

# Mitigating the SANS/FBI Top Twenty with Check Point Software Technologies

## In this Document

### 1 Introduction

### 2 Top Vulnerabilities to Windows Systems (W)

W1: Internet Information Services (IIS)

W2: IIS RDS exploit (Microsoft Remote Data Services)

W3: Microsoft SQL Server

W4: NETBIOS - Unprotected Windows Networking Shares

W5: Anonymous Logon — Null Sessions

W6: LAN Manager (LM) Authentication — Weak LM Hashing

W7: General Windows Authentication Accounts with No Passwords or Weak Passwords

W8: Internet Explorer

W9: Remote Registry Access

W10: Windows Scripting Host

### 3 Top Vulnerabilities to Unix Systems (U)

U1: Remote Procedure Calls (RPC)

U2: Apache Web Server

U3: Secure Shell (SSH)

U4: Simple Network Management Protocol (SNMP)

U5: File Transfer Protocol (FTP)

U6: R-Services — Trust Relationships

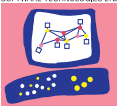
U7: Line Printer Daemon (LPD)

U8: Sendmail

U9: BIND/DNS

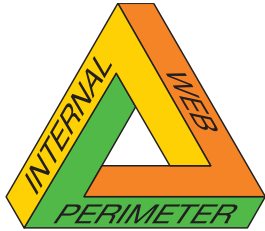
U10: General Unix Authentication — Accounts with No Passwords or Weak Passwords



Check Point  
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

## Introduction



## Intelligent Security

In July of 2000, the SANS Institute ([www.sans.org](http://www.sans.org)) published a document that detailed the top ten most critical Internet security threats. This listing has since been through two major revisions. The current version, published in combination with the FBI and the National Infrastructure Protection Center (NIPC), now includes a list of twenty critical vulnerabilities — ten each for Windows- and Unix-based systems. The current list is available from SANS at <http://www.sans.org/top20/>.

The majority of successful attacks on computer systems via the Internet can be traced to exploitation of the well-known set of security flaws. The SANS/FBI list details the vulnerabilities and provides instructions for mitigating them. Addressing these vulnerabilities significantly improves the security of an organization's network infrastructure.

While the steps outlined in the list would in theory protect organizations from attack, the reality is that many systems remain vulnerable. The reasons for this vary. Usually, in order to mitigate the wide range of vulnerabilities, administrators must deploy many tools and use different techniques, based on different technologies. Deployment of software across possibly hundreds of systems is difficult and very time-consuming. Further, sometimes patching systems causes conflicts with applications or other parts of the infrastructure; sometimes security administrators lack either the time or the expertise to properly configure systems; and sometimes new systems are simply overlooked. But the results of an exposure can be dramatic. SANS cites three prominent security incidents — the Solar Sunrise incident, the Code Red worm, and the NIMDA worm — as examples of exploits that took advantage of vulnerabilities on the Top Twenty list.

Check Point's Intelligent Security Solutions for Perimeter, Internal and Web Security provide a foundation for defending against the threats posed by these vulnerabilities. Check Point's approach to mitigating the SANS/FBI Top Twenty vulnerabilities is based on a multi-layered approach comprised of perimeter firewalls, internal and single-server firewalls, strong user authentication and active defense solutions that identify and block network-based attacks. These elements are combined with integrated management from a central console to provide the capability to quickly meet new security challenges. An important aspect of this approach is the ability to offer security without losing connectivity; blocking an essential service to protect against a specific attack is rarely an acceptable solution.

The remainder of this paper outlines how to approach each of the SANS/FBI Top Twenty critical Internet vulnerabilities using Check Point solutions. Readers will notice that the content of the vulnerability summary sections is based on the SANS/FBI Top Twenty list. These summaries are not intended to replace the detailed information readers will find there. For a complete, updated version of the SANS/FBI Top Twenty list, visit <http://www.sans.org/top20/>.

