GIAC Systems and Network Auditor (GSNA)
Practical Assignment v2.1
Option1-
Auditing CheckPoint NG Perimeter Firewall: An Auditor’s Perspective.

Kevin C. Liston

February 23, 2004

Abstract

The purpose of this document is to create a process to assess the risks and controls of a CheckPoint Firewall-1 NG firewall application running on a Nokia Security Appliance employed as a perimeter firewall in a large, financial organization. It includes the process behind the creation of assessment criteria, the measurement process to judge the firewall's adherence to these criteria, and an analysis of such an assessment. Tools developed for this process are included in appendices. Also note that all hostnames, IPs, networks, and references to the organization have been obfuscated.

Assignment 1

Forward

The data used in this document come from an actual audit; therefore the results have been obfuscated to protect the confidentiality of the donor. The original audit's scope covered a sampling of the enterprise's perimeter. This document intends to cover the process one would use to audit a large environment, while auditing only a single perimeter element to satisfy the detail requirements of the practical assignment.

Identification of the System

The original scope of the audit was the perimeter of an international financial organization with a net income exceeding $3.5 Billion. The system selected for this practical is a Nokia IP 380 security appliance with IPSO version 3.5.1 FCS 8 running the CheckPoint NG FP3 (hot fix 2.) The primary function of this device is to enforce that only HTTP and HTTPS traffic flows between the Internet and the web-layer and that only supported services (such as DNS, and SMTP) go to the services layer, and that outbound FTP, HTTP, and HTTPS comes from official proxy servers. In a secure configuration, according to policy, all traffic entering or leaving the enterprise must first terminate within the DMZ; this firewall also enforces this policy. Additionally, all traffic must originate from, or be destined to, a device located in the proxy-layer of the DMZ—desktops must not have direct communication to any external perimeter network. Furthermore, this device can only be managed from centralized consoles located in the management network; administrative traffic is not allowed from desktops, except for a collection of systems in a small IP range. Also, it must be fully encrypted and require strong two-factor authentication.

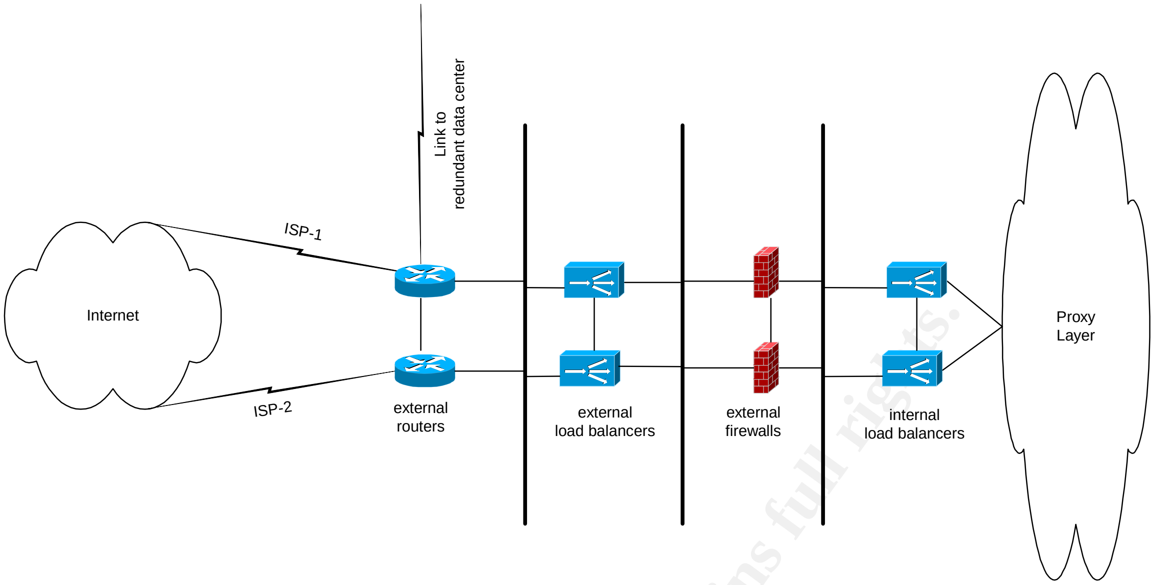


Figure 1: General Network Layout

Figure 1 depicts a logical layout of a subset of one data center. There are redundant border routers, each using different Internet Service Providers. The routers are cross-linked to each other, and one router has a high-speed connection to another geo-diverse data center. These external routers apply ingress and egress filters, and provide a comfortable amount of redundancy. Behind the routers are a pair of load balancing appliances, which are cross-linked to share state. The external firewalls are also linked to share state and provide high availability.

