Common Criteria Evaluated Configuration Guide for NetScaler 10.5 Platinum Edition

Version 3.6
Oct 13, 2015

citrix.com

Copyright and Trademark Notice

ALTHOUGH THE MATERIAL PRESENTED IN THIS DOCUMENT IS BELIEVED TO BE ACCURATE, IT IS PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE ALL RESPONSIBILITY FOR THE USE OR APPLICATION OF THE PRODUCT(S) DESCRIBED IN THIS MANUAL.

CITRIX SYSTEMS, INC. OR ITS SUPPLIERS DO NOT ASSUME ANY LIABILITY THAT MAY OCCUR DUE TO THE USE OR APPLICATION OF THE PRODUCT(S) DESCRIBED IN THIS DOCUMENT. INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE. COMPANIES, NAMES, AND DATA USED IN EXAMPLES ARE FICTITIOUS UNLESS OTHERWISE NOTED.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio- frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Citrix' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler Request Switch™ 9000 Series equipment. If the NetScaler equipment causes interference, you can try to correct the interference by taking one or more of the following measures:

- Move the NetScaler equipment to one side or the other of your equipment.
- Move the NetScaler equipment farther away from your equipment.
- Plug the NetScaler equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Citrix Systems, Inc., could void the FCC approval and negate your authority to operate the product.

BroadCom is a registered trademark of BroadCom Corporation. Fast Ramp, NetScaler, WANScaler, Citrix XenApp, and NetScaler Request Switch are trademarks of Citrix Systems, Inc. Linux is a registered trademark of Linus Torvalds. Internet Explorer, Microsoft, PowerPoint, Windows and Windows product names such as Windows NT are trademarks or registered trademarks of the Microsoft Corporation. NetScape is a registered trademark of Netscape Communications Corporation. Red Hat is a trademark of Red Hat, Inc. Sun and Sun Microsystems are registered trademarks of Sun Microsystems, Inc. Other brand and product names may be registered trademarks or trademarks of their respective holders.

Software covered by the following third party copyrights may be included with this product and will also be subject to the software license agreement: Copyright 1998 © Carnegie Mellon University. All rights reserved. Copyright © David L. Mills 1993, 1994. Copyright © 1992, 1993, 1994, 1997 Henry Spencer. Copyright © Jean-loup Gailly and Mark Adler. Copyright © 1999, 2000 by Jef Poskanzer. All rights reserved. Copyright © Markus Friedl, Theo de Raadt, Niels Provos, Dug Song, Aaron Campbell, Damien Miller, Kevin Steves. All rights reserved. Copyright © 1982, 1985, 1986, 1988-1991, 1993 Regents of the University of California. All rights reserved. Copyright © 1995 Tatu Ylonen, Espoo, Finland. All rights reserved. Copyright © UNIX System Laboratories, Inc. Copyright © 2001 Mark R V Murray. Copyright 1995-1998 © Eric Young. Copyright © 1995,1996,1997,1998. Lars Fenneberg. Copyright © 1992. Livingston Enterprises, Inc. Copyright © 1992, 1993, 1994, 1995. The Regents of the University of Michigan and Merit Network, Inc. Copyright © 1991-2, RSA Data Security, Inc. Created 1991. Copyright © 1998 Juniper Networks, Inc. All rights reserved. Copyright © 2001, 2002 Networks Associates Technology, Inc. All rights reserved. Copyright (c) 2002 Networks Associates Technology, Inc. Copyright 1999- 2001© The Open LDAP Foundation. All Rights Reserved. Copyright © 1999 Andrzej Bialecki. All rights reserved. Copyright © 2000 The Apache Software Foundation. All rights reserved. Copyright (C) 2001-2003 Robert A. van Engelen, Genivia inc. All Rights Reserved. Copyright (c) 1997-2004 University of Cambridge. All rights reserved. Copyright (c) 1995. David Greenman. Copyright (c) 2001 Jonathan Lemon. All rights reserved. Copyright (c) 1997, 1998, 1999. Bill Paul. All rights reserved. Copyright (c) 1994-1997 Matt Thomas. All rights reserved. Copyright © 2000 Jason L. Wright. Copyright © 2000 Theo de Raadt. Copyright © 2001 Patrik Lindergren. All rights reserved. Document code: June, 02, 2015 20:15:43

Table of Contents

Introduction Chapter 1

About this Guide

The Common Criteria Evaluated Configuration Guide for Citrix NetScaler 10.5 Platinum Edition describes the requirements and procedures for installing and configuring the Citrix NetScaler appliance in accordance with the Common Criteria evaluated deployment.

If your security requirements and policies require your NetScaler deployment to exactly match the Common Criteria Target of Evaluation configuration, follow the procedures in this guide.

Common Criteria Target of Evaluation

The Common Criteria Target of Evaluation (TOE) is a Citrix NetScaler MPX-FIPS appliance running NetScaler software release 10.5, Platinum Edition with the 53.22 build. The TOE operates as a dedicated self-contained appliance running on dedicated hardware provided as part of the TOE.

This guide supplements the core NetScaler documentation with details of how to configure a NetScaler appliance as a Common Criteria Target of Evaluation configuration.

The NetScaler Common Criteria evaluated deployment covers the following:

- NetScaler Operating System
- Load Balancing
- NetScaler Gateway
- SSL Offloading

This evaluated deployment does not include the following components:

- Application Firewall
- Global Server Load Balancing (GSLB)
- AAA-TM Authentication
- External authentication methods: Kerberos, TACACS+, Radius, SAML
- Responder
- Rewrite (URL Transformation)
- DNS
- EdgeSight
- Layer 3 Routing

- NetScaler GUI, Dashboard, Command Center application and NetScaler Nitro API
- vPath
- RISE
- High Availability
- CloudBridge
- CallHome
- Integrated Caching
- General TLS VPN functionality
- Clientless VPN
- Web Logging
- Use of superuser privileges, except as described in this guide

Citrix NetScaler Documentation

This guide occasionally refers to the following Citrix product documentation. Except for the first document in the list, all of the documentation is available at http://docs.citrix.com. The PDFs of these docs are also available in the CC documentation bundle and can be downloaded from https://www.citrix.com/content/dam/citrix/en_us/documents/downloads/netscaler-adc/Common-criteria-documents-for-NetScaler-10.5.zip.

- Common Criteria Security Target for Citrix NetScaler 10.5, Platinum Edition. Describes the Target of Evaluation, which details assumptions such as the physical environment, the password policy used, and the rights and assumptions concerning the administrators.
- The Citrix NetScaler 10.5 System Guide (See "ns-system-wrapper-10-con.new.generateall.pdf", dated Oct 13,2015 in the CC documentation bundle).
- The Citrix NetScaler 10.5 Getting Started Guide (See "ns-gen-getting-started-wrapper-10-con.new.generateall.pdf", dated Oct 13, 2015 in the CC documentation bundle).
- The Citrix NetScaler 10.5 Hardware Installation and Setup Guide (See "ns-gen-hardware-wrapper-10-con.new.generateall.pdf", dated Oct 13, 2015 in the CC documentation bundle).
- The Citrix NetScaler 10.5 Migration Guide (See "ns-gen-migration-wrapper-con-10.new.generateall.pdf", dated Oct 13, 2015 in the CC documentation bundle).
- The Citrix NetScaler 10.5 Traffic Management Guide (See "ns-tmg-wrapper-10-con.new.generateall.pdf", dated Oct 13, 2015 in the CC documentation bundle).
- The Citrix NetScaler 10.5 Optimization Guide (See "ns-optimization-wrapper-10-con.new.generateall.pdf", dated Oct 13, 2015 in the CC documentation bundle).

- The Citrix NetScaler 10.5 Security Guide (See “ns-gen-appsec-wrapper-10-con.new.generateall.pdf”, dated Oct 13, 2015 in the CC documentation bundle).
- The Citrix NetScaler 10.5 AppExpert Guide (See “ns-appexpert-con-10.new.generateall.pdf”, dated Oct 13, 2015 in the CC documentation bundle)
- The Citrix NetScaler 10.5 Reference Guide (See “ns-reference-con.new.generateall.pdf”, dated Oct 13, 2015 in the CC documentation bundle)

Overview Chapter 2

This section describes the Common Criteria evaluated deployment and explains what you must do before installing and configuring the Citrix NetScaler appliance. It also outlines the system requirements for the various components.

NetScaler Overview

The Citrix NetScaler product is an application delivery controller (ADC) that delivers dynamic and real-time content from web servers to clients and optimizes complex application environments. When deployed in the datacenter, it provides a single point of control for all the web servers and determines the security and performance needs of the applications

The NetScaler ADC is available on a range of hardware platforms, and as virtual appliances that you can host on your hardware or in a cloud.

To account for the different environments in which the NetScaler ADC might have to be deployed, it is available in multiple form factors.

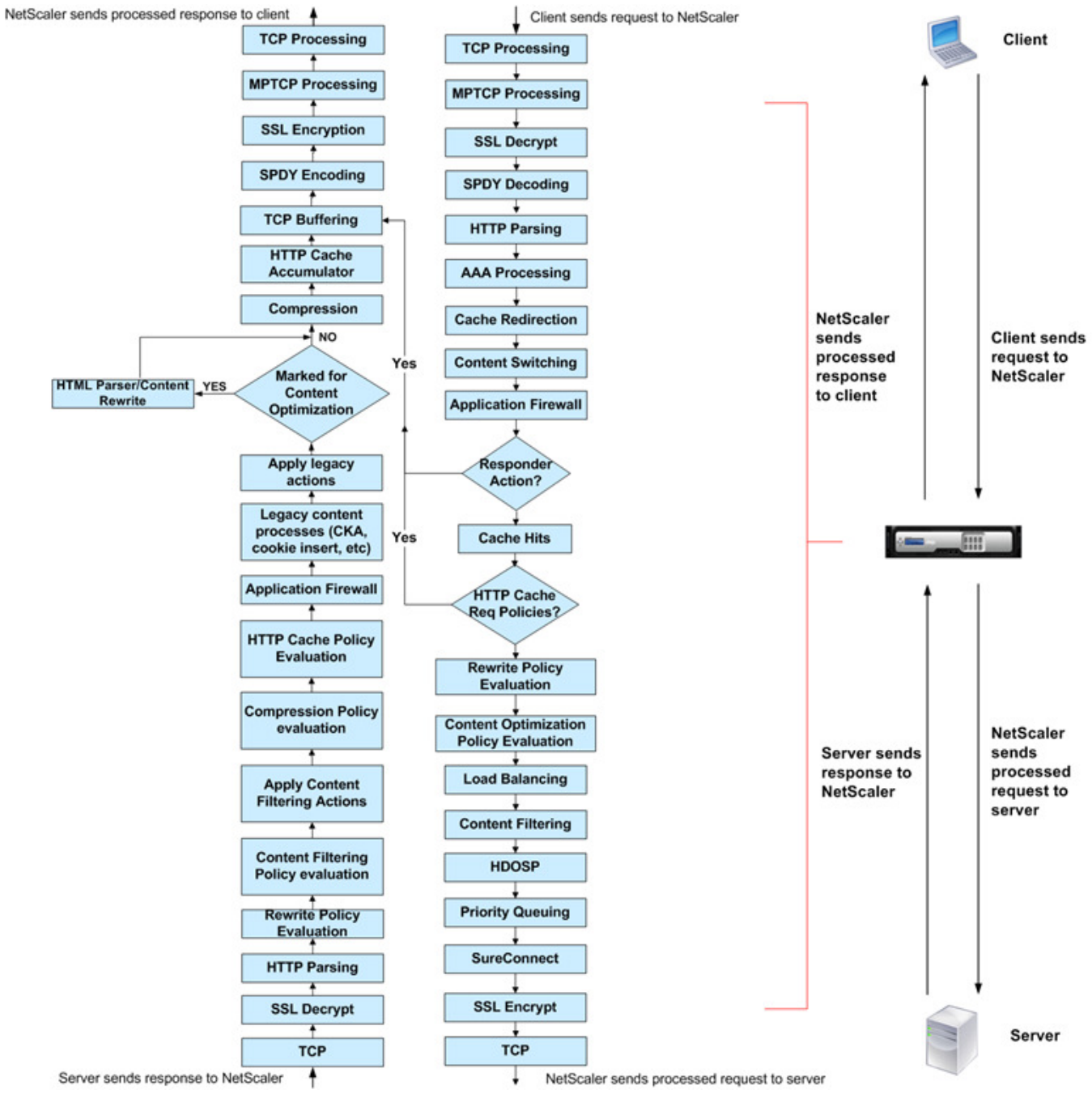
The NetScaler ADC can be delivered in the following form:

From factor	Description
NetScaler MPX-FIPS	NetScaler MPX-FIPS is a high-performance hardware platform, capable of operating at from 500 Mbps to 120 Gbps. NetScaler MPX-FIPS is available in a variety of models that broadly differ in their performance and hardware specifications.

Packet Flow through NetScaler

Depending on requirements, you can choose to configure multiple features. For example, you might choose to configure both compression and SSL offload. As a result, an outgoing packet might be compressed and then encrypted before being sent to the client.

The following figure shows the Layer-7 packet flow through a NetScaler appliance.



Common Criteria Evaluated Deployment

A NetScaler appliance resides between the clients and the servers, so that client requests and server responses pass through it. In a typical installation, virtual servers configured on the appliance provide connection points that clients use to access the applications behind the appliance. Privileged, competent users administer this Target of Evaluation (TOE).

The following Figure 1 shows the detailed deployment configuration of the TOE.

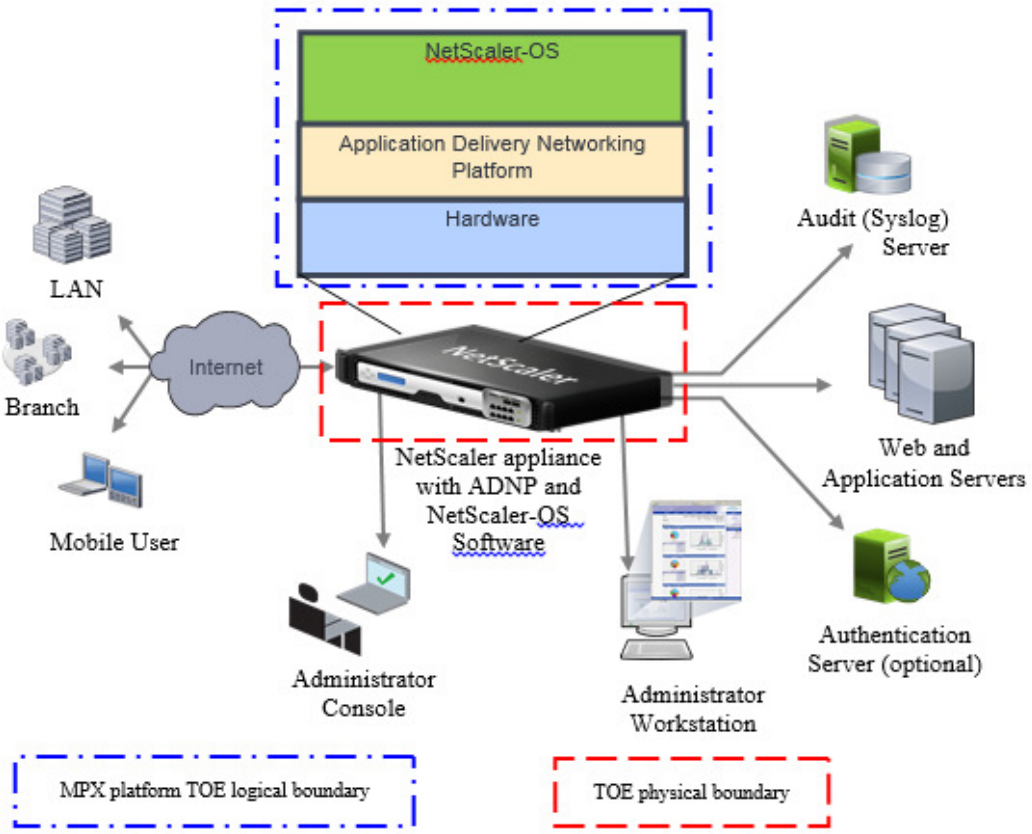


Figure 1: Deployment Configuration of the Product and TOE Boundaries

NetScaler optimizes delivery of applications over the Internet and private networks, combining application-level security and traffic management in a single, integrated appliance. You install a NetScaler appliance in your server room and route all connections to your managed servers through it. The NetScaler features that you enable and the policies you set are then applied to incoming and outgoing traffic.

Components

The Target of Evaluation (TOE) components of NetScaler in the common criteria evaluated deployment are:

- **Load Balancer**. Distributes client requests across several servers and thus optimizes the utilization of resources.
- **NetScaler Gateway**. Provides administrators with a means to securely access and manage the NetScaler appliance from remote locations through a TLS channel.
- **MPX-FIPS hardware platforms**. The hardware platforms available for the evaluated deployment are: MPX 9700 FIPS, MPX 10500 FIPS, MPX 12500 FIPS, MPX 15500 FIPS. For more information on the hardware platforms, see "Introduction to the Hardware Platforms" at www.edocs.citrix.com.

Environment Assumptions

The following assumptions are made regarding the Target of Evaluation (TOE).

- TOE-stored cryptographic data is physically and procedurally protected against tampering.
- Users and administrators choose sufficiently strong passwords (relative to the risk in the deployment environment, and any password policies in force), and maintain their confidentiality.

  Note: Make sure you choose a strong password. For more information on password complexity, see Setting Strong Passwords on page 27.

- The external authentication servers operate correctly and securely (relative to the risk in the deployment environment, and any relevant policies in force). Data transmitted between the TOE and the external servers is protected from tampering by untrusted parties during transfer to the external server, during storage on the external server, and during transmission to the TOE from the external server.
- The TOE is installed and configured according to the appropriate installation procedures, and all traffic between the internal and external networks flows through it.
- The TOE is located within a controlled access facility, which restricts physical access to the appliance to authorized persons only. The location must provide uninterruptible power (protected against surges), air conditioning, and all other conditions required for reliable operation of the hardware.
- One or more competent individuals are assigned the role of administrator to manage the TOE and the security of the information it contains.
- The TOE environment provides the required network connectivity, and the connectivity is protected from tampering. TOE management is performed only from the internal protected network.
- Users and administrators of the TOE are non-hostile, appropriately trained, and follow all user

guidance.

- Attackers who are not TOE users have public knowledge of how the TOE operates, have a basic level of skill and limited resources for altering TOE configuration settings or parameters, and have no physical access to the TOE.
- The TOE does not provide any computing capabilities such as hosting and running user applications. The only services available are for operation, administration, and support of TOE.
- The installer of the TOE is familiar with the documents listed in "Citrix NetScaler Documentation."

External Software and Hardware Requirements

The following table describes the external software and hardware requirements for the Target of Evaluation (TOE).

Category	**Requirements**
Management workstation	Any workstation capable of supporting the SSH client
Client workstations	Any client workstation capable of running the NS Gateway client plug-in's
Backend servers for load balancing	Any network enabled server that supports IPv4
Authentication server	A server that supports Lightweight Directory Access Protocol (LDAP)
Syslog server	Any network enabled server with SSH access
Network	TCP/IP network with IPV4 support

Installing and Verifying Citrix NetScaler Installation Chapter 3

This chapter explains how to install and perform initial configuration on the NetScaler hardware in the Common Criteria evaluated deployment. It also provides the upgrade procedures and tells you how to verify proper installation of the software.

