如何使用无线

IDS/IPS

如何使用无线 IDS/IPS

本专题可以帮助理解在无线网络中，无线入侵检测/防御系统（WIDS/WIPS）的价值，及时您所在的公司不支持无线局域网。此外，本专题还将介绍如何为公司环境选择合适的 WIDS，以及如何防御无线拒绝服务攻击。

无线拒绝服务攻击

尽管最近 802.11 的安全性提高了，但是无线局域网仍然很容易受到拒绝服务攻击的威胁。尽管可能不能够阻止拒绝服务攻击，但是无线入侵检测系统（WIDS）可以帮助检测到拒绝服务攻击什么时候发生及其来源，这样就可以把入侵者就地正法——或者至少把他吓走。本节中针对如何识别对无线局域网的拒绝服务攻击，并对其做出反应，提供了切实可行的意见。

- ❖ 作战无线拒绝服务攻击

无线网络中遏制流氓攻击

无线网络监测系统正迅速地从只进行检测转向了检测和预防双管齐下。特别是，许多系统现在通过阻止无线访问和有线访问，提供了“遏制”未经授权的流氓设备的功能。本文中，TechTarget 中国的特约专家探讨了流氓遏制方法的工作原理、其潜在的负面影响，以及在使用之前，网络管理员应该考虑的问题。

- ❖ 阻止还是不阻止：遏制流氓攻击的方法

无线入侵检测系统的分类

无线入侵检测系统（WIDS）可以监测 802.11 主要信息流，并将其发送到中央服务器，检测攻击、未经授权的使用和违反策略的行为。覆盖式无线入侵检测系统（比如，

AirDefense、AirMagnet、AirTight、Network Chemistry），使用一种专用的服务器和传感器进行监测。嵌入式无线入侵检测系统（比如，Aruba、Cisco、Trapeze）使用接入点在其空余时间监测无线局域网。本节对这些方法进行了比较，这样就可以选择最合适网络需求和安全需求的方法……

- 覆盖式 WIDS 传感器 VS 嵌入式 WIDS 传感器

无线入侵检测系统的使用

无线入侵检测：从这个名字想到的是安全。但是许多无线入侵检测系统（WINDS）产品也可以用于检测 WLAN 的性能，为故障排除、微调和使用规划提供有价值的见解。你如何利用 WIDS 从无线局域网（WLAN）中获得更多？

- 使用 WIDS 监测 WLAN 的性能

作战无线拒绝服务攻击

尽管最近 802.11 的安全性提高了，但是无线局域网仍然很容易受到拒绝服务攻击的威胁。尽管可能不能够阻止拒绝服务攻击，但是无线入侵检测系统（WIDS）可以帮助检测到拒绝服务攻击什么时候发生及其来源，这样就可以把入侵者就地正法——或者至少把他吓走。本文中，Techtarget 中国的特约专家针对如何识别对无线局域网的拒绝服务攻击，并对其做出反应，提供了切实可行的意见。

拥挤的天空

每个无线网络都会有意无意地受到无线电波的干扰。由于 802.11b/g 网络使用拥挤的 2.4 GHz 频段，因此受到其它无线电设备的干扰是常有的事，包括蓝牙、无线电话、微波炉和周边的无线局域网。802.11a 网络使用 5 GHz 频段，这个频段更大，更易于使用，这样就不容易受到干扰。然而，任何使用无线局域网来完成关键应用任务的公司都应该准备好应对可能发生的无线电波干扰。

抗干扰很困难。这些频带是没有限制的，每个人都拥有相同的权限来使用它们（受限于有关权利限制的监管规则，等等）。虽然一些建筑材料和涂料提供了射频屏蔽，但是对于现有设施可能不切实际，会干扰到你自己无线局域网的操作。因此，对于大多数无线局域网管理员而言，避免干扰是一项战略性的选择：

一些设备可以在你的无线局域网所使用的频带和频道中传输 802.11，使用无线入侵检测系统（WIDS）来检测这些看起来很新的设备。

使用 WIDS 警报来标记超载的信道（有过多的接入点或者点对点模式以特定的频率运行），或者标记过量的错误和转传输率（可能是非 802.11 干扰）。

使用无线网络入侵侦测系统在平面图上绘制一个近似的位置，进而追捕到干扰源。然后使用一个移动工具（stumbler 或者无线局域网分析仪）来查找这个区域并隔离该设备的地址。