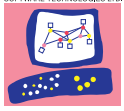
An important note to the defenses described below is that they are not intended to replace the steps outlined in the SANS/FBI Top Twenty list, but rather to supplement those steps and provide a layered defense approach to maximize the level of protection. One of the challenges addressed by the SANS/FBI Top Twenty list is the sheer number of vulnerabilities and the potential complexity of implementing appropriate mitigating measures for each. While the SANS/FBI Top Twenty list goes a long way in helping administrators to identify vulnerabilities and understand the steps needed to mitigate them, the problem of implementation remains. Properly applying system patches and software version updates can be a difficult and time-consuming task. Human interaction with the systems can introduce error into this process and often results



Intelligent Security

Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

in overlooked or misconfigured systems. In addition, it is not uncommon for system administration windows to be short compared to the time required to apply security updates. A layer of security that can be managed from a central point can buy administrators time to properly configure systems and help to mitigate the dangers of human error in the configuration process.

## Top Vulnerabilities to Windows Systems (W)

### W1: Internet Information Services (IIS)

#### Summary

The SANS list describes three major categories of vulnerabilities for IIS web servers: failure to handle unanticipated requests, buffer overflows, and sample applications. These flaws are susceptible to a variety of attacks that can cause damage ranging from denial of service to an attacker gaining complete control of the web server.

#### Challenges

Protecting IIS requires a hardening procedure, as well as the application of a list of patches to the server software. At any given time, these patches can generally be applied via a cumulative roll-up of previous updates. Staying current with the most recent security updates is a critical part of securing IIS and can be a time-consuming effort. Also, since many of the vulnerabilities have to do with the default IIS configuration, installation of new IIS instances can also be time-consuming.

#### Check Point's Solution

FireWall-1® includes multiple security tools that are designed to protect web servers and web applications:

- Stateful Inspection enforces access control and authorization rules, as well as verifying HTTP protocol integrity.
- SmartDefense™ includes a pattern-matching capability that can block requests designed to exploit each of the three broad categories of IIS vulnerability (failure to handle unanticipated requests, buffer overflows and sample applications). HTTP WormCatcher matches requests to patterns defined by regular expressions, making it possible to block requests for malicious URLs (unanticipated requests and buffer overflows). In addition to pre-configured patterns for known attacks, administrators can customize the pattern-matching capability to include new threats or unique requirements (for example, blocking requests for vulnerable sample applications).
- SmartDefense Subscription provides customers with updates to the pre-configured defenses within SmartDefense as new attacks and exploits become known.
- HTTP Security Server can be configured to block different MIME types, as well as strip and weed both scripts and tags. This will help to ensure that dangerous content will not be allowed into the network.

### W2: IIS RDS exploit (Microsoft Remote Data Services)

#### Summary

In older versions of Microsoft Data Access Components (MDAC), one of the components, Remote Data Services (RDS), has a vulnerability that can be exploited by remote users to run commands on the system with administrative privileges. Combined with other flaws, this exploit may also provide external access to internal databases for remote attackers.



Intelligent Security

Check Point  
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

## Challenges

Despite solutions to this vulnerability having been published for over two years, many systems remain unpatched and thus subject to exploitation.

## Check Point's Solution

Check Point's FireWall-1 can be configured to allow access to RDS services for authorized users only. For more information, see FireWall-1 NG SmartDefense Advisory CPAI-2002-15—<http://www.checkpoint.com/techsupport/documentation/smartdefense/cpai-2002-15.html>.

## W3: Microsoft SQL Server

### Summary

Microsoft SQL Server (MSSQL) contains a variety of serious vulnerabilities. By exploiting these flaws, remote attackers can perform a variety of malicious tasks, ranging from obtaining or altering database information to controlling servers hosting the application.

As a result, the default ports for MSSQL (1433 and 1434) are regularly among the most-scanned ports on the Internet as tracked in the Internet Storm Center (<http://isc.incidents.org/>). More detailed information about recent MSSQL exposures can be found in CERT Advisory 2002-22 — <http://www.cert.org/advisories/CA-2002-22.html>.