Physical Deployment Modes

You need to configure the NetScaler appliance in two-arm mode to comply with the Common Criteria evaluated configuration. In the two-arm mode, multiple network interfaces are connected to different Ethernet segments, and the appliance is placed between the clients and the servers. It has a separate network interface to each client network and a separate network interface to each server network. The appliance and the servers are on different subnets in this configuration.

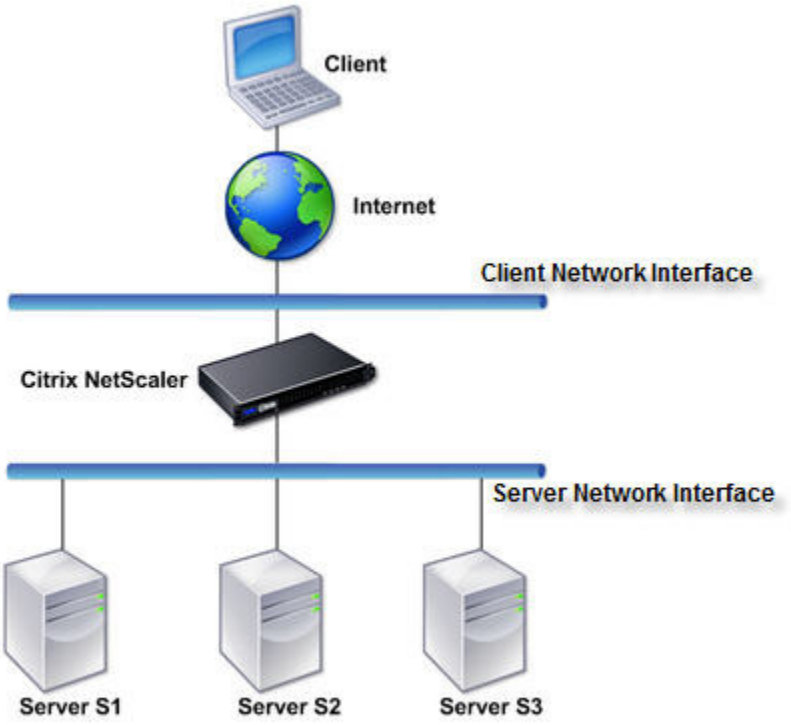
The basic variations of two-arm topology are multiple subnets, typically with the appliance on a public subnet and the servers on a private subnet, and transparent mode, with both the appliance and the servers on the public network.

Setting up a Simple Two-Arm Multiple Subnet Topology

In a simple two-arm multiple subnet topology, the NetScaler appliance is between the clients and the servers, with a virtual server configured to handle the client requests. This configuration is used when the clients and servers are on different subnets, the clients on public subnets and the servers on private subnets.

For example, consider a two-arm NetScaler deployment for managing servers S1, S2, and S3, with a virtual server of type HTTP configured on the NetScaler appliance, and with HTTP services running on the servers. The servers are on a private subnet, and a subnet IP (SNIP) address is configured on the appliance, for communication with the servers. The Use Source IP (USIP) option must be enabled on the appliance so that it uses the SNIP instead of a mapped IP (MIP) address.

In two-arm mode, the NetScaler appliance isolates the client and the server networks and has separate network interfaces for client and the server, as shown in the following figure.



For the configuration procedure, see “Setting up Common Two-Arm Topologies” at www.edocs.citrix.com.

Installing the NetScaler Hardware

After you have determined that the location where you will install your appliance meets the environmental standards listed in Environment Assumptions on page 6, and the server rack is in place as specified in the instructions, you are ready to install the hardware. After you mount the appliance, you are ready to connect it to the network, to a power source, and to the console terminal that you will use for initial configuration. Make sure that all the configurations are completed before you connect the appliance to the network. To complete the installation, you turn on the appliance. Be sure to observe the cautions and warnings listed with the installation instructions.

Common Criteria requirements must be applied before the NetScaler appliance is deployed for operational use.

For instructions on installing the NetScaler Hardware, see “Preparing for Installation” and “Installing the Hardware” at www.edocs.citrix.com.

Verifying the Hardware

You should make sure that the NetScaler hardware is authentic by first verifying that the shipping label on the outside of the package lists the exact hardware ordered, and then that the listed serial number matches the

serial number of the enclosed hardware. You should also examine the hardware to verify that the tamper seals are not damaged.

You should also compare the tracking number on the package to the shipping number provided by Citrix in an email, and verify that they are the same. In most cases, the tracking number is on the UPS label. You can also view the status of an order by logging onto the Citrix online customer support portal at http://support.citrix.com.

FIPS Mode Self-Test

When the NetScaler appliance is powered on, a FIPS card self-test checks the integrity of the card. The self-test runs every time the board comes up, and it blocks all data operations if the test fails. In that case, the startup console displays the error message `NGFIPS: ERROR!!! Secure handshake failed`.

The following three daemons use the OpenSSL FIPS module:

- nsaad
- sshd
- nsnetsvc

By default the daemons are not configured in FIPS mode. You need to first set the mode in NetScaler CLI, using the following commands. For additional details, see Enabling FIPS Mode.

- **set system parameter -fipsUserMode** (ENABLED | DISABLED)
- **save ns config**

Once this is done, an environment variable is set, which then informs the daemons to initialize themselves in FIPS mode. The device should be cold-rebooted after this. During reboot, if the bring-up of the FIPS lib fails, the following error message is reported:

error:2D06C06E:FIPS routines:FIPS_mode_set:fingerprint does not match

To verify that the FIPS Mode is working fine, drop into shell. Type the following command to verify that the value is 1, indicating that the FIPS Mode is on:

- **shell**

```
root@ns# sysctl netscaler.fips_mode
root@ns# netscaler.fips_mode: 1
```

If the FIPS module fails to start properly, the above daemons will not initialize. If any daemon fails to start, an error message is displayed on the console during reboot. You can try to reboot the device one more time to closely monitor the messages on the console. If the issue persists, contact Citrix support for further instructions and provide them the details of the console message(s).

Initial Access and Configuration

After installing the hardware, access the NetScaler appliance through the serial console for initial configuration. Through the serial console, you can change the system IP address, create a subnet or mapped IP address, configure advanced network settings, and change the time zone. You can run a script to perform most of the initial configuration. This script is part of the software and not provided separately. You then specify a route for administrative access to the appliance through your network, and you can specify administrator credentials. Only users with superuser privileges can perform the initial configuration.

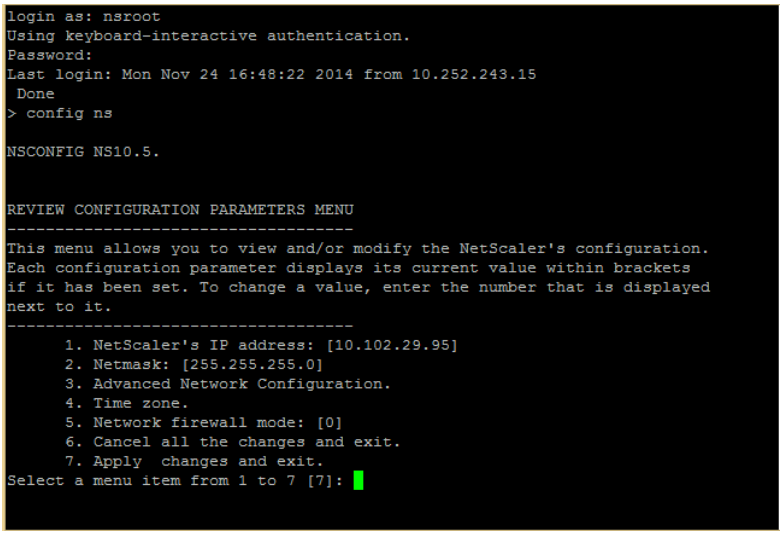
Note: The RS232 serial console port is on the front of each appliance and provides a connection between the appliance and a computer, allowing direct access to the appliance for initial configuration or troubleshooting.

To configure initial settings by using a serial console:

1. Connect the console cable to the appliance and your computer.
2. On your computer, run the vt100 terminal emulation program of your choice to connect to the appliance.
   - For Microsoft Windows, use a terminal emulation client such as PuTTy.
   - For Apple Macintosh OSX, use the GUI-based terminal program or the shell-based telnet client.

   Note: OSX is based on the FreeBSD UNIX platform. Most standard UNIX shell programs are available from the OSX command line.

   - For UNIX-based workstations, use the shell-based Telnet client or any supported terminal emulation program.
3. Press ENTER. The terminal screen displays the logon prompt.
4. Log on to the appliance with the administrator credentials.
   Your sales representative or Citrix Customer Service can provide the initial administrator credentials.
5. At the prompt, type `config ns` to run the NetScaler configuration command, which invokes a script. The script is built into the software.



When finished with the configurations in `config ns` script, run the following commands to set the NetScaler IP (NSIP) address (the management address) and administrator credentials:

- `add route <network> <subnetMask> <gateway>`
- `set system user <userName> <password>`
- `save ns config`

Example

```
add route 0.0.0.0 0.0.0.0 10.102.29.1

set system user nsroot administrator save ns config

reboot
```

Note:

1. The NSIP address should be non-routable, to prevent an attacker from breaching your ability to send packets to the appliance. This is because dynamic routing is always enabled on the NSIP address and cannot be disabled.
2. The NSIP address should not be publicly accessible, and proper security measures should be in place to authorize users who access the NSIP address to configure the TOE. For more information, see "User Access Control".

Accessing the NetScaler Appliance Through the CLI

After the NSIP address is configured as described in the previous section, the administrators can access the NetScaler appliance through the SSH Command Line Interface (CLI). To configure SSH for NetScaler, see Configuring SSH for NetScaler. The CLI is the primary interface for management access to the NetScaler appliance.

To log on to a NetScaler Appliance by using an SSH client

1. Start the SSH client.
2. For initial configuration, use the default NetScaler IP address (NSIP), which is 192.168.100.1. For subsequent access, use the NSIP that was assigned during initial configuration. Select SSH2 as the protocol.
3. Log on by using the administrator credentials, for example:

```
login as: nsroot
Using keyboard-interactive authentication
Password:
Last login Tue June 16 10:37:28 2014 from 10.102.29.9
```

To exit from the administrator session

To exit from the administrator session, type the following command at the command prompt:

```
#root quit
```

Accessing the Host Operating System Shell Through the CLI

Some low maintenance activities require access to the shell of the FreeBSD operating system. For example, upgrading the system firmware requires shell access. Only the system users who have been bound to the super user command policy can access the operating system shell.

To access the system shell

1. Using the CLI, log in as a super user.
2. At the CLI, enter the following command:

   - `shell`

   If the command succeeds, the following output appears:

   - `shell`

   ```
   Copyright (c) 1992-2008 The FreeBSD Project.
   Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,
   1994
   The Regents of the University of California. All rights reserved.


   root@ns#
   ```

3. To return to the NetScaler CLI, enter the following command:

   ```
   root@ns# exit
   ```

Verifying the Common Criteria Software Version Installed

The NetScaler hardware ships with the latest version of the product software already installed, which might or might not be the Common Criteria-certified version of the TOE software. You can verify the installed software version from the NetScaler CLI.

To verify whether the common criteria version of the software is installed, log on to the CLI and type:

- `Show version`

The correct Common Criteria version is marked on the download site. When making an SSL connection to the Citrix site, you should confirm that the URL in the browser is https://www.citrix.com/.

If the correct version is not installed, you can upgrade to the Common Criteria-certified version. You can find the latest version of security target (ST) at http://www.citrix.com/downloads/netscaler-adc.html. Login to your Citrix account to access the target download.

Configuring NetScaler Gateway

NetScaler Gateway provides administrators with a means to securely access and manage the NetScaler appliance from remote locations through a TLS channel. It gives IT administrators a single point of control, and tools to help ensure compliance with regulations and the highest levels of information security across and outside the enterprise.

Following is an overview of the main steps in configuring the SSL VPN:

- Enable SSL VPN feature.
- Create SSL VPN virtual server(vserver).
- Create and submit a CSR to get a signed certificate.
- Install the received certificate.
- Set the appropriate configuration parameters for the SSL VPN to establish a tunnel.
- Create AAA user accounts to access the SSL VPN.
- Set the appropriate IP ACLs to ensure that all traffic is flowing through the SSL VPN tunnel.
- Log on to the SSL VPN, using the AAA user account via the NS Gateway URL that has been configured for the appliance. Verify that the SSL VPN client is downloaded and installed.
- Log on to the NetScaler CLI, using the system account credentials assigned to the user.
- To log off, the user must log off from the CLI as well as from the SSL VPN.

Enabling NetScaler Gateway

Before configuring your initial NetScaler Gateway setup, enable the NetScaler Gateway feature.

To enable NetScaler Gateway by using the command line

At the NetScaler command prompt, type the following command to enable NetScaler Gateway and verify the configuration:

```
> enable ns feature SSLVPN

> show ns feature
```

Configuring an SSL VPN Virtual Server

To configure a SSL VPN virtual server

1. Add an SSL VPN server. At the command line, type:

   > add vpn vserver <name> <serviceType> (<IPAddress> [-range <positive_integer>]) <port>
   where
   <serviceType> is the protocol used by the NetScaler Gateway virtual server. This is a mandatory argument. Possible value: SSL. Default: SSL

   Example:
   add vpn vserver vs ssl 10.217.205.2 443

2. Add a certificate key pair. At the command line, type:

   > create fipskey <keyname> –modulus 1024

   > create certreq <reqFile> -fipsKeyName <keyname> -countryName <string> -stateName <string> -organizationName <string>

   > create cert <certFile> <reqFile> <certType> [-CAcert <input_filename>] [-CAkey <input_filename>] [-CAserial <output_filename>]

   Note: You can use the internal CAcert and CAkey to create the certificate as stated in the given example. You also have the option to submit the CSR to external CA, such as Thawte or VeriSign.

   > add certkey <fips.ckp file name> -cert <fips cert name> -fipsKey <keyname>

   Example:
   create fipsKey test_ndpp_key -modulus 2048 -exponent 3

   create certReq test_ndpp_csr -fipsKeyName test_ndpp_key -countryName us -stateName CA -organizationName Citrix -commonName test_ndpp_key

   create cert test_ndpp_cert test_ndpp_csr SRVR_CERT -CAcert ns-root.cert -CAkey ns-root.key -CAserial ns-root.srl

add ssl certkey test_ndpp_certKey -cert test_ndpp_cert -fipskey test_ndpp_key

3. Bind the SSL VPN server created in step 1 and the certkey create in step 2. At the command line, type:

   > bind ssl vserver <vServerName> -certkey <string>

   Example:
   bind ssl vserver vs -certkey test_ndpp_certKey

Once the TLS channel to VPN server is established, use a client such as putty to initiate an SSH connection to connect to the NetScaler appliance for administrative purposes.

Configuring ACLs for the SSH traffic

1. Deny all SSH connections from outside
   - add ns acl default_deny DENY -destIP = 10.217.206.60 -priority 100 -kernelstate SFAPPLIED61
2. Allow remote connection only from an internal SNIP. The SSH connection opened over the TLS –VPN comes with SNIP to the SSH daemon.
   - add ns acl local_access ALLOW -srcIP = 10.217.206.63 -destIP = 10.217.206.60 -destPort = 22 -protocol TCP -priority 5 -kernelstate SFAPPLIED61
3. Apply the ACL rules
   - apply ns acls

Creating Local AAA User Accounts

You can create user accounts locally on the NetScaler Gateway appliance to supplement the accounts on authentication servers. For example, you might want to create local user accounts for temporary users, such as consultants or visitors, without creating an entry for those users on the authentication server.

For local authentication, create users and then add them to groups that are created on the NetScaler Gateway. After configuring users and groups, you can apply authorization and session policies, create bookmarks, specify applications, and specify the IP address of file shares and servers to which the user has access.

System users need two accounts. In addition to system account to access CLI, each system user also needs to be added as AAA user to authenticate to the SSL VPN for remote as well as local management of the device.

To create local users

At the NetScaler command prompt, type

- `add aaa user <userName> {–password }`

Example:

```
add aaa user user1 password asDf@ns1
```

Accessing the NetScaler Appliance Remotely

You can remotely administer your NetScaler appliance. Remote access to NetScaler appliance is possible only through a TLS-VPN tunnel. You first need to authenticate to the VPN virtual server. After the authentication to the VPN virtual server succeeds, you can connect to the NSIP address through an SSH connection to access the CLI. This method of remote access to a NetScaler appliance provides two layers of security during a remote access.

Note: Depending on the routing configuration in your lab network, you might have to configure the NSIP and SNIP to be in the same network in order for the loopback communication between SNIP and NSIP to work.

To access NetScaler appliance remotely

1. Add a user as a system user and as an AAA user.

   - `add system user <userName>`

     `Enter password:`

     `Confirm password:`

   - `add aaa user <userName> password <Password>`

2. Verify that the ACLs are accurately configured to block SSH access except from the SNIP address, as described above in the *Configuring ACLs for the SSH traffic* section.

3. Bind the system user to the **sysadmin** policy, which is one of the default command policies.

   - `bind system user <userName> sysadmin <priority>`

4. Make sure that the VPN param has the authorization action set to Deny.

   - set vpn parameter -defaultAuthorizationAction DENY

5. Bind the following policy to allow SSH access.

   - add authorization policy Allow_SSH_Access "REQ.TCP.DESTPORT == 22" ALLOW
   - bind aaa user <username> -policy Allow_SSH_Access

Note: The user first logs into VPN using his AAA credentials. After AAA authentication to log into SSL VPN tunnel, the user can then use SSH to log into NSIP by providing his system user credentials. He now has access to the CLI to manage the appliance.

Upgrading the NetScaler Software Version

You can upgrade the software from an earlier release to the latest release, or you can upgrade from an earlier build to a later build of the same release.

Note: Prior to upgrading the appliance firmware, Citrix recommends that you back up the current system configuration. Refer to the section *Backing Up the Current NetScaler Installation* for details regarding the backup procedure.

Only the superuser role has privileges to perform this procedure.

Note: If access policies do not permit superusers to log on remotely, this procedure must be completed using local console access.

Download the Firmware Package onto a Staging Server or Workstation

To download or verify the correct Common Criteria version:

1. From a server or workstation with an Internet connection, go to download.citrix.com and click **Downloads**.
2. Under **Log in to access more downloads**, enter your username and password.
3. In **Search Downloads by Product**, select **NetScaler ADC**.
4. In **Select Product Version**, select the release number, NetScaler 10.5
5. Under **Results for**, in **Firmware**, click the relevant Common Criteria build, Release 10.5 Build 53.22 (nCore) (Common Criteria Build).
6. On the build page, scroll to the bottom of the page and click **Download**.
    a. Download both the firmware package and its SHA256 hash signature
7. In the **End-User License Agreement** pane, click **Yes** to accept the agreement, and then follow the instructions in the download pane.

Note: You can use your hardware serial number (HSN) or your license activation code (LAC) to allocate your licenses. Alternatively, if a license is already present on your local computer, you can upload it to the appliance. For details regarding Licensing framework, see NetScaler Licensing Overview.

Transfer the Firmware Package to the NetScaler Appliance and Verify its Integrity

After downloading the firmware upgrade package and the SHA256 signature to the staging server or workstation, complete the following steps:

Note: The activities that follow require superuser access. If access policies do not permit superusers to log on remotely, this procedure must be completed using local console access.

