Miercom

实验室测试总结报告

2005 年 10 月
报告 050914

产品种类：
统一威胁管理（UTM）安全设备

被测系统：
Cisco Systems® ASA 5520

Check Point® VPN-1® Pro

Fortinet® FortiGate™ 1000

Juniper Networks® NetScreen-208™

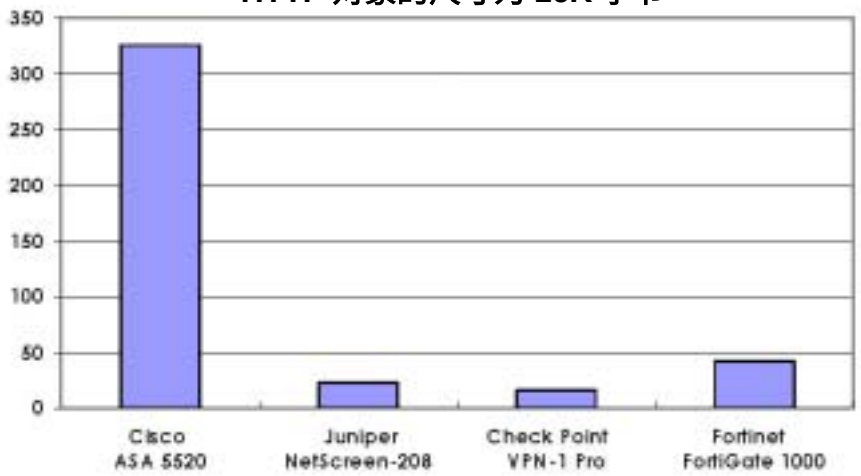
Miercom PERFORMANCE VERIFIED™

主要发现和结论

- **在实际的多功能威胁防御中，Cisco ASA 5520 的吞吐率比同类解决方案高六倍以上。**
- **在利用实际流量进行测试时，Cisco ASA 5520 可以提供比同类产品高出三倍的 3DES 加密 VPN 吞吐率。**
- **Cisco ASA 5520 可以 100%地检测出所有威胁；同类产品只能达到 30%到 40%。**
- **在实际的多功能威胁防御性能对比中，Cisco ASA 5520 具有最高的连接建立速度，比最接近的同类产品快四倍以上。**

思科系统公司®邀请 Miercom 对 Cisco ASA 5520 自适应安全设备与多款同类的、竞争性的统一威胁管理（UTM）安全设备（包括 Check Point® VPN-1® Pro，Fortinet® FortiGate™ 1000, Juniper Networks® NetScreen-208™）进行了独立的对比测试。考察的性能领域包括：统一防火墙和 IPS 吞吐率性能，VPN 吞吐率性能，IPS 威胁防御能力，以及每秒连接性能。

