

Network Appliance® Internet Access and Security Solution

Value Summary

Most organizations, when they first enabled Internet access for employees, deployed firewalls and, in many cases, proxy software on general-purpose servers as a means of providing some measure of security and performance. The Network Appliance solution:

- Reduces costs over 75% by replacing legacy proxy servers such as Netscape®, Microsoft®, or Squid; scaling firewalls; and preventing downtime based on customer surveys and analysis, largely due to higher reliability¹
- Increases security, by controlling access, blocking viruses and malicious code such as Nimda and Code Red, and filtering inappropriate content

Common Challenges

Internet access has become a vital business tool. The points at which an organization's internal network connects to the Internet are commonly called Internet gateways. Since fast access to information is critical to user productivity, the reliability and performance of the gateways are extremely important. An organization may have one or many of these gateways to the Internet, depending on size, geography, and user requirements. It is most common to have only a few main Internet gateways through which all employees access the Internet. Each gateway must be sized and configured to deliver Web pages to users at an acceptable speed while keeping the internal network secure from viruses and other concerns.

As Internet usage has grown, organizations that needed to scale access have added bandwidth, firewalls, and/or proxy servers. In addition, higher usage and more widespread security concerns have caused many organizations to install content-filtering and/or virus-scanning software on firewalls or standalone servers.

Challenges have arisen because legacy proxy servers such as Netscape, Microsoft, and Squid can be slow and unreliable; may have security holes in the application and/or on the server OS; and lack the breadth of features organizations need today. Several of these are no longer supported at all, and staying with them can lead to higher costs of administration, productivity loss, and security risks due to growing threats such as Nimda and Code Red.

An increasing number of organizations have addressed these cost and security issues by deploying complete, integrated solutions that address:

- Administration time and costs
- Growing Web security risks, including viruses and other malicious code (SoBig, Bluster, spyware)
- Infrastructure reliability and scalability
- Installation and management simplicity
- Flexible authentication requirements
- Support for all content types (Web, SOCKS, SSL, streaming media, Java™, FTP, NNTP, etc.)

INTERNET ACCESS AND SECURITY

Network Appliance storage solutions let you leverage information as competitive advantage, making data available, whenever, wherever, driving productivity all the way out to your branch and remote offices from the central office.

Solution Description

The Network Appliance Internet access and security solution includes:

- Highly reliable NetCache® appliances
- Integrated software for content filtering, virus scanning, usage reporting, and more

When using the Internet, content is often repeatedly requested from the same Web sites. This creates redundant traffic through the gateway. NetCache stores and serves copies of this redundant content, reducing network load and delays.

In addition to caching, since NetCache “sees” all the Web content coming through the Internet gateway, it is an ideal platform to use for:

- Access control and authentication integration
- Content security management, including filtering, virus scanning, and more
- Usage reporting

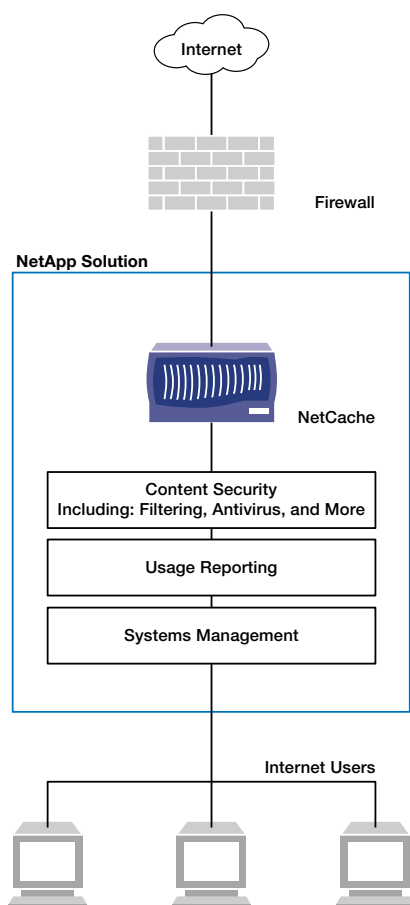


Figure 1) NetApp Internet access and security solution functional diagram.

