5505 type remote-access
tunnel-group Teleworker5505 general-attributes
 default-group-policy 5505-Policy
 authentication-server-group AD
tunnel-group Teleworker5505 ipsec-attributes
 ikev1 pre-shared-key [c1sco123]
```

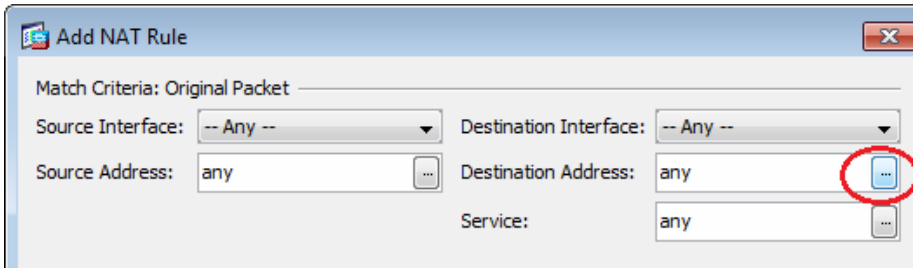
程序 2　配置 NAT 豁免策略

对于进出包含远程工作人员远程地址的 IP 子网的流量，互联网边缘设备不得应用网络地址转换 (NAT)。您必须配置一个策略来防止互联网边缘设备应用 NAT。

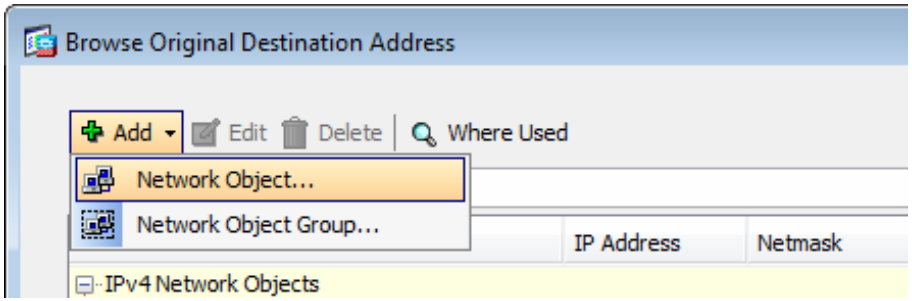
步骤 1：转至 Configuration（**配置**）> Firewall（**防火墙**）> NAT Rules（NAT **规则**），点击 Add（**添加**）旁边的下拉箭头，然后选择 Add NAT Rule Before“Network Object”NAT Rules...（“**网络对象**”NAT **规则前的添加 NAT 规则**...）



步骤 2：在 Add NAT Rule（**添加 NAT 规则**）窗口中，在 Match Criteria: Original Packet（**匹配标准：原始数据包**）下方，Destination Address（**目的地地址**）旁边，点击省略号(...)。

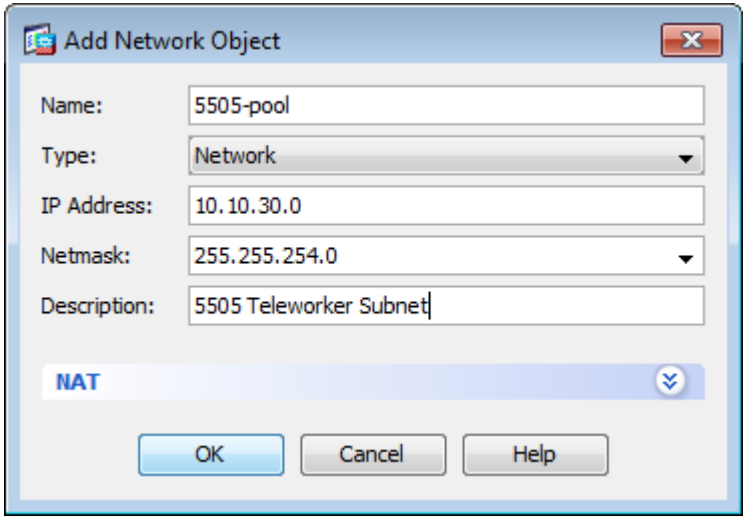


步骤 3：在 Browse Original Destination Address（**浏览原始目的地地址**）窗口，点击 Add（**添加**），然后点击 Network Object（**网络对象**）。

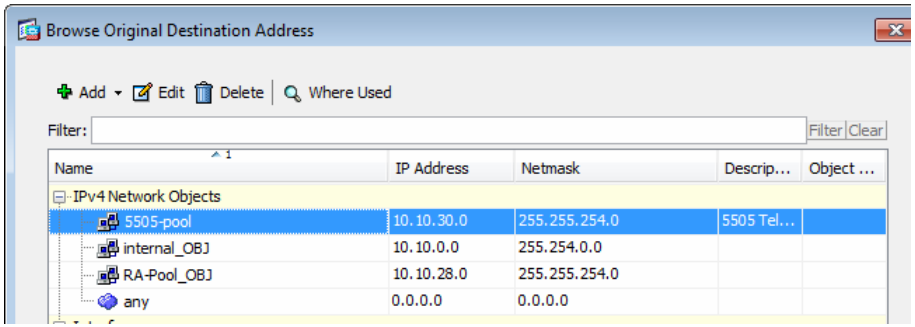


步骤 4：在 Add Network Object（**添加网络对象**）窗口中，输入以下值，然后点击 OK。

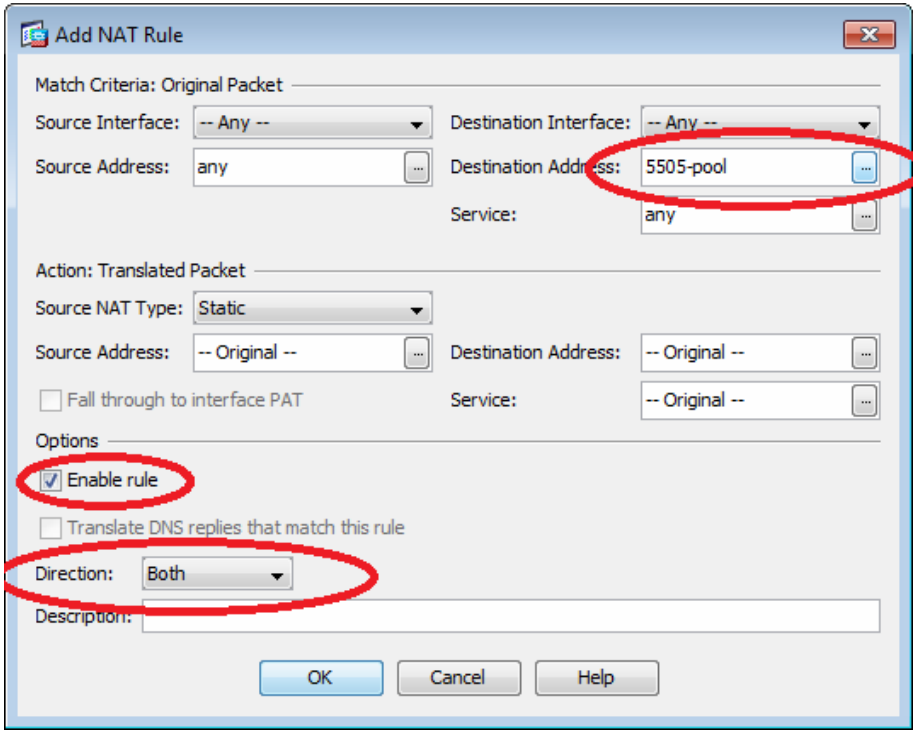
- 名称：5505-pool
- 类型：Network
- IP 地址：[10.10.30.0]
- 子网掩码：[255.255.254.0]
- 描述：5505 Teleworker Subnet



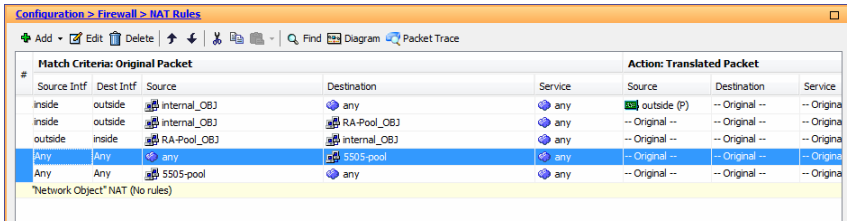
步骤 5：在 Browse Original Destination Address（浏览原始目的地地址）窗口中，在 IPv4 Network Objects（IPv4 网络对象）列表中，双击 5505-pool（选择 5505 远程工作人员子网作为原始目的地地址），然后点击 OK。



步骤 6：在 Add NAT Rule（添加 NAT 规则）窗口，Match Criteria:Original Packet > Destination Address（匹配标准：原始数据包 > 目的地地址）字段中，确认其值为 5505-pool。在 Options（选项）下，确保选择 Enable Rule（启用规则）且方向为 Both（双向），然后点击 OK。



步骤 7：查看配置，然后点击 Apply（应用）。



ASDM 将应用此配置：

