Global Information Assurance Certification Paper

Audit and Control Checklist for the Elron Internet Manager (IM) Firewall: An Auditor's Perspective

Mark Hill
GSNA Practical version 2.0, February 2002

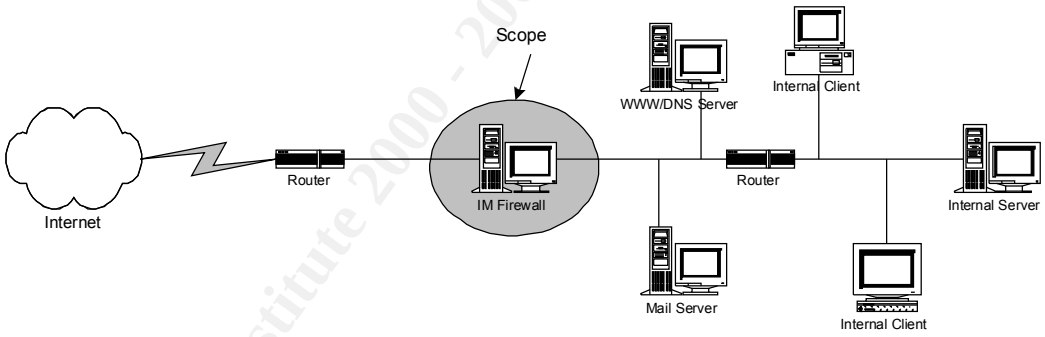
Table of Contents

Assignment 1 – Research in Audit, Measurement Practice and Control

System Identification:

This paper will document a review of Elron Software's product, Internet Manager (IM) Firewall version 3.0.5 installed on Windows NT Workstation version 4 SP6. The approach taken will be that of an independent auditor. The firewall is acting as a primary defense device against unauthorized access originating from a direct connection to the Internet. While very important to the overall security of the connection, controls applicable to Windows NT and a perimeter router will be considered outside the primary scope of the review. However, the IM Firewall is not an "all-in-one" device and the security of the IM product does depend heavily on some NT controls. Therefore, a few NT controls will have to be evaluated in this review to ensure logical security of the product.

The website protected by the firewall provides general information about a property and casualty insurance company. It also grants commercial customers access to view their policies as well as obtain claim status information through an in-house developed application called the Commercial Customer Information System (CCIS). No online transaction processing is performed at this time. The IM firewall does not provide the primary Internet connection for internal users (this is handled through another Internet connection), but it has been designated to act as a backup connection if needed.



Evaluation of Risks:

The most important tasks for the IM Firewall are to protect the internal network from attacks, to allow secure access to policy and claim information for authorized customers, and to enforce the company's Internet policy as applicable to the functions of this connection. In order to adequately accomplish these duties, the IM Firewall must be managed appropriately from a technical and operational perspective.

The following list attempts to identify and evaluate risks common to an Internet firewall. Some risks are technical in nature while others are more operationally oriented and could be applied to other IT systems within the company as well. Maintaining proper logical access, managing the firewall rule base and applying updates to the system (e.g. security patches) will be the most important technical requirements. As with other information systems within the company, the IM Firewall will have operational requirements such as physical access controls, configuration management, recovery precautions and associated company policies.

Risk	Probability of Occurrence	Impact
Improper installation that results in inappropriate access to Internet resources (sites and services)	High	Performance degradation, unnecessary exposure to Internet threats, compromise of system.
Compromise through a known vulnerability.	High	Loss of system availability, unauthorized disclosure of data, company's reputation damaged
Internet attacks not detected	High	Compromise of system, unauthorized disclosure of data, company's reputation damaged
Unauthorized logical access from internal sources	High	Compromise of system, customer information unavailable, unauthorized disclosure of data, company's reputation damaged
Mis-configuration of software	Medium	Improper function of system, exposure to Internet attacks.
Denial of service	Medium	Customer information unavailable
Buffer overflows	Medium	Customer information unavailable
Unauthorized physical access	Medium	Destruction of equipment, customer information unavailable.
Inability to recover timely in the event of a disaster	Medium	Customer information unavailable, company's reputation damaged.
Hardware failure	Medium	Customer information unavailable
Interference by obstructive software	Medium	Degradation of performance,
Exposure to environmental extremes	Low	Customer information unavailable
ISP failure	Low	Customer information unavailable

Current State of Practice:
Firewall auditing is commonplace in today's technological environments. Many checklists exist to evaluate the general controls of firewall configurations. Some of the checklists are more generic in nature while others concentrate on specific firewall systems. Many can be found on the Internet (e.g. two programs were found at http://www.auditnet.org/asapind.htm, one on http://www.ticm.com/info/insider/members/fwsecfaq/, several resources exist in the SANS Reading Room at http://rr.sans.org/signup/login.php, etc.). Several books also exist (e.g. "Building Internet Firewalls", Second Edition, by Zwicky, Cooper and Chapman, O'Reilly Press, June 2000 and "Information Security Handbook", by Tipton and Krause, CRC Press LLC, 2002, etc.).

Numerous organizations also provide training in firewall auditing. The MIS Training Institute, the SANS Institute, and Canaudit Inc. are just a few. Other organizations are able to provide firewall auditing as a service. RM Consulting (http://www.rmconsulting.com/firewall.htm), Shake Communications Pty Ltd. (http://www.shake.net/about.cfm), and MIS Corporate Defense Solutions (http://www.mis-cds.com/services/spirit/zone/) are three companies the author found that provide this type of service. These companies were found within a five-minute search using the search engine "Google" and searching for "firewall auditing services". In summary, innumerable sources exist on the subject of auditing firewalls.

Sources specific to auditing the Elron IM Firewall software, however, could not be located. Three popular search engines were used (www.lycos.com, www.google.com, and www.altavista.com) as well as most of the previously mentioned online references with no valuable results. Several online and brick and mortar bookstores were also searched and no material was found (www.amazon.com, Barnes and Noble, etc.).

Improvement of Current Methods and Techniques:
A comprehensive document covering both operational aspects (common controls) and technical aspects (configuration) of the IM Firewall product could not be found. It is the intent of this paper to create a checklist that does include both aspects. Several audit checklists, firewall "hardening" documents and audit programs from previous audits performed by the author will be combined to build a new audit program. Within this program, technical aspects will be included to specifically cover the Elron IM Firewall product. This is the author's first attempt at auditing the IM Firewall; therefore, the resulting checklist will most likely be incomplete to some extent. It is hoped, however, that this document will provide a good foundation for future auditors or security personnel to utilize when reviewing the IM Firewall.

Assignment 2 – Create an Audit Checklist

Overview

The Elron IM Firewall documentation describes the product as a third-generation firewall technology utilizing Stateful Multi-Layer Inspection. Stateful, meaning that the firewall monitors the "state" of any network transaction and it continuously monitors the conversation streams passing through it. Multi-layer, meaning that the firewall analyzes the OSI network traffic layers 2 through 7. Finally, Inspection, meaning that all network traffic is analyzed down to the packet level to filter out unwanted transmissions and ensure that the rules established in the configuration are enforced. The firewall can support two or three network interface cards, providing for a simple barrier between the internal and external network or providing for the implementation of a demilitarized zone. The firewall has modules, which can provide for Network Address Translation, Virtual Private Networking, and Remote User Authentication. The firewall also comes with many pre-defined services such as ActiveX, LDAP, Citrix, etc., which can be easily added to the firewall's rule-base.

The firewall is made-up of two primary components, the firewall service and the firewall manager. The firewall service, sometimes referred to as the SMLI Engine, is implemented as a physical and logical barrier between the Internet and the protected network. The firewall manager can, but does not have to be, installed on the same workstation and provides a GUI interface for configuring the firewall's rule-base. The firewall manager may be installed on another Windows NT or Windows 9X workstation and access the firewall workstation remotely. The IM Firewall configuration is contained within a "plan" (configuration file). A plan must be saved to a firewall service for the configuration to take effect. Plans can be worked on while attached to a firewall (i.e. in real-time) or offline.

Audit Checklist:

The following steps make up the audit checklist. This checklist has been designed to be applicable to almost any firewall environment. Of course, where appropriate, specific steps address the technical aspects and configuration of the Elron IM Firewall. It should be possible, however, to replace these environment specific steps with steps to address other firewall products. While many of the steps are subjective, these steps are necessary to ensure that a complete review is conducted successfully. Conversely, in the event that readers of this document already have a comprehensive firewall checklist, the steps specific to the Elron IM Firewall could be extracted/incorporated into a pre-existing audit program. The checklist contains steps to verify permitted services and to identify vulnerabilities with commonly available tools. The checklist does not contain any guidelines for conducting a Penetration Test and for exploiting any identified vulnerabilities.

Step 1 – Internet Policy

Reference:	**"***Information Security Management Handbook*" [ref. 1] Personal Experience
Control Objective:	This step will determine if an Internet/Information Security Policy exists and that it adequately addresses requirements regarding Internet access and applicable firewall controls.
Risk:	The firewall may not support the company policy regarding Internet access, or there may be no basis or justification for firewall settings if no policy exists.
Compliance:	This step has a range of possible results. An adequate policy could exist, no policy may exist or any degree in-between. The policy must be evaluated on how well it covers standard items as well as how it is constructed to support the organization's environment.
Testing:	1. Review the Internet and/or Security Policy for appropriate authorship and appropriate level of management approval and support. 2. Determine if, and how, compliance to the policy is enforced. 3. Determine how the policy can be changed and by whom. 4. Is the policy reviewed and re-assessed on an adequate basis?
Objective/Subjective:	Subjective
Comments:	"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." *Handbook of Information Security Management,* "How to Perform a Security Review of a Checkpoint Firewall" by Ben Rothke. [ref. 1]

Result

Step 2 – Firewall Documentation

Reference:	**"***Information Security Management Handbook*", [ref. 1] The Firewall Hardening Guide v0.1, [ref. 2] Personal Experience
Control Objective:	This step will determine whether adequate, up-to-date documentation exists for the firewall and whether the documentation sufficiently describes the firewall's settings and

	technical network details.
Risk:	Considerable time can be lost in managing, restoring, and changing the firewall, if key personnel are not available and no (or deficient) documentation exists.
Compliance:	A range of possible results exists for this step. The organization may have good documentation, no documentation or anything in-between. The level of documentation will be dependent on the complexity of operations needed to support the firewall and the organization's environment.
Testing:	1. Review to ensure that appropriate personnel have access to vendor documentation and network documentation. 2. The documentation should include vendor administration and support manuals, LAN and WAN diagrams, hardware and software descriptions, and documentation of control files and configuration settings.
Objective/Subjective:	Subjective
Comments:	Documentation goes out-of-date quickly, also ask how the documents are kept current.

Result

Step 3 – Management Procedures

Reference:	**"***Information Security Management Handbook*", [ref. 1] Personal Experience
Control Objective:	This step will determine whether adequate, up-to-date documentation exists for the administrative and support procedures necessary to manage the firewall.
Risk:	Lack of adequate procedural documentation can result in a considerable loss of time in managing, restoring, and changing the firewall, if key personnel are not available and no (or deficient) procedural documentation exists. Procedural documentation also serves as a good training tool for new staff
Compliance:	A range of possible results exists for this step. The organization may have good documentation, no documentation or anything in-between. The level of documentation will be dependent on the complexity of operations needed to support the firewall and the organization's environment.
Testing:	1. Review to ensure that appropriate personnel have access adequate and up-to-date procedural documentation. 2. The documentation should include account/services maintenance, log review, log retention, monitoring of

	threats, the company Internet policy, and proof of compliance with the policy.
Objective/Subjective:	Subjective
Comments:	

Result

Step 4 – Emergency Procedures

Reference:	**"***Information Security Management Handbook*", [ref. 1] The Firewall Hardening Guide v0.1, [ref. 2] Personal Experience
Control Objective:	This step will determine whether adequate procedures exist in the event of an internal or external attack.
Risk:	Loss of system availability, penetration of interior network and loss of data can result if attacks are not properly dealt with and controlled.
Compliance:	A range of possible results exists for this step. The organization may have good emergency procedures, no procedures or any level in-between. The organization should have at least a base line or minimum level of procedures.
Testing:	1. Review that appropriate response procedures exist to react to suspected attacks. Procedures should include actions to take regarding monitoring, logging, tracing the source of the attack, and shutting down systems to protect the internal network.
Objective/Subjective:	Subjective
Comments:	It is very helpful if any of the staff have had computer forensics training.

Result

Step 5 – ISP Availability

Reference:	Personal Experience
Control Objective:	This step will verify that the organization has a written agreement with a reputable vendor to provide for a consistent and reliable connection to the Internet.
Risk:	The organization's ability to conduct business normally may be hindered or prevented due to an unstable Internet connection.

Compliance:	While several subjective aspects may apply to this step, overall the company will either have a satisfactory contract or not. A respectable ISP will have a contract to protect its interests and the organization should have verified whether or not the provisions in the contract are acceptable.
Testing:	1. Review the organization's contract with its ISP. 2. Ensure that the contract clearly states the level of service to be provided and contains provisions for recourse in the event that the service level is not achieved
Objective/Subjective:	Objective
Comments:	

Result

Step 6 – Process Documentation

Reference:	"*Information Security Management Handbook*", [ref. 1] The Firewall Hardening Guide v0.1, [ref. 2] COBIT, [ref. 3]
Control Objective:	This step will determine whether changes to the firewall software and hardware are performed in a controlled and consistent method.
Risk:	Changes to firewall software and hardware result in unexpected functioning of the firewall and expose the internal/external network to vulnerabilities
Compliance:	A range of possible outcomes exists for this step. • The organization may have a very detailed and time-proven methodology for applying changes to all IT components, • The organization may have a deficient or incomplete process, or • The organization may not apply any change control measures to the management of the firewall.
Testing:	1. Review and assess that change control procedures exist for the firewall software and hardware. The procedures should outline an appropriate and controlled methodology for implementing modifications to the firewall configuration. 2. Select a sample of changes made to the firewall and request supporting documentation. 3. Review the documentation for appropriateness and ensure that it complies with the change management process. This sample will also be used for the completion of steps 7, 8, 9 and 10.

Objective/Subjective:	Subjective
Comments:	

Result

Step 7 – Segregation of Duties

Reference:	COBIT, [ref. 3] Personal Experience
Control Objective:	This step will verify that changes to the firewall's configuration are made and reviewed by appropriate personnel.
Risk:	Inappropriate or lack of proper separation of duties in regard to firewall changes can result in detrimental modifications to the firewall environment.
Compliance:	A range of possible results exists for this step. This aspect is an important component to the overall quality of the change management process itself. Major functions must be logically separated.
Testing:	1. Review the change management procedures to ensure that guidelines exist governing who may implement and who is responsible for reviewing changes made to the firewall. 2. Evaluate whether or not the personnel assigned these duties for the firewall are appropriate. 3. Verify that the procedures are being followed by reviewing the sample documentation selected in step 6.
Objective/Subjective:	Subjective
Comments:	Personnel should not be responsible for both the approval (covered in step 9), implementation and review of changes. A competent network/firewall manager could have the responsibility of implementing a modification, while an equally competent network/firewall manager reviews the change and ensures that the firewall change has been applied appropriately. Ideally, the review should be performed by a knowledgeable member of the quality assurance department.

Result

Step 8 – Updates and Fixes

Reference:	**"***Information Security Management Handbook***"**, [ref. 1] The Firewall Hardening Guide v0.1, [ref. 2] Personal Experience
Control Objective:	This step should determine if an approved process exists for applying "fixes" and other updates to the firewall so that emerging threats are addressed as soon as possible.
Risk:	If updates are not applied within an appropriate time period they expose the firewall and network to newly developed threats and vulnerabilities
Compliance:	A range of possible results exists for this step. While the existence of appropriate change management procedures is important, it is also important to have "emergency" change procedures. The company may have adequately addressed this in the change management procedures or this aspect may have been overlooked.
Testing:	1. Verify that the process for applying critical fixes to the firewall to prevent the exploitation of a newly discovered vulnerability exists and is being followed 2. Utilize the sample taken in step 6 to ensure that the process is functioning as intended (if any emergency changes have been made).
Objective/Subjective:	Subjective
Comments:	

Result

Step 9 – Approvals

Reference:	COBIT, [ref. 3] Personal Experience
Control Objective:	This step will verify that changes to the firewall environment are not applied unless properly approved.
Risk:	Unapproved changes to the firewall can result in the firewall not performing as intended or expected.
Compliance:	Approvals for changes to the firewall will either be documented or not. However, the evaluation of appropriateness of the approvals can vary. A change should only be approved by an appropriate level of management.

Testing:	1. Evaluate whether or not changes are approved by a proper level of management. 2. Review the sample documentation selected in step 6 to verify the procedures are being followed.
Objective/Subjective:	Subjective
Comments:	It is most likely impossible to ensure that all changes are properly reviewed and approved. Therefore, a compensating control should also be implemented through the host system, Windows NT. Logging access to the firewall libraries should be enabled and periodically reviewed by the security officer or a member of quality assurance. Changes should be able to be traced back to proper documentation.

Result

Step 10 – Test Plans

Reference:	COBIT, [ref. 3] Personal Experience
Control Objective:	This step will determine if changes to the firewall's hardware and software configuration are adequately tested before implementation to ensure that expected results are achieved.
Risk:	Untested software or hardware changes are implemented and result in unexpected functioning by the firewall system.
Compliance:	Testing plans for changes to the firewall will either be present or not in the change control documentation. However, there can be a wide range of results in this step depending on how thoroughly changes were tested before being promoted into the production environment.
Testing:	1. Utilize the sample selected in step 6 to ensure that recent changes are compliant with appropriate testing procedures. 2. Determine whether or not the tests conducted were adequate for the change being made.
Objective/Subjective:	Subjective
Comments:	

Result

Step 11 – Computer Room Access

Reference:	"*Information Security Management Handbook*", [ref. 1] COBIT, [ref. 3] Personal Experience
Control Objective:	This step will verify that access to the firewall hardware is restricted to appropriate personnel.
Risk:	Unauthorized physical access to firewall hardware can result in deactivation of the firewall as well as considerable damage to the physical equipment and the equipment of other computing systems.
Compliance:	Each staff member with access to the computer room will have a valid reason for such access. Any staff without an approved reason should be removed.
Testing:	1. Review the physical environment protection measures. 2. Review a list of personnel access to the computer room (or firewall hardware location) to ensure that only personnel with a verified need are allowed access.
Objective/Subjective:	Objective
Comments:	In most computing environments, only operations personnel, maintenance personnel and network engineers are allowed physical access to the firewall equipment. Some other exceptions may include vendors and custodial personnel. Any other access to computing resources should be investigated.

Result

Step 12 – Guest Access

Reference:	"*Information Security Management Handbook*", [ref. 1] COBIT, [ref. 3] Personal Experience
Control Objective:	This step will determine whether an approved process exists for granting visitors physical access to the computer resources. It will also verify that current access by guests is properly authorized.
Risk:	Access granted to non-employees presents substantial risk to the firewall hardware environment and risks the disruption of normal firewall operation.
Compliance:	Each guest with access to the computer room will have a valid reason for such access. Any access to the computer room that appears invalid should be discussed with management.
Testing:	1. Review the procedure for allowing non-employees access to the computer room or other area(s) housing the firewall.

