白皮书

入侵检测和防护

保护您的网络，有效防止攻击

Sarah Sorensen
产品市场经理

Juniper网络公司北京代表处
北京市东城区东长安街 1 号
东方经贸城西三办公楼15层1508室
邮政编码:100738
电话:8610-6528-8800
传真:8610-8518-2626

www.juniper.net
www.cn.juniper.net

文档编号：200065-001SC

目录

Copyright © 2004, Juniper网络公司

您的网络是否受到有效的攻击防护？

今天的商业环境大大不同于5年以前的商业环境。公司联网比以前任何时候都广泛，人们普遍认为网络扩展的趋势只会继续。因此，各公司必须努力设法在不影响增长和降低生产效率的前提下保护网络安全性。

为了保护安全性，几乎所有连接到互联网的公司所采取的第一步措施是安装防火墙，而且这样做也有很好的理由。防火墙可以作为网络的外围保护措施，决定允许或拒绝哪些流量进出网络。防火墙执行这一功能的方法是，根据各种标准（如涉及到的源、目的地和协议）来采用一套策略，其中包括“接受”和“拒绝”规则。通过提供接入控制功能，防火墙可以很好地提供网络安全保护的第一层保护功能。大多数防火墙策略可以支持SMTP、FTP、HTTP、SMTP和DNS等策略，这些策略可以使公司通过互联网安全地开展业务，并可拒绝那些有可能给内部系统带来安全威胁的流量。

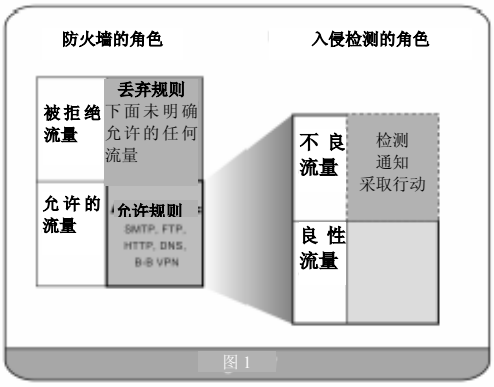


图 1

第二层保护是，检测那些被允许在网络中传输的流量中可能存在的攻击，并保护网络免受这些攻击的威胁。目前最普遍的观点是，被动的网络入侵检测系统(NIDS)可以保护企业免受这些攻击。然而遗憾的是，基于以下原因这一观点并不正确：

- **错误告警：**由于入侵检测机制很有限而且实施很不完善，所以许多NIDS解决方案会产生不准确的检测结果。以下情况便是很好的证明：由于产生大量的错误告警，系统管理员不得不经常花费大量时间来进行手工过滤，以在众多的错误告警中确定真正的攻击。因此，许多公司最终只能忽略这些信息，致使系统无效。

- **低可管理性，高维护成本：**当前的NIDS解决方案难以管理和维护已是众所周知的事实，因为这种解决方案经常需要花费大量的时间和精力来更新传感器和执行安全性策略。

- **认为需要外包：**许多公司认为，如果他们向系统中添加NIDS，他们必须将其维护工作外包给可以提供有效管理的安全服务供应商才能从中获得价值。

- **不能防止攻击：**目前的NIDS解决方案不能防止攻击。虽然厂商对外宣传可提供攻击防护功能，但这些产品实际上只是检测产品，而提供防护机制只不过是一句空话。

此白皮书介绍了有关可以解决这些问题的技术发展成果。它深入解释了在入侵检测设备正确实施的情况下，该设备如何提供功能强大且经济高效的解决方案来补充防火墙，从而更好地保护您的企业资产。这些技术成果包括更高的入侵检测准确性和防止入侵的能力，同时还可以简化系统的部署、配置和长期维护。Juniper网络公司的NIDS中包括了这些技术成果，该产品专门设计用于提供防护机制。Juniper网络公司的NetScreen-IDP™ (入侵检测和防护)产品系列不但可以准确地检测入侵，而且可以采取下一个逻辑步骤，那就是使企业具备攻击防护能力，以免网络资源遭到破坏。

在阅读完本白皮书之后，您将了解以下内容：

- 各种入侵检测机制的运行原理，以及联合实施这些机制的重要性。
- 为什么说最著名的入侵检测机制即数据包签名已经过时，而基于Stateful Signature™(状态式签名™)的系统可以提供更快速、更准确的入侵检测功能。
- 为什么入侵检测和防护解决方案必须在线内运行以防止被绕过，同时为您的网络提供全面的保护功能。
- 为什么需要细粒度的控制选项来使多个检测和响应机制发挥最大效用。

入侵检测和防护要求

NIDS能检测和不能检测什么？

每个网络中都有不良(恶意)流量。这可能是企图获取信息的外部用户，也可能是心怀不满、试图造成破坏的内部员工发出的。不管是谁发起攻击，您都会希望能够了解情况并采取相应措施。NIDS可以向您提供有关攻击的详细信息，从而使您可以防止攻击给您的业务带来不利影响。然而，系统的好坏取决于它的检测功能。因此，系统检测机制的精确性十分关键，它必须高度精确，以区分进入您网络的良性流量和不良流量。

以下部分列出了入侵检测可能导致的结果(见图2)：

1. **未检测到的不良流量**
2. **检测到的不良流量**
3. **被系统认为是不良流量的良性流量 (错误告警)**
4. **系统确定为正常的良性流量**

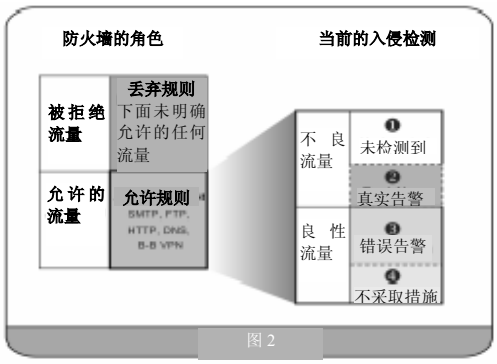


图 2

1. **对于不良流量：不能识别出恶意流量为攻击。**

这是可能出现的最糟糕的结果，因为这意味着入侵检测系统未能正确地执行其功能。不能检测到攻击，是由于在NIDS中没有正确实施足够的或全面的入侵检测机制；或是由于有新的攻击出现而没得到有效实施的检测机制未能检测到。尽管不可能检测出所有攻击类型，但任何系统的目标都应该是最大限度地减少不能检测到的攻击的数量。