```
object network 5505-pool
  subnet 10.10.30.0 255.255.254.0
  description 5505 Teleworker Subnet
nat 3 source static any any destination static 5505-pool 5505-pool
```

流程

配置远程工作人员 Cisco ASA 5505 终端

1. 定义全局设备配置
2. 配置内部 VLAN 和交换机端口
3. 配置外部 VLAN 和交换机端口
4. 配置 Cisco ASA 5505 DHCP 服务器
5. 配置 Cisco ASA 5505 Easy VPN 客户端

每位远程工作人员的 5505 设备都必须进行配置，以连接到总部的永续互联网边缘设备。因为此配置很有可能会部署在多个设备上，所以仅提供命令行界面配置，以简化部署。所有 5505 远程工作人员站点都将使用网络扩展模式进行连接，这种模式允许远程工作人员站点终端随意与企业局域网相连，这对于 IP 电话和视频监视摄像机等易受 NAT 数据流量修改影响的终端来说尤为重要。

每个站点必须使用一个独特的内部 IP 子网。否则，就会出现两个站点的所有配置都相同的情况。我们建议您制作并维护一个电子表格，其中记录将分发到 Cisco ASA 5505 远程办公设备的各用户的子网分配情况，以避免地址分配出现冲突。

用户名	ASA 5505 局域网地址	子网	主机名
Employee1	10.10.30.1	10.10.30.0/29	5505site1
Employee2	10.10.30.9	10.10.30.8/29	5505site2

程序 1　定义全局设备配置

步骤 1： 配置 Cisco ASA 5055 主机名和域名。

```
hostname 5505site1
domain-name cisco.local
```

步骤 2： 定义一个本地管理用户名。

username [admin] password [c1sco123] privilege 15

步骤 3： 设置启用密码。

enable password [c1sco123]

程序 2　配置内部 VLAN 和交换机端口

每个 5505 远程工作人员站点都需要一个独特的内部子网，您应在流程介绍部分建议的电子表格中找到它们。

步骤 1： 配置用于远程工作人员站点局域网的 VLAN 1 接口。

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 10.10.30.1 255.255.255.248
```

步骤 2： 将 Cisco ASA 5505 的以太网 0/1 到以太网 0/7 接口与 VLAN 1 相关联，并指导远程工作人员将 PoE 供电设备连接到以太网 0/6 和 0/7 端口。

```
interface Ethernet0/1
 switchport access vlan 1
 no shutdown
…
interface Ethernet0/7
 switchport access vlan 1
 no shutdown
```

步骤 3： 定义管理配置。

```
http server enable
http 10.0.0.0 255.0.0.0 inside
ssh 10.0.0.0 255.0.0.0 inside
management-access inside
```

程序 3　配置外部 VLAN 和交换机端口

步骤 1： 配置 VLAN 接口，以通过 DHCP 接收来自远程工作人员互联网网关设备的 IP 地址。

```
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp setroute
```

