CONFIGURATION GUIDE

Network OS Common Criteria

Supporting Network OS v6.0.2

53-100xxxx-01

Contents

Copyright Statement

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit http://www.brocade.com/support/oscd.

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names Identifies keywords and operands Identifies the names of user-manipulated GUI elements Identifies text to enter at the GUI
italic text	Identifies emphasis Identifies variables Identifies document titles
`Courier font`	Identifies CLI output Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options. In Fibre Channel products, square brackets may be used instead for this purpose.

Convention	Description
x | y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member...*].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

You can download additional publications supporting your product at www.brocade.com. Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information on Brocade products and resources, go to MyBrocade. You can register at no cost to obtain a user ID and password.

Release notes are available on MyBrocade under Product Downloads.

White papers, online demonstrations, and data sheets are available through the Brocade website.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to http://www.brocade.com/services-support/index.html.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone	E-mail
Preferred method of contact for non-urgent issues: • My Cases through MyBrocade • Software downloads and licensing tools • Knowledge Base	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • For areas unable to access toll free number: +1-408-333-6061 • Toll-free numbers are available in many countries.	support@brocade.com Please include: • Problem summary • Serial number • Installation details • Environment description

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/Solution Provider, contact your OEM/Solution Provider for all of your product support needs.

- OEM/Solution Providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/Solution Provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/Solution Provider.

Document feedback

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com.
- By sending your feedback to documentation@brocade.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

About This Document

Supported hardware and software

Brocade recommends to confirm if the Network OS device and the software version is Common Criteria certified.

To determine if the Network OS device and current software version is Common Criteria certified, refer to https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm.

Common Criteria Certification

Common Criteria overview

This section contains steps for configuring the Brocade Network OS switch for Common Criteria (CC) standards with Network OS version 5.0.1b1 Network Device Protection Profile (NDPP).

Common Criteria certification for a device enforces a set of security standards and feature limitations on a device to be compliant with the Common Criteria standards, similar to placing the device in FIPS mode. To better understand the Common Criteria certification and the associated security functions that have been subject to certification, refer to the *Brocade Communications Systems, Inc. Brocade Switches 5.0.1b1 (NDPP11e3) Security Target* document.

The Network OS device management functions are isolated through authentication. Once administrators log in with specific credentials, their access is limited to commands for which they have privileges and role-based permissions. Additionally, network management communication paths are protected against modification and disclosure using SSHv2.

FIPS 140-2 Security Level 2 specifies the security requirements that are satisfied by a cryptographic module utilized within a security system protecting sensitive information of the system.

Brocade Network OS switches running Network OS 5.0.1b1 are designed to support FIPS-compliance mode. All cryptographic algorithms required and used in CC are certified by FIPS certifications.

Firmware update

Firmware packages are signed using the 2048-bit RSA key with SHA-256 during firmware build and verified during firmware installation as specified in the following steps.

1. RPM packages are signed with the private key to create a SHA-256 digest when the firmware package is generated.
2. A public key is packaged in an RPM package as part of the firmware and is downloaded as the first file.
3. As part of firmware download, each package is validated by verifying the signature.
4. Installation begins after the packages are validated.
5. The switch restarts after the successful installation.

NOTE
If the installation fails, an error with details is displayed and the download procedure is terminated.

The public key file on the switch contains only one public key. It is only able to validate firmware signed using one corresponding private key. If the private key changes in future releases, you must change the public key on the switch by using the **firmware download** command. When a new firmware is downloaded, the firmware download always replaces the public key file on the switch with what is in the new firmware. This allows you to have planned firmware key changes.

You can download the signed firmware with its associated MD5 from MyBrocade.

Firmware download

Perform the following tasks to download the firmware.

1. Brocade uploads the signed firmware as a tar file with its associated MD5 on secure location.

   NOTE
   File location and version details are provided to the customer.

2. Download and verify with the MD5.

Configuring Common Criteria mode

To configure the Brocade Network OS switch for CC compliance mode, execute the following steps.

NOTE
Configuring a Brocade Network OS switch for CC compliance mode using NETCONF operations is not supported. NETCONF interface must be blocked before configuring the CC compliance mode.