2. **对于不良流量：确定“真正的攻击”为攻击。**

这是入侵检测系统的理想检测结果。快速而可靠地检测不良流量的能力被称为入侵检测精确度。系统的所有其他功能都与这一功能紧密相关。系统的检测精确度越高，系统功能就越值得依赖。在您采用某系统来采取必要的措施（如丢弃连接）来保护您的网络之前，您必须确保该系统可以提供经过验证的检测精确度。

3. **对于良性流量：将正常业务确定为攻击**(经常叫作错误告警或误报)。

目前市场上NIDS解决方案最麻烦、最耗时的方面。这种情况经常发生在NIDS错误地将合法的良性流量中的某些内容看作攻击。这是非常有害的，因为您需要调查每个告警才能确定攻击是否

成功并评估任何造成的危害。在调查错误告警方面花费的时间越多，就意味着用于调查真正攻击威胁的时间就越少。最终结果是，错误告警使您对所使用的产品丧失信任，有时侯甚至会导致真正的攻击告警被忽略(“狼来了”效应)。大多数NIDS产品可以进行调节以减少错误告警，然而，这一调节过程通常需要花费大量的时间和精力，有时可能需要几个星期才能完成。此外，由于当前NIDS产品的管理设计原因，调节经常是一种“或全部，或不动”的方法。这意味着您必须选择是否对特定的攻击类型进行检测。如果为了减少错误告警而将对特定攻击类型的检测设置为“关闭”，那么这些攻击就会顺利通过NIDS而不被检测。最后，大量错误告警使我们很难可靠地丢弃连接，而这是真正防止攻击的唯一方法(见第2.3部分)。

4. **对于良性流量：正确地确定良性流量。**
入侵检测机制的理想结果，正确地确定良性流量。

检测技术

NIDS性能的完美状态是能够检测尽可能多的攻击类型并限制错误告警数量。然而遗憾的是，目前还没有任何一种检测机制可以使NIDS部署用于检测所有的网络攻击类型。因此，系统只有结合多种技术来检测不同类型的攻击，才能够很好地完成任务。在Juniper网络公司的IDP系统(见第3.1部分)面世之前，联合实施多种检测方法的唯一有效方法是购买两种或更多种产品，然后同时运行。目前市场上两种最常用的网络入侵检测机制是签名检测和协议异常检测。基于签名的系统在流量中查找已知的攻击模式(签名)。签名检测可以检测出已撰写签名的攻击类型，但不能检测到新出现的攻击类型或许多非常复杂的攻击类型。与此相反，基于协议异常检测的系统可以很有效地检测到一些未知的攻击类型，但却无法识别那些不违反协议的攻击。因此，我们需要一种能够结合各种技术优点的全面方法。下一部分介绍了目前可用的技术，以及每一种检测方法的功能。

协议异常入侵检测

协议异常检测方法有时也叫协议分析。这种方法能够分析数据包流(两个系统间的单向通信)，来识别普遍接受的互联网通信规则中的异常情况。这些规则是根据开放协议、公布的标准(RFC)以及厂商定义的网络设备间通信规范来定义的。这样做的目标是实施一种入侵检测机制来识别不符合规范或相关标准的流量。一旦检测到异常情况，您可以使用这种方法来做出网络安全决策。这对于检测可疑的活动非常有效，如检测缓冲器溢出攻击。

协议异常检测方法的优势在于它可以检测到：

1. 未知的新的攻击，检测依据是这些攻击不符合协议标准。
2. 绕过实施其它检测方法的系统的攻击。

3. 经过少量修改的攻击。这种攻击改变了已知攻击模式的格式以绕过基于签名的系统，但没有降低攻击的力度。

实例1：检测FTP反弹攻击

本例介绍了FTP反弹攻击，以及如何使用协议异常检测来检测这种攻击。FTP反弹攻击利用FTP（文件传输协议）规范中的设计漏洞来发起攻击。为了下载或上传文件，用户(FTP客户)必须首先连接到FTP服务器(1)。连接建立后，服务器会要求该客户提供发送或获取该文件的IP地址及端口号码。这是通过一种名为“PORT命令”的机制完成的。实际上，IP地址就是用户的地址，但PORT命令规范不限定该IP地址必须为用户的地址。这样，攻击者可以要求FTP服务器打开一条连接，以连接到不同于用户地址（2）的另一个IP地址。然后攻击者利用这个开放端口来通过FTP服务器将包含有特洛伊木马病毒的文件传输到攻击目标(3)。该过程完成后，攻击者就可以接入攻击目标，并将攻击目标中的文件直接传送到自己的设备中。为了检测这种攻击，NIDS需要对PORT命令中的请求和该客户的IP地址进行对比。如果二者不匹配，NIDS就需要发出告警。这是不可能通过签名匹配方法完成的，因为这种检测方法不基于特定文本字符串（模式）的匹配，而是基于两个网络协议单元之间的关系。另一方面，协议异常检测设计用于检测网络关系，并确定这些关系是否符合常规规范。通过协议异常检测，NIDS可以随时分析PORT命令中的请求，并将它与PORT命令所指向的IP地址进行对比。

实例2：检测无记载的缓冲器溢出攻击

本例介绍了缓冲器溢出攻击，以及如何使用协议异常检测方法来检测这种攻击。这些类型的攻击利用常见的编程错误来发起攻击。这些错误将使无限量的数据被读取到固定容量的内存缓冲器中，而该缓冲器不检查溢出。因此，过量的输入数据会“溢”出缓冲器，并在不经过应用软件检查的情况下传输到网络中。在出现这种情况时，某个内存地址就会被过量数据改写。如果操作正确，程序会不情愿地执行这些过量的数据。如果成功，攻击者就可以在被攻击的主机上运行他们想运行的任何程序。

攻击者一般通过尝试—错误的方法来发起这种攻击。通常情况下，他们掌握了一些有关系统和应用如何运行的信息，然后有系统地发送一些在特定系统或应用处理范围以外的数据。此刻，由于攻击模式还不存在，所以检测这种攻击的唯一方法是使用协议异常检测。这种方法可以确定数据传输是否异常或不符合规范，从而确定是否构成攻击。