步骤 2： 将 Cisco ASA 5505 的以太网 0/0 接口与 VLAN 2 相关联，并指导远程工作人员将以太网 0/0 接口连接到互联网网关设备。

```
interface Ethernet0/0
 switchport access vlan 2
 no shutdown
```

程序 4　配置 Cisco ASA 5505 DHCP 服务器

Cisco ASA 5505 必须通过配置，为计算机、电话、打印机和视频监视设备等远程工作人员终端提供 IP 地址。每个站点必须使用一个独特的子网，您应在本流程介绍部分提及的电子表格中跟踪它们。

步骤 1：定义 DHCP 域的地址范围。DHCP 域必须与内部(VLAN 1)接口位于同一子网之中。

```
dhcpd address [10.10.30.2-10.10.30.6] inside
```

步骤 2： 配置将分发给客户的 DNS 和域名值。

```
dhcpddns10.10.48.10 interface inside
dhcpd domain cisco.local interface inside
```

步骤 3： 定义 DHCP 选项 150，为思科 IP 电话提供 Cisco Unified Call Manager Server 地址。

```
dhcpd option 150 ip 10.10.48.20
```

步骤 4： 启用 DHCP 域。

```
dhcpd enable inside
```

程序 5　配置 Cisco ASA 5505 Easy VPN 客户端

Cisco ASA 5505 使用 Easy VPN 网络扩展模式，与总部站点的 Cisco ASA 远程接入服务器进行有关 VPN 连接的协商。

步骤 1： 为远程工作人员的 Cisco ASA 5505 定义 Easy VPN 客户端连接属性：

- 将总部互联网边缘 ASA 的地址设定为 VPN 服务器值
- 设置网络扩展模式
- vpngroup 和密码值必须与您在总部设备上配置的 IPsec 远程接入连接配置文件相匹配。

```
vpnclient server 172.29.59.1
vpnclient mode network-extension-mode
vpnclient vpngroup Teleworker5505 password [c1sco123]
```

步骤 2： 启用 Cisco ASA 5505 Easy VPN 客户端：

```
vpnclient enable
```

远程工作人员必须手动启动其 VPN 连接；当用户通过 Web 浏览器访问总部网络上的 Web 内容时，Cisco ASA 5505 将截获该连接，并提供交互式登录提示。用户必须提供其登录证书，使用所提供的用户名和密码，协商 VPN 连接。

如果远程工作人员的 VPN 接入被宣告无效，则身份验证服务器将拒绝其访问。

OfficeExtend

业务概述

支持员工从居住环境访问联网业务服务，给最终用户和 IT 部门提出了严峻挑战。对于在家办公的远程工作人员，可靠一致地访问业务服务非常重要，他们需要获得与坐在公司大厦的格子间或办公室里相同的体验。然而，我们发现住宅和城市环境往往在常用的 2.4 GHz 无线频段上存在许多潜在的拥塞源。潜在的干扰源包括无绳手持设备、个人家用笔记本电脑、iPhone 或 iPod、婴儿监视器等等。此外，解决方案还必须支持众多具备不同技能集的远程工作人员，因而能够轻松、简便地部署可接入公司环境的设备至关重要。

IT 部门在部署远程办公解决方案方面，面临着一系列不同的挑战，包括如何从中央站点正确保护、维护和管理远程工作人员环境等。鉴于运营支出始终是一个重要考虑因素，IT 必须实施一款经济高效的解决方案，在不影响质量或功能的情况下提供全面的投资保护。

技术概述

Cisco OfficeExtend 解决方案专门针对主要使用无线设备的远程工作人员而设计，包含以下组件：

- Cisco Aironet 600 系列 OfficeExtend 接入点
- Cisco 5500 系列无线局域网控制器

Cisco OfficeExtend 解决方案配置、管理和故障排除工作在思科无线局域网控制器(WLC)上集中完成。每个 Cisco 5500 系列无线局域网控制器可支持多达 500 个 OfficeExtend 接入点。

本部署指南采用的 WLC 与局域网无线接入点所用的相同。这样就无需购买额外的硬件，降低了解决方案的总体成本。通常，提供面向公共互联网的服务的设备都部署在 DMZ 中，以降低内部主机的安全风险。鉴于由数据报传输层安全(DTLS)保护的无线接入点控制和配置流量是唯一被允许进出 WLC 的互联网流量，因而只存在极小的安全风险。此外，WLC 将配置为仅接受来自可信 OfficeExtend 接入点的连接，由此进一步降低了出现非法接入点连接的可能性。

为了使用户无需重新配置即可将其设备连接到企业的现场无线网络或家庭远程工作无线网络，OfficeExtend 远程工作解决方案在远程工作人员的家中提供了与在企业内部支持数据和语音服务所用的相同无线 SSID。

Cisco OfficeExtend 提供了全面的 802.11n 无线性能，可避免住宅设备由于同时在 2.4 GHz 和 5 GHz 无线频段运行所引起的拥塞。OfficeExtend 解决方案采用与网络核心相同的 QoS 和安全策略，因此没有要管理的叠加网络。

在家庭办公室进行初始设置时，远程员工可将接入点插入到与宽带调制解调器相连接或集成的家用路由器中。Cisco Aironet® 600 系列 OfficeExtend 接入点可以提前进行配置或由用户进行配置，将建立一个到位于公司总部的思科无线控制器的安全隧道。

部署详情

本部署指南采用了特定的标准设计参数，并参考了多种不属于 CVO 解决方案范畴的网络基础设施服务。这些参数如下表所列。

表 3. 通用设计参数

网络服务	IP 地址
域名	cisco.local
Active Directory、DNS 服务器、DHCP 服务器、Windows RADIUS	10.10.48.10
网络时间协议(NTP)服务器	10.10.48.17
IP 组播汇聚点	10.10.15.252

