DATA SECURITY MANAGEMENT

HOW TO PERFORM A SECURITY REVIEW OF A CHECKPOINT FIREWALL

Ben Rothke, CISSP

INSIDE
The Need for a Firewall Review; Review, Audit, Assessment; Steps in Reviewing a Firewall; Firewall-1 Network Objects; Implied Pseudo-Rules

INTRODUCTION
Altered States was not just a science fiction movie about a research scientist who experimented with altered states of human consciousness; it is also a metaphor for many firewalls in corporate enterprises.

In general, when a firewall is initially installed, it is tightly coupled to an organization's security requirements. After use in a corporate environment, the firewall rule base, configuration, and underlying operating system often gets transformed into a radically different arrangement. This altered firewall state is what necessitates a firewall review.

A firewall is only effective to the degree that it is properly configured. And in today's corporate environments, it is easy for a firewall to become misconfigured. By reviewing the firewall setup, management can ensure that their firewall is enforcing what they expect it to, and in a secure manner.

This article focuses on performing a firewall review for a Checkpoint Firewall-1.1 Most of the information is sufficiently generic to be germane to any firewall, including Cisco PIX, NAI Gauntlet, Axent Raptor, etc. One caveat: it is important to note that a firewall review is not a penetration test. The function of a firewall review is not to find exploits and gain access into the firewall; rather, it is to identify risks that are inadvertently opened by the firewall. Finally, it must be understood that a firewall review is also not a certification or guarantee that the firewall operating system or underlying network operating system is completely secure.

PAYOFF IDEA
This article focuses on performing a firewall review for a Checkpoint Firewall-1.1 Most of the information is sufficiently generic to be germane to any firewall, from a Checkpoint, to a Cisco PIX, NAI Gauntlet, and Axent Raptor, etc. One caveat: it is important to note that a firewall review is not a penetration test. The function of a firewall review is not to find exploits and gain access into the firewall; rather, it is to identify risks that are inadvertently opened by the firewall. Finally, it must be understood that a firewall review is also not a certification or guarantee that the firewall operating system or underlying network operating system is completely secure.
into the firewall; rather, it is to identify risks that are inadvertently opened by the firewall.

Finally, it must be understood that a firewall review is also not a certification or guarantee that the firewall operating system or underlying network operating system is completely secure.

THE NEED FOR A FIREWALL REVIEW

Firewalls, like people, need to be reviewed. In the workplace, this is called a performance review. In the medical arena, it is called a physical. The need for periodic firewall reviews is crucial, as a misconfigured firewall is often worse than no firewall. When organizations lack a firewall, they understand the risks involved and are cognizant of the fact that they lack a fundamental security mechanism. However, a misconfigured firewall gives an organization a false sense of security.

In addition, because the firewall is often the primary information security mechanism deployed, any mistake or misconfiguration on the firewall trickles into the entire enterprise. If a firewall is never reviewed, any of these mistakes will be left unchecked.

REVIEW, AUDIT, ASSESSMENT

Firewall reviews are often called audits. An audit is defined as “a methodical examination and review.” As well, the terms “review,” “assessment,” and “audit” are often synonymous. It is interesting to note that when security groups from the Big Five accounting firms perform a security review, they are specifically prohibited from using the term “audit.” This is due to the fact that the American Institute of Certified Public Accounts (www.aicpa.org), which oversees the Big Five, prohibits the use of the term “audit” because there is no set of official information security standards in which to audit the designated environment.

On the other hand, financial audits are performed against the Generally Accepted Accounting Principles (GAAP). While not a fixed set of rules, GAAP is a widely accepted set of conventions, standards, and procedures for reporting financial information. The Financial Accounting Standards Board (www.fasb.org) established GAAP in 1973. The mission of the Financial Accounting Standards Board is to establish and improve standards of financial accounting and reporting for the guidance and education of the public, including issuers, auditors, and users of financial information.

As of January 2001, the Generally Accepted System Security Principles (GASSP) Committee is in the early stages of drafting a business plan that reflects their plans for establishing and funding the International Information Security Foundation (IISF). While there is currently no set of generally accepted security principles (in which a firewall could truly be audited against), work is underway to create such a standard. Working groups for the GASSP are in place. Work is currently being done to re-
search and complete the Authoritative Foundation and develop and approve the framework for GASSP. The committee has developed a detailed plan for completing the GASSP Detailed Principles and plans to implement that plan upon securing IISF funding.

