

Citrix NetScaler Glossary

Citrix® NetScaler® 9.1

Copyright and Trademark Notice

© CITRIX SYSTEMS, INC., 2009. ALL RIGHTS RESERVED. NO PART OF THIS DOCUMENT MAY BE REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS OR USED TO MAKE DERIVATIVE WORK (SUCH AS TRANSLATION, TRANSFORMATION, OR ADAPTATION) WITHOUT THE EXPRESS WRITTEN PERMISSION OF CITRIX SYSTEMS, INC.

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

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

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

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

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler Request Switch™ 9000 Series equipment. If the NetScaler equipment causes interference, 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.

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

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

Last Updated: June 2009

Glossary

- access control list (ACL).** A set of rules for identifying packets and processing them appropriately.
- Access Gateway Enterprise Edition.** An appliance, built into a NetScaler, that uses SSL VPN to provide secure access to private networks, such as company LANs.
- address resolution protocol (ARP).** A network layer protocol used to convert an IP address into a physical address. A host that requires a physical address broadcasts an ARP request onto the TCP/IP network. The host at the IP address in the request then replies with its physical hardware address.
- agent.** The software process that provides communication to a SNMP manager. A network device that uses SNMP must be running an agent. *See* Simple Network Management Protocol (SNMP).
- alarm.** An SNMP notification sent to a designated server in response to certain system and firewall events.
- authentication.** The process of determining whether someone or something is who or what it is declared to be. Authentication is commonly accomplished using a logon password.
- authentication type.** A type of authentication, such as RADIUS, LDAP, and SafeWord.
- authorization.** The process of providing permission to access resources on a system or network.
- backup vserver.** A system entity that forwards client traffic to the services if the primary vserver is down or disabled. It can also send notification messages to clients regarding site outage or maintenance.
- binding.** An assigned relationship between two objects in the NetScaler operating system. For example, a policy must be bound to a profile in order to take effect, and a certificate must be bound to an SSL virtual server in order to secure traffic.
- bridge tables.** A method for storing MAC addresses and their interfaces on a NetScaler. When a new frame arrives, the system refers to the bridge table and determines whether it needs to filter or bridge the frame.
- certificate authority (CA).** An entity that issues certificates after verifying the identity of a server. *See* Secure Sockets Layer (SSL).
- certificate signing request (CSR).** A message requesting a certificate authority to sign the public key of the requesting server with the private key of the certificate authority for the purpose of receiving a new SSL certificate. *See* Secure Sockets Layer (SSL).
- Citrix AppCache.** An integrated caching feature that enables static and dynamic application content to be delivered directly from a NetScaler instead of the application server, freeing Web and application servers from generating and serving the same content.
- Citrix AppCompress.** An HTTP compression feature that compresses data before the NetScaler forwards it to application users, reducing the amount of data on the network.
- Citrix EdgeSight for NetScaler.** A feature that provides Web application performance monitoring. EdgeSight for NetScaler monitors Web applications from the perspective of the client, providing real-time and historic visibility into Web application performance.
- client certificate.** An optional security component that contains information about a user and the SSL client. *See* Secure Sockets Layer (SSL).
- client device.** Any hardware device used to access corporate resources.

