

HP Jetdirect 安全准则



目录:

简介	1
HP Jetdirect 概述	2
什么是 HP Jetdirect?	3
您的 HP Jetdirect 使用多久了?	4
升级	5
HP Jetdirect 管理准则	6
HP Jetdirect 黑客攻击: TCP 端口 9100	7
HP Jetdirect 黑客攻击: 密码和 SNMP 团体名称	8
HP Jetdirect 黑客攻击: 固件升级	8
HP Jetdirect 黑客攻击: 嗅探并重播打印作业	9
HP Jetdirect 黑客攻击: 打印机/MFP 访问	9
建议的安全部署: 第 1 组	10
建议的安全部署: 第 2 组	11
建议的安全部署: 第 3 组	17
建议的安全部署: 第 4 组	26
参考资料	31

简介

Internet 上充斥着大量有关对 HP Jetdirect 产品进行黑客攻击的信息，这促使客户向 HP 咨询如何保护其打印和成像设备以免受到此类攻击，以及 HP 正在采取哪些措施来防范这些攻击。公正地说，其中的某些公共信息简直就是粗制滥造，哗众取宠；但也有一些网站详细介绍了 HP Jetdirect 存在的漏洞以及受到的攻击，它们提供了一些有价值的信息并提出了需要解决的实质性问题。本白皮书旨在消除客户对这些攻击和漏洞的担忧，并建议了正确的安全配置以帮助客户保护其打印和成像设备。本白皮书只是 HP 内部庞大计划的一小部分，旨在为我们的客户群提供有关打印和成像安全保护方面的培训。安全打印网站 (<http://www.hp.com/go/secureprinting>) 等资源为客户提供了大量有关产品、解决方案以及配置建议的信息。一般而言，可以将其中的很多信息应用于现有 HP Jetdirect 产品，究其主要原因是，HP Jetdirect 是首批广泛实施各种安全协议的打印服务器之一，如 SSL/TLS、SNMPv3、802.1X 和 IPsec。

如果您不熟悉安全保护和安全配置，一定要记住“安全保护”是一项系统工程。实际上，目前被认为在未来几年都牢不可破的安全配置和协议很可能在今天早些时候即被攻破。一种极端情况是，成像和打印设备获得的最佳安全保护是在购买后从未拆开设备包装。另一种极端情况是，设备可获得的最差安全保护是拆开包装、接通电源、获取配置页以查找 IP 地址、将其添加到台式机系统或打印机后台处理程序中，然后就将它们抛在脑后。后一种情况听起来是否就像您所采取的打印和成像安全策略呢？

实际上，HP Jetdirect 遇到的一个安全保护难题是由同时保证“即插即用”和可靠性造成的。正如我们将会了解到的一样，“即插即用”与“安全性”通常是无法并重的。有数十万（或许数百万）个 HP Jetdirect 产品一直使用了多年，而从未更新过固件或更改过配置。在目前日益关注安全问题的大环境中，我们知道无论讨论的是什么类型的设备，这种做法都是不可取的，根本无法保证基础设施的正常运转。

HP Jetdirect 概述

几年前，人们通过并行端口或串行端口将打印机连接到称为后台处理程序的计算机上，从而将世界各地的打印机通过网络连接在一起。这些后台处理程序随后通过 LPD 等网络协议，将这些打印机与网络上的客户端进行共享。基于串行和并行端口的电缆受长度的限制，无法将打印机移到距后台处理程序较远的位置。

与当时的其它技术相比，HP LaserJet 打印机的打印质量超乎人们的想像，促使打印行业取得了前所未有的发展。随着打印机的复杂程度和功能的不断增加，需要连接到后台处理程序以共享打印机已变成了一种负担。HP Jetdirect 的设计宗旨是允许用户在网络上共享打印机，而无需直接连接到后台处理程序上。在迁移到网络打印机的同时，其目标是获得与直接连接的打印机相同的简便易用性。HP Jetdirect 尽最大努力自动初始化所有协议，以允许用户立即使用 Jetdirect 进行打印。常用的 HP 工具（如 Jetadmin）通过利用专用协议以及已知的默认安全设置，大大简化了 HP Jetdirect 设备的配置过程。

在推出 HP Jetdirect 的时候，市场上销售的协议集和网络基础设施品种繁多，它们之间的竞争非常激烈。AppleTalk、DLC/LLC 和 IPX/SPX 等协议集已得到了广泛部署，并获得了与 TCP/IP 大致相当的市场份额。此外，令牌环、FDDI、LocalTalk、ATM 和其它帧传输方法的采用率（或增长率）几乎与以太网不相伯仲。在网络打印飞速发展的这一时期，HP Jetdirect 中提供的功能旨在提高“简便易用性”、减少支持电话数量以及提供丰富的客户体验，而不论客户使用的是什么协议或网络基础设施。简而言之，HP Jetdirect 的设计宗旨是在网络上实现“即插即用”，其工作方式就好像是将打印机直接连接到 PC 上一样。

到目前为止，在内部网网络连接方面无可争议的大赢家是：TCP/IP 和以太网。“简便易用性”设计标准现在有一个主要障碍：“安全保护”。客户开始咨询如何安全地部署打印和成像设备，而不是如何以最便捷的方式进行部署。

什么是 HP Jetdirect?

将打印机直接连接到网络后台处理程序后，通常使用一个简单硬件协议将数据从 PC 发送到打印机中。并行端口上的 Centronics 模式就是一个例子。随着客户要求的数据传输速度越来越快、打印机状态越来越丰富，这些协议也变得越来越复杂（如 IEEE 1284.4 中所示）。简而言之，打印机使用直接连接的端口（如串行和并行端口）实施硬件协议，并将封装的数据转换为打印机所使用的数据。随着客户开始将其打印机连接到网络上，HP 决定着手制订以下策略（至今仍在使用）：使用智能网络卡实施各种网络基础设施组件，以便将封装的网络数据转换为打印机所使用的数据。因此，HP Jetdirect 应运而生，它是首批网络协议分载引擎之一。请参见图 1 – 功能图表。

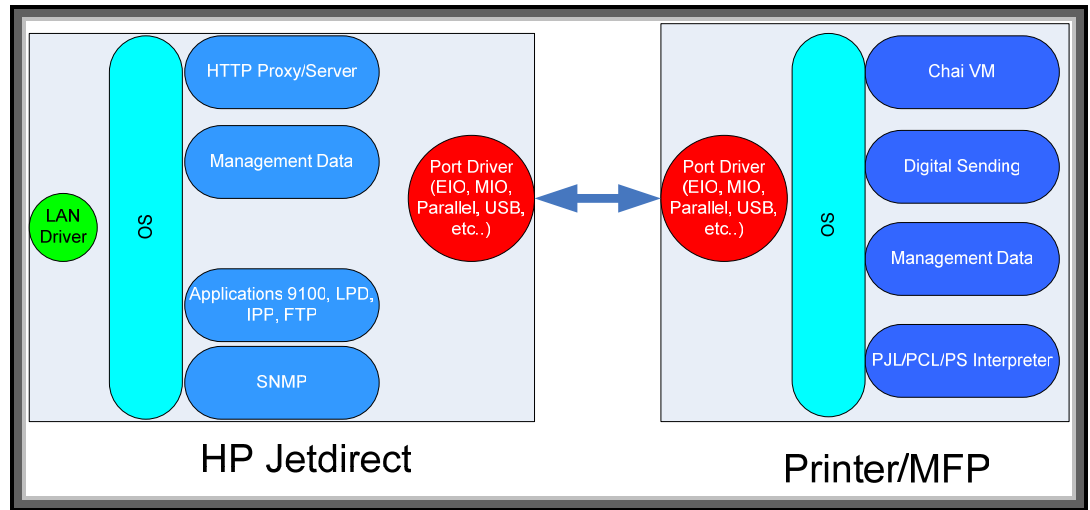


图 1 – 功能图表

在图 1 中，您可以看到标准的分载引擎图表。该图表并不全面，但可以从其中看出 HP Jetdirect 与打印机/MFP 平台之间的差别。该图表的重要性体现在哪里呢？首先，我们可以从中了解到，HP Jetdirect 可以为打印基础设施提供哪些安全功能。其次，我们还可以了解到 HP Jetdirect 没有哪些功能。例如，Internet 上的某些信息指出，HP Jetdirect 上实现了 PJI 分析器。我们可以从该图表中看出，这种说法是不正确的。如果通过升级 HP Jetdirect 卡为打印机提供更多 PJI 分析保护，这种投资并不可取。而通过升级 HP Jetdirect 卡来控制哪些人可以与打印机进行交互，哪些人不能进行交互，则是一项不错的投资。

您的 HP Jetdirect 使用多久了？

有时，管理员在清点网络时，可能会发现某些连接到网络上的设备虽然很旧，但仍能正常工作。这也适用于打印机和 HP Jetdirect 设备。一种获取 HP Jetdirect 设备清单的简便方法是使用 HP Download Manager，可以从以下位置下载该产品：http://www.hp.com/go/dlm_sw。通过使用该实用程序，您可以查找网络上的打印机及其 HP Jetdirect 设备。要使用全面深入的管理平台，请试一试 HP Web Jetadmin，可以从以下位置下载该产品：<http://www.hp.com/go/webjetadmin>。请注意，如果不希望更新 HP Jetdirect 产品上的固件，则不必进行更新（HP 建议进行更新），但对于此特定小节而言，我们只需要找出 HP Jetdirect 设备，然后根据产品编号了解其新旧程度即可。请参见表 1 – HP Jetdirect 的发展历程。

说明	发布日期
Microsoft Windows for Workgroups 3.11	1994 年 2 月
HP Jetdirect J2550A、J2552A MIO 打印服务器	1994 年 5 月
Microsoft Windows 95	1995 年 8 月
HP Jetdirect J2550B、J2552B MIO 打印服务器	1996 年 11 月
HP Jetdirect J3110A、J3111A EIO 打印服务器	1997 年 10 月
HP Jetdirect J3263A 300X 外置式打印服务器	1998 年 1 月
HP Jetdirect J3113A 600n EIO 打印服务器	1998 年 1 月
Microsoft Windows 98	1998 年 6 月
HP Jetdirect J3258A 170x 外置式打印服务器	1998 年 9 月
Microsoft Windows 2000 Professional	2000 年 2 月
HP Jetdirect J4169A 610n EIO 打印服务器	2000 年 10 月
Microsoft Windows XP	2001 年 10 月
HP Jetdirect J6057A 615n EIO 打印服务器	2002 年 4 月
Microsoft Windows 2003 Server	2003 年 4 月
HP Jetdirect J7934A 620n EIO 打印服务器	2004 年 4 月
HP Jetdirect J7961A 635n EIO 打印服务器	2005 年 10 月

表 1 – HP Jetdirect 的发展历程

表 1 并不全面。很多 Jetdirect 卡是在 1994 年以前推出的；上面列出了一些常用的 HP Jetdirect 产品，并将它们与某些 Microsoft Windows 发布日期进行了比较。在当前的环境中，很难找到一位知名安全分析师愿意花时间讨论与 Microsoft Windows for Workgroups 3.11 和 Microsoft Windows 95 有关的安全问题。在查看有关 HP Jetdirect 设备的安全漏洞的公共信息时，一定要切记设备的新旧程度。

到本文截稿时（2007 年 8 月），要为台式机和服务器提供最佳的安全保护，迁移到 Microsoft Windows XP SP2 和 Microsoft Windows 2003 SP2 是至关重要的。Microsoft 提供了很多对其产品进行正确配置的准则，很多安全顾问的职业就是帮助客户部署这些配置。客户愿意支付这笔开销，因为数据安全性对他们至关重要。如果打印基础设施对您非常重要，难道不应该考虑对其进行升级并使用建议的安全配置吗？与此相对的是，某些公司非常信赖他们在二十世纪 90 年代初期开发的打印基础设施。但在今天，这些客户中还有多少人愿意在台式机上运行 Microsoft Windows 95，而在服务器上运行 Microsoft Windows Advanced Server 3.51 呢？

升级

并不要求对 HP Jetdirect 设备进行升级，但强烈建议您这样做。如果客户选择升级设备，HP 可以提供一些指导原则。首先，如果 HP Jetdirect 设备是在 2000 年以前推出的，HP 建议您将其升级到较新的机型。表 2 – HP Jetdirect 机型中显示了自 2007 年 8 月起客户可以购买到的机型的一些安全功能：

HP Jetdirect	安全功能
J3258G 170x 外置式并行打印服务器	非加密安全保护，购买后无法升级到较新的固件
J6035G 175x 外置式 USB 1.1 打印服务器	非加密安全保护，购买后无法升级到较新的固件
J3263G 300x 外置式打印服务器	非加密安全保护，购买后可以升级
J7983G 510X 外置式三端口打印服务器	非加密安全保护，购买后可以升级
J7942G en3700 外置式 USB 2.0 打印服务器	用于管理的 SSL/TLS、SNMPv3 和 802.1X PEAP。
J7934G 620n EIO 10/100 打印服务器	用于管理的 SSL/TLS、SNMPv3 和 802.1X PEAP。
J7949E 内嵌式 Jetdirect 10/100（不单独出售，安装在某些打印机/MFP 设备的格式化板上）	运行 V.33.14 或更高版本的固件：用于管理的 SSL/TLS、SNMPv3 和 802.1X PEAP。
J7982E 内嵌式 Jetdirect 10/100（不单独出售，安装在某些打印机/MFP 设备的格式化板上）	防火墙、用于管理的 SSL/TLS、SNMPv3、802.1X PEAP 和 802.1X EAP-TLS。
J7997G 630n EIO 10/100/1000 打印服务器	防火墙、用于管理的 SSL/TLS、SNMPv3、802.1X PEAP 和 802.1X EAP-TLS。
J7961G 635n EIO 10/100/1000 IPv6/IPsec 打印服务器	IPsec/防火墙、用于管理的 SSL/TLS、SNMPv3、802.1X PEAP 和 802.1X EAP-TLS。

