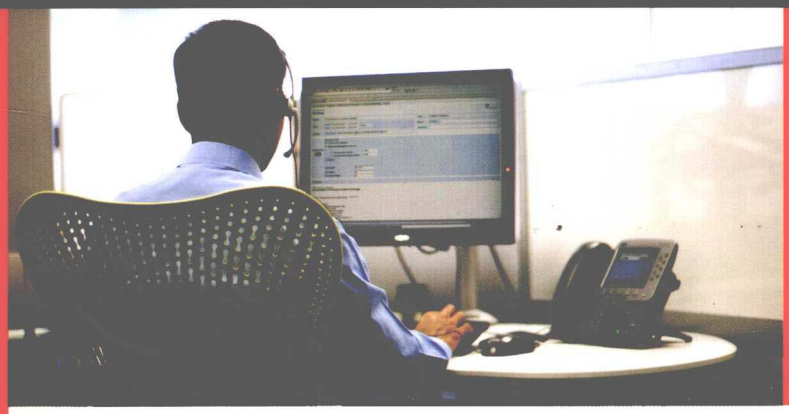
ciscopress.com



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（CIP）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



**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

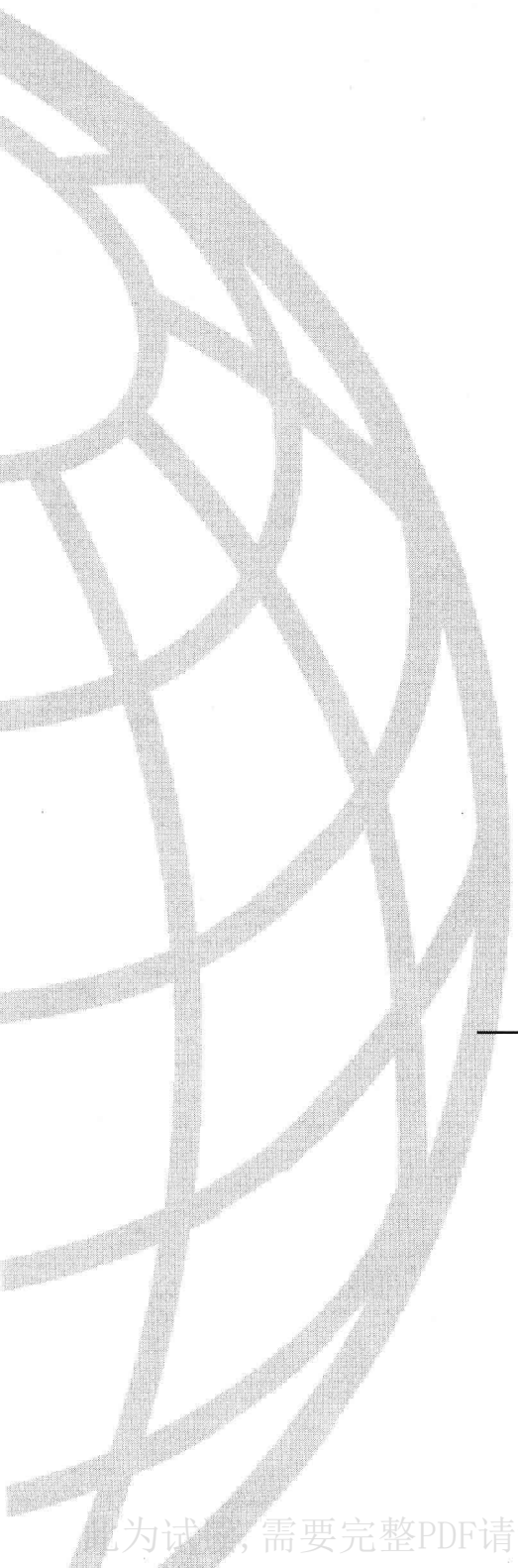
定价：118.00 元

**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

## 第六部分　案例研究



# 第一部分

# 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。

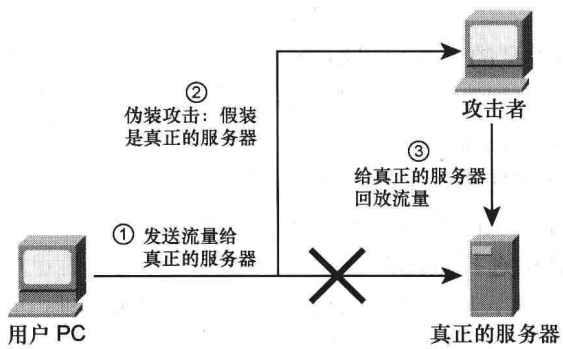



图 1-1 会话回放攻击

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。

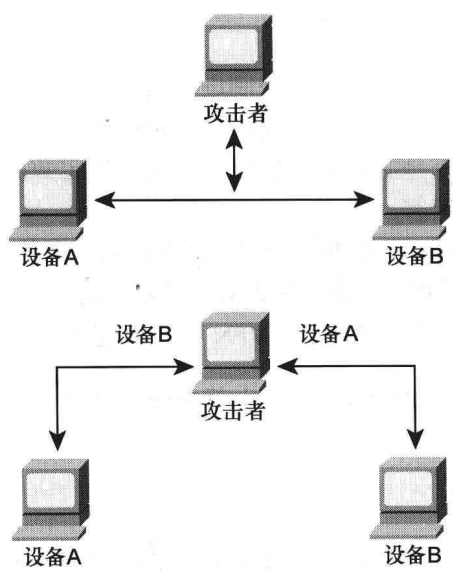



图 1-2 会话截获攻击

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会话截获攻击。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种攻击类型的数据包。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