

<<网络核心技术内幕>>

图书基本信息

书名：<<网络核心技术内幕>>

13位ISBN编号：9787900031716

10位ISBN编号：7900031715

出版时间：2000-02

出版时间：北京希望电子出版社

作者：（美）Cisco Systems公司

译者：希望图书创作室

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>

## <<网络核心技术内幕>>

### 内容概要

本书是21世纪网络工程师设计宝典系列之一，全面介绍了如何针对Cisco网络设备配置CiscoIOS安全特性。

通过CiscoIOS安全特性的配置，使我们的网络能够避免有意和无意的攻击，避免由于合法用户的误操作造成的数据丢失或泄露，从而保护网络系统的安全。

全书共分六部分：认证、授权及记帐（AAA）、安全服务器协议、流量过滤和防火墙、IP安全和加密技术、其它安全特性和附录。

认证提供了识别用户的方法，它在允许用户访问网络以及网络资源之前确认用户的身份；授权提供了远程访问控

制的方法，它包括一次性授权和对每个服务进行授权；记帐提供了收集和发送帐单信息、审计信息以及报告信息的手段。

安全服务器协议部分讲述了配置RADIUS、Kerberos、TACACS+、TACACS和扩展TACACS的方法、命令和过程。

流量过滤和防火墙部分讲述了如何配置网络设备进行流量过滤以及如何把网络设备配置成精细入微的防火墙。

IP安全与加密部分讲述配置Cisco加密技术、配置IPSec、配置证书认证机构（CA）的互操作能力以及配置Internet密钥交换的方法。

其它安全特性部分讲述了进一步加强网络安全的其它技术与措施。

本书内容极为丰富，技术新、指导性和实用性强，不但是从事网络规划和设计的广大工程人员、系统分析人员和网管人员的重要学习指导书，同时也是高等院校相关专业师生重要的自学、教学参考用书和社会相关领域培训班教材。

本书配套光盘内容包括与本书配套的电子书。

## <<网络核心技术内幕>>

### 书籍目录

(上)

引论：安全性概览

关于本书

建立有效的安全策略

识别网络风险以及Cisco IOS解决方案

关于Cisco IOS12.0参考库

使用 Cisco IOS 软件

第一部分认证授权及记帐AAA

第1章 AAA概要

AAA安全服务

从哪里开始

下面做什么

第2章 认证配置

AAA 认证方法列表

AAA认证方法

非 AAA 认证方法

认证示例

第3章 认证命令

aaa authentication arap

aaa authentication banner

aaa authentication enable default

aaa authentication fail-message

aaa authentication local-ovemde

aaa authentication login

aaa authentication nasi

aaa authentication password-prompt

aaa authentication ppp

aaa authentication username-prompt

aaa new-model

aaa processes

access-profile

arap authentication

clear ip trigger-authentication

ip trigger-authentication

(global configuration)

ip trigger-authentication

(interface configuration)

login authentication

login tacacs

nasi authentication

ppp authentication

ppp chap hostname

ppp chap password

ppp chap refuse

ppp chap wait

## <<网络核心技术内幕>>

ppp pap sent-username

ppp use-tacacs

show ip trigger-authentication

show ppp queues.

timeout login response

第4章 授权配置

AAA授权类型

授权的命名方法列表

AAA 授权方法

AAA 授权先决条件

AAA 授权配置

授权配置

使用命名方法列表配置AAA授权

关闭全局配置命令授权

反向Telnet授权

授权属性值对 (Attribute-ValuePair)

授权配置示例

第5章 授权命令

aaa authorization

aaa authorization config-commands

aaa authorization reverse-access

aaa new-model

authorizadon

ppp authorization

第6章 记帐配置

记帐的命名方法列表

AAA 记帐类型

AAA 记帐先决条件

AAA 记帐配置任务列表

使用命名方法列表配置AAA记帐

开放记帐

监督记帐

记帐属性值对 (Attribute-ValuePair)