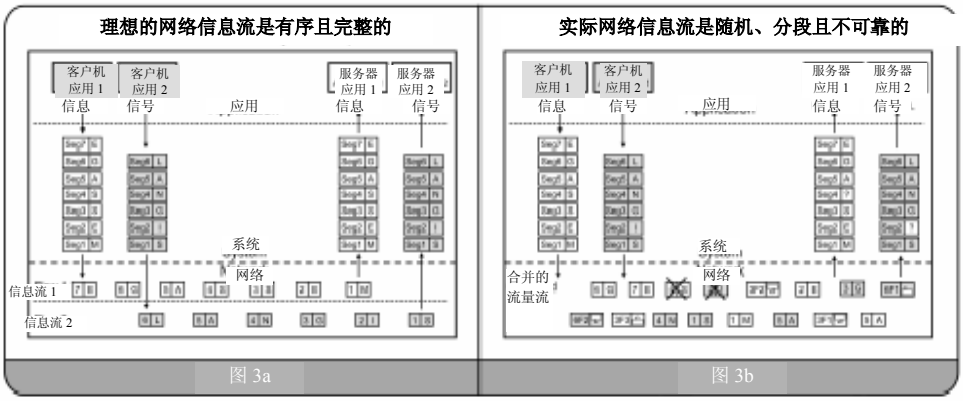
一个有趣的现象是，一旦缓冲器溢出攻击被发现、公布和辨别描述出（通过攻击者自己发起的攻击或已知的漏洞）后，基于签名的系统就可以将其确定为攻击。这是因为，一旦某种攻击被辨别出之后，其发起攻击的步骤也将被描述出来，由此建立了一种“攻击模式”。这样就可以撰写签名以便在将来“检测”这种攻击。

状态式签名入侵检测

基于识别和匹配攻击签名(模式)的入侵检测非常简单。从根本上讲，这种方法涉及到查找被辨别为薄弱环节或漏洞的流量中的特定模式。NIDS的演进过程中，起初实施的是一种名为“嗅探器（sniffer）”的无干扰式的数据包监控器，因为它可以嗅探网络中的数据包。入侵检测厂商使用数据包监控的概念来构建执行签名检测的系统。这意味着系统会查看数据包流中包含的信息，并将它与已知的攻击签名数据库进行对比。这种简单的入侵检测方法有很多缺点——尤其是需要花费很大的功夫来创建一个大型的攻击签名信息库，更不用说如何进行流量重组、解码、标准化和分析。

网络传输 – 所见非所得

当信息在网络中传输时，信息被分割成编了号的TCP(传输控制协议) 分段，并以数据包的形式进行发送。在理想情况下，数据包会按顺序传输而不会丢失(见图3a)。但遗憾的是实际情况并非如此。信息在实际传输时(见图3b)，网络会随机（不按顺序）传输数据包，或传输更小的数据片段（称为碎片），这种碎片由联网设备（如路由器）进行分隔以便于传输。更糟糕的情况是，数据包会由于各种各样的原因而被“丢弃”。接收系统负责将数据包重组为连贯的信息流并请求传输丢失的数据包，以便可以向应用提供完整的信息。图3a和图3b只显示了从客户机发往服务器的单一信息流；实际情况是，从客户机到服务器的大多数通信包含两个信息流：一个从客户机到服务器，另一个从服务器回到客户机。



为了准确地处理流量，必须使用正确的技术来消除对数据的错误解释。这些技术包括：

- IP碎片整理 – 能够正确地将数据包碎片组合为数据包
- TCP重组 – 能够以正确的顺序重组TCP分段，同时删除重复数据
- 流跟踪 – 能够跟踪信息流(从客户机到服务器的信息流，以及从服务器到客户机的信息流)，并使它们与单一通信会话相关联
- 标准化 – 能够解释并且在必要时从重组的信息中删除编码的表述和特殊字符

优化分析 = 状态式签名

在网络中传输、处理并重组数据包后，下一步工作是准确地检测该流量流中包含的入侵数据。目前市场上的大多数NIDS使用数据包签名检测方法，这意味着它们会查看信息流中每个数据包的原始字节，以试图发现是否与某种攻击模式相匹配。某些NIDS能够执行IP碎片整理和TCP重组功能以减少解释错误，然而当他们查看攻击模式时，他们仍需查看整个有序的数据流。这样会导致以下两个问题：

- 严重降低性能，因为这需要搜索整个数据流
- 产生误报的可能性更大，原因很简单：系统搜索的数据越多，将某签名与相关数据相关联的可能性就越大

现在要告诉您一个好消息，目前已开发出一种替代方案，可以克服数据包签名检测在性能和精确性方面的缺陷，即状态式签名检测（Stateful Signature™）。这种先进的检测机制可以同时利用状态式检查和协议分析来识别攻击模式，这是作为协议异常检测的一部分完成的。因此，状态式签名在传输时就可以了解到每个数据字节的上下文，以及客户机和服务器的状态。这意味着状态式签名只能根据与每种签名相关的通信状态与相关的数据字节进行对比。换句话说，状态式签名只在可能产生攻击破坏的通信状态下检查攻击，从而大大提高了性能并减少误报。

实例3：检测SMTP Wiz攻击

本例介绍了SMTP (sendmail) ‘wiz’攻击，以及如何使用状态式签名检测和数据包签名检测来检测这种攻击。wiz攻击使攻击者可以获得运行SMTP服务器的主机的根接入权限。攻击得逞后，攻击者可以完全控制“被攻击”的主机，并将它用作一个平台来发出进一步攻击，窃取电子邮件信息和其他数据，并最终获得接入网络和系统的更大权限。这种攻击是通过向服务器发送命令“wiz”实现的，此时客户机和服务器之间的sendmail会话处于“命令模式”。

让我们更深入地讨论一下一般的SMTP会话，了解如何使用状态式签名来更精确地检测攻击。图4显示了一般SMTP会话的4个阶段：

1. 建立TCP连接 (3方握手)
2. 命令模式：
    a. 设置发送器(“MAIL FROM”字段)
    b. 设置接收器(“RCPT TO”字段)
3. 执行其他命令
4. 数据模式(电子邮件的内容)
5. 断开TCP连接(4路断开)