表 2 – HP Jetdirect 机型

在表 3 – 停产的 HP Jetdirect 机型中，显示了 HP 不再销售的一些常用 HP Jetdirect 设备及其安全功能。

HP Jetdirect	安全功能
J4100A 400n 10/100 MIO 打印服务器	非加密安全保护，购买后可以升级
J4106A 400n 10Mbps MIO 打印服务器	非加密安全保护，购买后可以升级
J3110A 600n 10Mbps EIO 打印服务器	非加密安全保护，购买后可以升级
J3111A 600n 10Mbps EIO 打印服务器	非加密安全保护，购买后可以升级
J3113A 600n 10/100 EIO 打印服务器	非加密安全保护，购买后可以升级
J4169A 610n 10/100 EIO 打印服务器	用于管理的 SSL/TLS 和 SNMPv3
J6057A 615n 10/100 EIO 打印服务器	用于管理的 SSL/TLS 和 SNMPv3

表 3 - 停产的 HP Jetdirect 机型

正如您所看到的一样，如果将停产的 400n MIO 机型替换为新的外置式并行端口打印服务器（如 300X），并不会升级 Jetdirect 设备的安全功能。使用 MIO 插槽的打印机已经停产了很多年，如 LaserJet IIIsi 和 LaserJet 4si。使用 EIO 插槽的打印机和 MFP 至今仍在销售。在 HP LaserJet 4000 上引入 EIO 插槽将近有 10 年的历史了。使用基于 EIO 的打印机的一个重要功能是可以安装 J7961G 635n IPv6/IPsec 打印服务器。通过使用该产品，我们可以选用一个较早的打印机（如 HP LaserJet 4000），然后为其提供最新的网络协议和安全支持。在评估对 HP Jetdirect 实施的各种攻击以及一些防御这些攻击的方法时，这种灵活性是非常有用的。对于使用很多基于 EIO 的打印机的公司来说，正确部署 635n 不仅可以保护其打印机/MFP 投资，而且还可以提高其打印和成像基础设施的安全性。

HP Jetdirect 管理准则

在下面的材料中，本白皮书介绍了一些与 HP Jetdirect 漏洞或针对它的攻击有关的公共信息。为了正确建议 HP Jetdirect 配置，需要使用四项不同的管理准则。这些管理准则来自四个主要 HP Jetdirect 产品线（称为组）。

- **第 1 组：** 170x、300x、500x、510x、400n 和 600n 机型。下面的文档中提供了用于确保这些设备安全的管理准则：
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpi05999>。需要提醒您的是，这些设备没有加密安全功能。
- **第 2 组：** 610n、615n、620n、625n、en3700 和内嵌式 Jetdirect (J7949E) 机型。第 2 组可以使用为第 1 组产品提供的管理准则，但可通过 EWS 获取较新的管理工具以确保这些设备的安全，该工具位于：
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpi07576>。
- **第 3 组：** 630n 和内嵌式 Jetdirect (J7982E、J7987E、J7991E 和 J7992E) 机型。第 3 组可以使用为第 2 组产品提供的管理准则，但可通过防火墙获得更多的安全保护。防火墙可以根据 IPv4/IPv6 地址以及服务类型允许传输/丢弃数据包。
- **第 4 组：** 635n 机型和 CM8000 Color MFP 系列 (J7974E)。在 HP Jetdirect 产品线中，这些机型具有的安全功能最多。

在安全配置方面，人们要特别小心，“可别锁了前门却敞开了窗户”。在很多情况下，必须先“锁定”某些设备，然后才能有效地保护某个设备的安全。在使用此处介绍的方法之前，管理员应该**至少**执行以下操作：

- 将所有 HP Jetdirect 固件升级到最高级别。一种执行该操作的最简便方法是使用 HP Download Manager，可以从 http://www.hp.com/go/dlm_sw 中下载该产品。通过使用 Internet 模式，HP Download Manager 自动指示需要升级的设备。HP 建议始终先只升级几个设备并在网络上对这些设备执行评估，然后再将所有设备升级到最新固件。
- 指定了内嵌式 Web 服务器 (EWS) 密码。
- 更改了默认 SNMPv1/v2c 设置团体名称。
- 禁用了所有非活动协议（如 IPX/SPX 和 AppleTalk）。
- 将所有无法升级到固件最高级别的产品标记为安全风险。
- 表 4 中显示了自 2007 年 8 月起推出的常用 HP Jetdirect 设备及其应运行的固件的准则：

HP Jetdirect 产品编号	固件版本
J7949E 内嵌式 Jetdirect	V.33.14/V.33.15
J4100A 400n 10Mbps MIO 打印服务器	K.08.49
J4106A 400n 10Mbps MIO 打印服务器	K.08.49
J3110A 600n 10Mbps EIO 打印服务器	G.08.49
J3111A 600n 10Mbps EIO 打印服务器	G.08.49
J3113A 600n 10/100 EIO 打印服务器	G.08.49
J4169A 610n 10/100 EIO 打印服务器	L.25.57
J6057A 615n 10/100 EIO 打印服务器	R.25.57
J3263A/J3263G 300x 外置式打印服务器	H.08.60
J3265A 500X 外置式三端口打印服务器	J.08.60
J7983G 510X 外置式三端口打印服务器	J.08.60
J7942A/J7942G en3700 外置式 USB 2.0 打印服务器	V.28.22
J7934A/J7934G 620n EIO 10/100 打印服务器	V.29.20
J7960A/J7960G 625n EIO 10/100/1000 打印服务器	V.29.29
J7961A/J7961G 635n EIO 10/100/1000 IPv6/IPsec 打印服务器	V.36.11

表 4 – Jetdirect 固件版本

注：对于某些内嵌式 Jetdirect 产品，您需要升级打印机/MFP 固件以更新 JDI 固件。

现在，我们已介绍了足够多的背景信息，让我们看一看传闻中提到的一些 HP Jetdirect 漏洞和攻击。

HP Jetdirect 黑客攻击：TCP 端口 9100

TCP 端口 9100 是最初为将打印数据发送到打印机而开发出的方法之一。一些公共参考资料称 TCP 端口 9100 上存在一个打印协议，其实纯属子虚乌有。对于传送到 HP Jetdirect 设备上 TCP 层的原始数据，在将其发送到打印机时，就好像通过并行端口、串行端口或任何其它端口进行传送一样。TCP 端口 9100 是使用 TCP/IP 协议集将数据传送到打印机的最快捷、最有效的方式。

针对 TCP 端口 9100 的最常见黑客攻击是，向该端口发送包含一些 PJI 命令的作业。这些 PJI 命令可以执行各种操作，最常见的操作之一是更改控制面板显示。切记，HP Jetdirect 将剥离 TCP/IP 头，并将该数据直接提供给打印机。打印机在处理 PJI（数据）时，就好像打印机直接连接到 PC 上一样。很多年前，打印机驱动程序需要使用 PJI 命令集以某些方式控制打印机。正如我们看到的一样，网络环境中存在滥用的可能性。

管理员该如何防范 TCP 端口 9100 被滥用呢？根据我们目前所了解的 HP Jetdirect 信息，我们知道必须控制哪些人可以建立到 TCP 端口 9100 的 TCP 连接，而哪些人不能建立此类连接。表 5 中显示了一些选项，它们按照从最少安全功能（选项 1）到较高级别的安全功能（选项 > 1）的顺序排列：

需要进行打印的主机	选项
仅与 HP Jetdirect 位于相同子网的计算机	<p>选项 1) 用于第 1/2/3/4 组。删除默认网关（设置为 0.0.0.0）。这无法防止 HP Jetdirect 从其它子网接收数据包，但可以防止响应返回到这些远程子网。因此，无法形成 TCP 连接。</p> <p>选项 2) 用于第 1/2/3/4 组。使用本地子网的 IP 地址和掩码设置访问控制列表。</p> <p>选项 3) 用于第 3 组。设置规则以使用防火墙保护打印通信。</p> <p>选项 4) 用于第 4 组。设置规则以使用 IPsec 保护打印通信。</p>
位于不同子网上的 10 个或更少的单独计算机	<p>选项 1) 用于第 1/2/3/4 组。使用掩码 255.255.255.255 为每个单独的 IP 地址设置访问控制列表。</p> <p>选项 2) 用于第 3 组。设置规则以使用防火墙保护打印通信。</p> <p>选项 3) 用于第 4 组。设置规则以使用 IPsec 保护打印通信。</p>
公司中的所有主机	<p>选项 1) 用于第 1/2/3/4 组。为分配给公司的网络 ID 设置访问控制列表。例如，对于 HP 的内部网络，共有两个入口：IP - 15.0.0.0 掩码 - 255.0.0.0 和 IP -16.0.0.0 掩码 - 255.0.0.0。</p> <p>选项 2) 用于第 3 组。设置规则以使用防火墙保护打印通信。</p> <p>选项 3) 用于第 4 组。设置规则以使用 IPsec 保护打印通信。</p>

表 5 – 访问控制

由于 TCP 上支持很多打印协议，因此，接下来理应禁用管理员不使用的的所有打印协议。可以在相应产品组的管理准则中找到禁用这些协议的方法。

一定要注意，到未进行加密保护的任何设备（不仅仅是 HP Jetdirect）的所有 TCP/IP 通信容易受到 IP 地址诈骗和中间人 (MITM) 攻击。这些攻击可以针对任何 TCP/IP 通信。此外，还可能使用了一些加密保护功能，但没有正确地进行部署。例如，如果依靠 SSL/TLS 保护数据，则需要由可信认证机构对 SSL/TLS 使用的证书进行正确签名。否则，SSL/TLS 也容易受到 MITM 攻击，因为它依靠可靠的 PKI 来成功验证服务器端点（并且可以选择验证客户端端点）。

如果允许用户在工作时进行打印，但是该用户使用 TCP 端口 9100 不断更改显示或对打印机执行其它有害操作，那么该怎么办呢？如果用户在工作时打印个人材料、运行较大打印作业而将打印机耗材耗尽等，这实际上与前一种情况并没有什么差别。如果信任用户建立打印连接，就会信任他们的打印行为。可以通过 HP 通用打印驱动程序 (UPD) 以色彩访问和控制的形式提供一些额外的保护；管理员可通过色彩访问和控制对用户的色彩使用量进行控制。此外，HP Web Jetadmin 还包含一项称为“报告生成器”的功能，它有助于生成有关用户及其打印行为的报告。该功能对审计和了解打印机的使用情况非常有用。

HP Jetdirect 黑客攻击：密码和 SNMP 团体名称

这些年来，HP Jetdirect 密码和 SNMP 团体名称行为确实发生了一些变化。以下位置提供了一个很好的资源，可从中了解其历史行为和当前行为：

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00004828>。

简而言之，应始终更新 HP Jetdirect 上的固件、使用 HP 提供的最新客户端软件以及升级到最新的 Web Jetadmin 管理软件。在升级所有软件和固件后，请将这些设备上的密码更改为新密码。此过程有助于 HP Jetdirect 设备使用相同的方式处理密码。

为了更好地保护密码以免受到被动嗅探，请考虑使用 SSL/TLS。第 2/3/4 组支持到 SSL/TLS 的自动重定向，并可防止使用 HTTP 访问 EWS（如果管理员希望这样做）。但是，在使用 SSL/TLS 时，请确保将 HP Jetdirect 证书更新为由可信 CA 颁发的证书以正确避免 MITM 攻击。此外，还应考虑迁移到 SNMPv3。可以将 HP Web Jetadmin 配置为自动使用 SNMPv3。属于第 2、3 或 4 组的 HP Jetdirect 设备支持 SNMPv3。

HP Jetdirect 黑客攻击：固件升级

以下文档简要介绍了 HP Jetdirect 用于升级固件的各种方法，这是一篇非常精彩的文章：

http://www.hp.com/go/webjetadmin_firmware。

所有 HP Jetdirect 固件文件都采用相同的基本格式：一个恢复分区和一个主功能分区。如果升级编程失败（由于升级过程中网络中断、客户端锁定以及打印机断电等所致），HP Jetdirect 可以进行恢复，但功能较少。通过这种行为，管理员可以从恢复分区中重新启动升级过程并重新获得全部功能，而无需与 HP 支持部门联系。

