



INDEX

HC	Cisco IOS XR Interface and Hardware Component Configuration Guide
IC	Cisco IOS XR IP Addresses and Services Configuration Guide
MCC	Cisco IOS XR Multicast Configuration Guide
MNC	Cisco IOS XR System Monitoring Configuration Guide
MPC	Cisco IOS XR MPLS Configuration Guide
QC	Cisco IOS XR Modular Quality of Service Configuration Guide
RC	Cisco IOS XR Routing Configuration Guide
SC	Cisco IOS XR System Security Configuration Guide
SMC	Cisco IOS XR System Management Configuration Guide
VFC	Cisco IOS XR Virtual Firewall Configuration Guide

A

AAA (authentication, authorization, and accounting)

- accounting services, enabling [SC-53](#)
- authentication [SC-9](#)
- authorization, enabling [SC-51](#)
- configuring
 - AAA service restrictions [SC-3](#)
 - accounting method lists [SC-46](#)
 - authentication method lists [SC-40](#)
 - authorization method lists [SC-42](#)
 - individual users [SC-23](#)
 - login parameters [SC-55](#)
 - RADIUS server groups [SC-36](#)
 - remote AAA [SC-8](#)
 - router to RADIUS server communication [SC-25](#)
 - services (examples) [SC-56](#)
 - TACACS+ server [SC-33](#)
 - TACACS+ server groups, [SC-38](#)
 - task groups for task-based authorization [SC-19](#)
 - user groups [SC-21](#)
- database [SC-7](#)
- interim accounting records, generating [SC-48](#)

per VRF (VPN routing and forwarding) definition [SC-31](#)

task-based authorization

task groups, definition [SC-6](#)

task IDs [SC-12](#)

user and group attributes [SC-4](#)

user groups

definition [SC-5](#)

inheritance [SC-5](#)

predefined [SC-5](#)

privilege level mapping as an alternative to task IDs [SC-16](#)

XML schema [SC-16](#)

aaa accounting command [SC-48](#)

aaa accounting update command [SC-48](#)

accept-lifetime command [SC-162](#)

accept-tolerance command [SC-157](#)

address ipv4 (MPP) command [SC-185](#)

address ipv6 (MPP) command [SC-188](#)

algorithms

See IKE, algorithms

allow command [SC-185](#), [SC-188](#)

C

CAC (call admission control)

IKE SA configuration [SC-129](#)

overview [SC-114](#)

CAs (certification authorities)

authenticating [SC-71](#)

declaring [SC-69](#)

description [SC-63](#), [SC-213](#)

domain names, configuring (example) [SC-66](#)

host names [SC-66](#)

manual enrollment, how to cut-and-paste [SC-73](#)
 RSA (Rivest, Shamir, and Adelman) key pairs
 generating [SC-67](#)
 supported standards [SC-62](#)
 trusted point, configuring [SC-69](#)
 See also certificates; CRLs; IPsec; RAs
 certification authority interoperability
 See also certificates; CRLs; IPsec; RAs
 certificates [SC-63](#)
 requests [SC-72](#)
 See also CAs; CRLs; RSA keys
 certification authority interoperability
 authenticating the CA [SC-71](#)
 CA description [SC-63](#)
 configuring
 domain names (example) [SC-66](#)
 host names (examples) [SC-66](#)
 trusted points [SC-69](#)
 description [SC-213](#)
 generating RSA (Rivest, Shamir, and Adelman) key pairs [SC-67](#)
 manual enrollment, cutting and pasting [SC-73](#)
 requesting certificates from the CA [SC-72](#)
 supported standards
 Internet Key Exchange (IKE) Security protocol [SC-63](#)
 IP Network Security (IPsec) protocol [SC-62](#)
 Public-Key Cryptography Standard #10 (PKCS#10) [SC-63](#)
 Public-Key Cryptography Standard #7(PKCS#7) [SC-63](#)
 RSA (Rivest, Shamir, and Adelman) keys [SC-63](#)
 Secure Socket Layer (SSL) protocol [SC-63](#)
 X.509v3 certificate [SC-63](#)
 Cisco Systems-supported security standards [SC-107](#)
 clear crypto session command [SC-115](#)
 clock set command [SC-195](#)
 config-isakmp command mode, how to enable [SC-118](#)
 configuring
 outbound traffic (key chain) [SC-163](#)

control-plane command [SC-185](#)
 control plane protection, MPP
 definition [SC-183](#)
 cryptographic-algorithm command [SC-164](#)
 crypto ipsec transform-set command [SC-90](#)
 crypto keyrings
 configuration [SC-133](#)
 configuring [SC-133](#)
 guidelines and restrictions [SC-133](#)