- command-line interface (CLI).** The character-based interface to a NetScaler.
- command policies.** Rules that control which NetScaler units users may access and administer.
- community string.** An authentication and authorization method in SNMP version 1. When a manager attempts a connection with an agent, it passes a community string, which the agent evaluates to determine whether to reply to the query. *See* Simple Network Management Protocol (SNMP).
- compound expression.** A type of expression made up of logical combinations of existing simple and compound expressions. Compound expressions compare the results of the separate expressions with logical operators to determine whether the compound expression as a whole is true or false.
- compression.** A feature providing compression of HTTP responses to compression-aware browsers. The use of compression can improve the performance of network-based applications.
- configuration utility.** The Web-based graphical user interface (GUI) used to configure and administer a NetScaler.
- content filtering.** A feature providing content-level protection of Web sites from malicious attacks. When this feature is enabled, the NetScaler inspects every incoming request with the configured rules based on the HTTP URLs or headers.
- content switching.** A feature that directs requests to specific servers based on type of content requested.
- cookie.** A piece of data that a Web server sends to a Web browser, to be stored in RAM memory or on the hard disk of the local computer and sent back to the Web server with every request from that Web application. Web servers use cookies to track user sessions, identify users who have previously visited the site, and store user information for registered users.
- cookie insert persistence.** A type of session persistence in which a NetScaler inserts an HTTP cookie in the client response and uses the cookie to direct subsequent requests from the client to the same physical server that handled the initial request.
- Dashboard.** A Java-based, browser-accessible application that allows administrators to monitor the performance of the NetScaler appliance based on statistical counters. These counters are displayed graphically as charts and tables.
- DEFLATE.** An algorithm that a NetScaler uses to compress data for Web browsers that support DEFLATE compression.
- denial of service (DOS).** A general term for any one of many kinds of attacks that attempt to prevent a server from performing properly.
- digital certificate.** A small file that contains public keys and verifies the identity of the holder. Certificates are issued by a certificate authority (CA).
- direct server return (DSR) mode.** A NetScaler deployment scenario in which the server responds to clients directly, using a return path that does not flow through the NetScaler.
- distinguished encoding rules (DER).** A method to encode a data object, such as a certificate, so that it is digitally signed or its signature is verified.
- distributed denial of service (DDOS).** A denial of service (DOS) attack that makes use of potentially thousands of computers to perform a DOS attack. *See* denial of service (DOS).
- expression.** An operation that evaluates a request or response to determine what to do with that request or response.
- failover.** An event in which the primary node in a high availability (HA) pair becomes the secondary node and the secondary becomes the primary as a result of a failure of the primary node.
- Federal Information Processing Standards (FIPS).** A U.S. Government standard, for hardware protection of SSL certificates and keys, required for many government customers. Special models of the Citrix Access Gateway and Citrix NetScaler support FIPS management of SSL certificates and keys.
- file transfer protocol (FTP).** A protocol used to transfer data from one computer to another over a TCP/IP-based network. Commonly used to download programs and other files to your computer from other servers.
- flash memory.** Non-volatile memory, mounted on a NetScaler as /flash. When a `save config` command is executed, the running configuration is saved to this drive.

