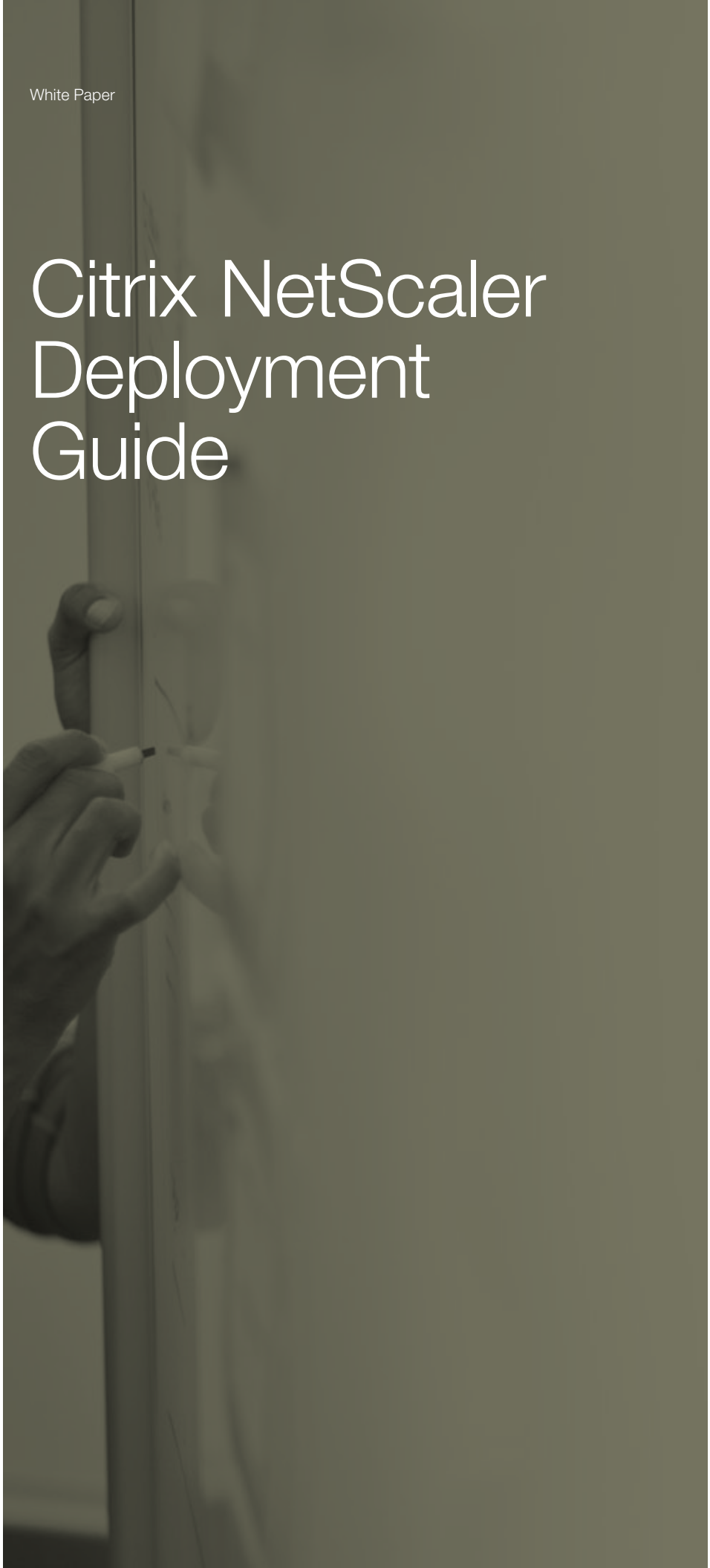
White Paper

Citrix NetScaler Deployment Guide



CITRIX®

Table of Contents

Citrix NetScaler ADC Overview

The Citrix® NetScaler® ADC product line optimizes delivery of applications over the Internet and private networks. NetScaler is an application delivery controller (ADC) that accelerates application performance, enhances application availability with advanced L4-7 load balancing, secures mission-critical apps from attacks and lowers server expenses by offloading computationally intensive tasks. All these capabilities are combined into a single, integrated appliance for increased productivity, with lower overall total cost of ownership.