流程

配置互联网边缘

1. 配置网络地址转换
2. 配置安全策略

程序 1　配置网络地址转换

局域网使用的专用网(RFC 1918)地址无法在互联网上路由，因此防火墙必须将 WLC 的内部地址转换为外部公共地址。下表中以示例方式列出了与 WLC 专用地址相对应的公共 IP 地址。

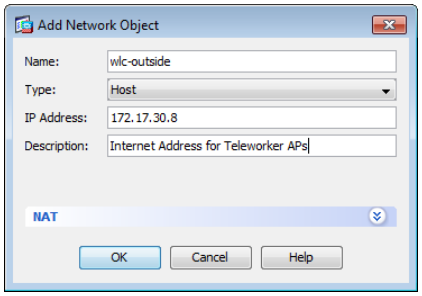
WLC 专用地址	WLC 公共地址（NAT 转换之后外部可路由）
10.10.50.11	172.17.30.8

步骤 1：转至 Configuration（配置）> Firewall（防火墙）> Objects（对象）> Network Objects（网络对象）/Groups（组）。

步骤 2：为 WLC 的公共地址添加一个网络对象。点击 Add（添加）> Network Object（网络对象）。

步骤 3：在 Add Network Object（添加网络对象）窗格中，配置以下属性：

- 在 Name（名称）框中，为 WLC 的公共 IP 地址输入一个描述。（例如：wlc-outside）
- 在 IP Address（IP 地址）框中，输入 WLC 的公共 IP 地址。（例如：172.17.30.8）

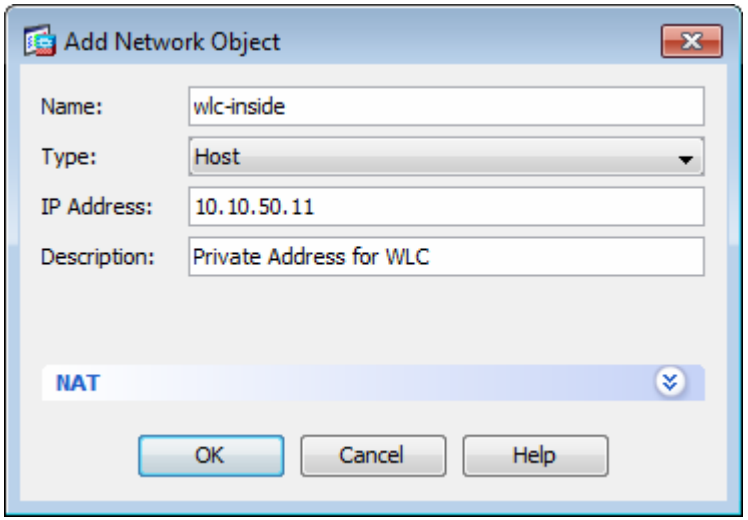


步骤 4：点击 OK。

步骤 5：为 WLC 的专用 DMZ 地址添加一个网络对象。点击 Add（添加）> Network Object（网络对象）。

步骤 6：在 Add Network Object（添加网络对象）窗格中，配置以下属性：

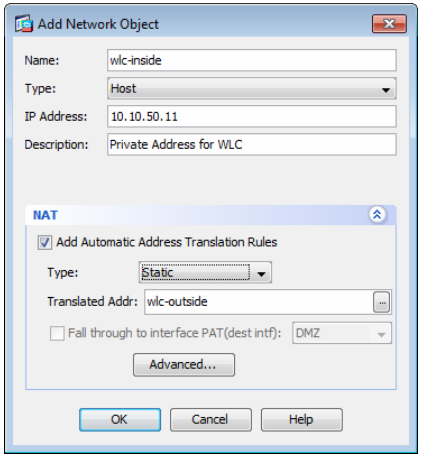
- 在 Name（名称）框中，为 WLC 的专用 IP 地址输入一个描述。（例如：wlc-inside）
- 在 IP Address（IP 地址）框中，输入 WLC 的专用 IP 地址。（例如：10.10.50.11）



步骤 7：点击双向下箭头。NAT 界面会展开。

步骤 8：选择 Add Automatic Address Translation Rules（**添加自动地址转换规则**）。

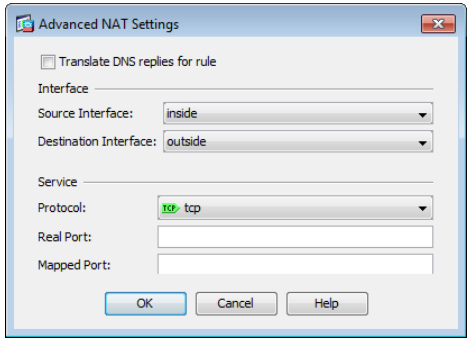
步骤 9：在 Translated Addr（**转换的地址**）列表中，选择在步骤 2 中创建的网络对象。



步骤 10：点击 Advanced（高级）。

步骤 11：在 Advanced NAT Settings（高级 NAT 设置）对话框中，配置以下值：

- 在 Source Interface（**源接口**）列表中，选择内部接口的名称。（例如：inside）
- 在 Destination Interface（**目的地接口**）列表中，选择互联网连接的接口名称。（例如：outside）



步骤 12：在 Advanced NAT Settings（**高级 NAT 设置**）窗口中点击 OK，然后在 Add Network Object（**添加网络对象**）中点击 OK 。

这一程序应用以下配置：

```
object network wlc-inside
  host 10.10.50.11
  description Private Address for WLC
object network wlc-outside
  host 172.17.30.8
  description Internet Address for Teleworker APs
object network wlc-inside
  nat (inside,outside) static wlc-outside
```