至于非 802.11 干扰源，使用一个频谱分析仪来监测传输，并且指纹鉴定你应当寻找的设备类型。

如果你不能消除罪魁祸首，重新配置接入点，使用不繁忙的信道。在干扰消除后，一些无线局域网交换器甚至可以自动分配信道。考虑将 802.11a 转至问题反复出现的地方，比如人口密集，租户众多的办公楼。

拒绝服务攻击发生

大多数无线局域网干扰是偶然发生的。当攻击者可以使用射频干扰，比如一个高功率的射频信号发生器，有许多便宜的方法可以有意地使用拒绝服务攻击你的无线局域网。比如：

- 802.11 的控制桢可以用来“清空”某个信道，这样没有其它任何工作站可以传输。进入这个持续的传输模式被称为昆士兰州拒绝服务攻击。
- 802.11 的认证桢可以用于与某个单独的工作站断开连接，或者是每个与特定接入点相关的工作站。源源不断地发送这些伪造的框架，被人们称为 Deauth Flood。
- 在接入点的关联表中创建条目，这样 802.11 的协助桢就消耗了接入点资源。使用来自随机站点 MAC 地址的协助桢来淹没接入点，这样可以使得接入点太繁忙，以至于无法为真正的用户服务。
- 使用伪造的 802.1X 信息包，可以启动类似的攻击——比如，802.1X EAP Logoff Flood、EAP Start Flood、和 EAP-of-Death 攻击。

这些以及许多其它无线拒绝服务攻击很可能发生，由于只有 802.11 数据桢携带了完整的校验代码，这些代码是用于识别伪造信息的。使用成品的无线网卡和随时可用的共享

软件或者开源工具，比如 airjack 和 void11，可以启动这些攻击。攻击者只需要足够接近你的无线局域网，便可以捕获一些信息流，进而查明受害者。

不幸的是，大多数无线网络入侵侦测系统可以认出这些拒绝服务攻击的签名。一个无线网络入侵侦测系统可以警告你发生了 802.11 洪流或者 802.1X 洪流，以配置好的速率阀值为基础。无线网络入侵侦测系统也可以帮助你为你的无线局域网建立一个性能基准，这样你可以调整攻击阀值。比如，当某个特定的接入点每秒接收到的协助桢数目多于 N 时，N 取决于网络正常用户的行为时，就会产生一个协助桢警告。

此外，无线网络入侵侦测系统可以帮助你侦查出涌现出的攻击模式。比如，一个攻击者可能优先使用 Deauth Flood，而不是 Evil Twin attack。无线网络入侵侦测系统可以帮助你将这两个攻击联系起来。攻击者可能会从一个接入点转向另一个接入点，从不同的 MAC 地址中运行类似的攻击。无线网络入侵侦测系统可以帮助你侦查到这种行为，生成一个升级的警报，对正在进行的攻击引起更快的注意力。没有无线网络入侵侦测系统，一些拒绝服务攻击可能会记下间歇性运行问题。无线网络侦测系统使你有能力回过头察看一下在无线局域网错误报告的时间前后是否发生了可疑活动或者已知的活动。

为了立即调查远程站点上的攻击，将无线网络侦测系统传感器放置到捕获的模式中。通过捕获正在发生的攻击，你可以确定受到影响的系统，并收集证据以支持规律和法案。你可能还希望将涉及到以往攻击的 MAC 地址置于一个“观察名单”中，这样如果当攻击者返回消息时，高度优先的警报可以及时行动。

至于干扰，无线网络入侵侦测系统可以帮助你找到拒绝服务攻击源的地址。然而，因为恶意攻击者可能无法坚持很久，因此，除非快速构建，否则现场搜索可以证明是徒劳的。此外，事先决定负责搜索工作的员工是否应当设法确定罪魁祸首、发出警报、请求安全性等等。切记，攻击者可能正在某个公共区域操作，比如附近的停车场，在那里你真的没有任何权限。