NetScaler is deployed in front of web, application and database servers. It combines high-speed L4-7 load balancing and content switching with application acceleration, data compression, static and dynamic content caching, SSL acceleration, network optimization, application performance monitoring application visibility and robust application security via an application firewall.

NetScaler appliances are installed in the data center and route all connections to back-end servers. The NetScaler features are enabled and the policies configured are then applied to incoming and outgoing traffic. NetScaler requires no additional client or server side software, and can be configured using the NetScaler web-based GUI, RESTful API ("Nitro") and CLI configuration utilities.

NetScaler is available as a high-performance network appliance and a virtual appliance for maximum deployment flexibility. The hardware based MPX appliances with multi-core processor designs are available with a wide range of appliance availability; from sub gigabit throughput to 50 Gbps. Each leverages a fully hardened and secure operating system.

NetScaler appliances provide multi-dimensional scalability for a superior ROI. Pay-As-You-Grow and Burst Pack upgrade licenses enable specific models to be upgraded to higher-end models within a particular platform via a software license. NetScaler SDX models allow up to 40 fully independently managed NetScaler instances to run on a single platform. NetScaler with Citrix TriScale clustering allows up to 32 NetScaler appliances (of the same platform, model and edition) to be aggregated into a single group to increase aggregate app delivery capacity.

NetScaler solutions are available in three software editions: Standard, Enterprise, and Platinum. These editions offer the following feature sets:

Standard Edition
NetScaler Standard Edition provides comprehensive layer 4-7 load balancing and content switching, SSL acceleration and server offload capabilities.

Enterprise Edition
NetScaler Enterprise Edition is a highly integrated application delivery solution. It includes all Standard Edition capabilities, plus dynamic routing support, data compression (AppCompress), global server load balancing (GSLB), surge protection, priority queuing, L7 DoS protection, AAA for traffic management and cache redirection. Enterprise Edition also includes Citrix Command Center software.

Platinum Edition
NetScaler Platinum Edition is the most integrated and feature-rich NetScaler offering. It includes all Enterprise Edition capabilities, plus content caching (AppCache), web application firewall, NetScaler Cloud Bridge and EdgeSight for NetScaler application performance monitoring. It also includes Citrix Command Center software and NetScaler Cloud Bridge.

Note: NetScaler clustering license upgrades are available on all NetScaler MPX and VPX models and software editions.

Software Options
The following options are available for NetScaler MPX appliances.

- Global Server Load Balancing (GSLB) - Directs user requests to the data center best able to handle it. Requests can be redirected based on dynamic changes in global network performance, site connectivity and availability. Server location, load and many other factors determine the optimal server to use.
- NetScaler AppCompress™ - Improves end-user performance and reduces bandwidth consumption by compressing HTML/text content before transmission to clients. AppCompress supports both encrypted and unencrypted data.
- AppCache™ – Citrix NetScaler AppCache improves application performance by storing cacheable content, both static and dynamic, directly on the NetScaler platform. Multiple techniques ensure content freshness.
- NetScaler Application Firewall™ – NetScaler Application Firewall ensures security at the application layer. It is an ICSA-certified web application firewall that automatically blocks malicious web traffic.
- Citrix EdgeSight™ for NetScaler – EdgeSight for NetScaler is a transparent tool to measure end-user performance, and does not require a client-based agent. EdgeSight for NetScaler helps evaluate performance issues and monitor trends to anticipate future unacceptable performance levels allowing proactive network changes. Numerous application performance parameters, such as time to download a page and round trip response times, are stored and displayed in a variety of formats.

Click here for the NetScaler Product Overview.

NetScaler ADC Features and Benefits

Table 1 summarizes the features and benefits of the NetScaler MPX Appliances.

Table 1: Features and Benefits

Feature	Benefit
Availability	
Application switching	The Citrix NetScaler appliances provide load-balancing and content-switching functions with granular traffic control based on customizable Layer 4 through 7 rules with support for both IPv4 and IPv6 addresses, virtual IP addresses (VIPs) and server farms. NetScaler can natively load-balance the following protocols in an IPv4 environment: HTTP/HTTPS, FTP, DNS, ICMP, SIP, RTSP, Extended RTSP, LDAP, RADIUS, SCCP and Microsoft RDP. In an IPv6 environment, it can natively load-balance HTTP, HTTPS and SSL protocols. It has generic protocol parsing capabilities that enable the configuration of application switching and persistence policies