	Each guest should have valid purpose for the access. 2. Procedures should exist stating that an appropriate employee of the company will accompany all other visitors to the computer room.
Objective/Subjective:	Objective
Comments:	Typically, only vendors and, in some cases, consultants will have this type of access.

Result

Step 13 – Monitoring

Reference:	"*Information Security Management Handbook*", [ref. 1] COBIT, [ref. 3] Personal Experience
Control Objective:	This step will verify that physical access to the firewall is documented and reviewed on a periodic basis.
Risk:	Inappropriate physical access may go undetected and result in the disruption of normal firewall operation.
Compliance:	Access to the computer room (or other area containing the firewall) is either logged/reviewed or not. Appropriate access consists of approved personnel during normal expected hours (per the employees schedule) and with normal frequency.
Testing:	1. Review physical access logs. 2. Ensure that any suspicious activity (e.g. unscheduled after-hours or weekend access) is noted and investigated. 3. Ensure that controls are in place to prevent the alteration of physical access logs.
Objective/Subjective:	Subjective
Comments:	

Result

Step 14 – User Accounts in IM

Reference:	CV Firewall Administrator's Guide, v 3.0, [ref. 4] COBIT, [ref. 3]
Control Objective:	This step will determine if access to the IM firewall Service and Firewall Manager is secured logically within the IM Firewall software.

Risk:	Unauthorized logical access can result in changes being made without management review or approval.
Compliance:	Appropriate logical access to the firewall can be determined by evaluating logical access controls. Each user established should have a valid need for such access. Any users without such a need should be removed.
Testing:	1. Identify all users with administrative access to the IM firewall. {The Windows NT "User Manager" utility must be used to identify accounts with "administrative" access. Start > Programs > Administrative Tools > User Manager then "double-click" on the "Administrators" group.} 2. Evaluate whether the access is appropriate and has been approved by management. 3. Determine if management periodically reviews access to the firewall. 4. Ensure that no generic accounts are being used and that no accounts are shared.
Objective/Subjective:	Objective
Comments:	The IM firewall does not have the capability to create individual user accounts within the Firewall Manager component to manage the firewall configuration. Users with "Administrator" access on the Windows NT box have the ability, given that they know the firewall password.

Result

Step 15 – IM Workstation

Reference:	CV Firewall Administrator's Guide, v 3.0, [ref. 4] The Firewall Hardening Guide v0.1, [ref. 2]
Control Objective:	This step will determine whether physical access to the IM workstation within the computer room and any remote workstations configured with the firewall-managing program is limited (as much as possible) to only authorized personnel. This step will also investigate what can be done if physical access is obtained.
Risk:	Unauthorized changes to the firewall configuration could occur and result in the firewall not performing as intended.
Compliance:	Access to IM terminal is limited to only approved users. Controls are implemented which prevent unauthorized users from modifying the firewall plan in the event that access is obtained (e.g., individual NT workstation accounts, keyboard

	lock, workstation lock, etc.)
Testing:	1. Ensure that physical access is as limited as possible. 2. Investigate if access to the firewall configuration can be achieved solely through physical access. {Utilize a non-administrator account and attempt to start the Firewall Manager and access configuration settings. Start > Programs > Internet Manager >Firewall Manager, you will then be prompted to enter a password and attach to a firewall, -try to enter a password and attach to a firewall, -try to check the "default password" password box and attach to a firewall, -try entering no password and attaching to a firewall, -try to enter a password and click the "work offline" button, -try to click the "work offline" button without a password, -etc. Most attempts will fail, however, it should be possible to execute the "work offline" option and open a firewall "plan" (configuration file). Firewall plan files end with an extension of ".ogm". If a plan is opened, try having an administrator alter a minor setting, and then try attaching to a firewall again by going to the File menu and selecting "Attach to Firewall".} NOTE: A change to the plan file will not alter the production firewall service unless the plan is saved to the firewall. No changes will occur upon attachment to a firewall. 3. Verify that a keyboard lock or other device is/can be used to secure any IM workstation. 4. If a physical mechanism cannot be used, ensure that procedures exist to lock the workstation before leaving it unattended. Determine whether a screen-saver lock is implemented. {A screen-saver, workstation lock is enabled within the Windows Display Options in the "Screen Saver" tab.} 5. Determine if the IM Firewall files are "audited" within NT to detect if files are altered. {Open Windows NT Explorer, identify the IM folders (usually "c:\imfw" and "c:\program files\elron software"), left-click on the folder, go to "Properties", then click on the "Security" tab, then press the "Auditing" button.}
Objective/Subjective:	Objective

Comments:	Physical access to any workstation with the capability to manage the firewall configuration presents a significant risk. It is not necessary to supply a password to work on a firewall "plan". The IM Firewall plans are actually configuration files that are applied to the firewall service. Plans can be modified "off-line" and then applied to the firewall service at a later date.

Result

Step 16 – Access to Files through Windows NT

Reference:	CV Firewall Administrator's Guide, v 3.0, [ref. 4] Personal Experience
Control Objective:	This step will evaluate whether logical access to all program and data files supporting the operation of the firewall are protected from unauthorized access.
Risk:	Unauthorized changes to the firewall programs or data files can result in the improper functioning of the firewall.
Compliance:	Appropriate logical access to the files that comprise the firewall can be determined by evaluating logical access controls implemented in Windows NT. Each user with such access should have a valid need for the access. Any users without such a need should be removed.
Testing:	1. Obtain dataset access list(s) for the IM Firewall files. {The Windows NT file permissions must be reviewed. One way to do this is to open the "Windows NT Explorer" and locate the directories where IM is installed. Typically in "c:\imfw" and "c:\program files\elron software". IF the "User Authentication" service is installed (for remote access), an additional directory will exist, "c:\ogua". See step17 for more information. "Right-click" on the directories and go to the "properties" option then to the "security" tab and then to "permissions".} 2. Review to ensure that access is appropriate, approved by management and periodically reviewed.
Objective/Subjective:	Objective
Comments:	

Result

Step 17 – User Authentication and Remote Access

Reference:	CV Firewall Administrator's Guide, v 3.0, [ref. 4]

Control Objective:	This step will determine if all remote access is appropriate and properly approved.
Risk:	The firewall and internal network may be compromised due to unauthorized remote access to the firewall configuration.
Compliance:	Remote access to the firewall parameters should be limited to as few personnel as possible. As with steps 15 and 16, existing access should be supported with a valid business need. Any unsupported access should be removed. .
Testing:	1. Ensure that remote access to the firewall is limited to only those personnel who require it to perform their job duties. {View the enabled services, the "User Authentication" service will be shown in the "Master Security Plan" window if remote access is permitted.} 2. If the "User Authentication" service is installed, users must be reviewed through the "UA Server" module. {When user authentication is installed, another directory is created which contains the "oguasrvr.exe" program (c:\ogua\). This service must be started and then a list of users with the current status of any connection is displayed. To get a complete list of remote users, the "configure" button must be pressed, Note that the remote administrator password is required to get the "User Authentication – Maintenance" screen. Also note that if a user is selected for "modify", the user's account password is displayed in clear text. This appears to be a system limitation.} 3. Check to see that access is regularly reviewed.
Objective/Subjective:	Objective
Comments:	

Result

Step 18 – Critical Files and Directories

Reference:	Internet Manager Firewall version 3.0.5 ReadMe file, [ref. 5]
Control Objective:	This step should ensure that the critical files and directories of the firewall are regularly backed-up and available on and off-site in the event of an emergency.
Risk:	The firewall's configuration cannot be restored in the event of an emergency or a timely recovery cannot be made.

Compliance:	The IM Firewall files and directories are identified within the ReadMe file above. These files/directories should also exist in backups jobs executed on the Windows NT computer.
Testing:	1. Identify the critical files of the Elron IM Firewall. 2. Ensure that these files are included in regular backups and that the backups can be available within a reasonable amount of time.
Objective/Subjective:	Objective
Comments:	

Result

Step 19 – Recovery Tests

Reference:	The Firewall Hardening Guide v0.1, [ref. 2] COBIT, [ref. 3] Personal Experience
Control Objective:	This step will verify that the procedures for restoring the IM Firewall hardware and software provide for recovery of the system within a reasonable time and that the procedures have been validated through regular testing.
Risk:	Recovery procedures do not adequately provide for the restoration of the firewall and, therefore, recovery of the firewall is significantly delayed or even prevented in the event of a disaster.
Compliance:	Testing documentation for the firewall will either be present or not. Factors such as whether a disaster recovery plan exists, whether the firewall is included in it, whether appropriate recovery steps are documented, and whether or not the plan has been tested and documented will need to be reviewed to determine if compliance is satisfactory or lacking.
Testing:	1. Verify that adequate recovery procedures are documented and stored both on and off-site. 2. Review documentation previous disaster recovery tests to ensure that the firewall has been successfully recovered in a reasonable amount of time.
Objective/Subjective:	Objective
Comments:	

Result

Step 20 – Services

Reference:	"*Information Security Management Handbook*", [ref. 1] The Firewall Hardening Guide v0.1, [ref. 2] SANS Institute [ref. 6]
Control Objective:	This step will verify that only the Internet services that have been expressly approved by management for valid business purposes are permitted to pass through the firewall.
Risk:	Internet services containing known vulnerabilities or exploits are allowed through the firewall and place the organization's internal network at risk of compromise. Internal services that consume significant resources and are not required for business purposes are allowed through the firewall and degrade the performance of the network.
Compliance:	All Internet services should be blocked. Any services that are allowed should have a valid business reason. Any rules that cannot be supported with a business need should be removed.
Testing:	1. Review the firewall settings and verify that only approved services are allowed (allowed services should also comply with the organization's Internet access policy). {Obtain the IM Firewall "Master Security Plan Details" report; File > Print MSP Details.} The only information not noted on the MSP report is "Application Filter Commands". {Application Filter Commands can be reviewed by left clicking on the Inbound/Outbound square next to each service and choosing "custom". If Application Filter Commands is enabled it will show under the "Action" heading. Double-click on the "Filter Application Layer Commands" box to view the services.} 2. If possible utilize network-scanning tools to ensure that only authorized services are enabled. Some tools are; Ceribus -- http://www.cerberus-infosec.co.uk/cis.shtml Netscan -- http://www.netscantools.com/nstdownload.html Sam Spade -- http://www.pelttech.com/security/tools.htm Superscan -- http://www.pelttech.com/security/tools.htm 3. If possible utilize network vulnerability tools to ensure that the firewall is not susceptible to know vulnerabilities. Some tools are; WINDump - http://windump.polito.it/ Nessus - http://www.nessus.org (Linux only) Internet Scanner - http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php NOTE: Always inform the appropriate networking personnel

	BEFORE executing any scans against the network. Obtain permission, in writing if possible, to use the tools chosen.
Objective/Subjective:	Objective
Comments:	The IM Firewall provides a very useful report for verifying enable services. The "Print MSP (master security plan) Details" under the file menu produces a document (print only) that details the firewall's configuration. This document is easily compared to the organization's Internet access policy. "**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.)" "*Information Security Management Handbook*", [ref. 1]

Result

Step 21 – Patches

Reference:	"*Information Security Management Handbook*", [ref. 1] The Firewall Hardening Guide v0.1, [ref. 2] Personal Experience
Control Objective:	This step will verify that the firewall software is up-to-date regarding fixes to know security vulnerabilities.
Risk:	The firewall and internal network are compromised through the exploitation of a known vulnerability for which a fix existed.
Compliance:	The current implementation of the firewall will be compliant if it is up-to-date on the latest vendor fixes that exist to correct vulnerabilities.
Testing:	1. Verify that the version of the firewall software is current. Review "reputable" resources to determine if any known vulnerabilities exist within the firewall software. {Under the "Help" menu choose "About".}

	2. Ensure that fixes (if they exist) to these vulnerabilities have been applied.
Objective/Subjective:	Objective
Comments:	Utilize (at least) the following web sites or equivalent sources to determine if known vulnerabilities exist: www.securitytracker.com, online.securityfocus.com and www.securiteam.com.

Result

Step 22 – Alerts

Reference:	**"***Information Security Management Handbook*", [ref. 1] The Firewall Hardening Guide v0.1, [ref. 2] SANS Institute [ref. 6] Personal Experience
Control Objective:	This step should verify that the firewall software protects the company's network by monitoring for potentially harmful activity and notifies appropriate personnel in the event such activity is detected
Risk:	Attacks from the Internet (e.g. Ddos) are not recognized or are not recognized within an appropriate amount of time, leading to the compromise of the organization's firewall and network
Compliance:	The firewall will be compliant if it is configured to monitor for possible Internet attacks and notify the appropriate personnel upon detection of an attack.
Testing:	1. Review to determine what events are being recorded. {Utilize the Logs > Events and Logs > Traps option to verify that events are being accumulated and that they are appropriate.} 2. Ensure that appropriate notification occurs when an alert is generated. {Review the e-mail alert settings by going to the "Options" menu and selecting "Notification".} {Review the on-screen alter configuration by clicking on the "Options" button in the "Firewall Traps" window.} 3. Ensure that personnel have procedures with appropriate response actions.
Objective/Subjective:	Objective
Comments:	NOTE: Events and traps in the Elron IM Firewall both accumulate and monitor network traffic. Traps are configured to notify personnel through e-mail and/or on-screen alerts when

	a threshold has been exceeded.

Result

Step 23 – Logs

Reference:	**"***Information Security Management Handbook*", [ref. 1] The Firewall Hardening Guide v0.1, [ref. 2] Personal Experience
Control Objective:	This step will verify that the firewall software logs significant activity and retains logs to aid in the detection of potential Internet attacks or to aid in diagnosis of firewall/network problems.
Risk:	Potential Internet attacks go undetected and/or network and firewall problems require an extensive amount of time to diagnose because appropriate logs are not recorded and retained.
Compliance:	The firewall will be compliant if it has been configured to log all significant activity. The logs are retained for a reasonable amount of time to aid in the detection of attacks or in the diagnosis of problems.
Testing:	1. Review to determine what events are being recorded. {Utilize the Logs > Statistics option to verify that logs are being accumulated and that they are appropriate.} 2. Ensure that the events are logged and retained for an appropriate amount of time.
Objective/Subjective:	Objective
Comments:	**"**You can save logs to the Firewall Manager computer for analysis and troubleshooting. When you attach to the firewall through Firewall Manager, you can view and save a file to the Firewall Manager computer. If you want a log of events at the beginning and end of the day, access the desired log once at the beginning of the day, then once at the end. Do this by clicking on the *Events* or *Traps* button in Firewall Manager or choosing the appropriate log from the **Logs** menu. This saves a copy of the log the *Program Files\Elron\Firewall Manager* directory. If you access the logs several times a day, rename the files in this folder so that nothing is overwritten. The Events Logs are saved as ".elg" files while the Traps Logs are saved as ".trp" files in the form of their corresponding date, e.g., 04101999.elg for April 10th, 1999." CV Firewall Administrator's Guide, v 3.0, [ref. 4], p. 176. The appropriate length of retention of logs can vary from company to company. It may be helpful to consult the legal

	department when determining this.

Result

Step 24 – Proactive Monitoring

Reference:	**"***Information Security Management Handbook*", [ref. 1] Personal Experience
Control Objective:	This step will determine whether network personnel (particularly the firewall administrator) frequently review relevant news and technical sources to determine whether new vulnerabilities to the firewall software have been discovered.
Risk:	The firewall and/or internal network is compromised due to a newly discovered vulnerability. Precautions could have been taken against the attack if network personnel had been knowledgeable.
Compliance:	There can be a range of results from this step. If the company has hired appropriately qualified and responsible personnel, it is likely that they proactively monitor for vulnerabilities.
Testing:	1. Interview network personnel and review relevant documentation if possible to determine that the firewall administrators stay current with issues regarding the firewall technology.
Objective/Subjective:	Subjective
Comments:	One of the only ways to keep up with emerging threats is to constantly review reliable sources for current news.

Result

Step 25 – Obstructive Software

Reference:	CV Firewall Administrator's Guide, v 3.0, [ref. 4] **"***Information Security Management Handbook*", [ref. 1]
Control Objective:	This should ensure that the firewall hardware and software functions as intended and is not impeded by the presence of other software running concurrently and utilizing the same computing resources.
Risk:	The firewall fails to function or functions inappropriately as a result of other software that interferes with its performance
Compliance:	The firewall is compliant if no other software or, at a minimum, no other resource intensive software operates on the same hardware as the firewall.

Testing:	1. Obtain an inventory of programs on the Windows NT box. {One way is to use the DOS "dir" command and export the results to a text file. "dir *.exe > pgms.txt"} 2. Review the inventory to identify programs that are not needed.
Objective/Subjective:	Objective
Comments:	"We strongly recommend using a dedicated computer for CV Firewall. While it is not required, we suggest not running other than default NT Services on this system. CV Firewall will be the last link on your network before the physical gateway to your Internet Service Provider (ISP). Keep this computer as secure as possible." CV Firewall Administrator's Guide, v 3.0, [ref. 4], p. 12. **Remove Unneeded System Components.** Software such as compilers, debuggers, security tools, etc. should be removed from the firewall. **"***Information Security Management Handbook*", [ref. 1]

Result

Step 26 – VPN

Reference:	CV Firewall Administrator's Guide, v 3.0, [ref. 4]
Control Objective:	This step will determine whether or not the VPN settings in the IM Firewall have been established according to company requirements.
Risk:	Inappropriate VPN settings could give users a false sense of security in the transfer of confidential information. Confidential information could subsequently be disclosed to unauthorized persons.
Compliance:	The firewall will be compliant if: an appropriate encryption method is used, the appropriate services are encrypted, and appropriate procedures exist for maintenance of the VPN, including key management.
Testing:	1. Verify that the VPN facility within the IM Firewall has been enabled and that an appropriate encryption and authentication protocol has been enabled. {Observe the services enabled in "Master Security Plan" window, VPN and a key management service such as IKE will be present. Display encryption by using the VIEW > VPN > Encryption Protocol. Display encryption by using the VIEW > VPN > Encryption Protocol.} 2. Ensure that the appropriate services (e.g. E-mail, FTP) have the encryption service enabled. The Internet Security policy

	should state what services are required to pass through a VPN. {At the "Master Security Plan" window left-click on the service (e.g. E-mail Outbound) that you want to verify. Select Custom and verify that the Action parameter has "Encrypt" enabled.} 3. Obtain and review policies and procedures applicable to the VPN and ensure that they are adequate to support its operation.
Objective/Subjective:	Objective
Comments:	The completion of this step should not be considered a full review of the company's VPN. The VPN itself can be a separate audit. This step should, however, verify that a VPN has been implemented and that the appropriate services are being encrypted. The module in IM Firewall is intended to create a VPN between two IM Firewalls. NOTE: Items 1 and 2 can also be verified through the printout of the "Master Security Plan details" report.