共有三种更新 HP Jetdirect 固件的常用方法：

- HP Download Manager / HP Web Jetadmin
- FTP
- 嵌入式 Web 服务器

在使用 HP Download Manager 或 HP Web Jetadmin 时，应用程序将向 HP Jetdirect 设备发出 SNMP 设置命令。如果应用程序具有正确的凭证，它可以使用 TFTP 服务器信息填充固件升级 MIB 表。HP Jetdirect 使用此信息启动 TFTP 客户端并接受下载文件。这些应用程序使用已知的默认 SNMP 团体名称。但是，如果管理员配置了 SNMP 设置团体名称，应用程序必须知道该名称才能为固件升级成功设置 TFTP MIB 对象。客户还可以自定义 SNMPv3 以获得额外的安全保护，并且 HP Web Jetadmin 简化了 SNMPv3 的使用过程。另请注意，Hewlett-Packard 对 HP Download Manager 和 HP Web Jetadmin 等应用程序进行了数字签名，以作为这些应用程序的来源证明。

以下文档介绍了可以使用 FTP 升级 HP Jetdirect 设备固件：

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj07129>。该文档结尾是一个安全保护章节，其中详细介绍了适用于 FTP 固件升级的安全注意事项。实质上：如果指定了密码，则需要输入密码才能使用 FTP 固件升级；如果禁用了 telnet 以避免以明文形式传输密码，则也会禁用 FTP 升级。

以下文档介绍了可以使用 EWS 升级 HP Jetdirect 设备：

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj07572>。EWS 的保护方式决定了 HP Jetdirect 固件升级功能的保护方式。对于 EWS 用户，HP 建议设置从 HTTP 到 HTTPS 的重定向，使用正确签名的证书，当然了，还应指定正确的密码。

HP Jetdirect 黑客攻击：嗅探并重播打印作业

人们很容易找到可对 TCP/IP 协议集实施有效 MITM 攻击的网络工具，这使客户非常担心安全问题。让我们看一下针对 TCP/IP 协议集的 MITM 攻击会执行哪些操作。一个节点通过伪装成另一个节点来截取来自某个节点的 IP 数据包，然后将 IP 数据包转发到下一个正确的节点，因此数据包可能最终会到达最终目标，就好像没有发生截取一样；此外，该 MITM 节点还会以相同方式截取在相反方向（从目标返回到源）上传输的数据包。这意味着，MITM 节点具有在该源和该目标之间发送的所有数据的副本。如果 MITM 节点具有在电子邮件客户端和电子邮件服务器之间发送的 PDF 文件的副本，则它可以使用 Adobe Acrobat Reader 打开该文件。如果 MITM 节点具有在 FTP 客户端和 FTP 服务器之间发送的文本文档的副本，则它可以使用文本编辑器打开该文档。如果 MITM 节点具有打印作业的副本，则它可以将其发送到打印机以“打开”该作业。在某些情况下，就像 PostScript 或简单文本一样，可以使用其它应用程序打开打印作业，而无需将其发送到打印机。虽然这的确是一个漏洞，但它只不过是常规 TCP/IP 协议集漏洞，而不是打印特有的漏洞。

被动嗅探攻击是指，网络上的另一个节点可以记录对话。这些攻击类似于以下情况：使用藏在会议室中的窃听设备记录会议谈话内容。也可以使用主动攻击，强制网络基础设施设备按允许被动嗅探的方式工作。这种主动/被动行为类似于以下情况：某个人无法将窃听设备藏在会议室中，而是拉响大楼的火灾警报，然后记录离开会议室的这些人的谈话内容。正确部署的加密协议可以很好地防御被动和主动嗅探攻击。可以对网络基础设施设备进行配置以帮助阻止主动攻击。端口访问控制（如 802.1X）可以帮助防范未经授权的连接。此外，很多交换机供应商还提供了各种类型的 ARP 保护和监控功能，因为破坏 ARP 是 MITM 攻击的一个重要步骤。

TCP/IP MITM 攻击的防御方法是，使用正确签名的 HP Jetdirect 证书来正确部署加密协议，例如，IPsec 和 SSL/TLS。HP 建议正确部署 IPsec（第 4 组）以作为此常规 TCP/IP 协议集漏洞的解决方案。

HP Jetdirect 黑客攻击：打印机/MFP 访问

到目前为止，我们主要讨论了 HP Jetdirect 安全保护。某些公开发布的应用程序通过打印连接直接与打印机/MFP 的 PJI 库进行交互。这些工具通常声称可绕过 HP Jetdirect 安全功能。但是，正如我们从功能图表中看到的一样，HP Jetdirect 控制网络堆栈并且不分析 PJI，因而无法将其配置来阻止 PJI 命令。但是，可以对打印机/MFP 进行配置以提供一些安全功能。对于担心打印机/MFP 安全问题的所有客户，HP 建议使用以下 NIST 检查清单作为指导原则：

http://www.hp.com/united-states/business/catalog/nist_checklist.html。

建议的安全部署：第 1 组

第 1 组代表的 HP Jetdirect 产品没有任何加密安全功能。因此，建议使用 BOOTP/TFTP 配置，因为我们可以通过 TFTP 配置文件指定一些控制参数。在配置该配置文件后，可以在产生非常小的管理开销的情况下提供大量功能。很多客户将 BOOTP/TFTP 与 UNIX 或 Linux 环境联系到一起；但是，有很多用于 Windows 的免费 BOOTP 和 TFTP 服务器，并且安装过程非常简单。下面提供了一个示例 UNIX 配置。

```
picasso:\
:hn:\
:ht=ether:\
:vm=rfc1048:\
:ha=0001E6123456:\
:ip=192.168.40.39:\
:sm=255.255.255.0:\
:gw=192.168.40.1:\
:lg=192.168.40.3:\
:T144="hpnp/picasso.cfg":\
:T151="BOOTP-ONLY":
```

该配置提供了以下内容：

- 系统日志服务器：192.168.40.3
- TFTP 配置文件：picasso.cfg，在 TFTP 守护程序主目录的“hpnp”的子目录下
- 强制 HP Jetdirect 始终使用 BOOTP；如果 BOOTP 服务器不可用，也不会转换到 DHCP。

以下是 TFTP 配置文件 picasso.cfg 的内容示例：

```
# Allow subnet 192.168.40.0 access
allow: 192.168.40.0 255.255.255.0
#
# Disable Telnet
telnet-config: 0
#
# Disable the embedded Web server
ews-config: 0
#
# disable unused protocols
ipx/spx: 0
dlc/lc: 0
ethertalk:0
#
# Set a password
passwd:Security4Me3
#
# Disable SNMP
# use with caution – breaks SNMP management tools
snmp-config:0
#
# if SNMP must be enabled, comment out the “snmp-config” command and
# uncomment out the following:
# set-community-name:Security4Me3
# get-community-name:notpublic
# default-get-community: 0
#
# parameter file
parm-file:hpnp/pj|protection
#
```


该 TFTP 配置文件指向一个名为“pj|protection”的参数文件。该文件将在开机时发送到打印机。以下是 pj|protection 文件的示例内容：

```
<ESC>%-12345X@PJL <CR><LF>
@PJL COMMENT **Set Password** <CR><LF>
@PJL COMMENT **& Lock Control Panel**<CR><LF>
@PJL JOB PASSWORD = 7654 <CR><LF>
@PJL DEFAULT PASSWORD = 1776 <CR><LF>
@PJL DINQUIRE PASSWORD <CR><LF>
@PJL DEFAULT CPLOCK = ON <CR><LF>
@PJL DINQUIRE CPLOCK <CR><LF>
@PJL EOJ <CR><LF>
<ESC>%-12345X
```

建议的安全部署：第 2 组

对于第 2 组中的 HP Jetdirect 产品，建议非 HP Web Jetadmin 用户使用安全向导。可通过依次选择 Networking（网络）标签、左侧导航栏中的 Settings（设置）和 Wizard（向导）标签来访问该安全向导。下面显示了一个示例配置：

<p>注：在浏览到该页面时，请确保使用的是 HTTPS。按 Start Wizard（启动向导）按钮以启动向导。</p> <ul style="list-style-type: none">• Networking（网络）• Settings（设置）• Wizard（向导）	
--	---

<p>要在 Jetdirect 上实施的安全级别。此处，我们将选择 Custom Security（自定义安全功能）以显示客户可以使用的所有选项。</p> <p>Security Level（安全级别）</p>	
---	--

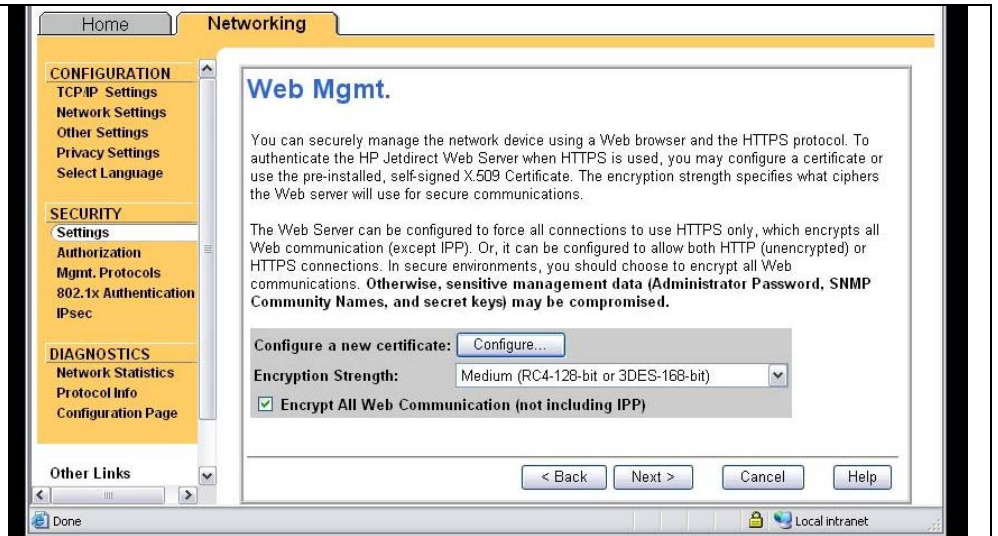
首先，设置一个密码。

Administrator Account
(管理员帐户)



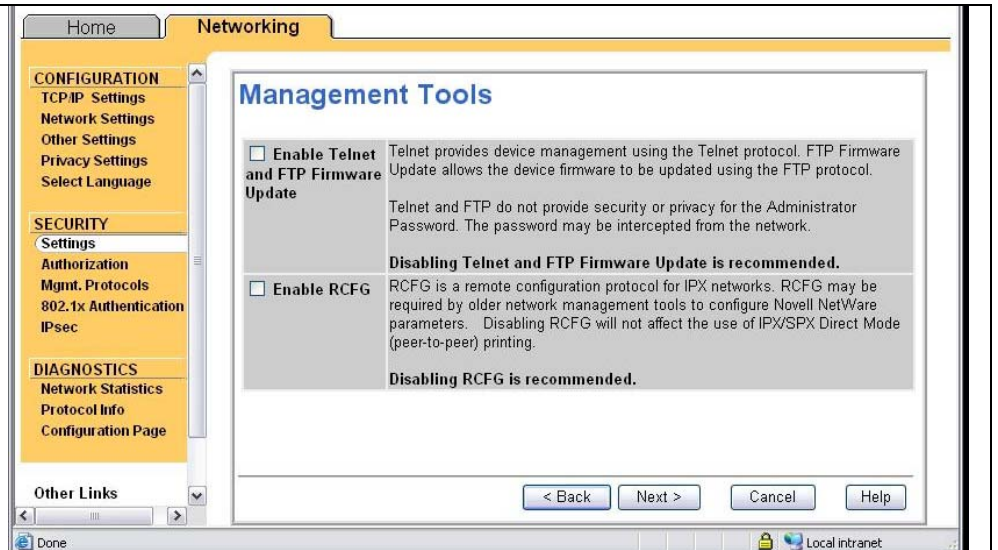
将加密强度更改为 Medium (中)，然后选中 Encrypt All Web Communication (加密所有 Web 通信) 复选框。该复选框强制所有 Web 通信都使用 HTTPS。

Web Management
(Web 管理)



取消选中 Enable Telnet and FTP Firmware Update (启用 Telnet 和 FTP 固件更新) 和 Enable RCFG (启用 RCFG)。

Management tools
(管理工具)



取消选中 Enable SNMPv1/v2 (启用 SNMPv1/v2) 并选中 Enable SNMPv3 (启用 SNMPv3)。

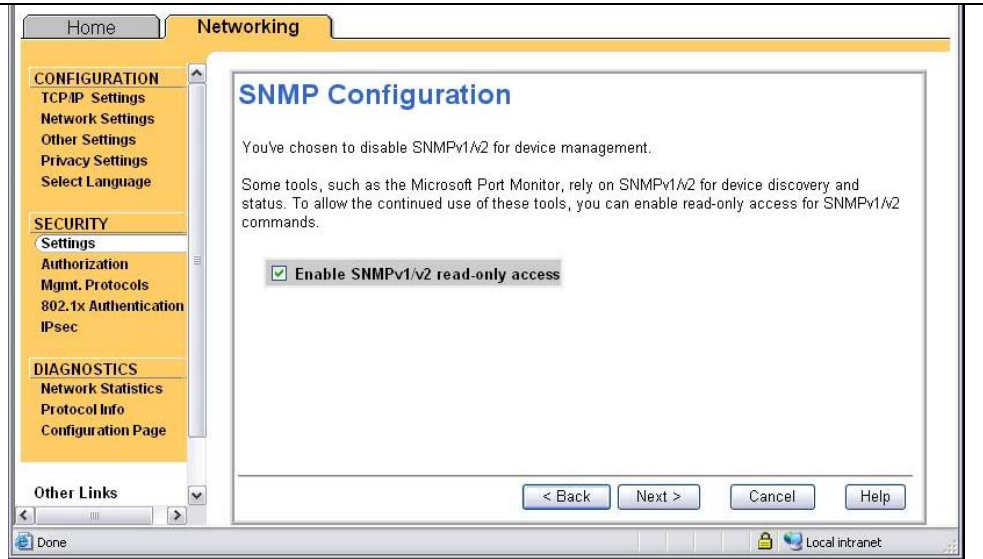
SNMP Configuration (SNMP 配置)