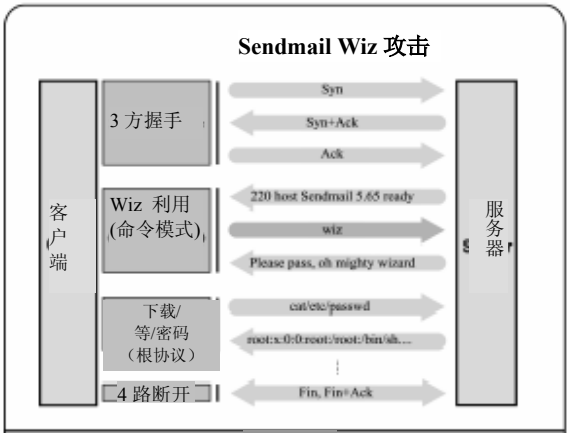


图 4

基于数据包签名检测机制的系统只是检查每个数据包来寻找攻击模式，而不考虑通信的环境和客户机及服务器的状态。这样一来，在通信会话中任何部分的任何字符串只要包含‘wiz’，该字符串都会被检测出来。这种方法很可能会触发错误告警，因为电子邮件正文(数据模式)或电子邮件接收器列表(命令模式)，以及“wiz”命令(命令模式)中也可能会包含“wiz”。这似乎微不足道，但实际上‘wiz’经常出现在电子邮件中。其实，只要用户发送的邮件附件超过100K，这种情况都会发生。原因是所有电子邮件附件都是使用‘base64’ (RFC 1421)来编码的。这种方法以46个可打印字符的格式显示二进制数据(Word、PowerPoint和其它应用)。这些字符中的6个字符为‘w’、‘W’、‘i’、‘I’、‘z’和‘Z’。由于附件中的数据随机性很大，所以在随机字符流(每个字母不分大小写)中出现‘wiz’的算术概率为，每32,768个字符(32*32*32)中出现一次。此外，‘wiz’还经常出现在电子邮件客户机或服务器中常用的词语中，例如，在电子邮件地址thewizard@company.com或包含“wizardry”或“wizened”等的电子邮件信息中。使用数据包签名检测时，所有这些情况都会触发告警。

使用状态式签名的系统，只查找在“命令模式”下的客户机到服务器SMTP信息流中包含的“wiz”模式。此外，状态式签名还可以忽略以这种模式出现的电子邮件地址，因为从这里不可能发起攻击。状态式签名在客户机-服务器会话中比较薄弱的部分来进行模式对比，而不是在整个会话中漫无目的地搜索字符串。因此，您可以在调节系统和调查误报方面花费更少的时间，同时可以信赖系统告警的准确性。

使用后门检测方法的入侵检测

我们已讨论了如何检测那些违反协议的攻击，和众所周知而且得到描述的攻击(签名检测)，但是我们还需要了解如何检测那些不为人们所知但又不违反协议的攻击，如特洛伊木马或蠕虫攻击。这些攻击安装在网络资源中，并打开网络资源后门。在攻击者激活并控制资源之前，这些后门一直处于休眠状态。这是通过一系列交互来实现的，在此过程中，攻击者发送命令，然后资源执行这些命令。由于没有攻击模式，也没有协议被违反，所以我们需要另一种方法来检测这种交互式流量。

由于蠕虫或特洛伊木马可能是通过后门 (调制解调器连接、即时消息、或连接到企业网络的家庭笔记本电脑) 进入网络的，又或者是另外一种检测机制未检测到的，所以使用多种检测方法可以大幅度提高攻击检测的准确性。

实例4：通过即时消息安装蠕虫

例如，许多公司允许员工使用即时消息。这虽然是一种有用的通信工具，但同时又为攻击者进入您的网络敞开了大门。大多数即时消息产品，如Yahoo! Messenger™允许用户发送附件。这些附件可能包含恶意代码，如蠕虫，蠕虫可以在用户向计算机下载附件的过程中安装，而用户不会有丝毫察觉。一旦安装成功，攻击者就可以返回并与这些恶意代码交互，指导它向他们发送文件，对硬盘进行重新格式化或发起其他攻击。这种类型的攻击使攻击者可以完全控制该资源并最终控制整个网络。

Juniper网络公司发明了一种名为后门检测的方法，可以检测出这种交互式流量的独特特点。Juniper网络公司的IDP查看所有的交互式流量，并根据规则库中管理员定义为“允许”的项目来检测未经过授权的流量。这种方法几乎可以检测到所有后门，即使流量是加密的，或者协议是未知的。

使用流量异常的入侵检测方法

虽然有许多攻击是包含在某个特定的通信会话中，但检测跨多个会话的流量中的攻击也非常重要。该类型攻击的最好例子是端口和网络扫描。发生端口和网络扫描时，攻击者使用一种工具来确定哪些业务是系统中允许的并得到响应。这是通过测试一台计算机上的所有端口（端口扫描），或整个网络上的特定端口（网络扫描）来实现的。

根据这些信息，攻击者将利用已知的漏洞来攻击这些开放端口上的响应业务。对于检测这些类型的攻击，需要在整个流量流中检测模式，并需要设定某种形式的频率和门限触发值。异常检测正是设计用于检测这些类型的攻击。

实例5：检测网络扫描

本例介绍了网络扫描“攻击”，以及如何检测这种攻击。如前所述，在网络扫描过程中，攻击者将试图在整个网络中接入特定的服务，如SMTP端口。这通常是向该业务发起攻击的前兆。协议异常检测和状态式签名检测都不能检测到这种“攻击”，因为扫描符合协议，而且模式不会出现在特定会话中。检测这种“攻击”的唯一方法是使用流量异常检测，这种方法可以对整个业务流执行模式匹配。最后需要说明的是，网络扫描并不是一种真正的攻击。然而，这是即将出现攻击的很好的征兆，因为这意味着有人在试图了解系统上正运行什么。如果您具有网络扫描知识，您就可以观察并预测接下来的攻击。因此，我们说检测网络扫描与检测攻击本身一样重要。