Result

Assignment 3 – Conduct the Audit

Overview

Overall, most of the "Objective" steps have been selected as having the most significant security concerns. These steps (14, 15, 16, 17, 18, 20, 21, 22, 23, and 25) are explained in greater detail. It can be difficult to quantify the implications resulting from a "Subjective" test. The resulting risk is highly dependent on the type of environment, compensating controls, and the opinion/evaluation of the reviewer. For the "Subjective" steps (and steps that have not been selected for a detailed explanation), a favorable evaluation will be assumed and qualities will be listed that would be present if the criteria for compliance were fully met.

The system parameters for Windows NT and the IM Firewall were verified with the help of the firewall administrator.

Step 1 – Internet Policy

Result:

1. The Internet Policy was developed by the security officer along with network personnel including the firewall administrator and Chief Information Officer. The CEO of the organization has endorsed the policy with a signature and fully supports its enforcement.
2. The policy was used as a guiding document during the configuration of the firewall and the policy is also used periodically to verify the firewall settings.
3. Changes to the policy can be initiated by supervisory level personnel or above as long as valid reasons exist for the change. Changes are reviewed by the security officer, CIO and firewall administrator and approved by the CEO.
4. The policy is reviewed each time a change is initiated to ensure that the appropriate control mechanisms are still in place and to determine if any other modifications need to be made. All employees of the company have signed an acknowledgement stating that they will abide by the policy.

Step 2 – Firewall Documentation

Result:

1. The firewall manager has a copy of "Command View Firewall Administrator's Guide" version 3.0.
2. The firewall manager and other support personnel have an up-to-date LAN and WAN diagram for the company's network. The firewall manager and other support personnel have a current hardware and software inventory for all resources supporting

the firewall. The firewall manager and other support personnel have also documented the firewall's current configuration.

Step 3 – Management Procedures

Result:

1. The organization's firewall management procedures were developed by the firewall manager with input from the security officer and network engineers.
2. The procedures contain documentation regarding Internet services management, review and retention of logs, and indicators of potential attacks. The procedures also include the latest version of the company's Internet security policy and a parameter-by-parameter confirmation of how the firewall's configuration is compliant with and enforces the Internet security policy. Procedures also exist to manage logical access to the firewall.

Step 4 – Emergency Procedures

Result:

1. The firewall manager, security officer and network engineers have developed a section within the management procedures that deals with response measures to be taken in the event of a suspected Internet attack. The procedures describe what types of events are to be logged and why. The procedures detail methods that can be used monitor and properly record relevant events and the proper responses to be to be taken if the attack presents the appearance of being damaging to the company's network and other computing resources.

Step 5 – ISP Availability

Result:

1. The organization does have a legally binding contract with its ISP. The contract details services, charges for those services, and the time-span during which the services are provided.
2. The contract also specifies a service-level to be provided to the organization as well as circumstances that will result in the refund of fees to the organization in the event that the service-level is not achieved.

Step 6 – Process Documentation

Result:

1. The organization has a successful SDLC methodology as well as a detailed change management process. These procedures are applied as applicable to the changes implemented on the company's firewall. The change management procedures provide a structured process to be followed that includes change initiation, analysis, testing, approval and implementation.
2. A sample of changes made over the past year was selected.
3. A cursory review of change documentation appears to validate adherence to the established procedures.

Step 7 – Segregation of Duties

Result:

1. The change management procedures do specify who should be responsible for implementation of changes and who should be responsible for the review of changes made to the firewall environment.
2. Changes are implemented by the firewall manager and reviewed by both a member of the quality assurance group and the security officer.
3. The sample documentation verifies that the procedures are being followed.

Step 8 – Updates and Fixes

Result:

1. The personnel responsible for firewall management have developed emergency "fix" procedures. The procedures allow the firewall manager to apply fixes at his/her discretion if the vulnerability is determined to be dangerous and/or the fix is determined to be essential for protecting network resources. After the change is implemented, the firewall manager must validate the application of the fix to both the security officer and network manager. The change must then be documented in accordance with the change management procedures.
2. The procedures are being followed.

Step 9 – Approvals

Result:

1. Changes are approved by an appropriate level of management. The security officer must review and agree with the change, while the network manager is responsible for final approval of the change. If a change is to be made that will have a high impact on the performance or security of the firewall, it must also be approved by the CIO.
2. The procedures are being followed.

Step 10 – Test Plans

Result:

1. Changes are applied to a duplicate test environment before implementation on the production system. Changes are then tested to determine that the expected result is achieved.
2. Only after all involved parties are satisfied that the testing goals are achieved, will the change be implemented on the production firewall. Test procedures in the sample reviewed appeared appropriate for the change being implemented. The last modified date on the current firewall plan was noted and traced back to appropriate supporting documentation.

Step 11 – Computer Room Access

Result:

1. The company offices are protected with a badge-reader physical access system. Additional badge-readers also exist at each entrance to the computer room. Approval of physical access to computing equipment is the responsibility of the computer operations manager or the CIO. Only approved personnel with a legitimate need have been granted physical access.
2. A list of personnel with physical access appears appropriate. This list is reviewed periodically by the computer operations manager.

Step 12 – Guest Access

Result:

1. Approval of guest access to computing equipment is the responsibility of the computer operations manager or the CIO. Only approved guests with a legitimate

need have been granted physical access. A list of guests who have had physical access is reviewed periodically by the computer operations manager.
2. Personnel other than approved employees (i.e. guests) are accompanied by an appropriate representative of the company.

Step 13 – Monitoring

Result:

1. Access to the computer room is automatically logged through the use of a badge-reader access system with built-in logging capabilities.
2. The computer room manager or designated subordinate regularly reviews recorded access to ensure that it appears normal. Any unusual accesses are investigated with the employee and/or the employee's manager.
3. Access to the physical access system is limited to only approved employees.

Step 14 – User Accounts in IM

Result:

1. The IM Firewall does not support individual accounts. Windows NT accounts with "Administrator" access must be used to attach to and change a firewall configuration. A listing of accounts with "Administrator" access is shown in diagram 1. The list was obtained through the Windows NT User Manager utility found within the Administrative Tools group.
2. Access is appropriately restricted and approved.
3. The network and communications manager regularly reviews administrator accounts.
4. No generic accounts are utilized (except for backup) and no accounts are shared.

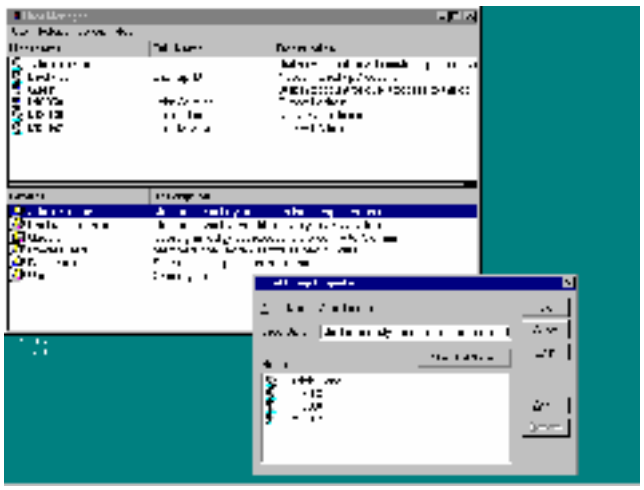


Diagram 1
Accounts with "Administrator" access are displayed (Start > Programs > Administrative Tools > User Manager).

Step 15 – IM Workstations

Result:

1. The workstation supporting the IM Firewall is physically secured within the computer room that has limited access. The computer room workstation is the only workstation that can manage the firewall.
2. Several attempts were made to gain access to the firewall manager program and alter the firewall configuration. The default password has been changed and attempts to log on with the default password or with an invalid password resulted in an "Authentication Error". The Elron software does allow an administrator (or other account) to work on a firewall "plan" through the "Work Offline" option. This option is available upon starting-up "Firewall Manager". A plan is basically a file containing configuration parameters that can be applied to firewall service itself. With physical access, any account can be used to start the firewall manager from the IM managing workstation and initiate this option without a password. Then a "plan" can be selected. (See diagram 2) If the plan is subsequently applied to a firewall service, the parameters will take effect on that firewall. The Firewall Manager must attach to a firewall before the plan can be applied. IM does require a password to attach to a firewall (firewall service). See diagram 3. Appropriate access through Windows NT is needed to alter a plan offline.
3. Due to the fact that the IM workstation is believed to be secure within the computer room, no keyboard lock or other locking mechanism has been installed.
4. Due to the fact that the IM workstation is believed to be secure within the computer room, administrators are not advised to log-off and lock the workstation when not in use. Due to the fact that the IM workstation is believed to be secure within the computer room, no workstation time-out is set, see diagram 4.

5. Due to the fact that the IM workstation is believed to be secure within the computer room, critical system files for the firewall are not audited, see diagram 5 and diagram 6. Windows NT security is not full proof. Tools such as "NTFSdos" and "L0phtcrack" can be utilized to compromise the system if physical access is gained to the workstation.

There is a risk that a firewall plan can be accessed and changed with prior management review or approval. Without auditing, this access could remain undetected. In addition, confidential control information can be obtained.

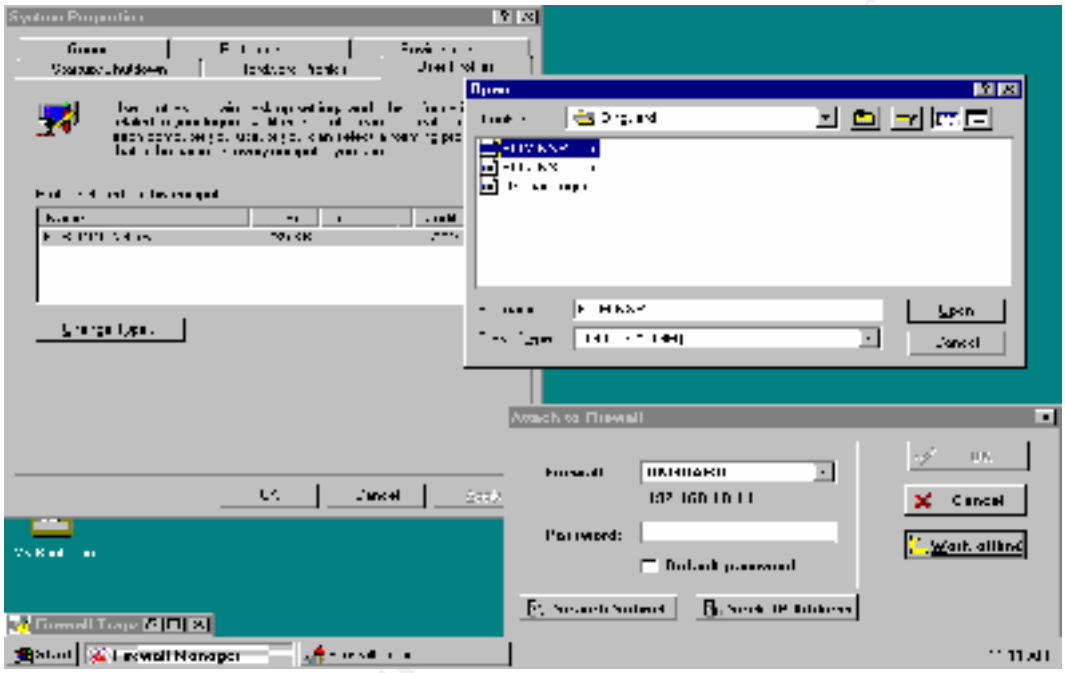


Diagram 2

The guest account (temporarily enabled for this test) is used to start "Firewall Manager", click on the "Work Offline" option and select the ELIMINSP firewall plan without a password. Note, however, that while the "Guest" account can read the information in the plan, it cannot modify the plan due to insufficient rights in Windows NT.

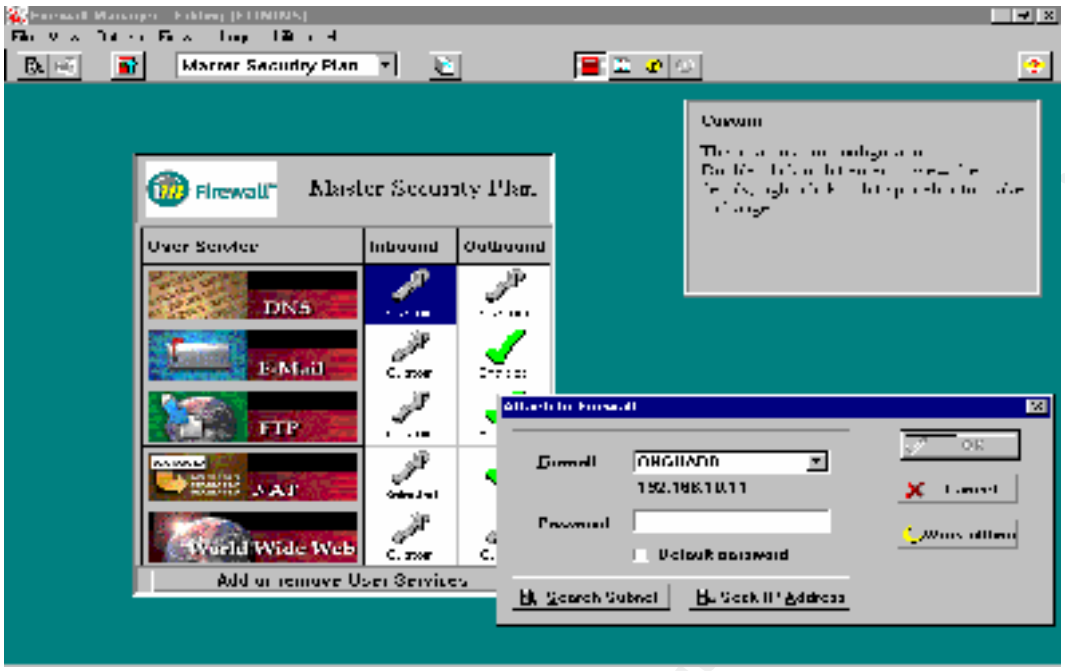


Diagram 3
The firewall manager will not attach to a firewall (firewall service) without a valid password.

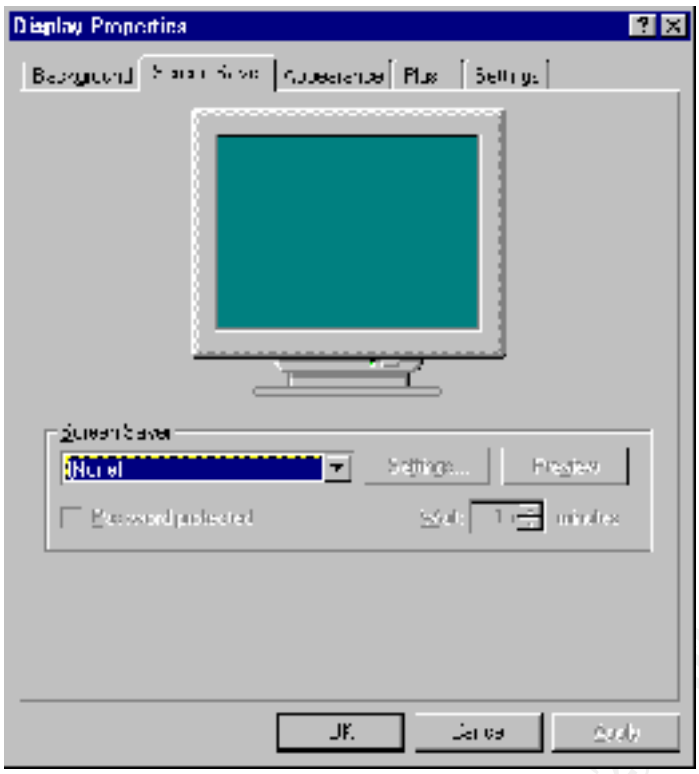


Diagram 4.
No workstation time-out parameters are implemented on Windows NT.

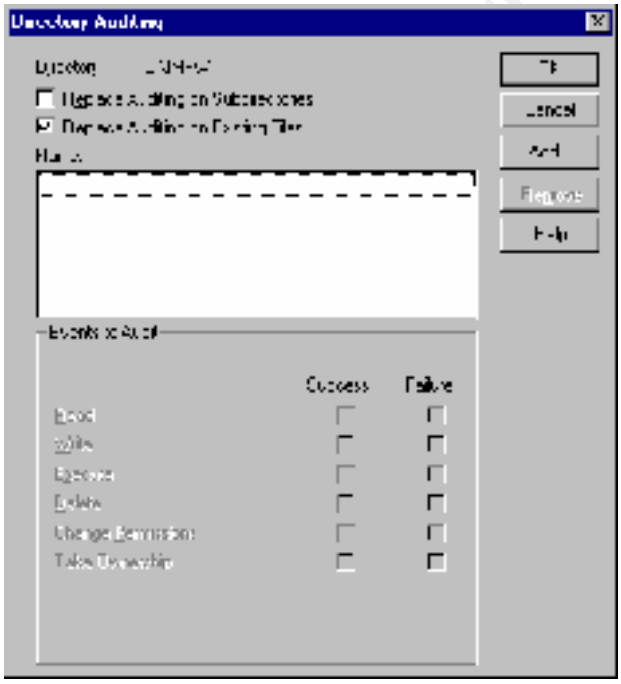


Diagram 5
NT Auditing controls on C:\IMFW.

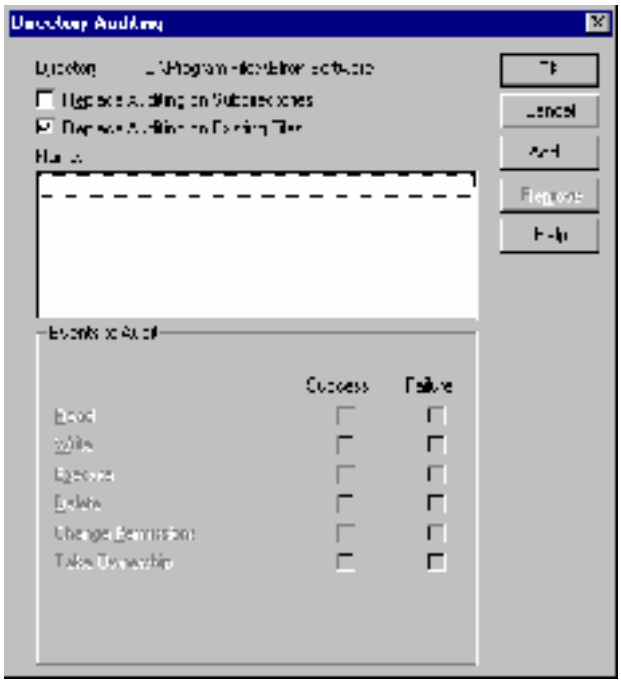


Diagram 6
NT Auditing controls on C:\Program Files\
Elron Software.

