
A

AAA

- configuring [3-7](#)
- support for [1-6](#)

abbreviating commands [1-25](#)

access control

- example [3-11](#)
- features [1-6](#)
- services [3-13](#)

access control lists

See ACLs

access modes [1-23](#)

ACLs

- applying to object groups [3-23](#)
- downloading [3-16](#)
- ICMP [2-12](#)
- IPSec [6-15](#)
- named [3-17](#)
- TurboACL
 - configuring [3-14](#)
 - description [1-7](#)

activation keys

- entering new [11-2](#)

ActiveX controls

- blocking [1-9](#)

Adaptive Security Algorithm

See ASA

addresses

- dynamic IP [8-1](#)
- global [2-11](#)
- IP [2-3](#)
- IP classes [2-4](#)

Address Resolution Protocol

See ARP

address translation

See NAT
See PAT

AH

- configuring [6-23](#)
- standard [E-1](#)

application inspection

- configuring [4-1 to 4-23](#)
- feature [1-10](#)

ARP

- clearing [2-2](#)
- failover [10-2](#)
- packet capture, example [9-28](#)

ASA [1-3, 4-1](#)

attacks

protection from [1-8](#)

authentication, accounting, and authorization

See AAA

Authentication Header

See AH

Auto-Update

- configuring [9-22 to 9-24](#)
- description [1-20](#)

B

backing up configurations [1-25](#)

Baltimore Technologies

CA server support [6-9](#)

blocking

ActiveX controls [1-9](#)

- Java applets [1-9](#)
- boot diskette
 - creating [11-12](#)
- broadcasts
 - See multicasts
- buffer usage
 - SNMP [9-32](#)

C

CA

- configuring in-house [7-13](#)
- configuring VeriSign [7-7](#)
- CRs. and [6-8](#)
- defined [1-16](#)
- public key cryptography [6-8](#)
- revoked certificates [6-8](#)
- supported servers [6-9](#)
- validating signature [6-8](#)

cable-based failover [10-3 to 10-8](#)

- FAQ [10-22](#)

cable status [10-1](#)

capturing packets

- feature [1-20](#)
- procedure [9-25](#)

CBC [E-2](#)

certificate enrollment protocol [6-9](#)

Certificate Revocation Lists

- See CRLs

certification authority

- See CA

Challenge Handshake Authentication Protocol

- See CHAP

CHAP [8-39](#)

Cipher Block Chaining

- See CBC

Cisco CallManager [4-12](#)

Cisco Intrusion Detection System

- See IDS

- Cisco IOS CLI [1-23](#)
- Cisco IP Phones
 - application inspection [4-12](#)
 - with DHCP [5-10](#)
- Cisco Secure Intrusion Detection System
 - See IDS
- Cisco Secure VPN Client
 - configuring [8-19 to 8-24](#)
 - using with Telnet [9-17](#)
- Cisco VPN 3000 Client
 - configuring [8-18](#)
 - downloading network parameters to [8-8](#)
 - using Telnet to outside interface [9-17](#)
- Cisco Works for Windows [9-35](#)
- CLI
 - abbreviating commands [1-25](#)
 - configuration mode [1-24](#)
 - editing with [1-25](#)
 - paging [1-26](#)
 - using PIX Firewall [1-23](#)
- client mode
 - configuring [5-2](#)
 - description [5-1](#)
- clients
 - Cisco Secure VPN Client [8-22](#)
 - Cisco VPN 3000 Client [8-18](#)
 - dynamic address assignment [8-1](#)
 - Easy VPN Remote device [5-1](#)
 - remote VPN [8-4](#)
 - using PIX Firewall as [1-17](#)
 - VPN [1-17](#)
 - Windows 2000 [8-34](#)
- clock, system [9-14](#)
- Command Authorization [9-5 to 9-6](#)
 - caution when using [9-5](#)
 - description [1-19](#)
 - recovering from lockout [9-9](#)
- command line interface
 - See CLI