Evaluation of Risk

Threats to availability, integrity and confidentiality, the historic three aspects of computer security[1], need to be considered. In this risk evaluation for the organization we consider the internal servers as the critical asset. In order to protect these assets, there are policy statements, or controls, specifically addressing access to and from the Internet. The firewall is how we satisfy these control requirements. Thus, risks to these assets are mitigated or minimized.

Any impact to this organization is financial impact. A given outcome may manifest itself as direct economic loss, or as damage to company's reputation—which itself leads to indirect economic loss. This tangible assessment of impact helps management understand the importance of risk management, which results in a higher level of internal support for the audit process.

We will implement Carnegie Mellon University's OCTAVE[2] method to prepare Threat Profiles for the organization. When creating these profiles, one defines the organization's critical assets and threats to these assets. Threats are described using these properties: actors that may violate an asset's confidentiality, integrity, and availability and the outcomes of these violations. The basic OCTAVE process considers four major themes of profiles:

1. Human actors using network access.
2. Human actors using physical access.
3. System problems.
4. Other problems, such as natural disasters, infrastructure failures (*e.g.* a water main break, flooding a data center,) and other acts outside the control of the organization.

When the critical asset under evaluation is the organization's files, the threat profiles generated by the OCTAVE process create a list of threats that the overall security plan of the

[1] Schneier.
[2] Alberts and Dorofee.

organization must address. The security policy will include control statements intended to eliminate, or mitigate these identified risks. One of the major themes covered in the Octave process is "Human actors using network access," (see figure 2.) A prudent method of addressing this set of risks is the use of a firewall.

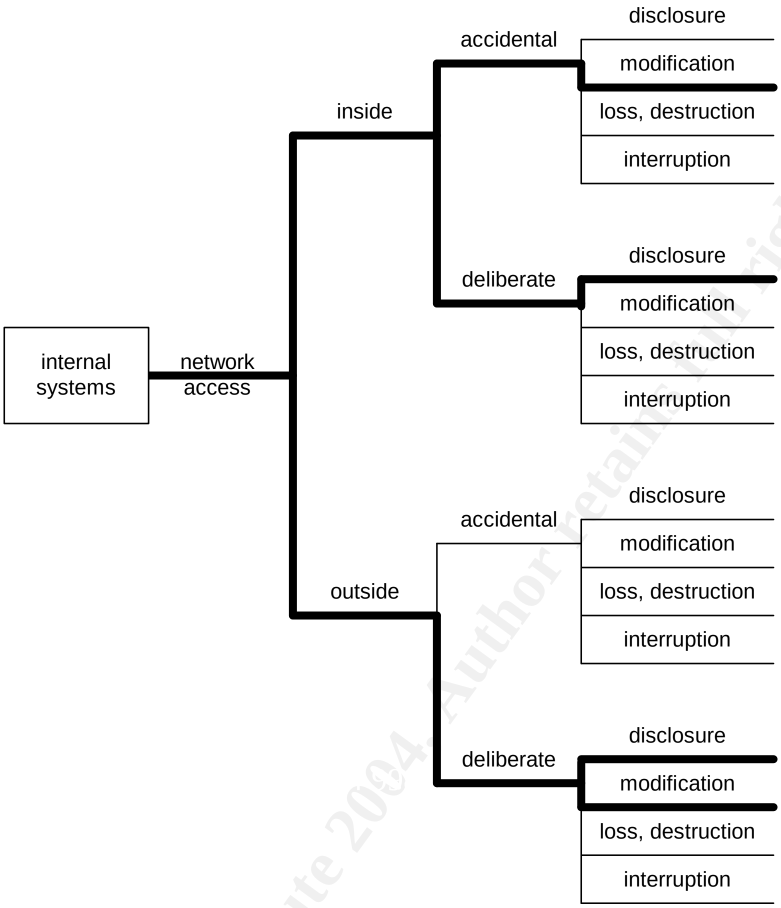


Figure 2: OCTAVE Threat Profile for internal systems, showing areas of concern when mapped to the Human Actors Using Network Access Threat Tree.

