> 华为ICT认证系列丛书

HUAWEI

强叔侃墙

华为防火墙技术漫谈

徐慧洋 白 杰 卢宏旺 编著

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

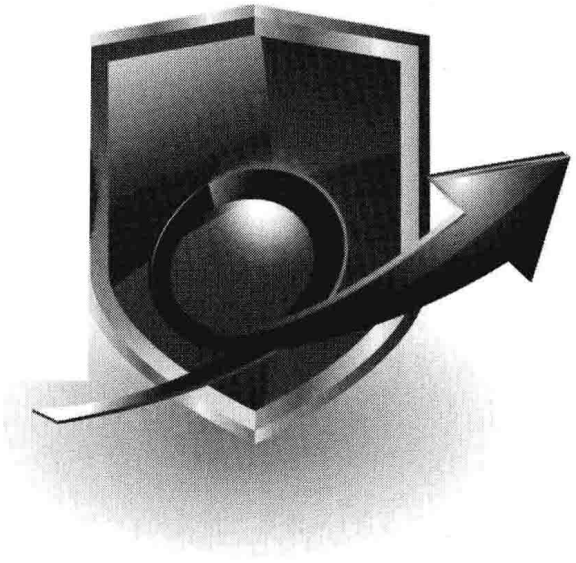
> 华为ICT认证系列丛书

HUAWEI

强叔侃墙

华为防火墙技术漫谈

徐慧洋 白 杰 卢宏旺 编著



人民邮电出版社

图书在版编目（CIP）数据

华为防火墙技术漫谈 / 徐慧洋，白杰，卢宏旺编著
. -- 北京 : 人民邮电出版社，2015.5
（华为ICT认证系列丛书）
ISBN 978-7-115-39076-9

Ⅰ. ①华… Ⅱ. ①徐… ②白… ③卢… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2015)第090956号

内 容 提 要

防火墙技术复杂，懂的人少，学的人有畏难心理。更令人困扰的是，目前市场上还没有一本系统介绍此类的书。

为此，华为策划了本书。本书深入介绍了华为防火墙的核心技术原理、应用场景及配置方法，并给出常见的实战案例，可以解决如下几个困扰大家已久的问题。

1．本书以防火墙核心技术为线索，内容覆盖了高端和中低端防火墙，以主流版本为例介绍配置。对于读者容易产生疑问的知识点，本书都有一一解答。所以本书可以帮助读者掌握华为防火墙产品的核心技术，而不是仅掌握某个型号或版本。

2．本书内容深度高于防火墙高级培训教材，原理讲解深入，有实验演示，有抓包分析，并能结合现网场景进行点评，可以解决当前高级培训教材内容不够深入的问题。

本书的原型是系列技术贴，部分内容在华为公司企业论坛“强叔侃墙”上发布过，大家可以先去了解一下，再决定是否购买。相关内容在论坛连载不足一年，累计点击量 25 万+，好评 1500+。我们在完善细节、扩展内容的基础上出版此书。可以说，“强叔”已然倾囊相授，希望本书能够不辱防火墙产品的重托，能够答谢广大“强粉”的厚爱。

◆ 编　　著　徐慧洋　白　杰　卢宏旺
责任编辑　李　静
责任印制　彭志环
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京昌平百善印刷厂印刷
◆ 开本：787×1092　1/16
印张：35.5　　2015 年 5 月第 1 版
字数：825 千字　　2015 年 5 月北京第 1 次印刷