- commands
 - command line editing [1-26](#)
 - command output paging [1-26](#)
 - configuring privilege levels [9-1 to 9-2](#)
 - creating comments [1-26](#)
 - displaying [1-26](#)
- compiling MIBs [9-35](#)
- conduits [1-7](#)
- Configurable Proxy Pinging
 - description [1-13](#)
- configuration examples
 - See examples
- configuration mode [1-24](#)
- configurations [1-26](#)
 - backing up [1-25](#)
 - comments [1-26](#)
 - copying with HTTP [11-5](#)
 - maximum size [1-26](#)
 - saving [2-15](#)
- connection states [1-3](#)
- connectivity
 - inbound [3-2](#)
 - outbound [3-4](#)
 - testing [2-12](#)
- converting from Private Link to IPSec [F-1](#)
- copying
 - configurations [11-5](#)
 - software [11-5](#)
- CPU utilization
 - SNMP [9-33](#)
- CRLs
 - time restrictions [6-9](#)
- crypto maps
 - applying to interfaces [6-14](#)
 - entries [6-13](#)
 - load sharing [6-24](#)
 - See also dynamic crypto maps
- CU-SeeMe application inspection [4-17](#)
- cut-through proxy [1-6](#)

D

- database application inspection [4-19](#)
- Data Encryption Standard
 - See DES
- debugging
 - IPSec [8-38](#)
 - SMR [2-31](#)
- default configurations [1-27](#)
- default routes [2-1](#)
- demilitarized zone
 - See DMZ
- denial of service attacks
 - protection from [1-8](#)
- DES
 - description [E-2](#)
 - IKE policy keywords (table) [6-3](#)
- DHCP
 - client [1-18, 5-11](#)
 - server [5-7](#)
- DHCP clients [1-18, 5-11](#)
 - default route [5-11](#)
 - PAT global address [5-11](#)
- DHCP leases
 - renewing [5-12](#)
 - viewing [5-12](#)
- DHCP servers [1-18, 5-7](#)
 - configuring [5-8](#)
 - with Cisco IP Phones [5-10](#)
- Diffie-Hellman [E-2](#)
- directory application inspection [4-19](#)
- DMZ
 - configuration example [2-20](#)
- DNS
 - application inspection [4-7](#)
 - inbound access [3-3](#)
 - protection from attacks [1-9](#)
- downgrading software [11-14](#)
- downloading

- ACLs [3-16](#)
 - IP addresses to VPN Clients [8-4](#)
 - network parameters to Cisco VPN 3000 Client [8-8](#)
 - dynamic crypto maps
 - adding to crypto maps [6-20](#)
 - entries [6-20](#)
 - referencing [6-20](#)
 - See also crypto maps [6-21](#)
 - sets [6-20](#)
 - Dynamic Host Configuration Protocol
 - See DHCP clients
 - See DHCP leases
 - See DHCP servers
 - dynamic IP address assignment [8-6](#)
 - dynamic IP addresses
 - assigning with IKE Mode Config [8-6](#)
 - dynamic NAT [2-9](#)
 - dynamic PAT [2-9](#)
-
- E**
- Easy VPN Remote device
 - configuring [5-1 to 5-3](#)
 - description [1-17](#)
 - Easy VPN Server
 - identifying [5-2](#)
 - using PIX Firewall with [5-1](#)
 - editing command lines [1-26](#)
 - EIGRP
 - not supported [B-2](#)
 - Encapsulating Security Payload
 - See ESP
 - Enhanced Interior Gateway Routing Protocol
 - See EIGRP
 - Entrust VPN Connector CA [7-14](#)
 - ESP
 - configuring [6-24](#)
 - standard [E-1](#)
 - examples
 - access control [3-11](#)
 - crypto maps [6-16](#)
 - IKE Mode Config [8-19](#)
 - IPSec with manual keys [7-25](#)
 - outside NAT [2-25](#)
 - outside NAT with overlapping networks [2-26](#)
 - packet capture [9-27](#)
 - port redirection [3-5](#)
 - pre-shared keys [7-2](#)
 - RADIUS authorization [8-8](#)
 - three interfaces with NAT and PAT [2-21](#)
 - three interfaces without NAT [2-20](#)
 - two interfaces with NAT and PAT [2-18](#)
 - two interfaces without NAT [2-15](#)
 - VeriSign CA [7-7](#)
 - VPN with manual keys [7-25](#)
 - wildcard pre-shared key [8-19](#)
 - Windows 2000 VPN client [8-35](#)
 - Xauth [8-19](#)
 - Extended Authentication
 - see Xauth
-
- F**
- factory defaults
 - See default configurations [1-27](#)
 - failover
 - cable status [10-1](#)
 - configuring [10-1 to 10-30](#)
 - failures [10-23](#)
 - flags [10-1](#)
 - interface tests [10-19](#)
 - models supporting [1-22](#)
 - Stateful Failover [10-20](#)
 - syslog messages [10-22](#)
 - syslog messages, SNMP [9-32](#)
 - See also cable-based failover
 - See also LAN-based failover
 - See also Stateful Failover

