Common Criteria Evaluated Configuration Guide for NetScaler 10 Platinum Edition

Copyright and Trademark Notice

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, try to correct the interference by using 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.

Document code: May 13, 2013 17:56:12

Contents

Chapter 4 Configuring Citrix NetScaler

Chapter 5 Securing the Deployment

CHAPTER 1

Introduction

About this Guide

The Common Criteria Evaluated Configuration Guide for Citrix NetScaler 10 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 you to deploy NetScaler to match the Common Criteria Target of Evaluation configuration exactly, follow the procedures in this guide.

Common Criteria Target of Evaluation

The Common Criteria Target of Evaluation (TOE) is the Citrix NetScaler Appliance 10, Platinum Edition. The TOE either operates as a dedicated self-contained appliance running on dedicated hardware provided as part of the TOE, or operates as a virtual appliance on the Citrix XenServer hardware virtualization product.

This guide supplements the core documentation and details how to configure NetScaler to match the Common Criteria Target of Evaluation configuration. The Target of Evaluation is a NetScaler deployment comprising:

- Citrix NetScaler 10 (Platinum Edition license)
- Citrix Access Gateway
- Citrix Application Firewall
- Citrix NetScaler Virtual Appliance (VPX) 10

Citrix XenServer 6.0.2 Platinum Edition components are also required to provide the NetScaler VPX in this deployment and so form part of the NetScaler Common Criteria environment but are not considered part of the TOE.

For information on the XenServer 6.0.2 Platinum Edition Common Criteria evaluated deployment, see the *Common Criteria Evaluated Configuration Guide for Citrix XenServer 6.0.2, Platinum Edition*.

For further information concerning the NetScaler Common Criteria evaluated deployment, see "Common Criteria Evaluated Deployment," on page 5.

This evaluated deployment does not include the following components:

- Content Switching
- Content Rewrite
- Caching
- Compression
- Web Logging
- Layer 3 Routing
- Load Balancing between NetScaler Appliances
- GUI Dashboard Command Center Application
- NetScaler XML-API interface

Citrix NetScaler Documentation

This guide occasionally refers to Citrix product documentation and other documentation that are essential references when deploying Citrix NetScaler in the Target of Evaluation configuration.

- *Citrix NetScaler Command Reference Guide*. A reference that includes all NetScaler commands.
- *Citrix NetScaler Log Message Reference*. A reference that includes syslog and Web server log messages.
- *Citrix NetScaler Hardware Installation and Setup Guide*. Provides hardware installation and initial configuration information for all hardware models and platforms.
- *Citrix NetScaler Migration Guide*. Describes migration instructions for setting up a new version of a NetScaler with a list of all new and deprecated commands, parameters, and SNMP OIDs.
- *Citrix NetScaler VPX Getting Started Guide*. Provides installation and configuration instructions for Citrix NetScaler Virtual Appliance.
- *Citrix NetScaler Administration Guide*. Describes how to manage and monitor the NetScaler using built-in features, such as AAA policies, role-based authorization, SNMP, and statistical counters.

- *Citrix NetScaler Traffic Management Guide*. Provides configuration and installation information for traffic management features, such as load balancing, content switching, and DNS.
- *Citrix NetScaler Networking Guide*. Describes configuration information for networking features with an emphasis on dynamic routing.
- *Citrix NetScaler Policy Configuration and Reference Guide*. Provides configuration and reference information for controlling the behavior of NetScaler functions by using advanced policies and expressions, classic policies and expressions, and HTTP callouts.
- *Citrix Application Firewall Guide*. Provides installation and configuration instructions for a standalone Citrix Application Firewall and the integrated Citrix NetScaler Application Firewall feature.

Note: The Application Firewall guide does not accurately reflect the syntax to be used for advanced expressions in the CLI (the guide reflects GUI usage). Escape characters must be provided to indicate a text string when entered via the CLI.

For example, the incorrect usage provided in the guide:

add appfw policy pl-blog
"HTTP.REQ.HOSTNAME.DOMAIN.EQ("blog.example.com")" pr-blog

The correct usage is:

add appfw policy pl-blog
"HTTP.REQ.HOSTNAME.DOMAIN.EQ(\"blog.example.com\")" pr-blog

- *Common Criteria Security Target for Citrix NetScaler 10, 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. This document is available only on the Citrix Web site.
- *Common Criteria Evaluated Configuration Guide for Citrix XenServer 6.0.2 Platinum Edition.* Describes how to install and configure the necessary XenServer components in accordance with the XenServer Common Criteria evaluated deployment. This document is available on the Citrix Web site.
- *Common Criteria Security Target for Citrix XenServer 6.0.2 Platinum Edition.* Describes the Target of Evaluation, which details assumptions such as the physical environment and the rights and assumptions

concerning the administrators. This document is available only on the Citrix Web site.

CHAPTER 2

Planning for Citrix NetScaler Deployment

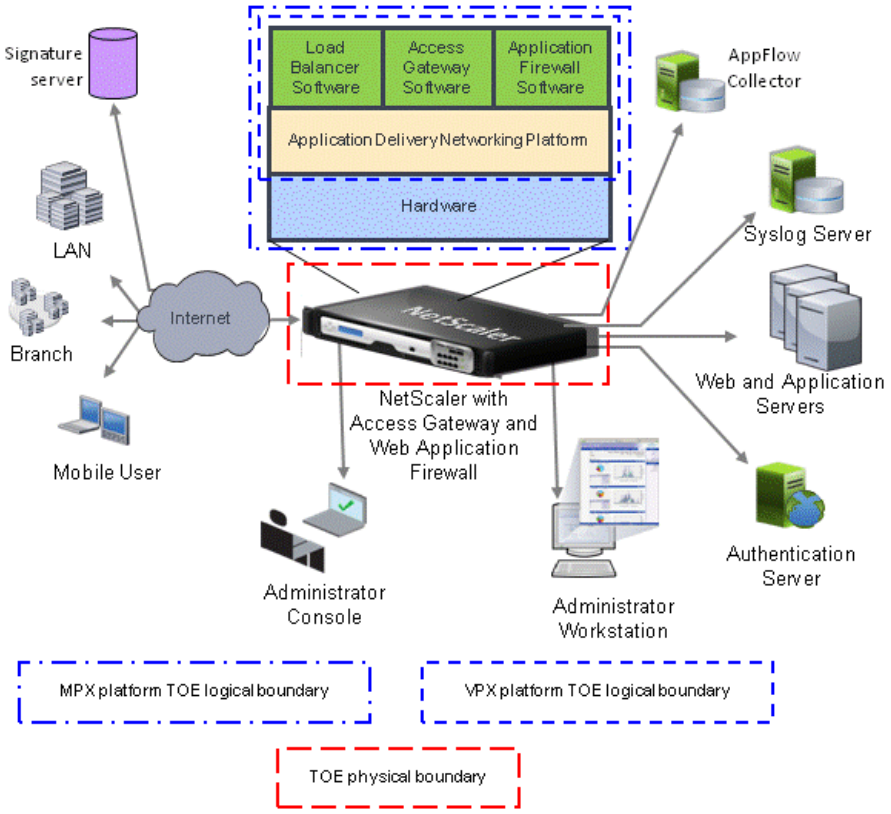
Overview

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

Common Criteria Evaluated Deployment

The NetScaler appliance is deployed between a Local Area Network (LAN) and a Wide Area Network (WAN), such as a Corporate Office Network and the Internet. Privileged, competent users administer this TOE.

The following figure shows the detailed deployment configuration of the TOE.



NetScaler optimizes delivery of applications over the Internet and private networks, combining application-level security and traffic management into 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.
- **Application Firewall**. Prevents security breaches, data loss, and possible unauthorized modifications to Web sites that access sensitive business or customer information. It accomplishes this by filtering both requests and

responses, examining them for evidence of malicious activity and blocking those that exhibit it.

- **Access Gateway**. Provides administrators granular application-level policy and action controls to secure access to applications and data while allowing users to work from anywhere.
- **MPX hardware platforms**. The hardware platforms available for the evaluated deployment are: MPX 5500, MPX 5650, MPX 5750, MPX 8200, MPX 8400, MPX 8600, MPX 8800, MPX 10500, MPX 12500, MPX 15500, MPX 17500, MPX 19500, MPX 9700-FIPS, MPX 10500-FIPS, MPX 12500-FIPS, MPX 15500-FIPS, MPX 11500, MPX 13500, MPX 14500, MPX 16500, MPX 18500, MPX 20500, MPX 17550, MPX 19550, MPX 20550, MPX 21550, and MPX 21500. For more information on the hardware platforms, see chapter “Introduction to the Hardware Platforms” in the *Citrix NetScaler Hardware Installation and Setup Guide*.
- **NetScaler VPX running on XenServer 6.0.2**. A virtual NetScaler appliance that supports all the features of a physical NetScaler, except interface-related events and tagged VLANs. The VPX versions available for the evaluated deployment are: VPX 10, 200, 1000, and 3000. To run the Common Criteria certified NetScaler VPX, you need the evaluated deployment of XenServer 6.0.2. For information on the evaluated XenServer 6.0.2, see the *Common Criteria Evaluated Configuration Guide for Citrix XenServer 6.0.2, Platinum Edition*.