The lack of a GASSP means that there is no authoritative reference on which to maintain a protected infrastructure. If there were a GASSP, there would be a way to enforce a level of compliance and provide a vehicle for the authoritative approval of reasonably founded exceptions or departures from GASSP.

Similar in theory to GASSP is the Common Criteria Project (http://csrc.nist.gov/cc). The Common Criteria is an international effort, which is being developed as a way to evaluate the security properties of information technology (IT) products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience.

The Common Criteria will permit comparability between the results of independent security evaluations. It facilitates this by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The evaluation process establishes a level of confidence that the security functions of such products and systems, and the assurance measures applied to them, meet these requirements. The evaluation results help determine whether the information technology product or system is secure enough for its intended application and whether the security risks implicit in its use are tolerable.

**STEPS IN REVIEWING A FIREWALL**

A comprehensive review of the firewall architecture, security plans, and processes should include:

- Procedures governing infrastructure access for employees and business partners accessing the infrastructure
- Physical and logical architecture of the infrastructure
- Hardware and software versions of the infrastructure and underlying network operating systems
- Infrastructure controls over access control information
- Review of log event selection and notification criteria
- All access paths, including those provided for maintenance and administration
- Security policies and administrative procedures (i.e., addition or deletion of users and services, review of device and system audit logs, system backup and retention of media, etc.)
- Access controls over the network operating system, including user accounts, file system permissions, attributes of executable files, privileged programs, and network software
• Emergency Response Plans for the infrastructure in the event of an intrusion, denial-of-service attack, etc.
• Access to and utilization of published security alert bulletins

There are many methodologies with which to perform a firewall review. Most center around the following six steps:

1. Analyze the infrastructure and architecture
2. Review corporate firewall policy
3. Run hosts and network assessment scans
4. Review Firewall-1 configuration
5. Review Firewall-1 Rule Base
6. Put it all together in a report

The following discussion expands on each step.

**Step 1: Analyze the Infrastructure and Architecture**

An understanding of the network infrastructure is necessary to ensure that the firewall is adequately protecting the network. Items to review include:

• Internet access requirements
• Understanding the business justifications for Internet/extranet access
• Validating inbound and outbound services that are allowed
• Reviewing firewall design (i.e., dual-homed, multi-homed, proxy)
• Analyzing connectivity to internal/external networks:
  – Perimeter network and external connections
  – Electronic commerce gateways
  – Inter- or intra-company LAN-WAN connectivity
  – Overall corporate security architecture
  – The entire computing installation at a given site or location
• Interviewing network and firewall administrators

If there is a fault in the information security architecture that does not reflect what is corporate policy, then the firewall can in no way substitute for that deficiency.

From a firewall perspective, to achieve a scalable and distributable firewall system, Checkpoint has divided the functionality of its Firewall-1 product into two components: a Firewall Module and a Management Module. The interaction of these components makes up the whole of the standard Checkpoint Firewall architecture.

The management module is a centralized controller for the other firewall modules and is where the objects and rules that define firewall functionality exist. The rules and objects can be applied to one or all of the...
firewall modules. All logs and alerts generated by other firewall modules are sent to this management system for storage, querying, and review.

The firewall module itself is the actual gateway system in which all traffic between separate zones must pass. The firewall module is the system that inspects packets, applies the rules, and generates logs and alerts. It relies on one or more management modules for its rule base and log storage, but may continue to function independently with its current rule base if the management module is not functioning.

An excellent reference to use in the design of firewall architectures is *Building Internet Firewalls* by Elizabeth Zwicky (O’Reilly & Assoc. ISBN: 1565928717).

**Step 2: Review Corporate Information System Security Policies**

Policy is a critical element of the effective and successful operation of a firewall. A firewall cannot be effective unless deployed in the context of working policies that govern use and administration.

Marcus Ranum defines a firewall as “the implementation of your Internet security policy. If you haven’t got a security policy, you haven’t got a firewall. Instead, you’ve got a thing that’s sort of doing something, but you don’t know what it’s trying to do because no one has told you what it should do.” Given that, if an organization expects to have a meaningful firewall review in the absence of a set of firewall policies, the organization is in for a rude awakening.

Some policy-based questions to ask during the firewall review include:

- Is there a published firewall policy for the organization?
- Has top management reviewed and approved policies that are relevant to the firewall infrastructure?
- Who has responsibility for controlling the organization’s information security?
- Are there procedures to change the firewall policies? If so, what is the process?
- How are these policies communicated throughout the organization?

