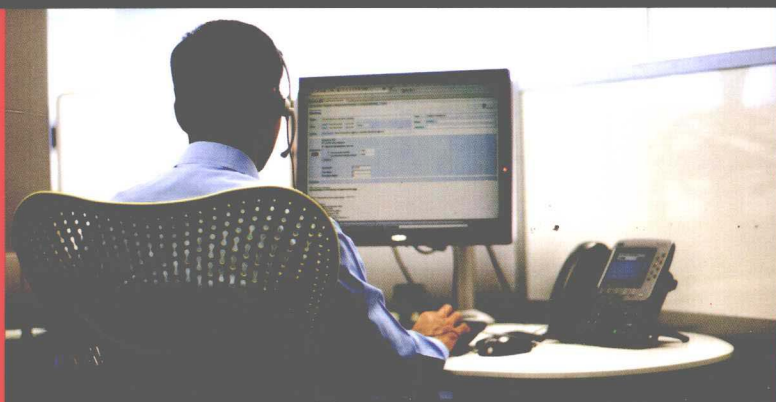




ciscopress.com



SECURITY

Cisco VPN 完全配置指南

The Complete Cisco VPN Configuration Guide

Use Cisco concentrators, routers, Cisco PIX and Cisco ASA security appliances, and remote access clients to build a complete VPN solution

[美] **Richard Deal** 著
姚军玲, CCIE #11470 译
郭稚晖

 **人民邮电出版社**
POSTS & TELECOM PRESS

ciscopress.com

Cisco VPN 完全配置指南

The Complete Cisco VPN Configuration Guide

〔美〕 **Richard Deal** 著
姚军玲, CCIE #11470 译
郭稚晖

人 民 邮 电 出 版 社

北 京

图书在版编目 (C I P) 数据

Cisco VPN完全配置指南 / (美) 迪尔 (Deal, R.) 著;
姚军玲, 郭稚晖译. — 2版. — 北京: 人民邮电出版社, 2012.10

ISBN 978-7-115-29375-6

I. ①C… II. ①迪… ②姚… ③郭… III. ①虚拟网
络—指南 IV. ①TP393.01-62

中国版本图书馆CIP数据核字(2012)第210393号

版 权 声 明

Richard Deal: The Complete Cisco VPN Configuration Guide (ISBN:1587052040)

Copyright © 2006 Cisco Systems, Inc.

Authorized translation from the English language edition published by Cisco Press.

All rights reserved.

本书中文简体字版由美国 Cisco Press 授权人民邮电出版社出版。未经出版者书面许可, 对本书任何部分不得以任何方式复制或抄袭。

版权所有, 侵权必究。

Cisco VPN 完全配置指南

- ◆ 著 [美] Richard Deal
- 译 姚军玲 CCIE#11470 郭稚晖
- 责任编辑 傅道坤
- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子邮件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
北京艺辉印刷有限公司印刷
- ◆ 开本: 787×1092 1/16
印张: 48.5
字数: 1 221 千字 2012 年 10 月第 2 版
印数: 6 001—8 500 册 2012 年 10 月北京第 1 次印刷

著作权合同登记号 图字: 01-2012-4892 号

ISBN 978-7-115-29375-6

定价: 118.00 元

读者服务热线: (010) 67132692 印装质量热线: (010) 67129223

反盗版热线: (010) 67171154

目 录

第一部分 VPN

第1章 VPN概述	3
1.1 流量问题	3
1.1.1 窃听攻击	3
1.1.2 伪装攻击	5
1.1.3 中间人攻击	5
1.2 VPN定义	7
1.2.1 VPN描述	8
1.2.2 VPN连接模式	9
1.2.3 VPN类型	11
1.2.4 VPN分类	14
1.3 VPN组件	15
1.3.1 验证	15
1.3.2 封装方法	17
1.3.3 数据加密	17
1.3.4 数据包的完整性	17
1.3.5 密钥管理	18
1.3.6 抗抵赖性	18
1.3.7 应用程序和协议的支持	18
1.3.8 地址管理	19
1.4 VPN设计	20
1.4.1 连接类型	20
1.4.2 VPN考虑	22
1.4.3 冗余	26
1.5 VPN实施	27
1.5.1 GRE	27
1.5.2 IPSec	28
1.5.3 PPTP	29
1.5.4 L2TP	29
1.5.5 MPLS	30
1.5.6 SSL	30
1.6 VPN: 选择解决方案	31
1.6.1 安全性	31
1.6.2 实施、管理和支持	31