Environment Assumptions

The following assumptions are made regarding the 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.
- 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 subjects 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 and are assumed to possess basic skill level, limited resources to alter TOE configuration settings or parameters, and no physical access to the TOE.
- The installer of the TOE is familiar with the documents listed in "Citrix NetScaler Documentation," on page 2.

NetScaler VPX Requirements

To install NetScaler VPX on XenServer, you must first install XenServer on a machine with adequate system resources. To perform the NetScaler VPX installation, you use Citrix XenCenter, which must be installed on a remote machine that can connect to the XenServer host through the network. Before you install NetScaler VPX, you should create virtual hardware components on XenServer and allocate them to NetScaler VPX by using XenCenter.

XenServer Hardware Requirements

For information on the evaluated system requirements for XenServer, see the *Common Criteria Evaluated Configuration Guide for Citrix XenServer 6.0.2, Platinum Edition*.

XenCenter System Requirements

XenCenter is a Windows client application. It cannot run on the same machine as the XenServer host. The following table describes the minimum system requirements.

Component	Requirement
Operating System	Windows XP, Windows Server 2003, Windows Vista, or Windows 7
.NET framework	Version 2.0 or later
CPU	750 megahertz (MHz) Recommended: 1 gigahertz (GHz) or faster
RAM	1 GB Recommended: 2 GB
Network Interface Card (NIC)	100 megabits per second (Mbps) or faster NIC

For XenCenter installation and configuration instructions, see the *Common Criteria Evaluated Configuration Guide for Citrix XenServer 6.0.2, Platinum Edition*.

External Software and Hardware Requirements

The following table describes the external software and hardware requirements for the TOE.

Category	Requirements
Management workstation	Windows XP Professional or Windows 7 Professional with SSH client installed
Client workstations	Windows XP Professional or Windows 7 Professional with Java Runtime version 6
Backend servers for load balancing	--
Authentication server	--
Syslog server	--

CHAPTER 3

Installing Citrix NetScaler

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 the software installed. This chapter further explains how to install NetScaler VPX on the XenServer evaluated deployment.

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 7 and the server rack is in place according to 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. To complete the installation, you turn on the appliance. Be sure to observe the cautions and warnings listed with the installation instructions.

Note that the Common Criteria requirements must be applied before you start using the NetScaler appliance. For information on the Common Criteria requirements, see chapter 2 "Planning for Citrix NetScaler Deployment," on page 5 and chapter 5 "Securing the Deployment," on page 57.

For instructions on installing the NetScaler Hardware, see chapters "Preparing for Installation" and "Installing the Hardware" in the *Citrix NetScaler Hardware Installation and Setup Guide*.

Verifying the Hardware

You can ensure 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 that the listed serial number matches the serial number of the enclosed hardware. You can also examine the hardware to verify that the tamper seals are not damaged.

You can be sure that a product is authentic by comparing the tracking number on the package to the shipping number provided by Citrix. All placed orders are confirmed through an e-mail to the e-mail, which includes the shipping carrier, tracking number, purchase order number, and a list of shipped items (including all corresponding serial numbers). You can also view the status of an order by logging onto the Citrix online customer support portal at http://support.citrix.com.

Verifying the Common Criteria Software Version Installed

The hardware that is delivered comes with the latest version of the product software already installed, which may or may not be the Common Criteria-certified version of the TOE software. You can verify the software version installed by accessing the NetScaler CLI.

For initial access, all NetScaler appliances ship with the default NetScaler IP address (NSIP) of 192.168.100.1 and default subnet mask of 255.255.0.0. You can assign a new NSIP and an associated subnet mask during initial configuration.

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 will be marked on the download site. When making an SSL connection to the Citrix site, you should confirm that the URL in the browser is under https://www.citrix.com/.

If the correct version is not installed, you can upgrade to the common criteria-certified version of the software.

To download the correct Common Criteria version

1. Go to www.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, for example, NetScaler 10.
5. Under **Results for**, in **Firmware**, click the relevant Common Criteria build, for example, Release 10 Build 74.4 (Common Criteria Build).
6. In the build page, scroll to the bottom of the page and click **Download**.

7. In the **End-User License Agreement** pane, click **Yes** to accept the agreement, and then follow the instructions in the download pane.

Verifying the Licensed Features

Before using a feature, make sure that your license supports the feature.

To verify the licensed features by using the NetScaler command line

1. Open an SSH connection to the NetScaler by using an SSH client, such as PuTTY.
2. Log on to the NetScaler by using the administrator credentials.
3. At the command prompt, enter the `sh ns license` command to display the features supported by the license.

Example

```
sh ns license
    License status:
        Load Balancing: YES
        SSL VPN: YES
        .......
        Application Firewall: YES
    Done
```

Physical Deployment Modes

You need to configure the NetScaler in the 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 NetScaler is placed between the clients and the servers. The NetScaler has a separate network interface to each client network and a separate network interface to each server network. The NetScaler and the servers exist on different subnets in this configuration.

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

Setting up a Simple Two-Arm Multiple Subnet Topology

In this topology, the NetScaler sits between the clients and the servers, with a vserver configured to handle the client requests. This configuration is used when the clients and servers reside on different subnets, the clients on public subnets and the servers on private subnets.

For example, consider a NetScaler deployed in two-arm mode for managing servers S1, S2, and S3, with a vserver of type HTTP configured on the NetScaler, and with HTTP services running on the servers. The servers are on a private subnet and a SNIP is configured on the NetScaler to communicate with the servers. The Use Source IP (USIP) option must be enabled on the NetScaler so that it uses the SNIP instead of the MIP.

For information on the configuration steps, see section “Setting up Common Two-Arm Topologies” in the *Citrix NetScaler Getting Started Guide*.

Setting up a Simple Two-Arm Transparent Topology

Use transparent mode if the clients need to access the servers directly, with no intervening vserver. The server IP addresses must be public because the client needs them.

For information on the configuration steps, see section “Setting up Common Two-Arm Topologies” in the *Citrix NetScaler Getting Started Guide*.

Upgrading the NetScaler Software Version

You can either 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. Upgrades or downgrades to the appropriate version are available on the Citrix Web site at http://support.citrix.com

Verifying the Integrity of the Downloaded Software

MD5 hashes are available via secure download from the Citrix Web site using SSL with every package. A customer can verify the integrity of a downloaded package by comparing the MD5 hash with a locally generated MD5 hash of the downloaded package.

A customer can generate the MD5 hash of the downloaded package using a program like md5sum on UNIX systems.

Example

```
$ md5sum build-10-74.4_nc.tgz
de0ff39959440be032336eefbb50f884 build-10.0-74.4_nc.tgz
$
```

The generated MD5 (in this case de0ff39959440be032336eefbb50f884) should match with the one provided on the Citrix SSL site.

Upgrading the NetScaler Software

For instructions on upgrading the NetScaler software, see chapter "Upgrading or Downgrading the System Software" in the *Citrix NetScaler Migration Guide*.

Reverting the Settings to Factory Defaults

You can clear the configuration on your NetScaler 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. This is done to ensure that the system does not lose network connectivity.

Installing the NetScaler VPX Version

To run the Common Criteria certified NetScaler VPX, you need the evaluated deployment of XenServer 6.0.2. For information on the evaluated XenServer 6.0.2, see the *Common Criteria Evaluated Configuration Guide for Citrix XenServer 6.0.2, Platinum Edition*.

After you have installed and configured the Common Criteria evaluated version of XenServer and XenCenter, you can use XenCenter to install NetScaler virtual appliance on XenServer.

You need to configure the NetScaler VPX in the two-arm mode to comply with the common criteria evaluated configuration. For information on the two-arm mode, see "Physical Deployment Modes," on page 13.

For your VPX installation, ensure that you create two virtual network interfaces (VIFs), each bound to a corresponding PIF representing one of the physical NICs for the two-arm configuration discussed in “Physical Deployment Modes,” on page 13) for the common criteria evaluated configuration.