Step 16 – Access to Firewall Files through Windows NT

Result:

1. The IM Firewall files are located in "C:\Program Files\Elron Software" and C:\IMFW". "User Authentication" is not installed. Access to these directories is shown in diagram 7 and diagram 8.
2. Only accounts in the "Administrator" group may alter these files. This access is periodically reviewed by the network and telecommunications manager.

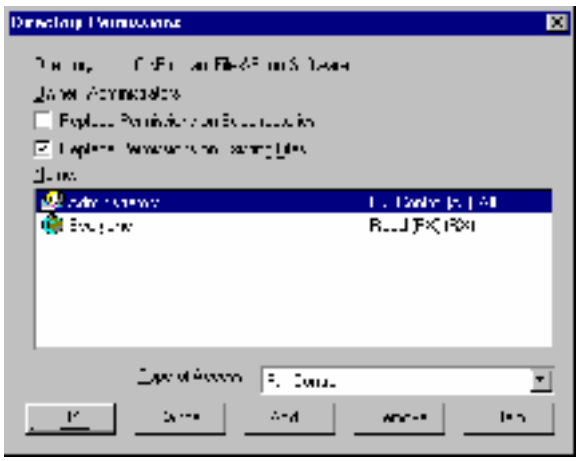


Diagram 7
Access to the "Elron Software" directory is shown (NT Explorer > right-click on directory > Properties > Security tab > Permissions)

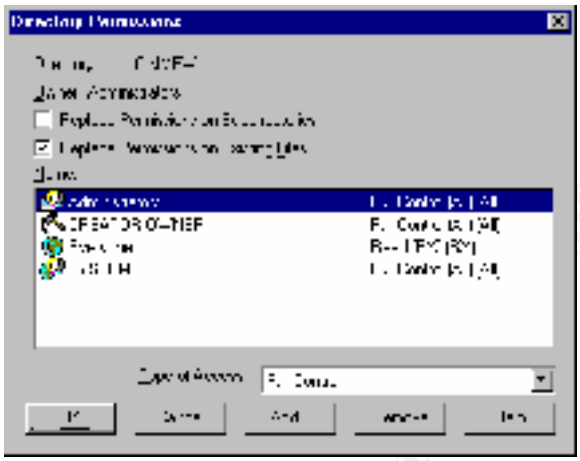


Diagram 8
Access to the "Elron Software" directory is shown (NT Explorer > right-click on directory > Properties > Security tab > Permissions)

Step 17 – User Authentication and Remote Access

Result:

1. In order for remote access to be installed, the "User Authentication" service must be selected. Utilizing the "Add or remove User Services" button the Master Security Plan window, all selected services were displayed (see diagram 9). Remote access to the Firewall Manager has not been activated.
2. Not applicable.
3. Not applicable.

"What Is Required To Run User Authentication?

- A dedicated PC that is using Windows 95 or NT 4.0 to be used as the *UA Server* .CV Firewall can double as your *Authentication Server*. The UA Server can be any PC with a fixed TCP/IP stack on the protected network. The PC needs to be up and running for remote users to login.
- One or more remote PCs running the UA Client software.
- A *CV Firewall* - installed and running.
- The *User Authentication User Service* must be added to CV Firewall's Master Security Plan.
- The *User Authentication Client* component must be added to each remote PC.
- Each user on a remote PC must be added to the *User Authentication Server* with a name and password."

Command View Firewall Administrator's Guide v 3.0, pp. 167-168.

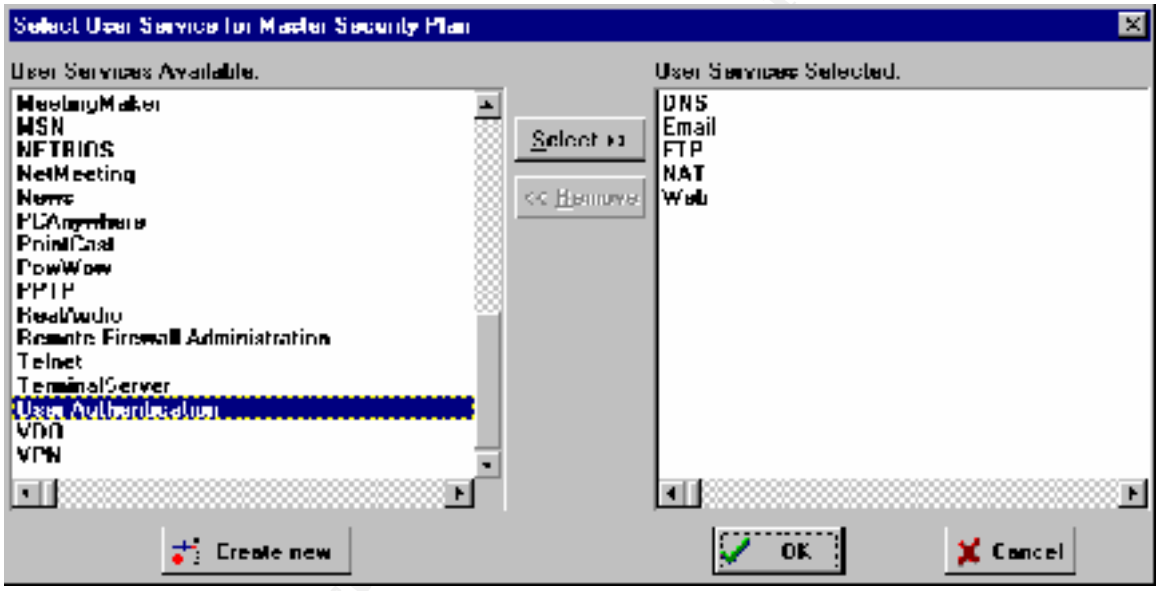


Diagram 9

The "User Authentication" service has not been activated.

Step 18 – Critical Files and Directories

Result:

1. Critical files of the Elron IM Firewall are listed in Appendix 1. The company utilizes the product "Arcserve" to perform nightly backups. Diagram 10 shows that the "ELRONNT" server is being backed-up.
2. Two backup tapes are made. One remains on-site and the other is rotated to an offsite location approximately 25 miles away. The backups could be available within a reasonable amount of time.

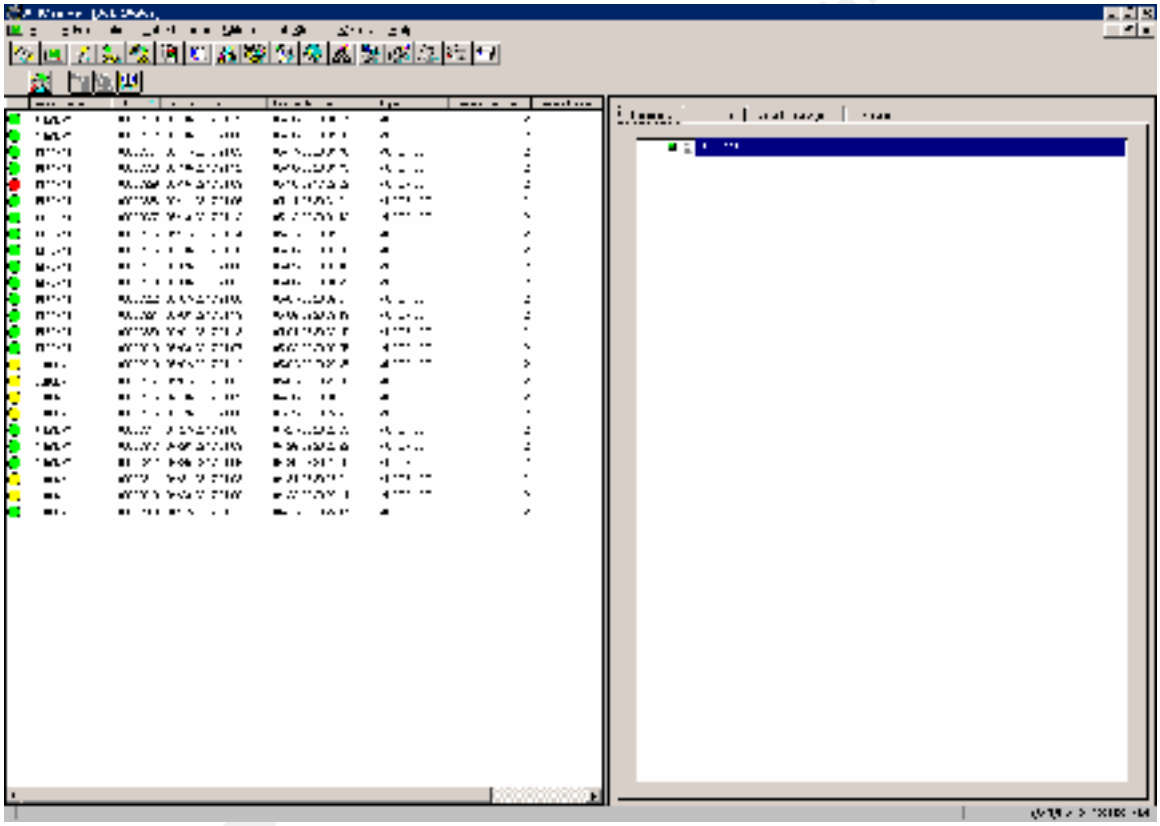


Diagram 10
Arcserve performs daily backups of the "ELRONNT" server.

Step 19 – Recover Tests

Result:

1. Recovery procedures for the Elron IM Firewall are documented. Multiple copies exist of which two are off-site.
2. Two tests performed to recover the firewall have been successful at the company's off-site facility. On-site backup equipment has not been tested. On-site backup equipment could not successfully recover the firewall due to hardware incompatibilities. On-site backup equipment was recently upgraded, however, the network cards (NICs) acquired were not supported by the IM Firewall. The Elron software lists only six certified NICs, see recommended specifications below.

The company may be unable to restore the firewall in the event of a hardware failure.

During the performance of this test, it was noted that the connection protected by Elron was also intended to be a backup connection in the event the company's primary "end-user" Internet connection was disabled. The requirements of the end-user connection are VERY different from the requirements of this connection; however, no alternate "plan" (firewall configuration file) exists for this situation.

"***Recommended Specifications***
• 128 MB RAM
• Pentium 300 MHz or faster
•CD-ROM d rive
• 500 MB Hard Drive Space
• Two 10Mb, 10/100 Mb or 100 Mb Ethernet NICs (three NICs for DMZ). CV Firewall works with a wide variety of NICs. Tested and certified NICs include:
— 3Com 3c509 10 Mb
— 3Com 3c905 10/100 Mb
— Intel EtherExpress 10/100 Mbps
— Intel Pro 10 and Pro100B 10 Mb NICs
— SMC EtherPower 100Mb NICs
— SMC EZ 10 Mb NICs"
Command View Firewall Administrator's Guide v 3.0, p. 12.

Step 20 – Services

Result:

1. A report of the IM Firewall "Master Security Plan" is located in Appendix 2. This plan contains detailed information on the services configured in the IM Firewall. After review and comparison to the Internet policy, some services (highlighted in yellow) appear to be excessive. As noted earlier, this firewall is not used for the primary Internet connection for end-users.
   The Elron firewall also allows administrators to filter application layer commands within the defined services, see diagram 11. Depending on the services permitted, it may be necessary to investigate these since they are not shown on the "Master Security Plan" printout. Only common services have been enabled on the firewall under review, however, a display of application layer commands available for Inbound and Outbound WWW commands was generated. See diagram 12 and diagram 13. The services FTP and E-mail are also configurable in this way. They were reviewed with no exceptions noted. It is important to note that the IM Firewall prevents the customization of application layer commands within services. The services you see listed are the only ones available. This is a good feature that prevents any application layer commands from being "hidden" within services.
2. An exterior scan of the IM Firewall using NetScan produced the following expected results and validated the information contained in the "Master Security Plan";
   "Target Computer List
   192.168.10.11
   00020 - TCP - ftp-data
   00025 - TCP – smtp
   00053 - TCP – domain
   00053 - UDP – domain
   00070 - TCP – unknown
   00080 - TCP – www
   00109 - TCP – pop
   00109 - TCP - pop2
   00110 - TCP - pop3
   00113 - TCP – auth
   00443 - TCP – unknown"
   Scan from: Northwest Performance Software, Inc.
   NetScanTools 4.23 (TM)
   Port 70 is "Gopher", port 443 is "SSL".

Diagram 11
Application Layer Command filter.

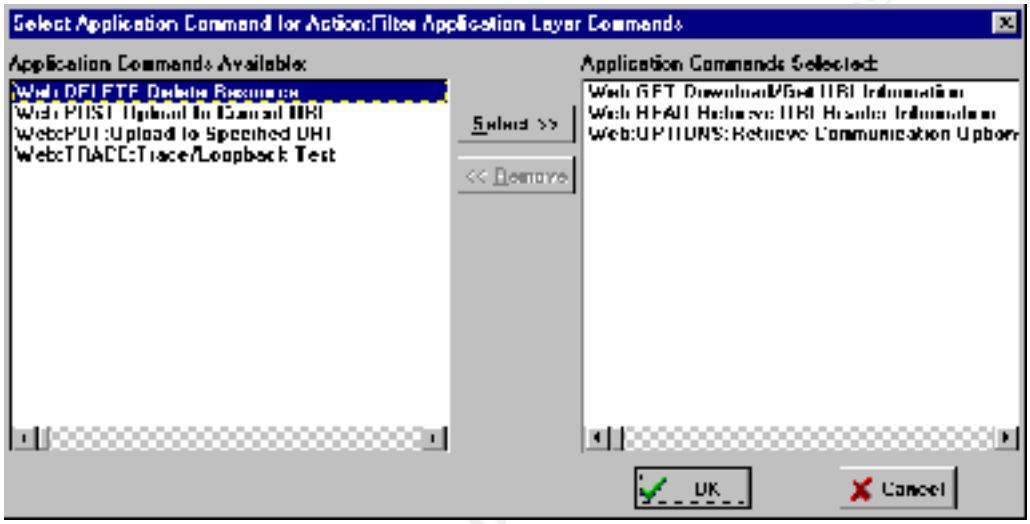


Diagram 12
Inbound Application Commands for Web.

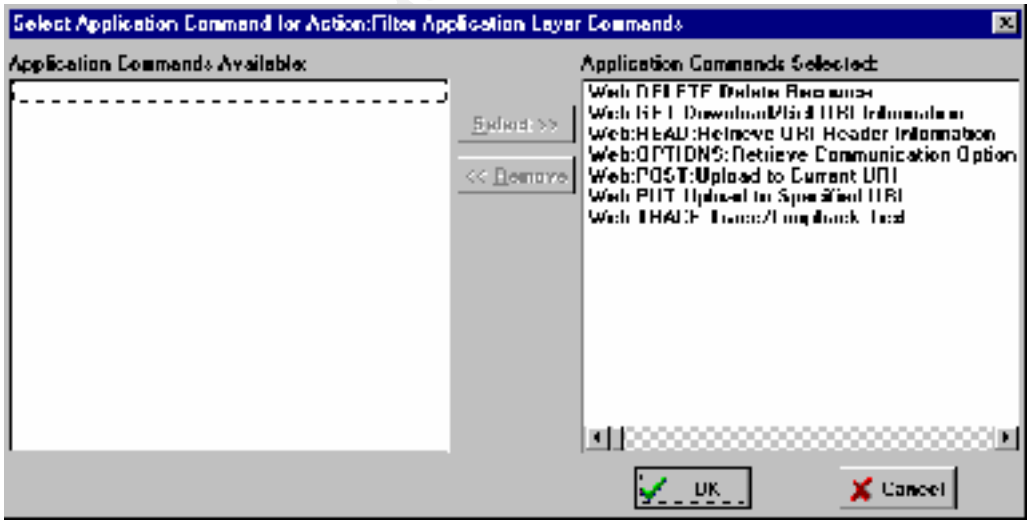


Diagram 13
Outbound Application Commands for Web.

3. Due to the results from step 19, a vulnerability scan could not be executed on the test firewall and system personnel were opposed to the utilization of a vulnerability scanner (e.g. Nessus) on the production firewall. (Step 19 discovered that the backup firewall equipment was not yet functional.) As an alternative to this step, evidence that the IM Firewall product *should be* compliant in this aspect was obtained from the International Computer Security Association (ICSA). This organization performed a "Product Certification" review on the IM Firewall last updated on April 4, 2002. The product was granted ICSA Certification. http://www.icsalabs.com/html/communities/firewalls/certification/rxvendors/elronmanager/labreport_cid302.shtml.
   The following is an excerpt from the ICSA's testing criteria that was used to evaluate the product.

" Security Testing

ST1 - Administrative Access Testing - The Candidate Firewall Product shall demonstrate through testing that no unauthorized control of its administrative functions can be obtained.

ST2 - Vulnerability Testing - The Candidate Firewall Product shall demonstrate through testing that it is not vulnerable to an evolving set of vulnerabilities that are known in the Internet community and that are capable of being remotely tested. Further, the Candidate Firewall Product shall demonstrate through testing that it does not introduce vulnerabilities to private or service network servers.

ST3 - No Other Traffic - The Candidate Firewall Product shall demonstrate through testing that nothing other than that specified in the Required Services Security Policy shall traverse the Candidate Firewall Product and be carried on the private network.

ST4 - Denial of Service - The Candidate Firewall Product shall demonstrate through testing that:

A. It is not rendered inoperable by any trivial denial of service type attacks.
B. It fails closed if rendered inoperable through any denial of service type attack for which there is no known defense. "

Full testing criteria is located on:
http://www.icsalabs.com/html/communities/firewalls/certification/criteria/criteria_3.0a.shtml. The IM Firewall was judged to not be susceptible to any vulnerabilities.

Several services were noted as being unnecessary and non-compliant with the Internet Policy (i.e. no defined business need). See the yellow highlighted portions in Appendix 2. In addition, the services may expose the firewall and interior network to potential threats. Those services are: Inbound - Gopher (port 70), and POP2 (port 109), Outbound – RealAudio (ports 6770 – 7170), RealPlayer (ports 7070 – 7071), RealPlayerUDP (ports

6970 – 7170), RealPlayerG2 (port 554) and Gopher (port 70). See diagram 14. These services are default "subservices" of the WWW user service. They appear to have been activated in error upon installation of the service.