How do we know if a firewall sufficiently addresses these areas of concern? We need to examine scenarios where the firewall fails. Let us now use the OCTAVE process recursively to discover these threats, by considering the firewall itself as the critical asset. Figures 3 and 4 illustrate possible results of such a process. Additional threats that must be considered are those that fall within the "system problems," and "other problems" themes. Under "system problems," possible threats are: software defects, malicious code, system crashes, and hardware defects. "Other problems" that may impact the firewall are: power supply issues, telecommunications outages, and natural disasters.

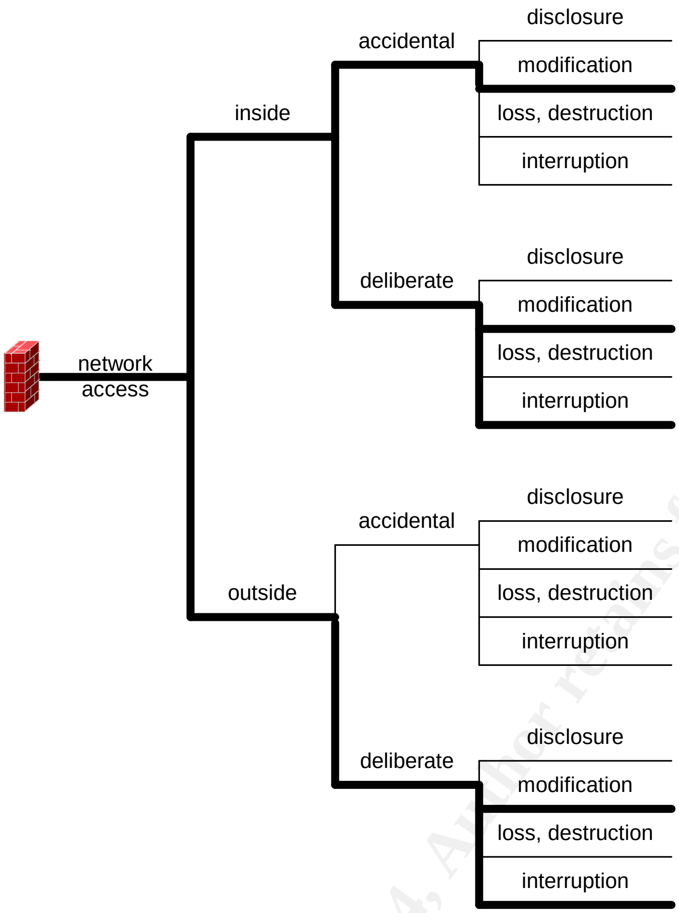


Figure 3: Areas of Concern for the Firewall, mapped to the Human Actor Using Network Access Threat Tree.