结论

这些措施有助于发现和诊断到无线电波干扰和拒绝服务攻击，并对其做出应对。但是，这些步骤中没有一个可以完全隔离你的无线局域网。如果无线网络对你的企业是至关重要的，那么就创建一个后备计划。有线网络通常采用高可用性措施，比如链接的多样性、多余的路由器、以及不间断的供电。将这一思想应用到你的无线局域网中，并且考虑有线网络替代品应该应用于哪里，以及如何应用。

（作者：Lisa Phifer　译者：Tina 来源：TechTarget 中国）

阻止还是不阻止：遏制流氓攻击的方法

无线网络监测系统正迅速地从只进行检测转向了检测和预防双管齐下。特别是，许多系统现在通过阻止无线访问和有线访问，提供了“遏制”未经授权的流氓设备的功能。本文中，TechTarget 中国的特约专家探讨了流氓遏制方法的工作原理、其潜在的负面影响，以及在使用之前，网络管理员应该考虑的问题。

有线遏制

流氓攻击可能是某个雇员为了方便起见而安装的未经授权的接入点（AP）、可能是某个根植于你办公室内部的接入点，进而创建一个无线后门，或者是一个软接入点（SoftAP），可以在你的有线局域网内架设攻击信息流。在每一种情况下，流氓攻击可以物理连接到你的企业网络上。禁用上游以太网的交换器端口就可以立即打破这一连接。

首先，通过扫描有线局域网，找到携带有流氓 MAC 地址的设备，进而确定目标交换器端口。或者与流氓接入点联合，然后使用跟踪路由建立流氓返回你网络的路径。你的无线网络入侵侦测系统（WIDS）会支持其中一种方法或者两种“链接检查”方法，这些方法都是从流氓附近的传感器上启动的。

如果可以识别到流氓使用的交换器，你的无线网络入侵侦测系统就能够发送该交换器的简单网络管理协议（SNMP）请求，进而中止那个端口。或者，无线网络入侵侦测系统可以向网络管理系统发送这样的请求——比如，AirDefense 可以向 Cisco 无线域名服务（WLSE）发送有线阻止请求。

有线遏制可能会需要一些预先的配置，比如在你的无线网络入侵侦测系统中添加管理子网和简单网络管理协议（SNMP）的查询密码，这样就可以发现交换器、或者在搜索列表中添加特定的交换器。在一些情况下，交换器并不由简单网络管理协议（SNMP）管理，或

者可能处于子网中，无法从无线网络入侵侦测系统的传感器和服务器中达到。此外，甚至有线遏制在技术上是可行的，但是由于组织策略，这也是不允许的。

无线遏制

凡是有线遏制是不可能的、不切实际的、不合适的情况下，考虑使用无线遏制。无线遏制不仅仅可以应用到流氓接入点，也可以应用到与你自己接入点相连接的流氓工作站，以及与点对点客户端连接的流氓工作站。无线遏制的方法有很大的不同。比如：

最差的方法是干扰——以指定的频率产生射频噪声，进而防止流氓（和其它任何人）有效地交流。干扰的破坏性很强，并且会违反频谱使用的规定，所以这种方法应该是最后考虑的方法。

最常见的方法是向流氓的 MAC 地址或者接入点的光笔地址发送一串稳定的解除验证信息包。比如，无线网络入侵侦测系统可能会对使用流氓接入点的每个人解除验证，或者会选择性地仅对那些使用合法接入点的流氓工作站解除验证。谨慎使用广播解除验证，以免意外地攻击到某个邻居的新接入点。虽然选择性的解除验证破坏性要小一些，但是一些使用 MAC 欺骗或者漫游的用户会将其规避到另一个合法接入点/信道。

网络化学公司的 UltraShield 方法使用蜜罐和焦油纸算法，来保持流氓处于忙碌状态，这样它就不会尝试与其它任何人通信。比如，某个流氓的点对点模式会被无线网络入侵侦测系统的传感器吸引，这个传感器假装成为一个同样的点对点模式。或者传感器会假装为某个接入点，保持流氓客户端与之保持联系，这样他们就无法漫游到真正的接入点。