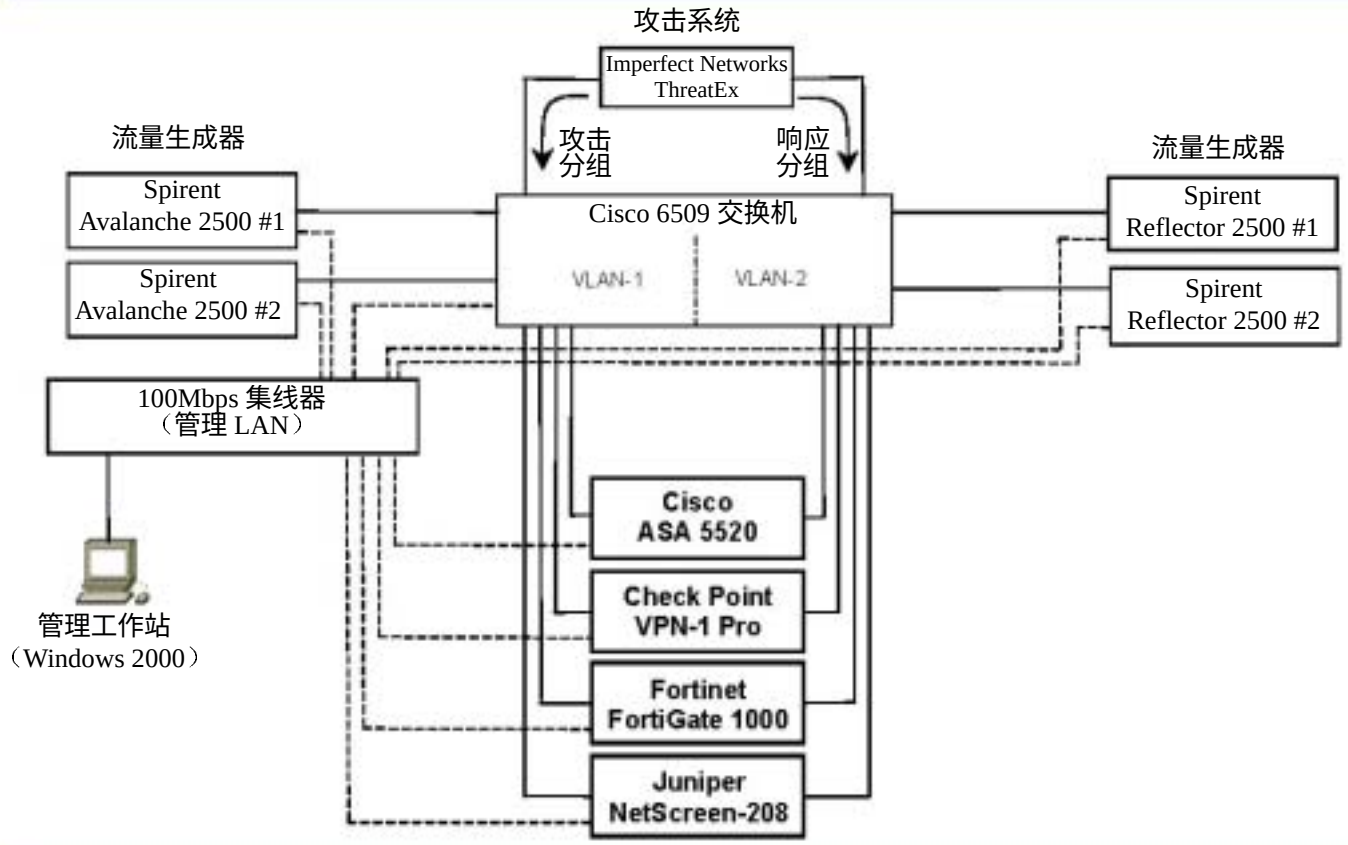
在启用所有攻击/病毒签名时的防火墙性能（Mbps），HTTP 对象的尺寸为 16K 字节



在使用实际流量和尺寸为 16K 字节的对象并启用全部威胁签名时，Cisco ASA 5520 的吞吐率明显高于其他同类产品。

对比测试说明：产生这些结果的测试和测试方法是由赞助本次对比评测的制造商所提议并协助创建的，并且可能受到该制造商的影响。Miercom 会确保公平、准确地运用这些测试和方法。这些评测结果不应作为选择或购买产品的唯一参照标准。

测试环境的设置



关于测试：对 Cisco ASA 5520 和本测试中的所有其他同类系统所使用的测试环境设置都是相同的。

Cisco ASA 5520（自适应安全设备）配备了 Cisco AIP SSM-20（高级检测和防御安全服务模块）。ASA 软件的版本为 7.0.2；AIP SSM-20 的版本为 5.0.4。签名定义文件的版本为 S187。

Check Point 系统位于一台采用了一个 2.4Ghz Xeon 处理器、1GB 内存和一个 Intel Pro. 1000 MT 双端口服务器适配器的 HP DL380 G3 上。所使用的软件为 VPN-1 Pro Gateway NGX 6.0, Build 244。Smart Defense Update 的版本为 591050816。软件包括 WebIntellegence 和 SecureXL。

Fortinet 的 FortiGate 1000 的操作系统版本为 2.80, Build 456。FortiGuard AV（防病毒）定义的版本为 6.037，FortiGuard 入侵定义的版本为 2.226。

Juniper Networks 的 NetScreen-208 的操作系统版本为 5.2.0 r2.0，深入检测签名升级的版本为 364。被测系统中包含了 NetScreen 的深入分组检测软件。

我们进行了四组测试。前两组测试——防火墙性能测试——在启用所有威胁签名的情况下测量了每秒连接数和防火墙吞吐率。通常，用户可以选择性地启用签名，以便最大限度地降低发生误报的可能性。但是在我们的测试中，我们需要检查每个 IPS 的完整检测功能，测试系统在承担负载时的性能。因此，我们在这些测试中启用了全部的签名组。第三组测试是两地间 VPN 端接测试；在这项测试中，我们使用了供应商的“缺省”防火墙设置。第四组测试是 IPS 威胁防御测试，其中我们启用了所有设备的所有签名。