- forced failover.** An administratively initiated failover on a node within a high availability (HA) pair. Commonly used when an administrator wants to verify that an HA configuration is performing correctly or to replace or upgrade the primary node. *See* high availability (HA).
- GZIP.** An algorithm a NetScaler uses to compress data for Web browsers that support GZIP compression.
- hard disk.** The hard disk on a NetScaler, used to store log data, core files, and unused builds. The /var directory represents the physical hard disk.
- health check.** A probe in which the state of the services on a NetScaler is periodically checked. *See* load balancing.
- high availability (HA).** A deployment scenario in which two NetScaler units are configured to operate as a single unit, with one NetScaler actively accepting and processing traffic while the other monitors it. If the first unit quits accepting and processing traffic, the second unit takes over.
- high availability (HA) monitor.** An entity that monitors an interface. When it is enabled on one of the interfaces and the status of the interface is DOWN, the state of the node becomes NOT UP.
- HTTP compression.** A feature implementing lossless compression that can be interpreted by popular browsers. The compression feature is implemented at origin sites that have HTML or other compressible content that is either statically or dynamically generated. *See* compression and Hypertext Transfer Protocol (HTTP).
- HTTP data.** The part of an HTTP request containing the information that the user typed into a Web form, or the part of an HTTP response that contains the Web content the user requested. *See* Hypertext Transfer Protocol (HTTP).
- HTTP header.** The part of an HTTP connection that contains information about the Web server or the user's browser and is intended to assist the Web server or browser in handling the connection. HTTP headers are the metadata portion of an HTTP request or response. *See* Hypertext Transfer Protocol (HTTP).
- HTTP request.** An HTTP connection from a user to a Web server, requesting content from the Web server. *See* Hypertext Transfer Protocol (HTTP).
- HTTP response.** An HTTP connection from a Web server to a user, sending information to the user. *See* Hypertext Transfer Protocol (HTTP).
- HTTP traffic.** Any HTTP connection, either from a user to a Web server or from a Web server to a user. *See* Hypertext Transfer Protocol (HTTP).
- Hypertext Transfer Protocol (HTTP).** A protocol for sending packets between a user's browser and a Web server.
- Hypertext Transfer Protocol Secure (HTTPS).** A protocol for sending HTTP packets securely between a user's Web browser and a Web server, in which packets are encrypted and cannot be read if intercepted. *See* Hypertext Transfer Protocol (HTTP) and Secure Sockets Layer (SSL).
- inline mode.** *See* two-arm mode.
- intermediate certificate.** A subordinate certificate issued by a trusted certificate authority and used to create server certificates in a certificate chain. *See* Secure Sockets Layer (SSL).
- Internet control message protocol (ICMP).** Control messages that provide feedback about problems in the network. Network operating systems use these messages to send error messages indicating, for instance, that a requested service is not available or that a host or router could not be reached.
- IP Security (IPsec).** A protocol used for negotiating encryption and authentication at the IP level. IPsec allows administrators to ensure that all packets between two hosts are encrypted, regardless of packet type or protocol used in transmission.
- key.** A string of bits used to encrypt and decrypt messages. *See* Secure Sockets Layer (SSL).
- Layer 2 mode.** A mode that controls the Layer 2 forwarding (bridging) function. This mode enables a NetScaler to bridge or process the packets that are not destined for its MAC address.
- Layer 3 mode.** A mode that controls the Layer 3 forwarding function. This mode enables a NetScaler to perform a route table lookup and forward the packets that are not destined for NetScaler-owned IP addresses.
- Layers 1-7.** *See* network layers.

- license.** A contractual agreement between a company and Citrix Systems that specifies which features can be used on a NetScaler.
- license key file.** A file provided by Citrix Systems that an administrator must upload to a NetScaler to enable it and its licensed features.
- lightweight directory access protocol (LDAP).** An application protocol to access information directories and to query and modify directory services running over TCP/IP.
- link aggregation.** A feature that combines or aggregates data from multiple ports into a single high-speed link. Link aggregation increases the capacity and availability of the communications channel between a NetScaler and other connected devices.
- load balancing.** A feature that balances the load among separately managed servers that serve the same applications or host the same data.
- local area network (LAN).** A network behind a firewall or router of a company, where Web servers, mail servers, and other protected resources are located.
- log.** One of a collection of text files, maintained by the Citrix NetScaler operating system, that consists of information about various activities and events that occur on that NetScaler. Log files usually contain a single line of text per logged event or activity.
- MAC-based forwarding (MBF).** A mode that enables the system to remember the MAC address of the source.
- managed devices.** Network nodes that reside in a managed network. Managed devices collect and store management information and make this information available to the network management system (NMS) using SNMP. *See* Simple Network Management Protocol (SNMP).
- management information base (MIB).** A collection of objects in a database used to manage entities in a network. A NetScaler provides a list of over a thousand variables in a MIB file. *See* Simple Network Management Protocol (SNMP).
- manager.** A device that polls agents for information. Managers can perform passive statistics-gathering, or they can attempt to manage the network actively by setting new values in read-write variables on some hosts. *See* Simple Network Management Protocol (SNMP).
- mapped IP (MIP) address.** An IP address assigned to a NetScaler so that it can communicate with the servers it protects.
- MIB.** *See* management information base.
- monitor.** An entity used by a NetScaler to periodically check the health of a service to determine its state and to mark it UP or DOWN accordingly.
- MySQL.** A multi-threaded, multi-user SQL database management system (DBMS). The basic program runs as a server providing multi-user access to a number of databases.
- NetScaler IP (NSIP) address.** A management IP address assigned to a NetScaler, used by administrators to connect to the NetScaler when configuring or managing it.
- NetScaler operating system (NetScaler OS).** An operating system that runs on all products in the Citrix NetScaler Application Delivery product line.
- network interface.** A point of interconnection between a user terminal and the network. In reference to hardware, any device that permits connection to an external network. In reference to software, a routine formats packets at the network layer into packets that specific network adapters can read and transmit.
- network layers.** Categories that define the protocols and types of traffic that a network device handles. For example, a Layer 3 device handles IP traffic that conforms to either TCP/IP or UDP protocol. A Layer 2 device handles MAC address traffic.
- network news transfer protocol (NNTP).** An Internet application protocol used primarily to read and post netnews articles and transfer news among news servers.
- node.** A single server, appliance, or device within a network.
- node property.** An attribute of a node, such as its IP address, host name, or domain.