1. Log in to the switch as admin.
2. Enter the **unhide fips** command. Enter the password as "fibranne" when prompted.

   ```
   device# unhide fips
   ```

   You will have access to all FIPS commands, such as the **fips zeroize** command.
3. Enter the **fips zeroize** command to zeroize all the existing security configurations and parameters.

   ```
   device# fips zeroize
   ```

4. Configure the system for crypto compliance.

   a) Enter the **cipherset ssh** command to configure SSH Server and Client ciphers and MAC addresses.

   ```
   device# cipherset ssh
   ```

   b) Enter the **cipherset ldap** command to configure TLS ciphers for LDAP authentication.

   ```
   device# cipherset ldap
   ```

   c) Enter the **cipherset radius** command to configure TLS ciphers for RADIUS authentication.

   ```
   device# cipherset radius
   ```

   d) Enter global configuration mode.

   ```
   device# configure terminal
   ```

   e) Enter the **ssh server key-exchange dh-group-14** command to configure the SSH Server key-exchange protocol.

   ```
   device(config)# rbridge-id 1
   device(config-rbridge-id-1)# ssh server key-exchange dh-group-14
   ```

   f) Enter the **ssh client key-exchange dh-group-14** command to configure the SSH Client key-exchange protocol.

   ```
   device(config-rbridge-id-1)# ssh client key-exchange  dh-group-14
   ```

   g) Enter the **no ssh server key dsa** command to remove the SSH DSA host key.

   ```
   device(config-rbridge-id-1)# no ssh server key dsa
   ```

   h) Enter the **ssh server shutdown** and **no ssh server shutdown** commands to restart the SSH server.

   ```
   device(config-rbridge-id-1)# ssh server shutdown
   device(config-rbridge-id-1)# no ssh server shutdown
   ```

5. Use IP ACLs to block Telnet, HTTP, HTTPS, SNMP, NETCONF, and Brocade internal ports 7110, 7710, 8008, 9110, and 9710 for IPv4 and IPv6. If SSH access is required, enter **seq permit** commands to allow access on port 22. If remote access is required, such as through SCP or LDAP, enter **seq permit** commands to allow UDP and TCP traffic on ports 1024 through 65535. Configure IP ACLs using the **ip access-list** command and use the **ip access-group** command to apply the rules to the management interface.

```
device(config)# ip access-list extended ccextACL
device(config-ip-ext)# seq 1 deny tcp any any eq 23
device(config-ip-ext)#seq 2 deny tcp any any eq 80
device(config-ip-ext)#seq 3 deny tcp any any eq 443
device(config-ip-ext)#seq 4 deny tcp any any eq 830
device(config-ip-ext)#seq 5 deny tcp any any eq 7110
device(config-ip-ext)#seq 6 deny tcp any any eq 7710
device(config-ip-ext)#seq 7 deny tcp any any eq 8008
device(config-ip-ext)#seq 8 deny tcp any any eq 9110
device(config-ip-ext)#seq 9 deny tcp any any eq 9710
device(config-ip-ext)#seq 10 deny udp any any eq 161
device(config-ip-ext)#seq 11 permit tcp any any range 1024 65535
device(config-ip-ext)#seq 12 permit udp any any range 1024 65535
device(config-ip-ext)#seq 13 permit tcp any any eq 22
device(config-ip-ext)#exit
device(config)# interface tengigabitethernet 1/0/49
device(conf-if-fo-1/0/49)# ip access-group ccextACL in

device(config)# ipv6 access-list extended ccextACL6
device(config-ip-ext)# seq 1 deny tcp any any eq 23
device(config-ip-ext)#seq 2 deny tcp any any eq 80
device(config-ip-ext)#seq 3 deny tcp any any eq 443
device(config-ip-ext)#seq 4 deny tcp any any eq 830
device(config-ip-ext)#seq 5 deny tcp any any eq 7110
device(config-ip-ext)#seq 6 deny tcp any any eq 7710
device(config-ip-ext)#seq 7 deny tcp any any eq 8008
device(config-ip-ext)#seq 8 deny tcp any any eq 9110
device(config-ip-ext)#seq 9 deny tcp any any eq 9710
device(config-ip-ext)#seq 10 deny udp any any eq 161
device(config-ip-ext)#seq 11 permit tcp any any range 1024 65535
device(config-ip-ext)#seq 12 permit udp any any range 1024 65535
device(config-ip-ext)#seq 13 permit tcp any any eq 22
device(config-ip-ext)#exit
device(config)# interface tengigabitethernet 1/0/49
device(conf-if-fo-1/0/49)# ipv6 access-group ccextACL6 in
```

NOTE
Do not use FTP mode for the following operations: copying startup or running configuration, copy support, and firmware download.