To verify the PIFs, run the following command:

```
xe pif-list
```

To create the VIFs, see http://docs.vmd.citrix.com/XenServer/6.0.2/1.0/en_gb/reference.html#networking-standalone_host_config-creating_networks

To verify the VIFs, run the following command:

```
xe vm-vif-list “vm=<NAME or UUID>”
```

Example

```
xe vm-vif-list “vm=NetScaler Virtual Appliance”
```

You can download the appropriate NetScaler VPX version from the Citrix Web site at http://support.citrix.com

Note that the evaluated configuration assumes that only one VM is present on the platform.

To install NetScaler virtual appliances on XenServer by using XenCenter

4. After logging on to the XenServer, on the **VM** menu, click **Import**.
5. In the **Import** dialog box, in **Import file name**, browse to the location at which you saved the NetScaler VPX .xva image file. Make sure that the **Exported VM** option is selected, and then click **Next**.
   Note that this step replaces the installation of Windows VM that is done for the evaluated configuration of XenServer.
6. Select the XenServer on which you want to install the virtual appliance, and then click **Next**.
7. Select the NFS-based storage repository in which to store the virtual appliance, and then click **Import** to begin the import process.
8. You can add, modify, or delete virtual network interfaces (VIFs) as required. As noted above, you must add two virtual network interfaces (each bound to a corresponding PIF representing one of the physical NICs for the two-arm configuration discussed in) for the common criteria evaluated configuration. When finished, click **Next**.
9. Click **Finish** to complete the import process.

Note: To view the status of the import process, click the **Log** tab.

Verifying the Common Criteria Software Version Installed

You can verify the software version installed by accessing the NetScaler CLI.

For initial access, use the default NetScaler IP address (NSIP) of 192.168.100.1 and default subnet mask of 255.255.0.0. You can assign a new NSIP and an associated subnet mask during initial configuration.

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 will be marked on the download site. When making an SSL connection to the Citrix site, you should confirm that the URL in the browser is under https://www.citrix.com/.

If the correct version is not installed, you can upgrade to the common criteria-certified version of the software.

To download or verify the correct Common Criteria version

1. Go to www.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, for example, NetScaler 10.
5. Under **Results for**, in **Firmware**, click the relevant Common Criteria build, for example, Release 10 Build 74.4 (Common Criteria Build).
6. In the build page, scroll to the bottom of the page and click **Download**.
7. In the **End-User License Agreement** pane, click **Yes** to accept the agreement, and then follow the instructions in the download pane.

Setting Up the Initial Configuration by Using the NetScaler VPX Console

Your first task after installing a NetScaler virtual appliance on a virtualization host is to use the NetScaler VPX console in the XenCenter client to configure the following initial settings.

- **NetScaler IP address (NSIP)**. The IP address at which you access a NetScaler or a NetScaler virtual appliance for management purposes. A physical NetScaler or virtual appliance can have only one NSIP. You must

specify this IP address when you configure the virtual appliance for the first time. You cannot remove an NSIP address.

- **Netmask**. The subnet mask associated with the NSIP address.
- **Default Gateway**. You must add a default gateway on the virtual appliance if you want access it through SSH from an administrative workstation or laptop that is on a different network.

To configure the initial settings on the virtual appliance through the VPX Console by using the management application

1. Connect to the XenServer on which the virtual appliance is installed by using XenCenter.
2. In the details pane, on the **Console** tab, log on to the virtual appliance by using the administrator credentials.
3. At the prompts, enter the NSIP address, subnet mask, and default gateway, and then save the configuration.

After you have set up an initial configuration through the NetScaler VPX Console in the management application, you can use the NetScaler command line interface to complete the configuration or to change the initial settings.

CHAPTER 4

Configuring Citrix NetScaler

Performing Initial Configuration

After you have installed your appliance in a rack, you are ready to perform the initial configuration.

When you first install the appliance, you can configure the initial settings by using the serial console. With 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.

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 into your appliance.
2. Run the vt100 terminal emulation program of your choice on your computer to connect to the appliance.
    - For Microsoft Windows, you can use a terminal emulation client such as PuTTy.
    - For Apple Macintosh OSX, you can 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, you can 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 you with the administrator credentials.
5. At the prompt, type **`config ns`** to run the NetScaler configuration script.
6. To complete the initial configuration of your appliance, follow the prompts.

Note: To prevent an attacker from breaching your ability to send packets to the appliance, choose a non-routable IP address on your organization's LAN as your appliance IP address.

You can replace steps 5 and 6 with the following NetScaler commands. At the NetScaler command prompt, type:

```
set ns config -ipaddress <IPAddress> -netmask <subnetMask>
add ns ip <IPAddress> <subnetMask> -type <type>
add route <network> <subnetMask> <gateway>
set system user <userName> <password>
save ns config
reboot
```

Example

```
set ns config -ipaddress 10.102.29.60 -netmask 255.255.255.0
add ns ip 10.102.29.61 255.255.255.0 -type snip
add route 0.0.0.0 0.0.0.0 10.102.29.1
set system user nsroot administrator
save ns config
reboot
```

Note: The management access through NSIP should not be publicly accessible and proper security measures should be in place to authorize users accessing NSIP for configuring the TOE. For more information, see "User Access Control," on page 58.

Note: Dynamic routing must always be enabled on the NSIP address. It cannot be disabled. The CLI however, inappropriately displays the "Done" message after you execute the command to disable dynamic routing.

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 by reverting the settings to factory defaults (see "Reverting the Settings to Factory Defaults," on page 15) and then change it.

To change the nsroot password

At the NetScaler command prompt, type

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

Disabling the Management GUI

To conform to the Common Criteria Evaluated deployment, you must disable the GUI.

To disable the GUI

At the NetScaler command prompt, type

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

Configuring System Settings

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

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 time zone for your NetScaler

At the NetScaler command prompt, type:

```
set ns config -timezone <timezone>
```

Example

```
set ns config -timezone GMT-07:00-PDT- America/Dawson
```

To set the current date and time on your NetScaler

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** denotes the month of the year
- **dd** denotes the day of the month
- **HH** is the hour of the day
- **MM** is the minute of the hour
- **ss** denotes the second of the minute

Example

To set August 23, 2010, 15 hours, 30 minutes, and 40 seconds, type:

```
date 201008231515.40
```

To set only the time on your NetScaler

At the NetScaler command prompt, type:

```
shell
```

At the shell prompt, type:

```
date <HHMM.ss>
```

To verify the date and time of your NetScaler

At the NetScaler command prompt, type:

```
shell
```

```
date
```

Configuring Administrator 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.

You must log on as an administrator to configure users, groups, and command policies. The default NetScaler administrator user name is nsroot and has superuser privileges.

Creating an Administrator User Account

You can either use the nsroot administrator account or create a new administrator account and assign various command policies to those accounts.

To create a user account by using the NetScaler command line

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 Admin
Enter password:
 Done
> sh system user
1)      User name: nsroot
2)      User name: user1
3)      User name: Admin
 Done
```

Note: You can also create a group and assign the user to that group and bind the command policies to the group.

Binding Command Policies to the Administrator User Account

Command policies regulate which commands, command groups, vservers, and other entities that 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.

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 would be 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 the following table.

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.

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

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
```

Note that in the above example, “1” is the highest priority. In the NetScaler operating system, policy priorities work in reverse order — the higher the number, the lower the priority.

Access Control Matrix for the Evaluated Deployment of the TOE

Role	read-only	operator	network	superuser	custom-defined role
Security Attributes					
Administrator roles				create, delete, query, modify	as defined
Administrator groups				create, delete, query, modify	as defined
Role policies				create, delete, query, modify	as defined
Role priorities				create, delete, query, modify	as defined
VPN user groups	query	query, modify	create, delete, query, modify	create, delete, query, modify	as defined
VPN user permissions	query	query, modify	create, delete, query, modify	create, delete, query, modify	as defined
Web Application firewall permissions	query	query, modify	create, delete, query, modify	create, delete, query, modify	as defined
Attack Signatures			import, delete	import, delete	as defined
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
Web Application firewall	Query the behavior of	Modify the behavior of	determine the behavior of, modify the behavior of	determine the behavior of, modify the behavior of	as defined

Role	read-only	operator	network	superuser	custom-defined role
Audit	determine the behavior of	determine the behavior of	determine the behavior of	determine the behavior of, modify the behavior of	as defined
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
Administrator accounts				create, delete, query, modify	as defined
VPN user accounts	query	create, delete, query, modify	create, delete, query, modify	create, delete, query, modify	as defined
Web Application firewall permissions			create, delete, query, modify	create, delete, query, modify	as defined
Attack Signatures	query for stats	query for stats	query for stats and logs	query for stats and logs	as defined

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 features of the NetScaler.