D

deadtime command [SC-37](#)
 DES (Data Encryption Standard)
 definition [SC-107](#)
 IKE policy parameter [SC-109](#)
 description (ISAKMP peer) command [SC-115](#)
 domain names, configuring CA interoperability [SC-66](#)
 DPD (Dead Peer Detection)
 periodic message [SC-115](#)
 DPD (Dead Peer Detection) message, configuring [SC-142](#)

E

encrypted nonces
 See RSA encrypted nonces
 encryption algorithm
 See also IKE algorithms
 See IKE, algorithms
 end-time, key chain management [SC-154](#)

H

hash algorithm
 See IKE, algorithms
 See IKE, algorithms
 hitless key rollover
 accept-tolerance command [SC-157](#)

hitless key rollover, configuring [SC-157](#)

host names, configuring CA interoperability (examples) [SC-66](#)

IKE (Internet Key Exchange) security protocol

algorithms

encryption [SC-118](#)

hash [SC-118](#)

options [SC-110](#)

authentication methods [SC-111, SC-118](#)

DH (Diffie-Hellman)

group identifier, specifying [SC-118](#)

IKE policy parameter [SC-109](#)

enabling and disabling [SC-116](#)

extended authentication [SC-113](#)

group identifier, specifying [SC-118](#)

ISAKMP identity, configuring [SC-112](#)

negotiations [SC-110](#)

policies

configuring [SC-117](#)

configuring (example) [SC-144](#)

identifying [SC-118](#)

multiple [SC-111](#)

parameters [SC-109, SC-110](#)

purpose [SC-108](#)

viewing [SC-119](#)

requirements

RSA encrypted nonces method [SC-112](#)

RSA signatures method [SC-112](#)

supported standards [SC-107](#)

See also IPsec; RSA encrypted nonces; SAs

IKE (Internet Key Exchange Security Protocol)

Advanced Encryption Standard (AES)

definition [SC-107](#)

algorithms

encryption [SC-118](#)

hash [SC-118](#)

MD5 (Message Digest 5) [SC-107](#)

options [SC-110](#)

SHA (Secure Hash Algorithm), definition [SC-108](#)

authentication methods [SC-111, SC-118](#)

Call Admission Control (CAC)

limiting CPU resources consumed [SC-114](#)

Call Admission Control (CAC) definition [SC-114](#)

configuring

IKE security association (SA) limit for call admission control [SC-129](#)

ISAKMP identity [SC-112](#)

policies [SC-117](#)

definition [SC-107](#)

DES (Data Encryption Standard)

definition [SC-107](#)

DH (Diffie-Hellman)

IKE policy parameter [SC-109](#)

specifying the group identifier [SC-118](#)

DPD (Dead Peer Detection)

periodic message [SC-116](#)

enabling and disabling [SC-116](#)

enabling config-isakmp command mode [SC-118](#)

extended authentication [SC-113](#)

Internet Security Association and Key Management Protocol (ISAKMP)

definition [SC-107](#)

ISAKMP peer description [SC-115](#)

keyring configuration mode enablement [SC-124](#)

negotiations [SC-110](#)

Oakley Key Exchange Protocol definition [SC-107](#)

policies

configuring (example) [SC-144](#)

identifying [SC-118](#)

multiple [SC-111](#)

parameters [SC-110](#)

purpose [SC-108](#)

viewing [SC-119](#)

Public Key Cryptographic Protocol

Diffie-Hellman [SC-107](#)