使用常规表达式的模式匹配

检测的准确性不仅受系统所使用的检测方法类型的影响，同时也和系统定义及检测攻击模式的方法有关。某些系统定义并搜索固定模式，这种方法效率非常低，因为有几十种不同排列的攻击签名。最理想的方法是提供对常规表达式模式匹配的支持。常规表达式可以提供通配符和复杂模式匹配，因此可以更准确地显示攻击。常规表达式还可以在控制系统行为方面提供很大的灵活性。

例如，为了查找一条带有可执行附件的电子邮件消息，NIDS应寻找以下模式：
name = “<some-name>.EXE”
其中*some-name*可以是任何有效的文件名。

问题是符号 ‘=’之前或之后可以有任何数量的空格和制表符。例如，该模式应匹配‘name = “run-me.ExE”’。没有常规表达式匹配功能的NIDS产品不能规定 ‘=’ 前后可以有任何数量的空格和制表符，而只会查找‘=’前后没有空格符的“标准”情况。通过在‘=’前后加上空格和制表符，任何攻击者都可以发送感染病毒的可执行文件，同时使没有常规表达式匹配功能的NIDS产品无法检测到攻击。

入侵检测和防护必须在线内运行

目前市场上的大多数NIDS产品不能防止攻击，因为它们只是基于嗅探器的“被动”入侵检测系统。这些系统只能“听取”流量，而不能在适当时通过丢弃、修改、指引、延迟数据包或者拒绝它们自己的数据包进入网络来控制流量。很容易理解为什么大多数NIDS只是作为被动设备运行。如果您不能相信攻击识别结果，那么任何数据包流进入网络都将可能带来危险。迄今为止，目前市场上NIDS产品由于误报和不准确的攻击识别而很难让人信任，因为它们采用的是没有得到完善实施的单一检测方法。然而，如果NIDS能够提供精确的检测结果，那么理解为什么NIDS需要在线内运行才能提供全面的保护就非常重要。

防止检测躲避

被动入侵检测系统在各种各样的攻击技术面前始终显得不堪一击。这是因为被动网络监控会使流量变得模糊，从而使系统很难提供一种可靠的入侵检测机制。这一部分内容将介绍躲避入侵检测系统的基本方法、在实际中它是如何操作的、以及为什么总是有可能避开被动入侵检测系统。阅读完本部分内容后，您将了解到防止躲避入侵检测的唯一有效方法是将入侵检测系统作为一种线内设备运行，以消除流量模糊性。

躲避入侵检测系统：理论

躲避检测的基本理念是欺骗入侵检测机制，使它“看到” 不同于目标主机（通常称为“攻击目标”）所看到的数据。这使攻击者可以有效地攻击主机而不被检测到。这同时适用于基于签名的入侵检测系统和基于协议异常的入侵检测系统。

要理解这一原理，您首先需要了解NIDS是如何进行TCP重组的。(实例请参见图5) 。应用1为通信生成信息以形成数据流（MESSAGE）。操作系统将这个信息流分进行分段(“TCP分段”)并将它们发送到网络中。接收操作系统收集这些TCP分段并将它们重新转换成数据流(MESSAGE)，然后该数据流被显示给接收应用。由于基础网络不能确保TCP分段的传输，所以接收器告知发送器已收到以及未收到哪些分段。然后，发送器可以重新发送未收到的分段。

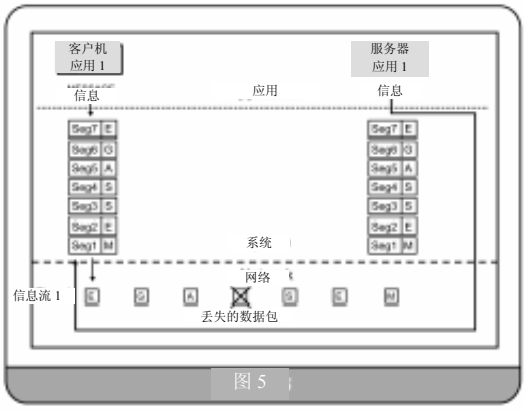


图 5

在NIDS环境中，TCP重组就是按照发送应用发送TCP分段、以及从这些分段中提取应用数据流的顺序来收集这些TCP分段的过程。作为被动系统执行TCP重组时，查看每一个TCP分段(数据包)非常简单，但要以与接收器所“看到”的相一致的方式进行TCP重组却非常困难。

接收到TCP分段后，NIDS传感器需要确定如何进行处理。TCP分段的接收器可以有以下几项处理选择：

1. **使用整个分段** – 这是最常见的情况
2. **使用部分分段**进行TCP重组，同时忽略其余部分 – 这种情况发生在新到达的分段与已接受的分段有重复时，或者分段的部分内容不在范围内（接收器预期的数据包序列号）而被忽略时。
3. **忽略整个分段** – 这种情况发生在分段被提前接收到或收到的分段无效时。无效的数据包包括包含不正确的IP或TCP校验和、无效的TCP标记、过时的TCP时间标记的数据包以及许多其他情况下的数据包。
4. **未接收到分段** – 接收器可能由于网络原因（分段丢失）或数据包设置（如IP TTL）原因而根本未接收到TCP分段。这类似于第3种情况。

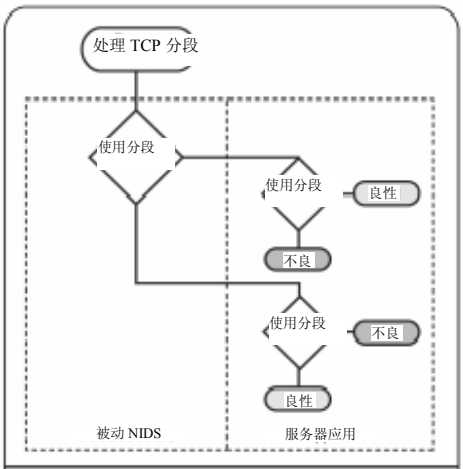


图 6

NIDS传感器必须推断出目标接收器将如何处理TCP分段并以完全相同的方式进行处理。如果NIDS做出错误的决策：

- NIDS传感器将使用接收器不使用的分段，从而检测到接收器将忽略的数据
- NIDS传感器将忽略接收器将使用的分段，从而造成数据丢失

不管是哪种情况，NIDS传感器都会对错误的数据（见图6）进行检查(签名匹配或协议异常检测)。

实际操作中的躲避

现在，我们已了解了NIDS TCP重组的基本原理，可以重新讨论NIDS躲避问题了：

当NIDS传感器错误地使用或没有使用部分或整个TCP分段来进行TCP重组时，将发生NIDS躲避。这种错误使NIDS看到的数据不同于TCP信息流发送器和接收器看到的数据。

