

## <<IPv6安全>>

### 图书基本信息

书名：<<IPv6安全>>

13位ISBN编号：9787115250445

10位ISBN编号：7115250448

出版时间：2011-5

出版时间：人民邮电出版社

作者：[美]霍格 等著,王玲芳 等译

页数：502

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<IPv6安全>>

### 内容概要

《IPv6安全》综述IPv6网络所面临的威胁，并提供应对这些威胁的解决方案，内容涵盖这些问题和当前的最佳实践。

书中首先讲述安全威胁，然后描述应对这些威胁的方式，列出所有的风险，并针对每种威胁指明存在的解决方案。

通过《IPv6安全》，读者将学习到攻击者可能用以攻破你的网络的技术以及如何使用Cisco的产品保护你的网络。

《IPv6安全》的目的是较深入地研究协议，并从一名安全实践人员的角度讨论协议细节。

书中涵盖理论知识，也同时给出实践例子。

《IPv6安全》适合负责网络安全的IT工作人员和在校学生阅读，另外，也可以作为从事网络安全的研究人员和学者的参考书。

<<IPv6安全>>

作者简介

作者:(美)Hogg

## &lt;&lt;IPv6安全&gt;&gt;

## 书籍目录

## 第1章 IPv6安全引言

- 1.1 重温IPv6
- 1.2 IPv6知识更新
- 1.3 IPv6弱点
- 1.4 黑客经验
- 1.5 IPv6安全缓解技术
- 1.6 小结
- 1.7 推荐读物和资料

## 第2章 IPv6协议安全弱点

- 2.1 IPv6协议首部
  - 2.1.1 ICMPv6
  - 2.1.2 多播安全
- 2.2 扩展首部威胁
  - 2.2.1 扩展首部综述
  - 2.2.2 扩展首部的弱点
  - 2.2.3 逐跳选项首部和目的地选项首部
  - 2.2.4 路由首部
  - 2.2.5 分段首部
  - 2.2.6 未知的选项首部
  - 2.2.7 上层首部
- 2.3 IPv6网络勘察
  - 2.3.1 扫描并评估目标
  - 2.3.2 加速扫描过程
  - 2.3.3 应对勘察攻击
- 2.4 三层和四层欺骗
- 2.5 小结
- 2.6 参考文献

## 第3章 IPv6 Internet安全

- 3.1 大型Internet威胁
  - 3.1.1 数据包泛洪
  - 3.1.2 Internet蠕虫
  - 3.1.3 分布式拒绝服务和机扑网(Botnets)
- 3.2 进/出过滤
  - 3.2.1 过滤IPv6流量
  - 3.2.2 对被分配地址的过滤
  - 3.2.3 虚假地址过滤
  - 3.2.4 虚假地址过滤挑战和过滤自动化
- 3.3 保障BGP会话安全
  - 3.3.1 显式配置的BGP对端
  - 3.3.2 使用BGP会话共享秘密
  - 3.3.3 利用一条IPSec隧道
  - 3.3.4 在BGP对端上使用环回地址
  - 3.3.5 在BGP数据包上控制存活时间(TTL)
  - 3.3.6 在对端关系接口上实施过滤
  - 3.3.7 使用链路本地对端关系

## &lt;&lt;IPv6安全&gt;&gt;

- 3.3.8 防止长的AS路径
- 3.3.9 限制接收到的前缀数量
- 3.3.10 防止包含私有AS号码的BGP更新
- 3.3.11 最大化BGP对端的可用性
- 3.3.12 对BGP邻居活动记录日志
- 3.3.13 保障IGP安全
- 3.3.14 保障BGP对端之间通信安全的极端措施
- 3.4 MPLS上的IPv6安全
  - 3.4.1 在PE路由器之间IPv4隧道上使用静态IPv6
  - 3.4.2 使用6PE
  - 3.4.3 使用6VPE产生支持IPv6的VRF
- 3.5 客户前端设备
- 3.6 前缀委派威胁
  - 3.6.1 SLAAC
  - 3.6.2 DHCPv6
- 3.7 多宿问题
- 3.8 小结
- 3.9 参考文献
- 第4章 IPv6边缘安全
  - 4.1 IPv6防火墙
    - 4.1.1 过滤IPv6未分配地址
    - 4.1.2 其他的过滤考虑
    - 4.1.3 防火墙和NAT
  - 4.2 Cisco IOS路由器ACL
    - 4.2.1 隐式IPv6 ACL规则
    - 4.2.2 Internet ACL范例
    - 4.2.3 IPv6反射性的ACL
  - 4.3 Cisco IOS防火墙
    - 4.3.1 配置IOS防火墙
    - 4.3.2 IOS防火墙范例
    - 4.3.3 IOS防火墙的IPv6端口到应用映射
  - 4.4 Cisco PIX/ASA/FWSM防火墙
    - 4.4.1 配置防火墙接口
    - 4.4.2 管理接入权限
    - 4.4.3 配置路由
    - 4.4.4 安全策略配置
    - 4.4.5 对象组策略配置
    - 4.4.6 分段保护
    - 4.4.7 检查流量统计信息
    - 4.4.8 邻居发现协议保护
  - 4.5 小结
  - 4.6 参考文献
- 第5章 局域网安全
  - 5.1 二层是重要的原因
  - 5.2 IPv6的ICMPv6二层弱点
    - 5.2.1 无状态地址自动配置问题
    - 5.2.2 邻居发现的问题