提供 SNMPv3 参数。

SNMPv3 Configuration (SNMPv3 配置)

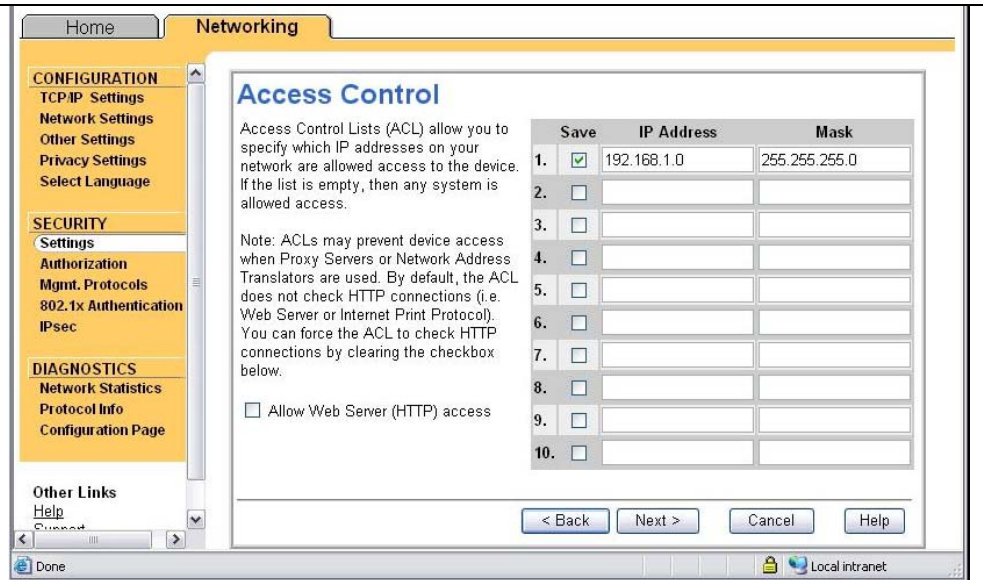
根据客户的环境，可能需要授予只读 SNMPv1/v2c 访问权限。某些工具（如 HP Standard Port Monitor）使用 SNMPv1/v2c 来查看状态。

Enable SNMPv1/v2 read only access（启用 SNMPv1/v2 只读访问）



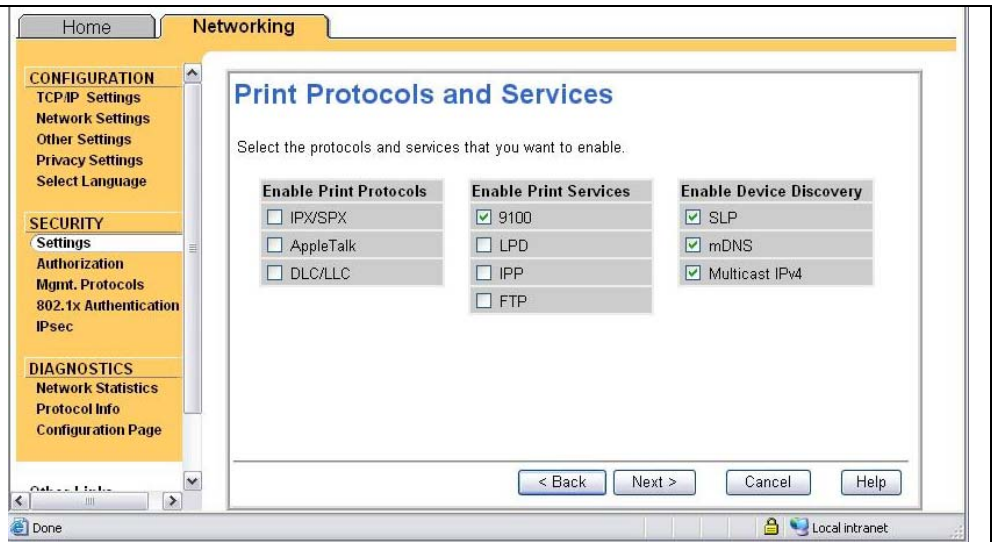
设置访问控制列表项。这是另一个客户环境特定的项。在该示例中，子网 192.168.1.0 是由 ACL 保护的。取消选中 Allow Web Server (HTTP) access（允许 Web 服务器 (HTTP) 访问）以强制在 ACL 中执行 HTTP 检查。

Access Control（访问控制）



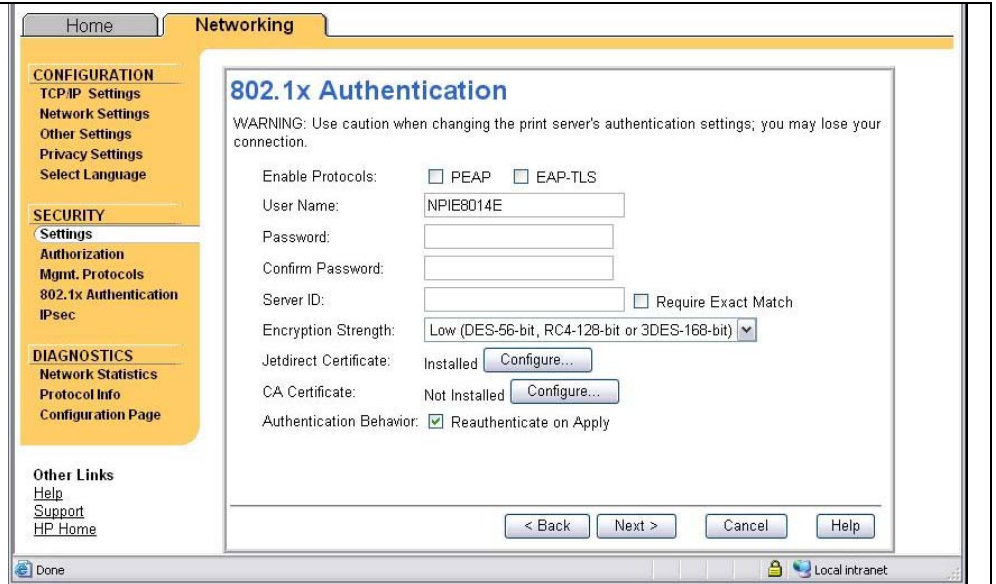
禁用未使用的打印协议和服务。允许设备查找有助于进行设备管理，但并非所有环境中都需要此功能。

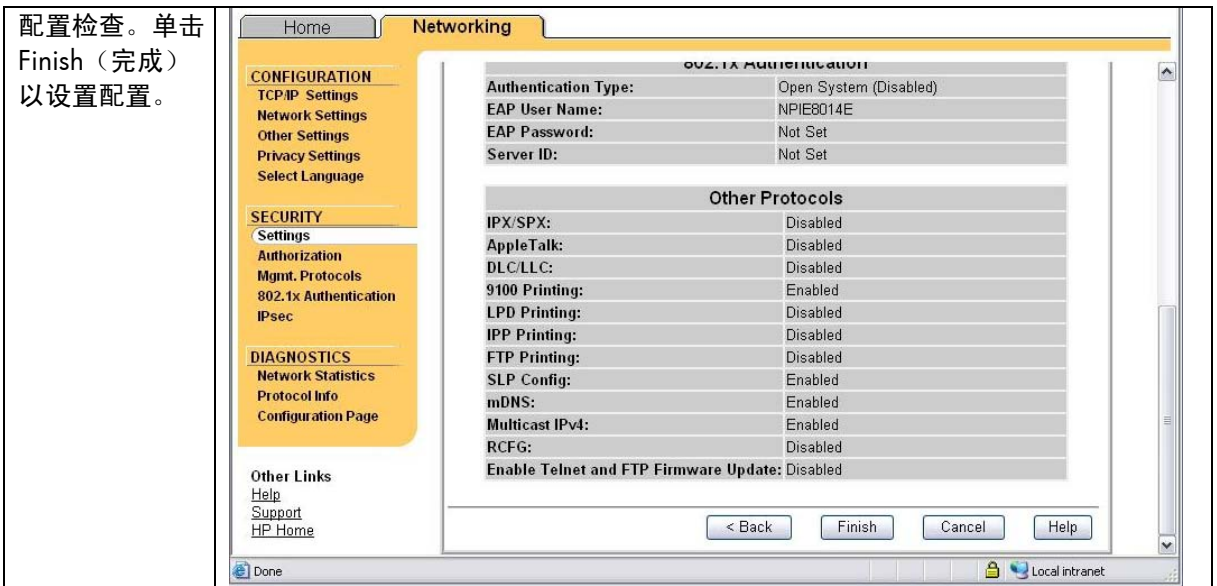
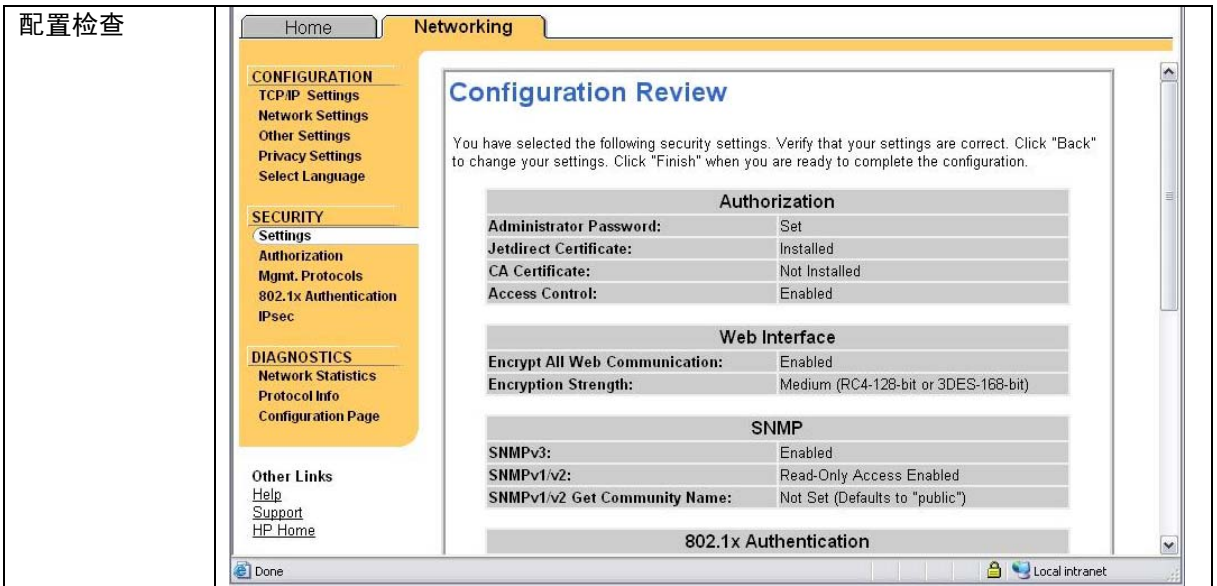
Print Protocols and Services
(打印协议和服务)



还可以执行 802.1X 验证。需要特殊设备。有关 802.1X 的完整讨论，请参见 HP Jetdirect 白皮书中有关该主题的内容。此时，将跳过该配置步骤。

802.1x
Authentication
(802.1x
验证)





建议的安全部署：第 3 组

首先，第 3 组配置需要执行用于第 2 组的安全向导。在完成安全向导配置后，我们即可开始进行防火墙配置。下面显示了一个示例防火墙配置，其中将管理协议限定在特定的 IP 子网范围内：

在浏览到该页面之前，请确保使用的是 HTTPS。在 Default Rule（默认规则）的下拉框中选择 Allow（允许），然后单击 Add Rules...（添加规则...）。

- Networking（网络）
- Firewall（防火墙）
- Firewall Policy（防火墙策略）
- Enable firewall（启用防火墙）

The screenshot shows the 'Firewall Policy' configuration page. The sidebar on the left is under the 'Networking' tab and includes sections for 'Configuration', 'Security', and 'Diagnostics'. The 'Firewall' option is selected. The main content area has a title 'Firewall Policy' and a 'Support' link. Below the title is an 'Enable Firewall' checkbox. A table titled 'Firewall Rules' has columns for 'Rule', 'Enable', 'Address Template', 'Services Template', and 'Action'. The table contains 10 rows, all with 'Enable' checkboxes unchecked. Below the table are buttons for 'Add Rules...', 'Delete Rules...', and 'Advanced'. A dropdown menu shows 'Default Rule', 'All IP Addresses', 'All Services', and 'Allow'. At the bottom, there are 'Apply' and 'Cancel' buttons and a warning message: 'Warning: Changing IPsec/Firewall settings may result in temporary loss of connection.'

