信息安全产品技术丛书

高性能入侵检测系统产品原理与应用

丛书主编　顾健

主编　顾健　沈亮　宋好好　王志佳

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

信息安全产品技术

高性能入侵检测系统产品原理与应用

丛书主编：顾　健

主编：顾　健　沈　亮　宋好好　王志佳

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书内容共分为5章。从高性能入侵检测系统产品的技术实现和标准介绍入手，对下一代互联网环境中部署的入侵检测系统产品的产生需求、发展历程、实现原理、技术标准、应用场景和典型产品等内容进行了全面翔实的介绍。

本书适合高性能入侵检测系统产品的使用者（系统集成商、系统管理员）、产品研发人员及测试评价人员作为技术参考，也可供信息安全专业的学生及其他科研人员作为参考读物。

图书在版编目（CIP）数据

高性能入侵检测系统产品原理与应用 / 顾健等主编. —北京：电子工业出版社，2017.7
（信息安全产品技术丛书）

ISBN 978-7-121-32113-9

Ⅰ. ①高… Ⅱ. ①顾… Ⅲ. ①计算机网络－网络安全 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2017）第 162168 号

策划编辑：李 洁
责任编辑：张 京
印 刷：北京季蜂印刷有限公司
装 订：北京季蜂印刷有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编：100036
开 本：720×1 000 1/16 印张：15.75 字数：257 千字
版 次：2017 年 7 月第 1 版
印 次：2017 年 7 月第 1 次印刷
印 数：2 500 册 定价：49.80 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：lijie@phei.com.cn。

前言

<<<<< PREFACE

经过多年的发展，基于 IPv6 的下一代互联网技术日益成熟，各种不同类型的支持 IPv6 的网络设备相继问世，并逐渐投入商业应用。

入侵检测系统作为典型的网络安全产品，通过收集信息、分析信息的模式来发现异常现象和攻击行为。随着网络技术的不断发展，攻击行为和攻击方式不断变种，对网络、主机和系统资源安全的威胁不断增加，因此对入侵检测系统产品的安全功能和处理性能提出了更高的要求，于是出现了具有更高性能的基于 IPv6 的入侵检测系统产品。

本书是“信息安全产品技术丛书”之一。本书在高性能入侵检测系统产品的产生需求、发展历程、实现原理、技术标准、典型应用等几大方面均有翔实的描述。与此同时，本书力求实用，收集了许多实际数据与案例，期望能对读者在了解高性能入侵检测系统产品的安全防护技术和标准上有一定的帮助。

本书的主要编写成员均来自公安部计算机信息系统安全产品质量监督检验中心，常年从事入侵检测系统产品等信息安全产品的测评工作，对入侵检测系统产品有着深入的研究。本书作者全程参与了高性能入侵检测系统产品标准从行业标准到国家标准的修订工作。因此，本书在标准介绍和描述方面具有一定的权威性。

丛书主编顾健负责把握本书的技术方向，第 1 章主要由顾健编写，第 2 章主要由沈亮、宋好好编写，第 3 章主要由宋好好编写，第 4、5 章主要由王志佳编写。此外，张艳、杨元原、邹春明等同志也参与了本书资料的收集和部分编

写工作。由于编写人员水平有限且时间紧迫，不足之处在所难免，恳请各位专家和读者不吝批评指正。

本书的编写得到了国家发改委信息安全专项“下一代互联网信息安全专项标准研制”项目（发改高技〔2012〕1615 号）的资金支持。

在本书的编写过程中，得到了华为技术服务有限公司、北京天融信网络安全技术有限公司、珠海经济特区伟思有限公司的大力协助，在此表示衷心的感谢！

编　者

目录

CONTENTS

第1章 综 述

美国时间 2011 年 2 月 3 日，国际互联网名称和编号分配组织（ICANN）官方网站宣布，最后一批 IPv4 地址分配完毕。各地区性互联网注册管理机构所掌握的 IPv4 地址也将分配殆尽。

IP 地址资源枯竭、物联网和云计算等新兴产业的发展，使得下一代互联网（IPv6）的商用地址成为互联网持续发展的必然选择。

1.1 下一代互联网（IPv6）简介

1.1.1 什么是 IPv6

IPv6 是 Internet Protocol Version 6 的缩写，其中 Internet Protocol 译为“互联网协议”。IPv6 是 IETF（互联网工程任务组，Internet Engineering Task Force）设计的下一代 IP 协议版本。目前 IP 协议的版本号是 4（简称为 IPv4），IPv6 正处在不断发展和完善的过程中，在不久的将来将取代目前被广泛使用的 IPv4。