### Challenges

Properly configuring access control for Microsoft SQL Server can be a time-consuming effort. Some of the exploits take advantage of inherent problems that are related to the system design. In addition, it is sometimes impossible or difficult to alter applications that are based on Microsoft SQL Server.

### Check Point's Solution

The SANS Top Twenty list recommends blocking inbound connections on ports 1433 and 1434. Depending on an organization's needs, this can be a reasonable first step to take. Using FireWall-1, administrators can block SQL traffic at the network perimeter. Not all deployments, however, can reasonably exclude inbound access to SQL Server applications.

For environments in which access to SQL Server applications is required from external sources, Check Point offers a multi-layered solution to mitigate the related security issues.

- FireWall-1's patented Stateful Inspection verifies that MSSQL connections are well formed.
- VPN-1® creates trusted tunnels and authenticates users to secure SQL Server traffic over public networks, preventing attackers from eavesdropping on, or modifying sessions.
- VPN-1 SecureClient's Security Configuration Verification (SCV) capabilities can be used to verify that SQL clients are up-to-date with the most current security patches.

## W4: NETBIOS - Unprotected Windows Networking Shares

### Summary

The Server Message Block (SMB) protocol, also known as the Common Internet File System (CIFS), enables file sharing over networks. Improper configuration can expose critical system files or give full file system access to hostile users. Both the Sircam virus (see CERT Advisory 2001-22 — <http://www.cert.org/advisories/CA-2002-22.html>) and Nimda worm (see CERT Advisory 2001-26 — <http://www.cert.org/advisories/CA-2001-26.html>) exploited aspects of unprotected Windows shares on victimized networks.



Intelligent Security

Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

## Challenges

Properly configuring access control for Windows network shares can be a time-consuming effort. Also, since the list of potentially vulnerable hosts includes both servers and clients, the likelihood of configuration mistakes or other inadvertent violations of security policies is high.

## Check Point's Solution

This vulnerability and the one that follows (W5: Anonymous Logon — Null Sessions) are closely related. For both, the SANS Top Twenty list recommends blocking a range of TCP and UDP ports (135, 137-139, 445) at the firewall. FireWall-1 provides the ability to perform this blocking.

In addition, FireWall-1 can statefully inspect CIFS traffic to enforce access policies based on a variety of network and user characteristics. The result is that administrators can authenticate users and provide access control even for shared files and directories not configured to require authentication.

However, the paper also (correctly) states that most firewall implementations only secure the network perimeter, and so only protect from external attacks and not from internal attacks launched by disgruntled employees, attackers, or malicious programs (e.g. worms) that have gained internal access in some way.

To address the need for securing network shares from internal threats, FireWall-1 gateways can be deployed in front of server farms or specific internal network segments. In addition, FireWall-1 SecureServer™, an instance of FireWall-1 that is installed on a single server, can be deployed to provide an additional, internal layer of security for sensitive servers running Microsoft Networking Services.

## W5: Anonymous Logon — Null Sessions

### Summary

Null sessions, or anonymous logons, allow unauthenticated users to retrieve network information via the SMB/CIFS protocol (see item W4) from other hosts. Typically, this information consists of user names or the names of shared files or directories.

### Challenges

The Windows SYSTEM account often uses null sessions to get information on other machines, making it necessary to allow null sessions to preserve normal (or at least expected) system behavior. An unfortunate side effect is that malicious users can also use null sessions to cull information from the network.

### Check Point's Solution

This vulnerability is closely related to W4.

For both, the SANS Top Twenty list recommends blocking a range of TCP and UDP ports (135, 137-139, 445) at the firewall. FireWall-1 provides the ability to perform this blocking.

In addition, FireWall-1 can statefully inspect CIFS traffic to enforce access policies based on a variety of network and user characteristics. The result is that administrators can authenticate users and systems attempting to access Microsoft Networking Services.

However, the paper also (correctly) states that most firewall implementations only secure the network perimeter, and so only protect from external attacks and not from internal attacks launched by disgruntled employees, attackers, or malicious programs (e.g. worms) that have gained internal access in some way.