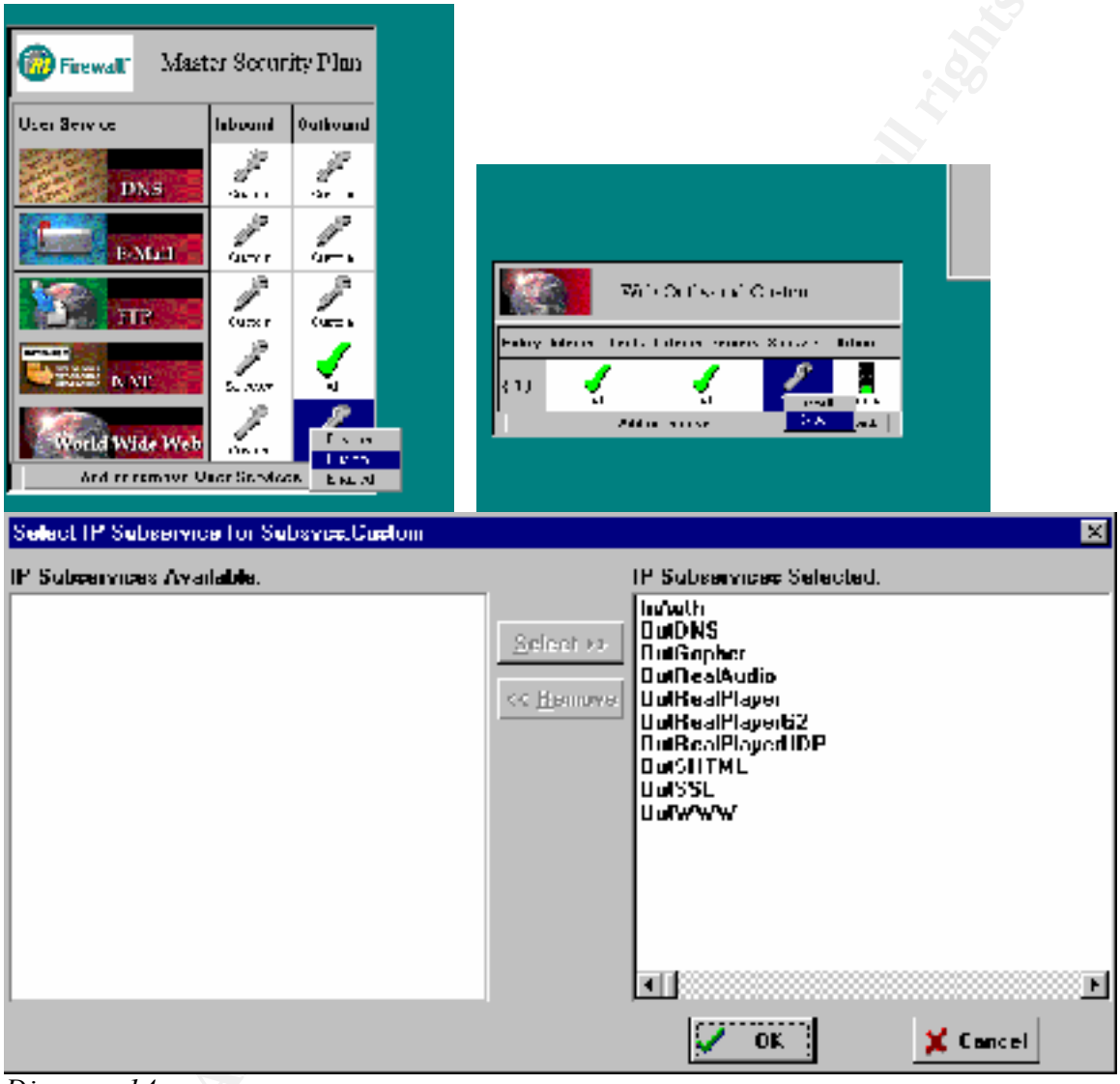


Diagram 14

Subservices of the WWW user service.

On the Master Services Window left-click on the Inbound/Outbound box and chose "custom", then left-click on the box under the "Subservices" heading and choose "custom".

Step 21 – Patches

Result:

1. The company utilizes version 3.0.5 of the IM Firewall, see diagram 15. This is the latest version of the firewall. Information regarding vulnerabilities was gathered from three web sites (see diagrams 16, 17 and 18). www.securitytracker.com, www.securiteam.com, and online.securityfocus.com/
2. Only the Elron Anti-Virus and Elron Message Inspector products have know vulnerabilities. The IM Firewall is not affected and does not require any patches at this time.

Diagram 15
Version 3.0.5, Elron Software's latest IM version.

Diagram 16
Screen-print from Security Tracker.

Diagram 17
Screen-print from Securiteam.

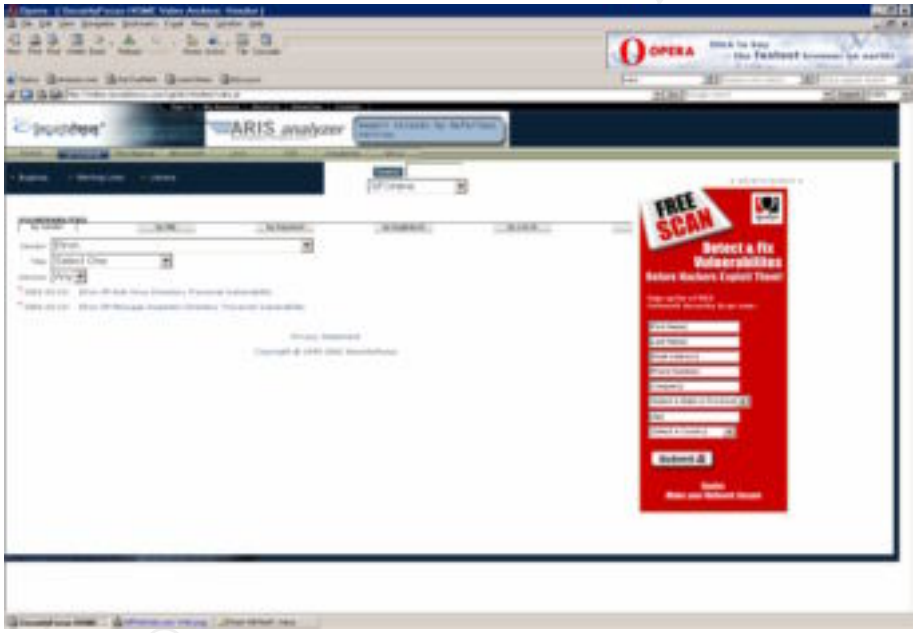


Diagram 18
Screen-print from Security Focus.

Step 22 – Alerts

Result:

1. Diagram 19 is a sample screen-print of IM Firewall Alerts. The firewall appears to record all relevant alert events.
2. The firewall is configured to notify the firewall administrators by e-mail if an event is classified as "Critical" or above. See diagram 20. On-screen alerts are also activated, see diagram 21.
3. Appropriate procedures exist to respond to alert events.

Diagram 19
Alert events in the IM Firewall, see severity explanation below.
Command View Firewall Administrator's Guide, p. 177.

Event Severity Explanation

Severity Levels	***Explanation***	***Examples of this are: (What may cause the event)***
Alarm	These highest severity events are generated when CV Firewall cannot function due to system hardware or software failure. Most of Alarm events are detected during fresh reboot or a power-on.	Failure to allocate memory at start-up because of memory failure on the PC. Ethernet NIC hardware or software failure during the operation.
Alert	Alert events are generated when CV Firewall detects a break-in attempt either by unauthorized users trying to log in or access protected services. These events do not disrupt CV Firewall in any way. Alerts are simply notifications of blocked hacking attempts. Detailed information about the attempt is	IP Spoofing or Impersonation is detected from outside. Authentication failure for a Firewall Manager command. Unauthorized File Transfer

Severity Levels	***Explanation***	***Examples of this are: (What may cause the event)***
	logged as proof of the break-in attempt.	attempt to or from CV Firewall. Certain IP services that are considered hacker favorites are being accessed. Service Restart or System Reboot
Critical	Critical events are generated when user configuration errors are detected. CV Firewall detects certain errors in your configuration that could potentially result in inadvertent break-ins. Critical events can halt the system and should be corrected immediately to ensure proper operation.	High bridge priority if one of bridging ports has been disabled. If this occurs, CV Firewall cannot operate as a security unit and a loop on the network could provide a path for the secure network traffic to flow in and out. Too many Gating Rules or Security Classes are configured for a low memory system. Some IP addresses are accessed that are not configured in the list of internal (secure IP) addresses. IP address conflict. IP address assigned to CV Firewall is used by some other computer.
Error	Error events are generated by CV Firewall System errors. Errors events are not fatal, but degrade CV Firewall system performance. Conditions that cause Error events do not halt CV Firewall operation.	CV Firewall may be running out of memory for storing Ethernet data.
Warnings	Warning events occur due to peculiar network behavior. Warning events are not fatal, but degrade CV Firewall system performance. Some internal system parameters may need adjusting for proper CV Firewall operation on your network. See "Troubleshooting" for more details.	Network Address Translation Table overflow (the table keeping track of NAT relays may fill up). Solution: restart the CV Firewall Service.
Notice	Notice events notify you of something that may be of interest to you. In most cases, Notice events are used for system notices. This is the default event priority for logging events on CV Firewall.	Every time CV Firewall allows or rejects a packet due to configured access rules on your network. A new user login (for Telnet, FTP etc.). A new IP address session establishment. An ARP request to CV Firewall's

Severity Levels	***Explanation***	***Examples of this are: (What may cause the event)***
		IP address. A successful or aborted File Transfer to or from CV Firewall.
Information	Information events are used for detailed packet logs at different protocol layers e.g. at Ethernet, Bridge, IP or IPX layer. These events are useful in tracing configuration problems in your access rule configurations. Information events can also log detailed traffic activity between your network and the outside world.	
Debug	Debug events are of little use to CV Firewall administrator and configuring this event as the event threshold is NOT recommended because the log fills very quickly and important information may be lost. It is good for troubleshooting, however.	

Command View Firewall Administrator's Guide, pp. 181-182.

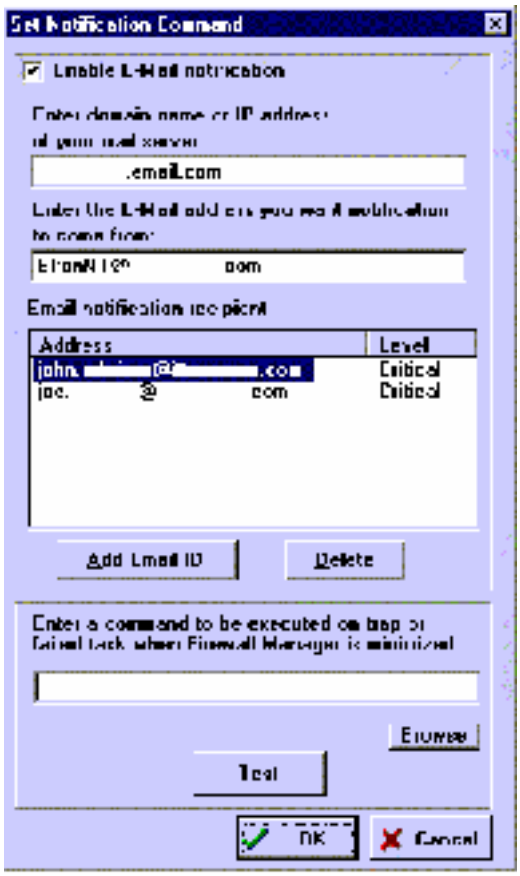


Diagram 20
E-mail notification parameters.

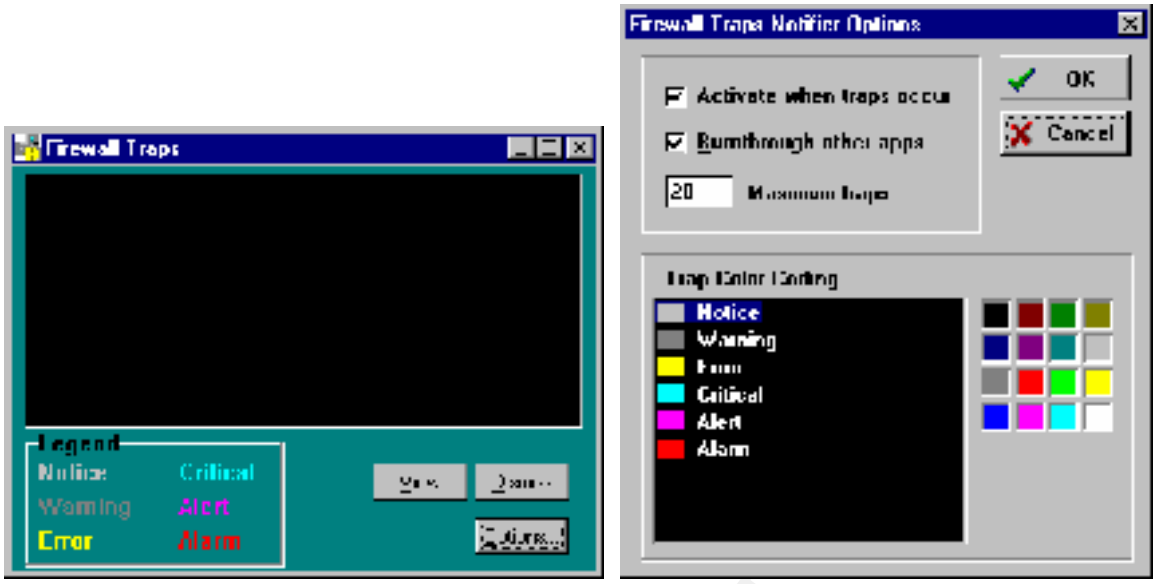


Diagram 21
Online alert notification settings.

Step 23 – Logs

Result:

1. Log activity is occurring, diagram 22 contains a sample screen-shot of log statistics. The IM Firewall also allows for logging certain traffic at a higher level. This is configured through the "Action" option as the services are enabled in the Master Security Plan. The option to "Allow" traffic associated with a certain service will log that traffic at a normal level. The option to "Log+Allow" logs the traffic at a higher level. The option to "Log+Disallow" disallows traffic and logs it at a higher level. See diagrams 23 through 25 below. These options can also be viewed on the "Master Security Plan" in Appendix 2, note blue highlights.
2. The logs are being retained for an appropriate length of time (one year). Backups are retained even longer.

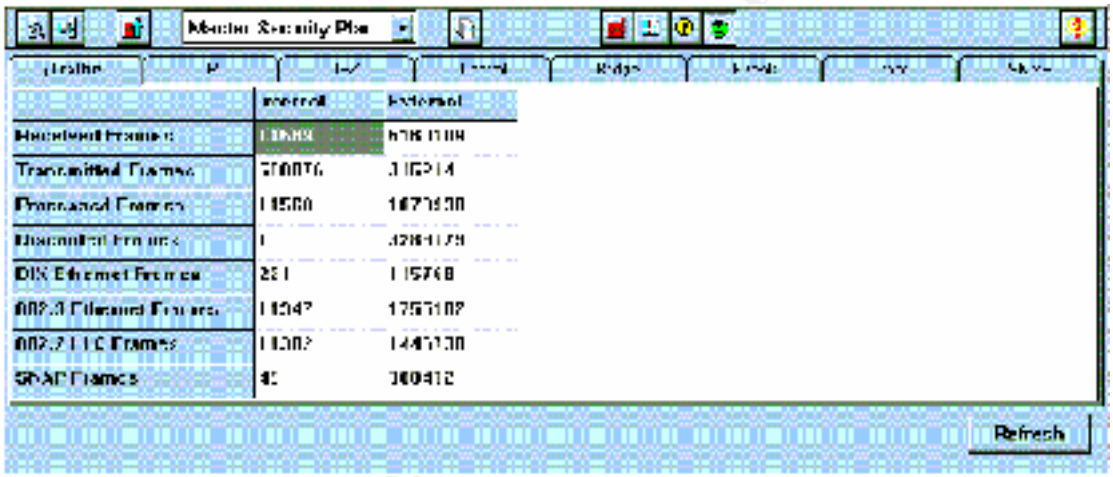


Diagram 22
Log statistics.
Command View Firewall Administrator's Guide, p. 185.

Diagram 23
Allow service, log at the normal level.

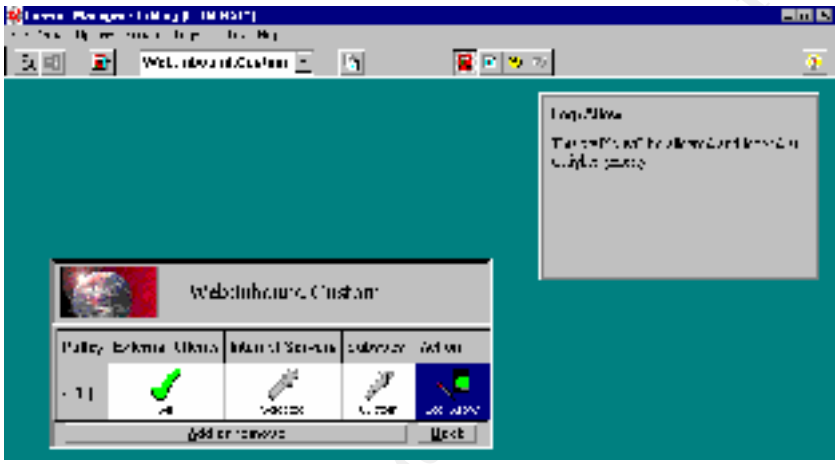


Diagram 24
Allow service, log at a higher level.

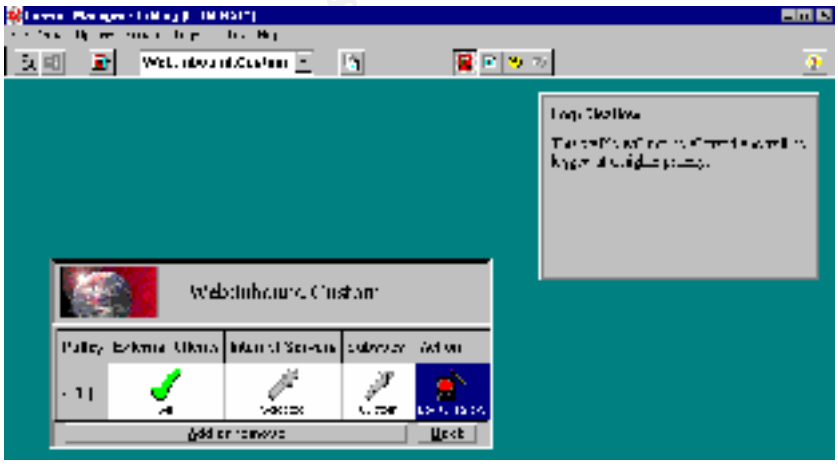


Diagram 25
Disallow service, log at a higher level.

Step 24 – Proactive Monitoring

Result:

1. The company's firewall administrators and network engineers have the appropriate background and training to adequately support the firewall. The administrators and engineers subscribe to periodicals, subscribe to list-servers, and attend group meetings (e.g. local chapter meetings of the Information System Security Association) to remain current in technologies and threats to technologies.

Step 25 – Obstructive Software

Result:

1. An inventory programs was taken from the firewall server, ELRONNT. It is located in Appendix 3.
2. Several programs, highlighted in yellow, do not appear to be needed. While some sources have recommended the removal of browsers, only Microsoft knows for certain whether Internet Explorer can be successfully un-installed ;-).

The applications highlighted in Appendix 3 (and possibly others) are not required and could be removed.