1.6.3 高可靠性.....	32	3.3.4 阶段 2 的传输集.....	90
1.6.4 扩展性和灵活性.....	32	3.3.5 数据连接.....	91
1.6.5 费用.....	32	3.4 IPSec 流量和网络.....	92
1.7 总结.....	33	3.4.1 IPSec 和地址转换.....	92
第 2 章 VPN 技术.....	35	3.4.2 IPSec 和防火墙.....	94
2.1 密钥.....	35	3.4.3 使用 IPSec 的其他问题.....	96
2.1.1 密钥的使用.....	35	3.5 总结.....	97
2.1.2 对称密钥.....	36	第 4 章 PPTP 和 L2TP.....	99
2.1.3 非对称密钥.....	36	4.1 PPTP.....	99
2.2 加密.....	39	4.1.1 PPP 回顾.....	100
2.2.1 加密的过程.....	39	4.1.2 PPTP 组件.....	102
2.2.2 加密算法.....	39	4.1.3 PPTP 是如何工作的.....	102
2.3 数据包验证.....	41	4.1.4 使用 PPTP 的问题.....	107
2.3.1 数据包验证的实施.....	41	4.2 L2TP.....	109
2.3.2 数据包验证的使用.....	43	4.2.1 L2TP 概述.....	109
2.3.3 数据包验证的问题.....	45	4.2.2 L2TP 操作.....	110
2.4 密钥交换.....	46	4.2.3 L2TP/IPSec 和 PPTP 的 比较.....	113
2.4.1 密钥共享的困惑.....	46	4.3 总结.....	115
2.4.2 Diffie-HellMan (赫尔 曼算法).....	48	第 5 章 SSL VPN.....	117
2.4.3 密钥刷新.....	50	5.1 SSL 回顾.....	117
2.4.4 密钥交换方法的限制.....	50	5.1.1 SSL 客户实施.....	118
2.5 验证方法.....	50	5.1.2 SSL 保护.....	119
2.5.1 中间人攻击.....	51	5.1.3 SSL 组件.....	121
2.5.2 验证的解决方案.....	51	5.2 什么时候使用 SSL VPN.....	124
2.5.3 设备验证.....	52	5.2.1 SSL VPN 的好处.....	124
2.5.4 用户验证.....	64	5.2.2 SSL VPN 的缺点.....	125
2.6 总结.....	65	5.3 Cisco 的 WebVPN 解决方案.....	127
第 3 章 IPSec.....	67	5.3.1 VPN 3000 系列集中器.....	127
3.1 IPSec 标准.....	67	5.3.2 WebVPN 的操作.....	127
3.1.1 IETF RFC.....	68	5.3.3 Web 访问.....	128
3.1.2 IPSec 连接.....	72	5.3.4 网络浏览和文件管理 访问.....	129
3.1.3 构建连接的基本过程.....	74	5.3.5 应用程序访问和端口 转发.....	129
3.2 ISAKMP/IKE 阶段 1.....	75	5.3.6 E-mail 客户的访问.....	130
3.2.1 管理连接.....	76	5.4 总结.....	131
3.2.2 密钥交换协议: Diffie- Hellman.....	78	第二部分 集 中 器	
3.2.3 设备验证.....	78	第 6 章 集中器产品信息.....	135
3.2.4 远程访问额外的步骤.....	79	6.1 集中器的型号.....	136
3.3 ISAKMP/IKE 阶段 2.....	87		
3.3.1 ISAKMP/IKE 阶段 2 组件.....	87		
3.3.2 阶段 2 安全协议.....	87		
3.3.3 阶段 2 的连接模式.....	90		