File Transfer Protocol

See FTP

filtering

ActiveX controls [1-9](#)Java applets [1-9](#)servers supported [1-9](#)URLs [1-9](#)

fixup

See application inspection

flags

failover [10-1](#)Flood Defender [1-8](#)Flood Guard [1-8](#)FragGuard [1-9](#)

FTP

application inspection [4-6](#)downloading software using [11-9](#)logging [1-21](#)packet capture, example [9-28](#)redirecting [3-6](#)secondary ports [1-11](#)full duplex [2-4, 2-5](#)**G**gateway addresses [2-6](#)generating RSA keys [6-10](#)

global addresses

specifying [2-11](#)

global lifetimes

changing [6-17](#)**H**H.245 tunneling [4-13](#)H.323 [4-13](#)changing default port assignments [4-6](#)support for [1-12](#)

hardware clients

See Easy VPN Remote device

using in SOHO networks [5-1](#)

hardware speed

requirements for Stateful Failover [2-4](#)help, command line [1-27](#)

home offices

See SOHO networks

HTTP

application inspection [4-8](#)copying configurations [11-5](#)copying software [11-5](#)filtering [1-9, 3-29](#)packet capture, example [9-27](#)redirecting [3-6](#)server access [3-1](#)HyperTerminal, configuring [11-6](#)

Hypertext Translation Protocol

See HTTP

IANA URL [D-5](#)

ICMP

application inspection [4-23](#)Configurable Proxy Pinging [1-13](#)configuring object groups [3-24](#)message reassembly [1-9](#)testing connectivity [2-12](#)testing default routes [2-14](#)

ICMP-type object groups

configuring [3-24](#)

IDS

support for [1-22](#)using [9-29 to 9-31](#)

IGMP

support for [1-14](#)

IKE

benefits [6-2](#)

- creating policies [6-4](#)
 - description [1-15](#)
 - disabling [6-6](#)
 - policy parameters [6-3](#)
 - policy priority numbers [6-4](#)
 - remote VPN clients [8-4](#)
 - using with pre-shared keys [6-6](#)
 - Xauth [8-2, 8-3, 8-16, 8-21](#)
 - IKE Mode Config
 - configuring [8-6](#)
 - exceptions for security gateways [8-5](#)
 - gateway initiation [8-5](#)
 - initiating [8-5](#)
 - standard [E-2](#)
 - types [8-5](#)
 - IKE Mode Configuration
 - See IKE Mode Config
 - ILS
 - application inspection [4-21](#)
 - feature [1-13](#)
 - images, software
 - See also software images
 - upgrading [1-22, 11-5 to 11-16](#)
 - inbound connectivity [3-2](#)
 - in-house CA, configuring [7-13](#)
 - interfaces
 - assigning names [2-4](#)
 - changing names [2-5](#)
 - configuring [2-3](#)
 - global address [2-11](#)
 - perimeter [2-10](#)
 - security levels and [1-4](#)
 - speed [2-4](#)
 - Internet Group Management Protocol
 - See IGMP
 - Internet Key Exchange
 - See IKE
 - Internet Locator Service
 - See ILS
 - Internet Security Association and Key Management Protocol
 - See ISAKMP
 - Intrusion Detection System
 - See IDS
 - IOS
 - See Cisco IOS CLI
 - IP
 - datagrams [8-32](#)
 - viewing configuration [2-4](#)
 - IP addresses
 - configuring
 - address, IP addresses [2-3](#)
 - IP Phones
 - See Cisco IP Phones
 - IPSec
 - ACLs [6-15](#)
 - clearing SAs [6-26](#)
 - configuring [6-12](#)
 - converting from Private Link [F-1 to F-7](#)
 - crypto map entries [6-13](#)
 - crypto map load sharing [6-24](#)
 - defined [1-15](#)
 - enabling debug [8-38](#)
 - manual [6-16](#)
 - manual SAs using pre-shared keys [6-12](#)
 - modes [8-32](#)
 - proxies [8-32](#)
 - viewing configuration [6-25](#)
 - viewing information [6-25](#)
 - IP Security Protocol
 - See IPSec
 - IP spoofing
 - protection from [1-8](#)
 - ISAKMP [E-2](#)
-
- J**
- Java applets

filtering [1-9, 3-27](#)