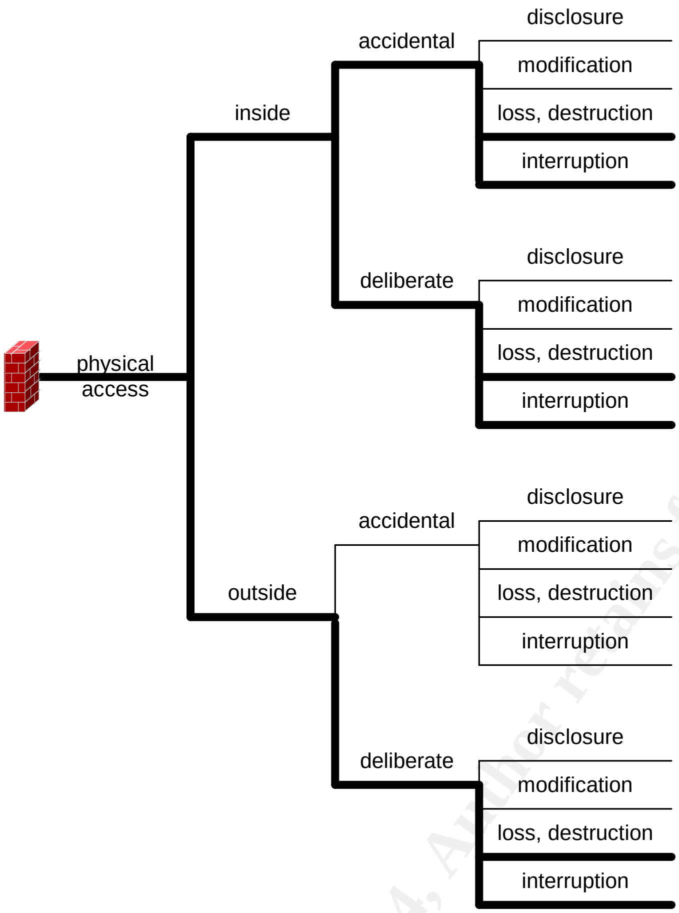


Figure 4: Areas of Concern for the Firewall, mapped to the Human Actor Using Physical Access Threat Tree.

From this discovery process, we generate the following table of threats. We expand upon the list of threats with the likelihood of its attempt, and the scale of the consequences of such an event, which yields a basic risk assessment of the device.

Table 1: Risk Analysis

Concern	Actor/Motive	Likelihood [3]	Consequences
Administrator error exposes internal network	Internal/Accidental Network Access	Medium	Confidentiality impact. A human or procedural error could increase the success probability of a malicious threat. Moderate economic impact, since the likelihood of exploitation of the exposure is reduced.
Administrator error causes outage	Internal/Accidental Network Access	Medium	Availability impact. A human or procedural error could result in a network outage. Loss of Internet for employees. Customers' cannot access corporate services. High economic and reputation impact, directly proportional to length of outage.
Compromised internal employee deliberately loosens or removes rules in the firewall.	Internal/Deliberate Network Access	Low	Confidentiality impact. An agent on the inside could greatly improve the success of an unauthorized access attempt. High economic impact from subsequent thefts or attacks.
Disgruntled employee launches DoS attack against firewall.	Internal/Deliberate Network Access	Low	Availability impact. An internally launched DoS attack would be more effective than an external DoS. Loss of Internet for employees. Customers' cannot access corporate services. High economic and reputation impact, directly proportional to length of outage.
Denial of Service attack launched from the Internet.	External/Malicious Network Access	High	Availability impact. Loss of Internet for employees. Customers' cannot access corporate services. High economic and reputation impact, directly proportional to length of outage.
External breech of an internal server.	External/Malicious Network Access	High	Confidentiality impact. Subsequent attacks leveraging this breech enjoy an increased probability of success. Severe financial impact is possible should

[3] This is the likelihood of the risk factor to occur or be attempted, not necessarily the likelihood of the controls to fail.

			this event occur.
Employee accidentally un-plugs firewall	Internal/Accidental Physical Access	Low	Availability impacted. Loss of Internet for employees. Customers' cannot access corporate services. High economic and reputation impact, directly proportional to length of outage.
Disgruntled employee un-plugs firewall	Internal/Deliberate Physical Access	Low	Availability impacted. Loss of Internet for employees. Customers' cannot access corporate services. High economic and reputation impact, directly proportional to length of outage.
External parties destroy data center	External/Deliberate Physical Access	Low	Availability impacted. Loss of Internet for employees. Customers' cannot access corporate services. High economic and reputation impact, directly proportional to length of outage.
Software failure causes an outage.	Software Defect System Crashes	Low	Availability impacted. Loss of Internet for employees. Customers' cannot access corporate services. High economic and reputation impact, directly proportional to length of outage.
Hardware failure causes an outage.	Hardware Defect System Problems	Low	Availability impacted. Loss of Internet for employees. Customers' cannot access corporate services. High economic and reputation impact, directly proportional to length of outage.
Software vulnerability in firewall application	Software Defect System Problems	Low	Confidentiality impacted. . A software error could create a vulnerability that may increase the success probability of a malicious threat. High economic impact if exploited.
Power grid failure takes out data center	Power Supply Issue Other Problems	Low	Availability impacted. Loss of Internet for employees. Customers' cannot access corporate services. High economic and reputation impact, directly proportional to length of outage.
Hard-line connection failure to ISP	Telecommunications Outages Other Problems	Low	Availability impacted. Loss of Internet for employees. Customers' cannot access corporate services. High economic and reputation

			impact, directly proportional to length of outage.
Tornado strikes data-center	Natural Disasters Other Problems	Low	Availability impacted. Loss of Internet for employees. Customers' cannot access corporate services. High economic and reputation impact, directly proportional to length of outage.