We Secure the Internet.

To address the need for securing Microsoft Networking Services from internal threats, FireWall-1 gateways can be deployed in front of server farms or specific internal network segments. In addition, FireWall-1 SecureServer, an instance of FireWall-1 that is installed on a single server, can be deployed to provide an additional, internal layer of security for sensitive servers running Microsoft Networking Services.

## W6: LAN Manager (LM) Authentication — Weak LM Hashing

### Summary

By default, installations of Microsoft NT, 2000 and XP locally store legacy LM password hashes (also known as LANMAN hashes). According to SANS, the hashing algorithm employed is weak, and can typically be broken in under a week's time on standard hardware. As such, passwords could be compromised relatively easily.

### Challenges

Since LM hashes are enabled by default and require pro-active effort on the part of administrators to correct, security models can easily be compromised by overlooked or misconfigured systems.

### Check Point's Solution

Security administrators can deploy FireWall-1 SecureServer, an instance of FireWall-1 that is installed on a single server, to provide granular access control for that server. With SecureServer, administrators can require strong authentication (via, for example, integration with certificates, third-party tokens or smart cards), for access to the server, thus mitigating the potential for damage should LM password hashes be overlooked on a particular server.

To make managing authentication models less complex, Check Point provides several key features and points of integration: Account Management Module integrates FireWall-1 with external Lightweight Directory Access Protocol (LDAP) directories. UserAuthority™ WebAccess requires users to authenticate to a web server and reduces the number of separate logins required ("reduced sign-on").

## W7: General Windows Authentication Accounts with No Passwords or Weak Passwords

### Summary

Many users passwords are not as strong as they should be, making them subject to compromise via dictionary-based password guessing attacks or brute force password cracking.

### Challenges

Setting and enforcing a strong password policy is not an easy task. Users tend to find ways around such policies like using the same password for multiple systems or using simple (and easily guessed) words as passwords. The imposition of character restrictions (such as requiring non-letter or non-alphanumeric characters) often results in users simply substituting different characters for certain letters of common words, which doesn't significantly improve password strength.

### Check Point's Solution

The problems presented by weak passwords are very similar to those related by the default presence of LM password hashes on many Windows-based systems (W6). As such, the mitigation techniques are very similar.



Intelligent Security



We Secure the Internet.

Security administrators can use FireWall-1 SecureServer, an instance of FireWall-1 that is installed on a single server, to provide granular access control for that server. With SecureServer, administrators can enforce password policies as well as require strong authentication (via, for example, integration with certificates, third-party tokens, or smart cards) for access to network resources.

To make managing authentication models less complex, Check Point provides several key features and points of integration: Account Management Module integrates FireWall-1 with external Lightweight Directory Access Protocol (LDAP) directories. User Authority WebAccess requires users to authenticate to a web server and reduces the number of separate logins required ("reduced sign-on").

## W8: Internet Explorer

### Summary

All existing versions of Microsoft Internet Explorer (IE), which is the default web browser installed on Windows platforms, have a range of critical vulnerabilities. According to SANS, the consequences of these vulnerabilities may include disclosure of cookies, local files or data, execution of local programs, download and execution of arbitrary code or complete takeover of the vulnerable system. An important note is that vulnerability is not limited to client machines, since IE is loaded by default on servers as well.

### Challenges

Since IE is the default web browser installed on Windows systems, nearly all Windows systems are potential victims. Older versions of IE, installed on older versions of Windows sometimes cannot be upgraded or patched with the most recent security updates. Ultimately, updating client patches for IE is an on-going and time-consuming task.

### Check Point's Solution

FireWall-1 includes multiple security tools that are designed to protect end-users browsing the Internet:

- Stateful Inspection verifies HTTP protocol integrity.
- HTTP Security Server can be configured to block different MIME types, as well as strip and weed both scripts and tags. This will help to ensure that dangerous content capable of executing code via the browser will not be allowed into the network.