记帐配置示例

第7章 记帐命令

aaa accounting

aaa accounting suppress null-username

aaa accounting update

accounting

ppp accounting

show accounting

第二部分 安全服务器协议

第8章 配置RADIUS

RADIUS 概览

RADIUS 操作

RADIUS 配置任务表

第9章 RADIUS命令

## <<网络核心技术内幕>>

aaa nas-port extended  
ip radius source-interfacr  
radius-server attribute nas-port extended  
radius-server configure-nas  
radius-server dead-time  
radius-server extended-portnames  
radius-server host  
radius-server host non-standard  
radius-server optional passwords  
radius-server key  
radius-server retransmit  
radius-server timeout.  
radius-server vsa send  
第10章 配置TACACS+  
TACACS+概览  
TACACS+操作  
TACACS+配置任务列表  
TACACS+配置示例  
第11章 配置TACACS和扩展TACACS  
TACACS 协议描述  
TACACS 和扩展TACACS配置任务列表  
TACACS 配置示例  
第12章 TACACS、扩展TACACS和TACACS+命令  
TACACS命令比较  
arap use-tacacs  
enable last-resort  
enable use-tacacs  
ip tacacs source-interface  
tacacs-server attempts  
tacacs-server authenticate  
tacacs-server directed-request  
tacacs-server extended  
tacacs-server host  
tacacs-server key  
tacacs-server last-resort  
tacacs-server login-timeout  
tacacs-server notify  
tacacs-server optional-passwords  
tacacs-server retransmit  
tacacs - servertimeout.  
第13章 配置kerberos  
Kerberos概览  
Kerberos客户机支持的操作  
Kerberos配置任务列表  
Kerberos配置示例  
第14章 kerberos命令  
clearkerberoscreds

## <<网络核心技术内幕>>

connect

kerberosclientsmandatory

kerberoscredentialsforward

kerberosinstancemap

kerberoslocal - realm

kerberospreauth

kerberosrealm

kerberosserver

kerberosrvtabentry

kerberosrvtabremote

keyconfig - key

showkerberoscreds

telnet

第三部分 流量过滤与防火墙

第15章 访问控制列表：概述与指导

关于访问控制列表

访问列表配置概述

查找访问列表的完整配置和命令信息

第16章 Cisco IOS防火墙概述

防火墙概述

Cisco IOS防火墙解决方案

创建专用的防火墙

配制防火墙的其它指导原则

第17章 配置锁定和密钥的安全性

（动态访问列表）

关于锁定和密钥

Cisco IOS版本11.1与早期版本的

兼容性

地址欺诈对锁定和密钥的威胁

使用锁定和密钥对路由器性能的影响

配置锁定和密钥的前提条件

配置锁定和密钥

检验锁定和密钥配置

锁定和密钥的维护

配置锁定和密钥示例

第18章 锁定和密钥命令

accessenable

access - template

clearaccess - template

showopaccounting

第19章 配置IP会话过滤

（反射访问列表）

关于反射访问列表

配置反射访问列表前的准备工作

配置反射访问列表

配置反射访问列表示例

第20章 反射访问列表命令

## <<网络核心技术内幕>>

eValuate

ipreflexive - listtimeout

permit ( reflexive )

第21章 配置TCP截取 ( 防止  
拒绝服务攻击 )

关于TCP截取

TCP截取的配置任务列表

TCP截取的配置范例

第22章 TCP截取命令

iptcpinterceptconnection - timeout

iptcpinterceptdrop - mode

iptcpinterceptfinrst - timeout

iptcpinterceptlist

iptcpinterceptmax - incompletehigh

iptcpinterceptmax - incompletelow

iptcpinterceptmode

iptcpinterceptone - minutehigh

iptcpinterceptone - minutelow

iptcpinterceptwatch - timeout

showtcpinterceptconnections

showtcpinterceptstatistics

第23章 配置基于上下文的访问控制

CBAC概述

CBAC配置的任务

CBAC配置示例

第24章 基于上下文的访问控制命令

ipinspectaudittrail

ipinspectdns - timeout

ipinspect ( interfaceconfiguration )

ipinspectmax - incompletehigh

iPinsPectmax - incompletelow

ipinspectname ( globalconfiguration )

ipinspectone - minutehigh

ipinspectone - minutelow

ipinspecttcpfinwait - time

ipinspecttcpidle - time

ipinspecttcpmax - incompletehost

ipinspecttcpsynwait - time

ipinspectudpodle - time

noipinspect

showiPinsPect

( 下 )

第四部分 IP安全和加密技术

第25章 IP安全加密技术概述

Cisco 加密技术

IPSec网络安全性

Internet密钥交换安全性协议

## <<网络核心技术内幕>>

身份认证互操作性

第26章 配置Cisco加密技术

为什么要加密

cisco 加密的实现

补充信息来源

准备工作：在配置加密之前

配置加密

GRE 隧道加密配置

VIP2 中 ESA 加密配置

对 Cisco 7200 系列路由器上的ESA

进行加密配置

定制加密（配置选项）

关闭加密

加密测试和故障排除

加密配置示例

第27章 Cisco加密技术命令

access-list (encryption)

clear crypto connection

crypto algorithm 40-bit-des

crypto algorithm des

crypto card

crypto card clear-latch

crypto cisco algorithm 40-bit-des

crypto cisco algorithm des

crypto cisco connections

crypto cisco entities

crypto cisco key-timeout

crypto cisco pregen-dh-pairs

crypto clear-latch

crypto esa

crypto gen-signature-keys

crypto key-exchange

crypto key exchange dss.