1. Using a secure file transfer utility, such as SCP or winSCP, transfer the firmware package and the signature file from the staging host to the `/var/nsinstall` directory of the NetScaler appliance.

   Note: You need the superuser credentials in order to authenticate to the secure file transfer utility.

2. Once the file transfer is complete, log on to the NetScaler CLI as a superuser using an SSH client.
3. Change your command prompt to the shell prompt by typing `shell` at the command line interface.
4. Navigate to `/var/nsinstall` directory:
   `root@ns# cd /var/nsinstall`
5. Locate the firmware package and execute following command to compute the SHA256 hash on the installation package:

   ```
   root@ns# openssl dgst –sha256 <firmware-installation-package>
   ```

6. The hash of the firmware update package is stored in the `sha256` output file. This should be compared with the hash that you got from download.citrix.com. If the hash values do not match, the downloaded firmware package should be discarded.

   Note: download.citrix.com is an HTTP site. After you sign in to download the software, you are directed to an HTTPS site for downloading the software.

Install the Firmware Update

1. If you have completed steps 1-6 in the above section, you should be logged in as a superuser and operating from the `/var/nsinstall` directory. If not, the execute the *shell* command and change to the directory into which the firmware update package was copied. That is, `cd /var/nsinstall`.
2. Citrix recommends that you create a location for the installation package under the `/var/nsinstall` directory as follows:
   `root@ns# mkdir <releasenumber>nsinstall`

3. Move the installation package into the newly created installation directory and unpack the archive as follows:

   ```
   root@ns# mv <releasenumber>nsinstall_nc.tgz <releasenumber>nsinstall
   root@ns# tar xvfz <releasenumber>nsinstall_nc.tgz
   ```

4. Run the installation script to install the new version of the system software as follows:

   ```
   root@ns# ./installns
   ```

When the installation script is complete, you will be prompted to reboot the appliance. Accept the prompt and wait for the appliance to restart.

Verifying that the Correct Software is installed

After the software update is complete, it is necessary to validate the installation. Refer to the Verifying the Common Criteria Software version Installed Verifying the Common Criteria Software Version Installed section for the verification steps. If verification fails to confirm the correct software version, it will be necessary to roll back the software upgrade. To roll back the software upgrade, downgrade to a previous firmware version as follows.

Downgrading to a Previous Firmware Version

Occasionally it may be desirable or necessary to downgrade the firmware installation to a previously installed version. You can downgrade a standalone NetScaler appliance to any earlier release by using the command line interface.

Note: Loss in configuration may occur when downgrading. You should compare the configurations before and after the downgrade, and then manually read any missing entries.

The activities that follow require superuser access. If access policies do not permit superusers to log on remotely, this procedure must be completed using local console access.

1. Open an SSH connection to the appliance by using an SSH client, such as PuTTY.
2. Log on to the appliance by using the superuser credentials.
3. Execute the shell command to escape to the FreeBSD shell, then change to the installation directory

   ```
   cd /var/nsinstall
   ```
4. If the installation package for the previous firmware version is not present in the installation directory, download and transfer the firmware package to the appliance as described in the above sub-sections entitled:

   a. Download the Firmware Package onto a Staging Server or Workstation, and
   b. Transfer the Firmware Package to the NetScaler Appliance and Verify its Integrity

   Important: If routing is enabled, perform step 5. Otherwise, skip to step 6

5. While still logged in to the appliance as a superuser and at the shell prompt, create a copy of the ns.conf file. At the shell prompt, type:

   ```
   cd /nsconfig
   cp ns.conf ns.conf.NS10.5<currentbuildnumber>
   ```

Note: You should back up the configuration file on another computer. You will need to use a secure file transfer tool on your workstation to copy the backup file from appliance to the backup location. For example:

Winscp.exe nsroot@<netscaler-nsip>:/nsconfig/ns.conf.<backup-version> c:/backups/ns.conf

The above is executed from a windows workstation to copy the backup from the NetScaler appliance to the workstation file system.

6. Copy the `<releasenumber>` configuration file `(ns.conf.NS<releasenumber>)` to `ns.conf`. At the shell prompt, type:

```
cp ns.conf.NS<releasenumber> ns.conf
```

Note: `ns.conf.NS<releasenumber>` is the backup configuration file that is automatically created when the system software is upgraded from release `<releasenumber>` to the current release. The downgrade might result in some loss of configuration. After the appliance restarts, compare the configuration saved in step 3 with the running configuration, and make any adjustments for features and entities configured before the downgrade. Save the running configuration after making the changes.

7. If routing is enabled, the ZebOS.conf file contains the configuration. At the shell prompt, type:

a. `cd /nsconfig`
b. `cp ZebOS.conf ZebOS.conf.NS`
c. `cp ZebOS.conf.NS<targetreleasenumber> ZebOS.conf`

8. When the above steps are completed change directories to the location of the downgrade installation package under the /var/nsinstall directory, unpack the firmware archive if necessary, and run the installation script as shown in the above sub-section entitled *Install the Firmware Update*.

Backing up the Current Installation

Depending on the type of data to be backed up and the frequency at which you create a backup, you can create a basic backup or a full backup.

- **Basic backup:** Backs up only configuration files. You might want to perform this type of backup frequently, because the files it backs up change constantly. The files that are backed up are:

Directory	Sub-Directory of Files
/nsconfig	• ns.conf

	• ZebOs.conf • rc.netscaler • snmpd.conf • nsbefore.sh • nsafter.sh • monitors
/var/	• download/* • log/wicmd.log • wi/tomcat/webapps/* • we/tomcat/logs/* • wi/tomcat/conf/catallina/localhost/* • nslw.bin/etc/krb.conf • netscaler/locdb/* • lib/likewise/db/* • vpn/bookmark/* • netscaler/crl • nstemplates/* • learnt_data/*
/netscaler/	• custom.html • vsr.htm

- **Full backup:** In addition to the files that are backed up by a basic backup, a full backup backs up some less frequently updated files. The files that are backed up when using the full backup option are:

Directory	Sub-Directory or Files
/nsconfig/	• ssl/* • license/* • fips/*
/var/	• netscaler/ssl/* • wi/java_home/jre/lib/security/cacerts/* • wi/java_home/lib/security/cacerts/*
/nsconfig	• ssh/* • sshd_config

The backup is stored as a compressed TAR file in the `/var/ns_sys_backup/` directory. To avoid issues due to non-availability of disk space, you can store a maximum of 50 backup files in this directory. You can use the rm system backup command to delete existing backup files so that you can create new ones.

Note:

- While the backup operation is in progress, do not execute commands that affect the configuration.
- If a file that is required to be backed up is not available, the operation skips that file.

To back up the NetScaler appliance by using the NetScaler command line interface:

At the command prompt, do the following:

1. Save the Netscaler configurations.
   `save ns config`
2. Create the backup file.
   `create system backup [<filename>] -level <basic|full> -comment<string>`

   Note: If the file name is not specified, the appliance creates a TAR file with the following naming convention: `backup_<level>_<nsip_address>_<date-timestamp>.tgz.`

   Example: The following command backs up the full appliance, using the default naming convention for the backup file.
   `> create system backup –level full`

3. Verify that the backup file was created.
   `show system backup`
   You can view properties of a specific backup file by including the **`fileName`** parameter.

Reverting the Settings to Factory Defaults

You can clear the configuration on your NetScaler appliance to revert the settings to factory defaults.

At the NetScaler command prompt, type:

`clear ns config <level>`

where level is one of the following:

- Basic. Clears everything except NSIP, MIPs, SNIPs, network settings, HA node definitions, features and mode settings, and the nsroot account.
- Extended. Clears everything except NSIP, MIPs, SNIPs, network settings, and HA node definitions.
- Full. All settings except the NSIP and default gateway are reset to their factory default values. The NSIP address is left unchanged so that the appliance does not lose network connectivity.

Understanding NetScaler Users and Roles
Chapter 4

Configuring System User Access Control

To configure NetScaler authentication and authorization, you must first define the users who have access to the NetScaler appliance, and then you can organize these users into groups. After configuring users and groups, you need to configure command policies to define types of access, and assign the policies to users and/or groups.

NOTE: You must log on as a super user to configure users, groups, and command policies. The default NetScaler super user name is nsroot and has the *superuser* command policy grant.

If access policies do not permit superusers to logon remotely, this procedure must be completed using local console access.

Creating System User Accounts

NetScaler system users who have the *superuser* command policy grant can create and modify system user accounts.

At the NetScaler command prompt, type the following command to create a user account and verify the configuration:

```
add system user <userName>

sh system user
```

Example

```
> add system user testusr

> Enter password:

Done
```

Note: You must enter a password for the new system user account to create the account.

```
> sh system user

1) User name: nsroot

2) User name: testusr

Done
```

Note: System users with the *superuser* command policy grant can also create a group, assign users to that group, and bind the command policies to the group.

Binding Command Policies to the System User Account

Command policies regulate which commands, command groups, virtual servers, and other entities users and user groups are permitted to use. The NetScaler appliance provides a set of built-in command policies, and you can configure custom policies. To apply the policies, you bind them to users and/or groups. Note that only a superuser is allowed to carry out this task.

Here are the key points to keep in mind when defining and applying command policies.

- You cannot create global command policies. Command policies must be bound directly to NetScaler users and groups.
- Users or groups with no associated command policies are subject to the default (DENY-ALL) command policy, and are therefore unable to execute any configuration commands until the proper command policies are bound to their accounts.
- All users inherit the policies of the groups to which they belong.
- You must assign a priority to a command policy when you bind it to a user account or group account. This enables the NetScaler to determine which policy has priority when two or more conflicting policies apply to the same user or group. Note that if the priorities assigned to conflicting policies are the same, they are evaluated in the order of definition, that is, the one defined earlier is evaluated first.
- The following commands are available by default to any user and are unaffected by any command policies you specify: help cli, show cli attribute, clear cli prompt, alias, unalias, batch, source, help, history, man, quit, exit, whoami, config, set cli mode, unset cli mode, show cli mode, set cli prompt, and show cli prompt.

NetScaler provides built-in command policies as described in table 1 below.

Table 1: Built-in NetScaler Command Policies

Policy Name	Allows
read-only	Read-only access to all show commands except show runningconfig, show ns.conf, and the show commands for the NetScaler command group.
operator	Read-only access and access to commands to enable and disable services and servers or place them in ACCESSDOWN mode.
network	Full access, except to the set and unset SSL commands, sh ns.conf, sh runningconfig, and sh gslb runningconfig commands.
superuser	All access. Same privileges as the nsroot user.

sysadmin	All access to the appliance with the exception of shell access and system user identity and access management

To bind command policies to a user by using the NetScaler command line

Note: Only system users who have the *superuser* command policy can bind command policies to system users. If access policies do not permit superusers to log on remotely, this procedure must be completed using local console access.

At the NetScaler command prompt, type the following commands to bind a command policy to a user and verify the configuration:

```
bind system user <userName> <policyName> <priority>

sh system user <userName>
```

Example

```
> bind system user Admin superuser 1 Done

> sh system user Admin User name:  Admin

Command Policy: superuser  Priority:1
```

In the above example, "1" is the highest possible priority. The higher the number, the lower the priority.

Creating a Superuser

The TOE is shipped with a default superuser, nsroot. This superuser cannot be removed. If multiple users require the superuser command policy grant, Citrix recommends that each user be assigned a unique system account ID with the superuser command policy grant rather than sharing the nsroot account among multiple users.

Note: The following activities require the *superuser* command policy. If access policies do not permit superusers to log on remotely, this procedure must be completed using local console access.

To create a superuser, complete the following steps:

1. Log in as a `super`user.

2. Create a system user.
   ```
   add system user <userName> [-externalAuth ( ENABLED | DISABLED )] [-
   promptString <string>] [-timeout <secs>] [-logging ( ENABLED | DISABLED )]
   ```

   For TOE, the logging parameter should not be used.

   For example:

```
add system user Testsysusr
```

Note: You will be prompted for a password after you enter the above command. You must provide the password to create the account.

3. Bind the user created to a superuser policy.

```
bind system user <userName> <command policy> <priority>
```

For example:

```
bind system user Testsysusr superuser 1
```

Superuser Capabilities and Entitlements

A NetScaler superuser is capable of executing all the CLI commands listed at http://support.citrix.com/proddocs/topic/ns-reference-map-10-5/netscaler-crg-gen-wrapper-con.html. In addition, the following activities are exclusively reserved for the superuser command policy:

1. Creating system users and binding them to the superuser and other command policies
2. Modifying (including password reset) and removing (except nsroot) system user objects
3. Executing the shell command
4. Setting the System time
5. Setting the system logon banner
6. Configuring the system for remote audit logging
7. Directly accessing or managing NetScaler audit logs and other system log files
8. Configuring SSH parameters by directly editing the sshd_config file
9. Directly managing or updating SSH host keys or user keys
10. Copying TLS certificates and keys to the NetScaler appliance by using SCP
11. Running the ldapsearch tool to test LDAP/LDAPS connectivity
12. Upgrading or downgrading the system firmware
13. Direct access to SCP, SFTP, OPENSSL, ssh-genkey, and all native OS commands through the FreeBSD shell.

Note: "nsroot" (default administrator account) and an account with "superuser" are the only accounts allowed to access the Audit data through Secure Shell File Transfer Protocol (SFTP) or Secure Copy (SCP) protocols. All other accounts will be denied access. The nsroot account provides complete access to all NetScaler features.

Creating a SysAdmin User

Note: The following activities require the *superuser* command policy grant. If access policies do not permit superusers to log on remotely, this procedure must be completed using local console access.

To create a *sysadmin* user, complete the following steps:

1. Log in as a `superuser`.

2. Create a system user.
   ```
   add system user <userName> [-externalAuth ( ENABLED | DISABLED )] [-
   promptString <string>] [-timeout <secs>] [-logging ( ENABLED | DISABLED )]
   ```

   For example:

   ```
   add system user Testsysusr_2
   ```

   Note: You will be prompted for a password after you enter the above command. You must provide the password to create the account.

3. Bind the user created to a super user policy.
   ```
   bind system user <userName> <policyName> <priority>
   ```

   For example:

   ```
   bind system user Testsysusr_2 sysadmin 1
   ```

Note: The logging parameter **for add system user** command controls the user's privilege to access the local logs. It is disabled by default. Since we are using scp and cron job to securely transfer the logs, the default setting of this parameter is appropriate.

SysAdmin Capabilities and Entitlements

The System Administrator command policy allows the execution of all documented CLI commands (http://support.citrix.com/proddocs/topic/ns-reference-map-10-5/netscaler-crg-gen-wrapper-con.html) except as follows:

1. The Sysadmin command policy is not able to use the CLI enumerate, create, modify, or remove system user, system group, or system policy objects.
2. The Sysadmin command policy cannot alter the system administrator's own command policy.
3. The Sysadmin command policy cannot execute the shell command to gain access to the FreeBSD shell
4. The Sysadmin command policy cannot perform any of the activities listed in items 4-13 of the section entitled *SuperUser Capabilities and Entitlements*. Additionally the Sysadmin cannot directly execute any native BSD operating system commands.

Recommended Appliance Management Use Cases

In keeping with the principle of least privilege, the sysadmIn command policy should be used for routine appliance administration and configuration activities. The use of the more powerful superuser command policy is intended for low-level activities involved with the initial configuration and setup of the appliance and non-routine maintenance activities such as firmware updates.

The number of users who are granted the superuser command policy should be restricted to the greatest extent possible, taking into account enterprise requirements. Additionally, more restrictive function-specific built-in command policies may be assigned to system users as required. These built-in policies are as follows:

1. read-only
2. operator
3. network

The capabilities and limitations of these built-in command policies are described above in table 1 in the Binding Command Policies to the System User Account section. For additional information concerning NetScaler identity and access management refer to the following:

- For information on configuring users and groups, see: http://support.citrix.com/proddocs/topic/ns-system-10-5-map/ns-ag-aa-config-users-and-grps-tsk.html
- For information on configuring command policies, see: http://support.citrix.com/proddocs/topic/ns-system-10-5-map/ns-ag-aa-config-cmd-poli-tsk.html

Creating a Custom Command Policy

Note: The following activities require the *superuser* command policy grant. If access policies do not permit superusers to log on remotely, this procedure must be completed using local console access.

In some cases, it may be desirable to create a custom command policy to accommodate specialized appliance management requirements. System users who hold the *superuser* command policy grant can create custom command policies as indicated below.

For example, to create a custom command policy that restricts access to the shell, do the following:

1. Add a system user. Type the following command at the command prompt:

```
> add system user Test_usr

Enter password:

Confirm password:

Done
```

2. Add the command policy to prevent access to the shell prompt. Type the following command at the command prompt:

```
> add system cmdPolicy noshell ALLOW  "^(?!(shell|sftp-
server|scp|system)(?!batch)(?!source)(?!diff ns config)).*$"
```

```
Done
```

3. Bind the policy. Type the following command at the command prompt:

```
> bind system user Test_usr noshell 0

Done
```

4. Show the policy bound to the administrator created in step 1.

```
> show system cmdPolicy noshell

Command policy: noshell                Action: ALLOW

cmdspec: ^(!(shell|sftp-server|scp|system)(!batch)(!source)(!diff ns
config)).*$

Done
```

5. Log in as the administrator.

```
> login Test_usr
Enter password:
Done
```

6. Change to the Shell prompt:

```
> shell
ERROR: Not authorized to execute this command [shell]
The error shows that the administrator created does not have access to
the shell prompt.
```

Note: While system users who hold the superuser command policy grant may modify built-in command policies, Citrix does not recommends this practice.

For additional information on creating custom command policies, see:
http://support.citrix.com/proddocs/topic/ns-system-10-5-map/ns-ag-aa-config-cmd-poli-tsk.html

Setting Strong Passwords

Users and administrators of the Target of Evaluation (TOE) must choose strong passwords relative to the risk in the deployment environment and any organizational password policies in force. Examples of password complexity requirements are as follows:

- The password must have a minimum length of eight characters.
- The password must not contain dictionary words or a combination of dictionary words.
- The password must at least include one uppercase letter, one lowercase letter, one number, and one special character.

Note: In UNIX and UNIX-like systems most characters (*, ', etc.) are not interpreted by the shell as special characters if they are placed in double quotes (""). They are treated as literals. However, ", $, `, and \ are still interpreted by the shell, even when they're in double quotes and may have to be escaped. The backslash (\) character is used to mark (escape) these special characters.

You can enforce strong passwords by setting two parameters, one for minimum length of password and the other to enforce complexity.

set system parameter –localAuth (**ENABLED** | **DISABLED**) **–minpasswordlen** <positive_integer> **–natPcbForceFlushLimit** <positive_integer> **–natPcbRstOnTimeout** (**ENABLED** | **DISABLED**) **–strongpassword** (**ENABLED** | **DISABLED**) **–promptString** <string> **–rbaOnResponse** (**ENABLED** | **DISABLED**) **–timeout** <secs>

To set the parameters, at the command line interface enter:

1. Login as a nsroot user.
2. At the command prompt, type:
   ```
   > set system parameter –strongpassword enabled
   Done
   ```
3. ```
   > add system user newUser
   Enter password:
   Confirm password:
   ERROR: Password length should adhere to minimum password length value in system parameter settings.
   ```
   ```

Configuring a NetScaler Appliance Chapter 5

Unless mentioned otherwise, only the NetScaler administrator role or the super user role has the required privileges to perform the configuration tasks described in this chapter.