L

L2TP

configuring [8-33](#)
 configuring Windows 2000 client [8-34, 8-37](#)
 description [8-31](#)
 transport mode [8-33](#)

LAN-based failover [10-8 to 10-15](#)

advantage [10-24](#)
 changing from cable-based failover [10-13](#)
 configuring [10-8](#)
 example [10-28](#)
 FAQ [10-24](#)

LAN-to-LAN VPNs

See site-to-site VPNs

Layer 2 Tunneling Protocol

See L2TP [8-31](#)

LDAP

application inspection [4-21](#)
 ILS [1-13](#)

lease

releasing DHCP [5-12](#)
 renewing DHCP [5-12](#)

licenses, software

requirements for Stateful Failover [10-25](#)
 See also UR licenses
 upgrading [1-22, 11-2 to 11-5](#)

link up and link down, SNMP [9-32](#)

LINUX

default routes [2-2](#)

literal port values [D - 2](#)

load sharing with crypto maps [6-24](#)

LOCAL database

Command Authorization with [9-5](#)
 user authentication to the PIX Firewall with [9-3](#)

lockout

recovering from [9-9](#)

logging

FTP [1-21](#)
 URLs [1-21](#)

M

MacOS

default routes [2-3](#)

manual configuration of SAs [6-22](#)

masks

See subnet masks

MD5 [6-3](#)

description [E-1, E-2](#)
 IKE policy keywords (table) [6-3](#)

Message Digest 5

See MD5

MIBs [9-32](#)

MIB II groups [9-32](#)
 updating file [9-35](#)

Microsoft Challenge Handshake Authentication Protocol

See MS-CHAP

Microsoft Exchange

configuring [C - 1](#)

Microsoft Remote Procedure Call

See MSRPC

Microsoft Windows 2000 CA

supported [6-9, 7-14](#)

modes

See access modes

monitor mode

description [1-24](#)
 using [11-10](#)

More prompt [1-26](#)

MS-CHAP [8-39](#)

MSRPC

See also RPC

multicasts

forwarding [2-29](#)
 receiving [2-27](#)

- support for [1-14](#)
- Multidevice Controller
 - See MDC
- multimedia applications
 - supported [1-11, D-5](#)
- multiple interfaces
 - configuring, example of [2-20](#)
 - security levels with [1-4](#)

N

- N2H2 filtering server
 - identifying [3-28](#)
 - supported [1-9](#)
 - URL for website [1-9](#)
- named ACLs
 - downloading [3-17](#)
- NAT
 - application inspection [1-10](#)
 - configuring [2-10](#)
 - description [1-5](#)
 - dynamic [2-9](#)
 - function [2-8](#)
 - outside [2-24, 2-25](#)
 - overlapping networks [2-26](#)
 - RCP not supported with [4-20](#)
 - RTSP not supported with [1-12](#)
 - server access [3-1](#)
 - static [2-9](#)
 - TFTP not supported with [4-12](#)
 - three interfaces [2-21](#)
 - two interfaces (figure) [2-18](#)
- nesting object groups [3-25](#)
- NetBIOS
 - support for [1-13](#)
- netmask
 - See subnet mask
- Netshow
 - application inspection [4-18](#)

- Network Address Translation
 - See NAT
- network extension mode
 - configuring [5-2](#)
 - description [5-1](#)
- Network File System
 - See NFS
- network object groups
 - configuring [3-24](#)
- Network Time Protocol
 - See NTP
- NFS
 - access [4-20](#)
 - application inspection [4-20](#)
 - testing with showmount [4-20](#)
- NT
 - default routes [2-3](#)
 - See Windows NT
- NTP
 - configuring [9-9 to 9-13](#)
 - feature [1-20](#)