所有性能测试所用的流量都是通过两对 Spirent Avalanche/Reflector 2500 流量生成器（软件版本为 7.0，build 36784）产生的。来自流量生成器的负载和攻击系统——Imperfect Networks ThreatEx Appliance（v1.60b）——的输出都通过一台 Cisco 6509 Catalyst 交换机（运行的 IOS 版本为 12.2）上的同一个 VLAN 进行连接。

注：为了确保竞争产品供应商的设备在每种测试环境中都可以得到合适的、最佳的配置，我们参考了这些供应商公开发布的所有文档和资料，以及测试人员的技术经验和判断能力。Check Point、Fortinet 和 Juniper 拒绝在本次测试中为 Miercom 提供直接技术支持。

统一威胁管理

统一威胁管理（UTM）设备最近得到了广泛的使用，因为它们可以通过单个设备防御多种与安全有关的威胁。目前市场上的很多 UTM 产品都是以安全设备的形式提供的（预装硬件和软件）。但是，有些则是运行在标准的 Intel PC/服务器平台上的软件产品。

在本次对比测试中，所有被测设备都可以提供防火墙功能、IPS（入侵防御系统）功能和 VPN 网关功能。

所有供应商都为实现这些功能提供了多种设备。我们之所以在本次评测中选用这些设备，是因为它们的价位相当。基本 Check Point VPN-1 Pro（配有 WebIntelligence 和 SecureXL）——一款纯软件产品——的价格略高于其他系统，但是仍然与其他被测系统接近。

这些产品的价格与性能密切相关。所有供应商都提供了具有更高性能和处理能力的高端设备，但是价格也要高得多。本次评测的目的是比较价格接近的系统。

工作负荷和性能

我们的性能测试的流量负荷是利用 Spirent 的 Avalanche/Reflector 流量生成器（参见第二页的详细介绍）产生的。Avalanche/Reflector 系统被设置为自动生成高速的 TCP/IP 流量，它们将会被发往指定的被测 UTM 设备（一次一个，按序发送）。所生成的 TCP/IP 流量可以模拟普通用户和 Web 服务器之间的实际 HTTP 1.1 Web 流量。

对于 HTTP 流量，我们在每次测试期间建立和端接了数千个 TCP/IP 连接。每次测试大约持续两到三分钟，包含“加速”、“稳定”和“减速”三个阶段。每个被测系统上的负荷会一直增加，直到连接开始被丢弃（依照 Avalanche/Reflector 系统的报告）。这时，“最大”吞吐率会被记录下来。为了确认这一点，流量负荷会被增加到这一点之上。在某些情况下，总体吞吐率会出现幅度极小的增加；但是在其他情况下，吞吐率会下降。随着流量的进一步增加，越来越多的连接会被丢弃。

更高的吞吐率可以通过 UDP 流量实现，但是 UDP 不需要建立和中断连接，也不需要执行其他一些与 TCP 相关的逻辑，而这正是防火墙操作和性能的核心。而且，目前绝大部分的网络流量都是 TCP/IP。

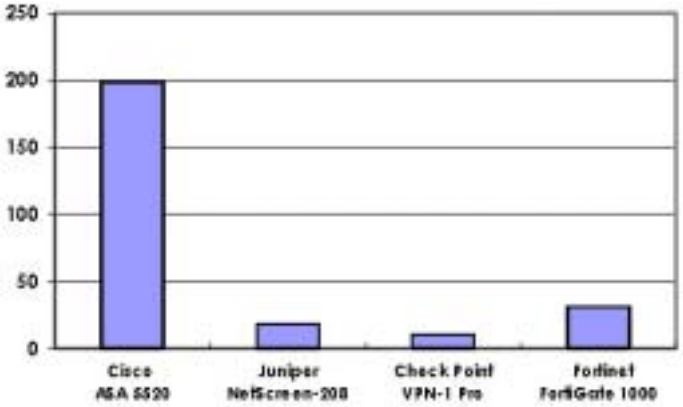
对于防火墙和 VPN 测试，测试环境都采用了尺寸为 4K 字节和 16K 字节的 HTTP 对象。它们可以模拟两种不同类型的用户：16K 字节对象模拟下载大型文件的用户，而 4K 字节对象更加接近事务处理型流量。