NOTE
Do not configure TACACS+ protocol for
authentication.

6. Configure PEAP MS-CHAP for RADIUS authentication, if required.

a) If the RADIUS server is configured for authentication, obfuscate the RADIUS shared secret during configuration.

b) Enter the **radius-server host** *ip-address* **protocol peap-mschap** [**port** *portnum*] [**key** *shared-key*] [**timeout** *secs*] [**retransmit** *num*] command in global configuration mode to configure the RADIUS server.

```
device(config)# radius-server host 10.24.65.6 protocol peap-mschap retransmit 100
```

c) Enter the **aaa authentication login radius local-auth-fallback** command.

```
device(config)# aaa authentication login radius local-auth-fallback
```

7. Configure LDAP if required.

   a) Enter the **certutil import ldapca directory** *ca-certificate-directory* **file** *filename* **protocol SCP host** *remote-ip* **user** *user-account* **password** *password* command in privileged EXEC mode to import the LDAP CA certificate.

   ```
   device# certutil import ldapca directory /usr/ldapcacert file cacert.pem protocol SCP host
   10.23.24.56 user admin password *****
   ```

   The CA certificate imported must be RSA-2048 with SHA-1 or SHA-256 encryption.

   b) Enter the **ldap-server host** *ip-address* **basedn** *domain-name* [**port** *portnum*] [**retransmit** *num*] command in global configuration mode to configure the LDAP server.

   ```
   device(config)# ldap-server host padl12r2.la12security.xyz.com basedn la12security.xyz.com
   ```

   c) Enter the **ip dns domain-name** and **ip dns name-server** commands to configure the DNS domain and server.

   ```
   device(config)# ip dns domain-name la12security.xyz.com
   device(config)# ip dns name-server 10.38.37.183
   ```

   d) Enter the **aaa authentication login ldap local-auth-fallback** command.

   ```
   device(config)# aaa authentication login ldap local-auth-fallback
   ```

8. Enable secure logging using the syslog server.

   a) Enter the **certutil import syslogca directory** *ca-certificate-directory* **file** *filename* **protocol SCP host** *remote-ip* **user** *user-account* **password** *password* command in privileged EXEC mode to import the syslog CA certificate.

   ```
   device# certutil import syslogca directory /usr/ldapcacert/ file cacert.pem protocol SCP host
   10.23.24.56 user admin password
   password:
   ```

   The CA certificate imported must be RSA-2048 with SHA-1 or SHA-256 encryption.

   b) Enter the **logging syslog-server** *ip-address* command in global configuration mode to configure the syslog server.

   ```
   device(config)# logging syslog-server 10.20.238.120  secure port 1999
   ```

9. Enter the **certutil import sshkey directory** *pubkey-directory* **file** *filename* **protocol SCP host** *remote-ip* **user** *user-account* *password password* command to import the public key.

   ```
   device# certutil import sshkey user admin host 10.70.4.106 directory /users/home40/bmeenaks/.ssh
   file id_rsa.pub login fvt
   Password: ***********
   switch# 2012/11/14-10:28:58, [SEC-3050], 75,, INFO, VDX, Event: sshutil, Status: success, Info:
   Imported SSH public key from 10.70.4.106 for user 'admin'.
   ```

   To support passwordless SSH authentication, externally generated RSA key pairs must only be imported if they are RSA 2048.

10. Enter the **telnet server shutdown** command in global configuration mode to disable the Telnet server.

    ```
    device(config-rbridge-id-1)# telnet server shutdown
    ```

11. Enter the **copy running-config startup-config** command to save all settings to the startup configuration file.

    ```
    device# copy running-config startup-config
    This operation will modify your startup configuration. Do you want to continue? [Y/N]: Y
    ```

Self-tests

The following table provides detailed information about the tests that are executed during the bootup of the switch to confirm the authenticity of the algorithms.