O

- Oakley key exchange protocol [E-2](#)
- object groups
 - applying ACLs to [3-23](#)
 - configuring [3-20 to 3-26](#)
 - feature [1-7](#)
 - ICMP-type [3-24](#)
 - nesting [3-25](#)
 - network [3-24](#)
 - port [3-24](#)
 - protocols [3-23](#)
 - removing [3-26](#)
 - service [3-24](#)
 - subcommand mode [3-20](#)
 - verifying [3-22](#)
- outbound connectivity [3-4](#)

outside interfaces

Telnet to [9-17](#)

outside NAT

configuring [2-24 to 2-26](#)example [2-25](#)

overlapping networks

configuring [2-26](#)example [2-26](#)**P**

packet capture

configuring [9-25 to 9-29](#)feature [1-20](#)formats (table) [9-27](#)viewing buffer [9-26](#)paging screen displays [1-26](#)

PAP

supported [8-39](#)

Password Authentication Protocol

See PAP

PAT

addresses [2-11](#)application inspection [1-10](#)configuring [2-10](#)DHCP clients and [5-11](#)dynamic [2-9](#)function [2-8](#)RTSP [4-17](#)server access [3-1](#)static [2-9](#)three interfaces [2-21](#)two interfaces [2-18](#)PCNFSD, tracking activity [4-20](#)perimeter interfaces [2-10](#)

perimeter networks

See DMZ

per-user access lists [1-7](#)

PFSS

executable file [11-7](#)phases, of IPSec [1-15](#)

ping

See ICMP

PIX 501

DHCP client configuration [5-11](#)DHCP client feature support [1-18](#)DHCP servers [5-7](#)failover not supported [1-22](#)using as Easy VPN Remote device [5-1](#)

PIX 506/506E

DHCP client configuration [5-11](#)DHCP client feature support [1-18](#)DHCP servers [5-7](#)failover not supported [1-22](#)using as Easy VPN Remote device [5-1](#)

PIX 520

backing up configuration [1-25](#)

PIX Firewall Syslog Server

See PFSS

PIX Firewall VPN Client [5-1](#)

See Easy VPN Remote device

PKCS [E-3](#)PKI protocol [6-9](#)

Point-to-Point Tunneling Protocol

See PPTP

Port Address Translation

See PAT [1-29, 2-11](#)PORT command, FTP [4-6](#)port redirection [3-5](#)

ports

literal names and numbers [D - 2](#)object groups [3-24](#)

PPPoE

configuring [5-3 to 5-6](#)description [1-18](#)packet capture, example [9-28](#)

PPTP

inbound access [3-3](#)

- VPNs [8-39](#)
 - pre-shared keys
 - configuring [7-1](#)
 - description [1-16](#)
 - example [7-2](#)
 - using with IKE [6-6](#)
 - primary Easy VPN Server [5-2](#)
 - Private Certificate Services (PCS) [7-14](#)
 - Private Link
 - conversion to IPSec [F-1](#)
 - example [F-5](#)
 - privilege levels
 - configuring [9-1 to 9-2](#)
 - description [1-19](#)
 - viewing [9-4](#)
 - protocols
 - object groups [3-23](#)
 - packet capture formats (table) [9-27](#)
 - port numbers [D - 4](#)
 - supported [1-10](#)
 - proxy servers
 - SIP and [4-15](#)
 - public key cryptography [6-8](#)
 - Public-Key Cryptography Standard
 - See PKCS
 - Public Key Infrastructure Protocol
 - See PKI protocol
-
- R**
- RADIUS
 - configuring [3-8](#)
 - support for [1-6](#)
 - viewing user accounts for Command Authorization [9-4](#)
 - VPN example [8-8](#)
 - Xauth [8-2](#)
 - RAS
 - support for [1-11](#)
 - Real Time Streaming Protocol
 - See RTSP
 - recovering from lockout [9-9](#)
 - redirecting service requests [3-5](#)
 - redundancy
 - See failover
 - Registration, Admission, and Status
 - See RAS
 - Registration Authority
 - description [6-8](#)
 - releasing DHCP lease [5-12](#)
 - remote access VPN
 - configuring [8-1 to 8-40](#)
 - description [1-17](#)
 - Remote Authentication Dial-In User Server
 - See RADIUS
 - Remote Procedure Call
 - See RPC
 - remote VPN clients
 - assigning IP addresses [8-4](#)
 - renewing DHCP lease [5-12](#)
 - reverse route lookup
 - See Unicast RPF
 - revoked certificates [6-8](#)
 - RFC 2637 [8-39](#)
 - RIP
 - PIX Firewall listening [2-6](#)
 - support for [1-13](#)
 - routing
 - default routes [2-1](#)
 - enabling SMR [2-27](#)
 - simplifying with outside NAT [2-25](#)
 - static routes [2-6](#)
 - Routing Information Protocol
 - See RIP
 - RPC
 - application inspection [4-20](#)
 - Sun [4-20](#)
 - testing with rpcinfo [4-20](#)
 - See also MSRPC