Setting Up Basic Load Balancing

The load balancing feature distributes user requests for Web site 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.

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 address (VIP) is a public IP address. If the application is accessible only from 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 time-out, 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
```

Parameters for configuring a server object

Creating a Service

Before you create a service, you need to understand the different service types and how each is used. The types of services supported on the NetScaler appliance are: HTTP, SSL, FTP, TCP, and so on.

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 places any that fail to respond to monitoring probes (called health checks) back in 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
```

Configuring Access Gateway

Access Gateway provides administrators granular application-level policy and action controls to secure access to applications and data while allowing users to work from anywhere. 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.

Enabling Access Gateway

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

To enable Access Gateway by using the command line

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

```
enable ns feature SSLVPN
show ns feature
```

Creating Local Users

You can create user accounts locally on the Access Gateway to supplement the users 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.

If you are using local authentication, create users and then add them to groups that are created on the Access 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.

To create local users

At the NetScaler command prompt, type

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

Example:

```
add aaa user 123 -password 123
```

Providing Access to Internal Resources

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

Configuring Authentication Policies

When users log on to the Access Gateway, they are authenticated by a policy. The policy defines the authentication type. A single authentication policy can be used for simple authentication needs. Multiple policies can also be configured and bound to create a detailed authentication procedure. An authentication policy is comprised 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.

Authentication polices are validated against those bound to the virtual server first and then globally. 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>]
```

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

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 ldap_pol_180 ns_true ldap_act_180
```

To bind an authentication policy to 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
```

Configuring Authorization Polices

When configuring an authorization policy, you can set it to ALLOW or DENY access to network resources in the internal network. For example, to allow users access to the 10.3.3.0 network, use the following expression:

```
REQ.IP.DESTIP==10.3.3.0 -netmask 255.255.0.0
```

Authorization policies are applied to users and groups. After a user is authenticated, the Access Gateway performs a group authorization check by obtaining the user's group information from either an LDAP server, a RADIUS server, or an SAML Identity Provider. If group information is available for the user, the Access Gateway checks the network resources allowed for the group.

Note: The use of TACACS+ server is not included in the evaluated configuration.

To control which resources clients have access to, you must create authorization policies and bind them to users or groups.

Authorization policies are applied first to users and then to groups. When a user logs on, the Access Gateway checks to see if an authorization policy is bound to the user. If an authorization policy is not bound to the user, the Access Gateway checks for group authorization policies. If none are found at the group level, the default global authorization policy is applied.

You can set the priority of an authorization policy. For example, if you have configured an authorization policy for a group and for a user, you can set the priority so that the Access Gateway checks the group policy before checking the user policy.

A numeric value is assigned to the priority. Priority numbers start at zero. A lower priority number gives the authorization policy higher precedence. For example, you can set the group priority to zero and the user priority to one for the Access Gateway to check the group authorization policy first.

Note: If an authorization policy that is set to DENY access has the same priority as the authorization policy set to ALLOW access, and if both are bound to the same user, the policy with DENY access gets precedence.

To create an authorization policy

At the NetScaler command prompt, type

```
add authorization policy <name> <rule> <action>
```

Example:

```
add authorization policy VIPDESK "REQ.IP.DESTIP == 10.199.0.0 -
netmask 255.255.0.0 && (REQ.TCP.DESTPORT == 1494 ||
REQ.TCP.DESTPORT == 2598 || REQ.TCP.DESTPORT == 80 ||
REQ.TCP.DESTPORT == 443)" ALLOW
```

To bind an authorization policy to a user or group

At the NetScaler command prompt, type

```
bind aaa user <userName> [-policy <string> [-priority
<positive_integer>]]
```

Example:

```
bind aaa user admin_user/admin_group -policy VIPDESK -priority 3
```

To bind an authorization policy to a user

At the NetScaler command prompt, type

```
bind aaa user admin -policy VIPDESK -priority 1
```

To bind an authorization policy to a group

At the NetScaler command prompt, type

```
bind aaa user admin_group -policy VIPDESK -priority 0
```

Configuring LDAP Authentication

You can configure the Access Gateway 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 Access Gateway. The characters and case must also be the same.

By default, LDAP authentication is secure using SSL/TLS.

To configure LDAP authentication

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>] [-
secType <secType>] [-passwdChange ( ENABLED | DISABLED )]
```

Note: If you select Plaintext or TLS for security, use port number 389. If you select SSL, use port number 636.

If you select PLAINTEXT as the security type, allowing users to change their passwords is not supported.

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

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 -
secType SSL -passwdChange ENABLED

add authentication ldapPolicy ldap_pol_180 ns_true ldap_act_180
```

Configuring RADIUS Authentication

You can configure the Access Gateway to authenticate user access with one or more RADIUS servers. If you are using RSA SecureID, SafeWord, or Gemalto Protiva products, each of these is configured using a RADIUS server.

To configure RADIUS authentication

At the NetScaler command prompt, type

```
add authentication radiusAction <name> {-serverIP
<ip_addr|ipv6_addr|*>} [-serverPort <port>] {-radKey } [-
radAttributeType <positive_integer>] [-ipAttributeType
<positive_integer>]

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

Example:

```
add authentication radiusAction freerad1 -serverIP 10.199.x.x -
serverPort 1812 -radKey xxxx -radAttributeType 11 -ipAttributeType
8

add authentication radiusPolicy freerad ns_true freerad1
```

After the RADIUS server settings are configured on the Access Gateway, bind the policy to make it active. This can be done either globally or to a virtual server. For more information about binding authentication policies, see “Configuring Authentication Policies,” on page 34.

Configuring SAML Authentication

You can configure SAML (Security Assertion Markup Language) authentication to enable single sign-on (SSO) on your NetScaler appliance for users who log on through a third party authentication server that supports SAML.

To configure SAML authentication

At the NetScaler command prompt, type

```
add authentication samlAction <name> [-samlIdPCertName <string>] [-
samlSigningCertName <string>][-samlRedirectUrl <string>][-
samlUserField<string> ][-samlRejectUnsignedAssertion ( ON )] [-
samlIssuerName <string>]
```

Setting Up Authentication Using Digital Certificates

Users logging on to an Access Gateway virtual server can also be authenticated based on the attributes of the client certificate that is presented to the virtual server. This can also be used with another authentication type, such as LDAP or RADIUS, to provide double-source authentication.

To authenticate users based on the client-side certificate attributes, client authentication should be enabled on the virtual server and the client certificate should be requested. A root certificate must be bound to the virtual server on the Access Gateway.

When users log on to the Access Gateway virtual server, after authentication, the user name information is extracted from the specified field of the certificate. Typically, this field is Subject:CN. If the user name is extracted successfully, the user is then authenticated. If the user does not provide a valid certificate during the SSL handshake or if the user name extraction fails, the authentication fails.

You can authenticate users based on the client certificate by setting the default authentication type to use the client certificate. You can also create a certificate action that defines what is to be done during the authentication based on a client SSL certificate.

To set up authentication using digital certificates

At the NetScaler command prompt, type

1. Create an RSA key and a Certificate Signing Request (CSR)

```
create rsakey 1024 key1024
create certreq req1024 -keyfile key1024
     Country Name (2 letter ISO code) :US
     State or Province Name (full name) :CA
     Locality Name (eg, city) :Santa
     Organization Name (eg, company) :dnpg
     Organization Unit Name (eg, section) :dnpr
     Common Name (eg, Domain Name) :cert1024.ctxtd.com
     Email Address :administrator@ctxtd.com
     A challenge password (min 4 letter) :nsroot
     An optional company name :citrix
```

2. Using the certkey req1024, get certificate from Certificate Authority and upload on NetScaler `/var/nsconfig/ssl as cert1024.cer`

```
add certkey cert1024-ck -cert cert1024.cer -key key1024.key
```

3. Bind this certkey to VPN vserver

```
bind certkey cert1024 cert1024-certck
```

Configuring Access Control Based on Certain Parameters

You can configure Access Gateway to configure access control based on username, source IP, certificate attributes, and date and time.

