Internet Access and Security Solution:

Description of Security Features and Benefits

Tobin Sears, Network Appliance, May 2006, TR-3236

Table of Contents

1. Introduction

Most organizations today use the Internet as a valuable business tool and depend upon it for their livelihood. However, that same Internet access exposes corporate resources to an ever-increasing number of security vulnerabilities. Whenever data is transferred between a company's internal network and an outside source, there are multiple risks—all of which can jeopardize data integrity. Many vendors offer disparate technologies to protect against these security risks. Only Network Appliance, however, has combined these technologies into a complete, integrated solution for securing Internet data access. This document summarizes these security features and describes their benefits as part of the overall solution.

2. Internet Security Challenges

Threats to corporate networks are growing every day. In fact, companies typically create IT departments specifically dedicated to managing and protecting against network security risks. Examples of today's security challenges include but are not limited to:

- Protecting data from viruses, spyware, and worms introduced into the network via downloaded files and e-mail attachments, at times prompted by phishing attempts
- Controlling access to business-sensitive data by internal and potentially external users; unauthorized access to protected data can result in legal issues and the loss of trade secrets
- Protecting corporate Web sites running on general-purpose operating systems from denial of service (DOS) attacks and service exploits both of which can render them inaccessible and unusable
- Preventing the exploitation of Internet access privileges by employees
- Preventing employees from visiting malicious sites through deceptive hyperlinks
- Preventing Internet users from drive-by-download applications, which attempt to compromise sensitive data by allowing the attacker to log keystrokes, steal cached passwords, and download files, exposing confidential information

The NetApp® Internet Access and Security solution consolidates the deployment and administration of many security technologies into a complete security solution for Web access, alleviating the aforementioned vulnerabilities and lowering management costs.

3. NetApp Solution Components

The components of the NetApp solution include:

- NetCache® content delivery appliances, which incorporate caching, authentication, access control, and policy management into one secure platform
- URL filtering software, which enables URL- and IP-based filtering by category
- Virus-scanning software to block executables, worms, and other threats
- Content filtering and inspection to protect against potentially harmful content present in common media types such as archive files, embedded objects, Active X, digital signatures, and business documents
- Usage-reporting software to help analyze traffic and load trends