定价：98.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

序

你了解网络安全吗？

你了解防火墙吗？

你了解防火墙的核心功能和技术要点吗？

很多小伙伴都反映安全产品很难学。为什么呢？概其原因就是交换路由理念早已深入人心，而防火墙设计思想大家接触很少；社会上的安全认证不够普及，厂商提供的产品培训材料数量不多、内容枯燥、晦涩难懂，难以吸引更多的数据通信工程师主动学习安全产品。在网络安全形势日益严峻的今天，安全已经是任何一个网络工程师都必须考虑的关键点。网络工程师急需既通俗又深入的学习教材，帮助自己恶补安全知识，本书的推出恰好抓住了这一点。华为防火墙产品领域的资深技术专家以“强叔”的名义，在华为企业技术论坛发表了系列技术贴“强叔侃墙”，以幽默、轻松的笔法系统地介绍了防火墙的相关知识和技术特点，好评如潮、粉丝云集。正如总编辑徐慧洋所写：“强叔侃墙”系列“恰如王阳明讲学，传递内功心法；又如诸葛武侯亲临，指点排兵布阵。文字诙谐风趣绝不照本宣科，核心技术深入挖掘绝不蜻蜓点水，现网场景演绎逻辑严密绝不简单堆砌”。

本人曾很幸运地每期拜读“强叔侃墙”连载贴，它让工作繁忙的我用较少的时间就能系统地学习安全领域的相关知识，使我有机会快速澄清和深入理解很多安全领域的概念和知识。在客户、经销商处也能经常听到大家聊“强叔侃墙”，大家都说“强叔侃墙”比手册讲得深入，却一点不枯燥。强叔以讲故事的方式让大家在不知不觉中就跟随故事情节深入到每个特性专题的细节，从字里行间就能够感受到强叔的丰富经验和良苦用心。

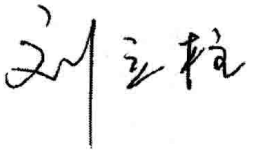
原以为技术贴演进到《强叔侃墙》电子专刊，强叔们的任务就光荣完成了。但是，2014 年底徐慧洋找到我，让我给准备正式出版的《华为防火墙技术漫谈（即原来的〈强叔侃墙〉）》写一篇序。这事给了我两个惊喜：一喜是本书为华为防火墙用户、工程师、学员送了一份新年大礼，弥补了防火墙产品多年的遗憾；二喜是本书的内容比原来的技术帖又丰富很多，不仅把强粉们提出来的问题和答案融合进去了，还补充了 DSVPN、多出口 NAT、各种特性的安全策略配置思路、防火墙旁路场景下的双机热备，以及第三代双机热备等许多内容，更加系统完整。

本书是一部传递防火墙技术精髓的武功秘籍，是学习华为防火墙首选的技术书籍。

学好技术需要坚持不懈、持之以恒，本书将会帮大家在技术专家的路上跑得更快、

更远。支持华为防火墙的朋友们，支持强叔吧。强叔不仅是防火墙的技术专家，还是大家的知心朋友！

最后，再次向本书的创作编著集体予以致敬，是你们的努力，让广大读者看到了这么好的技术专刊书籍。我衷心祝愿华为安全论坛英杰辈出，华为安全产品名满天下。



华为安全领域总经理

2015 年 2 月

前　言

读者对象

本书的目标读者为有数据通信基础，但需要系统学习安全技术的工程师，包括以下几类读者。

■ 华为防火墙的用户

本书可作为自学用书，帮助华为防火墙用户能够更快地熟悉防火墙，了解防火墙的关键技术原理，掌握防火墙部署技巧，找到解决防火墙问题的思路。

■ ICT 从业人员

本书可作为自学用书，帮助 ICT 从业人员能够更快地熟悉防火墙，了解防火墙的关键技术原理，掌握防火墙部署技巧，找到解决防火墙问题的思路。

本书可作为 HCIE 安全培训认证参考书，有助于 ICT 从业人员尽快通过华为认证，提升个人价值。

■ 高校学生

本书可作为计算机通信等相关专业学生的自学参考书。配合 eNSP 软件，可以帮助学生快速地熟悉防火墙的操作，使学生能更快地积累企业网络实践经验，在今后的职业生涯中有一个更好的起步。

■ 对信息和网络技术感兴趣的爱好者

本书可作为学习信息和网络技术的参考书籍，使爱好者了解华为的产品和技术特点，掌握华为产品和技术的应用，为其进一步的技术研究提供工具和指导。

主要内容

全书共分为两大部分，包括理论篇和实战篇。理论篇共包含 10 章，介绍了传统防火墙核心功能的原理、应用场景及配置方法；实战篇共包含 4 个实际案例，采用了先给出场景，再给配置，一边介绍配置一边点评的写作方式，帮助读者充分理解理论应用于实践时的技巧。