IPv4 的核心技术属于美国，它的最大问题是网络地址资源有限。从理论上讲，IPv4 可支撑编址 1600 万个网络、40 亿台主机。但采用 A、B、C 三类编址方式后，可用的网络地址和主机地址的数量大打折扣，以至于目前 IP 地址近乎枯竭。其中北美占有 3/4 约 30 亿个 IP 地址，而人口最多的亚洲却不到 4 亿个，中国只有 3 千多万个 IP 地址，只相当于美国麻省理工学院所拥有的数量。但

随着信息技术及网络技术的发展，计算机网络逐渐融入了人们的日常生活。网络 IP 地址不足，严重地制约了全世界互联网的应用和发展。在这样的环境下 IPv6 应运而生。

单从网络地址容量上来讲，理论上 IPv6 所拥有的地址容量是 IPv4 的 8×10^{28} 倍，达到 2^128-1 个。这不但解决了网络地址资源数量的问题，同时也为终端设备连入互联网在网络地址数量限制扫清了障碍。

如果说 IPv4 实现的是主机间对话，那么 IPv6 则扩展到任意事物之间的对话，它将服务于众多的硬件设备如智能家电、智能汽车、智能仪器等，它将是无时不在、无处不在地深入社会每个角落的真正的互联网。

1.1.2 IPv6 的十大主要技术特点

IPv6 协议在 IPv4 协议的基础上做了诸多改进，解决了 IPv4 网络地址容量的不足，其主要技术特点如下。

（1）地址扩展：IP 地址由原来的 32 位扩展到了 128 位，并且 IPv6 取消了 IPv4 地址的分类概念，可提供 3.4×10^{38} 个主机地址。IPv6 地址的文本格式为 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx，其中每个 x 是一个代表 4 位的十六进制数字，可省略前导零。

（2）报文头的简化：IPv6 的数据头与 IPv4 完全不同。简化了数据报文头部，减少了路由表长度，同时减少了路由器处理报头的时间，降低了报文通过网络的延迟。IPv4 报文头检查如 sum、IHL、认证标识和碎片等不再出现在 IPv6 中。

（3）可扩展性：支持扩展和选项的改进，IP 首部选项编码方式的修改导致更加高效的传输、在选项长度方面更少的限制及将来引入新的选项时更强的适应性。

（4）流量标识：对服务质量作了定义，可以标记数据所属的流类型，以便

路由器和交换机进行相应的处理。IPv6 中增加了“flow label”标识，提供特定的 QoS。

（5）路由选择：IPv6 路由与物理接口（链路，如 TNLCFG64 或 ETH03）而不是接口关联（绑定）。IPv6 与 IPv4 的源地址选择功能不同。允许重复路由以提高稳健性，但在路由查找时将忽略重复路由。

（6）对流的支持：在 IPv6 中 IP 头的格式里有专门的 20bit 流标签域。主机发送报文时，如果需要把报文放到流中传输，只需在流标签里填入相应的流编号，如在流标签里填零就做一般的报文处理。路由器收到流的第一个报文时，以流编号为索引建立处理上下文，流中的后续报文均按上下文处理。

（7）不需要 SUM 区域检查：在路由器中检查 SUM 区域的协议数据包被移除，数据包在网络传输前已通过检查，另外高层协议如 TCP 和 UDP 允许自我确认，在多数情况下移除 SUM 区域检查不会产生严重的问题。

（8）最大传输单元（MTU）：IPv6 的 MTU 结构化下限为 1280 字节。也就是 IPv6 不会在低于此极限时对信息包分段。要通过小于 1280MTU 的链路发送 IPv6，链路层必须明确地对 IPv6 信息包进行分段和合并。

（9）可扩展协议：与 IPv4 不同，IPv6 不再定义未来所有可能协议，允许发送人添加数据包信息，这样使 IPv6 比 IPv4 具有更广泛的灵活性，还可以设计新需求。

（10）安全性：IPv6 进行了数据完整性及数据保密的扩展。

1.1.3　IPv6 的安全机制

在安全机制方面，IPv6 最为显著的特征就是将 IP Sec 集成到协议内部，从此 IP Sec 将不再单独存在，而是作为 IPv6 协议固有的一部分贯穿于 IPv6 的各个领域。IP Sec 提供四种不同的形式来保护通过公有或私有 IP 网络传送的私有

数据，包括：安全关联（Security Associations，SA）、报头认证[Authentication only（Authentication Header，AH）]、IP 封装安全载荷（Encryption and Authentication known as Encapsulating Security Payload，ESP）和密匙管理（Key Management）。