As to the management of the firewall, some of the issues that must be addressed include:

- Who owns the firewalls, and is this defined?
- Who is responsible for implementing the stated policies for each of the firewalls?
- Who is responsible for the day-to-day management of the firewall?
- Who monitors the firewall for compliance with stated policies?
- How are security-related incidents reported to the appropriate information security staff?
• Are CERT, CIAC, vendor-specific and similar advisories for the existence of new vulnerabilities monitored?

• Are there written procedures that specify how to react to different events, including containment and reporting procedures?

Change control is critically important for a firewall. Some change controls issues are:

• Ensure that change control procedures documents exist.
• Ensure that test plans are reviewed.
• Review procedures for updating fixes.
• Review the management approval process.
• Process should ensure that changes to the following components are documented:
  – Any upgrades or patches require notification and scheduling of downtime
  – Electronic copies of all changes
  – Hard-copy form filled out for any changes

Finally, backup and contingency planning is crucial when disasters occur. Some issues are:

• Maintain a golden copy of Firewall-1. A golden copy is full backup made before the host is connected to the network. This copy can be used for recovery and also as a reference in case the firewall is somehow compromised.
• Review backup procedures and documentation. Part of the backup procedures must also include restoration procedures. A backup should only be considered complete if one is able to recover from the backups made. Also, the backups must be stored in a secure location. Should the firewall need to be rebuilt or replaced, there are several files that will need to be restored (see Exhibit 1). These files can be backed up via a complete system backup, utilizing an external device such as a tape drive or other large storage device. The most critical files for firewall functionality should be able to fit on a floppy disk.
• Review backup schedule.
• Determine if procedures are in place to recover the firewall system should a disruption of service occur.
• Review contingency plan.
• Contingency plan documentation.

Information Security Policies and Procedures (Thomas Peltier, Auerbach Publications) is a good place to start a policy roll-out. While not a panacea for the lack of a comprehensive set of policies, Information Se-


**EXHIBIT 1 — Critical Firewall-1 Configuration Files to Backup**

<table>
<thead>
<tr>
<th>Management Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>$FWDIR/conf/fw.license</td>
</tr>
<tr>
<td>$FWDIR/conf/objects.C</td>
</tr>
<tr>
<td>$FWDIR/conf/*.W</td>
</tr>
<tr>
<td>$FWDIR/conf/rulebases.fws</td>
</tr>
<tr>
<td>$FWDIR/conf/fwauth.NDB*</td>
</tr>
<tr>
<td>$FWDIR/conf/fwmusers</td>
</tr>
<tr>
<td>$FWDIR/conf/gui-clients</td>
</tr>
<tr>
<td>$FWDIR/conf/product.conf</td>
</tr>
<tr>
<td>$FWDIR/conf/fwauth.keys</td>
</tr>
<tr>
<td>$FWDIR/conf/serverkeys.*</td>
</tr>
<tr>
<td><strong>Firewall Module</strong></td>
</tr>
<tr>
<td>$FWDIR/conf/fw.license</td>
</tr>
<tr>
<td>$FWDIR/conf/product.conf</td>
</tr>
<tr>
<td>$FWDIR/conf/masters</td>
</tr>
<tr>
<td>$FWDIR/conf/fwauth.keys</td>
</tr>
<tr>
<td>$FWDIR/conf/product.conf</td>
</tr>
<tr>
<td>$FWDIR/conf/smtp.conf</td>
</tr>
<tr>
<td>$FWDIR/conf/fwauthd.conf</td>
</tr>
<tr>
<td>$FWDIR/conf/fwopsec.conf</td>
</tr>
<tr>
<td>$FWDIR/conf/product.conf</td>
</tr>
<tr>
<td>$FWDIR/conf/serverkeys.*</td>
</tr>
</tbody>
</table>


Curity Policies and Procedures enables an organization to quickly roll-out policies without getting bogged down in its composition.

It must be noted that all of this analysis and investigation should be done in the context of the business goals of the organization. While information systems security is about risk management, if it is not implemented within the framework of the corporate strategy, security is bound to fail.

**Step 3: Perform Hosts Software Assessment Scan**

A firewall misconfiguration can allow unauthorized parties, outsiders, to break into the network despite the firewall’s presence. By performing software scans against the individual firewall hosts, specific vulnerabilities can be detected. These scanning tools can identify security holes, detail system weaknesses, validate policies, and enforce corporate security strategies. Such tools are essential for checking system vulnerabilities.