理论篇

第 1 章　基础知识

本章介绍了防火墙的定义、发展史和华为防火墙的系列产品，另外还介绍了安全区域的概念、原理、配置方法。安全区域是防火墙产品设计理念的代表，是大家必须先掌握的入门级概念。

第 2 章　安全策略

本章介绍安全策略相关的概念、安全策略发展历史、安全策略配置方法，另外还对 ASPF 的原理（包括 Server-map 表）及配置进行了详细的分析。掌握这一章是学习后面

所有特性的基础。

第 3 章　攻击防范

本章介绍了单包攻击、流量型攻击的概念，重点介绍了 SYN Flood、UDP Flood、DNS Flood、HTTP Flood 攻击、防御原理以及常用的防御方法。

第 4 章　NAT

本章内容分为三个层次。首先介绍了源 NAT（包括 NAT、NAPT、Easy-IP、Smart NAT、三元组 NAT）、NAT Server、NAT ALG 等 NAT 基本技术的原理、应用场景及配置方法；然后介绍了多出口场景下的源 NAT、NAT Server，以及双向 NAT 的应用场景及配置技巧；最后详细分析了 NAT 场景下黑洞路由的作用，并为感兴趣的读者爆料了 NAT 地址复用技术的内幕。

第 5 章　GRE&L2TP VPN

基于 Internet 的 VPN 技术五花八门、名目繁多，本书只介绍企业用户使用较多的几种技术。作为专门介绍 VPN 技术的这一章，先介绍 VPN 技术的分类、各自的特点以及几种技术的对比，然后再重点介绍 GRE 和 L2TP VPN 两种技术的原理、应用场景、配置方法。由于 VPN 场景下防火墙安全策略配置有些难度，所以在介绍完 VPN 技术之后再详细讲解一下安全策略的配置思路。

第 6 章　IPSec VPN

IPSec 是融合了加密、验证以及密钥管理算法的隧道技术，非常复杂。本章从最简单的手工方式 IPSec VPN 开始介绍，把 IPSec 涉及的各种概念、技术原理，应用场景及配置技巧，由浅入深地推送到读者面前。考虑到配置 IPSec 容易出现错误，为此本章最后的故障处理一节用于帮助用户调试 IPSec VPN。

第 7 章　DSVPN

DSVPN 是采用 GRE 协议实现的动态 VPN 技术，本章重点介绍了 DSVPN 中静态隧道和动态隧道的建立过程，让读者充分感受到 DSVPN 的优越之处和巧妙之处。

第 8 章　SSL VPN

SSL VPN 是基于 HTTPS 的 VPN，能为用户提供 4 大功能，包括文件共享、Web 代理、端口转发、网络扩展。本章依次介绍 SSL 握手以及 4 种功能的基本原理，最后讲解 SSL VPN 的用户管理（角色授权）方法和 4 种功能混用时的设计技巧。

第 9 章　双机热备

防火墙双机热备功能是由 VRRP、VGMP、HRP 三个协议共同实现的，这三个协议是如何配合实现防火墙双机热备功能的呢？为了让广大读者充分领悟其中的奥妙，本章从路由器双机原理开始介绍，说明防火墙的双机热备的高深之处，并且对每个协议的价值及原理按需展开，徐徐渐进，保证大家丝毫没有被填鸭之感。为了让大家能够自如应对复杂的现网场景，本章还特别描述了防火墙旁路场景下的双机热备，NAT 和 IPSec 场景下的双机热备流量分析及配置技巧。最后，本章概要介绍了第三代双机热备的改进点，文字不多但句句切中要害。