与有线遏制方法不同，无线遏制通常不会要求与其它网络设备或服务协调。但是，无线遏制会消耗带宽和无线入侵侦测系统的资源。一些传感器可以共享时间，这样只不过缩短了监测间隔，而其它传感器在用于遏制的时候不能扫描信道。虽然一些传感器可以立即阻止几个流氓，但是，一个传感器尝试阻止流氓的个数越多，遏制（和无线入侵侦测系统监测）的效率会变得越低。

需要考虑的因素

遏制是一把双刃剑。它虽然对阻止干扰非常重要，但是流氓也可以对它进行研究，进而消除遏制。向远程站点派遣工作人员需要花费一些时间：流氓在仅仅几分钟内就可以造成破坏，然后继续前进。但是，不欠当的遏制行动也可以阻碍你自己的企业生产力，对你的邻居造成金融危害，或者承担法律责任。

因此，在使用这些遏制方法时，有必要了解遏制的性能。在单独测试无线局域网时，用遏制性能进行实验，直到你了解了有意的影响和意想不到的后果。当你考虑选择无线局域网产品时，首先至少要适用于遏制的方法。只有经过仔细分析和管理批准之后，才能实现自动遏制。

指定一个策略，规定何时使用遏制，以及授权哪个人做出遏制的决定。比如，你可能会要求进行人力调查，除了最优先的流氓事件，比如选择那些负责关键任务系统或者限制领域的人员。或者在保留更积极的升级方法的同时，你可以决定自动操作保护性的遏制情节。比如，停用你自己的交换器端口，或者从你自己的接入点中，有选择地对流氓解除验证，这些都视为在你的权限之内，并且不可能不经意间影响到你的邻居。

此外，确定什么时候应该取消遏制措施，或者使其成为永久的遏制措施。比如，无线遏制通常是一种停止损失的策略，适合短期实施，或者直到流氓变得气馁，转向另一个攻击目标。但是，无线入侵侦测防御系统也可以使用遏制来连续执行授权的使用政策——比如，通过阻止合法的站点保持与未经授权的接入点保持连接。

切记，双刃剑在熟练者的手里也可以是一个强有力的工具。在反击流氓的战争中，遏制政策是极其宝贵的，只要你用应有的尊重和细心来对待这些“反击”能力。

(作者：Lisa Phifer　译者：Tina 来源：TechTarget 中国)

覆盖式 WIDS 传感器 VS 嵌入式 WIDS 传感器

无线入侵检测系统（WIDS）可以监测 802.11 主要信息流，并将其发送到中央服务器，检测攻击、未经授权的使用和违反策略的行为。覆盖式无线入侵检测系统（比如，AirDefense、AirMagnet、AirTight、Network Chemistry），使用一种专用的服务器和传感器进行监测。嵌入式无线入侵检测系统（比如，Aruba、Cisco、Trapeze）使用接入点在其空余时间监测无线局域网。本节对这些方法进行了比较，这样就可以选择最合适网络需求和安全需求的方法。

成本

原则上，使用接入点监控无线入侵检测系统，可以通过充分利用现有的硬件和以太网交换器端口，运行 Cat5 电缆，降低电力消耗减少安装成本。由于你的无线局域网控制器或者管理器可以作为嵌入式无线入侵检测系统服务器，也就不需要另外一个平台来运行覆盖式无线入侵检测系统的服务器软件。

但是，在实际中，每个系统只能做这么多。你可能需要安装更多的接入点，以承担无线入侵检测系统的负担，或者完全覆盖易受攻击的区域。安置在无线入侵检测系统服务器中的 I/O 和 CPU 的负载是相当繁重的，这样无线局域网管理器平台可能还需要按比例相应地增加，进而立即进行这两项工作。

此外，一些传感器使用双 Power-over-Ethernet 端口来插在交换器和接入点之间，这样就不需要新的电缆了。除了专门的传感器外，大部分覆盖式无线入侵检测系统可以使用所选择的接入点（比如，Aironet）来进行监测、牺牲一些功能。另一方面，大多数嵌入式无线入侵检测系统允许将接入点配置为全职监测器。这样就无需因为标签而不安：确定你需要多少监控设备，然后比较安装的单位成本。

覆盖范围

对于使用无线入侵检测系统来执行“没有无线”策略的公司而言，覆盖式无线入侵检测系统是唯一真正的选择——现有的接入点都无法使用了。其它安装了无线局域网的公司应该认真审查一下其无线入侵检测系统的覆盖需求。