Note: If access policies do not permit superusers to log on remotely, this procedure must be completed using local console access.

Enabling FIPS Mode

The first configuration that needs to be done on TOE is to enable the FIPS mode. You can enable the FIPS mode on the NetScaler appliance by using the following command the shell prompt:

```
set system parameter –fipsUserMode ENABLED
```

NetScaler FIPS Configuration for the CC-Evaluated Deployment

The following recommendations are specific to the FIPS version of the NetScaler.

- **Change FIPS crypto card passwords**—When using a FIPS certified version of NetScaler with a Hardware Security Module (HSM), change the default Security officer (SO) and set a new user password as shown below. If you don't know the default SO password of an FIPS-enabled NetScaler appliance, contact Citrix Technical Support.

  Note: Only a super user or sysadmin can carry out this task.

  ```
  set ssl fips –initHSM Level–2 <soPassword> <oldSoPassword>

  <user–Password> [–hsmLabel <string>]

  save configuration

  initHSM

  FIPS initialization level. The appliance currently supports
  Level–2 (FIPS 140–2).
  This is a mandatory argument.
  Possible values: Level–2

  hsmLabel
          Label to identify the Hardware Security Module (HSM).
          Maximum Length: 31
  ```

  Note: All data on the FIPS card will be erased with the above command.

- **Store the HSM password in a secure location**—The HSM is locked after three unsuccessful login attempts. When locked, it becomes nonoperational and you cannot alter its configuration.

Note: Keys larger than 2048 bytes cannot be generated.

Changing the Default Administrator (nsroot) Password

The `nsroot` account provides complete access to all features of the Citrix NetScaler appliance. Therefore, to preserve security, the nsroot account should be used only when necessary, and only individuals whose duties require full access should know the password for the nsroot account. Frequently changing the nsroot password is advisable. If you lose the password, you can reset it to the default after reverting the settings to their factory defaults (see Reverting the Settings to Factory Defaults on page 23).

Note: Only a super user or sysadmin can carry out this task. If access policies do not permit superusers to log on remotely, this procedure must be completed using local console access.

To change the nsroot password

At the NetScaler command prompt, type:

```
set system user nsroot <very_long_password>
```

Note: Make sure you choose a strong password. For more information on password complexity, see Setting Strong on page 27.

Configuring Cryptography for NetScaler

Note: Cryptographic engines or algorithm other than those mentioned in CCECG have not been tested.

Creating the System Master Key for Data Protection

While the local data protection requirements for the NetScaler appliance are minimal, it is necessary to create a system master key to protect certain security parameters, such as service accounts passwords required for LDAP authentication and locally stored AAA User Accounts.

To create the system master key:

1. Using the command line interface, log in as a system administrator.
2. Enter the following command:

```
 create kek
Enter PassPhrase:
```

Note: The Pass Phrase must be at least 8 characters long.

Note: If you are changing the data protection key or rotating it, you must use SRM command to securely delete the old key files. To accomplish this, use the following steps:

1. Access the shell prompt. At the command line, type:
> shell
2. At the prompt, type the following command
`root@ns#` srm <keyfilename>

Configuring TLS for NetScaler

Configuring Close Notify

A close-notify is a secure message that indicates the end of SSL data transmission. In compliance with RFC 5246: The client and the server must share knowledge that the connection is ending in order to avoid a truncation attack. Either party may initiate the exchange of closing messages. Either party may initiate a close by sending a close_notify alert. Any data received after a closure alert is ignored, unless some other fatal alert has been transmitted. Each party is required to send a close_notify alert before closing the write side of the connection.

In order to ensure that audit events are captured for TLS termination events, log on to the CLI as a *superuser* or *sysadmin* and execute the following commands:

```
set ssl parameter -sendCloseNotify y

save ns config
```

Managing TLS Certificates and Keys

Configuring TLS Cipher Suites

The following is a list of TLS cipher suites that are supported for NDPP deployments:

1. TLS_RSA_WITH_AES_128_CBC_SHA
2. TLS_RSA_WITH_AES_256_CBC_SHA

To ensure that only the approved cipher suites are configured on the appliance, complete the following configuration steps from the CLI:

1. Unbind all ciphers from the virtual server
   `Unbind ssl vs v1 -cipherName FIPS`
2. Bind only `TLS1-AES-256-CBC-SHA` and then `TLS1-AES-128-CBC-SHA` with the command:
   `bind ssl vs v1 -cipherName <cipher>`

```
bind ssl vs v1 -cipherName TLS1-AES-256-CBC-SHA
```

Importing a Trusted Root CA Certificate

1. Using a secure file transfer utility, such as scp or WinSCP, transfer the server issuer (root) certificate to the `/nsconfig/ssl` directory of the NetScaler appliance.
   Note: You must authenticate as a super user through SCP or winSCP to complete this step.
2. Log on to the NetScaler appliance as a system administrator or super user and type the following command:

```
add ssl certkey <Certificate_Name> -cert <Cert_File_Name>
```

Note: Only install root CA certificates from certificate authorities that are known to be trustworthy. You must remove all other certificates.

Importing a PKCS#12 (.PFX) Certificate and Key File

1. Transfer the .pfx file to the `/nsconfig/ssl` directory, as mentioned in step 1 in the preceding section
2. Authenticate to the NetScaler appliance through the CLI as a Sysadmin or superuser and execute the following command:

```
convert ssl pkcs12 Cert-Client-1.pfx -export -certFile Cert-Client-1 -
keyFile Key-Client-1
```

3. Add the certificate to NetScaler as follows:

```
add ssl certkey Clent-Cert-1 -cert Cert-Client-1
```

4. Save the current configuration

```
save ns config
```

Installing Certificates and Key Pairs Using a Trusted CA

To obtain a certificate from a public or enterprise certificate authority (CA) you must first generate a private key and certificate signing request (CSR). This is done as follows:

1. Authenticate to the NetScaler CLI as a Sysadmin or superuser.
2. Create an RSA private key.

```
create fipsKey m1 -modulus 2048
```

3. Create the certificate signing request (CSR):

```
create certreq csr_1 –fipsKeyName m1 –countryName IN –stateName BA –
organizationName citrix
```

4. Submit the CSR to the CA
   For most commercial and enterprise CA's, this is usually done in an e-mail request. However, the method of submission may vary across enterprise CA environments. The CA returns a valid certificate by email, but this too may vary among enterprise CA's. After you receive the certificate from the CA, securely copy it to the `/nsconfig/ssl` directory.

   Log in as a *superuser* or *sysadmin* and run the following command:

   ```
   add ssl certKey ck_1 –cert cert1_1 –fipsKey m1
   ```

Configuring SSH for NetScaler

Configuring SSH to use NDPP Approved Algorithms

You need to modify the `sshd_config` file to add the following ciphers, MACs, and algorithms. Only the RSA algorithm is supported.

Note: Only the superuser role has privileges to perform this activity. If access policies do not permit superusers to log on remotely, this procedure must be completed using local console access.

To configure SSH for using NSPP approved algorithms:

1. Log in as a superuser
2. At the command line, type:
   ```
   shell
   ```
3. Edit the sshd_config file to add the NDPP approved algorithms mentioned below.
   ```
   vi nsconfig/sshd_config
   ```

4. Restart the SSHD daemon
   ```
   kill –HUP `cat /var/run/sshd.pid`
   ```

NDPP Approved Algorithms for SSH:

Encryption

1. AES128-CBC
2. AES256-CBC

Data Integrity

1. hmac-sha1
2. hmac-sha2-256
3. hmac-sha2-512.

Key Exchange

1. diffie-hellman-group14-sha1
2. ecdh-sha2-nistp256
3. ecdh-sha2-nistp384
4. ecdh-sha2-nistp521

Public Key Algorithms

1. SSH-RSA

Note: The algorithms are applied in the order of precedence in which they are specified in the file

---

After you have modified the `sshd_config` file in the `/etc` directory, and copied it to /nsconfig to maintain persistency, any updates that are pushed to the `/etc` directory during the upgrade might be lost.

To avoid losing these updates, create a `/var/nsconfig_backup` directory, and move the customized `sshd_config` file to this directory by running the following command:

```
mv /nsconfig/<filename> /var/nsconfig_backup
```

Note: The customized sshd_config file must be moved.

Example:

```
mv /nsconfig/sshd_config /var/nsconfig_backup
```

Configuring Citrix NetScaler to use SSH Public Key Authentication

If you administer a large number of NetScaler appliances, storing and looking up passwords for logging on to individual appliances can be cumbersome. To avoid being prompted for passwords, you can set up secure shell access with public key encryption on each appliance.

NetScaler features can also use SSH key based authentication for internal communication when the `nsinternal` user is disabled (by using the `set ns param –internaluserlogin disabled` command). In such cases, the key name must be set as "`ns_comm_key`".

To set up access using SSH keys, you must generate the public-private key pair on a client and copy the public key to the remote NetScaler appliance.

To generate the keys and connect to a remote NetScaler by using SSH keys:

Note: If you are changing the SSH keys or rotating them, you must use the SRM command to securely delete the old key files. To accomplish this, use the following steps:

1. Access the shell prompt. At the command line, type:
shell

2. At the prompt, type the following command
`root@ns#` srm <keyfilename>

---

1. On a client (Linux client or a NetScaler appliance) change directory to /root/.ssh.
   `cd /root/.ssh`
2. Generate the public-private key pair.
   `ssh-keygen –t <key_type> –f <optional_key_file_name>`
   Example: To create an RSA key with the default file name.
   `ssh-keygen –t rsa`
3. When prompted for a file name for the key pair:

   - To use the default file name, press ENTER.
   - If you enter a file name for the key pair, use that name instead of the default name in the rest of this procedure.
   - If you don't want to disable internal user login, use `ns_comm_key` as the file name for the public-private key pair.
4. Press ENTER two times when prompted for a passphrase
   Note:
   - If the client is a NetScaler appliance, move the private key file to a persistent location, such as a subdirectory of the `/flash` or `/var` directory.
5. Log on to the remote NetScaler appliance from the client by using a file transfer protocol, and do the following:
   a. Change directory to `/nsconfig/ssh`. At the prompt, type:
      cd /nsconfig/ssh
   b. Use the binary transfer mode to copy the public key to this directory.
      bin
      put id_rsa.pub
6. Open a connection to the remote NetScaler appliance, using an SSH client such as PuTTY, and do the following:
   a. Log on to the remote appliance, using the administrator credentials.
   b. Go the NetScaler shell
      `> shell`
   c. At the shell prompt, change the directory to `/nsconfig/ssh`
      `root@ns# cd /nsconfig/ssh`
   d. Append the public key to the `authorized_keys` file. At the shell prompt, type:
      `root@ns# cat id_rsa.pub >> authorized_keys`

      Note: If the `authorized_keys` file does not exist at the appliance, you need to first create the file and then append the contents.
   e. Change the permission of the `/flash`, `nsconfig`, and `ssh` directories to 755.
      `root@ns# chmod 755 /flash`
      `root@ns# chmod 755 /flash/nsconfig`
      `root@ns# chmod 755 /flash/nsconfig/ssh`
   f. Change the permission to authorized_keys file to 744
      `root@ns chmod 744 authorized_keys`
   g. Optionally, remove the public key
      `root@ns rm id_rsa.pub`

7. On the client, verify that you can connect to the remote NetScaler appliance by using SSH. If using the default file name for the public-private key pair, you should be able to log on without entering a password.

   ```
   ssh <user_name>@<NetScalerIPAddress>
   ```
   If using "ns_comm_key" (when nsinternal user is disabled) for the public-private key pair:
   ```
   ssh –i /nsconfig/ssh/ns_comm_key <user_name>@<NetScalerIPAddress>
   ```
   If using any other name for the public-private key pair:
   ```
   ssh –i <path_to_client_private_key><user_name>@<NetScalerIPAddress>
   ```

Configuring a Warning Message For SSH

Note: Only a superuser can carry out this task. If access policies do not permit superusers to log on remotely, this procedure must be completed using local console access.

To Configure a notice and a warning message, do the following:

1. Access the shell prompt

   ```
   > Shell

   Copyright (c) 1992-2008 The FreeBSD Project.

   Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,
   1994 The Regents of the University of California. All rights reserved.
   ```

2. Change the directory to /nsconfig/ssh

   ```
   root@ns# cd /nsconfig/ssh
   ```

3. Create a banner file

   ```
   root@ns#  vi sshd_banner
   ```

4. Enter the message that you want to be displayed, and save the file. For example:

   ```
   ********** Warning – Warning – Warning**********

   This system is restricted to authorized individuals and is the
   property of <Company>. Unauthorized access is prohibited and all
   access attempts are monitored.

   ********** Warning – Warning – Warning**********
   ```

5. Edit the `/nsconfig/sshd_config` file. If this configuration file does not exist, copy it from `/etc/sshd_config` to `/nsconfig/sshd_config`.

   ```
   root@ns#  cp /etc/sshd_config /nsconfig/sshd_config

   root@ns# vi /nsconfig/sshd_config
   ```

6. Add the following on a newline and write quit from vi:

```
Banner /nsconfig/ssh/sshd_banner
```

7. Restart the SSHD process by entering the following command:

```
root@ns#  kill -HUP `cat /var/run/sshd.pid`
```

Test the banner by issuing the SSH command to the system. The IP address in the following command is just an example. Use the IP address of the NetScaler Appliance.

```
root@ns# ssh 10.54.80.32
********** Warning - Warning - Warning**************************

This system is restricted to authorized individuals and is the property of
"Company". Unauthorized access is prohibited and all access attempts are
monitored.

********** Warning - Warning - Warning**************************
```

Updating SSH Host Keys

If your SSH host keys are compromised, you can update them to get a new set of keys. To do so, delete the compromised host key from the system and restart the appliance.

Note: If you are changing the SSH Host keys or rotating them, you must use SRM command to securely delete the old key files. To accomplish this, use the following steps:

1. Access the shell prompt. At the command line, type:
> shell

2. At the prompt, type the following command
`root@ns#` srm <keyfilename>

Disabling Features

You must disable the NetScaler features that are outside the scope of the common criteria deployment.

To disable features

At the NetScaler command prompt, type

```
> disable ns feature <feature> ...
```

To verify the status of all features

At the NetScaler command prompt, type

```
> sh ns feature
```

Disable L3 mode

NetScaler packet routing options are highly configurable and robust. If you accept the factory defaults, L3 mode is enabled. When operating the TOE in the Common Criteria evaluated configuration, the administrator must make sure that L3 mode is disabled.

To disable the L3 mode by using the NetScaler command line

Type the following command at the prompt:

```
> disable ns mode L3
```

Note: Only a super user or sysadmin can carry out this task.

Disable SNMP

When operating the TOE in the Common Criteria evaluated configuration, the administrator must make sure that SNMP is disabled.

Note: This action requires a super user command policy. If access policies do not permit superusers to log on remotely, this procedure must be completed using local console access.

To disable SNMP

At the NetScaler command prompt, type

```
> set ns ip <ip_address> –snmp disabled
```

To verify that SNMP is disabled

At the NetScaler command prompt, type

```
> sh ns ip <ip_address>
```

Output:

```
IP: 10.102.29.170
Netmask: 255.255.255.0
Type: NetScaler IP
state: Enabled
.
.
```

.

```
ssh: Enabled gui: Disabled

snmp: Disabled

Restrict access: Disabled
```

Disable FTP and Telnet

When the NetScaler appliance is shipped, Telnet is disabled by default. During configuration, you do not need to take any action to disable Telnet. To disable FTP, type:

```
set ns ip <NSIP>  –ftp disabled
```

Disabling NTP

When operating the TOE in the Common Criteria evaluated configuration, the administrator must make sure that NTP synchronization is disabled.

To disable NTP sync

At the NetScaler command prompt, type

```
disable ntp sync
```

Disable High Availability Mode

When operating the TOE in the Common Criteria evaluated configuration, the administrator must make sure that high availability mode is disabled.

To disable high availability mode

At the NetScaler command prompt, type

```
set ha node –hastatus disabled
```

Disable Port 4001

You have to disable TCP port 4001 to secure the deployment. Port 4001 is used by the ZebOS subsystem to transfer its config between the HA nodes.

Use access control lists (ACLs) to block port 4001. Blocking this port blocks all the SYN packets to this port.

To disable port 4001 on a NetScaler

At the NetScaler command prompt, type

```
add ns acl <ACL_Name> DENY –destIP <NSIP> –destPort 4001 –protocol
TCP –priority 10 –kernelstate SFAPPLIED61 apply ns acls
```

Example

```
add ns acl block4001 DENY –destIP 10.102.113.195 –destPort 4001
–protocol TCP –priority 10 –kernelstate SFAPPLIED61 apply ns acls
```

Disable IPv6

When operating the TOE in the Common Criteria evaluated configuration, the administrator must make sure that IPv6 protocol translation is disabled.

To disable IPv6

At the NetScaler command prompt, type

```
disable ns feature IPv6protocoltranslation
```

Note: Only a super user or sysadmin can carry out this task.

Disable Ports Not Used for Management Access

When operating the TOE in the Common Criteria evaluated configuration, the administrator can disable ports that are not used for management access. This ensures that the state of the port is filtered and you do not get responses on these ports.

To disable ports not used for management access

At the NetScaler command prompt, type

```
set ns ip <NSIP> –restrictaccess ENABLED
```

Disabling the Management GUI

To conform to the Common Criteria Evaluated deployment, you must disable the GUI. Disabling the GUI also disable other access methods, such as the NITRO API. No separate commands need to be run to disable those methods.

To disable the GUI

At the NetScaler command prompt, type

```
set ns ip <NSIP> –GUI DISABLED
```

Disabling SSLv3

To conform to the Common Criteria Evaluated deployment, you must disable SSLv3. You cannot disable it at the global level. It must be disabled for each individual virtual server (vserver).

To disable SSLv3

At the command prompt, type

```
set ssl vserver v1 –ssl3 disABLED
```

Where, v1 is the name of the virtual server.

Configuring a Warning Message for the Serial Console

To configure a warning message for the serial console, you must have superuser privileges.

Note: If access policies do not permit superusers to log on remotely, this procedure must be completed using local console access.

To configure a warning message for the serial console

1. Access the NetScaler CLI from console, using the superuser account.
   a. If you are accessing the DUT remotely, you can use telnet to the Advanced Console Server (ACS) to connect to the serial console as follows:
      telnet <ACS IP> <port number>
   b. If you have direct physical access to the DUT, you can use a laptop that has vt100 serial port and use the supplied red cable, using the RJ 45 to DB 9 dongle to connect to the DUT. You can use a terminal emulator, such as putty, and use COM4 at a baud rate 9600 kbps to connect to the serial console.
2. Access the shell prompt. At the command line, type:
   `> shell`
3. Copy the file `/etc/issue` to `/nsconfig`. (If the file does not exist, you have to create it.)
   `# cp /etc/issue /nsconfig`
4. Edit the /nsconfig/issue file to add the desired warning message.
   "Warning: You are connecting to a secure resource"
5. Restart your NetScaler appliance. At the command prompt, type:
   ```
   # exit
   > reboot
   Are you sure you want to restart NetScaler (Y/N)?[N]y
   Done
   >
   ```
6. Confirm that the banner "Warning: You are connecting to a secure resource" is displayed when you log on from the console.