crypto key exchange dss passive

crypto key-exchange passive

crypto key generate dss

crypto key pubkey-chain dss

crypto key-timeout

crypto key zeroize dss

crypto map(global configuraion)

crypto map(nterface configurat'on)

crypto pregen-dh-pairs

crypto public-key

crypto sdu connections

crypto sdu entities

crypto zeroize

deny

## &lt;&lt;网络核心技术内幕&gt;&gt;

ip access-list extended(Cencryption)  
match address  
permit.  
set alonhgm 40-bit-des  
set algorithm des  
setpeer  
show crypto algorithms  
show crypto card.  
show crypto cisco algorithms  
show crypto cisco connections  
show crypto cisco key-timeout  
show crypto cisco pregen-dh-pairs  
show crypto connections  
show crypto engine brief  
show crypto engine configuration  
show crypto engine connections active  
show crypto engine connections  
dropped-packets  
show crypto key mypubkey dss  
show crypto key pubkey-chain dss  
show crypto key-timeout  
show crypto map  
show crypto mypubkey  
show crypto pregen-dh-pairs  
show crypto pubkey  
show crypto pubkey name  
show crypto pubkey serial  
test crypto initiate-session

第28章 配置IPSec网络安全  
IPSec概述  
IPSec 配置任务列表  
IPSec 配置示例

第29章 IPSec网络安全性命令  
clear crypto sa  
crypto dynamic-map  
crypto ipsec security-association lifetime  
crypto ipsec transform-set  
cryptomap (globalconfiguration)  
cryptomap (interfaceconfiguration)  
crypto map local-address  
initialization-vector size  
match address  
mode  
set prs  
set security-association level per-host  
set security-association lifetime  
set session-key

## <<网络核心技术内幕>>

set transform-set.  
show crypto ipsec sa  
show crypto ipsec security-association  
lifetime  
show crypto ipsec transform-set  
show crypto dynamic-map  
show crypto map  
第30章 配置身份证互操作性  
CA互操作性概述  
证证机构概述  
CA互操作性配置任务列表  
下面要做什么  
CA 互操作性配置示例  
第31章 身份认证互操作性命令  
certificate  
crl optional  
crypto ca authenticate  
crypto ca certificate chain  
crypto ca certificate query  
crypto ca crl request  
crypto ca enroll.  
crypto ca identity  
crypto key generate rsa  
crypto key zeroize rsa  
enrollment mode ra  
enrollment retry-count  
enrollment retry-period  
enrollment url  
query url  
show crypto ca certificates  
第32章 配置Internet密钥交换  
安全协方  
IKE根本要  
IKE 配置任务列表  
下面做什么  
IKE 配置示例  
第33章 Internet密钥交换  
安全协议命令  
address  
addressed-key  
authentication^(IKE policy)  
clear crypto isakmp  
crypto isakmp enable  
crypto isakmp identity  
crypto isakmp key  
crypto isakmp policy  
crypto key generate rsa

## &lt;&lt;网络核心技术内幕&gt;&gt;

crypto key pubkey-chain rsa  
encryption(IKE policy)  
group(IKE policy)  
hash(IKE policy)  
key-string.  
lifetimeIKE policy)  
named-key  
show crypto isakmp policy  
show crypto isakmp sa  
show crypto key mypubkey rsa  
show crypto key pubkey-chain rsa  
第五部分 其它安全特性  
第34章 配置口令和特权  
保护到特权EXEC命令的访问  
加密口令  
配置多重特权级别  
恢复丢失的有效口令  
恢复丢失的有效口令  
配置标识支持  
口令矣特权配置示例  
第35章 口令和特权命令  
enable  
enable password  
enable secret  
ip identd  
password  
privilege level (global)  
privilege level (line)  
service password-encryption  
show privilege  
username  
第36章 邻接路由器认证：概要及方略  
邻接认证的优点  
使用邻接认证的协议  
何时配置邻接认证  
邻接认证工作原理  
密钥管理（密钥链）  
第37章 配置IP安全选项  
配置基本IP安全选项  
配置扩展IP安全选项  
配置DNSIX审计跟踪功能  
IPSO配置示例  
第38章 IP 安全选项命令  
dnsix-dmdp retries  
dnsix-nat authorized-redirectation  
dnsix-nat primary  
dnsix-nat secondary

<<网络核心技术内幕>>

dnsix-nat source  
dnsix-nat transmit-count  
ip security add.  
ip security aes0  
ip security dedicated  
ip security eso-info  
ip security eso-max  
ip security eso-min  
ip security extended-allowed  
ip security first  
ip security ignore-authorities  
ip security implicit-labelling  
ip security multilevel  
ip security reserved-allowed  
ip security strip  
show dnsix

第六部分 附录

附录ARADIUS属性

所支持的RADIUS属性

RADIUS属性完整列表

附录8TACACS + 属性值对

TACACS + 属性值 (AV) 对

TACACS + 记帐属性值 (AV) 对

<<网络核心技术内幕>>

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>