你的无线入侵检测系统脚本应该略大于无线局域网脚本。攻击者可能潜伏在合法接入点范围之外，吸引用户与之联系或者启动攻击，你用其它方式是无法看到这些攻击的。只有专门的传感器或者仅用于监控的接入点可以添加到扩大的空间覆盖面之中。

在这些频段中，接入点使用特定的频段和分配好的信道。无线入侵检测系统始终可以扫描这些信道之外的范围，这是由于未经授权的接入点和点对点站点更可能占用未被使用的信道。成品 802.11b/g 的接入点不能监测 802.11a 信道，以及 2.4GHz 频段中的频率，这些频率仅用于其它地方。特制的无线入侵检测系统传感器通常可以扫描更多的频率，尽管产品的性能各不相同。

注意广度

有了嵌入式无线入侵检测系统，接入点花费了其部分时间为无线网络客户服务。其余时间在监测信道，或者扫描其它信道。有了覆盖式无线入侵检测系统，监测信息流成为传感器的主要任务，尽管这可能在其它无线入侵检测系统的任务上花费一些时间，比如阻止流氓攻击。

每个无线入侵检测系统可能会错过一些信息流——入侵者可能很遥远，而信号可能太微弱，传输可能太短暂。实际上，任何设备在 RFMON 模式下扫描信道，就是连续地在列表中每条信道中采取信息流样本。目标是监听很长的时间 ，通常是足够长，进而有足够的机会发现攻击、违反策略、以及流氓设备。

在繁忙的无线局域网中，全职的传感器显然可以监听到更多的信息流。兼职的接入点往往更容易漏掉持续时间短的攻击，比如相对静止的流氓设备。兼职的接入点也很少有空余时间运行其它无线入侵检测系统的任务——比如，全职的传感器可能可以更坚持地阻止更多流氓，并且效率更高。

然而，在容易使用的无线局域网中，全职的传感器不能够很好地利用备件周期，而接入点却有足够的动力将两项工作都做好。为了平衡成本和风险，你可以在小型的分支机构中，将主要设施的全职传感器与兼职的接入点混合起来，增加更多的全职传感器，因为显而易见，需要这些传感器来满足安全需求。对无线局域网的影响。

接入点的时间分片不仅仅会影响无线入侵检测系统的效率——它也会影响到无线局域网的性能。但是这个影响很难量化。潜在影响取决于接入点的载荷、客户密度、应用程序的信息流、扫描列表/持续时间，以及其它无线入侵检测系统的任务。比如，阿鲁巴岛的文件报告称：多个厂商的实验室测试最近发现，当针对客户服务和关闭信道监测使用扫描接入点时，如果要求接入点花费大量时间关闭信道，那么吞吐量很可能会下降 16%。

专用的传感器和仅用于监控的接入点不会对无线局域网的性能产生不利影响。实际上，由于他们收集了更全面的信息，当遇到无线局域网的故障排除性能问题时，这些可能更有帮助。

另一方面，当攻击强劲袭来时——接入点失效，客户的请求突然中断——不能暂时授予专用的传感器活动的职责，来增强陷入困境的无线局域网的性能。从安全角度来讲，保持你的监测基础设施完整无缺是非常有用的，但是从业务角度来看，服务的可用性通常是最优先考虑的问题。

功能

无线入侵检测系统具备商业接入点所没有的功能，特制的传感器可以支持这些功能。扫描“关闭的”信道就是这些功能之一。特制的传感器甚至能够扫描非 802.11 信息流，进而用指纹识别射频干扰源，比如微波炉和蓝牙。

随着市场越来越成熟，覆盖式无线入侵检测系统对特制的传感器提出了更多的要求。特别是对那些用于执行新的欺诈防御策略的传感器。任何接入点可以产生解除验证信息包或者取消信息包，但是现在一些传感器可以用作无线客户端。比如，某个传感器可能与流氓接入点结合，进而追溯到网络连接。传感器可能会设法吸引某个流氓点对点模式，使其

