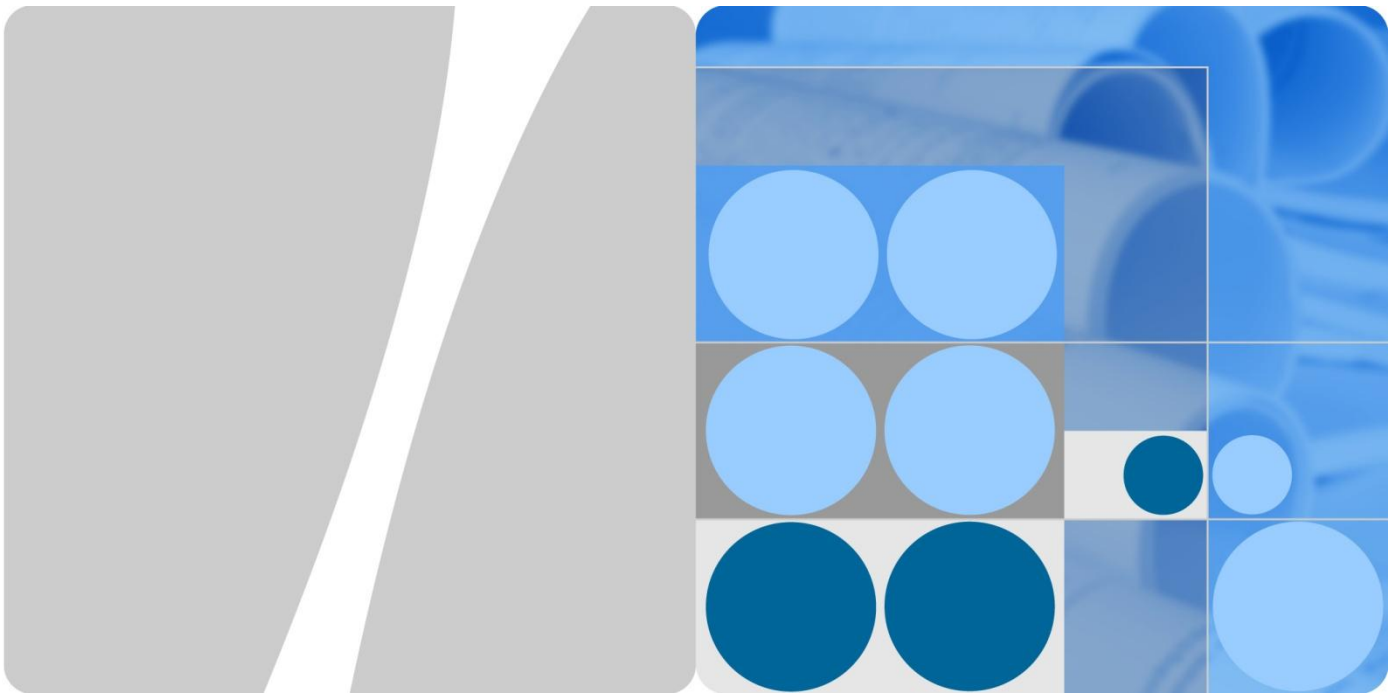


华为 AR G3 企业路由器

IPS技术白皮书

文档版本 V1.0

发布日期 2014.2.14

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://enterprise.huawei.com/cn/

目 录

IPS (Intrusion Prevention System) 是AR产品安全特性中一个非常重要的功能，提供一种主动的、实时的防护，对网络深层攻击行为进行准确的分析判断，阻止漏洞攻击的恶意流量，为企业网络提供“虚拟补丁”；支持检测SQL注入、XSS攻击、网页挂马等WEB安全威胁，为企业提供WEB安全的防护能力；支持检测网络中的木马、蠕虫、僵尸网络、间谍软件等恶意代码，为企业提供恶意流量净化及反间谍能力。