- nslog.** A propriety binary format that a NetScaler uses to record system events in more detail than in the syslog format. *See* syslog.
- nsroot.** The root user with full administrative privileges on a NetScaler.
- object identifier (OID).** The name of an object in an MIB database.
- one-arm mode.** A deployment scenario in which two NetScaler units are installed in a single subnet environment. The units are in a high availability (HA) setup. In this type of deployment, the client must access the servers through a VIP address configured on the NetScaler. *See* virtual IP address (VIP).
- operator.** The portion of an expression that specifies exactly what part of the qualifier the NetScaler should examine and what type of information it should look for. *See* expression.
- packet.** The basic unit of data routed between an origin and a destination on a TCP/IP or other packet-switching network. A packet contains part of a larger message and the destination address. On TCP/IP networks, packets are often called *datagrams*.
- packet switching.** A process for transmitting a message from one server to another on a network by dividing the message into smaller units, or packets, before sending them.
- persistence groups.** An aggregate of vservers. When persistence is set on the group of vservers, client requests are directed to the same selected server, regardless of which vserver in the group receives the client request.
- ping.** A network tool used to test whether a particular host is reachable using an IP address. The source host sends *echo request* packets to the target host and listens for *echo response* replies. Ping estimates the round-trip time, usually in milliseconds, records any packet loss, and prints a statistical summary when finished.
- policy.** A set of parameters created by the system administrator when configuring NetScaler traffic management features.
- port.** In reference to hardware, a server interface that connects to another server or network device. In reference to software, a number representing a virtual input location where a server program listens for connections.
- post office protocol version 3 (POP3).** A client/server protocol that enables an Internet server to receive e-mail and store it. Provides for periodically checking mail boxes on the server and downloading any mail.
- predefined roles.** A set of preconfigured command policies, which can be bound without any need for additional configuration.
- priority queuing.** A feature that uses set policies to prioritize users and tasks so that a NetScaler can give priority access to the most urgent tasks.
- protocol.** A specific type of communication between a server and client or two servers on the Internet.
- public-key encryption.** A method of encrypting messages that pairs a public key and a private key. Messages encrypted with the public key can be decrypted only by using the private key. In turn, messages encrypted with the private key can be decrypted only by using the public key.
- public-private.** A NetScaler deployment scenario in which the IP addresses of the servers managed by a NetScaler are hidden. This scenario is accomplished by placing the servers on non-routable IP subnets.
- public-public.** A NetScaler deployment scenario in which the servers managed by a NetScaler are on a publicly routable IP subnet.
- qualifier.** The portion of an expression that specifies what is to be examined.
- read-only.** A default role that allows read-only access to all show commands except for the system command group and ns.conf show commands.
- remote authentication dial-in user service (RADIUS).** An AAA (authentication, authorization, and auditing) protocol that controls access to the network resources. Used by ISPs and other companies that manage access to Internet or internal networks over an array of access technologies including modem, DSL, wireless, and VPN.
- remote procedure call (RPC).** A technology that allows one program to cause a subroutine or procedure to execute in a different address space within a network without understanding network details.
- request.** An inbound connection from a user to a Web server.