在实际操作中，为了躲避NIDS传感器检测，攻击者会调整TCP分段的格式，从而使NIDS

几乎不可能判断“攻击目标”是否会接受这些分段。如果攻击目标不接受这些分段，NIDS就不能确定它将使用分段的哪个部分。这种TCP分段被称为“*模糊TCP分段*。”

然后，攻击者将重新发送包含不同数据的同一个TCP分段，从而触发以下两种情况之一：

. NIDS传感器在重组过程中使用最初的伪TCP分段，攻击目标丢弃该分段。带有攻击的第2个TCP分段被NIDS传感器忽略(因为以前曾见到过该分段)，而被攻击目标使用(因为它忽略以前的分段)；或

. NIDS传感器在重组过程中忽略了最初的攻击TCP分段而攻击目标使用了这一分段。第二个伪TCP分段被NIDS传感器接受而被攻击目标忽略。

生成模糊TCP分段

本部分介绍了生成模糊TCP分段的几种不同方法。虽然其中的某些方法可能会使NIDS有效地检测到此类分段，但大多数并未提供一种理论算法来使NIDS确定攻击目标如何处理TCP分段。

毫不费力的模糊TCP分段生成方法

目前有几种非常简单的模糊TCP分段生成方法。一个好的NIDS必须能够消除这些模糊性以正确地解释发送的流量。生成模糊分段使用的技术包括：

. 无效的TCP校验和–攻击目标肯定将丢弃包含无效TCP校验和的数据包。不能验证TCP校验和的NIDS将接受被攻击目标丢弃的数据包。

. 窗口外数据 – 接收器只会接受一定窗口（称为接收器窗口）内的数据而忽略这一窗口以外的数据。然而，由于不是实际接收器，执行被动重组的NIDS很难准确地确定目前的接收器窗口。这样，攻击者就能够发送接近攻击目标接收器窗口内外的数据，使NIDS无法分辨。

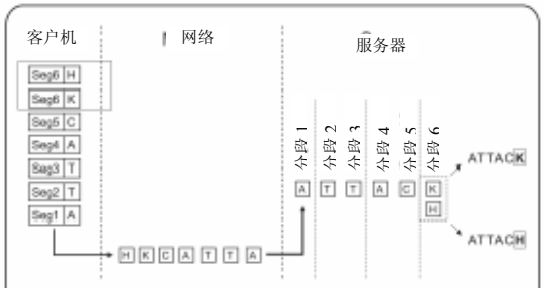
通过TCP实施来利用不一致的RFC解释

为TCP制定规范的各种RFC(RFC 793、RFC 1323等)非常复杂，同时也为实施人员做出解释留下了空间。此外，某些TCP实施有意或无意地与规范存在出入。最终的结果是相同的TCP分段可能被某些TCP堆栈实施接受而被另外一些拒绝，从而使攻击者有很多机会来生成模糊TCP分段。

实例5：重叠TCP分段

本例介绍了重叠TCP分段如何产生模糊性，以及如何防止出现这种模糊性。

攻击者可以在重叠的TCP分段（即两个包含不同数据的相同分段）中发送不同的内容。不同的TCP堆栈实施会以不同方式解释顺序，某些使用最初收到的，而另外一些可能会使用最后收到的。例如，Windows总是使用从较早的分段中收到的数据而Solaris使用新分段中的数据。BSD和Linux的情况不一定，它们有时候选择较早的TCP分段而有时候选择新近收到的分段。如果不了解受攻击主机的TCP实施的具体行为和环境，NIDS就不能确定什么是正确的行为以及是否应该发出告警。



本例显示了客户机如何通过发送重叠的数据来给 NIDS 制造“问题”。该客户机以正常方式发送第一组的 5 个分段，然后有意地生成两组不同的 6 个分段并将它们发往服务器。不同的 TCP 堆栈实施将以不同方式解释这些数据。大多数操作系统将把这些数据解析为“ATTACH(附加)”，而 Windows NT 和 Solaris 将解释为“ATTACK（攻击）”。

图 7

防止NIDS躲避

关于所有NIDS躲避技术的好消息是，现在我们可以非常轻松地检测到模糊数据包。例如，如果某入侵检测系统检测到两个包含不同内容的重叠TCP分段，那么这肯定是模糊分段而且很可能是一次攻击尝试。然而，虽然检测是可能的，但要确定目标主机将如何处理这些模糊数据包却不太可行。这意味着我们不可能确定目标主机是否已受到影响。此外，当在同一条连接上检测到多个模糊数据包时，入侵检测设备知道这**是**一次攻击，但要确定攻击者正在尝试发起**哪种攻击**却不太现实。这是因为重组模糊数据包的方法可能会有数百万种组合，但攻击只采用其中一种组合。找出这一种组合可能需要几个小时、几天甚至几年，而这对于实施入侵检测系统而言非常不切合实际。

这就导致我们作出以下结论：

一旦一个模糊数据包到达目标，入侵检测系统就会“失明”而不能确定发起的是哪种攻击以及攻击是否成功。

显而易见，防止入侵检测躲避的唯一有效方法是防止模糊数据包到达目的地。当然，这只能在入侵检测在数据传输路径上时才能实现，也就是在线内运行时才可以实现。

防止入侵

被动入侵检测系统的最主要缺点是它是***被动的***，而且不能控制是否允许攻击到达其目标。因此，被动系统实际上只能用于检测攻击而不能防止攻击。然而，目前有厂商声称被动设备中已采用了有效机制来防止攻击。这些机制是：