6.1.1 3005 集中器	136	7.4 总结	209
6.1.2 3015 集中器	137	第 8 章 使用 PPTP、L2TP 和 WebVPN	
6.1.3 3020 集中器	138	实现集中器远程访问连接	211
6.1.4 3030 集中器	138	8.1 PPTP 和 L2TP 远程访问	211
6.1.5 3060 集中器	138	8.1.1 PPTP 和 L2TP 组配置	212
6.1.6 3080 集中器	138	8.1.2 PPTP 全局配置	213
6.1.7 集中器型号的比较	139	8.1.3 L2TP 全局配置	214
6.2 集中器的模块	139	8.2 WebVPN 远程访问	215
6.2.1 SEP 模块	140	8.2.1 HTTPS 访问	215
6.2.2 SEP 操作	140	8.2.2 WebVPN 全局配置	217
6.3 集中器的特性	140	8.2.3 组配置	227
6.3.1 版本 3.5 特性	141	8.2.4 SSL VPN 客户端 (SSL	
6.3.2 版本 3.6 特性	142	VPN 客户端, SVC)	232
6.3.3 版本 4.0 特性	143	8.2.5 用于 WebVPN 访问的	
6.3.4 版本 4.1 特性	144	Cisco 安全桌面	235
6.3.5 版本 4.7 特性	144	8.3 总结	246
6.4 介绍对集中器的访问	145	第 9 章 集中器站点到站点的连接	249
6.4.1 命令行接口	145	9.1 L2L 连接例子	249
6.4.2 图形用户接口	149	9.2 ISAKMP/IKE 阶段 1 准备	251
6.5 总结	157	9.2.1 现有的 IKE 策略	251
第 7 章 使用 IPSec 实现集中器的		9.2.2 IKE 策略屏幕	252
远程访问连接	159	9.3 增加站点到站点的连接	253
7.1 控制对集中器的远程访问会话	159	9.3.1 添加 L2L 会话	253
7.1.1 组的配置	159	9.3.2 完成 L2L 会话	263
7.1.2 用户配置	173	9.3.3 修改 L2L 会话	265
7.2 IPSec 远程访问	175	9.4 地址转换和 L2L 会话	265
7.2.1 ISAKMP/IKE 阶段 1:		9.4.1 介绍集中器地址转换的	
IKE 建议	175	能力	266
7.2.2 ISAKMP/IKE 阶段 1:		9.4.2 需要 L2L 地址转换的	
设备验证	178	例子	266
7.2.3 ISAKMP/IKE 阶段 1:		9.4.3 建立 L2L 地址转换规则	267
IPSec 标签	188	9.4.4 启动 L2L 地址转换	268
7.2.4 ISAKMP/IKE 阶段 1: Mode/		9.5 总结	269
Client Config 标签	190	第 10 章 集中器的管理	271
7.2.5 ISAKMP/IKE 阶段 1:		10.1 带宽管理	271
Client FW 标签	198	10.1.1 建立带宽策略	271
7.2.6 ISAKMP/IKE 阶段 2:		10.1.2 激活带宽策略	274
数据 SA	204	10.2 集中器上的路由选择	277
7.3 对于 IPSec 和 L2TP/IPSec 用户		10.2.1 静态路由选择	277
的网络访问控制 (NAC)	205	10.2.2 RIP 路由选择协议	279
7.3.1 对于 IPSec, NAC 的		10.2.3 OSPF 路由选择协议	280
全局配置	206	10.3 机箱冗余	282
7.3.2 NAC 的组配置	207		

10.3.1 VRRP	282	12.3.5 客户端的连接状态	352
10.3.2 VCA	286	12.3.6 断开连接	354
10.4 管理屏幕	290	12.4 VPN 客户端的 GUI 选项	354
10.4.1 Administrator Access (管理员访问)	291	12.4.1 Application Launcher (应用程序发起器)	355
10.4.2 集中器的升级	293	12.4.2 Windows Login Properties (Windows 登录属性)	355
10.4.3 文件管理	294	12.4.3 Automatic Initiation (自动发起)	355
10.5 总结	295	12.4.4 Stateful Firewall (状态防火墙)	358
第 11 章 验证和故障诊断与排除		12.5 VPN 客户端软件的更新	361
集中器的连接	297	12.5.1 集中器: 客户端更新	361
11.1 集中器的工具	297	12.5.2 对于 Windows 2000 和 XP 的 VPN 客户端的 自动更新的准备	363
11.1.1 系统状态	298	12.5.3 客户端的更新过程	364
11.1.2 VPN 会话	299	12.6 VPN 客户端的故障诊断与 排除	366
11.1.3 事件日志	302	12.6.1 日志查看器	366
11.1.4 监控统计信息屏幕	313	12.6.2 验证问题	368
11.2 故障诊断与排除问题	315	12.6.3 ISAKMP/IKE 策略不 匹配的问题	369
11.2.1 ISAKMP/IKE 阶段 1 的 问题	315	12.6.4 地址分配的故障诊断与 排除	370
11.2.2 ISAKMP/IKE 阶段 2 的 问题	320	12.6.5 分离隧道问题	372
11.3 总结	322	12.6.6 地址转换问题	375
		12.6.7 碎片问题	376
		12.6.8 Microsoft 的网络邻居问题	380
		12.7 总结	381
第三部分 客 户 端		第 13 章 Windows 软件客户端	383
第 12 章 Cisco VPN 软件客户端	327	13.1 Windows 客户端	383
12.1 Cisco VPN 客户端的概述	328	13.1.1 理解 Windows 客户端的 特性	384
12.1.1 Cisco VPN 客户端的 特性	328	13.1.2 验证 Windows 客户端是 可操作的	385
12.1.2 Cisco VPN 客户端的 安装	329	13.2 配置 Windows VPN 客户端	386
12.2 Cisco VPN 客户端接口	335	13.2.1 建立一个安全的策略	386
12.2.1 操作模式	335	13.2.2 需要使用 L2TP	390
12.2.2 喜好	337	13.2.3 建立一个 Microsoft 的 VPN 连接	391
12.2.3 高级模式工具栏按钮和 标签选项	337	13.3 配置 VPN 3000 集中器	398
12.3 IPSec 连接	338	13.3.1 IKE 建议	398
12.3.1 使用预共享密钥建立 连接	338		
12.3.2 使用证书建立连接	342		
12.3.3 其他的连接配置选项	349		
12.3.4 连接到一台 Easy VPN 服务器	349		