To configure access control

1. Add local users and enter passwords

```
add aaa user user1 -password
add aaa user user2 -password
```

2. Add policy expression to only grant access between particular times and dates.

```
add policy expression time_exp “TIME BETWEEN
\’2009-12-18-14:25:44GMT-2009-12-21-14:25:56GMT\’”
```

3. Add policy to check for the source IP.

```
add policy expression src_ip_expr “REQ.IP.SOURCEIP ==
```

```
10.102.119.0 -netmask 255.255.255.0”
```

4. Create a compound expression that checks if the above two criteria are satisfied.

   ```
   add policy expression compound_exp1 “src_ip_expr && time_exp”
   ```

5. Bind the expression to a local policy.

   ```
   add authentication localpolicy local1 compound_exp1
   ```

6. Add an SSL VPN type vserver and bind a certificate key pair to it.

   ```
   add vpn vserver dummy SSL 10.102.6.92 443
   add certkey <certkey name> -cert < path to cert> -key <path to
   key >
   bind ssl vserver dummy -certkeyName rsa_root_cert -CA
   add ssl certKey rsa_srvr_cert -cert /nsconfig/ssl/
   rsa_srvr_cert.pem -key /nsconfig/ssl/rsa_srvr_key.pem
   bind ssl vserver dummy -certkeyName rsa_srvr_cert
   ```

7. Bind the policy to the vserver.

   ```
   bind vpn vserver dummy -policy local1
   ```

8. Set the client type to plug-in and split tunneling to off.

   ```
   set vpn parameter -transparentInterception OFF
   set vpn para -splittunnel OFF
   ```

Configuring Application Firewall

The Citrix Application Firewall prevents security breaches, data loss, and possible unauthorized modifications to Web sites that access sensitive business or customer information. It accomplishes this by filtering both requests and responses, examining them for evidence of malicious activity and blocking those that exhibit it.

To use the Application Firewall, you must configure at least one profile to tell it what to do with the connections it filters, one policy to tell it which connections to filter, and then associate the profile with the policy.

To perform a simple configuration, you need to do the following:

- Enable the Application Firewall feature
- Create profile
- Create a policy
- Bind the profile to the policy

Enabling Application Firewall

To enable Application Firewall using the NetScaler command line

Type the following command at the prompt:

```
enable ns feature ApplicationFirewall
```

Creating and Configuring a Profile

A profile is a collection of security settings that are used to protect specific types of web content or specific parts of your Web site or application. The Application Firewall has two categories of profile: built-in profiles and user-created profiles. Built-in profiles provide out-of-the-box tools for handling simple content that can either be passed on without further filtering, or blocked without further filtering. User-created profiles provide tools for handling more complex content that cannot simply be passed on or blocked without filtering.

To create and configure an HTML profile using the NetScaler command line

At the NetScaler command prompt, type the following commands:

```
add appfw profile <name> -defaults basic
set appfw profile <name> -type ( HTML | XML | HTML XML )
save ns config
```

Parameters for Creating and Configuring a New Profile

Parameter	Description
Name (<name>)	A name for the profile. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) symbols. You should choose a name that will make it easy for others to tell what type of content this profile was created to protect.
Defaults (-defaults (basic | advanced))	You can choose one of two default configurations when you create a profile: Basic or Advanced. A profile created with basic defaults should protect most Web sites while requiring little additional configuration. A profile created with advanced defaults is intended to protect more complex Web sites requiring additional configuration.
Type (-type (HTML | XML | HTML XML))	You can create three types of profile: HTML, XML, or Web 2.0. To designate a Web 2.0 profile, you type “HTML XML” after the -type parameter.

Creating and Configuring Application Firewall Policies

When configuring a new Application Firewall, after you create your profiles, you must create a policy for each profile. Policies are used to determine whether a request or a response meets specific criteria. When a request or response meets a policy's criteria, or matches a policy, the Application Firewall then filters the request or response using the associated profile.

A policy is a set of parameters that defines a particular type of web content or particular part of a Web site. The Application Firewall uses policies to determine which profile to use when filtering specific requests or responses.

You create and configure Application Firewall policies by using the NetScaler command line. The main task in configuring a policy is the creation of the rule, which consists of one or more classic or advanced expressions.

The following table describes the advanced expressions you can use while configuring application firewall policies.

Advanced Expressions

Rules	**Policies**
Destination IP address	add appfw policy po1_1_adv "CLIENT.IP.DST.EQ(<ip_address>)" APPFW_BLOCK
HTTP method used in the connection request	add appfw policy po1_2_adv "HTTP.REQ.METHOD.EQ(GET)" APPFW_BLOCK
URL tokens in the HTTP header	add appfw policy po1_3_adv "HTTP.REQ.URL.PATH_AND_QUERY.CONTAINS(\ "abc\")" APPFW_BLOCK
HTTP version of the connection	add appfw policy po1_4_adv "HTTP.REQ.VERSION.EQ(\"HTTP/1.1\")" APPFW_BLOCK
HTTP header contents (including source and destination IP addresses)	add appfw policy po1_5_adv "HTTP.REQ.HEADER(\"Header1\").CONTAINS(\"abc \")" APPFW_BLOCK
Length of the contents of the URL header	add appfw policy po1_6_adv "HTTP.REQ.URL.LENGTH.GE(10)" APPFW_BLOCK
URL header query	add appfw policy po1_7_adv "HTTP.REQ.URL.QUERY.CONTAINS(\"content\")" APPFW_BLOCK
Length of the URL header query	add appfw policy po1_8_adv "HTTP.REQ.URL.QUERY.LENGTH.GE(10)" APPFW_BLOCK

To create a policy by using the NetScaler command line

1. At the NetScaler command prompt, type the following command:

   ```
   add appfw policy <name> "<rule>" <profile>
   ```

   Make the following substitutions:

   - For <name>, substitute a name for the policy. The name can begin with a letter, number, or the underscore symbol, and can consist of from one to 127 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), and underscore (_) symbols. You should choose a name that will make it easy for others to tell what type of content this policy was created to detect.
   - For <rule>, substitute a NetScaler expression that defines the Web content you want to filter using this policy.

     Note: You can create a rule using either classic or advanced expressions using this command. You simply type the appropriate expressions and enclose them all in double straight quotation marks.

     - To create a classic expression, follow this syntax:

       ```
       "<flow type>.<protocol>.<qualifier>.<operator>
       [.<value>][.<header name>]"
       ```

       For each of the designated elements, substitute the appropriate value. The following list describes each element and provides the correct values or explains how to determine what the correct values are:

- **Flow type.** Whether the policy filters requests or responses. The flow type is always `REQ` for Application Firewall policies because the Application Firewall filters each request and its associated response as a unit.
- **Protocol.** The protocol of the connections that this policy will filter. For Application Firewall policies, this should be `HTTP`.
- **Qualifier.** The aspect of the protocol that the policy should consider. The following values are valid:
  - `METHOD`. The HTTP method used in the request.
  - `URL`. The contents of the URL header.
  - `URLTOKENS`. The URL tokens in the HTTP header.
  - `VERSION`. The HTTP version of the connection.
  - `HEADER`. The header portion of the HTTP request.
  - `URLLEN`. The length of the contents of the URL header.
  - `URLQUERY`. The query portion of the contents of the URL header.
  - `URLQUERYLEN`. The length of the query portion of the URL header.

- **Operator.** The symbol that describes the condition you want the Application Firewall to test. Depending on which qualifier you chose, two or more operators may be valid. The complete list of valid operators is:
  - `==`. Matches the following text string exactly.
  - `!=`. Does not match the following text string.
  - `>`. Is greater than the following integer.
  - `CONTAINS`. Contains the following text string.
  - `CONTENTS`. The contents of the designated header, URL, or URL query.
  - `EXISTS`. The specified header or query exists.
  - `NOTCONTAINS`. Does not contain the following text string.
  - `NOTEXISTS`. The specified header or query does not exist.
- **Value.** If you chose the equals (`==`), does not equal (`!=`), is greater than (`>`), `CONTAINS`, or `NOTCONTAINS` operators, you must include the string or value that the Application Firewall should test the qualifier against.

  For example, if you are testing the URL header to see if it contains the subdomain `shopping.example.com`, you type the string `shopping.example.com`.
- **Header Name.** If you type `HEADER` as your Protocol, you must also include the name of the header that contains the attribute or string you want the Application Firewall to use for the test.

  For example, the following expression tells the Application Firewall to check all requests to see that the URL header exists.

  ```
  "REQ.HTTP.HEADER URL EXISTS"
  ```

  Since all requests by definition have a URL header, this expression matches all requests.
- For `<profile>`, substitute the name of the profile you want to associate with this policy.

- To create an advanced expression, follow this syntax:

```
"<prefix>.<term>[.<term2>[.<term3>[...]]]"
```

For more information about advanced expression syntax, see the *Citrix NetScaler Policy Configuration and Reference Guide*.

2. Enter the following command to save your configuration.

   ```
   save ns config
   ```

3. Enter the following command to confirm that your policy was correctly created.

   ```
   show appfw policy <name>
   ```

   For <name>, substitute the name of the policy you created.

   - If your policy was correctly created, you do not need to do anything further.
   - If your policy was created with the wrong name or associated with the wrong profile, you modify it by deleting it as shown below, and then recreating it as described in this procedure.