RS-232 cable
See failover, serial cable [10-18](#)

RSA keys
described [E-3](#)
generating [6-10](#)

RSA signatures
IKE authentication method [6-8, E-2](#)

RTSP
changing default port assignments [4-17](#)
restrictions [4-17](#)
support for [1-12](#)

S

SAs
clearing IPsec [6-26](#)
description [1-15](#)
establishing manual with pre-shared keys [6-12](#)
lifetimes [6-17](#)

saving configurations [2-15](#)
Command Authorization (caution) [9-5](#)
upgrading versions (caution) [11-1](#)

SCCP
application inspection [4-12](#)
support for [1-12](#)

secondary Easy VPN Server [5-2](#)

Secure Hash Algorithm
See SHA

Secure Shell
See SSH

security associations
See SAs

security gateways
exceptions to IKE Mode Config [8-5](#)
exception to Xauth [8-3](#)
initiating IKE Mode Config [8-5](#)

security levels [1-4](#)
interfaces [2-5](#)
values [2-6](#)

serial cable
See cable-based failover

server access [3-1](#)

services
access control [3-13](#)
object groups [3-24](#)

Session Initiation Protocol
See SIP

SHA
IKE policy keywords (table) [6-3](#)

show commands [6-25](#)

showmount command
application inspection with [4-20](#)

Simple Client Control Protocol
See SCCP

Simple Mail Transfer Protocol
See SMTP

Simple Network Management Protocol
See SNMP

SIP [1-13, 4-15](#)
application inspection [4-15](#)

site-to-site VPNs
description [1-16](#)
examples [7-1 to 7-27](#)
exception to IKE Mode Config [8-5](#)
exception to Xauth [8-3](#)
redundancy [6-22](#)
See also VPNs

Skeme key exchange protocol [E-2](#)

Skinny Client Control Protocol
See SCCP

small office, home office networks
See SOHO networks

SMR
description [1-14](#)
enabling [2-27](#)

SMTP
application inspection [4-9](#)
protection from attacks [1-11](#)