13.3.2 IPSec SA	398	第 16 章 路由器的 ISAKMP/ IKE	
13.3.3 组配置	400	阶段 1 连接	451
13.3.4 地址管理	401	16.1 IPSec 的准备	451
13.3.5 用户配置	401	16.1.1 收集信息	452
13.4 Microsoft 客户端的连接	401	16.1.2 允许 IPSec 的流量	452
13.4.1 连接到 VPN 网关	402	16.2 ISAKMP/IKE 阶段 1 策略	453
13.4.2 核实 PC 上的连接	403	16.2.1 启动 ISAKMP	453
13.4.3 核实集中器上的连接	403	16.2.2 建立策略	453
13.5 故障诊断与排除 VPN 的		16.2.3 与对等体协商策略	454
连接	404	16.2.4 启动 IKE 死亡对等体	
13.5.1 集中器故障诊断与排除		检测	455
工具	404	16.3 ISAKMP/IKE 阶段 1 设备	
13.5.2 Microsoft 的客户端故障		验证	456
诊断与排除工具	405	16.3.1 ISAKMP/IKE 身份类型	456
13.6 总结	409	16.3.2 预共享密钥	457
第 14 章 3002 硬件客户端	411	16.3.3 RSA 加密的随机数	458
14.1 3002 硬件客户端概览	411	16.3.4 数字证书和路由器的	
14.1.1 3002 的特性	412	注册	462
14.1.2 3002 型号	412	16.4 监控和管理管理连接	480
14.1.3 3002 的实施	413	16.4.1 查看 ISAKMP/IKE 阶段 1	
14.2 对于 3002 的初始访问	414	的连接	480
14.2.1 命令行接口	415	16.4.2 管理 ISAKMP/IKE 阶段 1	
14.2.2 图形用户接口	415	的连接	481
14.3 验证和连接选项	423	16.4.3 路由器作为证书授权	481
14.3.1 单元验证	423	16.4.4 步骤 1: 产生和导出	
14.3.2 额外的验证选项	424	RSA 密钥信息	482
14.4 连接模式	429	16.4.5 步骤 2: 启动 CA	485
14.4.1 客户模式	429	16.4.6 步骤 3: 定义额外的 CA	
14.4.2 网络扩展模式	429	参数	488
14.4.3 路由和反向路由注入	433	16.4.7 步骤 4: 处理申请请求	490
14.5 管理任务	435	16.4.8 步骤 5: 吊销身份证书	493
14.5.1 从公有接口上访问 3002	435	16.4.9 步骤 6: 配置一台服务器	
14.5.2 升级 3002	436	使其运行在 RA 的模式	494
14.6 总结	439	16.4.10 步骤 7: 备份一个 CA	495
第四部分 IOS 路由器		16.4.11 步骤 8: 恢复一个 CA	496
第 15 章 路由器产品信息	443	16.4.12 步骤 9: 清除 CA 服务	497
15.1 路由器实施场景	443	16.5 总结	498
15.1.1 L2L 和远程访问连接	443	第 17 章 路由器站点到站点连接	501
15.1.2 路由器的特殊能力	444	17.1 ISAKMP/IKE 阶段 2 配置	501
15.2 路由器产品概述	447	17.1.1 定义被保护的流量:	
15.3 总结	448	Crypto ACL	502
		17.1.2 定义保护方法: Transform	
		Set (传输集)	503