Configuring System Settings

Timestamps

The TOE administrator must periodically perform a manual check of the NetScaler system clock to ensure the reliability of the TOE's timestamps. If the system clock has drifted from the actual time, the administrator must reset the system clock to the actual time.

You can set or change the time zone of your NetScaler appliance. You can also set the current time and verify the date and time settings.

Note that only the superuser role has privileges to modify system settings. If access policies do not permit superusers to log on remotely, this procedure must be completed using local console access.

Note: Ensuring that the NetScaler is configured with the correct time is important for maintaining accurate audit records, and for accurate application of any firewall rules that relate to the time of access. Administrators must, therefore, check periodically that the NetScaler time is correct.

To set the current date and time on your NetScaler appliance

At the NetScaler command prompt, type:

```
> shell
```

At the shell prompt, type: date <ccyymmddHHMM.ss>, where

- cc is the first two digits of the year (the century)
- yy is the second two digits of the year
- mm is the month of the year
- dd is the day of the month
- HH is the hour of the day
- MM is the minute of the hour
- ss is the second of the minute

Example

To set the date and time to August 23, 2010, 15 hours, 30 minutes, and 40 seconds, type:

```
date 201008231515.40
```

To set only the time

At the NetScaler command prompt, type:

```
> shell
```

At the shell prompt, type:

```
root@ns# date <HHMM.ss>
```

To verify the date and time setting

At the NetScaler command prompt, type:

```
> shell
root@ns# date
```

General NetScaler Management Chapter 6

The NetScaler Sysadmin

The *NetScaler System Administrator* command policy gives the administrative user full administrative access to all NetScaler features, through the Command Line Interface only. This includes access to the necessary commands to configure and manage the following functionality:

General System Management

The general system management activities consist of those operations that are frequently used on a day-to-day basis by system administrators to configure the supported features of the NetScaler appliance and user access to the appliance. The NetScaler System Administrator command policy allows the execution of all documented CLI commands listed at http://support.citrix.com/proddocs/topic/ns-reference-map-10-5/netscaler-crg-gen-wrapper-con.html, except as follows:

1. In addition to being constrained from the CLI activities defined in tasks 1, 2, and 3 as described in Superuser Capabilities and Entitlements, the built-in System Administrator account does not allow an administrator to elevate his or her own privileges.
2. The NetScaler System Administrator command policy does not grant the ability to use the CLI to enumerate, create, modify, or remove system user, system group, or system policy objects.

The System Administrator cannot perform any of the activities described in items 4 through 13 in Superuser Capabilities and Entitlements. Those activities require direct access to the FreeBSD shell.

Recommendations

The vast majority of routine system management tasks on the NetScaler appliance can be executed through the Command Line Interface (CLI). For this reason Citrix recommends that the *NetScaler System Administrator* command policy be assigned to engineers who are assigned to the routine daily management of NetScaler appliances. In keeping with the Principle of Least Privilege, the use of the *NetScaler Super User* command policy should be limited to initial appliance setup and the activities under advanced system management.

Configuring External User Authentication

External user authentication is the process of authenticating the users of the Citrix NetScaler appliance by using an external authentication server. The appliance supports LDAP authentication servers. To configure external user authentication, you must create authentication policies. You can configure one or many authentication policies, depending on your authentication needs. An authentication policy consists of an expression and an action.

After creating an authentication policy, you bind it to the system global entity and assign a priority to it. You can create simple server configurations by binding a single authentication policy to the system global entity. Or, you can configure a cascade of authentication servers by binding multiple policies to the system global entity. If no authentication policies are bound to the system, users are authenticated by the onboard system.

External Authentication Servers

The TOE provides the option of using external authentication servers for determining whether or not to grant administrative access to the TOE. The administrator must ensure that only the LDAP protocol over TLS (LDAPS) is used for external authentication when operating the TOE in the CC-evaluated configuration.

Configuring LDAP Authentication

You can configure the NetScaler appliance to authenticate user access with one or more LDAP servers. LDAP authorization requires identical group names in Active Directory, on the LDAP server, and on the appliance. The characters and case must also be the same.

By default, LDAP authentication is secured by using SSL/TLS protocol. Use port number 636 for secure LDAP connections.

External LDAP Authentication

To configure external LDAP authentication, complete the following steps:

1. Log on to the CLI as a superuser
2. Enter the shell prompt by typing:
   `shell`
3. Create an `ldap.conf` file under /nsconfig folder, using touch ldap.conf.
4. Create symbolic link by using the following command.
   ln –s /nsconfig/ldap.conf /etc/ldap.conf
5. Edit the ldap.conf file using a text editor such as vi and enter the Cipher in the format of :
   TLS_CIPHER_SUITE AES128-SHA

or
TLS_CIPHER_SUITE AES256-SHA

Save the file.

6. From the shell run the command ps -aux |grep aaa to find the aaad process, and kill it using kill -9 <PID> to restart the aaad process.

2. Import the issued root CA certificate for the remote LDAP server as follows:
   a. Using a secure file transfer utility such as SCP or WinSCP, copy the root CA certificate to the `/nsconfig/ssl` directory on the NetScaler appliance.

Note: You must authenticate as a superuser to access the scp or winSCP utility.

---

b. Authenticate to the NetScaler appliance through the CLI as a superuser. Upon authentication, escape to the Free BSD shell as described Chapter 3, "Accessing the Host Operating System Shell from the CLI."

Run the following shell commands:

```
mkdir /nsconfig/truststore
cd /nsconfig/truststore/
cp /nsconfig/ssl/nsi-test-ca.cer .
openssl x509 -hash -fingerprint -noout -in nsi-test-ca.cer
e72e679c MD5 \
Fingerprint=F5:58:33:0B:94:B7:C4:0E:54:A4:8C:BD:DC:39:FA:F3
ln -s nsi-test-ca.cer e72e679c.0_

exit
```

3. Make changes to the running configuration to set up LDAP:
   a. Log on to the NetScaler appliance as either a system administrator or a superuser and run the following command from the command line interface. To add an action profile for the LDAP server to be used:

```
add authentication ldapAction ldap22s -serverIP 10.102.229.222 -
serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -ldapBindDn
"cn=Administrator,cn=Users,dc=aaatm-test,dc=com" -
ldapBindDnPassword superSecretPassword -ldapLoginName
sAMAccountName -secType SSL  -validateServerCert YES -
ldapHostname nsi-dc1-2008.nsi-test.com
```

Note: Replace the parameter values in the above example with the actual values for your implementation.

---

b. Add an authentication LDAP policy. At the command line interface, type the following command:

```
add authentication ldapPolicy <name> <rule> [<reqAction>]
```

Example:

```
add authentication ldapPolicy ldap22spol ns_true ldap22s
```

Note: Replace parameter values in the above example with the actual values for your implementation.

c. Bind the corresponding policy to your appliance. At the command prompt, type the following command:

```
bind system global ldap22spol
Done
save ns config
```

4. Verify that the LDAP server is accessible

d. Log on to the NetScaler appliance as a superuser from command line interface.
e. Escape to the FreeBSD shell as described in Chapter 3, Accessing the Host Operating System Shell Through the CLI.
f. Run the `ldapsearch` utility as follows, using the parameters supplied to the `authentication ldapaction` in step 2.

```
LDAPTLS_REQCERT=never ldapsearch -H ldaps://10.102.229.222:636 -b
"cn=users,dc=aaatm-test,dc=com" -D Administrator@aaatm-test.com -
w freebsd@123 cn=Complex1
```

where

-b: base DN (distinguished name)
-D: Administrator Bind DN
-H: LDAP URL and port of Server
-w: Administrator Password
-x: Simple authentication rather than SASL
-s: search base; “sub” specifies all branches under the base DN

Note: The parameters values shown above are examples. Substitute your actual values for the ones shown above

Configuring NetScaler to Validate LDAP Server Certificate

If you are upgrading your NetScaler Appliance from 10.1 to an NDPP certified build, and the certificate is computed by using MD5, certificate validation fails. This happens only when NetScaler is configured with LDAP server certification validation and is upgraded from 10.1 to an NDPP build. The certification validation does not fail if it is a new installation or if the server certification is enabled after upgrading to an NDPP build.

If you are upgrading to an NDPP build, compute the hash value on the CA certificate and create a soft link.

```
In this example, aaatm-dc-ca.cer is the CA certificate that issued the LDAP server certificate.
root@ns220# cd /nsconfig/truststore
root@ns220# ls aaatm-dc-ca.cer
aaatm-dc-ca.cer
root@ns220# openssl x509 -hash -fingerprint -noout -in aaatm-dc-ca.cer
2f4c0bc7
SHA1 Fingerprint=94:57:A4:CE:8B:B8:B6:94:35:FF:1E:AE:B6:77:B5:80:07:B6:39:51
root@ns220# ln -s aaatm-dc-ca.cer 2f4c0bc7.0
root@ns220# ls -tlr 2f4c0bc7.0
lrwxr-xr-x  1 root  wheel  15 Feb 21 01:55 2f4c0bc7.0 -> aaatm-dc-ca.cer
```

Setting Up Basic Load Balancing

The load balancing feature distributes user requests for web pages and other protected applications across multiple servers that all host (or mirror) the same content. You use load balancing primarily to manage user requests to heavily used applications, preventing poor performance and outages and ensuring that users can access your protected applications.

In a basic load balancing setup, clients send their requests to the IP address of a virtual server configured on the NetScaler appliance. The virtual server distributes them to the load-balanced application servers according to a preset pattern, called the load balancing algorithm or load balancing method.

The entities that you configure in a typical NetScaler load balancing setup are:

- **Load balancing virtual server**: The IP address, port, and protocol combination to which a client sends connection requests for a particular load-balanced web site or application. If the application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible from only the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address.
- **Service:** The IP address, port, and protocol combination used to route requests to a specific load-balanced application server. A service can be a logical representation of the application server itself, or of an application running on a server that hosts multiple applications. Each service is bound to a specific virtual server.
- **Server object**: An entity that identifies a physical server and provides the server's IP address. If you want to use the server's IP address as the name of the server object, you can enter the server's IP address when you create a service, and the server object is then created automatically. Alternatively, you can create the server object first and assign it an FQDN or other name, and then specify that name instead of the IP address when you create the service.
- **Monitor:** An entity on the NetScaler appliance that tracks a service and ensures that it is operating correctly. The monitor periodically probes (or performs a health check on) each service to which you assign it. If the service does not respond within the time specified by the timeout, and a specified number of health checks fail, that service is marked DOWN. The NetScaler appliance then skips that service when performing load balancing, until the issues that caused the service to quit responding are fixed.

Before configuring your initial load balancing setup, enable the load balancing feature. Then begin by creating at least one service for each server in the load balancing group. With the services configured, you are ready to create a load balancing virtual server and bind each service to the virtual server. That completes the initial setup. Before proceeding with further configuration, verify your configuration to make sure that each element was configured properly and is operating as expected.

Enabling Load Balancing

You can configure load balancing entities such as services and virtual servers when the load balancing feature is disabled, but they will not function until you enable the feature.

To enable load balancing by using the NetScaler command line

At the NetScaler command prompt, type the following command to enable load balancing and verify the configuration:

```
enable ns feature LoadBalancing
show ns feature
```

Example

```
> enable ns feature LoadBalancing Done
> show ns feature
   Feature  Acronym    Status
   -------  -------    ------

   1) Web Logging WL    OFF
   2) Surge Protection SP    OFF
   3) Load Balancing   LB    ON
   .
   .
   .
   24)      NetScaler Push   push  OFF
   Done
```

Configuring Services

After you enable the load balancing feature, you must create at least one service for each application server that is to be included in your load balancing setup. The services that you configure provide the connections between the NetScaler appliance and the load balanced servers. Each service has a name and specifies an IP address, a port, and the type of data that is served. If you prefer to identify servers by name rather than IP address, you can create server objects and then specify a server's name instead of its IP address when you create a service.

Creating a Server Object

The NetScaler appliance can create server objects automatically. If, when you create a service, you enter the IP address of a server for which a server object has not already been created, the appliance creates the server object and uses the IP address as its name. If you want to assign a name to a server, you can do so by creating a server object manually. You can then enter the object's name instead of the server's IP address when you create a service.

To create a server object by using the NetScaler command line

At the NetScaler command prompt, type:

```
add server <name> <IP>
```

Example

```
add server Server-1 10.102.29.18
```

Creating a Service

Before you create a service, you need to understand the different service types and how each is used. A service type is a type of traffic, such as HTTP, SSL, FTP, or TCP.

Services are designated as DISABLED until the NetScaler appliance connects to the associated load-balanced server and verifies that it is operational. At that point, the service is designated as ENABLED. Thereafter, the NetScaler appliance periodically monitors the status of the servers, and puts those that fail to respond to monitoring probes (called health checks) back into the DISABLED state until they respond.

To create a service by using the NetScaler command line

At the NetScaler command prompt, type:

```
add service <name> <serverName> <serviceType> <port>
```

Example

```
add service Service-HTTP-1 10.102.29.5 HTTP 80
```

Creating a Virtual Server

After you create your services, you must create a virtual server to accept traffic for the load balanced Web sites, applications, or servers. Once load balancing is configured, users connect to the load-balanced Web site, application, or server through the virtual server's IP address or FQDN.

Note: The virtual server is designated as DOWN until you bind the services that you created to it, and until the NetScaler appliance connects to those services and verifies that they are operational. Only then is the virtual server designated as UP.

To create a virtual server by using the NetScaler command line

At the NetScaler command prompt, type:

```
add lb vserver <name> <serviceType> <ip> <port>
```

Example

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.30 80
```

Binding Services to the Virtual Server

After you have created services and a virtual server, you must bind the services to the virtual server.

The state of the services bound to a virtual server determines the state of the virtual server. If all of the bound services are DOWN, the virtual server is marked DOWN, and if any of the bound services is UP or OUT OF SERVICE, the state of the virtual server is UP.

To bind a service to a load balancing virtual server by using the NetScaler command line

At the NetScaler command prompt, type:

```
bind lb vserver <name> <serviceName>
```

Example

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
```

Verifying the Configuration

After finishing your basic configuration, you should view the properties of each service and load balancing virtual server in your load balancing setup to verify that each is configured correctly. After the configuration is up and running, you should view the statistics for each service and load balancing virtual server to check for possible problems.

To view the properties of server objects by using the NetScaler command line

At the NetScaler command prompt, type:

```
show server <serverName>
```

Example

```
show server server-1
```

To view the properties of a load balancing virtual server by using the NetScaler command line

At the NetScaler command prompt, type:

```
show lb vserver <name>
```

Example

```
show lb vserver Vserver-LB-1
```

To view the properties of services by using the NetScaler command line

At the NetScaler command prompt, type:

```
show service <name>
```

Example

```
show service Service-HTTP-1
```

To view the bindings of a service by using the NetScaler command line

At the NetScaler command prompt, type:

```
show service bindings <name>
```

Example

```
show service bindings Service-HTTP-1
```

To view the statistics of a virtual server by using the NetScaler command line

At the NetScaler command prompt, type:

```
stat lb vserver <name>
```

Example

stat lb vserver Vserver-LB-1

To view the statistics of a service by using the NetScaler command line

At the NetScaler command prompt, type:

```
stat service <name>
```

Example

```
stat service Service-HTTP-1
```

NetScaler Administration Command Policies

You can provide access to internal resources by configuring authentication policies and authorization policies.

The NetScaler superuser command policy permits the administrative user full administrative access to all NetScaler features via both the Command Line Interface and the BSD shell. This includes access to the necessary commands to configure and manage the following functionality:

- Superuser Capabilities and Entitlements
- SysAdmin Capabilities and Entitlements

Configuring Authentication Policies

When users log on to the NetScaler Gateway, they are authenticated by a policy. The authentication policies can be applied to both local and administrative users. The policy defines the authentication type. A single authentication policy can be used for simple authentication needs. Multiple policies can also be configured to create a detailed authentication procedure. An authentication policy consists of an expression and an action.

Once created, an authentication policy can be bound either at the global level or to virtual servers. When at least one authentication policy is bound to a virtual server, any authentication polices bound to the global level are not used when users log on to the virtual server.

By default, authentication polices bound to virtual servers are applied first, and then the globally bound policies are applied. If you have an authentication policy bound globally and want it to take precedence over an authentication policy bound to a virtual server, you can change the priority number of the policy. Priority numbers start at zero. A lower priority number gives the authentication policy higher precedence.

For example, if the global policy has a priority number of one and the virtual server has a priority of two, the global authentication policy is applied first. If a priority number is not assigned, the virtual server authentication policy is applied first and then the global policy.

To create an authentication policy

At the NetScaler command prompt, type

```
add authentication ldapAction <name> [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort
<port>] [-ldapBase <string>] [- ldapBindDn <string>] {-ldapBindDnPassword } [-
ldapLoginName<string>] [-groupAttrName <string>] [-subAttributeName <string>]
```

Example:

```
add authentication ldapAction ldap_act_180 -serverIP 172.173.3.180 -ldapBase
"dc=ctxtd, dc=com" -ldapBindDn administrator@ctxtd.com - ldapBindDnPassword
fd2604527edf7371a2 -encrypted -ldapLoginName samAccountName -groupAttrName memberOf
-subAttributeName CN
```

```
add authentication ldapPolicy <name> <rule> [<reqAction>]
```

Example:

```
add authentication ldapPolicy ldap_pol_180 ns_true ldap_act_180
```

To create a VPN server

At the NetScaler command prompt, type:

```
add vpn vserver <name> <serviceType>
```

Example

```
add vpn vserver vs  ssl 1.1.1.1 443
```

To bind an authentication policy to a VPN vserver

At the NetScaler command prompt, type:

```
bind vpn vserver <name> [-policy <string> [-priority <positive_integer>]]
```

Example:

```
bind vpn vserver vpn_vs_name -policy ldap_pol_180 -priority 2
```

To bind an authentication policy to an AAA group

At the NetScaler command prompt, type:

```
bind aaa group <groupName> [-policy <string> [-priority <positive_integer>]]
```

Example:

```
bind aaa group group_name -policy ldap_pol_180 -priority 3
```

To bind an authentication policy globally

At the NetScaler command prompt, type:

```
bind vpn global [-policyName <string> [-priority <positive_integer>]]
```

Example:

```
bind vpn global -policyName ldap_pol_180 -priority 1
```

Securing the Deployment Chapter 7

To maintain security through the deployment lifecycle, Citrix recommends addressing the following:

- Non-CC-Certified Product Updates
- Physical Security
- Appliance Security
- Network Security
- Administration and Management Security
- NetScaler FIPS Security
- NetScaler Gateway Security

Unless stated otherwise, only the Sysadmin or superuser role can perform the configuration tasks described in this chapter.

Non-CC-Certified Product Updates

From time to time, Citrix issues product updates, which sometimes correct flaws in the underlying software. Administrators should check with Citrix on a regular basis for these updates. Administrators can also opt to subscribe to proactive email alerts about product security vulnerabilities and their associated fixes. These alerts are sent on a regular basis whenever new fixes are available. Administrators can contact and work with Citrix Support directly if they require additional support in obtaining and deploying any fix. More information about the email alerts system can be found at http://www.citrix.com.

In the event that an update corrects a critical flaw, but the update has not yet been Common Criteria (CC) certified, the administrator should analyze the corrected flaw and the TOE's vulnerability to it when determining whether or not to install the non-certified update.

Vulnerabilities can be reported to Citrix in a number of ways:

- Through the secure@citrix.com e-mail address
- Through the customer's Support contacts
- Through other Citrix contacts, such as resellers or systems engineers.

