New and Changed Information xv

Preface xvii

Audience xvii

Document Organization xvii

Document Conventions xviii

Related Documentation iv-xix

Release Notes iv-xix

Regulatory Compliance and Safety Information iv-xix

Compatibility Information iv-xix

Hardware Installation iv-xix

Software Installation and Upgrade iv-xx

Cisco NX-OS iv-xx

Cisco Fabric Manager iv-xx

Command-Line Interface iv-xxi

Intelligent Storage Networking Services Configuration Guides iv-xxi

Troubleshooting and Reference iv-xxi

Obtaining Documentation and Submitting a Service Request xxi

xxi

CHAPTER 1 **Security Overview** 1-1

FIPS 1-1

Users and Common Roles 1-1

RADIUS and TACACS+ 1-2

IP ACLs 1-2

PKI 1-2

IPsec 1-3

FC-SP and DHCHAP 1-3

Port Security 1-3

Fabric Binding 1-3

TrustSec Fibre Channel Link Encryption 1-4

CHAPTER 2 **Configuring FIPS** 2-1

Configuration Guidelines 2-1
Enabling FIPS Mode 2-2
Displaying FIPS Status 2-2
FIPS Self-Tests 2-2

CHAPTER 3 **Configuring Security Features on an External AAA Server** 3-1

Switch Management Security 3-2
CLI Security Options 3-2
SNMP Security Options 3-2
Switch AAA Functionalities 3-2
Authentication 3-3
Authorization 3-3
Accounting 3-4
Remote AAA Services 3-4
Remote Authentication Guidelines 3-4
Server Groups 3-4
AAA Service Configuration Options 3-5
Error-Enabled Status 3-5
AAA Server Monitoring 3-6
Authentication and Authorization Process 3-7
Configuring Fallback Mechanism for Authentication 3-9
Verifying Authorization Profile 3-10
Testing Authorization 3-10
Configuring AAA Server Monitoring Parameters Globally 3-10
Configuring LDAP 3-11
LDAP Authentication and Authorization 3-12
Guidelines and Limitations for LDAP 3-13
Prerequisites for LDAP 3-13
Default Settings 3-13
Enabling LDAP 3-14
Configuring LDAP Server Hosts 3-14
Configuring the RootDN for an LDAP Server 3-15
Configuring LDAP Server Groups 3-15
Configuring the Global LDAP Timeout Interval 3-16
Configuring the Timeout Interval for an LDAP Server 3-17
Configuring the Global LDAP Server Port 3-17
Configuring TCP Ports 3-17

Configuring LDAP Search Maps 3-18
Configuring the LDAP Dead-Time Interval 3-19
Configuring AAA Authorization on LDAP Servers 3-19
Disabling LDAP 3-20
Configuration Examples for LDAP 3-20
Configuring RADIUS Server Monitoring Parameters 3-21
About RADIUS Server Default Configuration 3-21
Setting the RADIUS Server Address 3-21
About the Default RADIUS Server Encryption Type and Preshared Key 3-24
Configuring the Default RADIUS Server Encryption Type and Preshared Key 3-24
Setting the RADIUS Server Timeout Interval 3-24
Setting the Default RADIUS Server Timeout Interval and Retransmits 3-25
Configuring RADIUS Server Monitoring Parameters 3-25
Configuring the Test Idle Timer 3-25
Configuring Test User Name 3-25
Configuring the Dead Timer 3-26
About RADIUS Servers 3-26
Configuring the Test Idle Timer 3-27
Configuring Test User Name 3-27
About Validating a RADIUS Server 3-27
Sending RADIUS Test Messages for Monitoring 3-27
Allowing Users to Specify a RADIUS Server at Login 3-28
About Vendor-Specific Attributes 3-28
VSA Format 3-29
Specifying SNMPv3 on AAA Servers 3-29
Displaying RADIUS Server Details 3-29
Displaying RADIUS Server Statistics 3-30
One-Time Password Support 3-31
Configuring TACACS+ Server Monitoring Parameters 3-31
About TACACS+ 3-32
About TACACS+ Server Default Configuration 3-32
About the Default TACACS+ Server Encryption Type and Preshared Key 3-32
Enabling TACACS+ 3-32
Setting the TACACS+ Server Address 3-33
Setting the Global Secret Key 3-34
Setting the Default TACACS+ Server Timeout Interval and Retransmits 3-35
Setting the Timeout Value 3-35
About TACACS+ Servers 3-35
Configuring TACACS+ Server Monitoring Parameters 3-36