17.1.3 构建一个静态的 Crypto Map 条目	504	19.1 ISAKMP/IKE 阶段 1 连接	607
17.1.4 构建一个动态的 Crypto Map	511	19.1.1 阶段 1 命令的回顾	608
17.1.5 可区分的基于名字的 Crypto Map	518	19.1.2 show crypto isakmp sa 命令	608
17.2 查看和管理连接	520	19.1.3 debug crypto isakmp 命令	608
17.2.1 查看 IPSec 的数据 SA	520	19.1.4 debug crypto pki 命令	617
17.2.2 管理 IPSec 数据 SA	522	19.1.5 debug crypto engine 命令	618
17.3 站点到站点连接的问题	522	19.2 ISAKMP/IKE 阶段 2 连接	619
17.3.1 迁移到一个基于 IPSec 的设计	522	19.2.1 阶段 2 命令的回顾	619
17.3.2 过滤 IPSec 的流量	524	19.2.2 show crypto engine connection active 命令	620
17.3.3 地址转换和状态防火墙	526	19.2.3 show crypto ipsec sa 命令	620
17.3.4 非单播流量	528	19.2.4 debug crypto ipsec 命令	621
17.3.5 配置简化	534	19.3 新的 IPSec 故障诊断与排除特性	625
17.3.6 IPSec 冗余	536	19.3.1 IPSec VPN 监控特性	625
17.3.7 L2L 扩展性	551	19.3.2 清除 Crypto 会话	627
17.4 总结	570	19.3.3 无效的安全参数索引恢复特性	627
第 18 章 路由器远程访问连接	573	19.4 碎片问题	628
18.1 Easy VPN 服务器	574	19.4.1 碎片问题	629
18.1.1 Easy VPN 服务器的配置	574	19.4.2 碎片发现	630
18.1.2 VPN 组监控	582	19.4.3 碎片问题的解决方案	631
18.1.3 Easy VPN 服务器配置例子	582	19.5 总结	634
18.2 Easy VPN 远端	585	第五部分 PIX 防火墙	
18.2.1 Easy VPN 远端连接模式	585	第 20 章 PIX 和 ASA 产品信息	639
18.2.2 Easy VPN 远端配置	587	20.1 PIX 实施场景	639
18.2.3 Easy VPN 远端配置的例子	590	20.1.1 L2L 和远程访问连接	640
18.3 在同一路由器上的 IPSec 远程访问和 L2L 会话	592	20.1.2 PIX 和 ASA 的特殊能力	640
18.3.1 中心办公室路由器的配置	592	20.2 PIX 和 ASA 的特性和产品回顾	641
18.3.2 远程访问和 L2L 样例配置	595	20.2.1 PIX 和 ASA VPN 特性	641
18.4 WebVPN	597	20.2.2 PIX 型号	643
18.4.1 WebVPN 建立	598	20.2.3 ASA 型号	643
18.4.2 WebVPN 配置例子	603	20.3 总结	644
18.5 总结	604	第 21 章 PIX 和 ASA 站点到站点的连接	647
第 19 章 路由器连接的故障诊断与排除	607		

21.1 ISAKMP/IKE 阶段 1 管理连接	648
21.1.1 允许 IPSec 的流量	648
21.1.2 建立 ISAKMP	650
21.1.3 配置管理连接的策略	651
21.1.4 配置设备验证	652
21.2 ISAKMP/IKE 阶段 2 数据连接	660
21.2.1 指定被保护的流量	660
21.2.2 定义如何保护流量	661
21.2.3 构建 Crypto Map	661
21.2.4 激活一个 Crypto Map	664
21.2.5 数据连接管理命令	664
21.3 L2L 连接例子	665
21.3.1 FOS 6.3 L2L 的例子	666
21.3.2 FOS 7.0 L2L 的例子	668
21.4 总结	669
第 22 章 PIX 和 ASA 远程访问连接	673
22.1 6.x 对于 Easy VPN 服务器的支持	673
22.1.1 6.x 的 Easy VPN 服务器的配置	674
22.1.2 6.x 的 Easy VPN 服务器的例子	678
22.2 6.x 的 Easy VPN 远端支持	680
22.2.1 6.x 的 Easy VPN 远端配置	681
22.2.2 使用证书作为远程访问	682
22.2.3 核实您的 6.x 远端配置和连接	682
22.2.4 6.x 的 Easy VPN 远端设备的例子配置	684
22.3 对于 7.0 的 Easy VPN 服务器的支持	685
22.3.1 理解隧道组	686
22.3.2 定义组策略	686
22.3.3 建立隧道组	692
22.3.4 为 XAUTH 建立用户账号	696
22.3.5 远程访问会话的问题及在 7.0 中的解决方案	697
22.3.6 解释 7.0 的一台 Easy VPN 服务器配置的例子	702
22.4 总结	703
第 23 章 PIX 和 ASA 连接的故障诊断与排除	705
23.1 ISAKMP/IKE 阶段 1 连接	705
23.1.1 阶段 1 命令的回顾	705
23.1.2 show isakmp sa 命令	706
23.1.3 debug crypto isakmp 命令	707
23.1.4 debug crypto vpnclient 命令	714
23.2 ISAKMP/IKE 阶段 2 连接	716
23.2.1 阶段 2 命令的回顾	716
23.2.2 show crypto ipsec sa 命令	717
23.2.3 debug crypto ipsec 命令	719
23.3 总结	723
第六部分 案例研究	
第 24 章 案例研究	727
24.1 公司的概貌	727
24.1.1 总部办公室	729
24.1.2 区域办公室	731
24.1.3 分支办公室	732
24.1.4 远程访问用户	732
24.2 案例研究的配置	732
24.2.1 边缘路由器的配置	733
24.2.2 Internet 远程访问配置	739
24.2.3 主要园区无线的配置	749
24.3 总结	756