## &lt;&lt;IPv6安全&gt;&gt;

- 5.2.3 重复地址检测问题
  - 5.2.4 重定向问题
  - 5.3 ICMPv6协议保护
    - 5.3.1 安全邻居发现
    - 5.3.2 在Cisco IOS中实现CGA地址
    - 5.3.3 理解采用SEND的挑战
  - 5.4 ICMPv6攻击的网络检测
    - 5.4.1 检测伪造的RA消息
    - 5.4.2 检测NDP攻击
  - 5.5 针对ICMPv6攻击的网络应对措施
    - 5.5.1 Rafxid
    - 5.5.2 降低目标范围
    - 5.5.3 IETF工作
    - 5.5.4 扩展IPv4交换机的IPv6安全
  - 5.6 私有扩展地址的优劣
  - 5.7 DHCPv6的威胁和应对
    - 5.7.1 针对DHCPv6的威胁
    - 5.7.2 应对DHCPv6攻击
  - 5.8 点到点链路
  - 5.9 端点安全
  - 5.10 小结
  - 5.11 参考文献
- 第6章 加固IPv6网络设备
- 6.1 针对网络设备的威胁
  - 6.2 Cisco IOS版本
  - 6.3 禁止不必要的网络服务
  - 6.4 限制路由器访问
    - 6.4.1 物理访问安全
    - 6.4.2 保障控制台访问的安全
    - 6.4.3 保障口令的安全
    - 6.4.4 VTY端口访问控制
    - 6.4.5 路由器的AAA
    - 6.4.6 HTTP访问
  - 6.5 IPv6设备管理
    - 6.5.1 环回和Null接口
    - 6.5.2 管理接口
    - 6.5.3 保障SNMP通信的安全
  - 6.6 针对内部路由协议的威胁
    - 6.6.1 RIPng安全
    - 6.6.2 EIGRPv6安全
    - 6.6.3 IS-IS安全
    - 6.6.4 OSPF版本3安全
  - 6.7 第一跳冗余协议安全
    - 6.7.1 邻居不可达性检测
    - 6.7.2 HSRPv6
    - 6.7.3 GLBPv6
  - 6.8 控制资源

## &lt;&lt;IPv6安全&gt;&gt;

- 6.8.1 基础设施ACL
- 6.8.2 接收ACL
- 6.8.3 控制平面监控
- 6.9 QoS威胁
- 6.10 小结
- 6.11 参考文献
- 第7章 服务器和主机安全
  - 7.1 IPv6主机安全
    - 7.1.1 ICMPv6的主机处理
    - 7.1.2 侦听端口的服务
    - 7.1.3 检查邻居缓存
    - 7.1.4 检测不希望出现的隧道
    - 7.1.5 IPv6转发
    - 7.1.6 地址选择问题
  - 7.2 主机防火墙
    - 7.2.1 Microsoft Windows防火墙
    - 7.2.2 Linux防火墙
    - 7.2.3 BSD防火墙
    - 7.2.4 Sun Solaris
  - 7.3 采用Cisco安全代理6.0保障主机的安全
  - 7.4 小结
  - 7.5 参考文献
- 第8章 IPSec和SSL虚拟专网
  - 8.1 IPv6的IP安全
    - 8.1.1 IPSec扩展首部
    - 8.1.2 IPSec操作模式
    - 8.1.3 Internet密钥交换(IKE)
    - 8.1.4 IPsec和网络地址转换一起使用
    - 8.1.5 IPv6和IPSec
  - 8.2 主机到主机的IPSec
  - 8.3 站点到站点的IPSec配置
    - 8.3.1 IPv4之上的IPv6 IPSec例
    - 8.3.2 IPv6 IPSec示例
    - 8.3.3 动态多点VPN
  - 8.4 采用IPSec的远端访问
  - 8.5 SSL VPN
  - 8.6 小结
  - 8.7 参考文献
- 第9章 IPv6移动性安全
  - 9.1 移动IPv6操作
  - 9.2 MIPv6消息
    - 9.2.1 间接模式
    - 9.2.2 家乡代理地址确定
    - 9.2.3 直接模式
  - 9.3 与MIPv6有关的威胁
    - 9.3.1 保护移动设备软件
    - 9.3.2 伪造的家乡代理