Some of the myriad checks that scanners can identify include:

- Operating system misconfiguration
- Inappropriate security and password settings
- Buffer overflow
• Detection of SANS Top 10 Internet Security Threats
• Segmentation fault affecting FreeBSD
• Detection of unpassworded NT guest and administrator accounts

Some popular scanning tools\(^6\) are:

• **NAI Cybercop**, http://www.pgp.com/products/cybercop-scanner
• **ISS Internet Scanner**, http://www.iss.net/internet.Scanner/index.php
• **SAINT**, http://www.wwdsi.com/saint
• **Symantec (formerly Axent) NetRecon**, http://enterprisesecurity.symantec.com/products
• **Netcat**, http://www.l0pht.com/~weld/netcat/
• **nmap**, http://www.insecure.org/nmap/index.html

It must be noted that running host software assessment scan on a firewall is just one aspect of a firewall review. Tools such as Cybercop are extremely easy to run; as such, there is no need to bring in a professional services firm to run the tools. The value added by security professional service firms is in the areas of comprehensive architecture design, analysis, and fault amelioration. Any firm that would run these tools and simply hand the client the output is doing the client a serious injustice. This only serves to reiterate the point that a security infrastructure must be architected from the onset. This architecture must take into consideration items such as security, capacity, redundancy, and management. Without a good architecture, system redesign will be a constant endeavor.

**Step 4: Review Firewall-1 Configuration**

While Firewall-1 affords significant security, that security can be compromised if Firewall-1 is misconfigured. Some of the more crucial items to review are listed below (not in any specific order).

**IP Forwarding.** Set to *Control IP Forwarding*. IP Forwarding should be disabled in the operating system kernel. This ensures that IP Forwarding will be never be enabled unless Firewall-1 is operating.

**Firewall Administrators.** Ensure that the number of Firewall-1 administrators is limited only to those who truly need it. The purpose of every account on the firewall (both for the operating system and the firewall operating system) must be justified. Exhibit 2 provides a list of firewall administrators and their permissions.

**Trained Staff.** A firewall cannot be effective unless the staff managing the firewall infrastructure is experienced with security and trained in Firewall-1 operations. If a person is made responsible for a firewall simply
because he or she has experience with networking, the firewall should be expected to be filled with misconfigurations, which in turn will make it much easier for adversaries to compromise the firewall.

**SYN Flood Protection.** Denial-of-service (DoS) attacks enable an attacker to consume resources on a remote host to the degree it cannot function properly. SYN flood attacks are one of the most common types of DoS attacks.

Ensure that SYN flood protection is activated at the appropriate level: None, SYN Gateway, or Passive SYN Gateway (see Exhibit 3).

**Operating System Version Control.** For both the Checkpoint software and network operating system, ensure that the firewall is running a current and supported version of Firewall-1. While the latest version does not specifically have to be loaded, ensure that current patches are installed.
Physical Security. The firewall must be physically secured. It should be noted that all network operating systems base their security models on a secure physical infrastructure. A firewall must be located in areas where access is restricted only to authorized personnel; specifically:

- The local console must be secure.
- The management console should not be open to the external network.
- The firewall configuration should be fully protected and tamper-proof (except from an authorized management station).
• Full authentication should be required for the administrator for local administration.
• Full authentication and an encrypted link are required for remote administration.

**Remove Unneeded System Components.** Software such as compilers, debuggers, security tools, etc. should be removed from the firewall.

**Adequate Backup Power Supplies.** If the firewall lacks a UPS, security will not be completely enforced in the event of a power disruption.

**Log Review.** The logs of both the firewall and network operating system need to be reviewed and analyzed. All events can be traced to the logs, which can be used for debugging and forensic analysis.

Ideally, logs should be written to a remote log host or separate disk partition. In the event of an attack, logs can provide critical documentation for tracking several aspects of the incident. This information can be used to uncover exploited holes, discover the extent of the attack, provide documented proof of an attack, and even trace the attack's origin. The first thing an attacker will do is cover his or her tracks by modifying or destroying the log files. In the event that these log files are destroyed, backups will be required to track the incident. Thus, frequent backups are mandatory.