If one orders these risks by the severity of the consequences, we see that confidentiality impacts result in the most severe financial impacts. So logically, the security device should protect against unauthorized access first, and provide robust availability second. Firewalls are ideal tools for limiting access; when configured for fail-over and protected by a robust layer of routers and redundant access circuits, they also provide strong availability protection.

The costs of the control measures to address the risks to availability are sizeable, but when one considers the costs incurred due to an outage, the expenditure makes absolute sense. The costs of hardening the firewall policy to control unauthorized access are minimal compared to the costs of actually installing and maintaining the devices. Therefore, there is no reason not to tighten the rule-set—at least up to the point where it may place accessibility at risk. This conflict between availability versus confidentiality is an old one. It usually arises when a policy is put into place after the network is installed, which is a common situation in large, old networks built for acquisition-motivated companies.

One should not minimize the risks presented by Administrator Error. Lack of peer review, and the dreaded "fat-finger," can reduce an enterprise's symphony of layered defenses to a wide-open door for an attacker, or knock a company off-line for an unreasonable amount of time. The costs of implementing a sound change control process and change management tools can be sizable, and it may introduce dangers to productivity and increase risk to the environment should the process be implemented incorrectly. Also, note that the process of reducing the risk of Administrator Error imposes the largest manpower cost. On the other hand, the risk itself serves as a multiplier of the other risks. *I.e.*, if the occurrence of Administrator Error is high, availability is certain to be affected, and the odds of unauthorized access are likely to rise as well.

The Current State of Practice

Internally, the organization has a well-established audit process. It begins with well-defined security policies developed by the information security department. Engineers take these policies and create standard configurations for platforms (*e.g.* DMZ routers, or business partner firewalls.) The information security department verifies that these standards properly enforce the security policy and sign-off on the document. The auditor's job is to measure the existing implementation against these standards. Security incidents are collected and the outcomes of the lessons-learned stage of incident response are fed into the policy development process. If changes are needed in the policy, they are made, and the standards creation process is repeated.

The audit process begins with a definition of scope, which is created between the CTO and the manager of the audit team. This defines what is to be measured and an initial timeframe is established. The scope is sent to the appropriate managers in an engagement memo so they may allocate appropriate manpower to work with the audit team. Once participants of the audit are identified, a request for information (RFI) is sent to the identified points of contact. Once the documentation is collected, the audit team scores the documents against security policy and the standard configuration.

The current internal standard configuration for a perimeter firewall has over two hundred test points. With over one hundred external firewalls in the environment, the manpower requirements to perform an exhaustive audit far exceed the amount of manpower on the audit team. So, a sampling method is employed to measure the approximate security posture of the environment, and the implementation quality of the staff. The main requirements for an accurate audit in a large environment are a properly defined policy, and an accurate inventory. Without these foundations, any compliance audit will be suspect. Without the policy, you don't know what you're really measuring against, and without an inventory, you don't know if you're truly measuring your perimeter. Determining the perimeter of a large environment is outside the scope of this document. If you do not have accurate network topology documentation and system inventory, I recommend that your effort focus on these two prerequisites first.

I am not using the environment's internal checklist in this document. Instead, I am developing a new one using openly available sources. There are plenty of checklists online outlining basic steps to secure a network or system. Those that I used for this checklist are:

- The Twenty Most Critical Internet Security Vulnerabilities (http://www.sans.org/top20.) This is the list to address at the very minimum. If these issues are addressed, the system will at least satisfy *due care* requirements.
- The Security Consensus Operational Readiness Evaluation Firewall Checklist (http://www.sans.org/score/checklists/FirewallChecklist.pdf.) Which is a much more thorough checklist, and its real appeal is its vendor neutrality.
- The 60 Minute Network Security Guide (First Steps Toward a Secure Network Environment by the NSA's Systems and Network Attack Center (http://www.isaca-utah/org/pdf/sd-7.pdf.) This is also another good list that covers all of the basics.
- Federal Information Systems Controls Audit Manual from the General Accounting Office (http://www.gao.gov/special.pubs/ail2.19.6.pdf) addresses more procedural issues that should be considered in a serious security policy.
- IS Auditing Procedure, Firewalls, Document #6 by Information Systems Audit and Control Association (ISACA) (http://www.isaca.org/Template.cfm?Section=About_Isaca&Template=/ContentManagement/ContentDisplay.cfm&ContentID=7223) is also a good source for higher-level, procedural issues that your policy should address.