	based on any information in the traffic payload for custom and packaged applications without requiring any programming. NetScaler supports translation and load balancing between IPv4 and IPv6 networks and provides flexibility to customers in planning their IPv6 migration.
Persistency	Stickiness allows the same client to maintain multiple simultaneous or subsequent TCP or IP connections with the same real server for the duration of a session
Redundancy	Stateful failover capabilities help ensure resilient network protection for enterprise network environments. NetScaler integrates global server load balancing to provide a multiple data center scaling and failover system.
Server health monitoring	NetScaler checks the health of application servers and server farms through configuration of health probes.
Database load balancing	SQL-aware health monitors increase availability of database servers. SQL connection offload increases database server performance and aids in scaling database servers. SQL intelligent load balancing enables scaling out database deployments to routing SQL requests to the most appropriate server.
Clustering	Citrix TriScale clustering allows up to 32 appliances to work in concert to deliver one or multiple applications. The result is a cost effective and simple option for scaling out application delivery infrastructures.
Performance	
Compression	NetScaler delivers up to 11 Gbps data compression and provides faster application performance for application users.
SSL acceleration	NetScaler MPX and SDX integrates hardware-based SSL acceleration technology, which offloads the encryption and decryption of up to 11 Gbps of SSL traffic from servers,
TCP offload	Offload web, application, and database servers from compute intensive tasks such as TCP connection management, SSL encryption/decryption and in-memory caching of both dynamic and static content.
Caching	Deliver application content immediately, both static and Dynamic, without burdening servers.
Security	
Datacenter security	NetScaler protects the data center and critical applications from protocol and denial-of-service (DoS) attacks at both L4 and L7 and encrypts mission-critical content.
Application Security	NetScaler Web Application Firewall provides deep protocol inspection capabilities, which enables IT professionals to comprehensively secure high-value applications in the data center. It secures mission-critical applications and protects against identity theft, data theft, application disruption, and fraud and defends web-based applications and transactions against targeted attacks by professional hackers. NetScaler uses a hybrid model including scanning over 3000 signatures for preventing known attack vectors.
Content rewrite and response control	Policy-based bidirectional rewriting of HTTP header, payload elements and URLs. Policy-based redirection of incoming requests. Responder module with custom responses and redirects. Policy-based routing and network aware policies.
Packet filtering	L3 and L4 access control lists. Network Address Translation.
Virtualized Services	
Virtual contexts	NetScaler SDX provides a means for creating complete resource segmentation and isolation, allowing the NetScaler appliance to act as if it were several individual appliances within a single physical appliance. NetScaler SDX enable organizations to provide defined levels of service to up to 40 business departments, applications, or customers and partners from a single NetScaler SDX appliance.
Role-based access control (RBAC)	RBAC allows organizations to specify administrative roles and restrict administrators to specific functions within the appliance or virtual contexts, allowing each administrator group to freely perform its tasks without affecting the other groups.
Deployment and Management	
Function consolidation	Through consolidation of application switching, SSL acceleration, data center security, and other functions on one device, NetScaler helps achieve better application performance, with fewer devices, simpler network designs, and easier management.
Investment protection	NetScaler supports virtualization with one administrator device and up to 40 virtual contexts, 400,000 SSL transactions per second (TPS), and up to 11 Gbps of compression. The licensed throughput can be increased to up to 50 Gbps without the need for new equipment, through software license upgrades.

Operational visibility	Provides network administrators application level details; AppFlow extends network monitoring to include granular application-layer visibility. By using IPFIX standard extensions NetScaler can provide inputs into a wide variety of monitoring tools. This eliminates span ports and network taps.
AppExpert framework	AppExpert Visual Policy Builder visually builds the policy for every web app delivery feature without programming. AppExpert Templates provide pre-configured settings to optimize specific applications.
ActionAnalytics	Integrated, easy-to-use application analysis and policy-based control. Complements AppFlow with insight into full web application and SQL environments. Provides real-time monitoring and adaptive policy controls that transform raw data into actionable information to deliver better business intelligence and automatically tune application delivery policies.

NetScaler MPX portfolio and hardware information

Table 2: NetScaler MPX platform options and specifications.