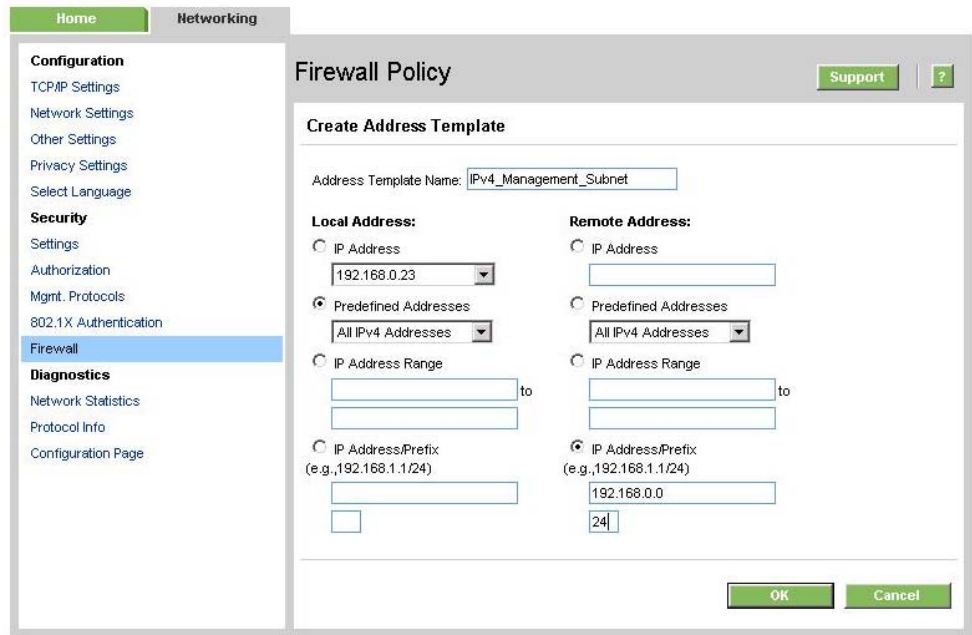
我们已经为打印和成像设备定义了一个特定的管理员子网。单击 New（新建）按钮，以便明确指定可以管理设备的地址。

- Rule 1: Specify Address Template（规则 1：指定地址模板）
- All IP addresses（所有 IP 地址）

The screenshot shows the 'Rule 1: Specify Address Template' configuration page. The sidebar on the left is under the 'Networking' tab and includes sections for 'Configuration', 'Security', and 'Diagnostics'. The 'Firewall' option is selected. The main content area has a title 'Rule 1: Specify Address Template' and a 'Support' link. Below the title is a text area for specifying the address template. A list titled 'Address Templates:' contains five items: 'All IP Addresses', 'All IPv4 Addresses', 'All IPv6 Addresses', 'All link local IPv6', and 'All non link local IPv6'. Below the list are buttons for 'New', 'View...', and 'Delete'. At the bottom, there are 'Next >' and 'Cancel' buttons and a note: 'Note: Predefined templates will create multiple rules.'

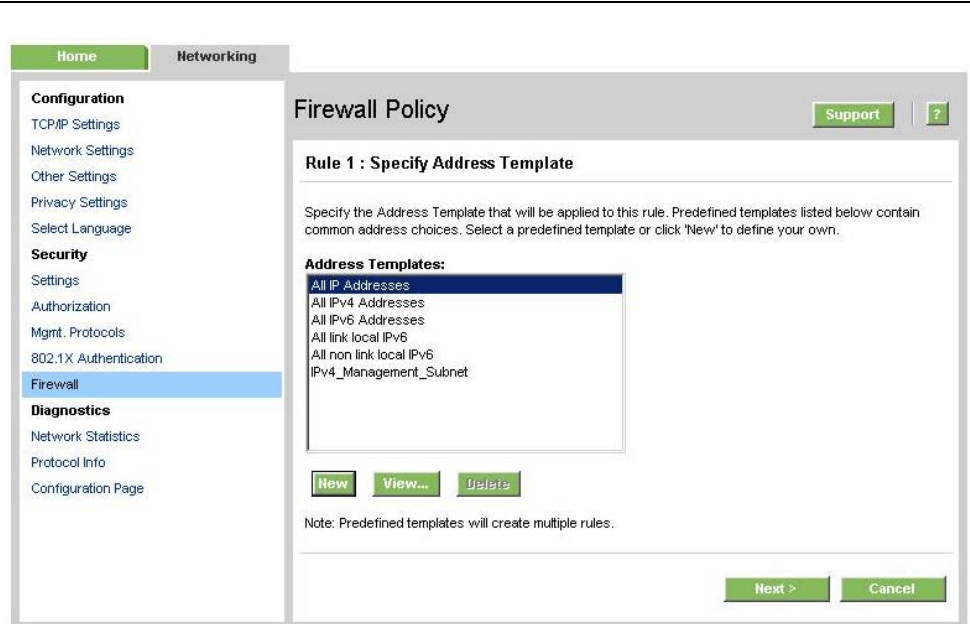
我们先定义 IPv4 地址范围。为 Local Address (本地地址) 选择 All IPv4 Addresses (所有 IPv4 地址), 然后为 Remote Address (远程地址) 指定 192.168.0/24 子网。我们也非常明确地命名了该地址模板。

Create Address Template (创建地址模板)



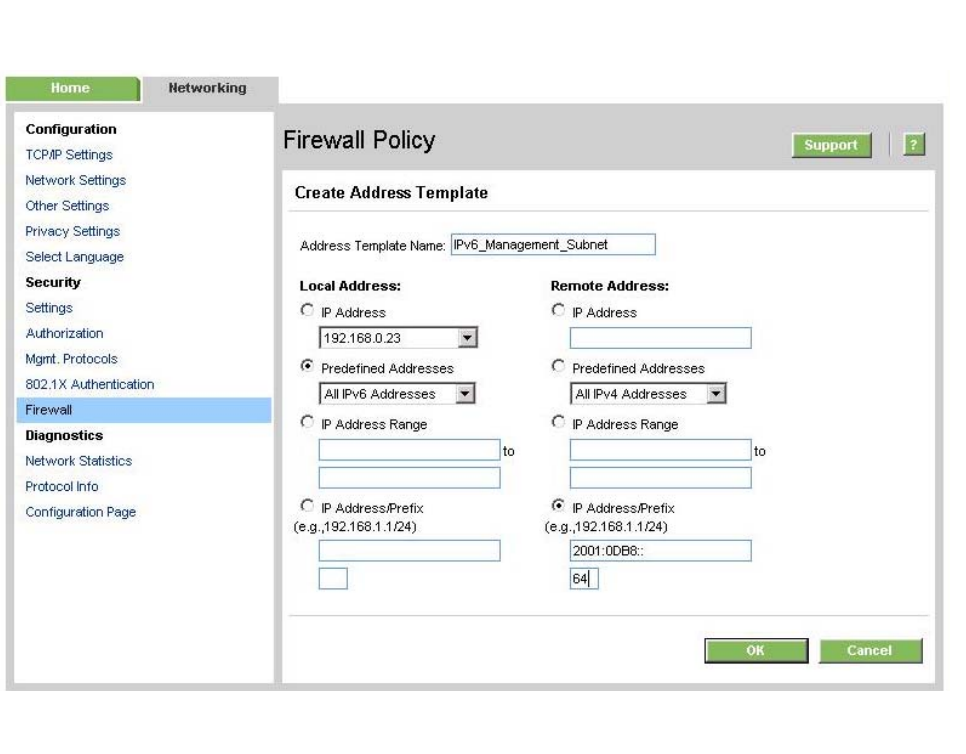
现在轮到定义 IPv6 了。再次单击 New (新建)。注: 如果网络中未使用 IPv6, 请转到 TCP/IP 设置, 然后禁用 IPv6 以提高安全性。也可以跳过此步骤, 以便在此配置中使用 IPv6。

- Rule 1: Specify Address Template (规则 1: 指定地址模板)
- All IP addresses (所有 IP 地址)



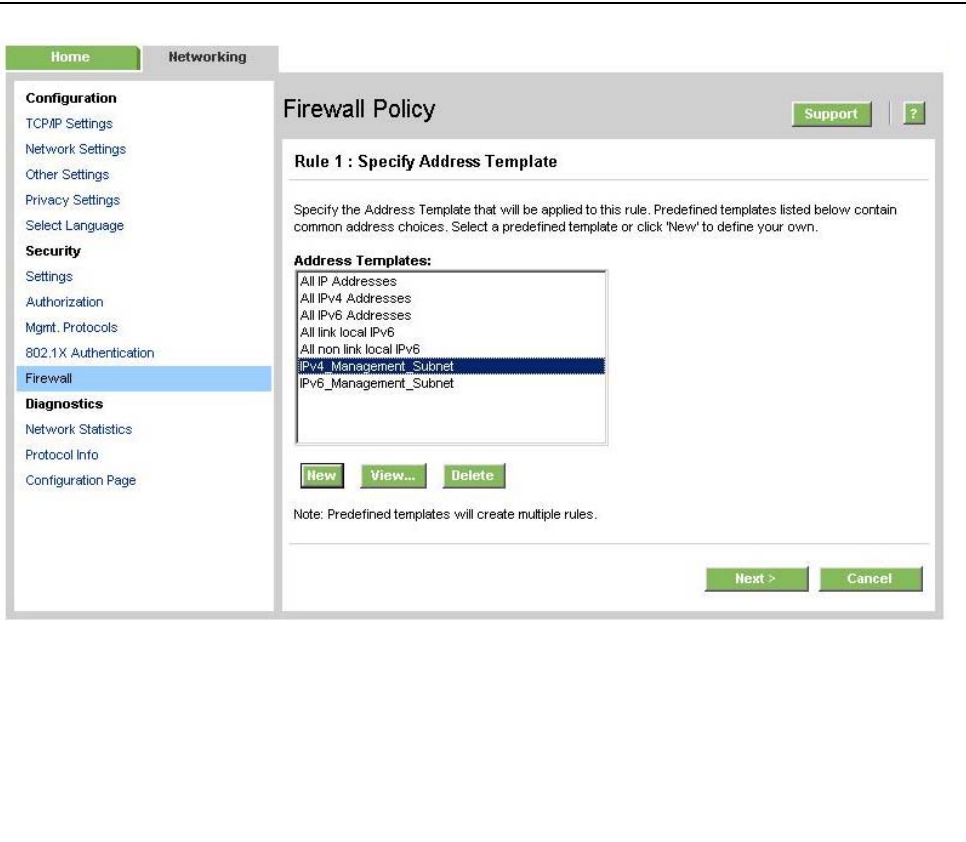
选择相应的 IPv6 地址，然后命名该地址模板。

Create Address Template
(创建地址模板)



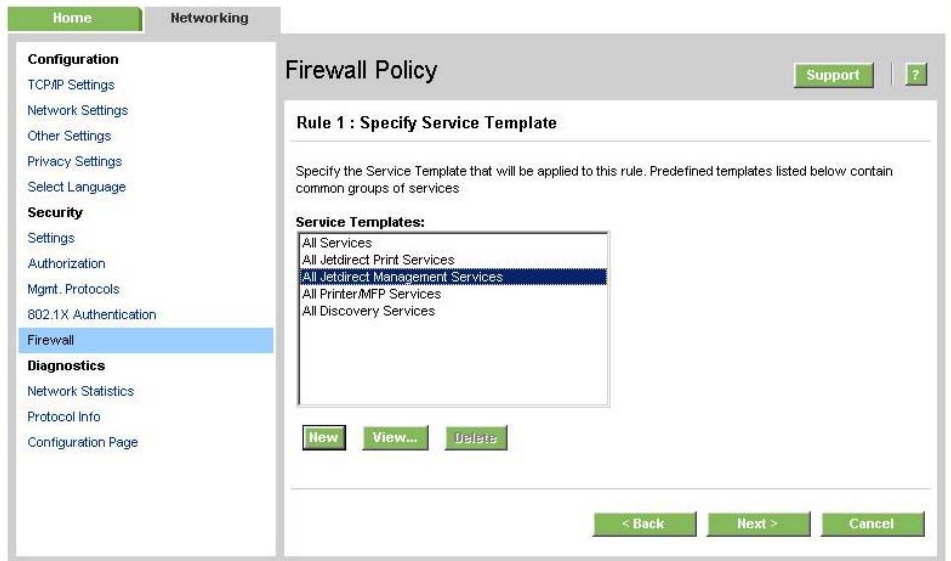
现在，我们已创建了地址模板，让我们创建一个规则。将按照从 1 到 10 的优先顺序来处理规则。我们先创建一个 IPv4 规则。选择创建的 IPv4 地址模板，然后单击 Next (下一步)。

- Rule 1: Specify Address Template (规则 1: 指定地址模板)
- All IP addresses (所有 IP 地址)



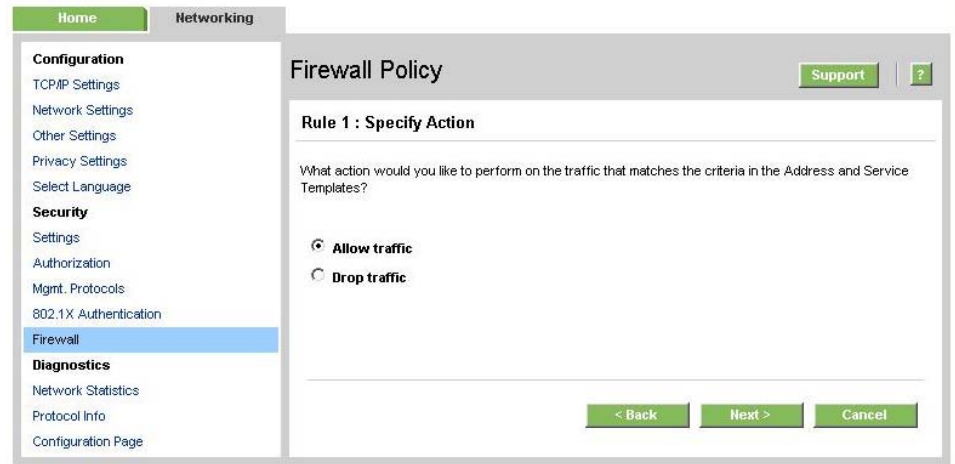
我们关心的是管理服务，因此，选择 All Jetdirect Management Services（所有 Jetdirect 管理服务）服务模板。单击 Next（下一步）。

Rule 1: Specify Service Template
（规则 1：指定服务模板）



选择 Allow Traffic（允许通信）。单击 Next（下一步）。

Rule 1: Specify Alarm
（规则 1：指定警报）



选择 Create another rule (创建另一个规则)。

Rule Summary (规则摘要)

The screenshot shows the 'Firewall Policy' configuration page. On the left is a navigation menu with categories: Configuration, Security, and Diagnostics. The 'Firewall' option is selected. The main content area is titled 'Firewall Policy' and contains a 'Rule Summary' section. Below this is a table of 'Firewall Rules' with columns for Rule, Match Criteria (Address Template, Services Template), and Action on Match. Rule 1 is highlighted, showing 'IPV4_Management_Subnet' as the address template and 'All Jetdirect Management Services' as the services template, with the action 'Allow traffic'. At the bottom, there are buttons for '< Back', 'Create Another Rule', 'Finish', and 'Cancel'. A warning message is present: 'Warning: Changing IPsec/Firewall settings may result in temporary loss of connection.'