In addition to a plethora of online sources, some print sources that should be considered are:

- Inside Network Perimeter Security, by Northcutt, Zeltser, Winters, Frederick and Ritchey, for an in depth look at perimeter design, implementation, and assessment.
- Information Security Management Handbook, 4th Edition, edited by Tipton and Krause for high level looks at security policy and design.
- Hacking Exposed: Network Security Secrets & Solutions, Fourth Edition, by McCLure, Scambray, and Kurtz, which was used to generate some of the live-fire tests used in the checklist.

Other sources that were not directly cited in the checklist, but should be considered are:

- Any CISSP Certification Study guide, for guidance on the audit process and policy considerations, specifically physical security issues.
- Essential Checkpoint FireWall-NG, by Dameon D. Welch-Abernathy (*a.k.a.* "PhoneBoy") not so much for checklist items, but how to implement and test for those items in Check Point and Nokia IPSO.

From these resources, ideas for checklist items were gathered and partitioned into the following topics:

1. **Information Technology Security Architecture**—where configuration of the firewall, and underlying OS are measured against the standard configuration.
2. **Monitoring and Logging**—where issues involving logging, monitoring, and response are considered.
3. **Change Management**—examines the day-to-day management of the firewall as well as its life cycle.
4. **Strategy and Policy**—where business practices are matched against the security policy.

In the enterprise's audit procedure there is a 5th category, Vendor Management, but those issue and concerns are out of scope for this document.

The results from this process were disappointing; this technique did not capture any personal experience. So a new strategy was employed. Instead of gathering sources and building a checklist from that, a checklist was created and the points were mapped back to supporting resources. This allowed little details to sneak into the checklist that might have been overlooked in the process of citation or correlation.

In this new list, a new set of categories were used:

1. **Availability**—inspired by the OCTAVE risk analysis, we must test how the firewall addresses risk to network availability
2. **Vulnerability**—how known vulnerabilities to the firewall are addressed.
3. **Rule Policy**—for checks against the firewall rule policy
4. **Intelligence Denial**—possibly a subset of rule policy, but this category is the checks for measures that would deny an external malicious entity from gathering security intelligence about the network.
5. **Logging**—proper and secure logging is critical for the enterprise's proper management.
6. **Secure Administration**—check for how the firewall device is managed technically.
7. **Change Management**—for management policies.

Assignment 2

Audit Checklist

Checklist sources are as follows:

- (Top20) The Twenty Most Critical Internet Security Vulnerabilities (http://www.sans.org/top20.)
- (SCORE) The Security Consensus Operational Readiness Evaluation Firewall Checklist (http://www.sans.org/score/checklists/FirewallChecklist.pdf.)
- (NSA) The 60 Minute Network Security Guide (First Steps Toward a Secure Network Environment by the NSA's Systems and Network Attack Center (http://www.isaca-utah/org/pdf/sd-7.pdf.)
- (FISCAM) Federal Information Systems Controls Audit Manual from the General Accounting Office (http://www.gao.gov/special.pubs/ail2.19.6.pdf)
- (ISACA) IS Auditing Procedure, Firewalls, Document #6 by Information Systems Audit and Control Association (ISACA) (http://www.isaca.org/Template.cfm?Section=About_Isaca&Template=/ContentManagement/ContentDisplay.cfm&ContentID=7223)
- (ISMH) Information Security Management Handbook, 4th Edition, edited by Tipton and Krause
- (HE) Hacking Exposed: Network Security Secrets & Solutions, Fourth Edition, by McCLure, Scambray, and Kurtz.

Is the firewall in a high-availability configuration? Are the members of the "cluster" synchronized? (SCORE,ISACA.)

Here the objective is to ensure the availability of network resources in the event of a hardware or software failure. If there is only a single firewall per Internet touch-point, a single point of failure could exist in the network placing the availability of resources at risk.