  The recommended route for customers to report suspected security vulnerabilities is through the secure@citrix.com e-mail address. This address is displayed prominently on both the main Citrix Web site and the Citrix Support Web site, and the associated mailbox is checked regularly by security engineering staff. Any new entries are entered into the vulnerability tracking tool, as are additional communications for existing issues.

  For issues that have been reported to a contact within Citrix, and for suspected security flaws that are discovered internally by Citrix staff, security engineering staff can be notified through the

secure@citrix.com address, an internal email distribution list, or direct contact with security engineering staff.

Ongoing communication can include requests for updates on a reported issue by the reporting party, requests for more information by security engineering staff, or feedback on a supplied mitigation.

Physical Security

NetScaler deployment requires a secure location. NetScaler appliances are intended to be physically secured from theft or tampering. Also see Environment Assumptions.

Appliance Security

- Protect the serial console port from unauthorized Access. This port can be used to configure and reset the appliance.
- Perform remote software updates. Apply updates as available to remediate any known issues. When updating the appliance, use a secure protocol like SFTP or HTTPS. Citrix does not provide patches to firmware. Only new images are provided as part of firmware updates.

  Note: An update requires a system restart.

- Do not modify system software. NetScaler is provided as a managed appliance and, apart from performing remote software updates, additional hardening or modification of system software is not necessary or desirable. Contact Citrix Support with any questions.
- Secure the front panel. Ensure that those with physical access to the machine do not modify the front panel settings once the appliance has been configured.

Network Security

- Non-routable management IP. Make sure that the management IP address is not routable on the public internet and is behind a firewall.
- Placement in the network. Review your organizational policy and compliance requirements to determine whether the NetScaler appliance needs to be deployed behind a stateful firewall.

Administration and Management Security

You must maintain and monitor secure accounts and configuration as described in this section.

User Access Control

You can control the system user's access by configuring ACLs as follows:

- Use a default deny action for NSIP.

  Example

  ```
  > add acl default_deny deny –destip 10.217.206.60 –priority 100

  > apply acls

  Done
  ```

- Identify and allow only specific IP address(es) to access the NSIP address.

  Example

  ```
  > add acl local_access alLOW –srcip 10.217.205.61 –destiP
  10.217.206.60 –destport 22 –protocol tcp –priority 5

  Done

  > apply acls

  Done
  ```

By default, everything is allowed access. So you need to specify a default deny action to deny everything, and then allow access explicitly. The default deny ACL should have low priority (a high priority number).

Note that in the NetScaler operating system, a lower priority number specifies a higher priority. The higher the number, the lower the priority. For example, if you have three ACLs with priorities of 10, 100, and 1000, the ACL assigned a priority of 10 is evaluated first, then the ACL assigned a priority of 100, and finally the ACL assigned an order of 1000.

Note: If you modify ACLs by adding or removing any ACL, you must execute "apply ACLs" command to activate the change.

Configure Session Inactivity Timeout

Configure the session inactivity timeout to ensure that inactive sessions do not remain active for a long duration of time. The session inactivity timeout applies to both local and remote interactive sessions.

To configure session inactivity timeout

1. At the NetScaler command prompt, type the following command to enable restricted timeout:

   - **set system parameter -restrictedtimeout enabled**

2. Set a system-user specific timeout. The timeout parameter sets the CLI session inactivity timeout, in seconds. Timeout can have values in the range 300-86400 seconds. For example, the following command sets the timeout to 400 seconds for the user **testusr**. The user will be logged out after 400 seconds.

- **set system user testusr -timeout 400**

Configuring Audit Server Logging

The audit server logging feature enables you to log the Citrix NetScaler states and status information collected by various modules in the kernel and in the user-level daemons. The audit server collects and stores the event history in chronological order, so that you can review to troubleshoot problems or errors and fix them.

When you configure audit server logging, you set up a log file to capture the NetScaler status information in the form of messages. These messages typically contain the following information:

- The source module that generates the message
- A time stamp
- The message type
- The predefined log levels (Critical, Error, Notice, Warning, Informational, Debug, Alert, and Emergency)
- The message information

To enable audit server logging, you must configure the NetScaler auditing parameters, set up and install the executable files on a computer from which you want to run the audit tool, and configure the parameters in the configuration file by defining the filters and filter parameters. The filters determine the type of information in the log files and the location at which to store the files.

Audit Log Storage

Since the TOE audit logs might contain sensitive data critical to the security of the TOE, the TOE administrator must ensure that only authorized administrators have access to the audit logs on the TOE, and to any backups of the audit logs that might exist outside of the TOE. If a backup of the audit logs is created (for example, to send to an external syslog server), the administrator must ensure that the audit logs are protected from disclosure to non-TOE administrators during transmission and storage.

Note that only users with superuser privileges can back up audit logs.

Audit Log Review

All audit events relating to evaluated security activities performed by the administrator at the CLI are recorded in the ns.log file, and stored locally on the NetScaler appliance. This log file is archived when it

reaches a predefined size, and the archives are named according to the date and time at which the archive was created.

Logging

The NetScaler log files contain log messages of all the states and status information collected by different modules in the kernel and in the user-level daemons, so that the administrator can see the event history in chronological order. These logs are periodically rotated and are saved in /var/log folder. To securely transfer the log files to a remote audit server, the NetScaler appliance runs a cron job using scp.

Following is a list of important log files and their contents:

- /var/log/cron: cron daemon messages
  Example:
  Sep 22 20:31:00 <cron.info> ns /usr/sbin/cron[51586]: (root) CMD (nsfsyncd -p)
  Sep 22 20:32:00 <cron.info> ns /usr/sbin/cron[51639]: (root) CMD (nsfsyncd -p)
  Sep 22 20:33:00 <cron.info> ns /usr/sbin/cron[51692]: (root) CMD (nsfsyncd -p)

- /var/log/auth.log: sshd related messages
  Example:
  Sep 22 07:16:50 <auth.info> ns sshd[9267]: Connection closed by 10.252.120.195
  Sep 22 07:16:50 <auth.info> ns sshd[9267]: Transferred: sent 6184, received 6736 bytes
  Sep 22 07:16:50 <auth.info> ns sshd[9267]: Closing connection to 10.252.120.195 port 56850
  Sep 22 07:17:02 <auth.info> ns sshd[9326]: FIPS mode initialized
  Sep 22 07:17:02 <auth.info> ns sshd[9326]: Connection from 10.252.120.195 port 56861

- /var/log/messages: system related messages
  Example:
  Sep 22 00:12:23 <user.notice> ns installns: [686]: Installation path for kernel is /flash
  Sep 22 00:12:23 <user.notice> ns installns: [686]: Size of kernel ns-10.5-53.20.gz is 132959 kilobytes
  Sep 22 00:12:23 <user.notice> ns installns: [686]: Available space on /flash/ filesystem is 3330098 kilobytes
  Sep 22 00:12:23 <user.notice> ns installns: [686]: Available space on /var is 299254110 kilobytes

- /var/log/notice.log: system events and bash logs
  Example:
  Sep 23 06:00:40 <local7.notice> ns bash[1326]: root on (null) shell_command="/bin/sleep $NSPROFLOG_MGMTINTERVAL"
  Sep 23 06:00:46 <local7.notice> ns bash[1326]: root on (null) shell_command="[$IDLE -lt $NSPROFLOG_THRESHOLD]"
  Sep 23 06:00:46 <local7.notice> ns bash[1326]: root on (null) return_code="1"

- /var/log/bash.log: bash commands logging
  Example:

Sep 23 06:02:13 <local7.notice> ns bash[1284]: root on (null) shell_command="if ! kill -0 $PROF_PIDS >/dev/null 2>&1; then kill -9 $PROF_PIDS >/dev/null 2>&1; return; fi; sleep 60"
Sep 23 06:02:13 <local7.notice> ns bash[1284]: root on (null) shell_command="if ! kill -0 $PROF_PIDS >/dev/null 2>&1; then kill -9 $PROF_PIDS >/dev/null 2>&1; return; fi"
Sep 23 06:02:13 <local7.notice> ns bash[1284]: root on (null) shell_command="! kill -0 $PROF_PIDS >/dev/null 2>&1"

- /var/log/sh.log: sh_commands logging
  Example:
  Sep 22 07:10:00 <local6.notice> ns sh[8939]: sh_command="NSLOG_PID=${^ANSPID_DIR}/nslog.pid "
  Sep 22 07:10:00 <local6.notice> ns sh[8939]: sh_command="NSLOG_TIME=2*24*60*60 "
  Sep 22 07:10:00 <local6.notice> ns sh[8939]: sh_command="NSLOG_NEXTFILE=${^ANSLOG_DIR}/nslog.nextfile "
  Sep 22 07:10:00 <local6.notice> ns sh[8939]: sh_command="NXTZIPNUM_FILE=${^ANSLOG_DIR}/nslog.nextzip "

- /var/log/ns.log : all UI commands
  Example:
  Sep 22 15:00:00 ns newsyslog[33977]: logfile turned over due to size>100K
  Sep 22 16:58:13 <local0.info> ns nscli: read_char(): CLI session timed out at Tue Sep 22 16:58:13 2015
  Sep 23 02:07:19 <local0.info> 10.217.206.60 09/23/2015:02:07:19 GMT ns 0-PPE-4 : CLI CMD_EXECUTED 270 0 : User nsroot - Remote_ip 127.0.0.1 - Command "logout" - Status "Success"
  Sep 23 02:07:29 <local0.info> 10.217.206.60 09/23/2015:02:07:29 GMT ns 0-PPE-4 : UI CMD_EXECUTED 271 0 : User nsroot - Remote_ip 127.0.0.1 - Command "login nsroot "********"" - Status "Success"

- /var/log/nsvpn.log – AAA auth and VPN related actions logged.

The following configuration files need to be modified to configure the ssh logging behavior. You can also change the log level if needed.

- /etc/syslog.conf
- /etc/sshd_config
- /etc/ssh/ssh_config

Note: In most cases the default log level is appropriate. The log level should be set to Info in sshd_config, ssh_config and syslog.conf for production purposes. However, if you need to debug/investigate an observed problem, you might want to change the log level to debug level in sshd_config, and ssh_config for trouble shooting. Similarly, you can change the log level to auth.* in syslog.conf to get more details in the log messages.

Editing /etc/syslog.conf

1. Go to /etc/syslog.conf and change auth.info to auth.*. (This will generate log messages for every log level and not just info in auth.log)

2. Copy to /etc/syslog.conf to /nsconfig.

Editing /etc/sshd_config

1. Edit /etc/sshd_config and make the following changes for ssh specification

Ciphers aes128-cbc,aes256-cbc

MACs hmac-sha1,hmac-sha1-96,hmac-sha2-256,hmac-sha2-512

KexAlgorithms diffie-hellman-group14-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521

LogLevel Debug3

2. copy the sshd_config file to /nsconfig for persistency.

Editing /etc/ssh/ssh_config

1. Edit the /etc/ssh/ and edit the ssh_config as follows:

Ciphers aes128-cbc,aes256-cbc

MACs hmac-sha1,hmac-sha2-256,hmac-sha2-512

KexAlgorithms diffie-hellman-group14-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521

LogLevel Debug

Globalknownhostsfile /var/NDPPkeys/known_hosts

2. Copy the ssh_config file to /nsconfig for persistency.

Reboot the box after making these changes.

Note: Each log message can have one of the severity levels described in the following table.

Log Level	Indicates
EMERGENCY	Critical problem that might make the system unusable.
ALERT	Noncritical problem that might cause the NetScaler appliance to function incorrectly. You must take immediate corrective action to prevent the appliance from experiencing a critical problem.
CRITICAL	Critical condition that does not restrict operation but might escalate to a larger problem.
ERROR	Failure of a NetScaler operation.
WARNING	Issue that might result in critical errors.
NOTICE	Same as INFORMATION, but in greater detail.

Log Level	Indicates
INFORMATION	Any action taken by the NetScaler appliance. This level of logging can help troubleshoot problems on the Citrix NetScaler product line.
DEBUG	Extensive, detailed information. Developers use this level of logging to troubleshoot problems.

Log Management and Rotation of Log Files

Log management and rotation of syslog files are done by using `newsyslog`. The configuration file is located in `/etc/newsyslog.conf`.

This file is present in the memory file system by default, and any changes to it are lost after a reboot. To ensure persistence between reboots, copy it to the `/nsconfig` directory and make the required changes to that file.

By default, the `ns.log` file is rotated when its size reaches 100KB, and the last 25 copies of the ns.log are archived and compressed with gzip. For more information on log files, see Appendix D: Audit Log Files

Note: Only the superuser role has the privileges to perform this task.

Securely Transfer Audit Records to a Remote Audit Server

You need to securely transfer the audit records to a remote audit server. An SSH user-key is used to secure the transfer the audit logs to a remote server. It is assumed that a public key is already configured in the authorized key file on the remote server. The private key on the NetScaler is encrypted using a pass-phrase and AES 128 bit encryption. The pass-phrase required to decrypt the key is given by sysadmin when NetScaler powers-up. The pass-phrase is not saved on the file-system, so it must be input at every NetScaler restart. The SSH key always remains in encrypted format on the file-system.

Note: To make sure that a superuser is not able to access private keys on the NetScaler Appliance, the passphrase that is used to encrypt the private key should be set by, and only known by, an administrator who does not have the superuser capabilities.

The audit records are transferred to remote server by running the `cron` daemon to copy the files in a secure way to the remote audit server by using `scp`. The following sections describe the process involved. To carry out these operations, you must have superuser privileges.

The log transfer process can be automated via use of a script by using the following steps:

- Use nsafter.sh file which executes after reboot to dynamically generate the script file that sets environmental variables, starts ssh_agent, and transfers the logs using scp.

- Generate the public/private rsa key pair using the passphrase. You may have to set the desired read/write/execute permission for the folder to protect the keys.
- Copy the above public key to remote Audit server Authorized_keys file and check public key login.
- Update the global known hosts file for persistency.
- Put proper entries in crontab for copying the files.
- Run the script to set up the environment variables to add the private key to ssh-agent.
- After reboot, run the script again to set up the environmental variables. Note: The script will fail now during first run but will succeed later during subsequent run.
- Provide the passphrase to ssh_add command to add the private key to ssh-agent.
- Run the script again. It should pass this time.
- Start the Cron daemon, if it is not running to securely scp the logs.

Note: The script used at /var/<username>/script is not hard coded. It is dynamically generated on every reboot. To achieve this dynamism, enter the following lines in /nsconfig/nsafter.sh.

ssh-agent -s > /var/<username>/script

echo "scp -i /var/<username>/id_rsa /var/log/ns.log /var/log/ns.log.0* 9.9.9.2:/var/<username> 2>&1 |tee -ai /var/log/auth.log" >> /var/<username>/script

Example: The following output shows the contents of the script

```
root@ns_change# cat /var/<username>/script

SSH_AUTH_SOCK=/tmp/ssh-sIN1cYu9oebd/agent.1325; export SSH_AUTH_SOCK;

SSH_AGENT_PID=1332; export SSH_AGENT_PID;

echo Agent pid 1332;

scp -i /var/<username>/id_rsa /var/log/ns.log /var/log/ns.log.0* <audit server IP>:/var/<username>
2>&1 |tee -ai  /var/log/auth.log
```

Client-side (NetScaler) changes for SSH

Access the remote audit server through passwordless authentication to copy the files to the server. To do so, set up public key based authentication from the NetScaler appliance to the audit server.

1. Log on to the NetScaler appliance and access the shell.
   #ssh nsroot@<nsip>
   >shell

2. Generate an rsa key pair by using the following command. ((Note: Store the private key and Public key in /var instead of default location /root/.ssh, to make sure they are not lost on reboot)

3. root@ns# **ssh-keygen -t rsa**

   a. Enter the path to the file name (For example, /var/<username>/id_rsa) at the following prompt:

   Enter file in which to save the key (/root/.ssh/id_rsa): **/var/<username>/id_rsa**

   b. At the prompt enter a passphrase and re-enter it to confirm.

      Enter passphrase (empty for no passphrase):

      Enter same passphrase again:

   c. Verify that the following messages are displayed to indicate that the key is successfully created.

      Your identification has been saved in **/var/<username>/id_rsa.**

      Your public key has been saved in **/var/<username>/id_rsa.pub.**

      The key fingerprint is:

      41:98:7b:4f:06:3e:65:48:1a:86:ad:fe:36:3d:c1:0c:de:c6:68:48 root@ns

      The key's randomart image is:

      +--[RSA 2048]----+

      | oo+o. |

      | ..++o o |

      | ..o.+ |

      | E o +.o |

      | o o OS= |

      | o + B . |

      | o o . |

      | + o |

      | . . . |

      +-----------------+

   d. Make sure that the /var/<username> directory has the correct permissions to protect the private key. The recommended permissions are :

      - chmod 600 <dir name>

   Example:

drw------- 2 root wheel 512 Sep 28 22:44 NDPPkeys

e. You can use the cat command to display the public key as follows:

root@ns# **cat /var/<username>/id_rsa.pub**

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCz+7jlqwcXzloiWuviCOObfrHoxqETRJpP1OAjVWJvsRQBrNt
M6LZhLPHOkwpS3sjQLCktoB1aWjRCA9o6oo/vic0ee39jgwLSuf/z3z70z/2sTj/RlIX83PNBkuth+2hHJwX
Ta9hkezBKqBbYiDOg6MJQ529nB7UlOTVItE6m8ZozR0ctN87QzShsuLHN17C+ZUPTsKpnt8gMkMh39x
Ulq9kgqE3v7OzVukroZOAF/PVBjNQEWvZmxz9X4Pg7VVDQZAhC1SJW8GPozlxRUqFFGYJLsGKBSv+6Zh
6hqxTpPeEbWEhNiT4E3Ba4wuFSNvrqsOaPz7TE0Whyj7qSALHN root@ns

4. Copy the `id_rsa.pub` key to the `authorized_keys` directory in `/root/.ssh` on the remote audit server.

5. Try connecting to the audit server from the NetScaler appliance by using SSH. You should be able to log on.
root@ns# ssh -i /var/<username>/id_rsa <audit server IP>

Note: The –i argument should take the value of private key generated in step 2.

6. The `known_hosts` file in the NetScaler appliance is lost after a reboot. This results in the scp process, initiated by the `cron` daemon to prompt for an interactive input to add the host key, and then it fails. To make this work automatically after reboot, make the following changes:
    a. Edit /etc/ssh/ssh_config and add a directive as in the following example:

    Globalknownhostsfile /var/<username>/known_hosts

    b. Save a copy of ssh_config in /nsconfig.
    c. Copy the host key of audit server to known hosts file.

    root@ns# ssh-keyscan -t rsa -H <audit server IP> > /var/<username>/known_hosts

    The file location used in step a and step c should match. Instead of `/var`, you can choose `/flash`.

Cron Tab Changes on the Appliance for persistency across reboots

1. Configure the Cron daemon to initiate scp every two minutes. This can be achieved with the following entry in the /etc/crontab :

0/2 * * * * root cd /var/<username> && bash script

Note: As indicated by the above entry in the crontab file, "script" is the name of the script that is executed. The change directory command reflects the location of the script.

root@ns_change# ssh-add /var/<username>/id_rsa

2. On reboot, log on to NetScaler, go to the shell prompt and execute as follows:

```
root@ns# . /var/<username>/script
```

This step sets up the proper environment variables.