1. 安全关联 Security Association（SA）

IP Sec 中的一个基本概念是安全关联（SA），安全关联包含验证或加密的密钥和算法。它是单向连接，为保护两个主机或者两个安全网关之间的双向通信建立两个安全关联。安全关联提供的安全服务是通过 AH 和 ESP 两个安全协议中的一个来实现的。如果要在同一个通信流中使用 AH 和 ESP 两个安全协议，那么需要创建两个（或者更多的）安全关联来保护该通信流。一个安全关联需要通过三个参数进行识别，它由安全参数索引（AH/ESP 报头的一个字段）、目的 IP 地址和安全协议（AH 或者 ESP）三者的组合唯一标识。图 1-1 列出了 AH 和 ESP 报头在传送模式和隧道模式下的区别。

	传送模式	隧道模式
AH	基本IP报头和扩展报头	原始的IP数据包外面 封装新IPv6报头和AH
ESP	压缩数据包和IPv6扩展 ESP报头	ESP报头
带AH的ESP	ES报头和HA扩展报头	

图 1-1 AH 和 ESP 报头在传送模式和隧道模式下的区别

2. 报头验证 Authentication Header（AH）

认证协议头（AH）是在所有数据报头中加入一个密码。AH 通过一个只有密匙持有人才知道的“数字签名”来对用户进行认证。这个签名是数据包通过特别的算法得出的独特结果；AH 还能维持数据的完整性，因为在传输过程中无论多小的变化被加载，数据报头的数字签名都能把它检测出来。IPv6 的验证主要由验证报头（AH）来完成。验证报头是 IPv6 的一个安全扩展报头，它为 IP 数据包提供完整性和数据来源验证，防止反重放攻击，避免 IP 欺骗攻击。

1）验证报头

验证报头的格式如图 1-2 所示。

图 1-2　验证报头的格式

验证报头包括以下内容。

（1）下一个报头字段（Next Header）：确定跟在验证报头后面的有效载荷类型（如 TCP）。

（2）载荷长度（Payload length）：验证报头的长度。

（3）安全参数索引（Security Parameter Index）：用来确定安全关联的安全参数索引。

（4）认证数据字段（Sequence Number）：一个变长字段，它包含完整性检查值（Integrity Check Value，ICV），用来提供验证和数据完整性。

（5）保留字段（Reserved）：（16 位）供以后使用。

2）验证数据（Authentication Data）

验证数据，它包含完整性检查值（ICV），用来提供验证和数据完整性。计算 ICV 的算法由安全关联指定。ICV 是在这种情况下计算的，即 IP 报头字段在传递过程中保持未变，验证报头带有的验证数据置 0，IP 数据包为有效载荷。有些字段在传递的过程中可能改变，包括最大跳数、业务类别和流标签等。IP 数据包的接收者使用验证算法和安全关联中确定的密钥对验证报头重新计算 ICV。如果 ICV 一样，接收者就知道数据通过验证并且没有被更改过。

3）防止重放攻击（Prevent Reply Attack）

重放攻击中，获得加密数据包，然后发送设定的目的地，收到复制加密数据包后，可能面临破解及其他意想不到的后果。序列号计数器可阻止此类攻击，当发送者和接收者之间的通信状态建立的时候，序列号被置 0。当发送者或者接收者传送数据的时候，它随后被加 1。如果接收者发觉一个 IP 数据包具有复制的序列号字段，它将被丢弃，这是为了提供反重放的保护。该字段是强制使用的，即使接收者没有选择反重放服务它也会出现在特定的安全关联中。验证报头带有的验证数据置 0，IP 数据包为有效载荷。

3. 封装安全有效载荷数据（Encapsulating Security Payload）

安全加载封装（ESP）通过对数据包的全部数据和加载内容进行全加密来严格保证传输信息的机密性，这样可以避免其他用户通过监听来打开信息交换的内容，因为只有受信任的用户拥有密钥打开内容。ESP 也能提供认证和维持数据的完整性。ESP 用来为封装的有效载荷提供机密性、数据完整性验证。AH 和 ESP 两种报文头可以根据应用的需要单独使用，也可以结合使用，结合使用时，ESP 应该在 AH 的保护下。