第一部分

VPN

第1章 VPN 概述

第2章 VPN 技术

第3章 IPSec

第4章 PPTP 和 L2TP

第5章 SSL VPN



第 1 章

VPN 概述

这一章介绍了虚拟专用网 (VPN) 的概念和为什么使用它们。我考察了业务量通过公网发送时产生的问题, 以及 VPN 如何做才可以保护这些流量。我介绍了 VPN 的连接方法、VPN 的类型、当使用 VPN 时要考虑的事情、VPN 的组件、VPN 的设计和问题、VPN 实施的例子和选择一个 VPN 实施类型时要考虑的问题。本书其他章节扩展了这里谈到的这些主题。

1.1 流量问题

VPN 最初开发的主要目的是处理将明文数据通过网络进行传输时的安全问题。明文数据指的是可以被任何人检查和理解的信息, 这包括源、目标和中间人。发送明文流量应用的例子包括 Telnet, 通过 FTP 或者 TFTP 的文件传输协议, 使用邮局协议 (POP) 或者简单邮件传输协议 (SMTP), 以及其他协议的电子邮件。不道德的个人, 例如黑客, 可以利用发送明文数据的应用程序来执行下面类型的攻击:

- 窃听;
- 伪装;
- 中间人。

每种类型的攻击都可以暴露您的数据和公司的资产, 使其处于不同的危险程度。下面的 3 小节更深入的讨论了这些攻击。

1.1.1 窃听攻击

针对明文数据的最常见的攻击类型是窃听 (eavesdropping)。在窃听攻击中, 当数据包通过两台设备传输时, 数据包的内容可以被人检查。某些类型的应用程序和协议易于受到窃听

攻击，包括 Telnet、POP、HTTP、TFTP、FTP、简单网络管理协议（SNMP）等。

在所有上述应用和协议中，用户名和密码之类的认证信息，都是在两台设备间以明文格式传送的，黑客可以使用这种信息来执行访问和实施其他类型的攻击。

注意：即使某些协议可能以明文的形式发送信息，在许多情况下，它们至少有最低限度的验证方法来使得在某人访问资源之前验证个人的身份。例如，Telnet、POP 和 SMTP 这些应用也考虑了认证问题，即使这些验证信息是以明文的形式发送的。实际上，这些协议初始不是为安全设计的，而是为了解决某些连接性问题。然而，自这些应用程序从 20 世纪 70 年代、80 年代和 90 年代初期发展以来，特别是 Internet 的使用激增，使得事情发生了改变。

一、窃听工具

通常情况下，一台协议分析仪可以用来检查（窃听）数据包。分析仪可以是基于硬件的解决方案或者是一台具有混杂网络接口卡（NIC）和相应软件的 PC 机。为了让这种类型的攻击奏效，攻击者必须对实际的源和目标设备之间的连接具有访问的能力。

主要有两种类别的协议分析仪：通用的和攻击型的。一台通用的协议分析仪能捕捉所有它看得见的数据包，并且通常是使用一种诊断工具来进行故障诊断与排除。市面上有许多基于软件的协议分析仪，采用免费软件就可以完成这一操作。

另一方面，攻击型协议分析仪是一台增强型的通用协议分析仪。攻击型的协议分析仪查看应用程序和协议的某些类型来寻找认证、金融和安全信息。一个攻击者将使用这些特定信息来执行其他类型的攻击。

二、窃听解决方案

敏感的信息包括信用卡信息、个人信息、社会保险号码、电话号码和地址、用户名和口令以及专利信息。因为许多协议和应用程序在传输敏感信息的时候是不安全的（他们将信息以明文的形式发送），所以保护信息非常必要。一种解决方案是利用令牌卡使用一次性口令（OTP）。这可以防止某些人使用协议分析仪来捕捉口令信息而执行访问攻击。然而，这种解决方案只对口令攻击有效；其他类型的在明文连接上传输的信息都不被保护。

对于公司来说，在电子商务环境下保护信用卡信息的最通常的解决方案是使用具有 SSL 加密的 HTTP（HTTPS）来加密特定用户的信息。对于合作伙伴的访问，通常采取的一种方式就是实施加密的 VPN。加密可以将明文的信息变成随机的字符串；只有目标设备可以解密这些信息。加密可以以下面的两种方法来实施：

- **链路加密**——整个数据帧（例如 PPP 或者 HDLC 帧）在两台设备之间加密；这用在直接连接的设备之间的点对点的连接上；
- **数据包的负荷加密**——只有数据包的负荷被加密，这种类型的加密可以在第 3 层的网络上路由，例如 Internet。