In addition, SecureClient's Security Configuration Verification (SCV) allows administrators to verify that a user is at least running a version of IE with the most recent security updates. SCV checking can also verify the security configuration of Internet Explorer on end-user machines.

Finally, Check Point's Content Vectoring Protocol (CVP), part of the Open Platform for Security (OPSEC™) suite of open protocols, can be used to integrate third-party content inspection tools, such as anti-virus software, within the overall security infrastructure.

## W9: Remote Registry Access

### Summary

The Registry is a database used by all Microsoft Windows based systems to manage user and system configuration settings. Improper registry security settings can allow for remote access to the registry by malicious users, resulting in the capability to adjust these permissions and lay the groundwork for installing/enabling code on the system.



Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

## Challenges

Properly configuring access control for Windows registry settings is a time-consuming effort. The list of potentially vulnerable systems include both servers and hosts at the organization premises as well as hosts that belong to traveling users. Often, applying a patch changes the registry permissions, making registry configuration and maintenance complex.

## Check Point's Solution

As previously described in sections W4 and W5, FireWall-1 implements a unique solution for securing Microsoft Networking Services. Based on this technology, FireWall-1 can verify that CIFS traffic is not being used for remote registry access.

In addition, in order to verify client security, administrators can use SecureClient Security Configuration Verification (SCV) to scan and verify the host's registry settings.

## W10: Windows Scripting Host

### Summary

The Windows Scripting Host (WSH) is intended to allow Visual Basic scripts to be executed on a system. It actually allows any file with a ".vbs" extension to be executed as a Visual Basic script. Several worms have been propagated by including a script disguised as the contents of another file. This script is then executed when the file is viewed (or sometimes previewed) on the target system. The first famous worm to take advantage of this vulnerability was the "I Love You" worm.

### Challenges

Windows Scripting Host can be safely disabled on most systems in a proactive effort to prevent worms from spreading. Maintaining security patches for systems and applications that use WSH, such as IE and its related components, however, is a time-consuming process that is prone to error as new systems are added to the network.

### Check Point's Solution

FireWall-1 is able to block files with .vbs extension that are received through email or HTTP. Unlike other systems, FireWall-1 performs complete fragmentation checking to verify that a file will not be hidden in fragmented packets. In addition, special security checks verify that a .vbs file is not hidden in multiple headers, messages or using different encoding schemes.

In addition, the security administrator can use SecureClient Security Configuration Verification (SCV) to verify that Windows registry settings on client systems conform to security policy (e.g., WSH is disabled). This is especially useful for clients located outside the organization's physical boundaries.

## Top Vulnerabilities to Unix Systems (U)

### U1: Remote Procedure Calls (RPC)

#### Summary

Many of the most successful attacks on American sites, notably the Solar Sunrise incident, have exploited weaknesses in Remote Procedure Calls (RPC) on Unix-based systems. RPCs are designed to allow for the remote invocation of services across systems in a distributed Unix environment. Since these services frequently are executed with root privileges, RPC vulnerabilities present a valuable target for attackers.



Intelligent Security

Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

## Challenges

RPC is a fundamental service to Unix and Linux systems. As such, RPC is frequently a requirement in these environments. Further, it is often difficult for administrators to identify, patch, and maintain the relevant vulnerable components.

## Check Point's Solution

The SANS Top Twenty paper recommends blocking the RPC port (port 111) at the border router or firewall, as well as blocking the RPC "loopback" ports (TCP and UDP 32770-32789).

In addition to providing a mechanism to perform this blocking, FireWall-1 can statefully inspect RPC services. As VPN-1/FireWall-1 RPC inspection is based on port mapping, which identifies specific RPC commands, it is more secure than simply filtering port 111. For example, one can specify access rules that will allow only authorized systems and authorized users to connect to RPC services.