3. Provide `ssh-add <private key>` to input the passphrase to the agent.

Example:
ssh-add /var/<username>/id_rsa

Note: When you reboot, the above two steps (2 and 3) need to be repeated.

This procedure uses `scp` with the `-i` option where the private key is specified, and also copies both the current ns.log and the immediate old log, which in this case is ns.log.0.gz.

Note: This approach can also be used to copy other logs such `/var/log/`messages, `/var/log/`messages.0.gz, /var/log/auth.log and so on. For a list of audit log files that are important for monitoring the various events on a NetScaler appliance, see Appendix D.

After the above changes, run the following command:

```
root@ns# kill -SIGHUP `ps -ax | grep cron | awk '{print $1}'`
```

The `cron` daemon is monitored by a process called monit. This process checks once every minute to verify that the cron daemon is running, and starts the process if it is not running.

4. After the setup is completed, check the time stamp of the log files on the remote audit server. The log files should get updated every two minutes.`

Notes:

1. Always use a persistence file system on the NetScaler appliance, such as the `/var` or `/flash` directory, to store private keys. Otherwise, they might be lost when the appliance is restarted.
2. Any logs from the NetScaler appliance can be securely transferred to the remote audit server by using this procedure.
3. The crontab changes in the `/etc` folder are lost after a reboot. Make sure you have a copy of this file in the `/nsconfig` directory to make it persistent.

Change the Password of the RPC Node

To communicate with other NetScaler Gateway appliances, each appliance requires knowledge of the other appliances, including how to authenticate on NetScaler Gateway. RPC nodes are internal system entities used for system-to-system communication of configuration and session information. One RPC node exists on each NetScaler Gateway and stores information, such as the IP addresses of the other NetScaler Gateway appliance

and the passwords used for authentication. The NetScaler Gateway that makes contact with another NetScaler Gateway checks the password within the RPC node.

NetScaler Gateway requires RPC node passwords on both appliances in a high availability pair. Initially, each NetScaler Gateway is configured with the same RPC node password. To enhance security, you should change the default RPC node passwords. You use the configuration utility to configure and change RPC nodes.

Note: The NetScaler Gateway administrator password and the RPC node password must be the same.

Change the password of the RPC node to secure your NetScaler. The password is stored in encrypted form. You can verify that the password has changed by using the show rpcNode command to compare the encrypted form of the password before and after the change.

Note: Only a super user or sysadmin can carry out this task.

To change the password of an RPC node

At the NetScaler command line, type

```
set ns rpcNode <IPAddress> {-password}
```

To verify that the password has changed

At the NetScaler command line, type

```
show rpcNode
```

Example

```
> set rpcNode 192.0.2.4 -password mypassword
Done
> show rpcNode
.
.
IPAddress: 192.0.2.4 Password: d336004164d4352ce39e
SrcIP: *                Secure: OFF
Done
```

Here the Secure parameter defines the state of the channel when talking to the node. In the above example output, the secure channel is OFF.

Drop Invalid HTTP Requests

Consider using strict HTTP Profiles to drop invalid HTTP requests before they reach the servers. These profiles are available on the NetScaler appliance under the name —nshttp_default_strict_validation.‖ They should be bound to the virtual server explicitly, as shown:

```
> show ns httpProfile (Shows the available http profile (default+user configured profiles))
> set lb vserver <vserver name> -httpProfileName nshttp_default_strict_validation
```

NetScaler Gateway Configuration for the CC-Evaluated Deployment

The following recommendations are in addition to the NetScaler recommendations above and are specific to NetScaler Gateway.

- Use default DENY. Globally deny all resources and use authorization policies to selectively enable access to resources on a per-group basis by setting the value of the defaultAuthorizationAction parameter to DENY.

  In NetScaler release 10, by default, the authorization action is set to DENY. You should make sure that this value set to DENY, and grant only explicit access.

  To set the authorization action to DENY, at the NetScaler command prompt, type:

  ```
  set vpn parameter –defaultAuthorizationAction DENY
  ```

  To verify the setting, at the command prompt, type:

  ```
  sh vpn parameter
  ```

  Example:

  ```
  sh vpn parameter
  Http ports: 80
  Split DNS: BOTH
  Authorization action : DENY
  .
  .
  .
  Client debug: OFF
  ICA Proxy: OFF
  ```

  The following examples provide further clarification for the TOE administrator.

  Example 1:

  Consider a case in which the authorization action is set to DENY.

  ```
  set vpn parameter –defaultAuthorizationAction DENY
  sh vpn parameter
  Http ports: 80
  Split DNS: BOTH
  ```

```
Authorization action : DENY
.
.
```

If you want user sjones to be able to access only .GIF files add a policy and set it to ALLOW only *.GIF files for user sjones.

At the NetScaler command prompt, type:

```
add authorization policy author-policy "URL == /*.gif" ALLOW
bind aaa user sjones –policy author-policy
```

In this case, `author-policy` has one rule: “If the user attempts to access a .GIF file, ALLOW the request.” The EXPLICIT rule is “ALLOW access to .GIF files,” and the IMPLICIT rule is “DENY access to everything except .GIF files.” Therefore, if user sjones attempts to access anything other than GIF files, access is denied.

Example 2:

Consider a case in which the authorization action is set to ALLOW.

```
set vpn parameter –defaultAuthorizationAction ALLOW
sh vpn parameter
Http ports: 80
Split DNS: BOTH
Authorization action : ALLOW
.
.
```

Now, you want that when the user “foo” logs on through NetScaler Gateway, “foo” should NOT be able to access only .GIF files. To do so, you need to add a policy and set it to DENY only *.GIF files for the user “foo”.

At the NetScaler command prompt, type:

```
add authorization policy author-policy "URL == /*.gif" DENY
bind aaa user foo –policy author-policy
```

In this case, the policy “author-policy” has one rule - “if the user attempts to access a .GIF file, DENY the request.” The EXPLICIT rule is “DENY access to .GIF files”, but the IMPLICIT rule is “ALLOW access to everything except .GIF files”. Therefore, if the user “foo” attempts to access files of any other format (other than .GIF), the user will be allowed access.

- Use the intranet applications feature. Use intranet applications to define which networks are intercepted by the NetScaler Gateway plug-in and sent to the gateway. For example:

```
add vpn intranetApplication intra1 ANY 10.217.0.0 –netmask
```

```
255.255.0.0 –destPort 1–65535 –interception TRANSPARENT
bind vpn vserver v1 –intranetapp intra1
```

- Configure the NetScaler appliance to drop and log invalid HTTP requests. At the NetScaler command prompt, run the following command:

```
set ns httpParam [–dropInvalReqs ( ON | OFF )]
```

- Restrict access to non-HTTP backend services. FTP, RPC, SMB, and so on should not be accessed through the VPN or clientless VPN. Define authorization policies and bind the policies to specified users. Add specific ports based on the requirement. For example:

```
add authorization policy portDeny1 "REQ.IP.DESTIP ==
192.168.10.1 && (REQ.TCP.DESTPORT == 20 || REQ.TCP.DESTPORT ==
21 || REQ.TCP.DESTPORT == 22 || REQ.TCP.DESTPORT == 389)" DENY
bind aaa user administrator –policy portDeny1
```

Testing the Deployment Chapter 8

After you complete installation and configuration of the deployment, test it to make sure that it works.

If the NetScaler appliance is rebooted, make sure that the connection to the remote syslog server is re-established. This requires re-executing the script to set-up environmental variables. Also, you need to again provide the passphrase to ssh_add command to add the private key to ssh-agent as described in Securely Transfer Audit Records to a Remote Audit server.

Testing NetScaler Gateway

Perform the following procedures to test the NetScaler Gateway deployment:

To verify that a user is granted access based on the source IP, SSL certificate attributes, and user name and password

1. Log on to NetScaler Gateway.
2. Enter the user name and password.
3. Provide a valid client certificate (if required per configuration)

To verify that users cannot access protected backend resources without first connecting and authenticating through the NetScaler Gateway server, access the NetScaler Gateway server.

The logon page should only allow you to enter your user name and password. No backend resources should be displayed.

To verify that only authorized users are allowed access to backend resources

1. Log on as an authorized user and establish a VPN session as described above.
2. Access a backend service for which access is allowed by a policy.
3. Log out and attempt to log on with an invalid user name and/or incorrect password. You should not be able to log on successfully.

Making Sure Features are Disabled

Only common criteria evaluated features need to be enabled. Log on to the NetScaler and verify that all other features are disabled. At the NetScaler command prompt, type:

```
show ns features
```

Appendix A: Audit Log Events

The following table list various audit log events and their formats. For information on configuring the log level for ns.log and syslog refer to *Configuring Audit Server Logging* on page 60 of this document. To change the log level for scp audits, it will be necessary to change the LogLevel parameter in /etc/ssh_conf, save the file, and make a copy of the saved ssh_conf file to the /nsconfig directory. SuperUser access is required for this activity.

Note: To generate all the audit events, the audit level should be set to the value indicated in the *Log Level* column.

Feature	Reason	Log Level	Example Message	ST Reference	File Location
TLS TLS VPN	Handshake failure due to incorrect authentication	Debug	Aug 12 02:20:35 <local0.debug> 10.102.47.3 08/12/2014:02:20:35 GMT CitrixNS_win 0-PPE-2 : SSLLOG SSL_HANDSHAKE_FAILURE 80 0 : SPCBId 472 - ClientIP 10.252.240.199 - ClientPort 55142 - VserverServiceIP 10.102.47.55 - VserverServicePort 443 - ClientVersion TLSv1.0 - CipherSuite "RC4-MD5 TLSv1 Non-Export 128-bit" - Reason "No client certificate received"	Section 6.11: FCS_TLS_EXT.1 Section 6.11: FCS_HTTPS_EXT.1 Section 6.11: FTP_TRP.1	/var/log/ns.log
TLS TLS VPN	Handshake Failure due to protocol version mismatch	Debug	Nov 8 22:49:56 <local0.debug> 10.102.113.18 11/08/2014:22:49:56 GMT ns 0-PPE-0 : SSLLOG SSL_HANDSHAKE_FAILURE 491 0 : SPCBId 744 - ClientIP 10.102.1.91 - ClientPort33174 - VserverServiceIP 10.102.113.2 1 - VserverServicePort 443 - ClientVersion SSLv3.0 - CipherSuite "NA" - Reason "SSLv3 protocol support disabled"	Section 6.11: FCS_TLS_EXT.1 Section 6.11: FCS_HTTPS_EXT.1 Section 6.11: FTP_TRP.1	/var/log/ns.log
TLS TLS VPN	Handshake failure due to cipher mismatch	Debug	Nov 8 22:51:20 <local0.debug> 10.102.113.18 11/08/2014:22:51:20 GMT ns 0-PPE-0 : SSLLOG SSL_HANDSHAKE_FAILURE 497 0 : SPCBId 746 - ClientIP 10.102.1.91	Section 6.11: FCS_TLS_EXT.1 Section 6.11: FCS_HTTPS_EXT.1 Section 6.11:	/var/log/ns.log

			- ClientPort33237 - VserverServiceIP 10.102.113.21 - VserverServicePort 443 - ClientVersion TLSv1.0 - CipherSuite "NA" - Reason "No shared cipher"	FTP_TRP.1	
TLS TLS VPN	Handshake failure due to Unknown CA	Debug	Nov 8 22:55:54 <local0.debug> 10.102.113.18 11/08/2014:22:55:54 GMT ns 0-PPE-0 : SSLLOG SSL_HANDSHAKE_FAILURE 5180 : SPCBId 749 - ClientIP 10.102.1.91 - ClientPort33514 - VserverServiceIP 10.102.113.21 - VserverServicePort 443 - ClientVersion TLSv1.2 - CipherSuite "AES-256-CBC-SHA SSLv2 Non-Export 256-bit" - CLIENT_AUTHENTICATION_FAILED - SerialNumber "8A" - Reason "No CA (Issuer) certificate found"	Section 6.11: FCS_TLS_EXT.1 Section 6.11: FCS_HTTPS_EXT.1 Section 6.11: FTP_TRP.1	/var/log/ns.log
TLS TLS VPN	Successful Handshake Negotiation	Debug	Oct 1 04:31:12 <local0.debug> 10.217.206.60 10/01/2015:04:31:12 GMT ns 0-PPE-0 : SSLLOG SSL_HANDSHAKE_SUCCESS 1040 : SPCBId 455 - ClientIP 10.215.136.76 - ClientPort 53069 - VserverServiceIP 10.217.205.63 - VserverServicePort 443 - ClientVersion TLSv1.2 - CipherSuite "AES-256-CBC-SHA SSLv2 Non-Export 256-bit" - Session New	Section 6.11: FCS_TLS_EXT.1 Section 6.11: FCS_HTTPS_EXT.1 Section 6.11: FTP_TRP.1	/var/log/ns.log
TLS VPN	Initiate Session	Info	Oct 1 04:31:10 <local0.info> 10.217.206.60 10/01/2015:04:31:10 GMT ns 0-PPE-4 : SSLVPN LOGIN 49 0 : Context aaatest@10.215.136.76 - SessionId: 5- User aaatest - Client_ip 10.21 5.136.76 - Nat_ip "Mapped Ip" - Vserver 10.217.205.63:443 - Browser_type "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0" - SSLVPN_client_type Agent -	Section 6.11 FTP_TRP.1 Section 6.11: FIA_UIA_EXT.1 Section 6.11: FIA_UIA_EXT.2	/var/log/ns.log

			Group(s) "N/A"		
TLS VPN	Terminate Session	Err/ Info	13:00 <local0.err> 10.217.206.60 10/05/2015:23:13:00 GMT ns 0-PPE-2 : SSLVPN REMOVE_SESSION 318 0 : Sessionid 40 - User aaatest - Client_ip 10.215.136.76 - Nat_ip "Mapped Ip" - Vserver_ip 10.217.205.63 - Errmsg "user initiated vpn remove session" Oct 5 23:13:00 <local0.info> 10.217.206.60 10/05/2015:23:13:00 GMT ns 0-PPE-4 : SSLVPN LOGOUT 702 0 : Context aaatest@10.215.136.76 - SessionId: 40- User aaatest - Client_ip 10.215.136.76 - Nat_ip "Mapped Ip" - Vserver 10.217.205.63:443 - Start_time "10/05/2015:23:11:57 GMT" - End_time "10/05/2015:23:13:00 GMT" - Duration 00:01:03 - Http_resources_accessed 0 - NonHttp_services_accessed 0 - Total_TCP_connections 17 - Total_UDP_flows 0 - Total_policies_allowed 0 - Total_policies_denied 0 - Total_bytes_send 9173 - Total_bytes_recv 35140 - Total_compressedbytes_send 0 - Total_compressedbytes_recv 0 - Compression_ratio_send 0.00% - Compression_ratio_recv 0.00% - LogoutMethod "Explicit" - Group(s) "N/A"	Section 6.11 FTP_TRP.1 Section 6.11: FIA_UIA_EXT.1 Section 6.11: FIA_UIA_EXT.2	/var/log/ns.log
CLI	Successful SSH administration session (Remote)	Info	Oct 13 05:08:09 <local0.info> 10.102.146.22 10/13/2014:05:08:09 GMT dk-cb-hasal01-csg1 PPE-0 : UI CMD_EXECUTED 108 : User nsroot – Remote_ip 10.105.180.13 – Command “login” – Status “Success”	Section 6:11: FCS_SSH_EXT.1 Section 6.11: FIA_UIA_EXT.1 Section 6.11: FIA_UIA_EXT.2 Section 6.11 FTP_TRP.1	/var/log/ns.log

CLI	SSH Session establishment (Remote)	Debug	Sep 30 02:04:08 <auth.debug> ns sshd[65075]: debug1: Entering interactive session for SSH2.	Section 6.11: FCS_SSH_EXT.1	/var/log/ auth.log
CLI	Console Session Establishment (Local)	Info	Oct 13 05:28:55 <local0.info> 10.102.146.23 10/13/2014:05:28:55 GMT 1-PPE-1 : UI CMD_EXECUTED 132 0 : User nsroot - Remote_ip 127.0.0.1 - Command "login nsroot "********"" - Status "Success"	Section 6.11: FIA_UIA_EXT.1 Section 6.11: FIA_UIA_EXT.2 Section 6.11 FTP_TRP.1	/var/log/ns.log
CLI	SSH Authentication Failure (Remote)	Info	Feb 1 13:30:52 <local0.info> 10.102.146.22 02/01/2014:13:30:52 GMT 0-PPE-0 : UI CMD_EXECUTED 1710 0 : User nsroot - Remote_ip 10.252.243.179 - Command "login nsroot "********"" - Status "ERROR: Invalid username or password"	Section 6:11: FCS_SSH_EXT.1 Section 6.11: FIA_UIA_EXT.1 Section 6.11 FTP_TRP.1 Section 6.11: FIA_UIA_EXT.2	/var/log/ns.log
CLI	Console Authentication Failure (Local)	Info	Oct 13 05:28:55 <local0.info> 10.102.146.23 10/13/2014:05:28:55 GMT 1-PPE-1 : UI CMD_EXECUTED 132 0 : User nsroot - Remote_ip 127.0.0.1 - Command "login nsroot "********"" - Status "ERROR: Invalid username or password"	Section 6.11: FIA_UIA_EXT.1 Section 6.11: FIA_UIA_EXT.2 Section 6.11 FTP_TRP.1	/var/log/ns.log
CLI	SSH Remote Session Termination due to Timeout	Info	Nov 2 06:42:27 <local0.info> DC1-N-NTSCLR2P nscli: read_char(): CLI session timed out at Sun Nov 2 06:42:27 2014 Nov 2 06:42:27 <local0.info> 10.102.146.23 11/02/2014:06:42:27 GMT DC1-N-NTSCLR2P 0-PPE-1 : CLI CMD_EXECUTED 210 0 : User test - Remote_ip 10.252.245.80 - Command "logout" - Status "Success"	Section 6:11: FCS_SSH_EXT.1 Section 6.11: FTA_SSL.3 Section 6.11 FTP_TRP.1	/var/log/ns.log

CLI	Console Local Session Termination due to Timeout	Info	Sep 18 02:54:22 <local0.info> CitrixNS nscli: read_char(): CLI session timed out at Thu Sep 18 02:54:22 2014 Sep 18 02:54:23 <local0.info> 10.102.47.3 09/18/2014:02:54:23 GMT CitrixNS 0-PPE-2 : CLI CMD_EXECUTED 176 0 : User test - Remote_ip 127.0.0.1 - Command "logout" - Status "Success"	Section 6.11: FTA_SSL_EXT.1 Section 6.11 FTP_TRP.1	/var/log/ns.log
CLI	SSH Termination of Remote Interactive Session	Info	Aug 12 11:08:13 <local0.info> 10.102.146.23 08/12/2014:11:08:13 GMT DC1-N-NTSCLR2P 0-PPE-0 : CLI CMD_EXECUTED 148 0 : User nsroot - Remote_ip 10.102.146.23 - Command "logout" - Status "Success"	Section 6:11: FCS_SSH_EXT.1 Section 6.11: FTA_SSL.4 Section 6.11: FIA_UIA_EXT.1 Section 6.11: FIA_UIA_EXT.2 Section 6.11 FTP_TRP.1	/var/log/ns.log
CLI	Console Termination of Local Interactive Session	Info	Sep 18 02:55:29 <local0.info> 10.102.47.3 09/18/2014:02:55:29 GMT CitrixNS 0-PPE-2 : CLI CMD_EXECUTED 178 0 : User nsroot - Remote_ip 127.0.0.1 - Command "logout" - Status "Success"	Section 6.11: FTA_SSL.4 Section 6.11: FIA_UIA_EXT.1 Section 6.11: FIA_UIA_EXT.2 Section 6.11 FTP_TRP.1	
CLI	SSH Handshake failure due to oversized packet	Info	Sep 30 02:04:08 <auth.info> ns sshd[65075]: Bad packet length 270028.	Section 6.11: FTA_SSL.4 Section 6.11: FIA_UIA_EXT.1 Section 6.11: FIA_UIA_EXT.2 Section 6.11 FTP_TRP.1	/var/log/ auth.log