NetScaler MPX Model	Throughput (Gbps)	Compression (Gbps)	SSL Throughput (Gbps)	SSL TPS: 1K & 2K Key (K)	HTTP Requests per Second (K/s)
5550	0.5	0.5	0.5	7.5/1.5	175
5650	1	1	1	10/2	250
8200	2	1.1	2	13/2.8	350
8400	4	2.3	4	25/5.7	600
8600	6	3.5	5.5	40/8.5	800
11500	8	3.5	6	80/15	1,200
13500	12	4.5	6.5	93/19	1,600
14500	18	5	7	105/22	1,800
16500	24	6	10	133/28	2,000
17550	20	7	8	150/33	2,400
18500	36	7	10.5	158/34	2,500
19550	30	8	9	245/50	3,500
20500	42	8	11	205/45	2,600
20550	40	9	10	330/73	4,000
21550	50	11	11	380/98	4,000

Network Topology

Where Does a NetScaler Fit in the Network?

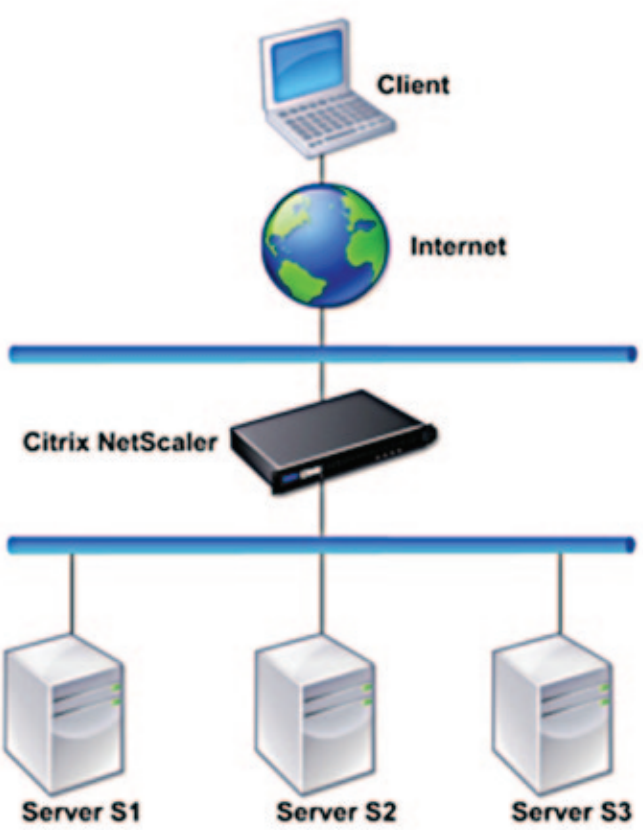
NetScaler resides in front of web and applications servers, so that client requests and server responses pass through it. In a typical installation, virtual servers (vservers) configured on the NetScaler provide connection/termination points that clients use to access the applications delivered by NetScaler. In this case, the NetScaler owns public IP addresses that are associated with its vservers, while the real servers are isolated in a private network. It is also possible to operate the NetScaler in a transparent mode as an L2 bridge or L3 router, or even to combine aspects of these and other modes.

Physical Deployment Modes

NetScaler can be deployed in either of two physical modes: inline and one-arm. In inline 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 can exist on different subnets in this configuration. It is possible for the servers to be in a public network and the clients to directly access the servers through the NetScaler, with the NetScaler transparently applying the L4-L7 features. Usually, vservers are configured to provide an abstraction of the real servers.

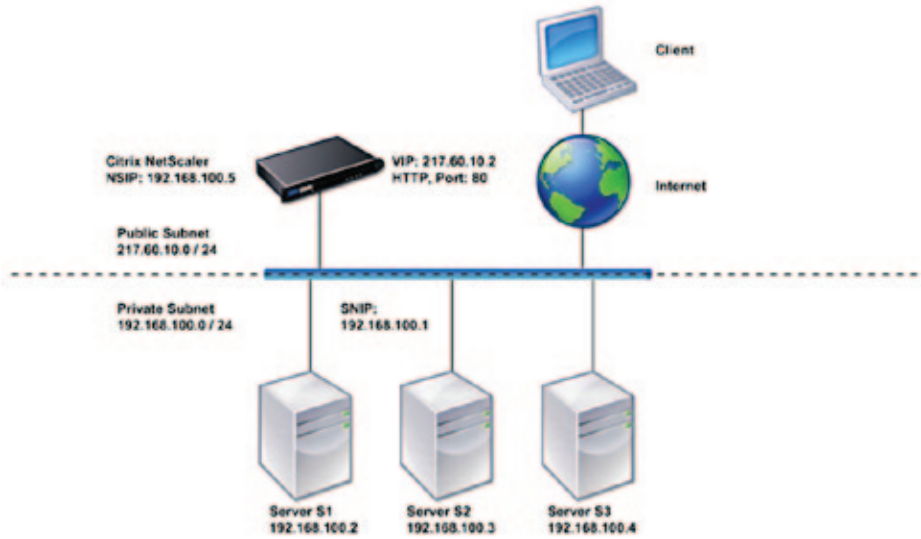
The following figure shows a typical inline deployment.