## U2: Apache Web Server

### Summary

Apache Web Server has a reputation for security, but as some recent exploits show, it does have some similar vulnerabilities. More detail on two recent examples of Apache vulnerabilities can be found in these CERT advisories:

- Apache/mod\_ssl Worm (CERT Advisory CA-2002-27)  
<http://www.cert.org/advisories/CA-2002-27.html>
- Apache Chunk Handling Exploit (CERT Advisory CA-2002-17)  
<http://www.cert.org/advisories/CA-2002-17.html>

An additional issue common to many Apache deployments is the presence of vulnerable Common Gateway Interface (CGI) scripts.

### Challenges

CGI scripting is an extremely common and extremely useful tool for web sites. As a result, security administrators may be able to eliminate demo scripts or unused scripts, but in many environments a variety of (potentially custom-developed) CGI scripts are required and the task of auditing a large number for various vulnerabilities can be daunting.

### Check Point's Solution

FireWall-1 includes a variety of security tools that are designed to protect web servers and web applications.

SmartDefense HTTP WormCatcher performs regular expression matching in order to block malicious HTTP requests, which are a common means of propagation for Internet worms. Because the WormCatcher can be updated to look for specific attacks as well as variants of those attacks, it can help to protect Apache installations as new vulnerabilities and new exploits are uncovered.

FireWall-1's Stateful Inspection enforces protocol integrity for HTTP traffic and can also be extended through INSPECT — an object-oriented language for defining support for new services. An example of the usefulness of this flexibility comes from SmartDefense NG Advisory 7 (<http://www.checkpoint.com/techsupport/documentation/smartdefense/cpai-2002-07.html>), which details how FireWall-1 can be configured to allow only SSLv3 connections, thus blocking the vulnerability exploited by the Apache/mod\_SSL worm while maintaining full state of a connection.



Intelligent Security

Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

## U3: Secure Shell (SSH)

### Summary

Many administrators use secure shell (ssh) instead of R-services for securing logins, command execution, and file transfers across a network. Although ssh is vastly more secure than R-services, multiple ssh vulnerabilities exist. The worst of these could allow attackers to obtain root access to vulnerable systems.

### Challenges

Under certain conditions, the SSH1 protocol itself has been demonstrated to be vulnerable to interception and decryption. The SANS Top Twenty paper recommends using version 2 instead. In some cases, ssh daemons will accept both ssh version 1 and version 2 traffic, making it necessary to enforce versioning for ssh in some other way.

### Check Point's Solution

Because ssh version 2 uses the same port as version 1, many port-filtering devices cannot distinguish between the two. FireWall-1 Stateful Inspection can distinguish between ssh versions and allow access only for version 2 traffic. In addition, VPN-1 clients (SecureClient™ and SecuRemote™) for Linux can be used to provide an additional layer of encryption, authentication, and authorization for ssh traffic.

## U4: Simple Network Management Protocol (SNMP)

### Summary

All versions of Simple Network Management Protocol (SNMP) have vulnerabilities. One of the primary problems is that the default authentication for SNMP is via an unencrypted “community string.” More detail on SNMP vulnerabilities can be found in both the SANS Top Twenty paper and in CERT Advisory CA-2002-03 (<http://www.cert.org/advisories/CA-2002-03.html>).

### Challenges

Many vendor products enable SNMP version 1 by default, and many do not offer products capable of using the version 3 security models, making it difficult to perform multi-vendor system and network management without enabling SNMP v1 on the infrastructure.

### Check Point's Solution

The SANS Top Twenty paper recommends blocking incoming SNMP traffic (port 161 TCP/UDP and 162 TCP/UDP) at network boundaries.

In addition to being able to perform this blocking, FireWall-1 statefully inspects SNMP traffic and distinguishes between different commands within the protocol. For instance, with FireWall-1 administrators can block write access and enforce read-only permissions on their networks.

## U5: File Transfer Protocol (FTP)

### Summary

A variety of vulnerabilities have been found in many different versions of File Transfer Protocol (FTP) server software. Many can be exploited by an attacker to gain root access, though most require anonymous FTP services be enabled on the target server. In addition, even authenticated FTP service transmit IDs and passwords in cleartext, so attackers can eavesdrop to intercept this information.



Intelligent Security



We Secure the Internet.