1 功能介绍

IPS主要通过匹配威胁的特征字段，来识别各种应用层攻击。基于特征的威胁检测主要针对漏洞攻击防护、WEB安全防护、恶意代码防护这几种主要场景：

（1）漏洞攻击防护

漏洞指系统中的安全缺陷，计算机硬件、软件、协议的具体实现或系统安全策略上存在的缺陷都可以称为漏洞（vulnerability），设备资产上存在漏洞攻击的威胁，则会导致入侵者访问未授权的文件、获取私密信息甚至执行任意程序。

零日漏洞是指在系统商在知晓并发布相关补丁前就被掌握或者公开的漏洞信息。该类漏洞信息还没有大范围传播开、大部分用户没有获得相关的漏洞信息、厂商也没有发布漏洞补丁，黑客有可能利用这些有利条件来达到攻击的目的。

（2）WEB安全防护

Web服务面临许多与Web应用程序面临的同样的安全漏洞，如SQL注入和XSS的攻击等。但是，与传统的Web页界面不同，Web服务程序更加开放，不仅存在大量攻击针对桌面客户端软件，还经常连接到企业核心的应用程序和数据。这就显著提高了它的风险并且使Web

服务成为一个非常吸引人的目标。Web服务通常在HTTP网络上应用，不用重新配置防火墙就可以允许交叉网站的通讯。这对于使用老式防火墙的网络来说是有问题的，因为传统的防火墙不能分析通过HTTP网络传输的Web服务通讯。

攻击者通过HTTP/HTTPS的应用绕过防火墙，并通过HTML躲避技术攻击WEB安全服务器。大量的不安全桌面应用程序被开发出来，攻击者针对桌面客户端的ActiveX控件和浏览器插件/组件/JavaScript的攻击也越来越多，安全的防护重心从服务端防护逐渐转移到客户端防护上。脚本编码的加密与混淆等处理方法，使用WEB安全的防护越来越难

用网站的安全漏洞，尤其是 WEB 应用程序漏洞：如 SQL 注入等，黑客能够得到 Web 服务器的控制权限，随意篡改网页内容或窃取重要内部数据，更为严重的则是在网页中植入恶意代码，通过“网页挂马”感染更多的客户端用户。通过这一行为，黑客可以控制网站的访问者甚至包括网站本单位的人员的计算机，从而实现盗取银行帐号、内部机密信息等各种不可告人的目的。由于网页木马制作的简单性和网络漏洞存在的必然性，通过网站漏洞进行网页挂马已经成为当前最流行的网站攻击方法和最受黑客青睐的木马散播方式。

（3）恶意代码防护

僵尸网络(Botnet)，是指采用一种或多种传播手段，将大量主机感染bot程序(僵尸程序)，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络。

1.Bot：Robet的缩写，可以自动地执行预定义的功能、可以被预定义的命令控制，Bot不一定是恶意的，但在僵尸网络中的Bot都是设计用来完成恶意功能的。

2.Zombie：被安装了恶意Bot或其它可以恶意远程控制程序的计算机（僵尸计算机）。

3.Command & Control Server：可以形象地将IRC Bot 连接的IRC 服务器称为命令＆控制服务器，简写为C&CS ，因为控制者通过该服务器发送命令，进行控制。

4.Botnet：由安装了恶意Bot的僵尸计算机所组成的可被攻击者控制的网络。

近年来, 由于巨大经济利益的驱动, 僵尸网络得到迅速发展,，僵尸网络的结构更加复杂，控制手段更加丰富多样，隐蔽性更强。僵尸网络的检测和控制技术面临巨大的挑战。

木马（Trojan）是一种由攻击者秘密安装在受害者计算机上的窃听及控制程序。特洛伊木马程序是一种程序，它能提供一些有用的，或是仅仅令人感兴趣的功能。但是它还有用户所不知道其他的功能，例如在你不了解的情况下拷贝文件或窃取你的密码。计算机一旦被植入木马，其重要文件和信息不仅会被窃取，用户的一切操作行为也都会被密切监视，而且还会被攻击者远程操控实施对周围其他计算机的攻击。

蠕虫是无须计算机使用者干预即可运行的独立程序，它通过不停的获得网络中存在漏洞的计算机上的部分或全部控制权来进行传播。蠕虫与病毒的最大不同在于它不需要人为干预，且能够自主不断地复制和传播。