Figure 1- Inline Deployment



In one-arm mode, only one network interface of the NetScaler is connected to an Ethernet segment. The NetScaler in this case does not isolate the client and server sides of the network, but provides access to applications through configured vservers. One-arm mode can simplify network changes needed for NetScaler installation in some environments.

Figure 2- Topology Diagram for One-Arm Mode, Multiple Subnets



Citrix NetScaler as an L2 Device

A NetScaler functioning as an L2 device is said to operate in L2 mode. In L2 mode, the NetScaler forwards packets between network interfaces when all of the following conditions are met:

- The packets are destined to another device's media access control (MAC) address.
- The destination MAC address is on a different network interface.
- The network interface is a member of the same virtual LAN (VLAN).

By default, all network interfaces are members of a pre-defined VLAN, VLAN 1. Address Resolution Protocol (ARP) requests and responses are forwarded to all network interfaces that are members of the same VLAN. To avoid bridging loops, L2 mode must be disabled if another L2 device is working in parallel with the NetScaler.

Citrix NetScaler as a Packet Forwarding Device

A NetScaler can function as a packet forwarding device, and this mode of operation is called L3 mode. With L3 mode enabled, the NetScaler forwards any received unicast packets that are destined for an IP address that it does not have internally configured, if there is a route to the destination. A NetScaler can also route packets between VLANs.

In both modes of operation, L2 and L3, a NetScaler generally drops packets that are in:

- Multicast frames
- Unknown protocol frames destined for a NetScaler's MAC address (non-IP and non-ARP)
- Spanning Tree protocol (unless BridgeBPDUs is ON)

How a NetScaler Communicates with Clients and Servers

A NetScaler appliance is usually deployed in front of a server farm and functions as a transparent TCP proxy between clients and servers, without requiring any client-side configuration. This basic mode of operation is called Request Switching technology and is the core of NetScaler functionality. Request Switching enables a NetScaler to multiplex and offload the TCP connections, maintain

persistent connections, and manage traffic at the request (application layer) level. This is possible because the NetScaler can separate the HTTP request from the TCP connection on which the request is delivered.

Depending on the configuration, a NetScaler may process the traffic before forwarding the request to a server. For example, if the client attempts to access a secure application on the server, the NetScaler might perform the necessary SSL processing before sending traffic to the server.

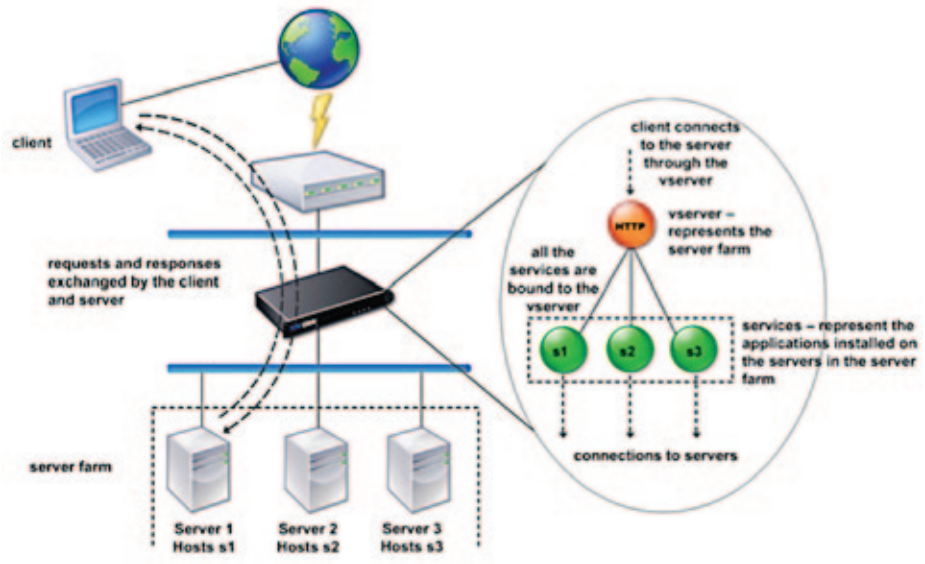
To facilitate efficient and secure access to server resources, a NetScaler uses a set of IP addresses collectively known as NetScaler-owned IP addresses. To manage your network traffic, you assign NetScaler-owned IP addresses to virtual entities that become the building blocks of your configuration. For example, to configure load balancing, you create virtual servers (vservers) to receive client requests and distribute them to services, which are entities representing the applications on your servers.