加密通常用于穿过公网的外部连接。然而，对于某些类型的敏感数据，您可能想在它穿过您的内联网时加密数据。在这两种解决方案中，您将会看到，数据包的负荷加密是 VPN 解决方案中的一种最常使用的方法。其原因是在许多情况下，数据必须传过多跳，因此数据包的负荷加密是最具有扩展性的：只需两台设备处理加密/解密的过程，而中间设备只是发送加密的数据。

1.1.2 伪装攻击

一个伪装攻击就是一个个体隐藏其身份，甚至会假冒别人的身份。在网络环境下，这是通过改变数据包中的源地址信息来实现的。在 TCP/IP 协议族中，这通常被称为欺骗 (spoofing)。使用欺骗的攻击者通常会把这种攻击和拒绝服务 (DoS) 攻击或者非授权访问攻击组合在一起。

一、伪装工具

不像窃听攻击，许多类型的工具可以用来实现伪装攻击。为了修改数据包中的源 IP 地址，需要一个特殊的数据包产生程序。这就让黑客能够指定数据包所用的源地址，而不是使用与黑客的 PC NIC 相关联的 IP 地址。

一个攻击者通常会试图使用一个授权的外部源地址来屏蔽数据包过滤器。当然，任何返回的流量都会返回到实际授权的外部地址，而不是返回到攻击者。为了看到返回的流量，攻击者将会把这种攻击和路由选择攻击结合起来，这就使得返回流量可以重定向到攻击者。为了实施一个简单的 DoS 攻击，攻击者试图使用一个内部的源地址，而数据包过滤器通常会允许它通过一种防火墙系统。

注意：在第 2 层的网络中，黑客可能使用 ARP 欺骗来将两台设备之间的流量重定向到黑客的设备。

二、伪装解决方案

当然，使用一个强壮的防火墙系统来限制进入到您的网络中的数据包的类型是必需的。然而，一个防火墙系统将允许流量是从授权的外部系统而来，即使它是 VPN 的流量。因此，某种类型的数据包的验证检查是必需的。例如，您需要决定数据包是否来自一个合法的源，而不是来自执行伪装攻击的黑客。

最通常的解决方案是使用一个数据包的完整性检查系统，它是通过散列函数来实施的。散列函数允许用户验证传输的数据包的源。因为散列函数使用具有共享密钥的单向散列，只有具有共享密钥的设备才能建立并验证散列值。VPN 中，最通常使用的散列函数是 MD5 和 SHA。

注意：数据包的验证在这章后面的 1.3.4 小节中还要讨论，而散列函数在第 2 章中将讨论。

1.1.3 中间人攻击

一个中间人攻击可以采取许多形式，包括下面最常用的两种：

- 会话回放攻击；
- 会话截获攻击。

使用会话回放攻击时，攻击者位于两台设备之间，捕捉来自会话中的数据包。攻击者将试图在以后使用捕捉到的数据包来回放（重新发送）它们。攻击者的目标就是使用相同的数据包来获取对远端系统的访问。在某些情况下，攻击者会改变数据包的内容来协助这一过程。

图 1-1 中的这幅图形解释了一个例子。在步骤 1 中，用户发送流量给真实的服务器。在

步骤 2 中, 攻击者截取了从用户到真实服务器的流量 (假设它是一个 Web 会话)。通常, 一个攻击者要么会用自己的源地址而不是真实的目标地址来仿冒 DNS 的回应包, 这也是一种伪装攻击, 要么与一种重路由选择攻击结合起来, 仿冒数据包。如果攻击者能够访问源和目标之间的链路, 攻击者可以很容易地使用协议分析仪来检查这个数据包。在这个例子中, 假设攻击者正在使用重定向攻击, 所有的流量都会发送给攻击者。攻击者伪装成真实的服务器, 而且发送响应给用户 PC, 甚至可能是恶意的 Java 或者 ActiveX 脚本, 来捕捉任意用户特定的敏感信息。在这个例子中, 攻击者会把用户原始的流量进行重定向, 并且发送响应给真正的目标, 如步骤 3 所示。