- response.** An outbound connection from a Web server to a user in response to a request sent by that user.
- reverse NAT (RNAT).** A method that a NetScaler uses to translate network addresses by replacing the source IP addresses of packets generated by the servers and replacing them with NAT IP addresses. The NAT IP addresses is a public IP addresses.
- rewrite.** A feature providing general purpose HTTP header modification. When configured, the rewrite feature modifies the header and body sections of an HTTP request or response.
- root certificate.** An unsigned public key certificate, or a self-signed certificate that is part of a public key infrastructure scheme. *See* Secure Sockets Layer (SSL).
- round robin.** A load balancing method that distributes traffic based on a server rotation system, regardless of load. *See* load balancing.
- rule-based persistence.** A persistence method in which a NetScaler compares a client request to a configured rule and creates a persistent session if the request is matched.
- Secure Shell (SSH).** A protocol that allows a user to establish an encrypted, secure connection to a server through port 22.
- Secure Sockets Layer (SSL).** A standards-based security protocol for encryption, authentication, and message integrity. Used to secure the communications between two systems across a public network, authenticate the two systems to each other based on a separate trusted authority, and ensure that the communications are not tampered with. SSL supports a wide range of cipher suites. The most recent version of SSL is Transport Layer Security (TLS).
- Secure Sockets Layer Virtual Private Network (SSL VPN).** A virtual private network that operates through an SSL Web link on port 443.
- security model.** The underlying reasoning used to protect the security of a server or any other computer or appliance on a network.
- server.** A Web server managed by a NetScaler.
- server certificate.** A copy of the server public key that is signed by the private key of the certificate authority and contains information about the server that allows a client to identify the server before sharing sensitive information. A server certificate is unique to a particular server FQDN. *See* Secure Sockets Layer (SSL).
- server farm.** A group of servers.
- server/application state protocol (SASP).** Provides a mechanism for load balancers and workload management systems to communicate in better ways of distributing the existing workload to the group members. This memo provides information for the Internet community.
- service.** A NetScaler entity that represents applications on a server. While services are normally combined with vservers, in the absence of a vserver, a service can still manage application-specific traffic.
- service groups.** A representation of one or more services. *See* services.
- service weight.** A metric that an administrator can use to manage load balancing decisions more closely. Also called a *priority*. *See* load balancing.
- session.** A single set of connections between a Web site and a specific user, including requests from the user to the Web site and responses by the Web site to the user.
- session initiation protocol (SIP).** An application-layer signaling protocol that is used to establish, modify, and terminate sessions with one or more participants in a network.
- session timeout.** The maximum period of inactivity before the Application Firewall stops tracking a user's session. The user must then establish a new session with the protected site by accessing a Start URL before continuing the activity.
- simple expression.** A type of expression that consists of a single logical comparison.
- Simple Network Management Protocol (SNMP).** A standard means of receiving important information from a network device by either polling variables—called *object identifiers (OIDs)*—or receiving alerts—called *traps*.