对于防火墙吞吐率测试、IPS 性能测试和每秒连接数测试，我们启用了供应商的所有威胁签名。对于两地间 VPN 测试，我们只使用了供应商的“缺省”防火墙设置——即产品出厂时本身携带的配置。IPS 测试专门用于评估设备检测每种威胁的能力。在进行威胁检测测试时，没有使用任何背景流量。

防火墙和 IPS 性能

为了测量防火墙性能，我们在测试中使用了尺寸分别为 4K 字节和 16K 字节的 HTTP 对象。本文的第一页显示了尺寸为 16K 字节的 HTTP 对象的测试结果。下表显示了尺寸为 4K 字节的 HTTP 对象的测试结果。这些结果表明，即使对于这些尺寸较小的事务处理型流量，在启用全部威胁签名的情况下，Cisco ASA 5520 仍然可以提供高于同类产品的吞吐率性能。

在启用所有攻击/病毒签名时的防火墙性能（Mbps），HTTP 对象的尺寸为 4K 字节

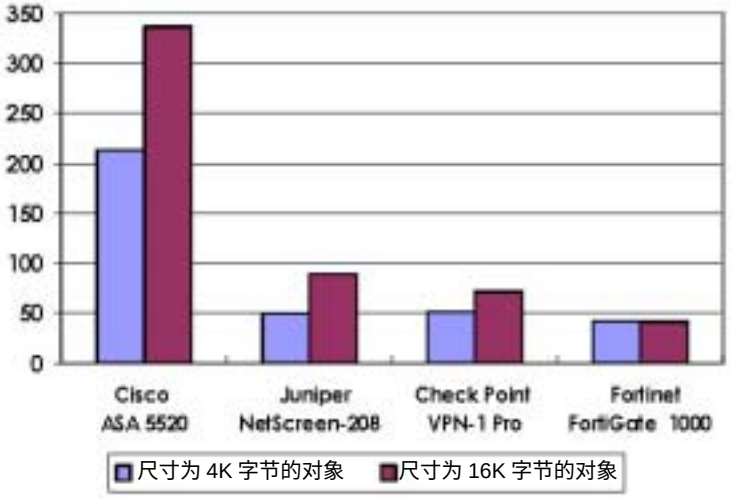


在使用尺寸为 4K 字节的 HTTP 对象并启用全部威胁签名时，Cisco ASA 5520 的吞吐率明显高于其他同类产品。

VPN 网关吞吐率性能

与防火墙性能类似，我们利用尺寸分别为 4K 字节和 16K 字节的 HTTP 对象评测了 VPN 性能。这些流量仍然是由 Spirent Avalanche/Reflector 系统生成的，可以模拟 HTTP-TCP/IP “实际”流量。VPN 测试采用了四个 VPN 隧道，模拟四个使用 3DES 加密的、安全的两地间 VPN 连接。VPN 测试只使用了供应商的缺省防火墙设置（没有启用其他的额外设置）。

VPN 4 隧道两地间性能（Mbps）



在使用尺寸分别为 4K 和 16K 字节的 HTTP 对象时，Cisco ASA 5520 在 4 隧道两地间 VPN 测试中的吞吐率明显高于其他同类产品。

IPS 测试

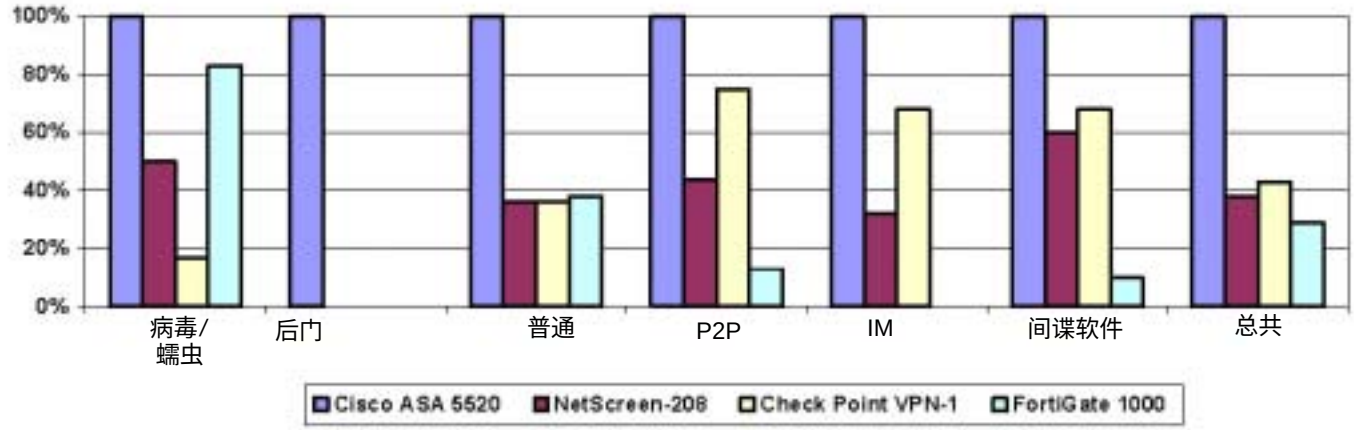
本页下方和下一页显示了 IPS 测试的结果。在一组不同种类的测试中（每个包含了一组不同的威胁），Cisco ASA 5520 可以在我们进行的所有测试中 100%地检测出所有威胁。