- requirements
 - RSA encrypted nonces method [SC-112](#)
 - RSA signatures method [SC-112](#)
 - RFC 2408, ISAKMP [SC-107](#)
 - RSA (Rivest, Shamir, and Adelman)
 - encrypted nonces [SC-108](#), [SC-109](#)
 - Skeme Key Exchange Protocol
 - definition [SC-107](#)
 - VPN monitoring
 - adding an IKE peer description [SC-136](#)
 - clearing a crypto session [SC-115](#), [SC-137](#)
 - X.509v3 certificates standard [SC-108](#)
 - See also* IPSec; RSA encrypted nonces; SAs
 - IKE peer, configuration
 - description (ISAKMP peer) command [SC-115](#)
 - how to add [SC-136](#)
 - inband management interface, MPP
 - allow command [SC-185](#)
 - definition [SC-183](#)
 - inband command [SC-185](#)
 - interface command [SC-185](#)
 - IP Network Security Protocol (IPSec)
 - definition [SC-107](#)
 - IPSec (IP Network Security Protocol)
 - CAs
 - implementing with [SC-65](#)
 - implementing without [SC-65](#)
 - checkpointing [SC-85](#)
 - crypto access lists [SC-83](#)
 - cautions, creating [SC-97](#)
 - creating [SC-88](#)
 - purpose [SC-83](#)
 - crypto profiles [SC-82](#)
 - applying to transport [SC-99](#)
 - applying to tunnel-ipsec interfaces [SC-98](#)
 - configuring static or dynamic [SC-91](#)
 - dynamic crypto profile description [SC-82](#)
 - PFS (perfect forward secrecy) description [SC-84](#)
 - prerequisites for implementation [SC-81](#)
 - restrictions for implementation [SC-81](#)
 - setting global lifetimes [SC-85](#)
 - transform sets
 - defining [SC-90](#)
 - description [SC-83](#)
 - IPSec (IPSec Network Security Protocol)
 - implementing without CAs [SC-65](#)
 - IPSec VPN SPA
 - DPD message [SC-115](#), [SC-116](#)
 - ISAKMP
 - definition [SC-107](#)
 - See also* IKE
 - ISAKMP profile
 - description [SC-113](#)
 - locally sourced and destined traffic procedure [SC-137](#)
 - overview [SC-113](#)
-
- ## K
- key (key chain) command [SC-159](#)
 - key chain command [SC-156](#)
 - key chain management
 - configuring [SC-155](#), [SC-167](#)
 - key identifiers [SC-158](#)
 - key string text [SC-159](#)
 - outbound traffic [SC-163](#)
 - description [SC-154](#)
 - end-time [SC-154](#)
 - key lifetime [SC-154](#)
 - key validation [SC-161](#)
 - start-time [SC-154](#)
 - keyring command [SC-138](#)
 - keyring configuration mode, enabling [SC-124](#)
 - keys
 - preshared
 - IKE policy parameter [SC-109](#)
 - key-string command [SC-161](#)

L

lawful intercept, implementing [SC-169](#)

M

MAC (message authentication code) [SC-164](#)

authentication option [SC-154](#)

cryptographic algorithm procedure [SC-164](#)

management plane

MPP feature [SC-184](#)

management-plane command [SC-185](#)

match identity command [SC-138](#)

MD5 (Message Digest 5)

IKE policy parameter [SC-109](#)

MD5 (Message Digest 5) algorithm

description [SC-107](#)

IKE policy parameter [SC-109](#)

MPP (Management Plane Protection)

benefits [SC-184](#)

control plane protection [SC-183](#)

description [SC-181](#), [SC-184](#)

device configuration [SC-185](#)

management interface

inband [SC-183](#)

out-of-band [SC-183](#)

management plane

description [SC-183](#)

peer-filtering option [SC-183](#)

N

nonces

See RSA encrypted nonces

O

Oakley key exchange protocol [SC-107](#)

See also IKE

See also IKE

out-of-band command [SC-188](#)

out-of-band management interface, MPP

definition [SC-183](#)

P

peer-filtering option

definition [SC-183](#)

peer keyword

inband interface [SC-186](#)

out-of-band interface [SC-189](#)

per VRF (VPN routing and forwarding) AAA

procedure [SC-31](#)

server-private command [SC-32](#)

supported VSAs [SC-31](#)

preshared keys

See keys, preshared; keys, preshared using AAA server

R

RADIUS

configuring

dead-server detection [SC-29](#)