NOTE
During a self-test failure, Brocade recommends that you restart the system and test again. If the failure persists, proceed with the Return Materials Authorization (RMA) request for the device.

Algorithm	Description
TDES	This module implements a KAT for the encrypt and decrypt operations of Triple DES in the CBC mode of operation. The test passes only if the calculated output equals the known output for both operations. The Triple DES KAT must execute successfully before using the Triple DES functionality
AES	This module implements a known answer test (KAT) for encrypt and decrypt operation of AES-128 block size and 256 key size in the CBC mode of operation. The test passes only if the calculated result equals the known result for both encryption and decryption. The AES KAT must execute successfully before accessing the AES functionality.
HMAC SHA-1	This module implements the short messages test as part of KAT for SHA-1 and later the HMAC validation testing is done. Short Messages Test tests the ability to correctly generate message digests for messages of smaller length.
HMAC SHA-256	This module implements the short messages test as part of KAT for SHA-256 and later the HMAC validation testing is done. Short Messages Test tests the ability to correctly generate message digests for messages of smaller length.
DRNG	This module tests whether the random number generated is deterministic. This test compares a known seed and known output against the random number generated.
RSA sign/verify	This module implements a KAT for signing and verification operation of RSA. The test passes only if the signature is verified. The KAT must execute successfully before the operator can access the RSA functionality.
AES GCM	This module implements a KAT for AES encryption and decryption using GCM.
SHA512	This module implements the SHA-512 short message test as part of KAT.
HMAC SHA512	This module implements the short messages test as part of KAT for SHA-512 and later the HMAC validation testing is done. Short Messages Test tests the ability to correctly generate message digests for messages of smaller length.
TLS	Implements the KDF for TLS as per the SP800-131A.
SSH	Implements the KDF for SSH as per the SP800-131A.
EC DSA	Implements the EC DSA pair-wise consistency test.
EC DH	Implements the EC DH test.

The network interface

The device running the Network OS software is managed through an Ethernet port where the following processes respond to process the network packets. All processes are executed under the root privilege.

- Secd: The primary process for major security-related functionality. It supports the following:
  - Authentication and authorization with LDAP and the RADIUS server
  - Authentication, authorization, and accounting with TACACS
  - Role-based access control (RBAC)
  - Authentication and authorization with the local user database management
  - ACL through IP filter on the TCP/UDP connections

- Authd: The process that supports authentication by DH-CHAP.
- TCP/IP stack: The Network OS IP stack from the kernel that accepts all packets from the network interface and applies IP filter rules as configured.
- Syslog-ng: The process that supports logging of audit messages through a TLS tunnel on a remote server.
- SSHd: The process available on port 22 that provides a terminal session after authentication using the SSH protocol.
- Telnetd: The process available on port 23 that provides a terminal session after authentication.

Cryptographic configurations in Common Criteria

The device in Common Criteria mode supports the following cryptographic configurations.

TLS cryptographic configurations

- TLSv1.0, TLSv1.1, and TLSv1.2 protocol versions for TLS communication are supported.
- TLS v1.2 is not supported on RADIUS.
- The AES-128 and AES-256 encryption algorithm (with SHA-1 and SHA-256 as MAC) are supported.
- RSA is used for authentication.
- DES-based cipher suites are not supported.

SSH cryptographic configurations

The following algorithms are supported:

- Host authentication
  - ssh-rsa
  - ecdsa-sha2-nistp256
- Ciphers
  - aes128-cbc
  - aes256-cbc
- Keyed-hash message authentication (HMAC) code
  - hmac-sha1
  - hmac-sha2-256
- Key exchange
  - diffie-hellman-group14-sha1

Commands supported in Common Criteria

The following commands are provided for administrative purposes

- Privileged EXEC mode commands
  - **unhide fips**
  - **fips zeroize**
  - **cipherset**

  - **certutil**
  - **copy**
- Global configuration mode commands
  - **ip access-list**
  - **ip access-group**
  - **ldap-server**
  - **radius-server**
- RBridge configuration mode commands
  - **ssh server key-exchange**
  - **ssh client key-exchange**