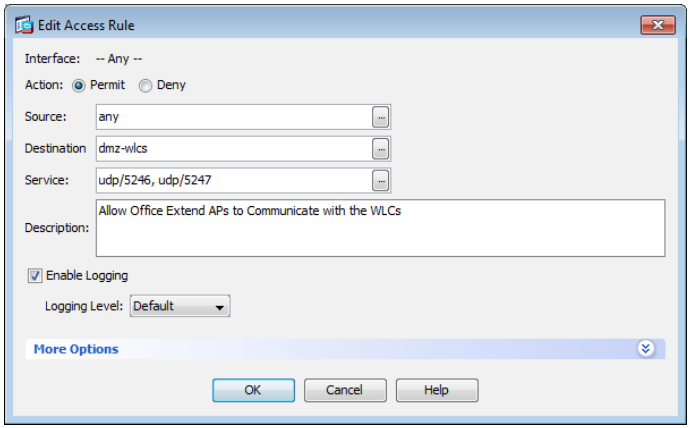
程序 2　配置安全策略

步骤 1：转至 Configuration（**配置**）> Firewall（**防火墙**）> Access Rules（**访问规则**）。

步骤 2：点击 Add（**添加**）> Add Access Rule（**添加访问规则**）。

步骤 3：定义一个规则，允许 600 系列 OfficeExtend 接入点使用具有以下值的 CAPWAP 与 DMZ 中的 WLC 进行通信：

- 在 Destination（**目的地**）列表中，选择程序 1 步骤 6 中创建的网络对象组。（例如：wlc-inside）
- 在 Service（**服务**）列表中，输入 udp/5246, udp/5247，然后点击 OK。



步骤 4：点击 Apply（应用）。

这一操作将会应用以下配置：

```
object-group service DM_INLINE_UDP_1 udp
  port-object eq 5246
  port-object eq 5247
access-list global_access line 1 remark Allow CAPWAP to WLC for Teleworker APs
access-list global_access line 2 extended permit udp any object wlc-inside object-group DM_INLINE_UDP_1
access-group global_access global
```

流程

配置局域网

1. 配置局域网核心层交换机
2. 配置服务器机房交换机

以下配置示例中所用的 VLAN 为：

- 无线数据：VLAN 116, IP: 10.10.16.0/24
- 无线语音：VLAN 120, IP 10.10.20.0/24
- 远程局域网：VLAN 134, IP 10.10.34.0/24

VLAN 116 和 120 专为《面向中小企业的 IBA 智能业务平台——无线网络基础部署指南》中的总部局域网接入点而配置，并且将被重新用于将总部无线局域网扩展到远程工作人员的家中。VLAN 134 是一个您将添加到总部局域网中的独立 VLAN，以便为连接到 OfficeExtend 接入点上家庭办公局域网端口的主机提供连接性。

程序 1　配置局域网核心层交换机

步骤 1：定义第二层 VLAN 配置：

```
vlan 134
 name OEAP-remote-LAN
```

步骤 2：配置 VLAN 接口(SVI)，为远程局域网 VLAN 提供路由：

```
interface Vlan134
 description OEAP Remote LAN Data Network
 ip address 10.10.34.1 255.255.254.0
 no shutdown
```

步骤 3：添加 VLAN 到与服务器机房交换机相连的端口通道：

```
interface Port-channel48
 description Trunk to Server Room switch
 switchport trunk allowed vlan add 134
```

程序 2　配置服务器机房交换机

步骤 1：定义第二层 VLAN 配置：

```
vlan 134
 name OEAP-remote-LAN
```

步骤 2：添加远程局域网的 VLAN 到与核心层交换机相连的端口通道：

```
interface Port-channel48
 description Trunk to Core switch
 switchport trunk allowed vlan add 134
```

步骤 3：添加远程局域网的 VLAN 到与 WLC 相连的端口通道：

```
interface Port-channel11
 description Trunk to WLC-1
 switchport trunk allowed vlan add 134
```

流程

配置 WLC

1. 针对 NAT 配置 WLC
2. 创建远程局域网接口
3. 配置远程局域网
4. 配置 OfficeExtend 接入点组

这一 WLC 配置以基础部署指南中的无线局域网控制器配置为基础。

程序 1　针对 NAT 配置 WLC

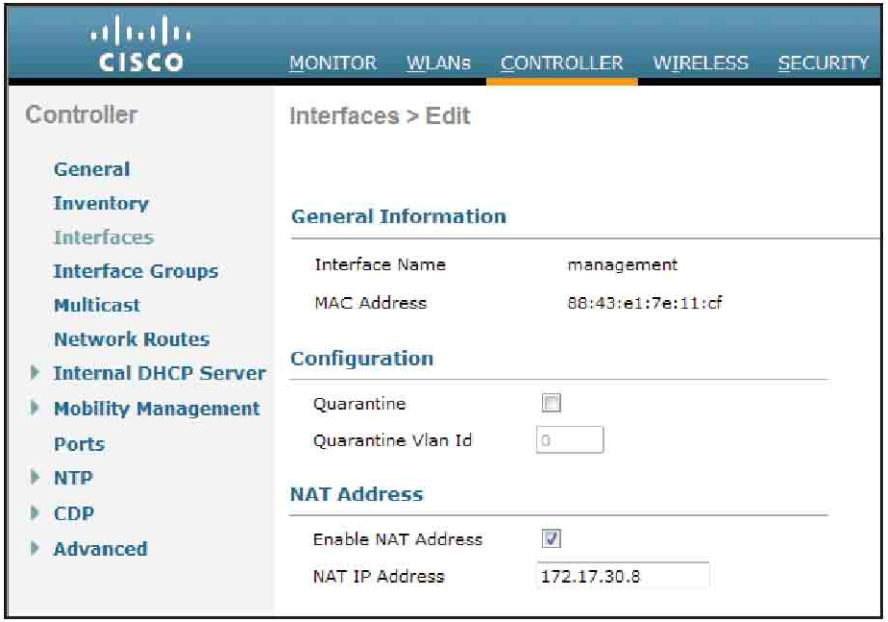
互联网边缘防火墙将 WLC 管理接口的 IP 地址转换为公共可到达的 IP 地址，以便远程办公地点的 600 系列 OfficeExtend 接入点能够访问 WLC。但是，为了使 600 系列 OfficeExtend 接入点能够与 WLC 进行通信，该公共可到达的地址也必须在 WLC 管理接口上进行配置。