Configuring the TACACS+ Test Idle Timer 3-36
Configuring Test Username 3-36
Configuring the Dead Timer 3-37
Sending TACACS+ Test Messages for Monitoring 3-38
Password Aging Notification through TACACS+ Server 3-38
About Validating a TACACS+ Server 3-39
Periodically Validating a TACACS+ Server 3-39
About Users Specifying a TACACS+ Server at Login 3-39
Allowing Users to Specify a TACACS+ Server at Login 3-39
Defining Roles on the Cisco Secure ACS 5.x GUI 3-39
Defining Custom Attributes for Roles 3-40
Supported TACACS+ Server Parameters 3-40
Displaying TACACS+ Server Details 3-41
Clearing TACACS+ Server Statistics 3-42
Configuring Server Groups 3-42
About Configuring Server Groups 3-42
About Bypassing a Nonresponsive Server 3-45
AAA Server Distribution 3-45
Enabling AAA Server Distribution 3-46
Starting a Distribution Session on a Switch 3-46
Displaying the Session Status 3-47
Displaying the Pending Configuration to be Distributed 3-47
Committing the Distribution 3-47
Discarding the Distribution Session 3-48
Clearing Sessions 3-48
Merge Guidelines for RADIUS and TACACS+ Configurations 3-49
CHAP Authentication 3-50
Enabling CHAP Authentication 3-50
MSCHAP Authentication 3-50
About Enabling MSCHAP 3-50
Enabling MSCHAP Authentication 3-51
Local AAA Services 3-52
Disabling AAA Authentication 3-52
Displaying AAA Authentication 3-52
Configuring Accounting Services 3-53
Displaying Accounting Configuration 3-53
Clearing Accounting Logs 3-54
Configuring Cisco Access Control Servers 3-55
Default Settings 3-58

CHAPTER 4 **Configuring IPv4 and IPv6 Access Control Lists** 4-1

About IPv4 and IPv6 Access Control Lists 4-2

IPv4-ACL and IPv6-ACL Configuration Guidelines 4-2

About Filter Contents 4-2

Protocol Information 4-3

Address Information 4-3

Port Information 4-4

ICMP Information 4-4

ToS Information 4-5

Creating IPv4-ACLs or IPv6-ACLs 4-5

Creating IPv4-ACLs or IPv6-ACLs 4-6

Adding IP Filters to an Existing IPv4-ACL or IPv6-ACL 4-7

Removing IP Filters from an Existing IPv4-ACL or IPv6-ACL 4-8

Verifying the IPv4-ACL or IPv6-ACL Configuration 4-8

Reading the IP-ACL Log Dump 4-9

Applying an IP-ACL to an Interface 4-10

Applying an IP-ACL to mgmt0 4-12

Verifying Interface IP-ACL Configuration 4-12

IP-ACL Counter Cleanup 4-13

CHAPTER 5 **Configuring Users and Common Roles** 5-1

Role-Based Authorization 5-1

About Roles 5-2

Configuring Roles and Profiles 5-2

Configuring Rules and Features for Each Role 5-2

Rule Changes Between SAN-OS Release 3.3(1c) and NX-OS Release 4.2(1a) Affect Role Behavior 5-3

Modifying Profiles 5-3

Configuring the VSAN Policy 5-4

Modifying the VSAN Policy 5-5

Role Distributions 5-5

About Role Databases 5-6

Locking the Fabric 5-6

Committing Role-Based Configuration Changes 5-6

Discarding Role-Based Configuration Changes 5-6

Enabling Role-Based Configuration Distribution 5-7

Clearing Sessions 5-7

Database Merge Guidelines 5-7

Displaying Role-Based Information 5-7
Displaying Roles When Distribution is Enabled 5-8
Configuring Common Roles 5-9
Mapping of CLI Operations to SNMP 5-10
Configuring User Accounts 5-11
Creating Users Guidelines 5-12
Checking Password Strength 5-12
Characteristics of Strong Passwords 5-12
Configuring Users 5-13
Logging Out Users 5-14
Displaying User Account Information 5-14
Configuring SSH Services 5-15
About SSH 5-16
Generating the SSH Server Key Pair 5-16
Specifying the SSH Key 5-16
Overwriting a Generated Key Pair 5-17
Clearing SSH Hosts 5-18
Enabling SSH or Telnet Service 5-19
Displaying SSH Protocol Status 5-19
SSH Authentication Using Digital Certificates 5-20
Passwordless File copy and SSH 5-20
Recovering the Administrator Password 5-22
Using the CLI with Network-Admin Privileges 5-22
Power Cycling the Switch 5-23
Default Settings 5-24