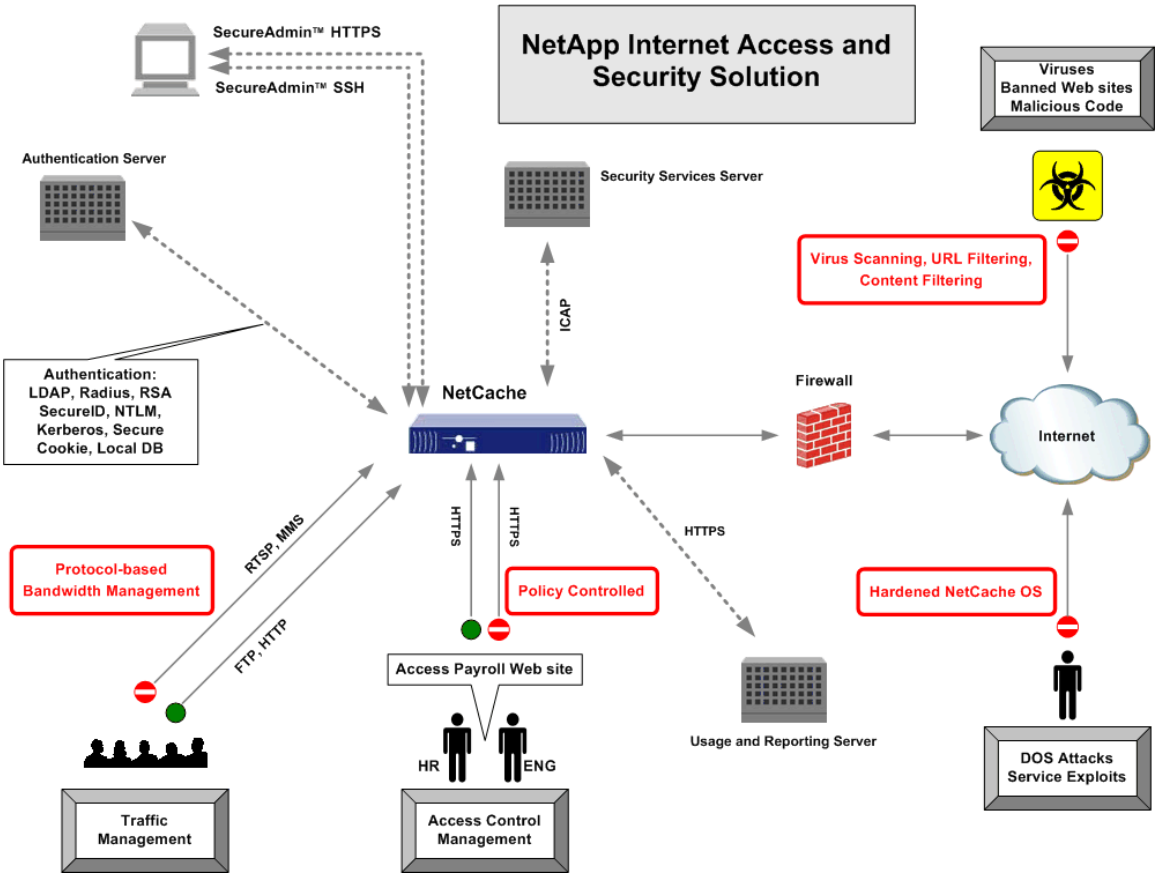

Figure 1) Network Appliance Internet Access and Security solution functional diagram.

4. NetCache Appliance Security Features

4.1. Appliance-Based

The NetCache appliance is a single-function appliance for Web security. It provides greater flexibility in terms of security features and controls, device management functionalities, and better performance through optimized hardware and operating system over similar solutions that are installed on general-purpose operating systems.

4.2. Hardened TCP Stack

NetCache appliances are built on Data ONTAP®, the same proprietary OS that runs on all Network Appliance™ devices. Data ONTAP was designed from the ground up to be simple, fast, and reliable.1 Unlike general-purpose operating systems that constantly require upgrades and patches in response to newfound exploits, Data ONTAP is specifically hardened against DOS attacks and has no known service exploits.

4.3. Authentication

NetCache offers extensive authentication support for easy integration into existing RADIUS, RSA SecureID, LDAP, NTLM, Kerberos, and SSO authentication environments. Users and groups can be authenticated by using any of the above methods, as well as the built-in appliance user database. Once a user is authenticated for a configured protocol, a multi-step process is performed before the request is fulfilled.

4.4. Access Control Policy (ACP)

4.4.1. Building an Access Control Policy

Administrators can control access to network resources by implementing policies through access control policy. Typical ACP usage includes but is not limited to:

- Controlling client requests for access to protocols (request-side policy)
- Controlling whether to direct a server response to a client (response-side policy)
- Controlling user and group access to the Internet
- Imposing restrictions inside the intranet domain

An ACP rule is constructed by combining an action with an expression. An expression can be a single variable or a combination of variables and values. Table 1 shows some examples of NetCache actions and variables. Table 2 shows how an expression is formed using variables and values.

DESCRIPTION	EXAMPLES
Actions Actions control client requests for access to Web content and supported protocols.	allow, auth, cache, deny, drop, icap, nolog, redirect, rewrite
Variables Variables, including those specific to streaming media, are used to create pattern-matching expressions.	accel, cache-ip, client-domain, client-ip, client-port, user, group, server-domain, server-ip, time, url, smartfilter, wsfilter, wwfilter

Table 1) ACP actions and variables.

TYPE	DEFINITION	EXAMPLE
Single predicate	<variable>	FTP
Variable-value pair	<variable> <value>	client-ip 128.48.37.17
Range matching	<variable> <value> - <value>	server-port 1 - 1024
Regular expression matching (regex)	<variable> matches <regex>	url matches "^http://[0-9.]+/redcodeworm.asp\?X+"

Table 2) ACP expressions.