第 10 章　出口选路

出口网关是防火墙最常用的场景，此场景要求防火墙必须提供多出口选路的能力。本章介绍了就近选路、策略路由选路、智能选路、DNS 选路 4 种选路方式的配置技巧。

有路由知识基础的读者，掌握本章非常容易；缺少路由知识基础的读者也不用担心，防火墙用到的路由知识都比较简单，按本章给出的思路学习是最短路径。

实战篇

第 11 章　防火墙在校园网中的应用

本章介绍了防火墙作为网关部署在校园网出口的方法，为校内用户提供宽带服务，为校外用户提供内网服务器访问。

第 12 章　防火墙在广电网络中的应用

本章介绍了防火墙作为网关双机部署在广电网络的 Internet 出口的方法，为广电用户提供宽带服务，为内外网用户提供服务器托管业务。

第 13 章　防火墙在体育场馆网络中的应用

本章介绍了防火墙作为网关双机部署在体育场馆网络出口的方法，为内网用户提供上网服务；还介绍了防火墙双机透明部署在内部数据中心网络出口的方法，保护数据中心服务器安全。

第 14 章　防火墙在企业分支与总部 VPN 互通中的应用

本章介绍了防火墙作为网关部署在企业分支和总部网络出口的方法，为分支和总部之间建立 IPSec VPN，保证分支访问总部的数据在 Internet 上安全传输。

附录

A　报文处理流程

在理论篇中，强叔深入地介绍了安全策略、攻击防范、NAT、VPN、路由等功能的实现原理。读者学习之后会有豁然开朗的感觉，但开朗之后会有一个新的问题提出来——这些功能在防火墙内部的处理顺序是什么？处理顺序是否影响这些功能的配置？回答是肯定的。在多功能综合应用场景下，不了解防火墙报文处理流程的人非常容易遇到一个问题——面对长长的配置脚本找不出问题所在。所以，本章虽然是附录，但是它可以帮助你把前面的内容融会贯通，理清思路，在迷茫时刻能够发现蛛丝马迹、找到处理问题的方向。建议大家务必阅读！

B　证书浅析

IPSec VPN 和 SSL VPN 中都用到了数字证书，强叔在这两章中介绍的生成密钥和证书的方法完全不一样。大家不要太奇怪，看完本章就能找到答案。

C　强叔提问及答案

给出每章的强叔提问的答案。

鸣谢

本书由华为技术有限公司“交换机与企业通信产品线资料开发部防火墙与应用网关资料组”（俗称强叔团队）编写，由人民邮电出版社出版上市。在此期间，培训认证部的领导、资料部领导、防火墙与应用网关产品领导给予了很多的指导、支持和鼓励，人民邮电出版社的编辑给予了严格、细致的审核。在此，诚挚感谢相关领导的扶持，感谢人民邮电出版社各位编辑，以及各位编委的辛勤工作！

以下是本书主创人员的介绍。

徐慧洋，具有十多年数通产品经验，六年防火墙产品经验。曾创作了《USG 防火墙 IPSec 专题》、《华为防火墙双机热备 HCIE 培训胶片》、《轻松玩转 BGP》等广受欢迎的作品，《强叔侃墙》总编。

白杰，具有八年防火墙产品经验，堪称最熟悉华为防火墙的资料开发专家。参与创作《华为网络技术学习指南》，《强叔侃墙》技术贴的主编。

卢宏旺，具有七年华为防火墙产品经验，曾写作《华为防火墙双机热备 HCIE 实验手册》，《强叔拍案》主编，《小强和小艾台历》主创。

以下是参与本书编写和技术审校人员名单。

主　　编：徐慧洋、白　杰、卢宏旺

编委人员：徐慧洋、白　杰、卢宏旺、王　蕾、刘　水、韩　姣、闫广辉、金德胜、惠　博、余　杨、李苗苗、赵　欢

技术审校：徐慧洋、白　杰

参与本书编写和审稿的老师虽然有多年 ICT 从业经验，但因时间仓促，错漏之处在所难免，望读者不吝赐教，在此表示衷心的感谢。读者对于本书有任何意见和建议可以发送邮件至 xuhuiyang.xu@huawei.com，或直接登录华为企业论坛“强叔侃墙”汇总贴反馈。

目　录

理 论 篇