### Challenges

FTP is a common requirement for many web sites and many networks. Often, anonymous FTP is desirable for allowing access to public information or for some other business reason.

### Check Point's Solution

FireWall-1 provides a layered approach to mitigating FTP security issues: the FTP Security Server has been designed to prevent a range of known FTP attacks. In addition, Stateful Inspection tracks every port connection as well as specific FTP commands, allowing the security administrator to granularly block dangerous FTP commands.

To address the issue of cleartext IDs and passwords, VPN-1 clients (SecureClient and SecuRemote) can be used to provide a layer of encryption, authentication, and authorization for FTP traffic.

## U6: R-Services — Trust Relationships

### Summary

Organizations often use “R-services” to allow administration of multiple Unix machines without re-authenticating the user to each one. Unfortunately R-services suffer from two critical security vulnerabilities. Communications are sent in plain text (allowing a potential attacker to eavesdrop on this information) and there is no authentication of the initiating device or user.

### Challenges

Since many Unix administrators are responsible for a large number of systems, R-services can help to make navigation from one machine to another much more convenient, increasing the administrator's productivity.

In addition, one of the methods recommended by SANS to mitigate R-services vulnerabilities is to configure secure shell (ssh) and other related secure components as a replacement. However, ssh is also listed as a one of the critical Internet security vulnerabilities for Unix-based systems (U3).

### Check Point's Solution

FireWall-1 can authenticate the use of R-services to verify the administrator's identity, thus preventing unauthorized usage of Unix resources via R-services.

VPN-1 clients (SecureClient and SecuRemote) for Linux can be used to provide an additional layer of encryption, authentication, and authorization for ssh traffic.

## U7: Line Printer Daemon (LPD)

<http://www.sans.org/top20/#U7>

### Summary

The Berkeley line printer daemon (LPD) is a common tool for providing user access to remote network printers. Many versions of LPD are vulnerable to buffer overflows that can allow attackers to gain root access on the system. Creating a very large number of simultaneous connections to the LPD daemon typically causes these overflows. For more information on LPD vulnerabilities, refer to CERT advisory CA-2001-30—<http://www.cert.org/advisories/CA-2001-30.html>.

### Challenges

LPD is a fundamental service that is required in order to perform and manage printing operations. Staying current with the most recent security updates is a critical part of securing LPD and can be a time-consuming effort.





We Secure the Internet.

### Check Point's Solution

FireWall-1 filters access to the LPD service. In addition to being deployed at the network boundary, it can be deployed in front of server farms, specific network segments, or even installed on an individual server (SecureServer). Using FireWall-1's ServerQuota feature, an administrator can control the number of requests for a given service (in this case LPD). If there are too many requests to open the LPD port, ServerQuota will alert the administrator and disable the additional connections, thus preventing a potential buffer overflow.

## U8: Sendmail

### Summary

The SANS Top Twenty paper splits Sendmail vulnerabilities into two major categories: privilege escalation caused by buffer overflows, and improper configuration that allows a machine to be a relay for electronic mail from any other machine. The proliferation of open mail relays is the chief obstacle to reducing the amount of "spam" being sent over the Internet.

### Challenges

Most Sendmail vulnerabilities apply to older versions of the software and are well understood, with straightforward patches or software version updates that fix the related issues. As with many vulnerabilities with established fixes, however, many systems remain unpatched and thus vulnerable.

### Check Point's Solution

The SMTP Security Server is a standard component in any FireWall-1 based installation. In addition to filtering non-RFC compliant commands and methods, SMTP Security Server is designed to shield internal mail servers from external access, mitigating both buffer overruns (by blocking inappropriate communications) and mail relaying (by enforcing access control for outgoing SMTP traffic).

## U9: BIND/DNS

### Summary

The Berkeley Internet Name Domain (BIND) package is the most widely used implementation of the Domain Name Service (DNS). Many vulnerabilities have been found in BIND. Exploits of the various vulnerabilities can result in attackers launching denial of service attacks or gaining root access.