**Time Synchronization.** Time synchronization serves two purposes: to ensure that time-sensitive events are executed at the correct time and that different log files can be correlated. Logs that reference an incorrect time can potentially be excluded as evidence in court and this might thwart any effort to prosecute an attacker.

The Network Time Protocol (NTP) RFC 1305 is commonly used to synchronize hosts. For environments requiring a higher grade and audit-able method of time synchronization, the time synchronization offerings from Certified Time (www.certifiedtime.com) should be investigated.

**Integrity Checking.** Integrity checking is a method to notify a system administrator when something on the file system has changed to a critical file. The most widely known and deployed integrity checking application is *Tripwire* (www.tripwire.com).

**Limit the Amount of Services and Protocols.** A firewall should have nothing installed or running that is not absolutely required by the firewall. Unnecessary protocols open needless communication links. A port scan can be used to see what services are open. Too many services can hinder the efficacy of the firewall, but each service should be authorized; if not, it should be disabled.
Dangerous components and services include:

- X or GUI related packages
- NIS/NFS/RPC related software
- Compilers, Perl, TCL
- Web server, administration software
- Desktop applications software (i.e., Microsoft Office, Lotus Notes, browsers, etc.)

On an NT firewall, only the following services and protocols should be enabled:

- TCP/IP
- Firewall-1
- Protected Storage
- UPS
- RPC
- Scheduler
- Event log
- Plug-and-Play
- NTLM Security Support provider

If other functionality is needed, add them only on an as-needed basis.

**Harden the Operating System.** Any weakness or misconfiguration in the underlying network operating system will trickle down to Firewall-1. The firewall must be protected as a bastion host to be the security stronghold. A firewall should never be treated as a general-purpose computing device.

The following are excellent documents on how to harden an operating system:

- *Armoring NT*, www.enteract.com/~lspitz/nt.html

Those needing a pre-hardened device should consider the Nokia firewall appliance (www.nokia.com/securitysolutions/network/firewall.html). The Nokia firewall is a hardware solution bundled with Firewall-1. It runs on the IPSO operating system that has been hardened and optimized for firewall functionality.

**Firewall-1 Properties.** Exhibit 4 shows the Security Policies tab. One should uncheck the Accept boxes that are not necessary:
• **ICMP.** In general, one can disable this property, although one will need to leave it enabled to take advantage of Check Point’s Stateful Inspection for ICMP in 4.0.

• **Zone transfer.** Most sites do not allow users to perform DNS downloads. The same is true for RIP and DNS lookup options.

**Firewall-1 Network Objects.** A central aspect of a Firewall-1 review includes the analysis of all of the defined network objects. Firewall-1 network objects are logical entities that are grouped together as part of the
security policy. For example, a group of Web servers could be a simple network object to which a rule is applied. Every network object has a set of attributes, such as network address, subnet mask, etc. Examples of entities that can be part of a network object include:

- Networks and sub-networks
- Servers
- Routers
- Switches
- Hosts and gateway
- Internet domains
- Groups of the above

Firewall-1 allows for the creation of network objects within the source and destination fields. These network objects can contain and reference anywhere from a single device to entire networks containing thousands of devices. The latter creates a significant obstacle when attempting to evaluate the security configuration and security level of a Firewall-1 firewall. The critical issue is how to determine the underlying security of the network object when it contains numerous objects.

This object-oriented approach to managing devices on Firewall-1 allows the firewall administrator to define routers or any other device as network objects, and then to use those objects within the rules of the firewall security policy. The main uses of network objects are for efficiency in referencing a large amount of network devices. This obviates the need to remember such things as the host name, IP address, location, etc. While network objects provide a significant level of ease of use and time-saving, by utilizing such objects, an organization needs to determine if it inherently trusts all of the devices contained within the object. Exhibit 5 shows the Network Objects box that shows some of the existing objects. Exhibit 6 shows an example of a Network Object with a number of workstations in the group.

As stated, such use of network objects is time-saving from an administrative perspective; but from a security perspective, there is a problem in that any built-in trust that is associated with the network object is automatically created for every entity within that network object. This is due to the fact that in large networks, it is time-consuming to inspect every individual entity defined in the network object. The difficulty posed by such a configuration means that in order to inspect with precision and accuracy the protection that the firewall rule offers, it is essential to inspect every device within the network object.