Step 26 – VPN

Result:

1. The company does not have a VPN implemented on this connection. However, through some research it was determined how this implementation would look. The VPN and IKE services are enabled and displayed in diagram 26. The encryption protocol used is 3DES, see diagram 27. The authentication protocol used is MD5, see diagram 28.
2. The Outbound E-mail service is being encrypted utilizing the above protocols, diagram 29.
3. Appropriate management procedures exist for the VPN.

Diagram 26
Virtual Private Network service enabled.

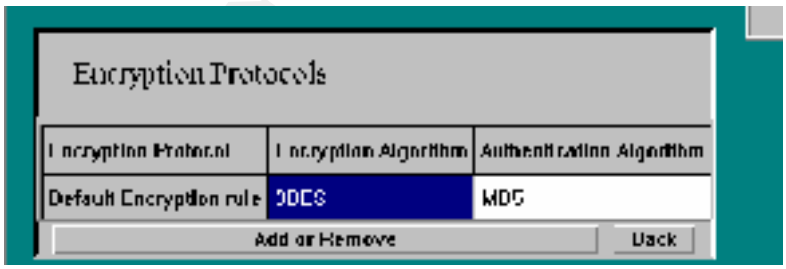


Diagram 27
Encryption protocol, 3DES.

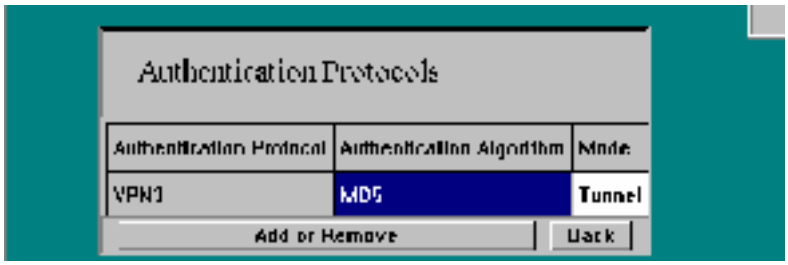


Diagram 28
Authentication protocol, MD5

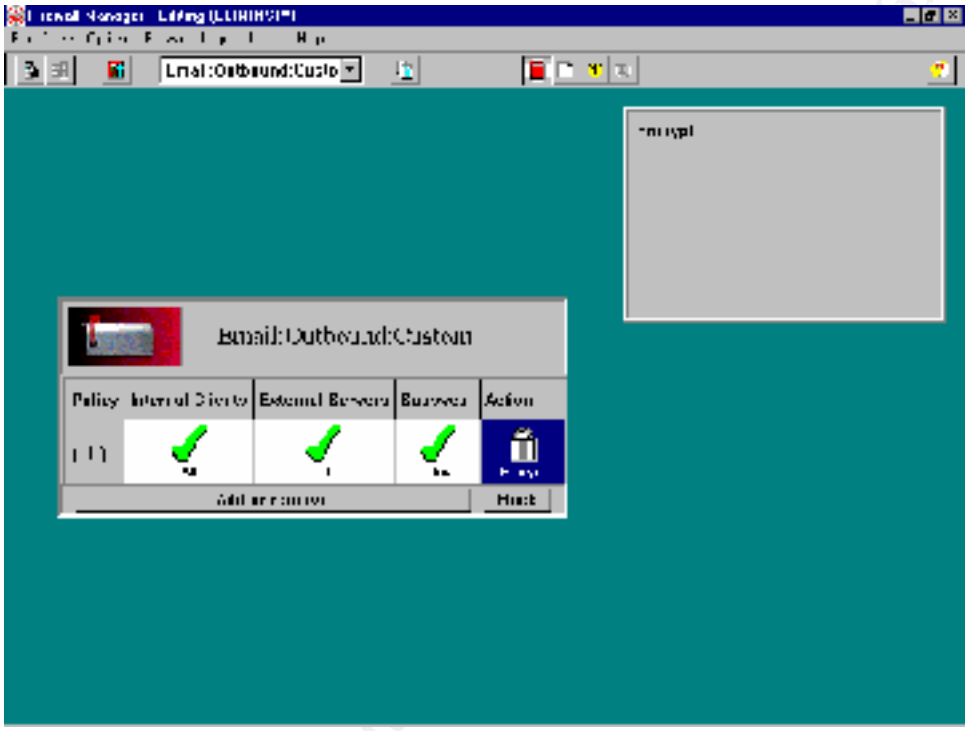


Diagram 29
VPN applied to Outbound Email service.

Summary

Step	Name	Compliant	Recommendation(s)*
1	Internet Policy	Yes	none
2	Firewall Documentation	Yes	none
3	Management Procedures	Yes	none
4	Emergency Procedures	Yes	none
5	ISP Availability	Yes	none
6	Process Documentation	Yes	none
7	Segregation of Duties	Yes	none
8	Updates and Fixes	Yes	none
9	Approvals	Yes	none
10	Test Plans	Yes	none
11	Computer Room Access	Yes	none
12	Guest Access	Yes	none
13	Monitoring	Yes	none
14	User Accounts in IM	Yes	none
15	IM Workstations	No	Enable workstation time-out on IM terminal, implement policy for Administrators to log-off IM terminal when done, enable auditing on IM Firewall libraries.
16	Access to Files in Windows NT	Yes	none
17	Remote Access	Yes	none
18	Critical Files and Directories	Yes	none
19	Recovery Tests	No	Ensure that compatible network cards are used for on-site backup hardware, develop an

			alternate "plan" to be implemented in the event that this connection must used for user access to the Internet.
20	Services	No	Review implemented services and remove all that do not have a legitimate business requirement.
21	Patches	Yes	none
22	Alerts	Yes	none
23	Logs	Yes	none
24	Proactive Monitoring	Yes	none
25	Obstructive Software	No	Remove all software from the firewall machine that is not absolutely necessary.
26	VPN	Yes	none

* These recommendations are meant to immediately address the identified weaknesses. Recommendations to address the root causes of the exceptions are described in the audit report.

System Ability to be Secured

The Elron IM Firewall measures up well against the audit checklist and business requirements in this environment. The firewall appears to have good features and does have the ability to be secured. The firewall interface is logical and provides ease of maintenance. According to the information gathered in the review, the firewall was relatively easy to install and configure. It is also easy to configure test "plans" (configuration settings) without having to alter the production configuration. Much of the system's security relies on the configuration and security of the host Windows NT operating system.

The IM Firewall does have to reside on a Windows NT machine. As a result, the firewall is highly dependent on the hardening of the operating system to ensure secure operation. The vulnerabilities found during this evaluation include:

- No individual accounts exist in the IM Firewall and access can be gained if the firewall password is known, in addition, firewall "plans" (configuration settings) can be altered offline without knowing the firewall password;
- Hardware compatibility must be carefully confirmed since only a few network interface cards are approved to be compatible with the software;
- In the current implementation, excessive Internet services are enabled and may pose unnecessary security risks; and
- In the current implementation, other programs reside on the Windows NT machine that are not required for the proper operation of the firewall.

The recommendations made for the immediate mitigation of these risks include:

- Physically securing the NT machine as much as possible, this includes implementing policies for the administrators to log-out of the machine when not in use as well as implementing and automatic time-out and enabling auditing to detect if any firewall files get altered without proper approval;
- The current implementation of hardware backup equipment contains incompatible network interface cards which must be replaced with compatible cards, also policies should be in place to ensure that compatibility issues are fully addressed in future acquisitions;
- All Internet services that are not support by a valid business need, must be disabled; and
- An inventory of current applications residing on the NT machine must be examined and any non-essential software must be removed.

The estimated costs associated with these recommendations are relatively low. Implementing physical security procedures and auditing controls and review should require less than two man-days. New network interface cards are required; the cards should not be more than $50.00 each. Investigating non-essential Internet services should not require more than two or three-man days. Eliminating unnecessary software on the NT machine should only require one to two man-days.

The control objectives for the review have been achieved. While not every conceivable control objective may have been included, the review has covered the most basic and important ones.

System Ability to be Audited

The audit process used to evaluate the IM Firewall was reasonably successful and sufficient to assess the overall security. Several audit checklists, the system's documentation, and widely available evaluation tools were included to help ensure that as many areas as possible were covered. As stated in the initial scope definition, the controls evaluated were restricted to cover only core aspects directly associated with the Elron software itself. During the performance of this review, it did not appear that there were many areas that could not be validated, with the exception of the company's claim that (the Elron IM Firewall is) "the highest rated security solution in value and performance for your growing network" (http://www.elronsoftware.com/productfamily/firewall.shtml). There was also a problem in verifying exactly what can be logged and what events can be configured to trigger an alert. The vendor's documentation did not list what specific activity and events are recorded.

Many subjective steps have to be evaluated on a case-by-case basis. It is not possible to state in an audit program specifically what features or aspects have to be present in an environment to achieve compliance. A company's industry, for example, can have a tremendous impact on the level of controls required. Luckily, many of the guides (see references) used to evaluate this firewall system provide some examples of what constitutes compliance.

A more complete reviewed can be achieved by widening the initial scope to also cover Windows NT controls. Other considerations include reviewing the parameters of the routers that interface with the firewall. There are many resources readily available that can assist in reviewing these components. It could be helpful to contact the vendor and determine if documentation exists that describes the logging and event capabilities of the software. If the IT environment containing the Elron Firewall has been reviewed previously, many of the steps (especially the subjective steps) could be removed if they have been evaluated in other reviews. This would allow a deeper concentration of effort of the software itself. It is assumed that more reviews performed on the Elron IM Firewall will result in additional control checks and specific software issues.

Assignment 4 – Independent Audit Report

Executive Summary

This review evaluated the controls surrounding the Elron Internet Manager (IM) Firewall currently installed to provide access to and protect the online Commercial Customer Information System (CCIS). CCIS provides commercial customers with access to policy information and claim status. The IM Firewall's primary function is to manage access by customers to CCIS. The firewall does not regulate access to the Internet by employees except in emergencies. The firewall is managed by network engineers within the Communications and Networking Division of the Information Technology Department.

Overall, the objectives of the review were achieved. While further testing of the firewall was planned using automated tools, this step was deferred due to the fact that some of the tools can have unexpected results. This objective was compensated with information that the Elron firewall has been recently certified by a reputable source (The International Computer Security Association). The current policies and procedures established to manage the firewall are functioning properly with only a small number of exceptions. Specifically, weaknesses were found in the physical access controls of the firewall, compatible backup hardware for the firewall, unneeded Internet services running on the firewall, and unneeded software installed on the firewall. These issues are explained in greater detail in the Audit Issues section of the report.

Audit Issues

Finding 1: IM Workstation Physical Controls

Description: During the review, physical access controls were reviewed and testing was performed to determine what could be done to the firewall once physical access was gained. It was determined that, with physical access to an unattended workstation, full control could be obtained to the current production firewall if the proper password was provided. More likely, however, it was discovered that firewall "plans" (configuration files for backup and testing) could be accessed without a password. Changes could be made to the firewall plans by anyone with access to the computer room. Once made, the changes would take effect if the plan were "applied" (i.e. configuration file was loaded) to the production firewall. See step 15.

Background/risk: Changes could be made to the firewall by anyone with access to the computer room if the workstation is left unattended. This even includes guests if not properly supervised. Unauthorized changes to the firewall can result in the firewall not functioning properly. Primarily, the firewall could be configured to bypass security controls necessary to protect the internal network from hostile Internet connections. This, in turn, could lead to a compromise of the internal network as well as unauthorized disclosure of customer information. If not addressed, it is probable that an unauthorized modification (either intentional or unintentional) will eventually occur.

Recommendation(s): Even though the computer room provides a good level of protection, managers need to be made aware that not all personnel allowed in the computer room have a need to access all systems in the computer room. Managers should be informed that they are ultimately responsible for both the physical and logical security of the systems under their control. It should be stressed that all feasible protective measures should be taken. This could include workstation locks, procedures informing network engineers to always log-off workstations when maintenance is not being performed and procedures and controls to audit configuration files for unauthorized changes. Most importantly, managers should perform a risk assessment when any new system is implemented and examine/evaluate physical controls. This could help prevent future occurrences of this nature.

Costs: Costs of the recommendation can be measured in human resources. A project to increase management awareness could be performed within one man-week. Procedures to require that the risk analysis include an evaluation of the physical security controls could require up to another man-week. Continuing performance of the risk analysis (physical controls) could add anywhere from two man-days to one man-week per new system. These costs should have no impact on system performance and could prevent a very costly incident involving the compromise of internal systems and disclosure of customer information.

Compensating Controls: A compensating control applicable to the risks of physical access to the firewall workstation is the fact that the workstation is protected within the

computer room and that access to the firewall's configuration is only accessible from the one workstation. In addition, any account accessing the plan has to have appropriate access in Windows NT to alter a plan. However, even "Read" access can disclose the confidential configuration of the firewall.

Finding 2: IM Backup Hardware

Description: During the review, disaster recovery precautions for the firewall were examined. It was noted that even though on-site backup hardware exists for the firewall, it has not been properly configured and tested. Personnel attempted to accomplish configuration and testing during the review, however, it was discovered that incompatible network interface cards had been obtained. See step 19.

Additionally, it was noted that while the Internet connection and the firewall are intended to act as a backup to the primary employee Internet connection, no configuration settings (i.e. a "plan" file) exist that would supply the necessary functionality needed by the employee connection.

Background/risk: In the event of firewall equipment failure, the organization may not be able to recover the firewall within a reasonable time. The disruption will result in commercial customers being unable to access the data within the CCIS. A prolonged recovery time could also result in a negative perception of the company or its services. While some computer equipment can last for years, there is still a strong possibility of an unforeseen hardware failure.

In regards to the backup firewall configuration, employees who depend upon the Internet and e-mail to perform their job duties can be hindered or even prevented from completing their work.

Recommendation(s): While plans exist to conduct complete recovery tests off-site, no formal plans are in place to test on-site equipment. An inventory of equipment located within the computer room should be examined. Any equipment designated as "backup", should be periodically tested to ensure that it would function as expected in the event of an emergency. In addition, full testing of hardware should be performed as the last step in the installation process. Appropriate procedures addressing these issues should be documented.

To address the backup plan for the firewall, network engineers should analyze the types of services required by the primary firewall and reproduce those services in a backup plan for the IM firewall. Testing of this backup file should also be conducted.

Costs: Costs to implement the recommended measures primarily consist of human resources. Exact resources depend upon the amount of backup equipment located on-site. Testing and documentation could take one or two man-days per piece of equipment. On-going, periodic tests should require approximately the same amount of time and should occur at least annually. Updating IT procedures should not require more than two man-

days. These costs should be considered a cost of installing of new equipment and will have no impact on system performance. These costs could mitigate the impact a prolonged outage would incur.

The costs of developing a backup plan should not consume more than one man-week. The backup plan could then be implemented in a matter of minutes if needed.

Compensating Controls: A compensating control that exists is the fact that replacement-networking equipment is usually common and readily obtained from local sources. However, the organization must consider exactly how close the nearest equipment source is and what is the availability of the source to provide the equipment (i.e. 24 hours a day).

Finding 3: Excessive Internet Services

Description: During the review, the configuration of the firewall was reviewed to ensure that only approved Internet services are allowed into the internal network or out to Internet sources. The organization's own Internet Security policy was used to verify the appropriateness of the configuration. See step 20. It was noted that several Internet services could be removed due to the fact that there is no current business need for them to be active. This violates the Internet Security policy. The services are; Gopher (an Internet application that hierarchically organizes text files for viewing), POP2 (an older version of Post Office Protocol which manages e-mail retention and retrieval), RealAudio (a streaming audio application that allows audio (music, radio stations, etc.) to be played over the Internet), RealPlayer (very similar to RealAudio except that video can also be played), and RealPlayerG2 (another version of RealPlayer).

Background/risk: Excessive Internet services can unnecessarily consume system resources and degrade the performance of the firewall. More importantly, each service can pose risks to the firewall and the interior network. Some risks can lead to the compromise of the firewall and the interior network or, can result in the unauthorized disclosure of customer information. Chances are good that if a vulnerability is found within these services, it will be exploited on the company's network.

Recommendation(s): The current network engineers are well qualified to manage network firewalls. However, the Elron IM Firewall is relatively new technology to this organization and no formal training on the firewall has been obtained. Preferably both, but at least one of the network engineers should attend a formal training class on configuring and supporting the firewall. Technical training should also be included as part of the implementation of the system. At least one network engineer should obtain continuing technical training on the Elron firewall if and when the system is significantly changed due to version upgrades.

Costs: Costs to implement the recommended measures are (per person) two man-days, a $1295.00 course fee, plus travel and expenses for two days in Burlington, MA.

Compensating Controls: A compensating control could be to contract with an independent outside party to provide periodic audits/security reviews of the firewall. However, this could potentially be more expensive and less timely.

Finding 4: Obstructive Software

Description: During the review, an inventory of applications residing on the firewall computer was conducted. See step 25. It was noted that several application programs were not required for the proper functioning of the firewall and, therefore, could be removed. The inventory includes programs such as Microsoft Word, Microsoft Outlook Express, Microsoft Internet Information Server, etc. The complete inventory is located in Appendix 3. This list was also provided to the network engineers.

Background/risk: Obstructive application software can unnecessarily consume system resources and degrade the performance of the firewall. In some instances it is possible that an application program competing for resources with the firewall can cause the firewall to crash. A firewall crash would prevent commercial customers from accessing policy and claim information. A prolonged disruption could result in a negative perception of the company or its services. There is a moderate risk that a program will be started (intentionally or unintentionally) that will degrade or crash the firewall and/or operating system.

Recommendation(s): The current network engineers are well qualified to manage network firewalls. However, the Elron IM Firewall is relatively new technology to this organization and no formal training on the firewall has been obtained. Preferably both, but at least one of the network engineers should attend a formal training class on configuring and supporting the firewall. Technical training should also be included as part of the implementation of the system.

Costs: Costs to implement the recommended measures are (per person) two man-days, a $1295.00 course fee, plus travel and expenses for two days in Burlington, MA. At least one network engineer should obtain continuing technical training on the Elron firewall if and when the system is significantly changed due to version upgrades. This cost could be divided between the recommendation stated in Finding 3.

Compensating Controls: A compensating control is that the firewall workstation is solely dedicated to the support of the firewall. It is not intended that the firewall perform any other services, therefore, no other programs *should* be running.