步骤 1：在 **Controller（控制器）** > **Interfaces（接口）**中，点击 **management（管理）**接口。

步骤 2：选择 **Enable NAT Address（启用 NAT 地址）**。

步骤 3：在 **NAT IP Address（NAT IP 地址）**框中输入公共可到达的 IP 地址。（例如：172.17.30.8）

步骤 4：点击 **Apply （应用）**。



程序 2　创建远程局域网接口

添加一个允许远程局域网上的设备与企业中其他设备进行通信的接口。

步骤 1：在 Controller（控制器）>Interfaces（接口）中，点击 New（新建），然后输入以下值：

- 输入 Interface Name（接口名称）。（例如：teleworker-LAN）
- 输入 VLAN identifier（VLAN 标识符）（例如：134）

步骤 2：点击 Apply（应用）。

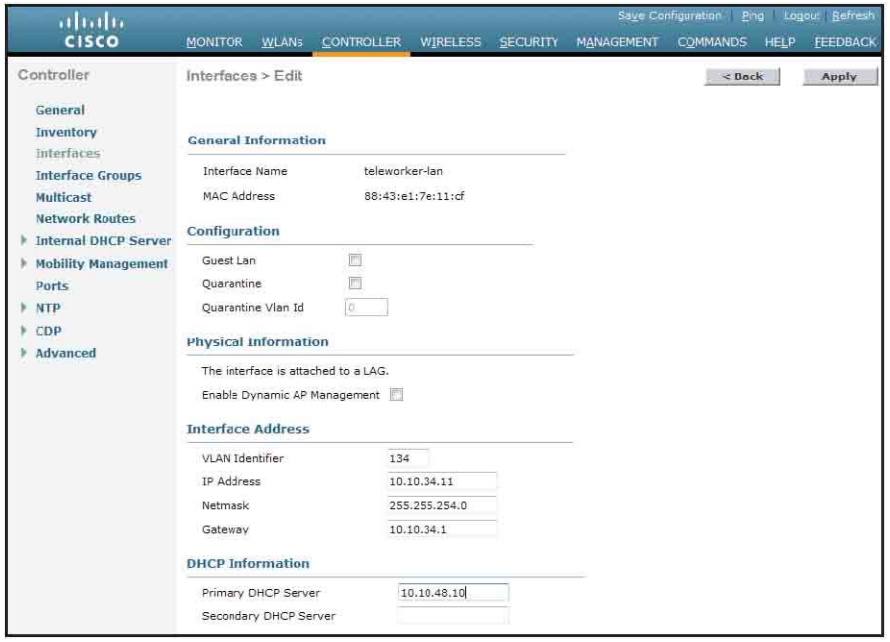
步骤 3：在 IP Address（IP 地址）框中，输入分配给 WLC 接口的 IP 地址。（例如：10.10.134.11）