在进行同一组测试时，同类安全产品总是会不同程度地遗漏部分威胁。所有其他系统所检测出的威胁都没有超过所有种类中全部威胁的 45%。例如，虽然 FortiGate 1000 可以检测出 83%的病毒/蠕虫威胁，但是总共检测出的威胁在所有威胁中的比例只有 29%。Cisco ASA 5520 可以检测出所有后门威胁，而令人惊讶的是，所有其他同类系统都无法检测出我们所测试的任何一个后门威胁。

我们所测试的 IPS 功能包括基本攻击（通常包含在大部分 IPS 测试中）和额外测试，包括攻击和威胁防御、策略违反，以及对广告软件和间谍软件的检测。

我们对全部四个被测系统发出了总共 126 个威胁（测试案例）。每个测试案例都是针对每个系统单独执行的。每个系统的所有签名（或者任何其他 IPS 型设置）都被启用。测试结果利用每个系统的主管理界面查看——它们都是基于 Web 的应用，可以在检测到攻击之后立即在界面上显示。

对不同种类的威胁的检测情况



Cisco ASA 5520 可以 100%地检测出全部的威胁，而 Juniper、Check Point 和 Fortinet 的同类竞争产品只能检测出全部威胁的 30%到 40%。

我们将测试案例分为六类：

病毒/蠕虫和后门是两种最传统的攻击方式，通常可以被 IPS 所发现。我们使用的测试案例包括“zotob”、“rbot.cbq”和“netsky”病毒和蠕虫。

普通类是最大的威胁类别，包含了很多新旧攻击、针对不同类型的客户端和服务器（不同操作系统）的攻击；以及针对特定类型的网络设备的攻击。这一类的代表性威胁包括“Veritas 注册溢出”和“javaproxy.dll 堆积溢出”攻击。

P2P（点对点）和 IM（即时消息）类属于策略违反种类的一部分。最近，企业开始在工作场所限制 P2P 和 IM 活动。P2P 测试案例包括“KaZaa”、“Napster”和“Gnutella”客户端流量。IM 签名包括“AIM”、“Yahoo”和“MSN”客户端流量。这些签名通常在防火墙上并不使用，但是在需要时可以启用。

最后一类是间谍软件和广告软件。为了保护敏感数据，这些软件正在引起日益广泛的注意。测试案例包括“Gator beacon”和“Gain adware”恶意软件。

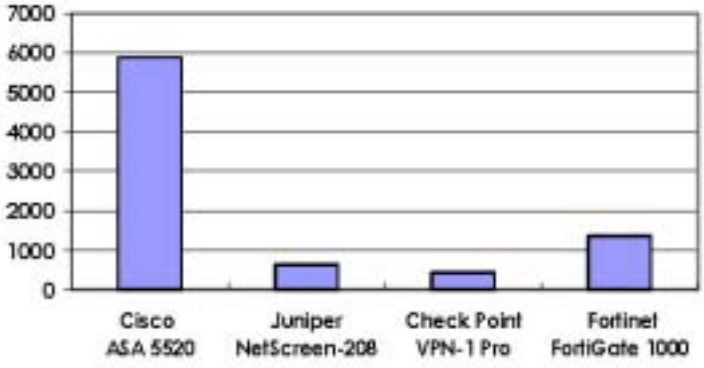
所有用于 IPS 测试的测试案例都来自于在实验室环境中进行的实际攻击。从这些实际攻击中获取的跟踪分组（被称为“pcap”文件）会被一个名为 ThreatEx（Imperfect Networks 的一款设备）的工具加以处理，再由 ThreatEx 对待测设备发动攻击。