System Time	System Time Change	Notice	Jan 3 05:43:20 <local7.notice> ns bash[32717]: root on /dev/pts/1 shell_command="date 1501010101" Jan 1 01:01:00 <auth.notice> ns date: date set by root	Section 6.11: FPT_STM.1	/var/log/ns.log
Audit	Shutdown of Audit Function	Debug	Aug 28 02:38:50 <syslog.err> citrixnetscaler syslogd: exiting on signal 15	Section 6.11: FAU_GEN.1	/var/log/ messages /dev/console
Audit	Startup of Audit Function	Info	Aug 28 02:38:50 <local0.info> 10.102.146.4 2014/08/28:13:38:50 GMT 0-PPE-1 : default CLI CMD_EXECUTED 97 0 : User nsroot - Remote_ip - Command "reboot" - Status "Success" Aug 28 02:45:06 <local0.info> citrixnetscaler nssetup: _checkconfigsrc(): NetScaler will be started from the last saved config	Section 6.11: FAU_GEN.1	/var/log/ns.log
Trusted Channel	Success using LDAP over TLS	Debug	See Appendix E: *Additional Audit Messages/LDAP/Success Messages* for examples	Section 6.11: FTP_ITC.1	/var/log/ns.log
Trusted Channel	Failure using LDAP over TLS	Debug	See Appendix E: *Additional Audit Messages/LDAP/Failure Messages* for examples	Section 6.11: FTP_ITC.1	/var/log/ns.log
Trusted Channel	Failure using SSH (cipher mismatch)	Debug	debug1: SSH2_MSG_KEXINIT sent debug1: SSH2_MSG_KEXINIT received no matching cipher found: client aes256-cbc server aes128-cbc	Section 6.11: FTP_ITC.1 Section 6.11: FCS_SSH_EXT.1	/var/log/ auth.log
Trusted Channel	Failure using SSH (MAC mismatch)	Debug	debug1: SSH2_MSG_KEXINIT sent debug1: SSH2_MSG_KEXINIT	Section 6.11: FTP_ITC.1 Section 6.11:	/var/log/ auth.log

			received no matching mac found: client hmac-sha1,hmac-sha1-96,hmac-sha2-256,hmac-sha2-512 server hmac-md5-96	FCS_SSH_EXT.1	
Trusted Channel	Failure using SSH (KEX mismatch)	Debug	debug1: SSH2_MSG_KEXINIT sent debug1: SSH2_MSG_KEXINIT received debug1: kex: server->client aes128-ctr hmac-md5 none debug1: kex: client->server aes128-ctr hmac-md5 none Unable to negotiate a key exchange method	Section 6.11: FTP_ITC.1 Section 6.11: FCS_SSH_EXT.1	/var/log/ auth.log
System Update	Update system firmware	Info	See Appendix E: *Additional Audit Messages/LDAP/System Update* for examples	Section 6.11 FPT_TUD_EXT.1	/var/log/ns.log

Appendix B: Access Control Matrix

Role	read-only	operator	network	superuser	custom - defined role	System Administrator (sysadmin)
Security Attributes						
Administrator roles				create, delete, query, modify	as defined	create, delete, query, modify
Administrator groups				create, delete, query, modify	as defined	create, delete, query, modify
Role policies				create, delete, query, modify	as defined	create, delete, query, modify
Role priorities				create, delete, query, modify	as defined	create, delete, query, modify
VPN user groups	query	query, modify	create, delete, query, modify	create, delete, query, modify	as defined	create, delete, query, modify
VPN user permissions	query	query, modify	create, delete, query, modify	create, delete, query, modify	as defined	create, delete, query, modify
Attack Signatures			import, delete	import, delete	as defined	import, delete
Functions						
SSL VPN	determine the behavior of	determine the behavior of	determine the behavior of, modify the behavior of	determine the behavior of, modify the behavior of	as defined	determine the behavior of, modify the behavior of

Role	read-only	operator	network	superuser	custom-defined role	System Administrator (sysadmin)
Audit	determine the behavior of	determine the behavior of	determine the behavior of	determine the behavior of, modify the behavior of	as defined	determine the behavior of, modify the behavior of
Attack Signatures	Not available at the CLI. Signatures file is edited directly to enable or disable signatures and set the options to block, log, or collect statistics					
TSF Data						
Audit Data				query, delete	as defined	query, delete
Administrator accounts				create, delete, query, modify	as defined	create, delete, query, modify
VPN user accounts	query	create, delete, query, modify	create, delete, query, modify	create, delete, query, modify	as defined	create, delete, query, modify
Attack Signatures	query for stats	query for stats	query for stats and logs	query for stats and logs	as defined	query for stats and logs

Appendix C: Processes Running on NetScaler

S.No	Process Name	Description	Privilege
1.	nspitboss (pitboss)	Watchdog for critical NetScaler processes	root
2.	/usr/sbin/syslogd	syslogd daemon	root
3.	/usr/sbin/inetd	Internet service daemon	root
4.	/usr/sbin/cron	cron job	root
5.	/bin/httpd	httpd daemon	root
6.	/usr/local/bin/monit -c /etc/monitrc	Watchdog to restart specific processes	root
7.	/usr/sbin/sshd -f /etc/sshd_config	ssh daemon	root
8.	nsppe (NSPPE-00)	Packet engine service to handle NetScaler features	root
9.	/netscaler/nsnetsvc	Handles IOCTLS between nsconfigd and Netscaler packet engine	root
10.	/netscaler/nsaggregatord	Aggregator daemon that aggregates traffic statistics	root
11.	/netscaler/nsclusterd	Runs the cluster protocol	root
12.	/netscaler/monuploadd	Monitors the NetScaler for critical issues and potential hardware failures. If this process detects such a condition, it automatically creates a showtechsupport archive and uploads it to the Citrix TaaS servers. Also sends corresponding SNMP traps, if they are enabled.	root
13.	/netscaler/nsconfigd -S	Process that handles symantic validations and HA	root
14.	/netscaler/nsfsyncd -d	Nsfsync uses rsync to copy a set of files from primary to secondary.	root
15.	/netscaler/imi -d -f /nsconfig/ZebOS.conf	Daemon for configuration management for routing protocols	root
16.	/netscaler/nskrb nsauth	Kerberos authentication daemon	root
17.	/netscaler/nscrlrefresh	CRL (Certification Revocation List) refreshing daemon	root
18.	/netscaler/nsm	Manages kernel routing table management and redistribution between different routing protocols.	root
19.	/netscaler/nsvpnd	SSL VPN daemon	root
20.	/netscaler/nsaaad	Authentication daemon. Supports authentication for SSLVPN users and Netscaler system/admin users	root
21.	/netscaler/ripd	RIP routing daemon	root
22.	/netscaler/nsclfsyncd	File sync daemon in cluster mode	root

23.	/netscaler/provserverd	Interface for communicating with CloudStack to facilitate Policy Autoscaling	root
24.	/netscaler/nsrised	Daemon for communication with the Cisco N7k switches, using RISE protocol.	root
25.	/netscaler/syshealthd	System health check daemon	root
26.	/netscaler/nscollect	Historical charting daemon	root
27.	/netscaler/nscac64p	Caching daemon	root
28.	/netscaler/nscopo	Daemon for FEO feature: optimizes CSS, JS, images	root
29.	/netscaler/nssync	Synchronize the configuration from primary	root
30.	/netscaler/nsumond	Scriptable monitoring daemon. Periodically invokes user provided scripts which monitor health of the servers.	Root, nsmonitor
31.	/netscaler/aslearn	AppFW learning daemon	root
32.	/usr/libexec/getty	Get teletype to manage physical and virtual terminals	root
33.	login [pam] (login)	Logon process	root
34.	-bash [bash]	Bash shell process	root

Appendix D: Audit Log Files

Following is a list of audit log files that are important for monitoring the various events on a NetScaler appliance:

- Auth.log
- Bash.log
- Cron
- Messages
- Notice.log
- Ns.log
- Nsvpn.log
- Sh.log

These files are located in `/var/log` directory. These log files have a default minimum size of 100 KB. They are securely transferred to an external audit log server once every hour or when they reach a size of 100 KB. These files are listed in the `/etc/newsyslog.conf` file. The following screen output shows a sample of the `newsyslog.conf` file:

```
# Netscaler newsyslog.conf

# This file is present in the memory filesystem by default, and any changes
# to this file will be lost following a reboot. If changes to this file
# require persistence between reboots, copy this file to the /nsconfig
# directory and make the requried changes to that file.
#
# logfilename          [owner:group]    mode count size when  flags [/pid_file] [sig_num]
/var/log/cron                           600  3     100  *     Z
/var/log/amd.log                        644  7     100  *     Z
/var/log/auth.log                       600  7     100  *     Z
/var/log/kerberos.log                   600  7     100  *     Z
/var/log/lpd-errs                       644  7     100  *     Z
/var/log/maillog                        640  3     *    @T00  Z
/var/log/sendmail.st                    640  3     *    168   B
/var/log/messages                       644  25    100  *     Z
/var/log/all.log                        600  7     *    @T00  Z
/var/log/slip.log                       640  3     100  *     Z
/var/log/ppp.log                        640  3     100  *     Z
/var/log/security                       600  10    100  *     Z
/var/log/wtmp                           644  3     *    @01T05 B
/var/log/daily.log                      640  7     *    @T00  ZN
/var/log/weekly.log                     640  5     1    $W6D0 ZN
/var/log/monthly.log                    640  12    *    $M1D0 ZN
/var/log/console.log                    600  5     100  *     Z
/var/log/ns.log                         600  25    100  *     Z
/var/log/nitro.log                      600  10    100  *     Z
/var/log/nsvpn.log                      600  5     100  *     Z
/var/log/httperror.log                  600  5     100  *     B   /var/run/httpd.pid 30
/var/log/httpaccess.log                 600  5     100  *     Z   /var/run/httpd.pid 30
/var/log/wicmd.log                      600  5     100  *     Z
/var/nslog/aslearn.log          644      10              100     *       ZN
/var/log/callhomedebug.log              600  5     100  *     Z
/var/log/callhome.log                   600  5     100  *     Z
~
```

You can configure the count and size of the file to decide when the files are transferred to the external audit log server. To edit the `newsyslog.conf` file in the `/etc` directory, first make a copy of the file in the /nsconfig folder. After the `newsyslog.conf` file is copied to the `/nsconfig` folder, you can edit the file.

Appendix E: Additional Audit Messages

LDAP

Success Messages

Under /var/log/ns.log:

Nov 2 07:00:46 <local0.info> 10.102.146.23 11/02/2014:07:00:46 GMT DC1-N-NTSCLR2P 0-PPE-2 : AAA Message 62 0 : "In update_aaa_cntr: Succeeded policy for user testuser = ldap22new1"

Nov 2 07:00:46 <local0.info> 10.102.146.23 11/02/2014:07:00:46 GMT DC1-N-NTSCLR2P 0-PPE-1 : UI CMD_EXECUTED 233 0 : User testuser - Remote_ip 10.252.245.80 - Command "login testuser "*********"" - Status "Success"

Under /var/log/nsvpn.log:

ANov 2 06:58:59 <local1.err> DC1-N-NTSCLR2P [1121]: In start_ldap_auth: For user testuser, Null password check failed in ldap authentication: 2

Nov 2 07:00:46 <local1.info> DC1-N-NTSCLR2P [1121]: In start_ldap_auth: attempting to do ldap auth for testuser @ 10.102.229.222

Nov 2 07:00:46 <local1.info> DC1-N-NTSCLR2P [1121]: In ns_ldap_set_up_socket: Server certificate hostname = NULL

Nov 2 07:00:46 <local1.info> DC1-N-NTSCLR2P [1121]: In ns_ldap_set_up_socket: setting up for SSL connection to : 10.102.229.222:636

Nov 2 07:00:46 <local1.info> DC1-N-NTSCLR2P [1121]: In ns_ldap_set_up_socket: Successfully established connection to NULL

Nov 2 07:00:46 <local1.info> DC1-N-NTSCLR2P [1121]: In receive_ldap_user_search_event: Admin authentication(Bind) succeeded, now attempting to search the user testuser

Nov 2 07:00:46 <local1.info> DC1-N-NTSCLR2P [1121]: In receive_ldap_user_search_event: User search succeeded, attempting user authentication(Bind) for testuser

Nov 2 07:00:46 <local1.info> DC1-N-NTSCLR2P [1121]: In receive_ldap_user_bind_event: User authentication (Bind event) for user testuser succeeded

Note: The last message in the above log output also indicates the termination of the LDAP connection.

Failure Messages

Under /var/log/ns.log:

Nov 2 07:04:55 <local0.err> 10.102.146.23 11/02/2014:07:04:55 GMT DC1-N-NTSCLR2P 0-PPE-0 : AAA Message 109 0 : " In receive_ldap_user_bind_event: ldap_bind user failed for user testuser"

Nov 2 07:04:55 <local0.info> 10.102.146.23 11/02/2014:07:04:55 GMT DC1-N-NTSCLR2P 0-PPE-2 : AAA Message 63 0 : "In update_aaa_cntr: Failed policy for user testuser = ldap22new1"

Nov 2 07:04:55 <local0.info> 10.102.146.23 11/02/2014:07:04:55 GMT DC1-N-NTSCLR2P 0-PPE-1 : UI CMD_EXECUTED 235 0 : User testuser - Remote_ip 10.252.245.80 - Command "login testuser "*********"" - Status "ERROR: Invalid username or password"

Note: The last message in the above log output also indicates the termination of the LDAP connection.

Under /var/log/nsvpn.log

Nov 2 07:04:55 <local1.info> DC1-N-NTSCLR2P [1121]: In start_ldap_auth: attempting to do ldap auth for testuser @ 10.102.229.222

Nov 2 07:04:55 <local1.info> DC1-N-NTSCLR2P [1121]: In ns_ldap_set_up_socket: Server certificate hostname = NULL

Nov 2 07:04:55 <local1.info> DC1-N-NTSCLR2P [1121]: In ns_ldap_set_up_socket: setting up for SSL connection to : 10.102.229.222:636

Nov 2 07:04:55 <local1.info> DC1-N-NTSCLR2P [1121]: In ns_ldap_set_up_socket: Successfully established connection to NULL

Nov 2 07:04:55 <local1.info> DC1-N-NTSCLR2P [1121]: In receive_ldap_user_search_event: Admin authentication(Bind) succeeded, now attempting to search the user testuser

Nov 2 07:04:55 <local1.info> DC1-N-NTSCLR2P [1121]: In receive_ldap_user_search_event: User search succeeded, attempting user authentication(Bind) for testuser

Nov 2 07:04:55 <local1.info> DC1-N-NTSCLR2P [1121]: In ns_ldap_check_result: For user testuser, LDAP authentication failed (error 49): Invalid credentials

Nov 2 07:04:55 <local1.err> DC1-N-NTSCLR2P [1121]: In receive_ldap_user_bind_event: ldap_bind user failed for user testuser

Note: The last message in the above log output also indicates the termination of the LDAP connection.

System Update

Oct 1 04:18:52 <local7.notice> ns bash[7010]: root on /dev/pts/0 shell_command="./installns"

Oct 1 04:18:52 <user.notice> ns installns: [7443]: BEGIN_TIME 1443673132 Thu Oct 1 04:18:52 2015

Oct 1 04:18:52 <user.notice> ns installns: [7443]: VERSION ns-10.5-53.22.gz

Oct 1 04:18:52 <user.notice> ns installns: [7443]: VARIANT v

Oct 1 04:18:52 <user.notice> ns installns: [7443]: No options

Oct 1 04:18:52 <user.notice> ns installns: [7443]: installns version (10.5-53.22) kernel (ns-10.5-53.22.gz)

Oct 1 04:18:57 <user.notice> ns installns: [7443]: Installation is starting ...

Oct 1 04:18:57 <user.notice> ns installns: [7443]: detected Version >= NS6.0

Oct 1 04:18:57 <user.notice> ns installns: [7443]: Installation path for kernel is /flash

Oct 1 04:21:25 <user.notice> ns installns: [7443]: Size of kernel ns-10.5-53.22.gz is 133038 kilobytes

Oct 1 04:21:25 <user.notice> ns installns: [7443]: Available space on /flash/ filesystem is 3069926 kilobytes

Oct 1 04:21:25 <user.notice> ns installns: [7443]: Available space on /var is 296254618 kilobytes

Oct 1 04:21:25 <user.notice> ns installns: [7443]: Checking directories ...

Oct 1 04:21:27 <user.notice> ns installns: [7443]: Checksumming ns-10.5-53.22.gz ...

Oct 1 04:21:27 <user.notice> ns installns: [7443]: Checksum ok.

Oct 1 04:21:27 <user.notice> ns installns: [7443]: Copying ns-10.5-53.22.gz to /flash/ns-10.5-53.22.gz ...

Oct 1 04:21:27 <user.notice> ns installns: [7443]: BEGIN KERNEL_COPY

Oct 1 04:21:57 <user.notice> ns installns: [7443]: END KERNEL_COPY

Oct 1 04:21:57 <user.notice> ns installns: [7443]: Changing /flash/boot/loader.conf for ns-10.5-53.22 ...

Oct 1 04:21:57 <user.notice> ns installns: [7443]: Installing XML API documentation...

Oct 1 04:21:57 <user.notice> ns installns: [7443]: Installing NSConfig.wsdl...

Oct 1 04:21:57 <user.notice> ns installns: [7443]: Installing NSStat.wsdl...

Oct 1 04:21:57 <user.notice> ns installns: [7443]: Installing online help...

Oct 1 04:22:00 <user.notice> ns installns: [7443]: Installing Cisco online help...

Oct 1 04:22:04 <user.notice> ns installns: [7443]: Installing SCOM Management Pack...

Oct 1 04:22:04 <user.notice> ns installns: [7443]: Installing LoadBalancer Pack...

Oct 1 04:22:16 <user.notice> ns installns: [7443]: Installing EPA Package ...

Oct 1 04:22:10 <user.notice> ns installns: [7443]: Installing GUI...

Oct 1 04:22:16 <user.notice> ns installns: [7443]: Installing EPA Package ...

Oct 1 04:22:16 <user.notice> ns installns: [7443]: Installing NITRO...

Oct 1 04:22:17 <user.notice> ns installns: [7443]: Installing Jazz certificate ...

Oct 1 04:22:17 <user.notice> ns installns: [7443]: Installing Call Home certificate ...

Oct 1 04:22:17 <user.notice> ns installns: [7443]: Creating after upgrade script ...

Oct 1 04:22:17 <user.notice> ns installns: [7443]: prompting for reboot

Oct 1 04:22:17 <user.notice> ns installns: [7443]: END_TIME 1443673337 Thu Oct 1 04:22:17 2015