保持忙碌，而反应器设法找到并消除这个设备。由于特制的传感器不能具备接入点的功能，因此也存在较低的风险，即利用固件漏洞，在有线网络中创建一个无线后门。

虽然，增加兼职接入点可以提供额外的无线入侵检测系统性能，但是，实际上，与新的无线入侵检测系统相比，应该优先考虑开发新的无线局域网性能。此外，不论接入点的能力有多大，兼职的接入点不适用于执行无线入侵检测系统的任务，这些任务要求持续的活动（比如，为特定的信道或设备创建信息流捕获功能，不断地对大量的流氓解除验证）。

关于任何类型的覆盖式 WIDS，另一个关注点是控制台和数据库的扩散，并且将它们结合起来，以便于协调和避免重复。

嵌入式的无线入侵检测系统更可能提供单一的、集成的管理界面，这样你既可以配置你的无线局域网，也可以监测无线局域网。嵌入式无线入侵检测系统拥有内置的标准，这些标准可以区分合法的接入点和流氓接入点，而必须采用合法接入点的列表，才能对覆盖式无线入侵检测系统进行配置。当嵌入式无线入侵检测系统决定终止某个流氓对有线网络的访问时，无论如何，这个无线局域网控制器可能会直接负责管理这个端口（比如，Cisco WLSE）。而许多覆盖式无线入侵检测系统可以直接向以太网交换器发送简单网络管理协议（SNMP）请求，将交换器的配置请求直接发送到所负责的管理系统，这种方式可能更为可取。

随着产品一体化的发展，这种差别会越来越不明显。比如，虽然，Trapeze 在其无线局域网移动系统（一种嵌入式无线入侵检测系统）中包括了无线入侵检测系统的“核心”性能，但是，也已经与 AirDefense（一种覆盖式无线入侵检测系统）结合起来。Colubris 网络公司最近将 AirTight 网络公司的无线入侵检测系统技术融入到其自己的 InCharge 射频管理器中。

职责分工

最后，除了方法和产品的不同，还要考虑组织的影响和策略要求。在一些公司，网络运作和安全法规遵从由不同的组织机构负责。选择无线局域网组件是以其产生网络的能力为基础的，而不是以安全和服务为基础。那些负责安全监测的组织可能无权使用无线入侵检测系统的现有接入点。实际上，一些公司明确要求安全审计人员和工具进行职责分工。

结论

选择一种无线入侵检测系统，需要考虑许多因素——嵌入式与覆盖式（虽然很重要）只是其中一个考虑因素。我们希望本文可以帮助你更好地理解这个考虑因素，这样你就可以使专用传感器和接入点的监测功能与贵公司的要求相符合。

（作者：Lisa Phifer　译者：Tina 来源：TechTarget 中国）

使用 WIDS 监测 WLAN 性能

无线入侵检测：从这个名字想到的是安全。但是许多无线入侵检测系统（WIDS）产品也可以用于检测 WLAN 的性能，为故障排除、微调和使用规划提供有价值的见解。你如何利用 WIDS 从无线局域网（WLAN）中获得更多？

无线局域网 WLAN 性能分析及其工具

许多情况都需要分析 WLAN 的性能，从最初的设计和新安装的设备的调试，到优化覆盖面和规划扩展。在这一生命周期中，许多工具都是有用的，包括站点调查工具、射频设计仪、频谱分析仪和无线流量分析仪。

无线流量分析仪是非常必要的，可以捕获 802.11 信息流并对其进行编码，然后重新将信息包装配到联合和射频设备关系之中。分析仪有助于在有限的时间内，理解 WLAN 特定地址中正在发生的情况。但是有时也需要退回去，查看 WLAN 信息流的更多的情况，收集更长的时间内的信息。而 WIDS 可以提供帮助。

WIDS 可以监测整个 WLAN，将由分布式传感器捕获的主要信息流转发到中央服务器。收集这些信息流，将其联系起来，分析安全事故。WIDS 会显示由此产生的警报，并将其转发到另一个系统，或者记录在数据库中，供将来参考。当然，这些信息流也可以用于监测 WLAN 的性能。