sniffing packets

See packet capture

SNMP

Cisco syslog MIB 9-35

read-only (RO) values 9-32

SNMPc (Cisco Works for Windows) 9-35

support for 1-21

traps 9-32

using 9-31 to 9-41

software

copying with HTTP 11-5

downgrading 11-14

downloading 11-7

downloading with FTP 11-9

downloading with HTTP 11-8

requirements for Stateful Failover 10-25

upgrading system 1-22

SOHO networks

configuring 5-1 to 5-12

features 1-17

split tunnel mode 8-7

SSH 9-19 to 9-22

Stateful Failover 1-3, 10-20

state information 1-3

static

NAT for server access 3-1

translation 1-5

static NAT

description 2-9

static PAT

description 2-9

static routes

configuring 2-7

stub multicast routing

See SMR

subcommand mode 1-24

subnet masks D-7

configuring 2-3

subnets 2-11

Sun RPC 4-20

SYN packet attack

protection from 1-8

syslog

Cisco MIB 9-35

MIB files 9-35

SNMP 9-32

SNMP traps 9-34

support for 1-21

system clock 9-14

system recovery 11-12

T

TACACS+

caution when using with Command Authorization 9-7

inbound access 3-3

using with Command Authorization 9-8

viewing user accounts for Command Authorization 9-4

Xauth 8-2

TCP

Intercept feature 1-9

port literal names D-2

Telnet

configuring 9-15 to 9-19

configuring RIP (note) 1-13

interfaces 1-20

outside interfaces 9-16

redirecting 3-6

Terminal Access Controller Access Control System Plus

See TACACS+

testing connectivity 2-12

TFTP servers

downloading with HTTP 11-7

using to download software 1-23

time, setting system 9-14

Trace Channel

description 9-18

disadvantages (note) 9-19

- transform sets
 - configuring [6-23](#)
 - description [6-13](#)
- transport mode
 - description [8-32](#)
- traps, SNMP [9-32](#)
- Triple DES
 - description [E-2](#)
 - IKE policy keyword (table) [6-3](#)
- Trivial File Transfer Protocol servers
 - See TFTP servers
- troubleshooting
 - connectivity [2-12](#)
 - license upgrades [11-3](#)
 - See also packet capture
- tunnel mode [8-32](#)
- TurboACL [1-7, 3-14](#)
 - configuring [3-14 to 3-16](#)
 - viewing configuration [3-15](#)

U

- UDP
 - connection state information [1-3](#)
 - port literal names [D - 2](#)
- Unicast Reverse Path Forwarding
 - See Unicast RPF
- Unicast RPF [1-8](#)
- UniCERT Certificate Management System
 - configuring, example [7-14](#)
 - supported [6-9](#)
- Universal Resource Locators
 - See URLs
- UNIX
 - default routes [2-2](#)
 - getting console terminal [11-6](#)
- unprivileged mode [1-23](#)
- upgrading
 - activation keys [11-2](#)

- feature licenses [1-22, 11-2](#)
- image [11-7 to 11-16](#)
- images [1-22](#)
- UR license [10-1](#)
- URLs
 - filtering [1-9](#)
 - filtering, configuration [3-33](#)
 - logging [1-21](#)
- user authentication
 - See also Xauth
 - to the PIX Firewall [9-2](#)
- User Datagram Protocol
 - See UDP

V

- validating CAs [6-8](#)
- VDO LIVE [4-19](#)
- VeriSign
 - CA [7-7](#)
 - CA example [7-7](#)
 - configuring CAs, example [6-9](#)
- video conferencing applications, supported [D - 5](#)
- viewing
 - Command Authorization settings [9-7](#)
 - default configurations [1-27](#)
 - IPSec configuration [6-25](#)
 - NTP [9-10](#)
 - privilege levels [9-4](#)
 - RMS [9-24](#)
 - SMR configuration [2-31](#)
 - SSH [9-22](#)
 - user accounts for Command Authorization [9-4](#)
- Virtual Private Networks
 - See VPNs
- Virtual Re-assembly [1-9](#)
- Voice over IP
 - See VoIP
- VOIP

SCCP [1-12](#)

VoIP

- application inspection [4-11, 4-15](#)
- gateways and gatekeepers [4-13](#)
- H.323 [1-12](#)
- proxy servers [4-15](#)
- SIP
 - description [1-13](#)

VPN clients

- Easy VPN Remote device [1-17, 5-1](#)
- IKE Mode Config [8-5](#)
- modes [5-1](#)
- SOHO networks and [5-1](#)

VPNs

- configuration examples [7-25](#)
- Easy VPN Remote device in [5-1](#)
- overview [1-14 to 1-17](#)
- peer identity [6-7](#)
- PPTP [8-39](#)
- remote access [8-1 to 8-40](#)
- site-to-site [1-16, 7-1 to 7-27](#)
- split tunnel [8-8](#)
- Windows 2000 client [8-34](#)

W

Websense filtering server [1-9](#)

web server access [3-1](#)

Windows 2000 setting default routes [2-2](#)

Windows 2000 VPN client

- configuring [8-34](#)

Windows 95

- setting default routes [2-2](#)

Windows 98

- setting default routes [2-2](#)

Windows NT

- setting default routes [2-3](#)

winipcfg, view default route [2-2](#)

X

X.509v3 certificates [E-3](#)

Xauth

- configuring [8-2, 8-3](#)
- configuring Cisco VPN client, example [8-21](#)
- enabling [8-16](#)
- exception for security gateways [8-3](#)
- IKE [8-2, E-2](#)

X Display Manager Control Protocol

- See XDMCP

XDMCP

- application inspection [4-23](#)
- support for [1-21](#)