- 发送TCP复位
- 向防火墙或路由器发送信令，以阻止流量

本部分内容将介绍这些机制，并说明为什么它们不能真正防止攻击。

TCP复位

TCP复位的基本机制是，入侵检测设备在检测到一次攻击时向客户机和服务器同时发送一个复位数据包。这种方法存在几个方面的问题。首先，入侵检测设备需要一段时间来确定有人发起入侵并发送复位数据包。而在这段时间内，发起攻击的分段以及很有可能是随后的一些数据包已经被发送到目标网络并且已经到达了它们的“攻击目标”。因此，在检测到攻击后再发送的任何复位都为时已晚了。TCP复位的第二个缺点是它们只适用于TCP协议而不适用于基于UDP的协议，如DNS。第三个问题（也是最重要的一个问题）与TCP复位的运行方式有关。TCP复位信息必须包含一个有效的序列号才能使服务器接受它。为了确保有效，该序列号必须在某个相对较小的“接收器窗口”内。熟练的攻击者可以迅速发送自己的攻击分段并迅速地改变接收器窗口，从而使被动设备很难确定应该为其复位数据包分配什么序列号。因此，大多数TCP复位尝试将无法有效地防止攻击；有时候可能会起作用，但大多数情况下不能。

防火墙信令

防火墙信令实际上根本不是一种防护措施。相反，它实际上是接入控制系统（通常为防火墙或路由器）的有效反馈机制。防火墙信令使入侵检测系统能够告诉防火墙它应“阻止”哪种类型的流量。最理想的效果是能够调节防火墙策略以防止未来的攻击。这听起来很不错，但事实证明这种方法带来的危险要大于它的优点。攻击者可以很轻松地隐瞒攻击来源并使NIDS相信攻击是从另一个IP地址发起的。例如，如果某攻击者窃取到某大型互联网服务供应商代理服务器的IP地址，如美国在线(AOL)，而NIDS指示防火墙屏蔽该IP地址，那么提供给整个AOL用户群的服务都将被屏蔽。有时候攻击者甚至不需要窃取IP地址就可以实现这一目标：他们可以以AOL用户的身份发起攻击。这样，NIDS-防火墙结合就成了简单而又危害极大的拒绝服务(DoS)攻击的大门。

主动防护设备必须在线内运行

防止入侵的唯一有效方法是使防护设备作为一种线内设备运行，使网络安全设备能够在连接点上丢弃发起攻击的数据包。这样，系统就可以处理所有类型的流量，而且当与适当的入侵检测机制结合使用时就能够提供最高的安全性。

可管理性

任何NIDS的一个不可或缺的部分是您如何与系统交互。如果NIDS的配置和管理很困难，那么从这些功能中获益也将非常困难，即使它包含了世界上所有的检测机制和响应选项。目前市场上最理想的解决方案使用了一种基于规则的集中管理机制，来提供非常细粒度的系统功能控制。事实证明这种方法对于管理防火墙非常有效。用于NIDS时，这种方法使您可以通过一套由各种规则组成的单一逻辑安全性策略来控制需要管理的所有设备。基于角色的管理的理念是使用一系列易于定义的序列逻辑表达式（或规则），其中包含基本的匹配标准以及相关行动规范的格式。这种格式使您可以精确地控制系统在查找哪种流量以及检测到这种流量时作何处理。这种基于规则的集中方法还可以使您决定应用每条规则的方式。例如，您可以将一条规则应用于一个或所有传感器，然后按下一个按钮就可以使该规则立即生效。利用集中管理系统时，您不需要花费时间和精力来更新每一台传感器，您只需要更新集中安全性策略，然后对应的传感器可以自动得到更新。这种方法可以简化配置和签名更新，同时可以提高系统的总体准确性，因为它使您可以根据网络中的薄弱环节和具体需求来为特定设备应用相应的功能。

Juniper网络公司的方法

利用Juniper网络公司的入侵检测和防护产品系列(Juniper网络公司NetScreen-IDP™10、100、500和1000)，Juniper网络公司推出了一种创新的方法来保护网络安全性。Juniper网络公司的IDP是完全重新设计的，也是目前市场上采用本文介绍的许多先进技术的第一种产品。它的第一项创新成果实施了一种名为多方法检测（MMD™）的技术。通过MMD，Juniper网络公司使用了8种不同的检测方法，包括协议异常检测、流量异常检测和某些先进的技术，如状态式签名（Stateful Signature™）、后门检测以及其他一些不在本文讨论范围内的技术，从而最大限度地增加可以检测到的攻击数量，同时减少错误告警。第二项创新成果是Juniper网络公司的IDP是作为一种线内解决方案运行的，这是防止检测躲避技术并提供真正的入侵防护的唯一有效方法。第三项创新成果提供了一种基于规则的集中管理框架。这种集中管理功能可以使管理员高细粒度地控制Juniper网络公司的IDP系统，同时简化安全性策略和签名更新。

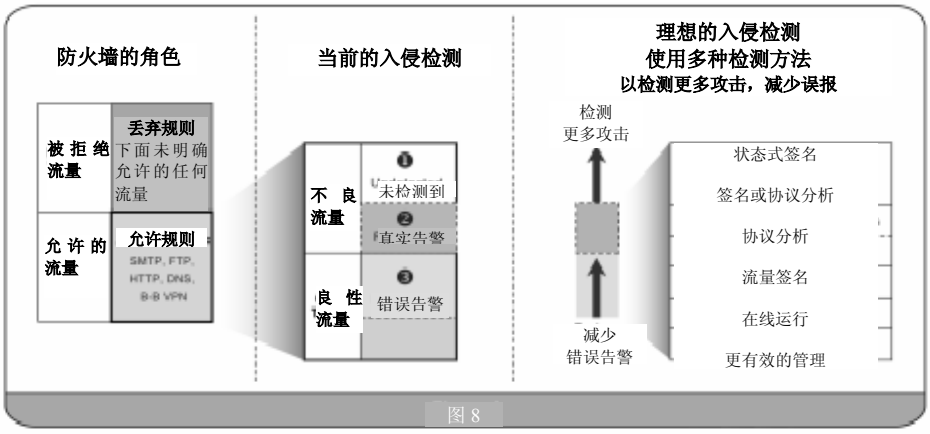


图 8

多方法检测(MMD)提高准确性

认识到没有任何一种方法可以检测所有网络入侵企图后，Juniper网络公司设计了一种通过多方法检测（MMD）来优化对可疑流量检测的系统。通过实施8种不同的检测方法，包括协议异常、状态式签名、流量异常检测、后门检测、Syn-flood（同步攻击）、IP欺骗和第2层检测以及网络陷阱（network honeypot），Juniper网络公司的IDP系统可以准确地识别入侵。与其他厂商只使用一种入侵检测机制来主导整个产品体系结构的做法不同，Juniper网络公司的体系结构能够使用所有可用的检测机制。这些检测方法共享信息并协同运行，以最高效率的方式来在网络层和应用层识别所有类型的攻击。这种检测机制优化用于以最高的数据速率进行分析，而且几乎不会降低性能。您再也不需要绞尽脑汁来考虑是应该购买基于协议异常的系统还是基于签名的系统，更不用花钱购买两种甚至更多种产品，因为Juniper网络公司的IDP可以为您提供全面的检测功能。此外，由于该系统采用了多方法检测（MMD），管理员可以相信告警的真实性而不必担心需要花费大量时间来调查错误告警。