**Step 5: Review Firewall-1 Rule Base**

The purpose of a rule base review is to actually see what services and data the firewall permits. An analysis of the rule base is also meant to identify
EXHIBIT 5 — Existing Objects

EXHIBIT 6 — A Network Object with a Number of Workstations in the Group
any unneeded, repetitive, or unauthorized rules. The rule base should be made as simple as possible. One way to reduce the number of rules is by combining rules, because sometimes repetitive rules can be merged.

The function of a rule base review is to ensure that the firewall is enforcing what it is expected to. Lance Spitzner writes in *Building Your Firewall Rule Base* that “building a solid rule base is a critical, if not the most critical, step in implementing a successful and secure firewall. Security administrators and experts all often argue what platforms and applications make the best firewalls. However, all of this is meaningless if the firewall rule base is misconfigured.”

The rule base is the heart and soul of a Checkpoint firewall. A rule base is a file stored on the firewall that contains an ordered set of rules that defines a distinct security policy for each particular firewall. Access to the rule base file is restricted to those that are either physically at the firewall or a member of the GUI client list specified in the configuration settings.

A rule describes a communication in terms of its source, destination, and service. The rule also specifies whether the communication should be accepted or rejected and whether a log entry is created.

The Firewall-1 inspection engine is a “first-fit” as opposed to a “best-fit” device. This means that if one has a rule base containing 20 rules, and the incoming packet matches rule #4, the inspection engine stops immediately (because rules are examined sequentially for each packet) and does not go through the remainder of the rule base.

As for the rule base review, security expert Lance Spitzer recommends that the goal is to have no more than 30 rules. Once there are more than 30 rules, things exponentially grow in complexity and mistakes then happen.

Each rule base has a separate name. It is useful to standardize on a common naming convention. A suggested format is: firewall-name_administrators-initials_date-of-change; for example, fw1_am_071298.

The result of this naming convention is that the firewall administrator knows exactly which firewall the rule base belongs to; when the rule base was last changed; and who last modified the current configuration. For the rule base review, each and every rule must be examined.

An example of a simple rule base with six rules is as shown in Exhibit 7:

- **Rules 1 and 2** enforce the concept of the stealth rule, in that nothing should be able to connect directly to the firewall, other than administrators that are GUI authorized. Rule 1 tells Firewall-1 to drop any packet unless it is from a member of the FW_Administrators group. The Firewall-1 service is predefined and defines all the Firewall-1 administrative ports. For the stealth rule, one specifically wants to drop the packet, as opposed to rejecting it. A rejected packet tells the sender that there is something on the remote side, while a dropped packet does not necessarily indicate a remote host. In addition, this
EXHIBIT 7 — A Simple Rule Base
rule is logged; thus, detailed information can be gleaned about who is attempting to make direct connections to the firewall.

• **Rule 3** allows any host e-mail connectivity to the internal mail servers.
• **Rule 4** allows any host HTTP and HTTPS connectivity to internal Web servers.
• **Rule 5** allows internal host connectivity to the Internet for the four specified protocols.
• **Rule 6** is the cleanup rule. Any packet not handled by the firewall at this point will be dropped and logged. The truth is that any packet not handled by the firewall at that point would be dropped anyway. The advantage to this cleanup rule is that these packets will be logged. In this way, one can see which packets are not being handled by the firewall. This can be of assistance in designing a more scalable firewall architecture.

The above rule base example had only six rules and was rather simple. Most corporate rule bases are more detailed and complex. Going through a rule base containing 50 rules and thousands of network objects could take a while to complete.

Exhibit 8 displays a rule base that is a little more involved:

• **Rule 1** enforces the stealth rule.
• **Rules 2–4** allow mail traffic between the mail servers and clients.
• **Rule 5** allows any host HTTP connectivity to internal Web servers.
• **Rule 6** stops traffic between the DMZ and an intranet.
• **Rules 7–8** stop incoming and outgoing traffic between the DMZ and an intranet.
• **Rule 9** drop protocols that cause a lot of traffic — in this case, nbdatagram, nbname, and nbsession.
• **Rule 10** is the cleanup rule.

When performing a review and there is a doubt if a specific rule is needed, it can be disabled. As a general rule, if a rule is disabled and no one complains, then the rule can be deleted. Exhibit 9 shows an example of a disabled rule.

**Implied Pseudo-Rules.** Implied pseudo-rules are rules that do not appear in the normal rule base, but are automatically created by Firewall-1 based on settings in the Properties Setup of the Security Policy. These rules can be viewed along with the rule base in the Security Policy GUI application. Exhibit 10 displays an example of the implied pseudo-rules from a rule base with a single rule.