CHAPTER 6 **Configuring Certificate Authorities and Digital Certificates** 6-1
About CAs and Digital Certificates 6-1
Purpose of CAs and Digital Certificates 6-2
Trust Model, Trust Points, and Identity CAs 6-2
RSA Key-Pairs and Identity Certificates 6-3
Multiple Trusted CA Support 6-3
PKI Enrollment Support 6-4
Manual Enrollment Using Cut-and-Paste Method 6-4
Multiple RSA Key-Pair and Identity CA Support 6-4
Peer Certificate Verification 6-5
CRL Downloading, Caching, and Checking Support 6-5
OCSP Support 6-5
Import and Export Support for Certificates and Associated Key-Pairs 6-5

Configuring CAs and Digital Certificates 6-6
Configuring the Host Name and IP Domain Name 6-6
Generating an RSA Key-Pair 6-6
Creating a Trust Point CA Association 6-8
Authenticating the CA 6-8
Configuring Certificate Revocation Checking Methods 6-9
Generating Certificate Requests 6-10
Installing Identity Certificates 6-11
Saving Your Configuration 6-12
Ensuring Trust Point Configurations Persist Across Reboots 6-12
Monitoring and Maintaining CA and Certificates Configuration 6-13
Exporting and Importing Identity Information in PKCS#12 Format 6-13
Configuring a CRL 6-14
Deleting Certificates from the CA Configuration 6-14
Deleting RSA Key-Pairs from Your Switch 6-15
Displaying Key-Pair and CA Information 6-16
Example Configurations 6-16
Configuring Certificates on the MDS Switch 6-16
Downloading a CA Certificate 6-19
Requesting an Identity Certificate 6-24
Revoking a Certificate 6-30
Generating and Publishing the CRL 6-33
Downloading the CRL 6-34
Importing the CRL 6-36
Maximum Limits 6-38
Default Settings 6-39

CHAPTER 7 **Configuring IPsec Network Security** 7-1
About IPsec 7-2
About IKE 7-3
IPsec Prerequisites 7-4
Using IPsec 7-4
IPsec Compatibility 7-4
IPsec and IKE Terminology 7-5
Supported IPsec Transforms and Algorithms 7-6
Supported IKE Transforms and Algorithms 7-7
IPsec Digital Certificate Support 7-7
Implementing IPsec Without CAs and Digital Certificates 7-7
Implementing IPsec with CAs and Digital Certificates 7-8

How CA Certificates Are Used by IPsec Devices 7-9
Manually Configuring IPsec and IKE 7-10
About IKE Initialization 7-10
Enabling IKE 7-11
About the IKE Domain 7-11
Configuring the IKE Domain 7-11
About IKE Tunnels 7-11
About IKE Policy Negotiation 7-11
Configuring an IKE Policy 7-13
Optional IKE Parameter Configuration 7-14
Configuring the Lifetime Association for a Policy 7-15
Configuring the Keepalive Time for a Peer 7-15
Configuring the Initiator Version 7-16
Clearing IKE Tunnels or Domains 7-16
Refreshing SAs 7-16
Crypto IPv4-ACLs 7-16
About Crypto IPv4-ACLs 7-17
Crypto IPv4-ACL Guidelines 7-17
Mirror Image Crypto IPv4-ACLs 7-19
The any Keyword in Crypto IPv4-ACLs 7-20
Creating Crypto IPv4-ACLs 7-21
About Transform Sets in IPsec 7-21
Configuring Transform Sets 7-22
About Crypto Map Entries 7-23
SA Establishment Between Peers 7-23
Crypto Map Configuration Guidelines 7-24
Creating Crypto Map Entries 7-24
About SA Lifetime Negotiation 7-25
Setting the SA Lifetime 7-25
About the AutoPeer Option 7-25
Configuring the AutoPeer Option 7-26
About Perfect Forward Secrecy 7-27
Configuring Perfect Forward Secrecy 7-27
About Crypto Map Set Interface Application 7-27
Applying a Crypto Map Set 7-27
IPsec Maintenance 7-28
Global Lifetime Values 7-28
Displaying IKE Configurations 7-29
Displaying IPsec Configurations 7-30