Traffic Management Building Blocks

The configuration of a NetScaler is typically built up with a series of virtual entities that serve as building blocks for traffic management. The building block approach helps separate traffic flows. Virtual entities are abstractions, typically representing IP addresses, ports, and protocol handlers for processing traffic. Clients access applications and resources through these virtual entities. The most commonly used entities are vservers and services. Vservers represent groups of servers in a server farm or remote network, and services represent specific applications on each server.

Most features and traffic settings are enabled through virtual entities. For example, you can configure a NetScaler to compress all server responses to a client that is connected to the server farm through a particular vserver. To configure the NetScaler for a particular environment, you need to identify the appropriate features and then choose the right mix of virtual entities to deliver them. Most features are delivered through a cascade of virtual entities that are bound to each other. In this case, the virtual entities are like blocks being assembled into the final structure of a delivered application. You can add, remove, modify, bind, enable, and disable the virtual entities to configure the features. The following figure shows the concepts covered in this section.

Figure 3. How Traffic Management Building Blocks Work

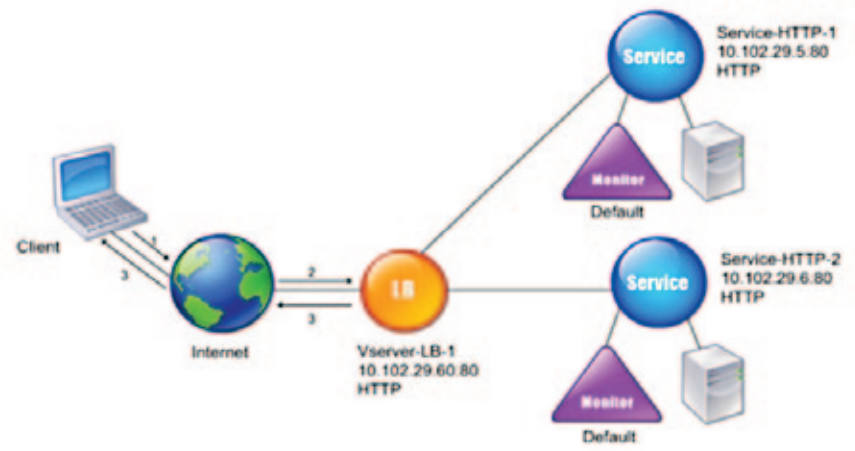


A Simple Load Balancing Configuration

In the example shown in the following figure, the NetScaler is configured to function as a load balancer. For this configuration, you need to configure virtual entities specific to load balancing and bind them in a specific order. As a load balancer, a NetScaler distributes client requests across several servers and thus optimizes the utilization of resources.

The basic building blocks of a typical load balancing configuration are services and load balancing vservers. The services represent the applications on the servers. The vservers abstract the servers by providing a single IP address to which the clients connect. To ensure that client requests are sent to a server, you need to bind each service to a vserver. That is, you must create services for every server and bind the services to a vserver. Clients use the VIP to connect to a NetScaler. When the NetScaler receives client requests on the VIP, it sends them to a server determined by the load balancing algorithm. Load balancing uses a virtual entity called a monitor to track whether a specific configured service (server plus application) is available to receive requests.

Figure 4. Load Balancing Virtual Server, Services, and Monitors



In addition to configuring the load balancing algorithm, you can configure several parameters that affect the behavior and performance of the load balancing configuration. For example, you can configure the vserver to maintain persistence based on source IP address. The NetScaler then directs all requests from any specific IP address to the same server.