Product Description

NetCache appliances. Store, deliver, and control access to the Web and applications to speed delivery and manage access; maintain measured, installed appliance reliability of over 99.99%.²

- *Access control lists (ACLs)* allow powerful access rules to be created to improve security and productivity. Rules can be applied across the organization or for employee groups, to manage who can access which sites at what times. ACLs can be integrated with filtering software and applied to each filtering category. ACLs can also block malicious code such as Nimda and Code Red.
- *Authentication support* ensures that the NetApp solution integrates simply and easily with an organization's existing security infrastructure. NetCache supports all major authentication methods, including NTLM, Kerberos for Windows® 2000, Radius, and LDAP.

Content-filtering software. On-box lists include Secure Computing's Smartfilter, Websense's Enterprise, and Webwasher's DynaBLocator. Off-box ICAP-enabled software includes Trend Micro's InterScan Web Security Suite (IWSS), Websense's Enterprise, and Webwasher's Content Security Management (CSM) Suite.

- *Content filtering* improves security and productivity by preventing access to unwanted Internet content. Features include URL filter lists as well as options to block banners and pop-up ads and executable files.

Virus-scanning software. Off-box ICAP-enabled software includes Symantec's AntiVirus Scan Engine, Trend Micro's IWSS, and Webwasher's CSM Suite.

- *Virus scanning* prevents viruses and malicious code from entering the corporate network. The software examines each Web object, strips viruses, then notifies NetCache that the object is now safe to serve to users. ICAP integration delivers higher virus-scanning performance compared to standalone antivirus servers.

Usage reporting software. Webwasher's ContentReporter™ runs on a separate server.

- *Usage reporting* allows administrators to analyze traffic load patterns, track Web surfing, and enable capacity planning.

For a full list of partners, their status, and key contacts, contact NetApp content delivery marketing.

For more information about NetApp Internet security offerings, see this white paper:

www.netapp.com/tech_library/3236.html.

Business Benefits

Cost Savings

- Reduce TCO up to 75% by replacing proxy servers, even freeware-based servers
- Increase uptime to months or years
- Scale firewall deployments

Improved Security

- Manage usage with integrated access controls and authentication support
- Filter objectionable Web sites and ads
- Keep network available by blocking viruses, malicious code, spyware, and other threats

Comprehensive, Integrated, Scalable Solution

- Combat security risks caused by growing Internet usage
- Provide foundation for an integrated Web and application delivery system to accelerate applications, streaming video, and more, as access to information becomes a growing challenge in remote locations

Service Overview

With the expertise to help your business, NetApp delivers global, enterprise-class services and support to help ensure your long-term success, free up your internal resources, minimize disruption, and maximize uptime. NetApp offers services and support programs to complement every phase of the solution, from evaluation within your environment to installation, including services to maximize your return on investment throughout the life of your systems.

One example is the NetApp Internet Traffic Assessment, which gives insight into employee Internet usage and identifies the related vulnerabilities and risks.

Customer Examples

NetApp was the first to integrate caching and content filtering and has deployed the solution to hundreds of customers, including Ford Motor Company, Lehman Brothers, Motorola, the Singapore Ministry of Education, and the U.S. Army.

The Network Appliance Content Delivery Business Unit (CDBU) delivers solutions to improve access to information in a cost-effective, secure manner, based on a true appliance architecture that scales across a wide variety of applications.

Unleash the Power of Information

See how Network Appliance can bring data management and content delivery solutions to your enterprise network. Visit our Web site at www.netapp.com and let us show you what “The evolution of storage™” can mean for your business.

¹ IDC White Paper: *Quantifying the Business Benefits of Appliance-Based Internet Access and Security Solutions*, Lucinda Borovick, April 2003

² NetApp Engineering, 2003



Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089
www.netapp.com

© 2004 Network Appliance, Inc. All rights reserved. Specifications subject to change without notice. NetApp, the Network Appliance logo, and NetCache are registered trademarks and Network Appliance and The evolution of storage are trademarks of Network Appliance, Inc. in the U.S. and other countries. Netscape is a registered trademark of Netscape Communications Corporation. Microsoft and Windows are registered trademarks of Microsoft Corporation. Java is a trademark of Sun Microsystems, Inc. ContentReporter is a trademark of webwasher.com. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such **IA-001 0904**