数据包处理实现准确的数据显示

为了正确地解释并显示流量流，Juniper网络公司的IDP系统采用了多种数据包处理技术来确保准确的数据显示。这些技术包括：

1. *IP碎片整理*和*TCP重组*，以正确地重组流量，从而使流量被观察的方式与目标系统观察流量的方式相一致。
2. *信息流跟踪*，将多条连接作为一个会话处理，实现更精确的分析。
3. *协议标准化*，将数据流解码为通用格式，进而进行精确的分析。

线内运行提供真正的保护功能

Juniper网络公司的IDP设计用于在数据传输路径上线内运行。在这种配置下，IDP通常安装在防火墙之后来检查发往或发自每个受保护网络的各个数据包。当Juniper网络公司的IDP检测到恶意流量时，它可以丢弃连接，使它永远无法到达网络。当然，您可以全面控制收到哪种流量时丢弃连接。相反，当被动NIDS检测到恶意流量时，它唯一的反应措施是发送一条TCP复位信息来尝试阻止攻击。遗憾的是，由于TCP复位本身的特点(见第2.3.2.1部分)，您不能确定是否及时阻止了攻击。这意味着您需要花费时间来调查攻击是否到达了其“攻击目标”。然后，您必须知道攻击是如何发起的，并尝试调节NIDS来防止将来出现类似的攻击。最后，如果攻击得逞，您必须评估攻击者带来的危害大小，包括这一过程中产生的硬性和软性成本。利用Juniper网络公司的IDP，您可

以及时丢弃发起攻击的流量并确保这些流量永远不会到达其攻击目标。

在数据包传输路径上运行Juniper网络公司的IDP有多个方面的优点：

. 攻击可以在被检测到后立即被阻止（丢弃），从而保证攻击不会得逞，以避免攻击得逞后所造成的危害。

. 您可以确信被丢弃的入侵没有得逞，因此您只需要根据具体情况进行调查。这可以为您节约时间，使您可以集中精力开展其它项目。

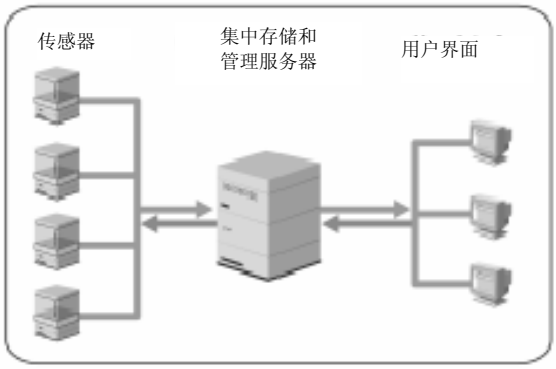
. 利用Juniper网络公司的IDP在数据包到达其目标之前检查其结构和内容，可以应对躲避IDS设备的常见方法。这样就可以防止攻击者利用模糊性来发起攻击。

需要注意的是，作为一种线内设备，Juniper网络公司的IDP既可以用作路由器又可以用作透明交换机，而不要求IP地址和路由修改。Juniper网络公司的IDP还可以作为一种被动NIDS(嗅探器)来部署，以提供MMD的优势，当然这不能用于防止攻击。最后，为了支持容错运行，Juniper网络公司的IDP系统还可以支持高可用性配置。

基于规则的集中管理实现更有效的控制

Juniper网络公司的IDP系统采用一种基于规则的集中管理方法来提供：

. 真正的3层管理体系结构，包括检测和实施层（传感器）、管理层(服务器)和应用层(用户界面)。多个管理界面可以连接到一台管理服务器以执行所有管理操作。



. 基于规则的管理可以实现对IDP行为的细粒度控制。为了应用规则，您可以通过规定源、目的地、服务以及需要搜索并匹配的攻击来制定规则。然后，这些规则可以规定检测到这种攻击时如何处理，如丢弃或允许连接以及如何记录攻击。

. 集中安全性策略，使同一安全性策略可以根据需要应用于多个实施点。设备之间的差异不要求制定新的安全性策略；这可以通过规定安全性策略中的哪条规则适用于哪种设备来实现。

. 闭环调查，使您可以在汇总报告、各个日志、触发日志记录的规则以及日志的数据包数据之间自由切换。关联不同数据点并在不同级别的信息之间切换的功能，使您可以轻松了解网络中发生的情况并立即采取行动来抵御新的攻击。

结语

防火墙系统可以很好地控制哪些流量被允许进入或离开网络。然而，它们难以避免地会允许某些恶意流量进入网络。您需要第二层防护来补充防火墙，以检测并防止所有类型的攻击。迄今为止，人们普遍部署被动网络入侵检测系统(NIDS)来检测网络攻击。遗憾的是，当前的入侵检测解决方案一般只采用单一的入侵检测机制，这会产生大量的误报和漏报。此外，它们是被动的，因此不能阻止攻击，而且其难以管理是众所周知的。

Juniper网络公司开发了IDP系统来克服这些缺陷，可为您提供了一种真正有效的产品来保护您的企业资产。Juniper网络公司的IDP系统在一种产品中结合了多种经过验证的著名设计理念，可为您提供值得信赖的解决方案。这些功能包括：

- 多方法检测 (MMD™)
- 线内运行
- 基于规则的集中管理

下一次当您考虑可靠的网络安全性时，请采用这些功能。

Juniper网络公司
1194 N. Mathilda Ave.Sunnyvale, CA 95014 ATTN：General Counsel