Although the single and only rule implicitly drops all traffic, there is a lot of traffic that can still pass through the firewall. As seen from these
### EXHIBIT 8 — Complex Rule Base

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>Main_PIV</td>
<td>Any</td>
<td>drop</td>
<td>Alert</td>
</tr>
<tr>
<td>2</td>
<td>Intranet_NY</td>
<td>Mail_Server</td>
<td>pop-3</td>
<td>accept</td>
<td>Long</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Mail_Server</td>
<td>smtp</td>
<td>accept</td>
<td>Long</td>
</tr>
<tr>
<td>4</td>
<td>Mail_Server</td>
<td>Any</td>
<td>smtp</td>
<td>accept</td>
<td>Long</td>
</tr>
<tr>
<td>5</td>
<td>Any</td>
<td>Web_Servers</td>
<td>http</td>
<td>accept</td>
<td>Long</td>
</tr>
<tr>
<td>6</td>
<td>DMZ_Net</td>
<td>Intranet_NY</td>
<td>Any</td>
<td>reject</td>
<td>Alert</td>
</tr>
<tr>
<td>7</td>
<td>Intranet_NY</td>
<td>DMZ_Net</td>
<td>Any</td>
<td>reject</td>
<td>Alert</td>
</tr>
<tr>
<td>8</td>
<td>Intranet_NY</td>
<td>Any</td>
<td>Permitted_Internet_Services</td>
<td>accept</td>
<td>Long</td>
</tr>
<tr>
<td>9</td>
<td>Any</td>
<td>Any</td>
<td>Chatty_Protocols</td>
<td>drop</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>drop</td>
<td>Alert</td>
</tr>
</tbody>
</table>
EXHIBIT 9 — Disabled Rule

- Internal_Network
- Any
- http
- https
- gopher
- riltp
- accept
- Border_FW
**EXHIBIT 10 — Implied Pseudo-rules**

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
<th>Time</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><a href="http://www.FRM.Host">www.FRM.Host</a></td>
<td><a href="http://www.FRM.Host">www.FRM.Host</a></td>
<td>Port</td>
<td>accept</td>
<td></td>
<td>Gateways</td>
<td>Any</td>
<td>Enable Port Control Connections</td>
</tr>
<tr>
<td>2</td>
<td><a href="http://www.FRM.Host">www.FRM.Host</a></td>
<td><a href="http://www.FRM.Host">www.FRM.Host</a></td>
<td>Port_log</td>
<td>accept</td>
<td></td>
<td>Gateways</td>
<td>Any</td>
<td>Enable Port Control Connections</td>
</tr>
<tr>
<td>3</td>
<td>www_gui-stmts</td>
<td><a href="http://www.FRM.Management">www.FRM.Management</a></td>
<td>Port_right</td>
<td>accept</td>
<td></td>
<td>Gateways</td>
<td>Any</td>
<td>Enable Port Control Connections</td>
</tr>
<tr>
<td>4</td>
<td>www_FrmGui-1.Host</td>
<td><a href="http://www.FRM.Management">www.FRM.Management</a></td>
<td>Port_right</td>
<td>accept</td>
<td></td>
<td>Gateways</td>
<td>Any</td>
<td>Enable Port Control Connections</td>
</tr>
<tr>
<td>5</td>
<td>Any</td>
<td><a href="http://www.FRM.Host">www.FRM.Host</a></td>
<td>Port_Org</td>
<td>accept</td>
<td></td>
<td>Gateways</td>
<td>Any</td>
<td>Enable Port Control Connections</td>
</tr>
<tr>
<td>6</td>
<td>Any</td>
<td><a href="http://www.FRM.Host">www.FRM.Host</a></td>
<td>Port_Org</td>
<td>accept</td>
<td></td>
<td>Gateways</td>
<td>Any</td>
<td>Enable Port Control Connections</td>
</tr>
<tr>
<td>7</td>
<td>Any</td>
<td><a href="http://www.FRM.Host">www.FRM.Host</a></td>
<td>Port_Org</td>
<td>accept</td>
<td></td>
<td>Gateways</td>
<td>Any</td>
<td>Enable Port Control Connections</td>
</tr>
<tr>
<td>8</td>
<td>Any</td>
<td><a href="http://www.FRM.Host">www.FRM.Host</a></td>
<td>Port_Org</td>
<td>accept</td>
<td></td>
<td>Gateways</td>
<td>Any</td>
<td>Enable Port Control Connections</td>
</tr>
<tr>
<td>9</td>
<td>Any</td>
<td><a href="http://www.FRM.Host">www.FRM.Host</a></td>
<td>Port_Org</td>
<td>accept</td>
<td></td>
<td>Gateways</td>
<td>Any</td>
<td>Enable Port Control Connections</td>
</tr>
<tr>
<td>10</td>
<td>Any</td>
<td><a href="http://www.FRM.Host">www.FRM.Host</a></td>
<td>Port_Org</td>
<td>accept</td>
<td></td>
<td>Gateways</td>
<td>Any</td>
<td>Enable Port Control Connections</td>
</tr>
<tr>
<td>11</td>
<td>Any</td>
<td><a href="http://www.FRM.Host">www.FRM.Host</a></td>
<td>Port_Org</td>
<td>accept</td>
<td></td>
<td>Gateways</td>
<td>Any</td>
<td>Enable Port Control Connections</td>
</tr>
<tr>
<td>12</td>
<td>Any</td>
<td><a href="http://www.FRM.Host">www.FRM.Host</a></td>
<td>Port_Org</td>
<td>accept</td>
<td></td>
<td>Gateways</td>
<td>Any</td>
<td>Enable Port Control Connections</td>
</tr>
<tr>
<td>13</td>
<td>Any</td>
<td><a href="http://www.FRM.Host">www.FRM.Host</a></td>
<td>Port_Org</td>
<td>accept</td>
<td></td>
<td>Gateways</td>
<td>Any</td>
<td>Enable Port Control Connections</td>
</tr>
<tr>
<td>14</td>
<td>Any</td>
<td><a href="http://www.FRM.Host">www.FRM.Host</a></td>
<td>Port_Org</td>
<td>accept</td>
<td></td>
<td>Gateways</td>
<td>Any</td>
<td>Enable Port Control Connections</td>
</tr>
</tbody>
</table>
implied pseudo-rules, most of the connectivity deals with the internal operations of the firewall.