UDP ports [SC-26](#)

operation [SC-18](#)

radius-server dead-criteria time command [SC-30](#)

radius-server dead-criteria tries command [SC-30](#)

radius-server deadtime command [SC-29](#)

RAs (registration authorities)

See CAs

See CAs

reverse-route command [SC-92](#)

RFC 2408, ISAKMP [SC-107](#)

RFC 2409, The Internet Key Exchange [SC-107](#)

RFC 2409, *The Internet Key Exchange* [SC-107](#)

RSA (Rivest, Shamir, and Adelman)

- encrypted nonces [SC-108](#)
 - requirements [SC-111, SC-112](#)
 - keys
 - configuring manually [SC-121](#)
 - configuring peers [SC-123](#)
 - definition [SC-63](#)
 - deleting [SC-68](#)
 - generating [SC-122](#)
 - signatures [SC-112](#)
 - requirements [SC-111](#)
 - RSA (Rivest, Shamir, and Adelman) encrypted nonces
 - IKE policy parameter [SC-109](#)
 - requirements [SC-111, SC-112](#)
 - RSA (Rivest, Shamir, and Adelman) keys
 - configuring, manually [SC-121](#)
 - peer configuration [SC-123](#)
 - RSA (Rivest, Shamir, and Adelman) signatures
 - IKE configuration [SC-112](#)
 - requirements [SC-111](#)
-
- S**
- SAM (Software Authentication Manager)
 - description [SC-195](#)
 - SAs (security associations)
 - global values [SC-84](#)
 - lifetimes
 - configuring [SC-118](#)
 - IKE policy parameter [SC-109](#)
 - operation [SC-84](#)
 - resource limit configuration [SC-131](#)
 - self-identity command [SC-138](#)
 - send-lifetime command [SC-164](#)
 - server-private command [SC-32, SC-36](#)
 - set interface tunnel-ipsec command [SC-138](#)
 - set pfs command [SC-85](#)
 - set security-association idle-time command [SC-92](#)
 - set security-association lifetime command [SC-92](#)
 - set security-association replay disable command [SC-92](#)
 - set session-key inbound ah command [SC-92](#)
 - set session-key inbound esp command [SC-92](#)
 - set session-key outbound ah command [SC-92](#)
 - set session-key outbound esp command [SC-92](#)
 - SHA (Secure Hash Algorithm)
 - definition [SC-108](#)
 - IKE policy parameter [SC-109](#)
 - show crypto session command [SC-115](#)
 - show key chain command [SC-156](#)
 - show mgmt-plane command [SC-185](#)
 - show radius dead-criteria host command [SC-30](#)
 - Skeme key exchange protocol [SC-107](#)
 - See also IKE
 - See also* IKE
 - SSH (Secure Shell)
 - client
 - 3DES support [SC-202](#)
 - configuring [SC-207](#)
 - description [SC-202](#)
 - server support [SC-202](#)
 - configuring [SC-204](#)
 - prerequisites [SC-200](#)
 - restrictions [SC-200](#)
 - server [SC-201](#)
 - SFTP (Standard File Transfer Protocol)
 - description [SC-202](#)
 - supported versions [SC-199](#)
 - troubleshooting [SC-208](#)
 - SSL (Secure Socket Layer)
 - configuring [SC-213](#)
 - description [SC-211](#)
 - prerequisites [SC-212](#)
 - start-time, key chain management [SC-154](#)
-
- V**
- VPN monitoring
 - crypto session, how to clear [SC-115, SC-137](#)
 - enhancements [SC-114](#)

- how to add IKE peer [SC-136](#)
- per-IKE peer, function [SC-115](#)
- show crypto session command [SC-115](#)
- summary status [SC-115](#)
- vrf (AAA) command [SC-32](#)
- vrf (MPP) command [SC-188](#)
- VSAs (vendor-specific attributes)
 - per VRF AAA [SC-31](#)
 - supported VSAs [SC-31](#)