步骤 4：输入 Netmask（子网掩码）。（例如：255.255.254.0）

步骤 5：在 Gateway（网关）框中，输入您添加到核心层交换机中的 VLAN 134 接口的 IP 地址。（例如：10.10.134.1）

步骤 6：在 Primary DHCP Server（主用 DHCP 服务器）框中，输入企业 DHCP 服务器的 IP 地址。（例如：10.10.48.10）

步骤 7：点击 Apply（应用）。

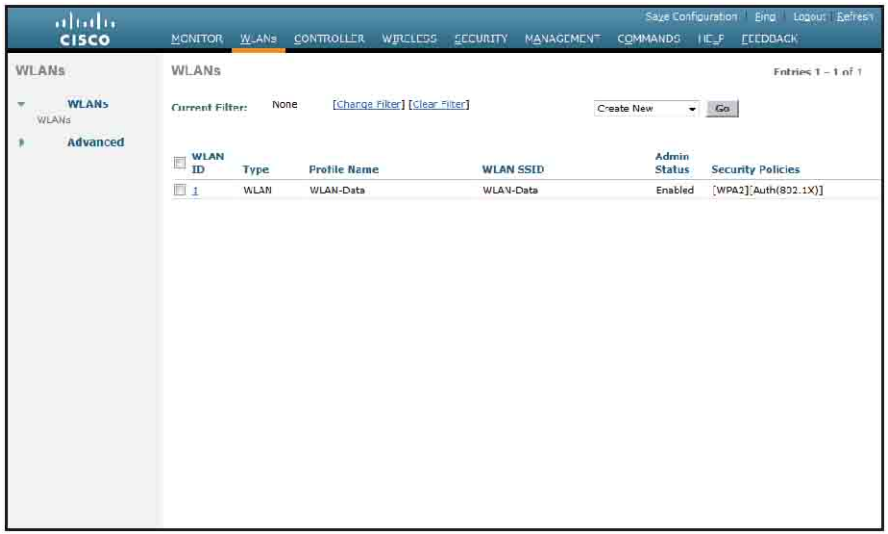


程序 3　配置远程局域网

远程局域网类似于无线局域网（WLAN），区别在于它被映射到 600 系列 OfficeExtend 接入点背部的一个以太网端口。

步骤 1：转至 **WLAN**。

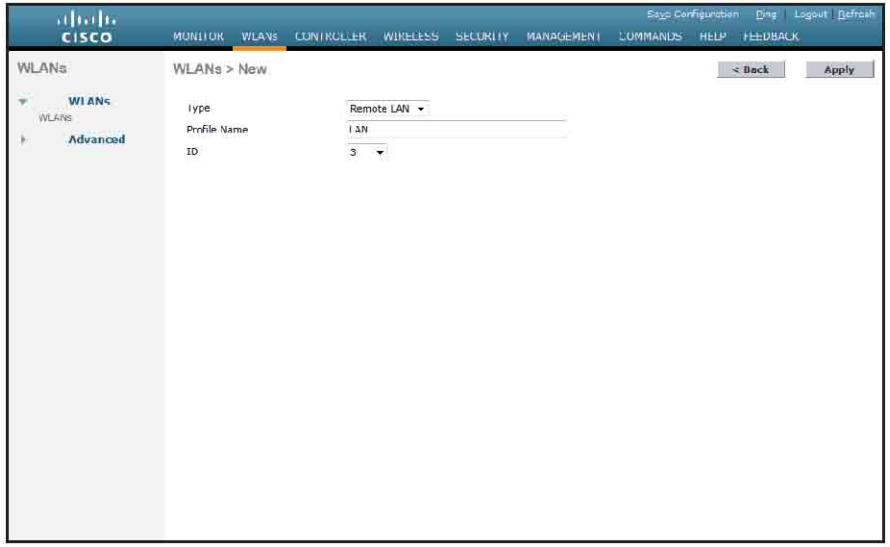
步骤 2：从下拉列表中选择 **Create New（新建）**，点击 **Go（开始）**。



步骤 3：在 **Type（类型）**列表中，选择 **Remote LAN（远程局域网）**。

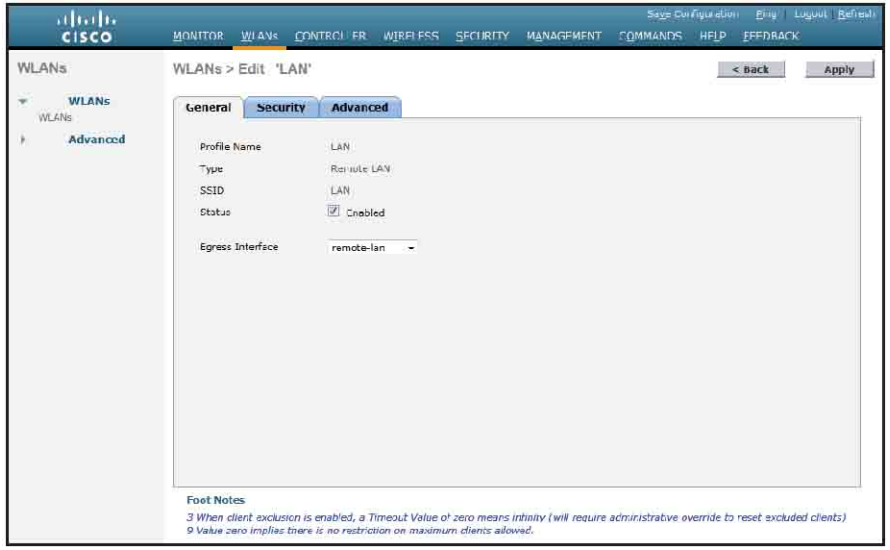
步骤 4：输入 **Profile Name（配置文件名称）**。（例如：OEAP-LAN）

步骤 5：点击 **Apply（应用）**。



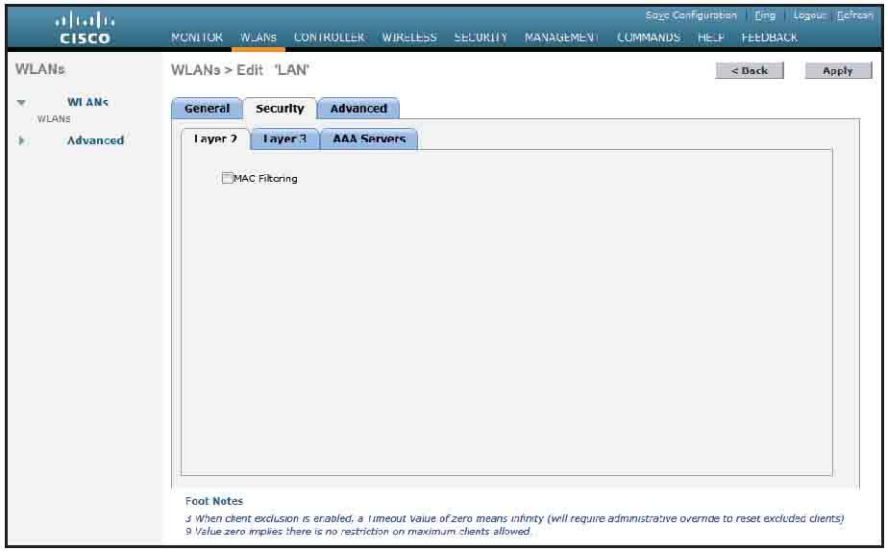
步骤 6：在 General（常规）选项卡上，在 **Status（状态）**一项选择 **Enabled（启用）**。

步骤 7：在 **Interface（接口）**列表中，选择在程序 2 中创建的接口。（例如：Remote-LAN）



步骤 8：单击 **Security（安全）**选项卡。

步骤 9：在 Layer 2（第二层）选项卡上，取消勾选 **MAC Filtering（MAC 过滤）**，然后点击 **Apply（应用）**。



程序 4　配置 OfficeExtend 接入点组

600 系列 OfficeExtend 接入点最多可支持两个无线局域网和一个远程局域网。远程工作人员站点将提供与总部局域网相同的 SSID，以分离语音和数据流量。然而，OfficeExtend 接入点不应提供访客 WLAN。OfficeExtend 接入点将分配给可提供一组不同 WLAN SSID 的接入点组。为了向 OEAP 连接的用户提供正确的 WLAN 和远程 LAN，OfficeExtend 接入点必须连接到一个独立的接入点连接组，而不是那些与总部或远程站点局域网相连的接入点组。接入点按其 MAC 地址分配给 OEAP 组，当必须要撤销远程工作人员的连接时，也需要该地址。您必须维护一个列表来记录针对远程工作人员的接入点 MAC 地址分配情况。