This is a fairly straightforward question. Either the configuration supports high-availability or not. This is verified by inspection of the firewall configuration. Furthermore we ensure that it is working by running **cphaprob state**, or comparing the output of **fw tab –t connections –s** between the members of the cluster.[4]

Scoring is Green if both questions are answered in the affirmative, Yellow if it is configured for HA but not currently synchronized, and Red if there is no HA configuration.

Is there a process to verify they are synchronized?

This is a policy-based follow-up question. It is asked to ensure that availability of the network is protected, and that there are no undetected exposures to this risk. If an ongoing procedure is not in place, firewalls that are not synchronized will result in some outages should a member of the HA cluster fail.

In order to pass, the firewall managers must produce the documented policy, and output of their reports. Ideally there is a monitor in place testing the state of synchronization in the cluster, and alerts when they become synchronized.

Scoring is Green if there is a monitor in the management system for this cluster. Otherwise it is red.

[4] Welch-Abernathy

Does a vulnerability-scan report any vulnerabilities when run from the outside or from the inside? (SCORE)

In order to protect against a malicious outage or compromise, the firewall application and underlying OS should patched against all published vulnerabilities. Otherwise there are known, exploitable weaknesses in the system that an external/malicious entity could use to impact the enterprise's confidentiality or availability.

By using the organization's official vulnerability scanner, scan each interface on the firewall from inside and out.

Scoring is Green if no vulnerabilities are found, Yellow if vulnerabilities are visible from the inside, and Red if vulnerabilities are visible on the outside.

Is there a process to periodically scan the firewall for vulnerabilities? (SCORE)

This is another policy follow-up question. Since vulnerabilities are constantly coming out, relying on quarterly or yearly audits to find vulnerabilities on the firewall is not exercising *due care*. A system may be unnecessarily at risk if there is no periodic vulnerability scanning.

The scanning schedule and past reports are required for passing. Ideally the schedule should be at least weekly, and the process should allow for tactical scans when a recently released vulnerability is being actively exploited in the wild.

Scoring is Green if there is a schedule, and past reports, otherwise it is Red.

Is there a process to resolve vulnerabilities when they are found? (SCORE)

The enterprise must resolve any known vulnerabilities in the system, either through patching or mitigation. This risk of leaving known vulnerabilities in the system unacceptably increases the probability of an attack's success.

A vulnerability resolution process document and a demonstrated history of resolution are required to pass.

Scoring is Green if these requirements are met; otherwise it is Red.

No unnecessary services should be running on the firewall. The following services must not be running on the firewall: FTP, TFTP, telnet, SMTP, POP3, IMAP, rlogin, rsh, HTTP, RPC, DNS, NFS, NIS and any load balancing services. HTTPS is permitted. (Top20, SCORE, ISACA)

The aim is to ensure that only critical services are running on the firewall. Unnecessary services on the firewall increase the number of attack vectors a malicious entity may exploit to compromise or disable the firewall, thus impacting availability or confidentiality of the network.

The only acceptable open ports on a firewall are those required to manage the box, HTTPS, SSH, and the checkpoint management ports. Access control lists or firewall rules should be used to protect these services.

Scanning every firewall interface for open ports, inspecting of the running process table, and examining the inetd configuration file can objectively test for compliance. A network scan should not show any of the forbidden services available. The process table should not show them running, and if inetd is running on the firewall, it should not be configured to start the processes.

Scoring is Green if there are no forbidden services, Red otherwise.

No dynamic routing protocols are to be used by the firewall. (ISACA)

This policy is in place to ensure that data flows through the firewall and not around it. The firewall plays a critical role in controlling availability and confidentiality risks to the network. Exploits involving dynamic routing protocols could remove the firewall from the dataflow, or creatively route traffic past an attacker's machine where interception or malicious modification could occur.

The firewalls process stack should not show a routing daemon running, if so, the routing daemon's configuration should only support static routes.

Scoring is Red if there is a routing daemon running that supports dynamic routing protocols, otherwise Green.

Is there a default-deny cleanup rule that appears at the end of the rule base? Is egress filtering in place? Are spoofed/illegal addresses blocked? (Top20, ISACA, SCORE, ISMH)

Here the aim is to define a perimeter. With egress and ingress filtering, an inside and an outside are defined. A default-deny policy creates a perimeter that passes only what is explicitly permitted. Failure to define a perimeter places network confidentiality at risk.