     ```
     rm appfw policy <name>
     ```

     If your policy was created with a flawed regular expression, you modify it by issuing the following command.

     ```
     set appfw policy <name> "<rule>" <profile>
     ```

     You substitute values for <name>, <rule>, and <profile> as described in the first step of this procedure.

Globally Binding a Policy

To put a policy and its associated profile into effect, you globally bind the policy and assign it a priority. The priority you assign determines the order in which your policies are evaluated. Set the priorities to evaluate the most specific policy first, and then more general policies in descending order, finishing with the most general policy.

Note: All Application Firewall policies that are bound to global or to a bind point must use the same type of syntax: either classic or advanced syntax, but not a mixture of both. You can bind only one type of policy at a time.

To globally bind a policy by using the NetScaler command line

1. At the NetScaler command prompt, type the following command to globally bind the policy.

   ```
   > bind appfw global <policy> <priority>
   ```

For <policy>, substitute the name of the policy you want to globally bind. For <priority>, substitute a positive integer that represents the priority of this policy.

In the NetScaler operating system, policy priorities work in reverse order—the higher the number, the lower the priority. The minimum value allowed for priority is 1, which means the highest priority. The maximum value allowed is 2147483647, which means the lowest priority. For example, if you have three policies with priorities of 10, 100, and 1000, the policy assigned a priority of 10 is performed first, then the policy assigned a priority of 100, and finally the policy assigned an order of 1000. Since the Application Firewall implements only the first policy that a request matches, not any additional policies that it might also match, policy priority is important to getting the results you intend.

Note: You cannot bind two application firewall policies with the same priority.

---

2. Enter the following command to save your configuration.

```
> save ns config
```

Enabling the Signatures Feature

The application firewall signatures function provides specific, configurable rules that protect your web sites against known attacks. A signature represents a pattern that is a component of a known attack on an operating system, a web server, a web site, an XML-based web service, or any other server that is connected to a web site or web service. A signature can consist of a literal string or a PCRE-compliant regular expression.

To enable the signatures feature, you need to perform the following tasks:

- Download the default signature file
- Make a copy of the signature file and provide a meaningful name to it
- Edit the XML file to enable the required signatures
- Import the XML configuration to your NetScaler appliance
- Set the target profile to use this signature object

Downloading the Signature File

Download the default signature file from the Citrix support site at: http://www.citrix.com/English/ss/downloads/details.asp?downloadId=2309856&productId=21679

Editing the Signature File

You need to edit the XML file to enable the required signatures. The Default Signatures file is structured as described below.

- **File header**. The file header appears as follows:

```
<!--Default SQL/XSS parameters-->
<!--/nsconfig/appfw_customsettings.conf-->
<AppFwCustomSettings>
```

- **SQL Injection section header**. The SQL injection header and opening tag follow the File header:

```
<!--SQL injection parameters-->
<!--SQL delimiter is to be specified as an attribute of
injection node-->
<injection type="SQL" delimiter="not_alphanum">
```

- **SQL Keywords subsection**. The header for the SQL keywords subsection follows immediately after the SQL injection section header. The SQL keywords follow this header. The list varies in length and composition, but each term is enclosed in `<keyword></keyword>` tags. You add SQL keywords to the list by entering each keyword on a separate line and enclosed in the specified tags. The SQL keywords section is terminated with a blank line.

  Following are some of the default SQL keywords, in context:

```
      <!--SQL keywords-->
<keyword>select</keyword>
<keyword>insert</keyword>
...
<keyword>SYS.USER_SYS.PRIVS</keyword>
<keyword>SYS.USER_TAB_PRIVS</keyword>
```

- **SQL Special Strings subsection**. The header for the SQL special characters subsection follows the SQL keywords subsection, and the SQL special characters follow this header. Each special string is on a single line and is enclosed in `<specialstring></specialstring>` tags. You add special strings to the list by entering each string on a separate line and enclosing it in the specified tags. The section is terminated by a blank line, and it is followed by the closing tag for the SQL Injection section.

  The default SQL special strings section appears as follows:

```
      <!--SQL special strings-->
```

```
      <specialstring>'</specialstring>
      <specialstring>\\</specialstring>
      <specialstring>;</specialstring>
</injection>
```

- **Transform Patterns section header**. The Transform Patterns subsection header and opening tags follow the SQL Special Strings subsection ending tag:

```
<transformrules>
      <!--SQL transform patterns-->
<!--Note:
1)This is an ordered match of 'from' patterns
2)Empty tags can be specified to omit matched pattern-->
<transform>
```

- **Transform Patterns subsection**.The Transform Patterns subsection follows the section header, with the section header at the top and a list of transform patterns beneath it. Each transform pattern consists of two lines:
  - The pattern to be transformed, enclosed in `<from></from>` tags.
  - The pattern that replaces the transformed pattern, enclosed in `<to></to>` tags.

  Both sets of patterns and tags are then enclosed in `<transform></tranform>` tags.

  You add transform patterns to the list by entering sets of transformations as shown below. The subsection is terminated by a blank line.

```
<transform>
<from>'</from>
<to>''</to>
</transform>

<transform>
<from>\</from>
<to>\\</to>
</transform>
```

  To delete the transformed pattern from a request entirely, you simply leave the between the `<to></to>` tags empty, as shown below.

```
<transform>
<from>;</from>
```

```
<to></to>
</transform>
```

- **Cross-Site Scripting (XSS) section header**. The XSS section header and opening tags follow the Transform Patterns section ending tag:

```
<!--XSS parameters-->
<xss>
      <allowed>
```

- XSS Allowed Attributes subsection. The XSS allowed attributes subsection follows the XSS section header, with the section header at the top and a list of allowed attributes beneath it. Each allowed tag is on a separate line and is enclosed in `<attribute></attribute>` tags. You add XSS allowed attributes to the list by entering each attribute on a separate line and enclosing it in the specified tags. The subsection is terminated by a blank line, followed by the closing tags for the XSS section, another blank line, and the closing tag for the custom settings file.

  Following are some of the default XSS allowed attributes, in context:

```
      <!--XSS allowed attributes-->
<attribute>abbr</attribute>
<attribute>accesskey</attribute>
...
<attribute>vspace</attribute>
<attribute>width</attribute>
      </allowed>
</xss>
</AppFwCustomSettings>
```

- **XSS Allowed Tags subsection**. The XSS allowed tags subsection follows the XSS allowed attributes subsection, with the section header at the top and a list of allowed tags beneath it. Each allowed tag is on a separate line and is enclosed in `<tag></tag>` tags. You add XSS allowed tags to the list by entering each tag on a separate line and enclosing it in the specified XML tags. The subsection is terminated by a blank line.

  Following are some of the default XSS allowed tags, in context:

```
      !--XSS allowed tags-->
<tag>a</tag>
<tag>address</tag>
<tag>b</tag>
<tag>basefont</tag>
```

```
...
<tag>tr</tag>
<tag>tt</tag>
<tag>u</tag>
<tag>ul</tag>
```

- **XSS Denied Patterns subsection**. The XSS denied patterns subsection follows the XSS allowed tags subsection, with the subsection header at the top and a list of denied patterns beneath it. Each denied pattern is on a separate line and is enclosed in `<pattern></pattern>` tags. You add XSS denied patterns to the list by entering each pattern on a separate line and enclosing it in the specified XML tags. The subsection is terminated by a blank line.

  Following are some of the default XSS denied patterns, in context:

```
      <!--XSS denied patterns-->
<denied>

<!-- HTML 4.0 -->
<pattern>\bonblur\b</pattern>
<pattern>\bonchange\b</pattern>
<pattern>\bonclick\b</pattern>
<pattern>\bondblclick\b</pattern>
...
<pattern>\bjavascript:</pattern>
<pattern>&amp;\{.+};</pattern>

<!-- HTML 5.0 -->
<pattern>\bonabort\b</pattern>
<pattern>\bonafterprint\b</pattern>
<pattern>\bonbeforeprint\b</pattern>
<pattern>\bonbeforeunload\b</pattern>
...
<pattern>\bonvolumechange\b</pattern>
<pattern>\bonwaiting\b</pattern>
      </denied>
```

- **Signatures section header**. The Signatures section header and opening tags follow the XSS section ending tag:

```
</xss>
<Signatures>
```

- **Signatures section**. The signatures section follows the XSS section. Each signature consists of the following elements:
  - **Signature rule**. Identifies and defines the rule, indicating whether it is enabled or disabled and which check actions it performs when one or more signature patterns match a request.
  - **Log string**. Describes the purpose of the signature, for logging.
  - **Patterns**. Defines the patterns that must be matched before the signature rule is implemented. Each pattern consists of an optional location area, which defines the specific portion of the request or response that is to be analyzed, and a match string.
  - **Reference**. Specifies bug tracking IDs associated with this signature rule.