与总部和远程站点局域网相连的接入点将连接至默认组，该组不提供 OEAP 的远程 LAN。

步骤 1：转至 **WLANs > Advanced（高级）> AP Groups（接入点组）**，然后点击 **Add Group（添加组）**。

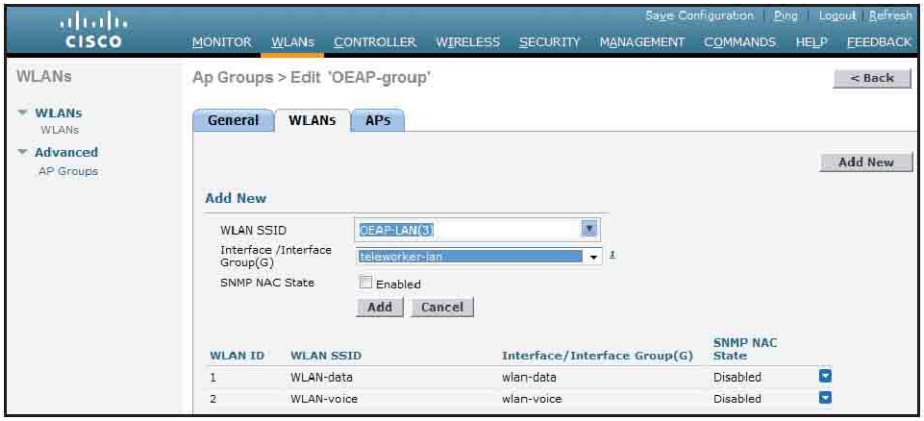
步骤 2：在 **AP Group Name（接入点组名称）**框中，填写 OfficeExtend 远程工作人员接入点组的名称（例如：OEAP-group）：

步骤 3：点击 **Add（添加）**。

步骤 4：在 **WLANs > Advanced（高级）> AP Groups（接入点组）**页面，点击您刚刚创建的接入点组的名称：

步骤 5：在 WLANs 选项卡上，点击 Add New（添加新 WLAN）按钮，选择 WLAN-data WLAN。确保选择了 wlan-data Interface group（wlan-data 接口组），然后点击 Add（添加）：

步骤 6：重复步骤 5，将 WLAN-voice 和 OEAP-LAN SSID 添加到 OEAP-group 接入点组中：



流程

配置 600 系列 OfficeExtend 接入点

1. 配置远程工作人员的 OEAP
2. 配置远程工作人员的 OEAP

OfficeExtend 接入点可以在用户提供前由 IT 员工进行配置，或是由用户在家中进行设置。请注意：分发给远程工作人员的新接入点必须分配给正确的接入点组，以便接入点能够提供正确的 WLAN。如果员工配置了自己的接入点，他们必须要联系 IT 人员将其接入点分配到正确的接入点组。

程序 1　配置远程工作人员的 OEAP

步骤 1：将 600 系列 OfficeExtend 接入点背部的广域网端口连接到您的家用路由器/网关。600 系列 OfficeExtend 接入点将从家用路由器/网关获取一个 IP 地址。

技术提示

600系列OfficeExtend接入点并非设计用于替代家用路由器的功能，并且它不应直接连接到电信运营商网关。

步骤 2：一旦 600 系列 OfficeExtend 接入点开始运行，将计算机连接到以太网端口 1、2 或 3。该计算机将从 10.0.0.0/24 默认 DHCP 地址池获取一个 IP 地址。

步骤 3：使用 OEAP 的默认地址 https://10.0.0.1/，转至 600 系列 OfficeExtend 接入点的 web 界面。

步骤 4：使用默认凭证：**admin/admin**，登录到 Administration（管理）页。

步骤 5：在 600 系列 OfficeExtend 接入点 Welcome（欢迎）页面，点击 **Enter（输入）**。Summary（总结）页面出现。

步骤 6：转至 **Configuration（配置）> WAN（广域网）**。

步骤 7：在 **Primary Controller IP Address（主用控制器 IP 地址）**字段中，输入主用 WLC 的外部 IP 地址，然后点击 **Apply（应用）**。

步骤 8：屏幕切换到验证界面。待该界面出现后，点击 **Continue（继续）**。

步骤 9：600 系列 OfficeExtend 接入点连接到控制器并下载最新的软件映像。留出 5 分钟以便设备进行下载并采用新代码和配置重启。

技术提示

建立到WLC的连接后，接入点顶部的Status LED（状态LED）指示灯将会闪烁。状态LED指示灯持续闪烁，直到下载完成。下载完成后，接入点重启。连接到控制器后，状态LED指示灯会持续显示蓝色或紫色。

程序 2　配置远程工作人员的 OEAP

将远程工作人员的接入点分配至正确的接入点组。

步骤 1：转至 **WLANs > Advanced（高级） > AP Groups（接入点组）**，然后点击 OEAP-group 链接：

步骤 2：选择 **APs（接入点）**选项卡，将接入点背后标签上的 MAC 地址与表中的地址进行匹配，找到远程工作人员的接入点。选择复选框，然后点击 **Add APs（添加接入点）**：

接入点将重启，并为远程工作人员的家庭办公室提供连接。

附录 A：产品列表

以下产品与软件版本经验证适用于思科 IBA 智能业务平台：

功能区域	产品	产品编号	软件版本
OfficeExtend 总部 WLC	5508 无线局域网控制器	AIR-CT5508-100-K9 5508 无线局域网控制器，带 100 个接入点许可证	7.0.116.0
OfficeExtend 远程工作人员站点	600 系列接入点	AIR-OEAP602I-A-K9	7.0.116.0
互联网边缘防火墙	自适应安全设备 ASA 5540，带 SSM-40 IPS 模块 ASA 5520，带 SSM-20 IPS 模块 ASA 5510，带 SSM-10 IPS 模块	ASA5540-AIP40-K9 ASA5520-AIP20-K9 ASA5510-AIP10-K9	8.4.1.ED 7.0(2)E4
ASA 5505 远程工作人员站点	自适应安全设备 ASA 5505	ASA5505-BUN-K9 ASA 5505 设备，带软件，10 个用户，8 个端口，3DES/AES	8.4.1

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-2800034-1 8/11