- simple network time protocol (SNTP).** An adaptation of the Network Time Protocol (NTP) that is used to synchronize computer clocks on the Internet when the ultimate performance of the complete NTP implementation described in RFC 1305 is not needed or justified.
- simple object access protocol (SOAP).** An XML-based syntax for exchanging messages. Using SOAP, Web services on different platforms with normally incompatible technologies can exchange information.
- SSL client certificate verification.** A feature that verifies the authenticity of the user requesting Web object or resource. Web access can be logged and billed on a per user basis. *See* Secure Sockets Layer (SSL).
- SSL offload.** A feature that transfers SSL encryption and decryption tasks from the managed servers to a NetScaler. *See* Secure Sockets Layer (SSL).
- subnet IP (SNIP) address.** An IP address, on the NetScaler, used to originate traffic to services, perform NAT translation, and provide management access (optional).
- superuser.** A default role that grants full system privileges, which are exactly the same privileges that belong to the nsroot user.
- SureConnect.** A feature that provides users with real-time estimates of Internet response times, interactive priority queuing, and guaranteed content delivery.
- surge protection.** A feature that regulates the opening of new connections to servers and controls the number of clients that can simultaneously access the resources on those servers. Queues any additional requests once the servers have reached their capacity.
- syslog.** A format for logging system events.
- TCP buffering.** A feature that breaks the dependencies between the client and server connections, increasing transaction management performance. Because the server-side network has better bandwidth and less packet loss than the client network, the NetScaler can process the entire response faster than can the client. The system buffers the server response and delivers it to the client at the client's speed, enabling faster server offload. TCP buffering is disabled by default.
- TCP optimization.** A feature that transfers certain TCP protocol overhead from the managed servers to the NetScaler, reducing CPU load on managed servers and improving performance. Part of the TCP optimization on a NetScaler includes TCP multiplexing. TCP multiplexing maximizes server efficiency by consolidating application level requests, reducing the number of times that server connections are made.
- threshold.** The absolute number of times a behavior occurs on a protected site, and the percentage of total Web site connections that exhibit this behavior, before the Adaptive Learning feature learns a particular pattern or rule.
- transmission control protocol (TCP).** A core Internet protocol that provides reliable, in-order delivery of a stream of bytes, and makes it suitable for applications like file transfer and e-mail.
- Transport Layer Security (TLS).** *See* Secure Sockets Layer (SSL).
- trap.** An alert sent by an SNMP agent to the manager. This is the only type of communication initiated by an agent.
- two-arm mode.** A NetScaler deployment scenario in which two NetScaler units are installed in a two-arm configuration on a single subnet. The units are in a high availability setup and are placed between two Layer 2 switches.
- Uniform Resource Locator (URL).** A standard address for an HTML page or other resource on the Web.
- URLPassive persistence.** A type of persistence in which the NetScaler extracts the server ID from the server response and embeds it in the URL query of the client request. The NetScaler extracts the Server ID from subsequent client requests and uses it to select a server.
- use subnet IP (USNIP) mode.** A mode that allows a NetScaler to use an appropriate subnet IP address as the source IP address for all packets originating from the system.
- user datagram protocol (UDP).** A protocol used by application programs to send messages to other programs with a minimum of protocol overhead. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed.
- value.** A field within an expression that specifies with what the qualifier is compared.

- virtual IP (VIP) address.** An IP address associated with a virtual server.
- virtual LANs (VLANs).** A group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location.
- virtual MAC (VMAC).** A floating entity that is shared by the primary and secondary nodes in a high availability setup.
- virtual private network (VPN).** A method of tunneling secure communication through the Internet or a different network.
- virtual server (vserver).** A NetScaler entity that represents one or more applications in a server farm. External clients can use vservers to access applications hosted on the servers. It is represented by an alphanumeric name, virtual IP address (VIP), port, and protocol.
- Web application.** An application that is accessed with a Web browser over a network, such as the Internet or an intranet.
- Web server.** A system that delivers Web pages to browsers, and delivers other files to applications, using Hyper Text Transfer Protocol (HTTP).
- Web service.** Web-based content that employs one or more of three technologies— SOAP, WSDL, and UDDI—to offer structured content to users through the Web.
- Web Services Definition Language (WSDL).** An XML-based language for defining Web services and explaining how to access those services.
- Web site.** A collection of content hosted on a single Web server and accessed through a single host name.
- wide area network (WAN).** A network that covers a large area, most of which is outside a company's firewall or router but has access to the company's resources. WANs are used to connect local area networks (LANs) to other types of networks, so that users and computers in one location can communicate with users and computers in other locations.
- wildcard.** The * character used within an expression to match the string within the specified qualifier.
- XML.** A text markup language that supports interchange of structured data. A subset of SGML. The Application Firewall protects a subset of XML-based Web content called Web services.