Understanding Policies and Expressions

A policy defines specific details of traffic filtering and management on a NetScaler. It consists of two parts: the expression and the action. The expression defines the types of requests that the policy matches. The action tells the NetScaler what to do when a request matches the expression. As an example, the expression might be to match a specific URL pattern to a type of security attack, with the action being to drop or reset the connection. Each policy has a priority, and the priorities determine the order in which the policies are evaluated.

When a NetScaler receives traffic, the appropriate policy list determines how to process the traffic. Each policy on the list contains one or more expressions, which together define the criteria that a connection must meet to match the policy.

For all policy types except Rewrite policies, a NetScaler implements only the first policy that a request matches, not any additional policies that it might also match. For Rewrite policies, the NetScaler evaluates the policies in order and, in the case of multiple matches, performs the associated actions in that order. Policy priority is important for getting the results you want.

Accelerating Load Balanced Traffic by Using Compression

Compression is a popular means of optimizing bandwidth usage, and all modern web browsers support compressed data. If you enable the AppCompress feature, the Citrix NetScaler intercepts requests from clients and determines whether the client can accept compressed content. After receiving the HTTP response from the server, the NetScaler examines the content to determine whether it is compressible. If the content is compressible, the NetScaler compresses it, modifies the response header to indicate the type of compression performed, and forwards the compressed content to the client.

NetScaler compression is a policy-based feature. A policy filters requests and responses to identify responses to be compressed, and specifies the type of compression to apply to each response. The NetScaler provides several built-in policies to compress common MIME types such as text/ html, text/ plain, text/xml, text/css, text/rtf, application/msword, application/vnd.ms-excel, and application/vnd.mspowerpoint.

You can also create custom policies. The NetScaler does not compress compressed MIME types such as application/octet-stream, binary, bytes, and compressed image formats such as GIF and JPEG.

To configure compression, you must enable it globally and on each service that will provide responses that you want compressed. If you have configured vservers for load balancing or content switching, you should bind the polices to the vservers. Otherwise, the policies apply to all traffic that passes through the NetScaler.

Accessing a Citrix NetScaler

A NetScaler® appliance has both a command line interface (CLI) and a graphical user interface (GUI). The GUI includes a configuration utility for configuring the appliance and a statistical utility, called Dashboard. 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.

Using the Command Line Interface

You can access the CLI either locally, by connecting a workstation to the console port, or remotely, by connecting through secure shell (SSH) from any workstation on the same network.

For more information about the features of the CLI, including SSH, see the Citrix NetScaler Command Reference Guide.

Logging on to the Command Line Interface through the Console Port

The NetScaler has a console port for connecting to a computer workstation. To log on to the NetScaler, you need a serial crossover cable and a workstation with a terminal emulation program.

To log on to the CLI through the console port

1. Connect the console port to a serial port on the workstation, as described in "Connecting the Console Cable" section in the Citrix Hardware Installation and Setup Guide.
2. On the workstation, start HyperTerminal or any other terminal emulation program. If the logon prompt does not appear, you may need to press ENTER one or more times to display it.
3. Log on by using the administrator credentials. The command prompt (>) appears on the workstation monitor.

Logging on to the Command Line Interface by using SSH

The SSH protocol is the preferred remote access method for accessing a NetScaler remotely from any workstation on the same network. You can use either SSH version 1 (SSH1) or SSH version 2 (SSH2.)

To log on to a NetScaler by using an SSH client

1. On your workstation, start the SSH client.
2. For initial configuration, use the default NetScaler IP address (NSIP), which is 192.168.100.1. For subsequent access, use the NSIP that was assigned during initial configuration. Select either SSH1 or SSH2 as the protocol.
3. Log on by using the administrator credentials.

Using the Graphical User Interface

The graphical user interface includes a configuration utility and a statistical utility, called Dashboard, either of which you access through a workstation connected to an Ethernet port on the NetScaler. If your computer does not have a supported Java plugin installed, the utility prompts you to download and install the plug-in the first time you log on. If automatic installation fails, you can install the plug-in separately before you attempt to log on to the configuration utility or Dashboard.