Rule	Match Criteria		Action on Match
	Address Template	Services Template	Action
1	IPV4_Management_Subnet	All Jetdirect Management Services	Allow traffic
2			
3			
4			
5			
6			
7			
8			
9			
10			
Default Rule	All IP Addresses	All Services	Allow

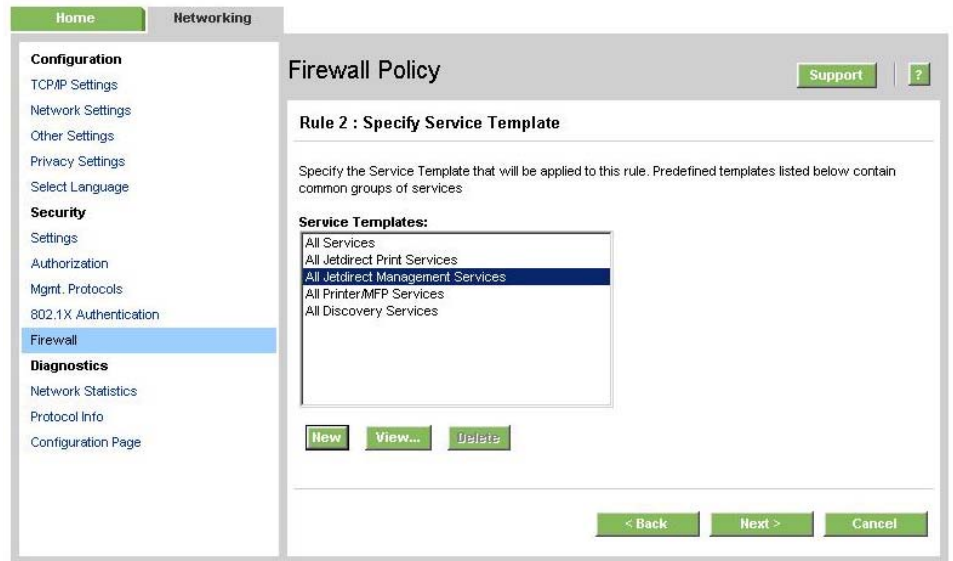
选择创建的 IPv6 地址模板，然后单击 Next (下一步)。

Rule 2: Specify Address Template (规则 2: 指定地址模板)

The screenshot shows the 'Firewall Policy' configuration page at the 'Rule 2: Specify Address Template' step. The left navigation menu is the same as in the previous screenshot. The main content area is titled 'Rule 2: Specify Address Template'. It contains a text box for specifying the address template and a list of predefined templates. The 'IPv6_Management_Subnet' template is selected. Below the list are buttons for 'New', 'View...', and 'Delete'. At the bottom, there are buttons for 'Next >' and 'Cancel'. A note states: 'Note: Predefined templates will create multiple rules.'

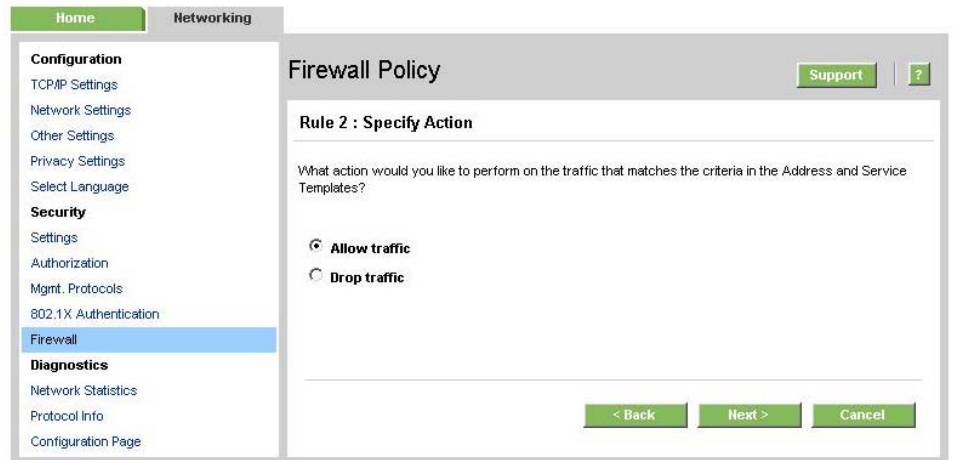
选择 All Jetdirect Management Services (所有 Jetdirect 管理服务) 服务模板。单击 Next (下一步)。

Rule 2: Specify Service Template (规则 2: 指定服务模板)



选择 Allow Traffic (允许通信)。单击 Next (下一步)。

Rule 2: Specify Alarm (规则 2: 指定警报)



我们已允许了来自 IPv4/IPv6 管理子网的管理通信。现在，我们必须创建规则以丢弃所有其它管理通信。单击 Create another rule（创建另一个规则）。

Rule Summary
(规则摘要)

The screenshot shows the 'Firewall Policy' configuration page. On the left is a navigation menu with sections: Configuration, Security, and Diagnostics. The 'Firewall' option under Configuration is selected. The main content area is titled 'Firewall Policy' and contains a 'Rule Summary' section. Below this is a table of 'Firewall Rules' with columns for Rule, Address Template, Services Template, and Action. The table shows two rules, both allowing traffic from management subnets. At the bottom, there are buttons for '< Back', 'Create Another Rule', 'Finish', and 'Cancel'. A warning message is displayed below the table, stating that an invalid configuration could make the device inaccessible.

Match Criteria			Action on Match
Rule	Address Template	Services Template	Action
1	IPv4_Management_Subnet	All Jetdirect Management Services	Allow traffic
2	IPv6_Management_Subnet	All Jetdirect Management Services	Allow traffic
3			
4			
5			
6			
7			
8			
9			
10			
Default Rule	All IP Addresses	All Services	Allow

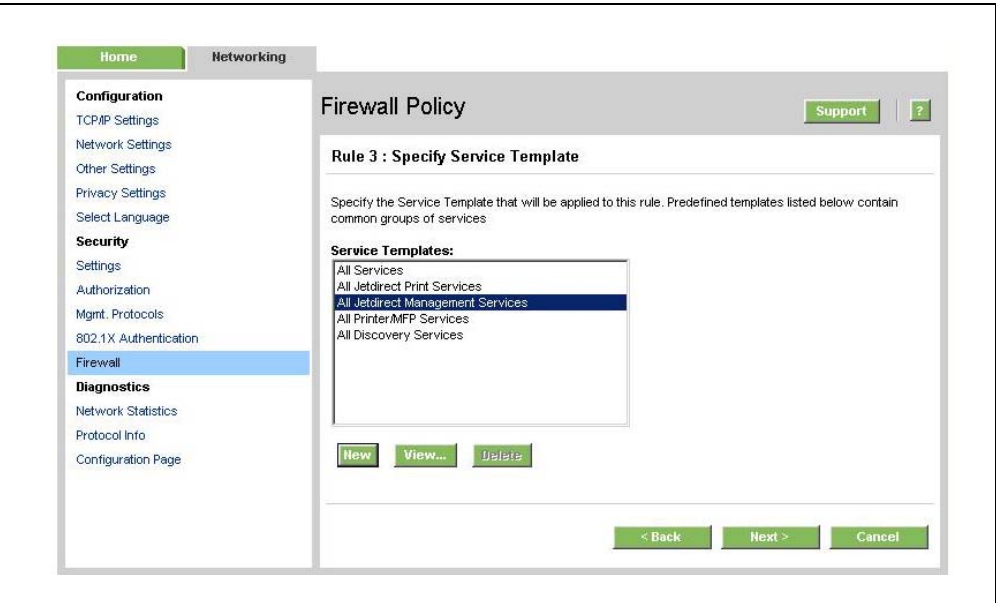
此处，我们选择 All IP addresses（所有 IP 地址），其中包括 IPv4 和 IPv6。单击 Next（下一步）。

Rule 3: Specify Address Template
(规则 3: 指定地址模板)

The screenshot shows the 'Firewall Policy' configuration page at the 'Rule 3: Specify Address Template' step. The left navigation menu is the same as in the previous screenshot. The main content area is titled 'Rule 3: Specify Address Template'. It contains a list of 'Address Templates' with 'All IP Addresses' selected. Below the list are buttons for 'New', 'View...', and 'Delete'. At the bottom right, there are buttons for 'Next >' and 'Cancel'. A note states that predefined templates will create multiple rules.

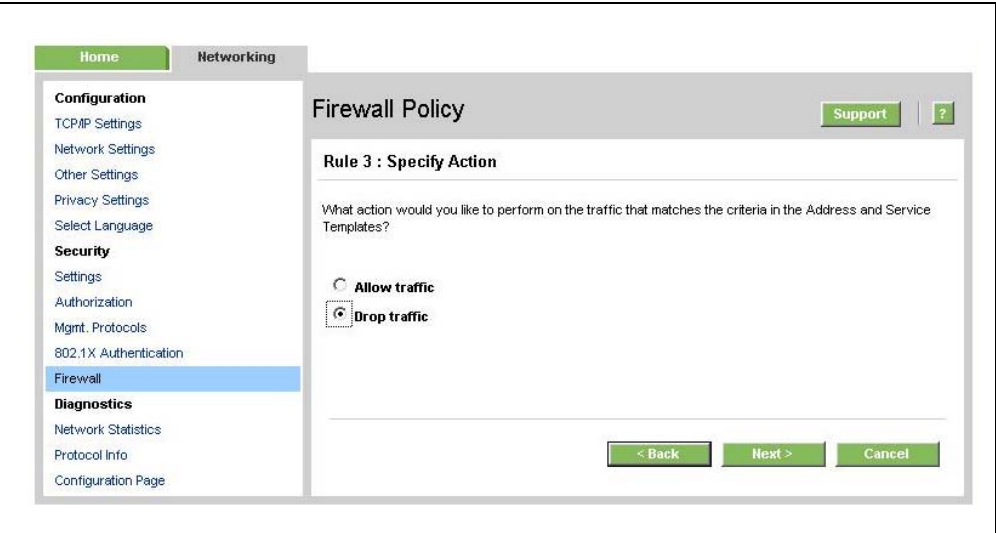
再次选择 All Jetdirect Management Services（所有 Jetdirect 管理服务）作为服务模板，然后单击 Next（下一步）。