Appendices

Appendix 1: Critical Files

DISTRIBUTION
==========

The IM Firewall installs the following files and directories:

C:\Program Files\Elron Software\IM\Firewall Manager

class.txt
Data.TAG
Data1.CAB
fixed.txt
FWUPGTok.exe
gtc.exe
gtcpif.pif
gtctest.exe
inactivex.rcd
indns.rcd
inemail.rcd
inftp.rcd
inimap.rcd
injava.rcd
inldap.rcd
insmtp.rcd
install.txt
intelnet.rcd
inwww.rcd
Lang.DAT
Layout.BIN
ogmdll.dll
ogmgr.exe
OGSENTRY.exe
onguard.apd
Os.DAT
outtelnet.rcd
protocol
README.TXT
service
Setup.ico
Setup.INI
Setup.INS
Setup.LID

template.txt
testpif.pif
Uninst.EXE
inst32i.EX
_setup.DLL
_sys1.CAB
_user1.CAB

C:\Program Files\Elron Software\IM\Firewall Manager\Firewall

CGS.exe
cvfw.dll
default.cfg
default.ogm
elfire.dll
elfire.sys
filesnt.lst
FWMail.exe
onguard.cfg
onguard.ogm
onguard.prm
RebootNT.exe
sshalgs.spd

C:\Program Files\Elron Software\IM\Firewall Manager\ONGuard

ELFWNT.ON
onguard.cfg
ONGUARD.DN1
onguard.err
ONGUARD.OGM
ONGUARD.TBL
onguard.txt

C:\Program Files\Elron Software\IM\CVBin

BGRestart.exe
CardInst.exe
CGS.exe
CGS.LOG
cgslog.bak
elfire.dll
elfire.sys
ETLDLL32.DLL
FWMail.exe

restart.bat

C:\Program Files\Elron Software\IM\Data

C:\Program Files\Elron Software\IM\Firewall

cvfw.dll
CVFWVPN.spd
default.cfg
default.ogm
ELFWNT.ON
event.log
onguard.cfg
onguard.ogm
onguard.prm
onguard.tbl
sshalgs.spd
system.ath

C:\Program Files\Elron Software\IM\uninst

CVUninst.exe
DATA.TAG
data1.cab
lang.dat
layout.bin
os.dat
SETUP.INI
Setup.Ins
setup.lid
INST32I.EX
_SETUP.DLL
_sys1.cab
_user1.cab

C:\WINNT

ogmgr.ini
ogsentry.ini

C:\WINNT\system32\drivers

elfire.sys

Appendix 2: Master Security Plan

System Information

Name: ONGUARD
Version:
IP Address: 192.168.10.11
IP Mask: 255.255.255.0
Default Gateway: 192.168.10.12
NAT IP Address: 192.168.40.11
NAT IP Mask: 255.255.255.0
Event threshold: Notice
Trap threshold: Error

Contact Information

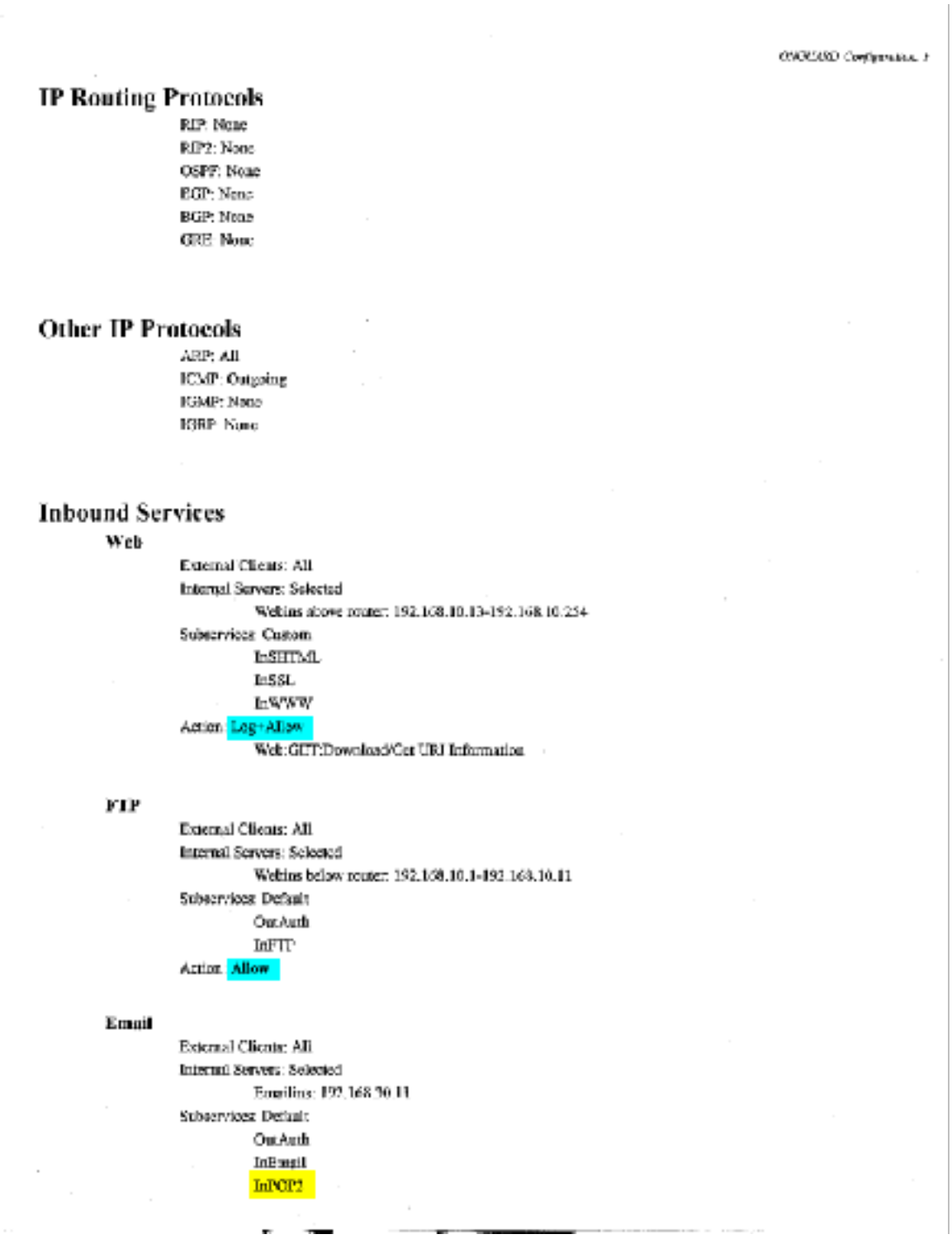
Location:
Name: ONGUARD
Title: Network Engineer
Company: Insurance Company
Address: 1234 Avenue A
City: Dallas
State: TX
Country: US
Postal Code: 77777
Phone: 214-123-4567
Fax: 214-123-8901
Email: John.[redacted]@[redacted].com

Internal IP Addresses and Ranges

Webins below router: 192.168.10.1-192.168.10.11
Webins above router: 192.168.10.13-192.168.10.254
Dnsins: 192.168.20.11
Emailins: 192.168.30.11
InWebins: 192.168.50.11

Advanced IP Options

Multicast: None
Broadcast: None
Record Route: None
Time Stamp: None
Loose Source Routing: None
Strict Source Routing: None



IP Routing Protocols

RIP: None
RIP2: None
OSPF: None
EGP: None
BGP: None
GRE: None

Other IP Protocols

ARP: All
ICMP: Outgoing
IGMP: None
IGRP: None

Inbound Services

Web

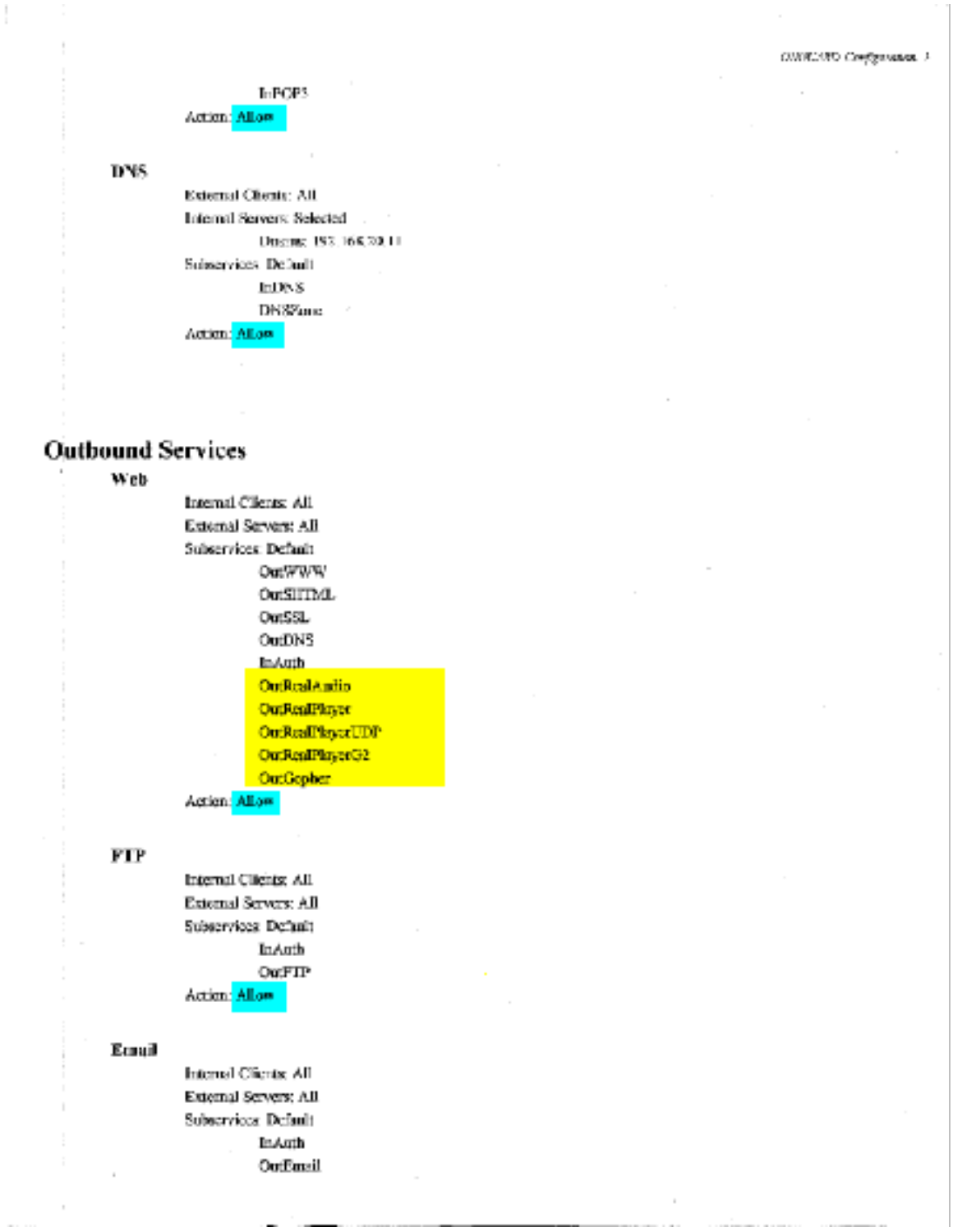
External Clients: All
Internal Servers: Selected
Webins above router: 192.168.10.13-192.168.10.254
Subservices: Custom
InSHTML
InSSL
InWWW
Action: Log+Allow
Web:GET:Download/Get URI Information

FTP

External Clients: All
Internal Servers: Selected
Webins below router: 192.168.10.1-192.168.10.11
Subservices: Default
OutAuth
InFTP
Action: **Allow**

Email

External Clients: All
Internal Servers: Selected
Emailins: 192.168.50.11
Subservices: Default:
OutAuth
InEmail
InNCP2



InPOP3
Action: Allow

DNS

External Clients: All
Internal Servers: Selected
Dnsmg: 193.168.30.11
Subservices: Default
InDNS
DNSZone
Action: Allow

Outbound Services

Web

Internal Clients: All
External Servers: All
Subservices: Default
OutWWW
OutSHTTP/L
OutSSL
OutDNS
InAuth
OutRealAudio
OutRealPlayer
OutRealPlayerUDP
OutRealPlayerG2
OutGopher
Action: Allow

FTP

Internal Clients: All
External Servers: All
Subservices: Default
InAuth
OutFTP
Action: Allow

Email

Internal Clients: All
External Servers: All
Subservices: Default
InAuth
OutEmail

OutDNS
OutPOP2
OutPOP3
Action: Allow

DNS

Internal Clients: All
External Servers: All
Subservices: Default
OutDNS
Action: Allow

Subservices

Name	Source port	Destination port
InSHTML	1024-65535 443-443	443-443 1024-65535
InSSL	443-443 1024-65535	1024-65535 443-443
InWWW	80-80 1024-65535	1024-65535 80-80
OutAuth	113-113 1024-65535	1024-65535 113-113
InFTP	20-20 21-21 1-65535 1-65535	1-65535 1-65535 20-20 21-21
InAuth	113-113 1024-65535	1024-65535 113-113
OutFTP	20-20 21-21 1-65535 1-65535	1-65535 1-65535 20-20 21-21
InEmail	25-25 1024-65535	1024-65535 25-25

InPOP2	109-109 1024-65535	1024-65535 109-109
InPOP3	1024-65535 110-110	110-110 1024-65535
OutEmail	25-25 1024-65535	1024-65535 25-25
OutDNS	53-53 1-65535	1-65535 53-53
OutPOP2	109-109 1024-65535	1024-65535 109-109
OutPOP3	1024-65535 110-110	110-110 1024-65535
InDNS	53-53 1-65535	1-65535 53-53
DNSZone	53-53	53-53
OutWWW	80-80 1024-65535	1024-65535 80-80
OutSHTML	1024-65535 443-443	443-443 1024-65535
OutSSL	443-443 1024-65535	1024-65535 443-443
OutRealAudio	1024-65535 6770-7170	6770-7170 1024-65535
OutRealPlayer	1024-65535 7070-7071	7070-7071 1024-65535
OutRealPlayerUDP	6970-7170	6970-7170
OutRealPlayerG2	1024-65535 554-554	554-554 1024-65535
OutGopher	70-70	1024-65535