  The section is terminated by a blank line.

  Following is an example of a signature rule:

```
<SignatureRule id="803" version="16" enabled="OFF"
actions="block,log" category="web-cgi" type="PlaceHolder">
<LogString>WEB-CGI HyperSeek hsx.cgi directory traversal
attempt</LogString>
<PatternList>
<Pattern>
<Location area="HTTP_URL"></Location>
<Match type="LITERAL">/hsx.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">../../</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">%00</Match>
</Pattern>
</PatternList>
<Reference>bugtraq,2314</Reference><Reference>cve,2001-0253</
Reference><Reference>nessus,10602</Reference>
</SignatureRule>
```

Caution: Do not modify any of the header sections.

Importing the Signature File

Import the XML configuration in the signature file to your NetScaler appliance by running the following command at the NetScaler command prompt:

```
import appfw signatures <src path> <signature object name>
```

where,

`src path` specifies the source of the signature file. This is a URL of the form <protocol>://<host>[:<port>][/<path>]

`signature object name` specifies the name of the signature object.

Note: The signature file associated with an application firewall policy is not reflected in the log messages.

For more information about the Signatures feature, see the chapter “Signatures” in the *Citrix Application Firewall Guide*.

Setting the Application Firewall Profile

Set the application firewall profile with the signature object name by running the following command at the NetScaler command prompt:

```
set appfw profile <profile name> signatures <signature object
name>
```

where,

`profile name` specifies the name of the application firewall profile that you have created. For information on creating profiles, see “Creating and Configuring a Profile,” on page 41.

`signature object name` specifies the name of the signature object.

For more information about the Signatures feature, see the chapter “Signatures” in the *Citrix Application Firewall Guide*.

Setting Up a Default deny all Policy

When operating the TOE in the Common Criteria-evaluated configuration, the administrator must configure the Application Firewall to define a deny all policy to block all requests that do not match an Application Firewall policy and bind this policy globally.

To configure a default deny all policy

At the NetScaler command prompt, type

```
add appfw profile default_deny_profile –defaults advanced
add appfw policy default_deny_policy NS_TRUE default_deny_profile
bind appfw global default_deny_policy PRIORITY
```

Note: The PRIORITY setting should be set so that the default policy will get evaluated in the end, that is, if the request does not match any other configured policies, the default policy is evaluated and used.

Configuring Audit Server Logging

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 events history in a 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 auditing parameters on the NetScaler, set up and install the executable files on a computer from where 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.

For information on procedures to configure audit parameters, configure audit policies to enable logging, and configure an external syslog server, see chapter “Audit Logging” in the *Citrix NetScaler Administration Guide*.

CHAPTER 5

Securing the Deployment

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
- Access Gateway Security
- Application Firewall Security
- Customer Reporting and Communication

Non-CC-Certified Product Updates

Citrix will, from time to time, issue product updates which may correct flaws in the underlying software. Administrators should check with Citrix on a regular basis for these updates. Administrators may also opt to subscribe to proactive email alerts about product security vulnerabilities and their associated fixes. These alerts are sent out on a regular basis whenever new fixes are available. Administrators may 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 is issued which corrects a critical flaw, but which 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-CC certified update.

Physical Security

You must deploy the NetScaler appliance in a secure location. NetScaler is intended to be physically secured from theft or tampering.

Appliance Security

- **Protect the Console Port from Unauthorized Access -** The serial console 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 NetScaler, use a secure protocol like SFTP or HTTPS. Note: Updates require 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 additional 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 is not routable on the public internet and it is behind a firewall.
- **Placement in the network** - Review your organizational policy and compliance requirements to determine if NetScaler 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

- Identify and allow only specific IP addresses access to the NSIP.

  Example

  ```
  > add acl local_access allow -srcip 192.168.0.1-192.168.0.3
  -destip 192.168.0.1-192.168.0.3
  ```

```
 Done
> apply acls
 Done
```

- If Administrators use SSH to log on to a NetScaler, access should be permitted strictly from one or more bastion hosts. This ensures that no one can access the nsroot account without first authenticating with their regular user name/password to the bastion host. Following is an example of the commands needed to explicitly allow access from a particular IP range to NSIP of a range of NetScaler appliances:

  ```
  > add acl bastion1-ssh ALLOW -srcip 10.0.0.1-10.0.0.20 -destip
  192.168.0.2-192.168.0.6 -destport 22 -protocol tcp
   Done
  > add acl bastion2-ssh ALLOW -srcip 172.16.0.1-172.16.0.20
  -destip 192.168.0.2-192.168.0.6 -destport 22 -protocol tcp
   Done
  > apply acls
   Done
  ```

- Use a default deny action for NSIP and MIP.

  Example

  ```
  > add acl default_deny deny -destip 192.168.0.1-3
  > apply acls
   Done
  ```

  By default everything is allowed for access. So we need to put a default deny action to deny everything and then allow access explicitly. The default deny ACL should have low priority.

  Note that in the NetScaler operating system, policy priorities work in reverse order—the higher the number, the lower the priority. For example, if you have three policies with priorities of 10, 100, and 1000, the policy assigned a priority of 10 is performed first, then the policy assigned a priority of 100, and finally the policy assigned an order of 1000.

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 RADIUS protocol or LDAP protocol is used for external authentication when operating the TOE in the CC-evaluated configuration. The RADIUS and LDAPv3 protocols may be used since it makes use of a shared secret to authenticate the client and server and ensures that passwords are sent encrypted between clients and RADIUS servers. Additionally, if facilities exist to encrypt the communications between the TOE and the RADIUS or LDAP server then the administrator should implement this.

Administrators may specify how passwords are encoded in RADIUS packets using the `passEncoding` option of the `set authentication radiusAction` command.

The administrator can also enable single sign-on (SSO) configuration on the NetScaler for users who log on by using a third party authentication server that supports SAML (Security Assertion Markup Language). The Authentication Interface provides the connection between the Authentication Subsystem and external authentication servers using SAML Token over HTTP POST Binding. SAML is an XML-based standard for exchanging authentication and authorization data between Identity Provider and Service Provider. This supports authentication for multiple domains. The SAML 2.0 Consumer handles SAML assertions sent by any Identity Provider (IdP) and associated user with a session.

Logging

Audit server enables logging of all the states and status information collected by different modules in the kernel as well as in the user-level daemons so that the administrator can see the event history in chronological order.

- **Local Configuration**

  The Audit Server can be configured by setting nslogparams.

  ```
  set audit nslogparams -serverip <hostname> -serverport <port>
  ```

- **Remote Configuration**

  Remote configuration needs the Audit Server to be installed on the remote machine. The Audit Server options are described below.

  ```
  ./audserver  -help
  usage : audserver -[cmds] [cmd arguements]
           cmds  cmd arguemnts: -f <filename> -d debug
          -help    - detail help
     -start   - cmd arguements,[starts audit server]
  ```

```
-stop    - stop audit server
-verify  - cmd arguements [verifies config file]
-addns   - cmd arguements [add a netscaler to conf file]
-version - prints the version info
```

For information on configuring nslog server, see the *Citrix NetScaler Administration Guide*.

To log all syslog messages

Remove the log file specifications in the /nsconfig/syslog.conf file for the local facilities and replace them with the log host name or IP address of the remote syslog host, as shown below.

```
local0.* @10.100.3.53
local1.* @10.100.3.53
```

Note: You need to copy the `syslog.conf` file from the `/etc` folder to the `/nsconfig` folder before making the above changes. This is to ensure that you do not overwrite the existing `/etc/syslog.conf` defaults and you always have a copy of the original file.

You must also configure the syslog server to accept log entries from both these logging facilities. To determine how to do this, see the syslog server documentation. For most UNIX-based servers using the standard syslog software, you must add a local facility configuration line for both the messages and nsvpn.log files to the syslog.conf configuration file. The facility values must correspond with those configured on the NetScaler.

The remote syslog Server in any Unix-based machine will not listen for remote logs by default. So it should be started with following options.

```
syslogd -m 0 -r
```

Disable L3 mode

The NetScaler offers highly configurable and robust packet routing options. When set to the factory defaults, the L3 mode is enabled on the NetScaler. When operating the TOE in the Common Criteria evaluated configuration, the administrator must ensure that L3 mode is disabled.

To disable the L3 mode using the NetScaler command line

Type the following command at the prompt:

```
disable ns mode L3
```

Disable SNMP

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

To disable SNMP

At the NetScaler command prompt, type

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

To verify whether 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 the High Availability Mode

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

To disable high availability mode on a NetScaler

At the NetScaler command prompt, type

```
set ha node -hastatus disabled
```

Disable Port 4001

You need 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 (ACL) 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 ensure that the IPv6 protocol translation is disabled.