Sample FCIP Configuration 7-34
Sample iSCSI Configuration 7-38
Default Settings 7-40

CHAPTER 8 **Configuring FC-SP and DHCHAP** 8-1
About Fabric Authentication 8-1
DHCHAP 8-2
DHCHAP Compatibility with Existing Cisco MDS Features 8-3
About Enabling DHCHAP 8-4
Enabling DHCHAP 8-4
About DHCHAP Authentication Modes 8-4
Configuring the DHCHAP Mode 8-5
About the DHCHAP Hash Algorithm 8-5
Configuring the DHCHAP Hash Algorithm 8-6
About the DHCHAP Group Settings 8-6
Configuring the DHCHAP Group Settings 8-6
About the DHCHAP Password 8-7
Configuring DHCHAP Passwords for the Local Switch 8-7
About Password Configuration for Remote Devices 8-8
Configuring DHCHAP Passwords for Remote Devices 8-9
About the DHCHAP Timeout Value 8-9
Configuring the DHCHAP Timeout Value 8-9
Configuring DHCHAP AAA Authentication 8-9
Displaying Protocol Security Information 8-10
Sample Configuration 8-11
Default Settings 8-13

CHAPTER 9 **Configuring Port Security** 9-1
About Port Security 9-1
Port Security Enforcement 9-2
About Auto-Learning 9-2
Port Security Activation 9-3
Port Security Configuration 9-3
Configuring Port Security with Auto-Learning and CFS Distribution 9-4
Configuring Port Security with Auto-Learning without CFS 9-4
Configuring Port Security with Manual Database Configuration 9-5
Enabling Port Security 9-5
Port Security Activation 9-5

Activating Port Security 9-6
Database Activation Rejection 9-6
Forcing Port Security Activation 9-6
Database Reactivation 9-7
Auto-learning 9-7
About Enabling Auto-learning 9-7
Enabling Auto-learning 9-8
Disabling Auto-learning 9-8
Auto-learning Device Authorization 9-8
Authorization Scenarios 9-9
Port Security Manual Configuration 9-10
About WWN Identification 9-10
Adding Authorized Port Pairs 9-11
Port Security Configuration Distribution 9-12
Enabling Distribution 9-12
Locking the Fabric 9-12
Committing the Changes 9-13
Discarding the Changes 9-13
Activation and Auto-learning Configuration Distribution 9-13
Database Merge Guidelines 9-14
Database Interaction 9-15
Database Scenarios 9-15
Copying the Port Security Database 9-16
Deleting the Port Security Database 9-17
Cleaning the Port Security Database 9-17
Displaying Port Security Configuration 9-18
Default Settings 9-20

CHAPTER 10 **Configuring Fabric Binding** 10-1
About Fabric Binding 10-1
Licensing Requirements 10-1
Port Security Versus Fabric Binding 10-1
Fabric Binding Enforcement 10-2
Fabric Binding Configuration 10-3
Enabling Fabric Binding 10-3
Configuring Switch WWN List 10-3
Fabric Binding Activation 10-4
Forcing Fabric Binding Activation 10-5
Saving Fabric Binding Configurations 10-5

Clearing the Fabric Binding Statistics 10-6
Deleting the Fabric Binding Database 10-6
Verifying Fabric Binding Configurations 10-6
Default Settings 10-9

CHAPTER 11 **Configuring Cisco TrustSec Fibre Channel Link Encryption** 11-1
Cisco TrustSec FC Link Encryption Terminology 11-1
Support for AES Encryption 11-2
About Cisco TrustSec FC Link Encryption 11-2
Supported Modules 11-2
Enabling Cisco TrustSec FC Link Encryption 11-2
Setting Up Security Associations 11-3
Setting Up Security Association Parameters 11-3
Configuring ESP Settings 11-4
Configuring ESP on Ingress and Egress Ports 11-4
Configuring ESP Modes 11-6
Viewing Cisco TrustSec FC Link Encryption Information 11-7
Viewing FC-SP Interface Information 11-8
Viewing Running System Information 11-8
Viewing FC-SP Interface Statistics 11-8
Cisco TrustSec FC Link Encryption Best Practices 11-9
General Best Practices 11-9
Best Practices for Changing Keys 11-9

INDEX