The following is an example of a simple rule:

```
<action> <variable-value expression>    deny wwfilter sex
```

4.4.2. Lists and Macros

A list groups a common set of variables under a list name, which is referred to in the policies. A macro is a set of rules that represent an enterprise business policy for controlling access to services. The following set of rules is an example of macro and list working together to represent an enterprise antivirus scanning policy:

Lists

```
enterprise_filers : server-ip = {
    10.10.10.100,
    10.10.20.100,
    10.10.30.100
}
trusted_domains : server-domain = {
    “mycorp.com”,
    “myintranet.com”
}
```

Macro

```
anti_virus_scan_policy {
    allow server-ip in enterprise filers
    allow server-domain in trusted_domains
    icap (virus_scan)
}
```

Rule

```
auth http
if (group "all") anti_virus_scan_policy
deny ftp
```

This set of lists, macros, and rules forms an enterprise virus-scanning policy that can be stated as follows:

- Authenticate all HTTP requests with one of the configured databases.
- For all downloads other than matching the server IP address in the “enterprise_filers” list and server domains in the “trusted_domain” list, the contents are scanned via the ICAP server. It is assumed that the files stored in the servers have already been scanned for viruses.
- Deny any FTP request.

4.5. Integrated SSL Termination

NetCache supports SSL termination for both intranet (forward proxy)[2] and Web site (reverse proxy)[3] acceleration deployment scenarios. In both instances, NetCache retains a copy of the central server's certificate and private keys; both are required to terminate connections and decrypt the data for storage. Integrated SSL termination allows NetCache to decrypt, cache, and serve objects that are common between unique client sessions, while maintaining its own secure connection back to the origin server for request

resumption. These benefits equate to a decrease in bandwidth utilization, end-user latencies, and origin server load.

4.6. Secure Administration

NetCache can be securely administered using the SSH (Secure Shell) and SSL (Secure Sockets Layer) protocols.

SSH provides an encrypted administrative exchange between the appliance and an SSH 1.X- or 2.X-compliant client. SSH replaces Telnet and RSH clients and provides a confidential channel for administering NetCache in a nontrusted environment. SecureAdmin SSH uses a public key encryption algorithm for server authentication and session key encryption.

The SSL protocol is used for secure data transmission. SSL ensures confidentiality by using an RSA public key encryption algorithm in combination with self-signed or CA (Certificate Authority) signed certificates. NetCache can act as both an SSL server and an SSL client. SSL allows secure administrative access to the admin port and allows the secure transfer of files to and from the appliance.

4.7. Bandwidth Management

NetCache has an integrated bandwidth-allocation engine that lets the user create and define bandwidth-allocation rules based on protocol. Sets of bandwidth-allocation rules can be combined to form bandwidth policies that help organizations to guarantee a certain level of service for a given protocol. For example, in order to guarantee that an organization's network is not overpowered by streaming media during a Webcast, one could configure a bandwidth-allocation rule limiting the amount of streaming media that can be viewed through the cache during the hour of the broadcast. Rules can be configured for the following protocols and protocol categories: ICMP, IP, TCP, UDP, HTTP, NFS, NNTP, RTSP, MMS, FTP, streaming, and content distribution. Some of the filtering options applicable to a rule include user, group, IP (source/destination), time of day, and URL-based ACP triggers.

4.8. Secure Log File Pushing

Detailed access and usage logging is available for all NetCache-supported protocols. Log files can be securely transferred to an HTTPS server, where they can be used in conjunction with log analysis software to analyze network usage, monitor Web access, and estimate future infrastructure requirements.

5. Third-Party Software Security Features

5.1. Virus Scanning

NetApp supports content virus scanning through its security partner solutions,[4] which incorporate virus scanning engines like Sophos®, McAfee®, and Computer Associates®. Additionally, NetCache supports other virus scanning engines like Trend Micro® and Symantec® via the Internet Content Adaptation Protocol (ICAP)[5]. ICAP is a lightweight, HTTP-based remote procedure call protocol designed to allow dedicated content-modification servers, such as virus scanners, to integrate with caching devices for higher overall performance. Once a file is passed to a dedicated virus-scanning server, the scrubbed data is returned to the NetCache appliance, where it is cached for subsequent user requests. NetApp partner virus-scanning offerings protect against a wide range of Web and e-mail based threats, including executables, Java™, ActiveX, cookies, embedded objects, and active scripts.