**Step 6: Put It All Together in a Report**

After all the work has been completed, the firewall review needs to be documented. The value in a post-review report is that it can be used as a resource to correct the anomalies found.

As previously stated, the ease of use afforded by scanning tools makes the creation of a huge report effortless. But for a firewall review to have value for a client, it should contain the following:

- Current security state: detail the baseline of the current networking environment and current security posture; this must reference the corporate risk assessment to ensure synchronization with the overall security goals of the organization
- Identification of all security vulnerabilities
- Recommend corrections, solutions, and implementation priorities; a detailed implementation plan must be provided, showing how all of the solutions and fixes will coalesce
- Detailed analysis of security trade-offs, relating the risks to cost, ease of use, business requirements, and acceptable levels of risk
- Provide baseline data for future reference and comparison to ensure that systems are rolled out in a secure manner

**CONCLUSION**

A firewall is effective to the degree that it is properly implemented. And in today’s corporate environments, it is easy for a firewall to become misconfigured. By reviewing the firewall setup, firewall administrators can ensure that their firewall is enforcing what they expect it to, in a secure manner. This makes for good sense and good security.

Ben Rothke, CISSP, is a senior security consultant with Baltimore Technologies and can be reached at ben.rothke@baltimore.com.

**References**

Further Reading

Resources and Mailing Lists
8. Bugtraq, Bugtraq-request@fc.net.
9. NTBugtraq, Ntbugtraq-request@fc.net.

Notes
1. Screen shots in this article are from Firewall-1 v4.1 for Windows NT, but are germane for all platforms and versions. See www.phoneboy.com/fw1/docs/4.0-summary.html for the new features and upgrades in Firewall-1 version 4.x.
2. PricewaterhouseCoopers, Ernst & Young, Deloitte & Touche, Arthur Andersen, KPMG.
5. It should be noted that while many safes will physically protect backup media, they will not protect this media against the heat from a fire. The safe must be specifically designed for data storage of media such as tapes, floppies, and hard drives.
6. A comprehensive list of tools can be found at www.hackingexposed.com/tools/tools.html.
7. See www.enteract.com/~lspitz.
8. See www.phoneboy.com/fw1/faq/0345.html for a comprehensive list of what the Firewall-1 control connections allow by default.