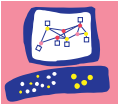
### Challenges

DNS is typically a critical service on IP networks, so extended downtime for applying patches is not always practical. Further, securing BIND requires significant technical skill.

### Check Point's Solution

FireWall-1 SmartDefense includes a DNS protocol verification security enhancement. This security tool performs protocol validation and verification for DNS traffic. Buffer overruns are prevented by blocking non-ASCII response strings and restricting the response length for DNS traffic. DNS poisoning attacks are prevented via unique Stateful Inspection of the DNS protocol.



Check Point  
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

## U10: General Unix Authentication — Accounts with No Passwords or Weak Passwords

### Summary

Many users passwords are not as strong as they should be, making them subject to compromise via dictionary-based password guessing attacks. This issue was covered for Windows-based systems in item W7. The same issues apply to weak passwords on Unix-based systems.

### Challenges

Setting and enforcing a strong password policy is not an easy task. Users tend to find ways around such policies like using the same password for multiple systems or using simple (and easily guessed) words as passwords. The imposition of character restrictions (such as requiring non-letter or non-alphanumeric characters) often results in users simply substituting different characters into common words, which doesn't significantly improve password strength.

### Check Point's Solution

The problems presented by weak passwords are very similar to those described in item W7. As such, the mitigation techniques are identical.

Security administrators can use FireWall-1 SecureServer, an instance of FireWall-1 that is installed on a single server, to provide granular access control for that server. With SecureServer, administrators can enforce password policies as well as require strong authentication (via, for example integration with certificates, third-party tokens, or smart cards) for access to network resources.

To make managing authentication models less complex, Check Point provides several key features and points of integration: Account Management Module integrates FireWall-1 with external Lightweight Directory Access Protocol (LDAP) directories. User Authority WebAccess requires users to authenticate to a web server and reduces the number of separate logins required ("reduced sign-on"). In addition, the Internal Certificate Authority (ICA) of FireWall-1 makes the usage of certificates extremely easy and simple (FireWall-1 also provides integration with third-party PKI products via OPSEC). Extensive support of Certificate Revocation Lists (CRLs) ensures that certificates that are used for authentication are valid.



Intelligent Security

Check Point  
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

## About Check Point Software Technologies

Check Point Software Technologies is the worldwide leader in securing the Internet. It is the confirmed market leader of both the worldwide VPN and firewall markets. Check Point provides Intelligent Security Solutions for Perimeter, Internal and Web Security. Based on INSPECT, the most adaptive and intelligent inspection technology and, SMART Management, which provides the lowest TCO for managing a security infrastructure, Check Point's solutions are the most reliable and widely deployed worldwide. Check Point solutions are sold, integrated and serviced by a network of 1,900 certified partners in 86 countries. For more information, please call us at (800) 429-4391 or (650) 628-2000 or visit us on the Web at <http://www.checkpoint.com> or at <http://www.opsec.com>.

### CHECK POINT OFFICES:

#### International Headquarters:

3A Jabotinsky Street, 24th Floor  
Ramat Gan 52520, Israel  
Tel: 972-3-753 4555  
Fax: 972-3-575 9256  
e-mail: [info@Checkpoint.com](mailto:info@Checkpoint.com)

#### U.S. Headquarters:

800 Bridge Parkway  
Redwood City, CA 94065  
Tel: 800-429-4391 ; 650-628-2000  
Fax: 650-654-4233  
URL: <http://www.checkpoint.com>

© 2004 Check Point Software Technologies Ltd. All rights reserved. Check Point, Check Point Express, the Check Point logo, ClusterXL, ConnectControl, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FireWall-1 VSX, FireWall-1 XL, FloodGate-1, INSPECT, INSPECT XL, IQ Engine, Open Security Extension, OPSEC, Provider-1, Safe@Office, SecureKnowledge, SecurePlatform, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, , and VPN-1 VSX are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668 and 5,835,726 and may be protected by other U.S. Patents, foreign patents, or pending applications.

P/N 000000