5.2. URL and Content Filtering

Access to specific Web sites or Web-site categories can be controlled by using URL filtering solutions from NetApp security partners like Secure Computing®, Websense®, and Webwasher®. Filtering categories can be combined with NetCache ACP to fine-tune access permissions, such as making exceptions to the policies configured for entire content-filtering categories. This enables administrators to control different levels of Internet access for different groups of users.

Additionally, NetCache offers an extensive set of Internet content filters through its partner solutions to help protect network and business resources. Some of the filters[6] included are:

- Archive Handler: Opens archive files (for example, .zip and .gzip) so that other filters can be applied to the contents of the archive. Also applies to archives with recursive hierarchies.
- Media-Type filters: Manage the bi-directional flow of inbound and outbound media in such forms as mp3s, mpegs, sales data, and classified information.
- Security filters: Detect embedded objects and media types such as JavaScript, macros, and ActiveX content.
- Advertising filters: Eliminate pop-up windows, banner ads, scripts, applets, Flash animations accompanying Web pages, and URLs.
- Privacy filters: Offer protection from cookies, Web bugs, and referrers.
- Customer categories[7]: Added for more granular control for URL filtering.
- Coaching[8]: Provides an information page and then allows or blocks access.

5.3. IM and P2P Filtering

NetCache ACPs, combined with content filtering solutions from security partners[9], can provide another layer of protection against dynamic threats like IM and peer-to-peer (P2P) traffic within the enterprise. The solution detects, reports, and selectively blocks the unauthorized use of high-risk and evasive P2P file sharing and public instant messaging (IM) from enterprise networks.

For more information, see the NetCache Technical Advisory “Controlling P2P Traffic.”[10]

5.4. Spyware Protection

NetCache provides preventive actions to protect against spyware, which is generally a software program that gets installed on a PC either through freeware applications or through drive-by downloads without the knowledge of the user. The installed application mainly aims at collecting user keystrokes (Keyloggers), installs other malicious application (modular malicious code), allows an unauthorized user to control the user’s desktop remotely (Bots), and many other malicious functionalities. NetCache, combined with its security partner9 solutions, blocks known spyware sites through URL filtering and implements digital signature verification, heuristics scanning, and exploit methods for all files that get downloaded, stopping the threat at the edge of the network.

For more information, see the NetCache Technical Advisory “Spyware/Adware: A Serious Security Threat to Your Company.”[11]

5.5. Phishing

The NetCache URL filtering feature blocks users from visiting phishing sites, which use deceptive hyperlinks to hijack the user to malicious sites in order to collect confidential information, such as credit card and bank account details.

5.6. Usage Reporting

All the security partner[9] solutions are bundled with software that provides usage reporting and analysis based on information from NetCache and content filtering logs. The software aggregates log into a database, generate reports, and can distribute those reports via e-mail. The reports can include colorful usage charts and can be based on custom queries. Log collection, report generation, and report distribution can all be automated.

6. Summary

The NetApp Internet Access and Security solution plays a fundamental role in controlling access to information. The solution's ability to integrate into existing security architectures allows organizations to gain greater control over their network access and usage while minimizing implementation and management costs.

[1] http://www.netapp.com/tech_library/3001.html
http://www.netapp.com/tech_library/3002.html
http://www.netapp.com/tech_library/3014.html

[2] In a forward-proxy deployment, the NetCache appliance acts as a client accelerator, intercepting and making requests for content on behalf of the client. Internet gateway deployments, for example, are typically in forward-proxy mode.

[3] In a reverse-proxy deployment, the NetCache appliance acts as a server accelerator, servicing client requests on behalf of the server. Web acceleration helps to offload busy Web servers and adds a layer of protection between the server and clients.

[4] The Webwasher CSM™ suite incorporates virus scanning engines from McAfee and Computer Associates

[5] For more information on ICAP, visit www.i-cap.org.

[6] All the filters listed are supported through the Webwasher off-box solution.

[7] Supported also through the Secure Computing off-box solution.

[8] Supported also through the Secure Computing off-box solution

[9] Security partners: Secure Computing, Websense, and Webwasher

[10] http://www.netapp.com/library/tr/3333.pdf

[11] http://www.netapp.com/ftp/spyware-security-threat.pdf

[12] Symantec Internet Security Threat Report, March 2006: http://www.symantec.com/enterprise/threatreport/index.jsp