The system requirements for the workstation running the GUI are as follows:

- For Windows-based workstations, a Pentium® 166 MHz or faster processor with at least 48 MB of RAM is recommended for applets running in a browser using a Java plugin product. You should have 40 MB free disk space before installing the plug-in.
- For Linux-based workstations, a Pentium platform running Linux kernel v2.2.12 or above, and glibc version 2.12-11 or later. A minimum of 32 MB RAM is required, and 48 MB RAM is recommended. The workstation should support 16-bit color mode, KDE and KWM window managers used in conjunction, with displays set to local hosts.
- For Solaris-based workstations, a Sun running either Solaris 2.6, Solaris 7, or Solaris 8, and the Java 2 Runtime Environment, Standard Edition, version 1.6 or later.

Your workstation must have a supported web browser and version 1.6 or above of the Java® applet plug-in installed to access the configuration utility and Dashboard.

Quick Start Installation and Configuration

Configuration Requirements

Determine the following information for performing the initial configuration.

- NetScaler IP address: The management IP address of the appliance.
- Subnet IP address or Mapped IP address: The IP address used by the appliance to represent the client when communicating with a server.
- Default gateway: The IP address of the router that forwards traffic out of the appliance's subnet.
- Root password: The root user (nsroot) has full administrative privileges on the appliance. The root password is used to authenticate the root user.

Setting Up Connectivity

Connect the appliance to a management workstation or the network by using the NetScaler configuration utility, the command-line interface (CLI), or the LCD keypad.

Configuration Utility Setup

To set up the appliance by using the configuration utility, you need a management workstation or laptop configured on the same network as the appliance. To run the configuration utility, the Java RunTime Environment (JRE) version 1.4.2_04 or later must be installed on the workstation or laptop.

Note: The Setup Wizard automatically opens upon log on when the appliance is configured with the default IP address, when licenses are not installed on the appliance, and when either the mapped IP address or subnet IP address is not configured.

To configure the NetScaler by using the configuration utility

1. Connect the NetScaler to a management workstation or network.
2. Open a browser and type: http://192.168.100.1
   Note: The NetScaler is preconfigured with the IP address 192.168.100.1.
3. In **User Name**, type nsroot.
4. In **Password**, type nsroot.
5. In the **Setup Wizard**, click **Next** and follow the instructions in the wizard.
6. To confirm that the NetScaler is configured correctly, you can either ping the new NetScaler IP address (NSIP) or use the new NSIP to open the configuration utility in a browser.

CLI Setup

To set up the appliance by using the command-line interface (CLI), connect the serial cable to the console port. Access the command line with a terminal or terminal emulator with the following settings:

- Baud rate: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Log on to the NetScaler with the following credentials:

User name: nsroot

Password: nsroot

To configure the NetScaler by using the NetScaler command line

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

LCD Keypad Setup

To set up the appliance by using the LCD keypad on the front panel of the appliance, enter the following initial settings in the following order:

1. Subnet mask

2. NSIP

3. Gateway

The NSIP and the default gateway should be on the same subnet.

The subnet mask, NSIP, and gateway values are saved in the configuration file. You can then use the NSIP to connect to the appliance remotely. For more information, see the Citrix NetScaler Hardware Installation and Setup Guide at http://support.citrix.com/ article/CTX132365.

Additional Information

A complete set of documentation is available on the Documentation tab of your NetScaler and from http://support.citrix.com/. (Most of the documents require Adobe Reader, available at http://adobe.com/ .)

To view the documentation

1. From a Web browser, log on to the NetScaler.
2. Click the Documentation tab.
3. To view a short description of each document, hover your cursor over the title. To open a document, click the title.

If you have support questions, please contact Citrix Technical Support at 1-800-4-CITRIX (1-800-424-8749). For additional contact information, see Support Phone Numbers at http://support.citrix.com/. If you have comments or feedback on this documentation, please email to nsdocs_feedback@citrix.com.

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix
Citrix Systems, Inc. (NASDAQ:CTXS) is a leading provider of virtual computing solutions that help companies deliver IT as an on-demand service. Founded in 1989, Citrix combines virtualization, networking and cloud computing technologies into a full portfolio of products that enable virtual workstyles for users and virtual datacenters for IT. More than 230,000 organizations worldwide rely on Citrix to help them build simpler and more cost-effective IT environments. Citrix partners with over 10,000 companies in more than 100 countries. Annual revenue in 2010 was $1.87 billion.

0112/PDF

citrix.com