间谍软件是一种能够在用户不知情的情况下，在其电脑上安装后门、收集用户信息的软件。它能够削弱用户对其使用经验、隐私和系统安全的物质控制能力；使用用户的系统资源，包括安装在他们电脑上的程序；或者搜集、使用、并散播用户的个人信息或敏感信息。

IPS主要采用的是误用检测模型，将入侵特征以知识库的形式进行固化，通过将网络数据流与知识库中的特征进行匹配，从而发现威胁。这种方式的主要优点是检测效率高、误报率低，检测代价小；而因为该方法依赖积累特征库，因此需要长期维护特征库，对于一些未知威胁效果不好。

对于漏洞的攻击防护，往往进行漏洞的原理分析，提取公共签名特征，然后进行模式匹配，从而检测出漏洞攻击。对于WEB安全防护而言，除了常规的系统漏洞，更重要的是HTTP应用的安全防护，需要做一些例如URL的防躲避，HTML的防混淆等，然后再进行模式匹配，从而检测出HTTP应用的攻击。对于僵尸网络、木马、蠕虫，则是通过分析，提取通信的网络特征，然后利用该特征进行角色识别，从而发现威胁。

2 关键技术

2.1 协议识别技术

为了能够对应用层数据进行入侵检测、病毒检测以及内容过滤，首先需要识别应用层协议类型，然后才能针对不同的协议给出相应的具体处理方法。

AR的IPS引入DPI识别技术，通过动态分析网络报文中包含的协议特征，可自动准确识别运行于非标端口下的应用层协议。

2.2 高精度协议解码规范

IPS通过深度应用识别之后，还需进行协议解码，对威胁作深层检测，才能有效的精确识别攻击。协议解码规范是深度检测必不可少的环节，可以减少特征匹配的计算量、识别及处理反躲避的技术、协议异常攻击的检测，提高威胁检测的精度。

AR支持近百种的协议变量字段的详细解码，包含常见协议的变量字段。详细解码的协议变量字段是建立对网络攻击研究的基础上，对特征库中需要的协议信息进行分析后形成的。

通过协议解码的处理，IPS能防护协议异常的攻击检测。黑客通常利用网络上很多应用服务器在设计的不完善，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。IPS支持对多种协议进行异常检测，通过深度协议解码，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，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，IMAP，MSRPC，NETBIOS，

SMB，TDS、TNS，TELNET，IRC，DNS等，覆盖常用的40多种协议。

2.3 基于文件的检测技术

在IPS引擎中，引入了文件的异常检测技术，对文件的检测同协议检测一样，把文件视为一种“协议”。如果网络中传输的文件是恶意文件，IPS同样能进行检测。

IPS支持大部分互联网协议上传输的文件检测：HTTP、SMB、FTP、SMTP、POP3、IMAP、NFS。同样，AR中内置的文件类型识别引擎提供包括PE、ZIP、OFFICE、PDF、JPG、AVI、SWF等上百种文件类型的识别能力，可以做到对网络中传输的恶意文件的检测。

2.4 基于网络特征的模式匹配技术

网络流量中存在入侵攻击行为、木马病毒传播行为、漏洞攻击行为、木马僵尸网络通信行为等特征。通过对这些行为特征进行分析，形成相关的网络行为特征码来检测网络中的恶意流量，以达到阻断网络恶意行为的目的。对于大部分的网络恶意行为，通过一个报文的特征就能进行检测。IPS引擎提供了多模匹配技术，并且支持正则规则表达式，可以极大的提高规则的灵活度和准确性。

2.5 基于协议异常检测技术

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。

IPS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。

同样的，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，IPS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。

2.6 基于 WEB 攻击行为检测技术

除了对常规的HTTP流量进行异常检测外，还对用户提交的信息进行数据还原，然后行为特征检测；检查用户是否是正常提交数据，还是进行注入、XSS等攻击行为。

2.7 全方位的防躲避技术

由于网络协议的复杂性和TCP/IP的开放性，攻击者会对协议流量进行变形，由于设备无法区分是由于网络原因无意的变形还是攻击者有意的变形，对于变形的流量不能简单的进行丢弃（可能会影响正常业务）或者放行（会造成攻击漏过）处理，这时候就需要引擎能提供流量归一化（整形）的处理，比如：