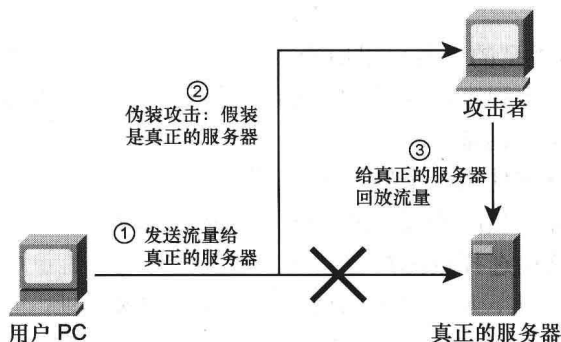


图 1-1 会话回放攻击

在一个会话截获攻击中, 攻击者试图将自己插入到已有的连接中, 接着控制两台设备之间的连接。图 1-2 解释了一个会话截获攻击。

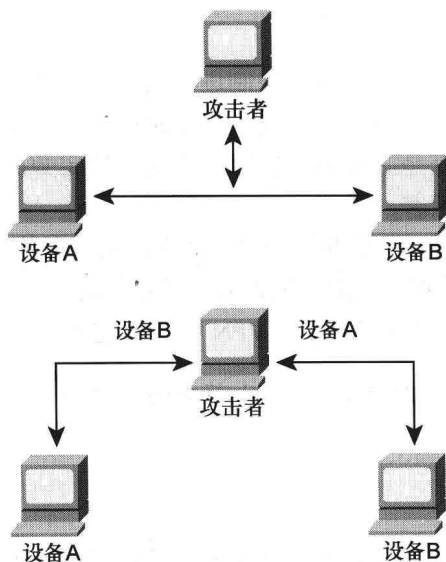


图 1-2 会话截获攻击

为了执行这种攻击, 攻击者不得不执行伪装, 攻击者假装是源和目标设备。而且, 攻击者必须对源和目标设备之间流动的数据包具有访问的能力。本质上, 这看起来像图 1-2 的上部分所示。

另一方面, 图 1-2 的下面部分更具有代表性, 表明会话截获攻击是如何发生的。在这个例子中, 当设备 A 发送流量给设备 B 时, 攻击者截取了流量并且假装是设备 B, 他给设备 A

发送响应，发送的信息类似于设备 B 发送的信息。从设备 A 的角度来看，他认为自己实际上是和设备 B 交互的。攻击者也使用同样的过程和设备 B 交互。当数据流在设备 A 和设备 B 之间来回流动时，攻击者将会执行数据操作攻击——修改两台设备之间的数据来实施实际的话截获攻击。攻击者使用这个过程来了解两台设备的信息，包括其安全弱点。

对于 UDP 和 ICMP 之类的协议，实施会话截获攻击对于黑客来说是非常简单的过程，这是因为没有相应的机制来定义连接是如何维护的。对于 TCP，特别是 TCP 的定序过程，会话截获则会难一些。序列号应当是随机的，对于黑客来说去猜测下一段的序列号是非常困难的事情。因此，截获 TCP 会话是一件很困难的事情。然而，并不是所有的 TCP 应用程序都使用随机的序列号。在许多情况下，基于现有连接中过去的序列号去猜测现有的序列号是一件非常容易的事情。一名有经验的黑客可以将自己插入到现有的 TCP 的连接中。当然，这不是一个简单的过程。黑客需要执行许多步骤并且使用某些复杂的工具来实施攻击。

一、中间人攻击工具

攻击者通常会使用一种攻击协议分析仪来捕捉上述所描述的两类攻击类型的数据包。使用会话回放攻击，黑客甚至可以使用 Java 或者 ActiveX 脚本来捕捉来自 Web 服务器会话的数据包。使用 TCP 会话截获攻击，攻击者需要某种类型的特殊 TCP 序列号猜测程序来成功地截获并且控制一个现有的 TCP 连接。

二、中间人攻击解决方案

对中间人攻击有几种解决方案。例如，为了防止 TCP 会话的截获，您应当有一个防火墙系统来随机化 TCP 的序列号，确保对于攻击者来说预测会话的下一个序列号成为几乎不可能的事情。Cisco PIX 安全设备和其他的可用设备可以执行这种功能。然而，攻击者可以使用其他方法，如前一小节所讨论的，来控制会话。

注意：TCP 序列号是 32 位的长度，提供了大约 20 亿个可能的组合，随机化序列号使得去猜测连接中的下一个序列号成为几乎是不可能的事情。

这种类型的问题的最好解决方案就是使用 VPN。VPN 提供了 3 种工具来抗击中间人攻击：

- 设备验证；
- 数据包完整性检查；
- 加密。

使用设备验证，您可以确保正在给您发送流量的设备就是一台授权的设备，而不是一台伪装的设备。使用数据包完整性检查，您可以确保发给您的数据包来自一个授权的源，而且没有被损害或者被假冒。使用加密，您可以确保中间人攻击设备不能去窃听两台设备之间正在共享的数据。这些主题将会在本章的 1.3 节中进行更多的讨论。

1.2 VPN 定义

我在前面的小节中曾经提到，VPN 可以用来处理某种类型的攻击。因此，问题是：什么