Rule 3: Specify Service Template（规则 3: 指定服务模板）



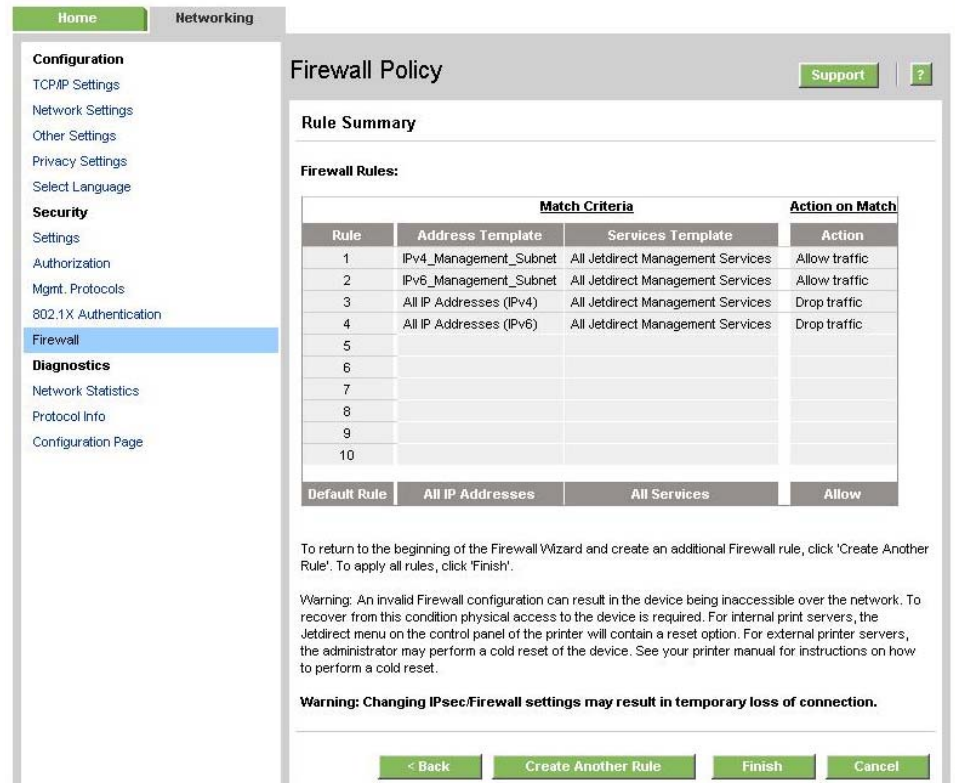
选择 Drop（删除）。单击 Next（下一步）。

Rule 3: Specify Alarm（规则 3: 指定警报）



我们现在可以看一下策略。规则是按照从 1 到 10 的顺序处理的。如果数据包来自或发送到我们定义的 IPv4/IPv6 子网，规则将与之相匹配并允许传输数据包。否则，如果数据包是管理服务，则将其丢弃。将允许所有其它通信；默认规则为 Allow（允许）。单击 Finish（完成）。

Rule Summary（规则摘要）



Home Networking

Configuration

- TCP/IP Settings
- Network Settings
- Other Settings
- Privacy Settings
- Select Language
- Security**
 - Settings
 - Authorization
 - Mgmt. Protocols
 - 802.1X Authentication
 - Firewall**
- Diagnostics**
 - Network Statistics
 - Protocol Info
 - Configuration Page

Firewall Policy

Support ?

Rule Summary

Firewall Rules:

Rule	Match Criteria		Action on Match
	Address Template	Services Template	Action
1	IPv4_Management_Subnet	All Jetdirect Management Services	Allow traffic
2	IPv6_Management_Subnet	All Jetdirect Management Services	Allow traffic
3	All IP Addresses (IPv4)	All Jetdirect Management Services	Drop traffic
4	All IP Addresses (IPv6)	All Jetdirect Management Services	Drop traffic
5			
6			
7			
8			
9			
10			
Default Rule	All IP Addresses	All Services	Allow

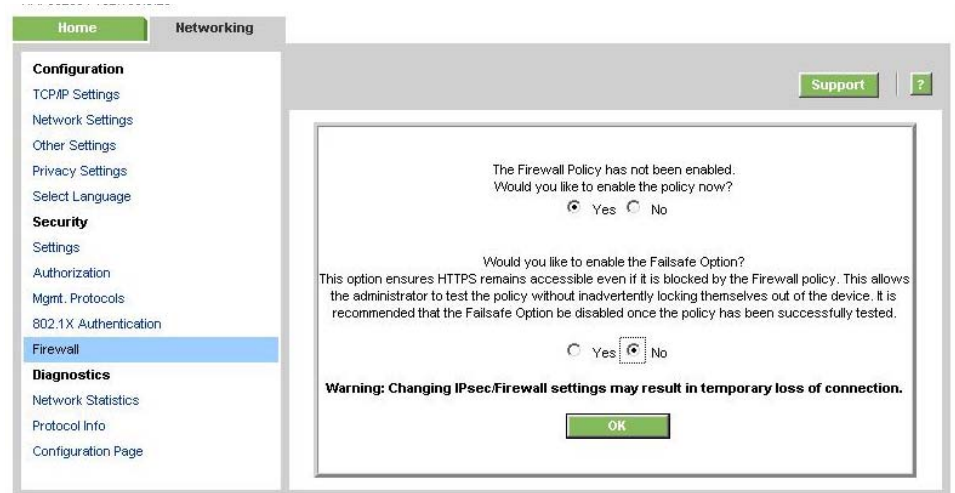
To return to the beginning of the Firewall Wizard and create an additional Firewall rule, click 'Create Another Rule'. To apply all rules, click 'Finish'.

Warning: An invalid Firewall configuration can result in the device being inaccessible over the network. To recover from this condition physical access to the device is required. For internal print servers, the Jetdirect menu on the control panel of the printer will contain a reset option. For external printer servers, the administrator may perform a cold reset of the device. See your printer manual for instructions on how to perform a cold reset.

Warning: Changing IPsec/Firewall settings may result in temporary loss of connection.

< Back Create Another Rule Finish Cancel

对于 Enable Policy（启用策略），选择 Yes（是）。检验配置时，可以使用 HTTPS 防故障功能。如果这是第一个防火墙配置，您可能需要将其启用，然后在进行测试后将其禁用。单击 Ok（确定）。



Home Networking

Configuration

- TCP/IP Settings
- Network Settings
- Other Settings
- Privacy Settings
- Select Language
- Security**
 - Settings
 - Authorization
 - Mgmt. Protocols
 - 802.1X Authentication
 - Firewall**
- Diagnostics**
 - Network Statistics
 - Protocol Info
 - Configuration Page

The Firewall Policy has not been enabled.
Would you like to enable the policy now?

Yes No

Would you like to enable the Failsafe Option?
This option ensures HTTPS remains accessible even if it is blocked by the Firewall policy. This allows the administrator to test the policy without inadvertently locking themselves out of the device. It is recommended that the Failsafe Option be disabled once the policy has been successfully tested.

Yes No

Warning: Changing IPsec/Firewall settings may result in temporary loss of connection.

OK

建议的安全部署：第 4 组

首先，第 4 组配置需要执行用于第 2 组的安全向导。在完成安全向导配置后，我们即可开始进行 IPsec 配置。让我们执行与第 3 组相同的过程，简单地说，只是在这次配置中，所有 IP 地址必须使用 IPsec 来使用管理协议。如果终端站尝试通过管理协议与 Jetdirect 进行通信，而不使用 IPsec，IP 层将丢弃数据包。

在浏览到该页面之前，请确保使用的是 HTTPS。选择 Allow（允许）作为默认规则，然后单击 Add Rules...（添加规则...）。

- IPsec/Firewall Policy（IPsec/防火墙策略）
- IPsec/Firewall Rules（IPsec/防火墙规则）

Rule	Enable	Address Template	Services Template	Action
1	<input type="checkbox"/>			
2	<input type="checkbox"/>			
3	<input type="checkbox"/>			
4	<input type="checkbox"/>			
5	<input type="checkbox"/>			
6	<input type="checkbox"/>			
7	<input type="checkbox"/>			
8	<input type="checkbox"/>			
9	<input type="checkbox"/>			
10	<input type="checkbox"/>			

选择 All IP Addresses（所有 IP 地址），然后单击 Next（下一步）。

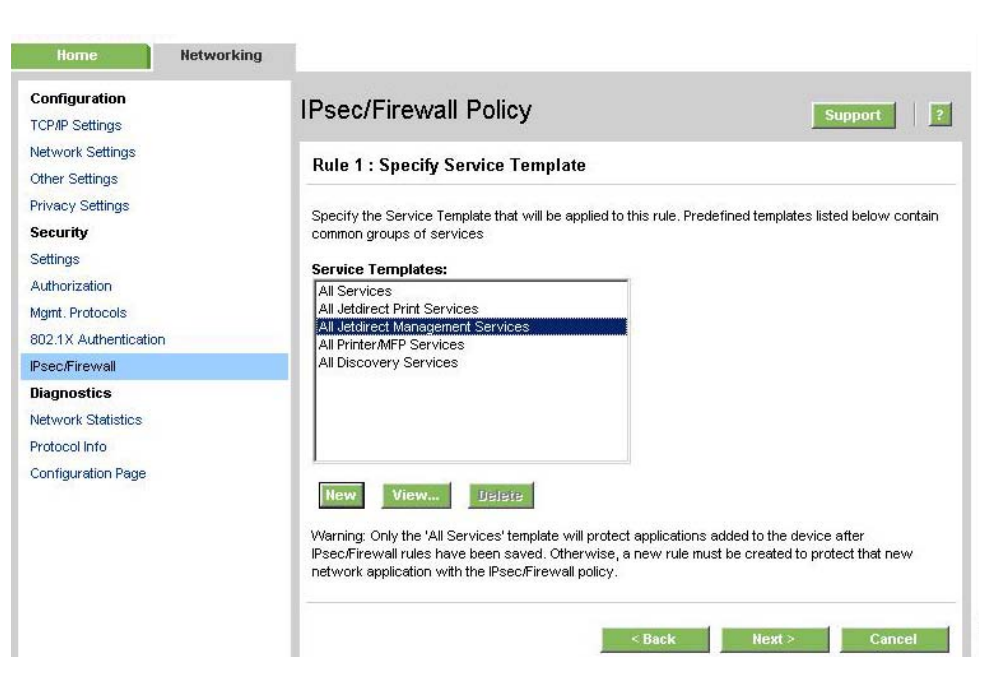
Rule 1: Specify Address Template（规则 1：指定地址模板）

Address Templates:

- All IP Addresses
- All IPv4 Addresses
- All IPv6 Addresses
- All link local IPv6
- All non link local IPv6

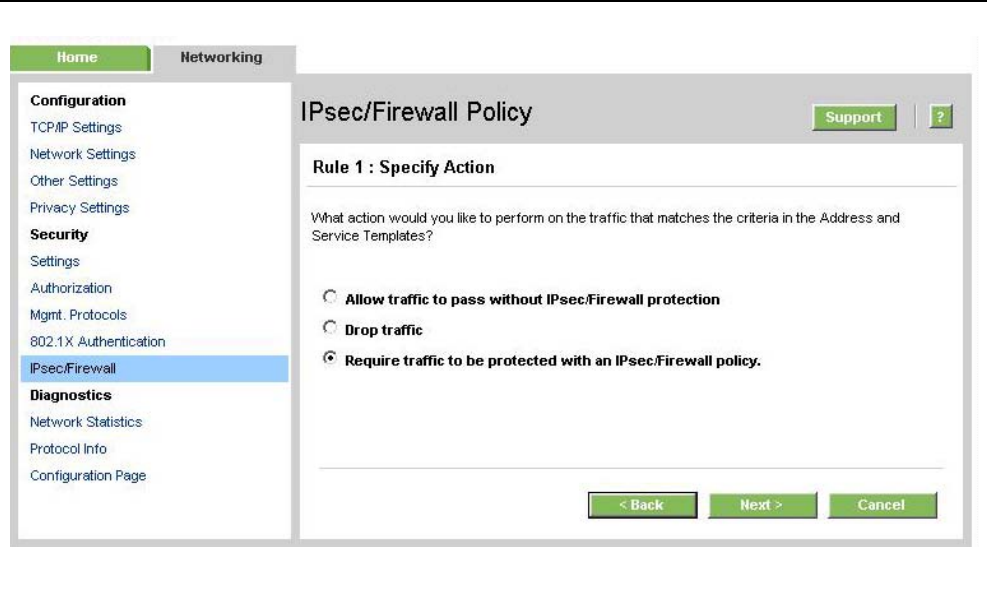
选择 All Jetdirect Management Services（所有 Jetdirect 管理服务）。单击 Next（下一步）。

Rule 1: Specify Service Template（规则 1：指定服务模板）



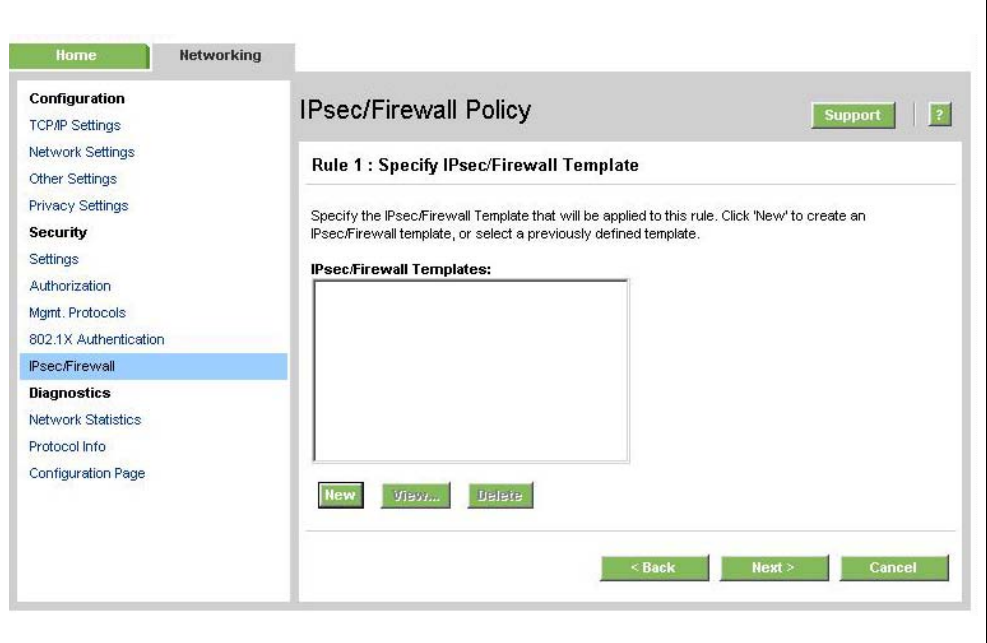
选择 Require traffic to be protected with an IPsec/Firewall Policy（要求使用 IPsec/防火墙策略保护通信）。单击 Next（下一步）。