## &lt;&lt;IPv6安全&gt;&gt;

- 9.3.3 移动媒介安全
- 9.3.4 中间人威胁
- 9.3.5 连接截获
- 9.3.6 伪造MN到CN绑定
- 9.3.7 DoS攻击
- 9.4 在MIPv6中使用IPSec
- 9.5 针对MIPv6的过滤
  - 9.5.1 CN处的过滤器
  - 9.5.2 在MN/异地链路处实施过滤
  - 9.5.3 在HA处实施过滤
- 9.6 其他IPv6移动性协议
  - 9.6.1 其他IETF移动IPv6协议
  - 9.6.2 网络移动性(NEMO)
  - 9.6.3 IEEE 802.16e
  - 9.6.4 移动Ad-Hoc网络
- 9.7 小结
- 9.8 参考文献
- 第10章 保障迁移机制的安全
  - 10.1 理解IPv4到IPv6的迁移技术
    - 10.1.1 双栈
    - 10.1.2 隧道
    - 10.1.3 协议转换
  - 10.2 实现双栈安全
    - 10.2.1 利用双栈环境
    - 10.2.2 保护双栈主机
  - 10.3 对隧道实施破坏
    - 10.3.1 安全的静态隧道
    - 10.3.2 保障动态隧道的安全
    - 10.3.3 保障6VPE的安全
  - 10.4 攻击NAT-PT
  - 10.5 针对IPv4网络的IPv6潜在威胁
  - 10.6 小结
  - 10.7 参考文献
- 第11章 安全监视
  - 11.1 管理和监视IPv6网络
    - 11.1.1 路由器接口性能
    - 11.1.2 设备性能监视
    - 11.1.3 路由器Syslog消息
    - 11.1.4 准确时间的益处
  - 11.2 管理IPv6隧道
  - 11.3 使用法医证据方法
  - 11.4 使用入侵检测和防御系统
    - 11.4.1 Cisco IPS版本6.1
    - 11.4.2 测试IPS签名
  - 11.5 采用CS-MARS管理安全信息
  - 11.6 管理安全配置
  - 11.7 小结



## <<IPv6安全>>

- 11.8 参考文献
- 第12章 IPv6安全结论
  - 12.1 比较IPv4和IPv6安全
    - 12.1.1 IPv4和IPv6之间的相似性
    - 12.1.2 IPv4和IPv6之间的差异
  - 12.2 变化的安全边缘
  - 12.3 生成一项IPv6安全策略
    - 12.3.1 网络边缘
    - 12.3.2 扩展首部
    - 12.3.3 LAN威胁
    - 12.3.4 主机和设备安全加固
    - 12.3.5 迁移机制
    - 12.3.6 IPSec
    - 12.3.7 安全管理
  - 12.4 保持警醒状态(On the Horizon)
  - 12.5 建议的合并列表
  - 12.6 小结
  - 12.7 参考文献

## 章节摘录

第1章 IPv6安全引言     Internet协议（IP）是使用最为广泛的通信协议。因为IP是一项最普遍的通信技术，所以它是数十万IT专业人士的关注焦点。因为这么多的人依赖该协议进行通信，所以通信的安全就是人们最关心的。好人和坏人都在进行IP上的安全研究，所有这些安全研究导致人们对IP进行修补和调整，原因是IP已经被在国际范围内部署。以事后诸葛亮的说法就是，在IP被广泛部署之前，如果给予这个协议的安全以较深入考虑的话，可能会更好。

本书为您提供IP的一个新版本，并关注其安全性，并给出在部署之前避免这些问题的指南建议。本章给出有关IP的下一版本（IPv6）的简短背景。您将认识到，在IPv6大规模部署之前，考虑IPv6的安全为什么是重要的。本章给出IPv6当前风险的回顾和其弱点的业界知识，以及可保障IPv6安全的常用方式。  
&hellip;&hellip;

#### 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>