	1024-65535	70-70
InGopher	70-70	1024-65535
	1024-65535	70-70

Appendix 3: ELRONNT Program Inventory

"dir *.exe /s > pgms.txt"

```
 Volume in drive C has no label.
 Volume Serial Number is B890-DB85


 Directory of C:\IMFW

11/24/98  03:10p            60,416 SETUP.EXE
12/17/97  06:30p             8,192 _ISDEL.EXE
           2 File(s)         68,608 bytes

 Directory of C:\IMFW\Doc\Reader

01/06/00  10:36a         5,682,336 ar40eng.exe
           1 File(s)      5,682,336 bytes

 Directory of C:\IMFW\ntfw

11/24/98  03:10p            60,416 SETUP.EXE
12/17/97  06:30p             8,192 _ISDEL.EXE
           2 File(s)         68,608 bytes

 Directory of C:\IMFW\ntmgr

11/24/98  03:10p            60,416 SETUP.EXE
12/17/97  06:30p             8,192 _ISDEL.EXE
           2 File(s)         68,608 bytes

 Directory of C:\IMFW\ua

03/22/01  02:20p           808,990 uaclient.exe
03/22/01  02:20p           815,435 uaserver.exe
           2 File(s)      1,624,425 bytes

 Directory of C:\Program Files\Adobe\Acrobat 4.0\Reader
[Required for IM Help File]

11/03/99  09:38a         2,333,184 AcroRd32.exe
           1 File(s)      2,333,184 bytes

 Directory of C:\Program Files\Elron Software\IM\CVBin
```

```
03/22/01  02:16p            36,864 BGRestart.exe
03/22/01  02:19p           221,184 CardInst.exe
03/22/01  02:16p           163,840 CGS.exe
01/23/01  10:39a            40,960 FWMail.exe
          4 File(s)        462,848 bytes

 Directory of C:\Program Files\Elron Software\IM\Firewall Manager

01/23/01  10:39a           374,784 FWUPGTok.exe
03/22/01  02:16p           147,456 gtc.exe
03/22/01  02:16p            57,344 gtctest.exe
03/22/01  02:19p         2,069,504 ogmgr.exe
03/22/01  02:19p           241,664 OGSENTRY.exe
11/24/98  12:10p            60,416 Uninst.EXE
          6 File(s)      2,951,168 bytes

 Directory of C:\Program Files\Elron Software\IM\Firewall Manager\Firewall

03/22/01  02:16p           163,840 CGS.exe
01/23/01  10:39a            40,960 FWMail.exe
01/23/01  10:39a            19,968 RebootNT.exe
          3 File(s)        224,768 bytes

 Directory of C:\Program Files\Elron Software\IM\uninst

01/13/99  03:38p            61,440 cvuninst.exe
          1 File(s)         61,440 bytes

 Directory of C:\Program Files\Microsoft Office\Office

07/11/97  08:37a             3,072 MSO7FTP.EXE
07/11/97  08:37a             3,072 MSO7FTPA.EXE
07/11/97  08:37a             3,072 MSO7FTPS.EXE
02/09/99  08:14p            41,011 MSOHTMED.EXE
02/17/99  08:05p            65,588 OSA9.EXE
03/18/99  05:38a         8,798,260 WINWORD.EXE
          6 File(s)      8,914,075 bytes

 Directory of C:\Program Files\Microsoft Office\Office\1033

02/01/99  08:18p           122,939 MSOHELP.EXE
          1 File(s)        122,939 bytes

 Directory of C:\Program Files\NetMeetingNT
```

```
05/14/02  02:15p           207,120 cb32.exe
05/14/02  02:15p           243,472 conf.exe
05/14/02  02:15p           359,696 wb32.exe
           3 File(s)        810,288 bytes

 Directory of C:\Program Files\Outlook Express

05/14/02  02:15p            42,528 msimn.exe
05/14/02  02:15p            65,344 oemig50.exe
05/14/02  02:15p            74,560 setup50.exe
05/14/02  02:15p            21,168 wab.exe
05/14/02  02:15p            35,168 wabmig.exe
           5 File(s)        238,768 bytes

 Directory of C:\Program Files\Plus!\Microsoft Internet

03/18/99  12:00a            78,272 IEXPLORE.EXE
           1 File(s)         78,272 bytes

 Directory of C:\Program Files\Plus!\Microsoft Internet\Connection Wizard

05/14/02  02:14p           182,032 icwconn1.exe
05/14/02  02:14p            60,176 icwconn2.exe
05/14/02  02:14p            14,608 icwrmind.exe
05/14/02  02:14p            59,152 icwtutor.exe
05/14/02  02:14p            11,024 inetwiz.exe
05/14/02  02:14p             6,416 isignup.exe
           6 File(s)        333,408 bytes

 Directory of C:\Program Files\Plus!\Microsoft Internet\Setup

03/18/99  12:00a             8,304 IEBATCH.EXE
03/18/99  12:00a           353,280 SETUP.EXE
           2 File(s)        361,584 bytes

 Directory of C:\Program Files\Web Publish

09/11/98  04:16a            12,768 WPWIZ.EXE
           1 File(s)         12,768 bytes

 Directory of C:\Program Files\Windows Media Player

05/14/02  02:16p            67,584 logagent.exe
05/14/02  02:16p             4,880 mplayer2.exe
           2 File(s)         72,464 bytes
```

```
 Directory of C:\Program Files\Windows NT

10/13/96  08:38p              42,256 dialer.exe
04/30/97  11:00p              10,000 HYPERTRM.EXE
           2 File(s)         52,256 bytes

 Directory of C:\Program Files\Windows NT\Accessories

10/13/96  08:38p             204,560 wordpad.exe
           1 File(s)        204,560 bytes

 Directory of C:\Program Files\Windows NT\Accessories\ImageVue

10/13/96  08:38p             427,792 wangimg.exe
           1 File(s)        427,792 bytes

 Directory of C:\Program Files\Windows NT\Windows Messaging

10/13/96  08:38p              25,360 mlset32.exe
           1 File(s)         25,360 bytes

 Directory of C:\WINNT

04/30/97  11:00p             234,256 EXPLORER.EXE
03/18/99  12:00a             103,424 EXTRAC32.EXE
05/14/02  02:12p             100,864 extract.exe
05/14/02  02:14p              26,896 hh.exe
05/14/02  02:12p              17,655 iextract.exe
10/29/98  03:45p             306,688 IsUninst.exe
10/13/96  08:38p              45,328 NOTEPAD.EXE
10/13/96  08:38p              71,952 REGEDIT.EXE
10/13/96  08:38p              32,016 TASKMAN.EXE
10/13/96  08:38p              22,288 welcome.exe
10/13/96  08:38p             256,192 WINHELP.EXE
04/30/97  11:00p             311,056 WINHLP32.EXE
          12 File(s)      1,528,615 bytes

 Directory of C:\WINNT\$NtServicePackUninstall$

10/13/96  08:38p             381,200 autochk.exe
10/13/96  08:38p             402,704 autoconv.exe
10/13/96  08:38p              28,432 bootok.exe
10/13/96  08:38p              20,752 bootvrfy.exe
10/13/96  08:38p              65,808 cacls.exe
```

```
10/13/96  08:38p            79,632 calc.exe
10/13/96  08:38p            42,256 clock.exe
10/13/96  08:38p           208,144 cmd.exe
10/13/96  08:38p            53,008 compact.exe
10/13/96  08:38p            89,360 dcomcnfg.exe
10/13/96  08:38p            33,040 ddeshare.exe
10/13/96  08:38p            27,408 ddhelp.exe
10/13/96  08:38p            36,152 dosx.exe
10/13/96  08:38p            65,808 drwtsn32.exe
10/13/96  08:38p           234,256 explorer.exe
10/13/96  08:38p            31,504 fontview.exe
10/13/96  08:38p            41,232 ftp.exe
10/13/96  08:38p            46,864 grpconv.exe
10/13/96  08:38p            10,000 hypertrm.exe
10/13/96  08:38p           742,160 iexplore.exe
10/13/96  08:38p            85,632 krnl386.exe
10/13/96  08:38p            32,016 label.exe
10/13/96  08:38p            19,728 lodctr.exe
10/13/96  08:38p             9,488 lsass.exe
10/13/96  08:38p           339,728 mspaint.exe
10/13/96  08:38p            14,096 nddeagnt.exe
10/13/96  08:38p             8,464 nddeapir.exe
10/13/96  08:38p            55,056 net.exe
10/13/96  08:38p           142,608 net1.exe
10/13/96  08:38p           117,008 netdde.exe
10/13/96  08:38p            26,896 netstat.exe
10/13/96  08:38p            62,736 nslookup.exe
10/13/96  08:38p           709,904 ntbackup.exe
10/13/96  08:38p           868,288 ntoskrnl.exe
10/13/96  08:38p           407,312 ntvdm.exe
10/13/96  08:38p           443,664 os2.exe
10/13/96  08:38p           130,832 os2srv.exe
10/13/96  08:38p            49,424 pentnt.exe
10/13/96  08:38p           185,616 perfmon.exe
10/13/96  08:38p            15,120 ping.exe
10/13/96  08:38p           117,520 rasmon.exe
10/13/96  08:38p            52,496 rasphone.exe
10/13/96  08:38p            63,760 rdisk.exe
10/13/96  08:38p            23,824 recover.exe
10/13/96  08:38p            28,944 replace.exe
10/13/96  08:38p            93,968 rpcss.exe
10/13/96  08:38p           131,344 services.exe
10/13/96  08:38p            34,576 spoolss.exe
10/13/96  08:38p           120,592 tapisrv.exe
10/13/96  08:38p            84,240 taskmgr.exe
```

```
10/13/96  08:38p            19,728 unlodctr.exe
10/13/96  08:38p            47,360 user.exe
10/13/96  08:38p            27,408 userinit.exe
10/13/96  08:38p           175,888 windisk.exe
10/13/96  08:38p           250,640 winfile.exe
10/13/96  08:38p           310,032 winhlp32.exe
10/13/96  08:38p            47,376 xcopy.exe
          57 File(s)      7,993,032 bytes

 Directory of C:\WINNT\INF

05/14/02  02:16p            88,848 unregmp2.exe
           1 File(s)         88,848 bytes

 Directory of C:\WINNT\Installer\{00010409-78E1-11D2-B60F-006097C998E7}

05/14/02  02:17p           155,136 accicons.exe
05/14/02  02:17p            22,528 bindico.exe
05/14/02  02:17p            73,216 fpicon.exe
05/14/02  02:17p            28,160 misc.exe
05/14/02  02:17p           104,960 outicon.exe
05/14/02  02:17p            11,264 PEicons.exe
05/14/02  02:17p            30,208 pptico.exe
05/14/02  02:17p            35,328 wordicon.exe
05/14/02  02:17p            69,120 xlicons.exe
           9 File(s)        529,920 bytes

 Directory of C:\WINNT\system32

05/03/02  10:41a            26,384 actmovie.exe
10/13/96  08:38p            10,774 append.exe
10/14/96  01:38a            22,800 ARP.EXE
10/13/96  08:38p            27,920 at.exe
10/13/96  08:38p            22,800 atsvc.exe
10/13/96  08:38p            27,920 attrib.exe
04/30/97  11:00p           419,600 AUTOCHK.EXE
04/30/97  11:00p           439,568 AUTOCONV.EXE
10/13/96  08:38p            11,536 autolfn.exe
10/13/96  08:38p            36,092 backup.exe
04/30/97  11:00p            28,432 BOOTOK.EXE
04/30/97  11:00p            20,752 BOOTVRFY.EXE
04/30/97  11:00p            65,808 CACLS.EXE
04/30/97  11:00p            79,632 CALC.EXE
10/13/96  08:38p            86,288 cdplayer.exe
10/13/96  08:38p            63,248 charmap.exe
```

```
10/13/96  08:38p            33,552 chkdsk.exe
04/30/97  11:00p            25,872 CHKNTFS.EXE
03/18/99  12:00a             9,648 CKCNV.EXE
11/13/98  12:23p            37,136 CLICONFG.EXE
10/13/96  08:38p           133,392 clipbrd.exe
10/13/96  08:38p            59,152 clipsrv.exe
04/30/97  11:00p            42,256 CLOCK.EXE
04/30/97  11:00p           208,144 CMD.EXE
10/13/96  08:38p            36,624 comp.exe
04/30/97  11:00p            53,008 COMPACT.EXE
10/13/96  08:38p             8,976 control.exe
10/13/96  08:38p            32,528 convert.exe
05/14/02  02:17p           122,128 cscript.exe
10/13/96  08:38p             7,440 csrss.exe
04/30/97  11:00p            89,872 DCOMCNFG.EXE
04/30/97  11:00p            33,040 DDESHARE.EXE
01/11/99  08:50a            47,616 ddexinst.exe
04/30/97  11:00p            28,432 DDHELP.EXE
10/13/96  08:38p            20,634 debug.exe
10/13/96  08:38p            35,600 diskperf.exe
04/30/97  11:00p            11,536 DLLHOST.EXE
10/13/96  08:38p            35,088 doskey.exe
04/30/97  11:00p            36,344 DOSX.EXE
10/13/96  08:38p            28,368 drwatson.exe
04/30/97  11:00p            65,808 DRWTSN32.EXE
03/18/99  12:00a            24,336 DSSSIG.EXE
10/13/96  08:38p            12,642 edlin.exe
05/14/02  02:14p            12,768 esserver.exe
10/13/96  08:38p           111,888 eventvwr.exe
10/13/96  08:38p             8,424 exe2bin.exe
10/13/96  08:38p            58,640 expand.exe
10/13/96  08:38p               882 fastopen.exe
10/13/96  08:38p            40,208 fc.exe
10/13/96  08:38p            30,480 find.exe
10/13/96  08:38p            25,360 findstr.exe
10/14/96  01:38a            11,536 FINGER.EXE
05/14/02  02:15p             7,440 fixmapi.exe
04/30/97  11:00p            32,016 FONTVIEW.EXE
10/13/96  08:38p            22,800 forcedos.exe
10/14/96  01:38a            41,232 FTP.EXE
10/13/96  08:38p            21,504 gdi.exe
10/14/96  01:38a            13,584 gdsset.exe
03/18/99  12:00a            59,584 GRPCONV.EXE
10/13/96  08:38p            31,504 help.exe
10/14/96  01:38a            11,024 HOSTNAME.EXE
```

```
03/18/99  12:00a          28,112 IE4UINIT.EXE
10/13/96  08:38p          13,584 inetins.exe
10/13/96  08:38p          17,168 internat.exe
10/14/96  01:38a          21,776 IPCONFIG.EXE
04/30/97  11:00p          89,360 IPROP.EXE
10/14/96  01:38a          20,752 IPXROUTE.EXE
04/30/97  11:00p          85,664 KRNL386.EXE
04/30/97  11:00p          32,016 LABEL.EXE
10/13/96  08:38p          35,600 lights.exe
10/14/96  01:38a          86,800 LMREPL.EXE
03/18/99  12:00a          29,472 LOADWC.EXE
10/14/96  01:38a         118,032 LOCATOR.EXE
04/30/97  11:00p          19,728 LODCTR.EXE
04/30/97  11:00p          10,000 LSASS.EXE
10/13/96  08:38p          39,386 mem.exe
05/14/02  02:14p         117,792 mobsync.exe
10/13/96  08:38p         138,000 mplay32.exe
10/13/96  08:38p          23,312 mpnotify.exe
10/13/96  08:38p             917 mscdexnt.exe
03/18/99  12:00a          42,400 MSHTA.EXE
03/09/99  02:22p          38,672 msiexec.exe
04/30/97  11:00p         339,728 MSPAINT.EXE
05/14/02  02:13p         116,496 mstask.exe
05/14/02  02:13p          10,000 mstinit.exe
10/13/96  08:38p         251,152 musrmgr.exe
10/14/96  01:38a          18,704 NBTSTAT.EXE
04/30/97  11:00p          14,096 NDDEAGNT.EXE
04/30/97  11:00p           8,464 NDDEAPIR.EXE
04/30/97  11:00p          55,056 NET.EXE
04/30/97  11:00p         142,608 NET1.EXE
04/30/97  11:00p         118,032 NETDDE.EXE
10/14/96  01:38a          26,896 NETSTAT.EXE
10/13/96  08:38p           7,052 nlsfunc.exe
05/14/02  02:15p          10,000 nmpgmgrp.exe
10/13/96  08:38p          45,328 notepad.exe
10/14/96  01:38a          62,736 NSLOOKUP.EXE
04/30/97  11:00p         711,440 NTBACKUP.EXE
04/30/97  11:00p         914,688 NTOSKRNL.EXE
04/30/97  11:00p         408,336 NTVDM.EXE
10/14/96  01:38a           3,252 NW16.EXE
10/14/96  01:38a         147,728 NWSCRIPT.EXE
01/22/99  02:04p           9,216 ODBCAD32.EXE
04/30/97  11:00p         443,664 OS2.EXE
04/30/97  11:00p         130,832 OS2SRV.EXE
10/13/96  08:38p           8,976 os2ss.exe
```

```
10/13/96  08:38p            74,512 packager.exe
10/13/96  08:38p            54,032 pax.exe
10/13/96  08:38p             7,952 pbrush.exe
04/30/97  11:00p            67,856 PENTNT.EXE
04/30/97  11:00p           186,128 PERFMON.EXE
10/14/96  01:38a            15,120 PING.EXE
10/13/96  08:38p            34,576 portuas.exe
10/13/96  08:38p            68,368 posix.exe
10/13/96  08:38p            26,384 print.exe
10/13/96  08:38p           192,272 progman.exe
03/18/99  12:00a            81,680 PSTORES.EXE
10/13/96  08:38p            93,968 psxss.exe
10/13/96  08:38p           254,799 qbasic.exe
10/13/96  08:38p           126,224 rasadmin.exe
04/30/97  11:00p           118,544 RASMON.EXE
04/30/97  11:00p            52,496 RASPHONE.EXE
10/14/96  01:38a            20,752 RCP.EXE
04/30/97  11:00p            68,368 RDISK.EXE
04/30/97  11:00p            23,824 RECOVER.EXE
10/13/96  08:38p             3,338 redir.exe
10/13/96  08:38p           197,904 regedt32.exe
05/14/02  02:12p            37,136 regsvr32.exe
04/30/97  11:00p            28,944 REPLACE.EXE
10/13/96  08:38p            64,272 restore.exe
10/14/96  01:38a            14,608 REXEC.EXE
10/14/96  01:38a            26,896 ROUTE.EXE
04/30/97  11:00p           103,184 RPCSS.EXE
10/14/96  01:38a            14,608 RSH.EXE
10/13/96  08:38p            12,048 rundll32.exe
10/13/96  08:38p            13,584 runonce.exe
10/13/96  08:38p            23,312 savedump.exe
05/14/02  02:14p            33,952 sens.exe
04/30/97  11:00p           131,344 SERVICES.EXE
10/13/96  08:38p            24,848 setup.exe
10/13/96  08:38p            11,717 setver.exe
10/13/96  08:38p               882 share.exe
10/13/96  08:38p            43,792 shmgrate.exe
10/13/96  08:38p            48,400 skeys.exe
10/13/96  08:38p            40,208 smss.exe
10/13/96  08:38p           114,960 sndrec32.exe
10/13/96  08:38p            62,736 sndvol32.exe
10/13/96  08:38p            24,848 sort.exe
10/13/96  08:38p            19,728 spinit.exe
04/30/97  11:00p            35,600 SPOOLSS.EXE
10/13/96  08:38p            10,512 sprestrt.exe
```

```
10/13/96  08:38p            26,896 subst.exe
10/13/96  08:38p            28,432 syncapp.exe
10/13/96  08:38p            18,896 sysedit.exe
04/30/97  11:00p            38,160 SYSKEY.EXE
10/13/96  08:38p            33,040 systray.exe
04/30/97  11:00p           120,592 TAPISRV.EXE
10/13/96  08:38p            32,016 taskman.exe
04/30/97  11:00p            84,752 TASKMGR.EXE
10/14/96  01:38a            21,264 TCPSVCS.EXE
10/14/96  01:38a            79,632 telnet.exe
10/14/96  01:38a            18,192 TFTP.EXE
10/14/96  01:38a            12,048 TRACERT.EXE
05/03/02  10:41a            66,048 unam4ie.exe
05/14/02  02:17p            47,616 unaxa.exe
04/30/97  11:00p            19,728 UNLODCTR.EXE
10/13/96  08:38p            15,632 ups.exe
04/30/97  11:00p            47,392 USER.EXE
04/30/97  11:00p            26,896 USERINIT.EXE
03/18/99  12:00a            21,056 USERSTUB.EXE
10/14/96  01:38a             1,129 VWIPXSPX.EXE
10/13/96  08:38p            65,296 winchat.exe
04/30/97  11:00p           175,888 WINDISK.EXE
04/30/97  11:00p           250,640 WINFILE.EXE
10/13/96  08:38p            23,824 winhlp32.exe
04/30/97  11:00p           183,056 WINLOGON.EXE
10/13/96  08:38p           152,848 winmsd.exe
10/13/96  08:38p             2,112 winspool.exe
10/13/96  08:38p            20,752 winver.exe
10/13/96  08:38p             2,768 wowdeb.exe
10/13/96  08:38p            10,352 wowexec.exe
10/13/96  08:38p            10,000 write.exe
05/14/02  02:17p           130,320 wscript.exe
04/30/97  11:00p            47,376 XCOPY.EXE
         184 File(s)     12,768,488 bytes

 Directory of C:\WINNT\system32\inetsrv

10/14/96  01:38a            62,736 convlog.exe
10/14/96  01:38a            13,584 gdsset.exe
10/14/96  01:38a             7,440 inetinfo.exe
10/14/96  01:38a           100,624 inetmgr.exe
10/14/96  01:38a           129,296 keyring.exe
10/14/96  01:38a           392,976 setup.exe
          6 File(s)        706,656 bytes
```

```
 Directory of C:\WINNT\system32\inetsrv\tools

10/14/96  01:38a              14,096 dsnform.exe
10/14/96  01:38a              13,072 getdrvrs.exe
10/14/96  01:38a              15,120 mkilog.exe
10/14/96  01:38a              13,584 newdsn.exe
               4 File(s)         55,872 bytes

 Directory of C:\WINNT\system32\viewers

10/13/96  08:38p              56,592 quikview.exe
               1 File(s)         56,592 bytes

 Directory of C:\WINNT\system32\ZoneLabs

11/14/01  07:18p              28,624 minilog.exe
11/14/01  07:18p             482,608 vsmon.exe
               2 File(s)        511,232 bytes

     Total Files Listed:
          332 File(s)     49,439,782 bytes
                      1,546,434,048 bytes free
```

References:

[1] Handbook of Information Security Management, Edited by Harold F. Tipton and Micki Krause, CRC Press LLC, 2002, "How to Perform a Security Review of a Checkpoint Firewall" by Ben Rothke.

[2] Technical Incursion Countermeasures, The Firewall Hardening Guide v0.1, http://www.ticm.com/info/insider/members/fwsecfaq/

[3] Control Objectives for Information and Related Technology, Third Edition, COBIT Steering Committee and IT Governance Institute, July 2000.

[4] Command View Firewall Administrator's Guide, version 3, Elron Software Incorporated, Burlington, MA, November 1999.

[5] Internet Manager Firewall version 3.0.5 ReadMe file, March 2001, Elron Software (provided with the installation program).

[6] SANS Institute, Track 7 Training (7.1.99), Firewall Checklist, Krishni Naidu.

[7] Building Internet Firewalls, 2nd Edition, Zwicky, Cooper and Chapman, O'Reilly and Associates Inc., June 2000.

[8] www.securitytracker.com, Vulnerability database.

[9] online.securityfocus.com, Vulnerability database.

[10] www.securiteam.com, Vulnerability database.

Scanning/Vulnerability Assessment Tools

[11] Ceribus -- http://www.cerberus-infosec.co.uk/cis.shtml

[12] Netscan -- http://www.netscantools.com/nstdownload.html

[13] Sam Spade -- http://www.pelttech.com/security/tools.htm

[14] Superscan -- http://www.pelttech.com/security/tools.htm

[15] WINDump - http://windump.polito.it/

[16] Nessus - http://www.nessus.org

[17] Internet Scanner - http://www.iss.net/products_services/