Rule 1: Specify Alarm（规则 1：指定警报）



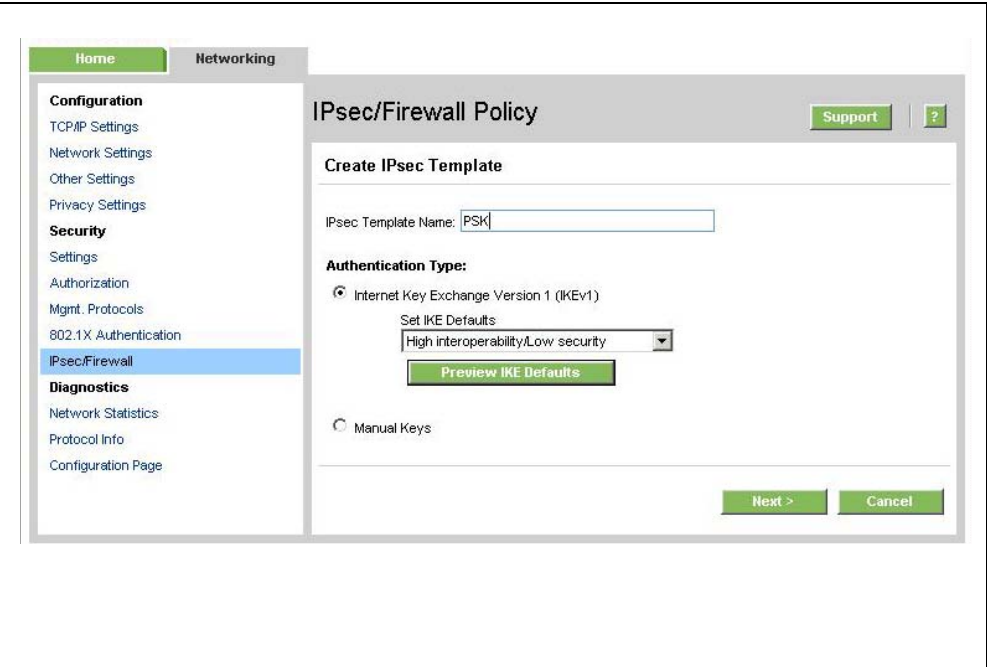
单击 New (新建)。

Rule 1: Specify IPsec Firewall Template (规则 1: 指定 IPsec 防火墙模板)



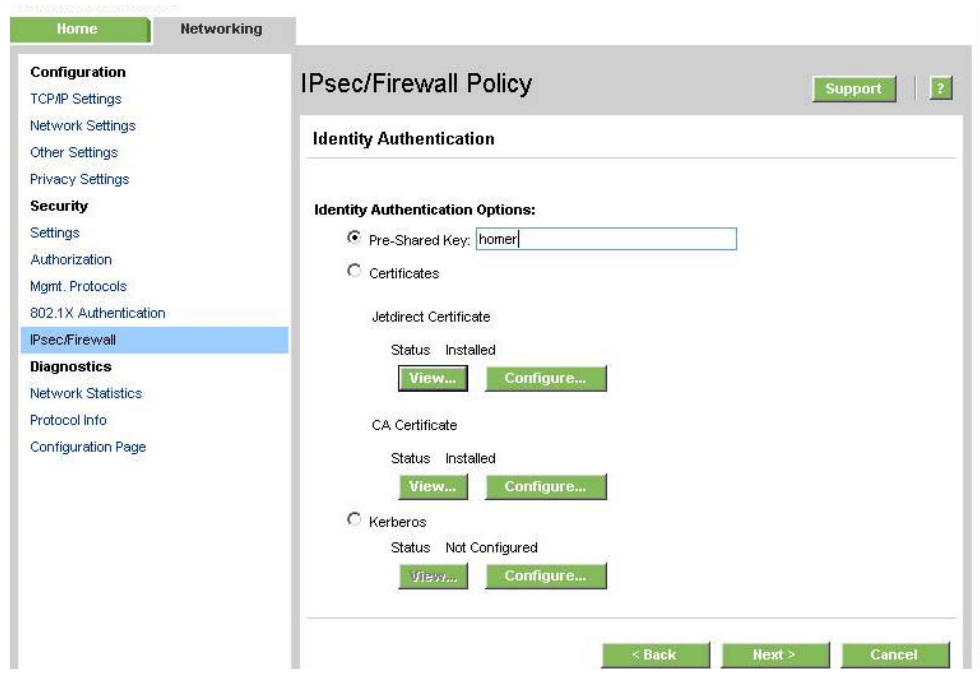
命名 IPsec 模板。某些 Jetdirect 机型可能要求配置 IKE 参数。但是，该机型具有一组可以使用的快速 IKE 默认值。选择的参数值着重强调的是互操作性，而不是安全性。单击 Next (下一步)。

Create IPsec Template (创建 IPsec 模板)



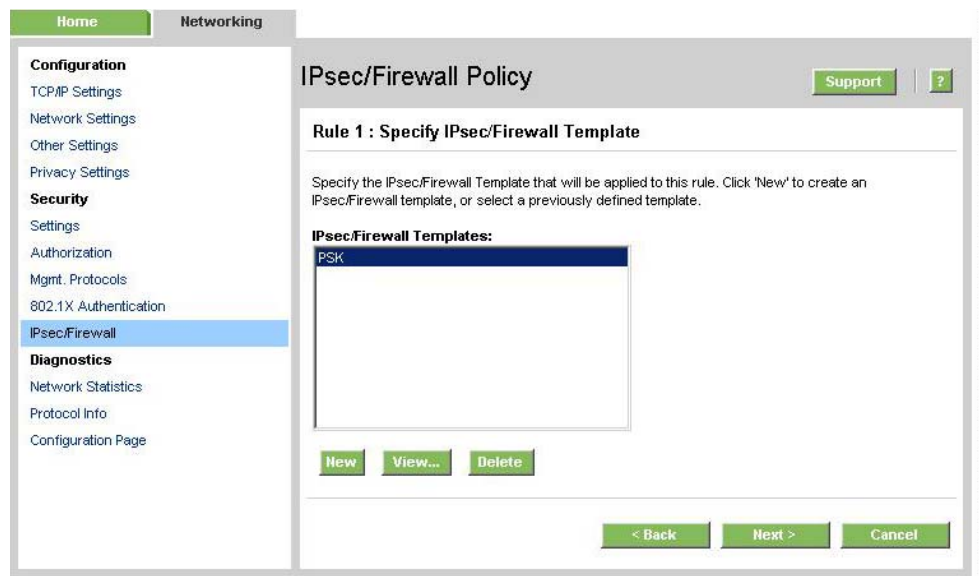
仅出于示例目的，使用了预共享密钥验证。HP 建议不要使用预共享密钥验证。强烈建议使用证书或 Kerberos。
单击 Next（下一步）。

Identify Authentication
(指定验证)



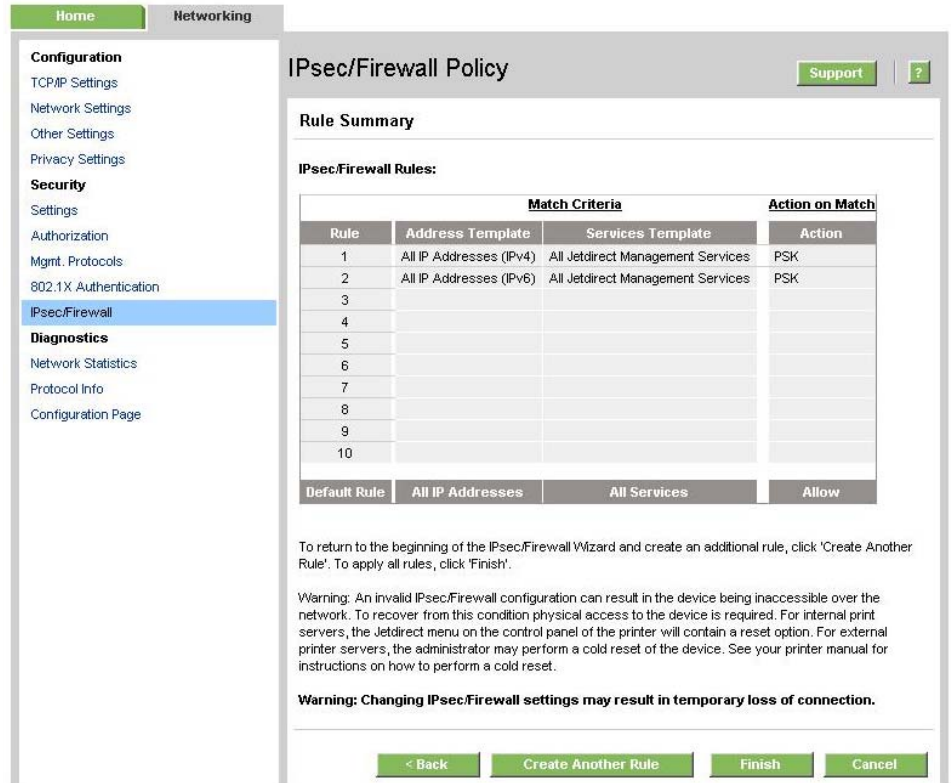
选择刚才创建的 IPsec 模板。
单击 Next（下一步）。

Rule 1: Specify IPsec Firewall Template
(规则 1: 指定 IPsec 防火墙模板)



此处为 IPsec 策略。如果要使用管理协议，它必须使用 IPsec。根据默认规则，将允许所有其它通信。单击 Finish (完成)。

Rule Summary (规则摘要)



IPsec/Firewall Policy

Support ?

Rule Summary

IPsec/Firewall Rules:

Rule	Match Criteria		Action on Match
	Address Template	Services Template	Action
1	All IP Addresses (IPv4)	All Jetdirect Management Services	PSK
2	All IP Addresses (IPv6)	All Jetdirect Management Services	PSK
3			
4			
5			
6			
7			
8			
9			
10			
Default Rule	All IP Addresses	All Services	Allow

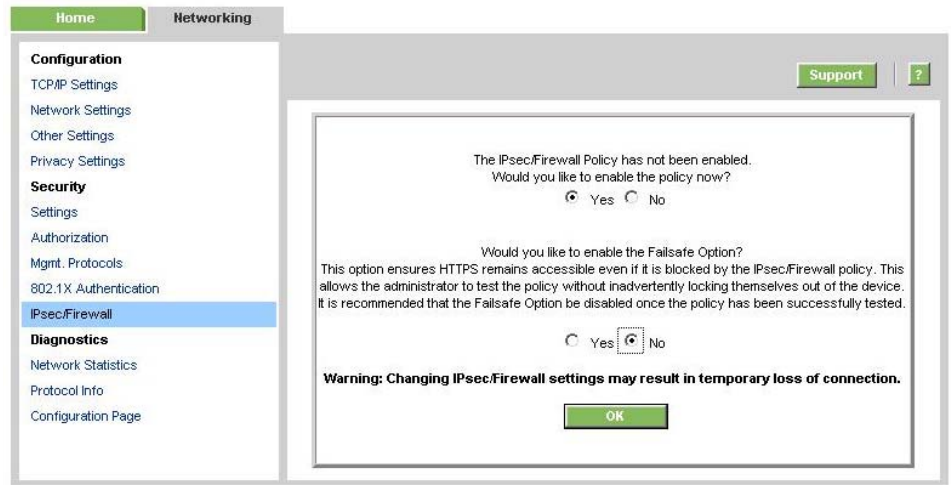
To return to the beginning of the IPsec/Firewall Wizard and create an additional rule, click 'Create Another Rule'. To apply all rules, click 'Finish'.

Warning: An invalid IPsec/Firewall configuration can result in the device being inaccessible over the network. To recover from this condition physical access to the device is required. For internal print servers, the Jetdirect menu on the control panel of the printer will contain a reset option. For external printer servers, the administrator may perform a cold reset of the device. See your printer manual for instructions on how to perform a cold reset.

Warning: Changing IPsec/Firewall settings may result in temporary loss of connection.

< Back Create Another Rule Finish Cancel

选择 Yes (是) 以启用 IPsec 策略。如果需要，也可以选择使用防故障功能。单击 OK (确定)。



The IPsec/Firewall Policy has not been enabled.
Would you like to enable the policy now?

Yes No

Would you like to enable the Failsafe Option?

This option ensures HTTPS remains accessible even if it is blocked by the IPsec/Firewall policy. This allows the administrator to test the policy without inadvertently locking themselves out of the device. It is recommended that the Failsafe Option be disabled once the policy has been successfully tested.

Yes No

Warning: Changing IPsec/Firewall settings may result in temporary loss of connection.

OK

参考资料

802.1X: <http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00731218/c00731218.pdf>

IPsec: <http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01048192/c01048192.pdf>

IPv6: <http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00840100/c00840100.pdf>

使用网络基础设施以更好地保护打印和成像设备:

<http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00707837/c00707837.pdf>