（1）IP分片的重组，对乱序到达的分片报文进行缓存，重组。保证从首分片开始，顺序到达。

（2）TCP流量的流重组，包括TCP状态维护，TCP分段重叠处理，丢弃重叠部分；TCP选项检查等。

（3）RPC（DCERPC、SUNRPC）分片重组、多请求绑定等逃避方式。

（4）URL的插入字符、编码、路径等归一化处理

（5）FTP插入字符处理

（6）NETBIOS、SMB的虚假请求躲避

（7）HTTP的编码、折叠、异常头部等混淆躲避技术

2.8 特征库升级

华为IPS专业安全团队密切跟踪全球知名安全组织和软件厂商发布的安全公告，对这些威胁进行分析和验证，生成保护各种软件系统（操作系统、应用程序、数据库）漏洞的特征库；此外通过部署的信息搜集系统，实时捕获最新的攻击、蠕虫病毒、木马等，提取威胁的签名，发现威胁的趋势。AR能够在最短时间内获取最新的签名，及时地获取最新的IPS引擎，从而具备防御零日攻击的能力。

IPS签名库升级方式分为以下几种，分别适用与不同的操作场景：

（1）自动定时升级：更新及时，能第一时间对新产生的攻击进行防御，且不需要用户干预操作，比较适用于能连接到升级服务器的设备。如果需要确认新下载的签名库是否安全可用，可以采用确认机制，定时下载新版本，但不立即应用，确认后应用。

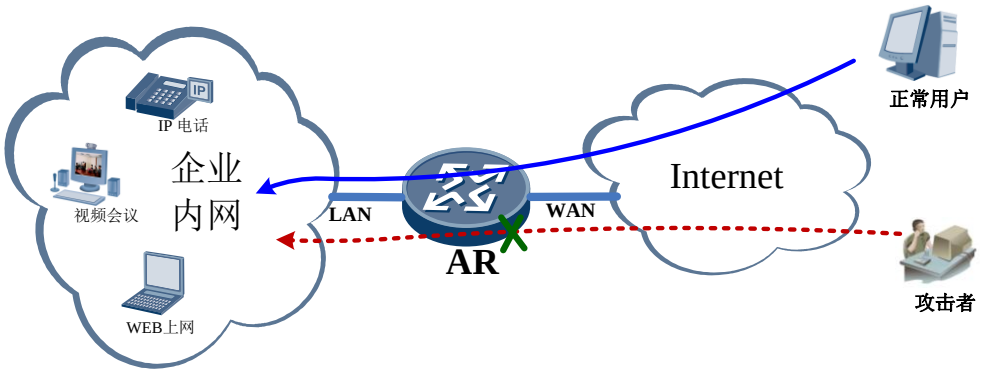
（2）实时升级：当可能有新版本发布，但未到自动升级的时间的时候，可以手工进行定时升级，优点是实时性高，且能立刻知道升级结果。

（3）本地升级：当设备无法与升级服务器建立连接或者需要将版本回退到较早之前的一个版本的时候，可采用本地升级，将版本切换到本地升级指定的版本。

（4）版本回退：可回退到上一个正常应用的版本。如果发现当前版本可能误报率较高，检测率较低或者其它不合理的因素时，可将版本回退到上一个正常应用的版本。

3 应用场景

入侵防御功能通常用于防护来自内部或外部网络对内网服务器和客户端的入侵。如下图所示，AR部署在企业网的出口。当外网用户访问企业内网（包括服务器、PC及其他设备）时，AR会对该行为进行检测。如果发现该行为为入侵，则进行阻断；如果不是入侵，则允许其建立连接。



术语与缩略语

缩略语	英文全名	中文解释
IPS	Intrusion Protect System	入侵防护系统
IDS	Intrusion Detection System	入侵检测系统
DPI	Deep Packet Inspection	深度报文检查
SQL	Structured Query Language	结构化查询语言
XSS	Cross-site Scripting	跨站脚本攻击
URL	Uniform Resource Locator	通用资源定位器