1）封闭安全有效载荷数据包

封装安全有效载荷数据包格式如图 1-3 所示。

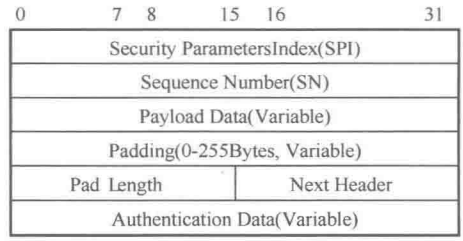

图 1-3 封装安全有效载荷数据包格式

封装安全有效载荷数据包含以下字段。

（1）SPI 字段［Security Parameters Index（SPI）］：确定安全关联的安全参数

索引。

（2）序列号字段（Sequence Number）：用来提供反重放保护，跟验证报头中描述的一样。

（3）有效载荷数据（Payload Data）：存放加密数据。

（4）填充字段（Padding：Extra Bytes）：加密算法需要的任何填充字节。

（5）填充长度（Pad Length）：包含填充长度字段的字节数。

（6）下一报头（Next Header）：描述有效载荷数据字段包含的数据类型。

（7）验证数据（Authentication Data）：用 ICV 加密算法加密的所有数据（非加密数据区）。

2）ESP 计算（ESP Computation）

在 IPv6 中，加密是由 ESP 扩展报头来实现的。ESP 用来为封装的有效载荷提供机密性、数据来源验证、无连接完整性、反重放服务和有限的业务流机密性。

3）局限性

ESP 不保护任何 IP 报头字段，除非这些字段被 ESP 封装（隧道模式），而 AH 则为尽可能多的 IP 报头提供验证服务。所以，如果需要确保一个数据包的完整性、真实性和机密性，则需同时使用 AH 和 ESP。先使用 ESP，然后把 AH 报头封装在 ESP 报头的外面，从而接收方可以先验证数据包的完整性和真实性，再进行解密操作，AH 能够保护 ESP 报头不被修改。

4. 钥匙管理（Key Management）

密钥管理包括密钥确定和密钥分发两个方面，最多需要四个密钥， AH 和 ESP 各两个发送密钥和接收密钥。密钥本身是一个二进制字符串，通常用十六进制表示，例如，一个 56 位的密钥可以表示为 5F39DA752E0C25B4。注意全部

长度总共是64位，包括了8位的奇偶校验。56位的密钥（DES）足够满足大多数商业应用。密钥管理包括手工管理和自动管理两种方式。

1）手工管理（Manual）

手工管理方式是指管理员使用自己的密钥及其他系统的密钥手工设置每个系统。这种方法在小型网络环境中使用比较实际。

2）自动管理（Automated）

自动管理方式可以随时建立新的SA密钥，并可以对较大的分布式系统上使用的密钥进行定期更新。自动管理模式弹性很强，但需要花费更多的时间和精力去设置，同时，还需要使用更多的软件。

IP Sec的自动管理密钥协议的默认名称是ISAKMP/Oakley。

（1）Oakley协议（Oakley Key Determination）

Oakley协议，其基本机制是Diffie-Hellman密钥交换算法。Oakley协议支持完整转发的安全性，用户通过定义抽象的群结构来使用Diffie-Hellman算法，密钥更新及通过带外机制分发密钥集，并且兼容管理SA的ISAKMP协议。

（2）ISAKMP协议（Internet Security Association and Key Management Protocol）

互联网安全关联和密钥管理协议（ISAKMP）定义了程序和信息包格式的建立、协商、修改和删除安全连接（SA）。SA包括各种网络安全服务执行所需的所有信息，这些安全服务包括IP层服务、传输或应用层服务、流通传输的自我保护的各种各样的网络协议。ISAKMP定义交换密钥生成和认证数据的有效载荷。ISAKMP通过集中安全连接的管理减少了在每个安全协议中复制函数的数量。ISAKMP还能通过一次对整个服务堆栈的协议来减少建立连接的时间。

1.2　为什么需要高性能入侵检测系统

1.2.1　“IPv6+IP Sec=安全”吗

IPv6 及其嵌入的 IP Sec 机制提供了一种很好的端到端之间通信的隐私保护能力。但网络层的安全改进无法解决其他层面的诸多安全问题。

1. IPv6 自身带来的多种安全威胁

1）IPv6 和 IPv4 传输数据报文的基本机制没有发生改变，IPv4 网络中除 IP 层以外的其他四层中面临的攻击，在 IPv6 网络中依然会存在。

2）IPv6 协议本身存在着以下安全隐患。

（1）攻击者可能利用 IPv6 报文的扩展报头（可选且有多种扩展报头），通过违背 IPv6 标准报文格式的畸形数据包或者特定格式的恶意数据包来攻击路由器和主机；

（2）攻击者还可能利用邻居发现协议发送错误的路由器宣告和重定向消息等让 IP 数据流向不确定的方向，进而达到拒绝服务、拦截和修改数据的目的；

（3）无状态地址自动分配可能使非授权用户很容易地接入和使用网络。

3）IPv6 的地址扩展虽然能够解决网络地址的紧缺问题，但是它的规模也为安全检测带来了难题，如海量地址的查询变得更加复杂等问题。

2. IPv4 向 IPv6 长期过渡共存引发的诸多安全隐患

虽然 IPv4 地址资源紧缺，但到目前为止 IPv6 网络还缺少商业需求，在未来很长一段时间内 IPv4 与 IPv6 将共存。同时，由于 IPv6 地址的扩展、IPv4 与 IPv6 间的非对称性、过渡形式的多样性等一系列问题，过渡期间安全防护将面临更