每秒连接数

与同类安全产品相比，Cisco ASA 5520 可以在一个包含实际流量的多功能环境中表现出卓越的性能。因此，我们进行了每秒连接数或者每秒处理事务数测试。

每秒连接数的测试方式与本评测中的其他测试类似。事务处理速率由 Spirent Avalanche 工作负荷生成器提高，直到被测系统开始丢弃事务处理请求为止。每秒最大连接数会被记录下来。这是在没有丢弃事务处理请求的情况下 Spirent Avalanche 所记录的最大负荷值。所有每秒连接数测试都采用了尺寸为 64 字节的对象。下表对比了不同产品的每秒连接数性能。

每秒连接数性能



在启用所有威胁签名的情况下，Cisco ASA 5520 在一个包含实际流量的多功能环境中的每秒连接数性能是同类系统的四倍以上。

	Cisco ASA 5520	Juniper NetScreen-208	Check Point VPN-1	Fortinet FortiGate 1000
测试攻击				
病毒/蠕虫	100%	50%	17%	83%
后门	100%	0%	0%	0%
普通	100%	36%	36%	38%
P2P	100%	44%	75%	13%
IM	100%	32%	68%	0%
间谍软件	100%	60%	68%	10%
总体防御	**100%**	**38%**	**43%**	**29%**

Cisco ASA 5520 成功地、100%地检测出了所有种类的全部威胁，而价格相当的同类系统只能检测出全部威胁的 30%到 40%。

经过 Miercom 验证的性能

根据 Miercom 对这四个系统的运行状况、功能和特性的评测，Miercom 得出了下列结论：

- 在使用实际流量的多功能威胁防御（防火墙、IPS、网络防病毒）对比测试中，Cisco ASA 5520 的吞吐率比同类解决方案高六倍以上。
- 在使用实际流量时，Cisco ASA 5520 的 3DES VPN 吞吐率是同类解决方案的 3.5 倍以上。
- Cisco ASA 5520 的威胁防御能力是被测的 Check Point、NetScreen 或者 FortiGate 设备的两倍以上。Cisco ASA 5520 在每项测试中达到了 100%的检测精确度，而同类解决方案平均只能检测出 30%到 40%的威胁。
- 在使用实际流量的多功能威胁防御（防火墙、IPS、网络防病毒）对比测试中，Cisco ASA 5520 具有最高的连接建立速度，比最接近的同类产品高出了四倍以上。

供应商信息：

思科系统公司
170 West Tasman Drive San Jose, CA 95134 USA
www.cisco.com
电话：408 526-4000
800 553-NETS (6387)
传真： 408 526-4100

Check Point Software
800 Bridge Parkway
Redwood City, CA 94065
www.checkpoint.com
电话：800-429-4391
650-628-2000
传真： 650-654-4233

Fortinet
920 Stewart Drive
Sunnyvale, CA 94085 USA
www.fortinet.com
电话：408-235-7700
传真：408-235-7737

Juniper Networks
1194 North Mathilda Ave.
Sunnyvale, CA 94089 USA
www.juniper.net
电话：888-586-4737
408-745-2000
传真：408-745-2100

Miercom 产品测试服务简介

Miercom 已经在《商业通信评论》和《网络世界》等著名的网络期刊上发表了数百篇产品比较分析文章，是公认的业界领先的独立产品测试中心。Miercom 创建于 1988 年，一直致力于网络硬件和软件的比较评估，已经为 SAN 交换机、VoIP 网关和 IP PBX 等产品的测试开发出一套成熟的方法。Miercom 的专业测试服务包括竞争产品分析以及独立产品评估。提交评审的产品一般都按照“NetWORKS As Advertised™”计划进行评估。根据该计划，与网络相关的产品将在产品的可使用性和性能方面接受全面的独立评估。满足相应条件和性能水平的产品将获得“NetWORKS As Advertised™”称号以及 Miercom 实验室颁发的证书。

379 Princeton-Hightstown Road, Cranbury, NJ 08512
609-490-0200 • 传真 609-490-0610 • www.miercom.com

报告 050914