性能警报

虽然 WIDS 的性能分析与警报功能不同，但是这里有一个性能警报样本，这是 WIDS 能够监测到的：

- 站点的接入点超载
- 接入点或者信息流的信道超载

- 管理费用过多
- 客户端发送/接收的恒定信息流
- 接入点配置不合理或者不兼容
- 同步 PCF/DCF（集中式协调功能/分布式协调功能）操作
- 接入点的电能解除 DTIM 冲突
- 802.11g 接入点无法使用 802.11b 接入点附近的保护
- 802.11g 接入点提供了不恰当的短期插槽
- 接入点提供了非标准的数据率
- 过多的重试或者 CRC 错误
- 过度漫游或者再连接
- 过度低速传输
- 过度分散
- 侦测到隐藏的站点
- 侦测到雷达干扰
- 信道噪声级过高

一些警报表明可能发生了配置错误（比如，保护），而其它警报指出了会降低性能的潜在的执行错误（比如，DTIM 冲突）。关于超载或者射频干扰方面的警报可以通过扩展 WLAN 或者重新分配信道得以解决。以阀值为基础的警报可能需要使用基线测量法调试，它可以反映出什么对 WLAN 而言是“正常的”（比如，每个接入点工作站的预计数量、典型的信道使用方法）。你会希望停用任何与 WLAN 无关的 WIDS 的警报（比如，如果不使用 802.11b，就可以停止 802.11g 保护）。

性能故障排除

虽然，扫描模式下的 WIDS 可以监测到性能问题，但是诊断却需要一个更为全面的信息流样本。为了推动这一项工作，许多 WIDS 可以使用远程传感器，创建信息流捕获文件。通常情况下，可以将结果输入到无线信息流分析仪中仔细审查。

故障排除通常需要活跃的工具。比如，AirMagnet 企业版可以从 WIDS 的控制台研究到远程传感器，这样可以联系到某个目标接入点，并且运行网络诊断工具，比如 ping 和跟踪路由器。你也可以查看近实时信道的性能图表，这些图表中显示了信号的强度、噪声、CRC 错误、重试、使用等情况，就好像在传感器的地址中运行 AirMagnet Laptop 所得到的信息一样。

虽然从中央地址进行调查可以节省时间，但是，一些性能问题仍然需要在线调查，使用移动的无线分析仪来调查。从你所学的知识开始，将 WIDS 和无线分析仪结合起来可以加速调查进程。比如，Network Chemistry 公司的移动式 RFprotect 可以与分布式 RFprotect 分享信息，这样移动式 RFprotect 现场获得的资料可以反馈到分布式 RFprotect 的数据库中，为特定的地址创建统一的“噪声规划”。

你的最终目标并不是仅仅找到潜在的性能问题，而是修复它们。为此，WIDS 会为某个特定的警报或者测试结果提供修复措施。比如，AirTight 企业版包括了一个以知识为基础的故障排除向导，帮助解决客户端的性能问题。

性能报告

WIDS 收集的信息也可以创建历史数据库，可以用于健康报告和容量规划。WIDS 的性能报告包含了带有性能警报的前 10 个接入点、过去制定的活跃站点的数量、频谱的使用情况和性能总结、以及性能报告在类型、地址、及设备方面的趋势。

举例来说，前 10 份报告可能会请你注意陷入困境的接入点。该接入点的性能警报会趋向于显示这些问题是否是新出现的、是否是间歇性的、是否还在增加。研究最近和过去的警报也会显示出诸如利用率和错误阀值是否保持稳定等问题。检查同一位置其它接入点的警报可能有助于区分这个位置中单个失效的设备和影响到每个接入点的环境条件。另一方面，对跨多个站点的类似接入点进行比较，可以发现由特定产品、固件版本、或者配置选项导致的性能问题。

结论

WIDS 设计主要用于监测，并且对监测到的事件做出响应。当谈到性能管理时，虽然，WIDS 不能够取代便捷的无线流量分析仪，但是 WIDS 可以补充移动分析仪的不足，它对性能问题提供了更广泛的状况，突出重点。那些负责大型企业的 WLAN 工作者更喜欢分布式网络流量分析平台，比如 WildPackets Omni 或者 Network Instruments Observer Expert。这类产品可以对各种网络的信息流进行监测（包括 WLAN），并且还提供应用层协议分析和报告。

（作者：Lisa Phifer　译者：Tina 来源：TechTarget 中国）