To disable IPv6 on a NetScaler

At the NetScaler command prompt, type

```
disable ns feature IPv6protocoltranslation
```

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 response on these ports.

To disable ports not used for management access

At the NetScaler command prompt, type

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

Disable NetScaler Features Not Applicable to the Common Criteria Deployment

You must disable the 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
```

The following figure shows the status (ON/OFF) of all the features in the CC deployment.

```
> sh ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  OFF
 3)     Load Balancing                  LB                  ON
 4)     Content Switching               CS                  OFF
 5)     Cache Redirection               CR                  OFF
 6)     Sure Connect                    SC                  OFF
 7)     Compression Control             CMP                 OFF
 8)     Priority Queuing                PQ                  OFF
 9)     SSL Offloading                  SSL                 OFF
 10)    Global Server Load Balancing    GSLB                OFF
 11)    Http DoS Protection             HDOSP               OFF
 12)    Content Filtering               CF                  OFF
 13)    Integrated Caching              IC                  OFF
 14)    SSL VPN                         SSLVPN              ON
 15)    AAA                             AAA                 OFF
 16)    OSPF Routing                    OSPF                OFF
 17)    RIP Routing                     RIP                 OFF
 18)    BGP Routing                     BGP                 OFF
 19)    Rewrite                         REWRITE             OFF
 20)    IPv6 protocol translation       IPv6PT              OFF
 21)    Application Firewall            AppFw               ON
 22)    Responder                       RESPONDER           OFF
 23)    HTML Injection                  HTMLInjection       OFF
 24)    NetScaler Push                  push                OFF
 Done
```

Change the Password of the RPC Node

You need to 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.

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
```

Turn off SSLv2 Redirect

At the NetScaler command prompt, type:

```
> set ssl vserver <vserver_name> -sslv2redirect DISABLED
-cipherredirect DISABLED
```

Drop Invalid HTTP Requests

For increased availability of your backend servers, consider allowing only valid HTTP requests to reach them.

At the NetScaler command prompt, type:

```
> set ns httpParam -dropInvalReqs ON
```

Turn off SSL Renegotiation

At the NetScaler command prompt, type:

```
> set ssl parameter -denySSLReneg ALL
```

Password Complexity

Users and administrators of the 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 password length of eight characters
- the password must not contain dictionary words

- the password must not contain combinations of dictionary words
- the password may include uppercase letters, lowercase letters, numbers, symbols, and the space character

Audit Logs

This section provides clarifying information about audit logs.

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 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 an external syslog server), the administrator must ensure that the audit logs are protected from disclosure to non-TOE administrators during transmission and storage.

Audit Log Review

All audit events relating to the evaluated security functions are recorded in the file ns.log, and stored locally on the NetScaler. This log file is archived when it reaches the pre-defined size, and the archives are named according to the date and time at which the archive was created. To search the audit logs the administrator can use the Unix “grep” command, specifying the key words that are to be searched for (e.g. if interested in the creation of new administrative accounts, the administrator could grep for “create system user”). Note that the log entries record the long form of the CLI command, even if the short form of the command was entered at the CLI by the administrator.

Administrators can review audit logs and also filter messages based on the module, event type, and severity. In addition, there is a Search string facility for the message allowing it to be searched on any field contained in the message including: Command, Remote_ip, Status, and User.

For more information, see the chapter “Audit Logging” in the *Citrix NetScaler Administration Guide*.

Timestamps

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

NetScaler FIPS Configuration for the CC-Evaluated Deployment

The following recommendations are in addition to the NetScaler recommendations above and are specific to the FIPS version of the NetScaler.

- **Change FIPS crypto card passwords** - If you are 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 follows:

  ```
  set ssl fips -initHSM Level-2 <soPassword> <oldSoPassword>
  <user-Password> [-hsmLabel <string>]
  save configuration
  ```

  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. This means once it is locked, it will cease to be operational and you will not be able to alter its configuration.

Note: Keys larger than 2048 bytes cannot be generated.

Access Gateway Configuration for the CC-Evaluated Deployment

The following recommendations are in addition to the NetScaler recommendations above and are specific to Access 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 ALLOW or DENY as is required. The value of this parameter decides whether the default authorization action should be ALLOW or DENY.

  In NetScaler 10, by default, the authorization action is set to DENY. Users should ensure that this value is deny by default and they should give the access explicitly.

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

  ```
  set vpn parameter -defaultAuthorizationAction DENY
  ```

To verify whether the setting is deny, at the NetScaler 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 on this issue.

Example 1:

Consider that the authorization action is implicitly set to DENY.

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

Now, you want that when the user “foo” logs on through Access Gateway, “foo” should be able to access *only* `.GIF` files. To do so, you need to add a policy and set it to ALLOW only *.GIF files for the user “foo”.

At the NetScaler command prompt, type:

```
add authorization policy author-policy "URL == /*.gif" ALLOW
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, then ALLOW the request.” The EXPLICIT rule is “ALLOW access to `.GIF` files”, but the IMPLICIT rule is “DENY 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 denied access.

Example 2:

Consider that the authorization action is implicitly 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 Access 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, then 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 Access 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 NetScaler to drop and log invalid HTTP requests - To do this, 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 used through the VPN or clientless VPN. To do this, you need to define authorization policies and bind the policies to specified users. You need to 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
```

Application Firewall Configuration for the CC-Evaluated Deployment

The following recommendations are in addition to the NetScaler recommendations above and are specific to the Application Firewall feature.

- **Deploy in two-arm mode** - With a two-arm mode installation, the appliance is physically located between the Web servers it protects and your users. Connections must pass through it, minimizing chances that a route can be found around it.
- **Use default deny** - Configure a global deny all policy to block all requests that do not match an Application Firewall policy.

  ```
  add appfw profile default_deny_profile -defaults advanced

  add appfw policy default_deny_policy NS_TRUE
  default_deny_profile

  bind appfw global default_deny_policy <PRIORITY>
  ```

  Note: The PRIORITY setting should be set so that the default policy will get evaluated in the end if the request does not match any other configured policies and fails.

  In NetScaler 10, we have default profiles and one of which called appfw_block when configured will block the requests that are not matching the appfw policies.

  ```
  set appfw settings -defaultProfile appfw_block
  ```

Customer Reporting and Communication

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

- Using the secure@citrix.com e-mail address
- Using the customers' Support contacts.
- Using other Citrix contacts such as Resellers or Systems Engineers.

The recommended route for customers to report suspected security vulnerabilities is via 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 will be 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 suspected security flaws that are discovered internally by Citrix staff, security engineering staff can be notified via the secure@citrix.com address, an internal email distribution list or direct contact with security engineering staff.

The types of ongoing communication can include a request for an update on a reported issue by the reporting party, a request for more information by security engineering staff, or the reporting of feedback on a supplied mitigation.

CHAPTER 6

Testing the Deployment

After you complete installation and configuration of the deployment, you need to test that your deployment works. This chapter describes how to log on and test the system.

Testing Access Gateway

To test the Access Gateway deployment, perform the procedures described in this section.

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

1. Log on to Access Gateway.
2. Provide a valid client certificate.
3. Enter the user name and password.

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

Access the Access Gateway server

The Log In page should allow you to only 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.
2. Access a backend service for which access is allowed by a policy.
3. Log out and attempt to log on using an invalid user name and/or incorrect password.
   You should not be able to log on successfully.

Testing Application Firewall

To test the Application Firewall deployment, perform the procedures described in this section.

To verify that traffic to a destination IP is blocked

Access the load balancing virtual server for which you have configured the application firewall policy and access any file in the backend.

The access should be blocked as 402 and the following example message should be seen in the logs.

Dec 10 04:55:05 <local0.info> <ip_address> 12/10/2009:04:55:05 GMT ns PPE-3 : APPFW APPFW_STARTURL 53 : 10.103.4.21 3qk//H ILTsJZHbtukA90syLxh7oA0 pr1 Disallow Illegal URL: http://<ip_address>/ <blocked>

To verify that traffic containing POST is blocked

Access the load balancing virtual server by doing POST.

The access should be blocked and the following example Log message should be shown.

Dec 10 09:19:06 <local0.info> <ip_address> 12/10/2009:09:19:06 GMT ns PPE-6 : APPFW APPFW_STARTURL 31 : <ip_address> nh1GLgKv482m6JeYGLt+y5bVYDEA0 pr1 Disallow Illegal URL: http:// <ip_address>/ <blocked>

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
```