If we had asked: “does the firewall form an effective perimeter?” it would have been too vague and subjective of a test. These questions, on the other hand, are definitive, testable, and satisfy the definition of a perimeter.

Inspection of the firewall rule policy is required to determine the presence and location of the default-deny cleanup rule. Egress and spoofing rules are tested via the scanning process. Egress and spoofing rules pass if the network scans to not pass through the firewall.

Scoring is Green if all three tests pass, Yellow if one fails, otherwise Red.

Is there a process to periodically test this? (SCORE)

Another follow-up policy question to ensure that the perimeter remains defined. The main risk to not keeping tabs on this is the unintended exposure of the network because of accidental changes.

The administration staff should produce the procedure documentation, the schedule of the tests, and reports of past tests.

Scoring is Green if the documentation is provided; otherwise it is Red.

Is the firewall invisible from the outside? Is there a stealth rule present near the top of the policy? The Check Point management ports: 256, 257, 258, 259, 18210, 18211, 18186, 18190, 18191, and 18192 must not be open to the outside. The firewall must not identify itself as such in banners, MOTD files, hostname, or DNS records. (Top20, HE, ISACA, SCORE)

These steps are taken to deny intelligence to an external/malicious entity. If you allow an attacker to know where the firewall is and what kind it is, this helps focus their strategy, thus increasing the chances of success in their attack.

This is verified by scanning the firewall from the outside, connecting to the firewall from the inside to capture the banner and message-of-the-day. DNS look-ups are also made and inspected for obvious giveaways. The evaluation of the anonymity of hostname and DNS names is somewhat subjective. As a guideline, the following should not be part of these strings: checkpoint, cp, firewall, nor fw.

Scoring would be red if the firewall is pingable or any of the Check Point management ports were open to the outside scan, Yellow if the device is identifiable via banners, message of the day, hostname, or DNS, otherwise Green. One may ask why we inspect the local hostname—each check should be relatively independent and not rely on other items to meet policy. We do not know if encryption is used to manage the server, so the hostname may be in the clear and it should be kept as anonymous as possible.

Does the firewall effectively cloak assets behind it? Block incoming ICMP echo requests, outgoing echo replies, time exceeded, and destination unreachable except for ICMP type 3/code 4. UDP traceroute should not work through the firewall. Scans using a source port of 53/TCP, 53/UDP, 520/UDP, and TCP/20 should fail. Scans using high source ports should also fail. (SCORE, HE, ISACA)

The firewall should only allow connections to explicitly permitted service ports. Packets intended for non-service ports should be denied. This not only denies intelligence to an external/malicious entity, it protects the servers behind the firewall by blocking potentially malicious packets from reaching any unnecessary services that may be running. The risk of not screening the servers exposes the layout of the network to a potential attacker. Unblocked ports can serve as actual attack vectors.

This is measured by scanning through the firewall and capturing the packets that penetrate it. The firewall will fail should any of the scan packets leave the internal interface, even if the target server does not reply to the stimulus packet, this is not sufficient to pass. The only exception is for explicitly accepted service ports, *e.g.* allowing scan packets for TCP/80 and TCP/443 to the identified web server farm.

In order to score Green, the firewall must not allow any of the scans to penetrate, should it fail any of the ICMP tests, it will score Yellow—any failure to block the TCP or UDP scans will score Red.

Is the system set to GMT? Is it using NTP and synchronizing to at least 2 servers? (NSA)

This is to ensure that reported logs are synchronized. Since this is an international organization, GMT is used for the universal time zone of all devices in the environment. Lack of time synchronization and use of a non-GMT time zone injects unnecessary confusion into the troubleshooting process and will make the logs less useful should they ever be needed for prosecution.

To test, inspect the IPSO active configuration file looking for `timezone Etc/Greenwich` which will identify that the time zone is set correctly. Look for `ntp server` lines to ensure that at least two servers are set. These servers should be official production level NTP servers of the organization.

Scoring is Green only if the firewall is set to GMT and at least two NTP servers are configured, Red if it is neither set to use NTP nor GMT; otherwise it is Yellow.

Is there a syslog server defined? Is the syslog server a dedicated syslog server? (SCORE, NSA, FISCAM, ISACA)

This is asked to ensure that logs are being captured. If there is no logging, the debugging process is severely affected which will have a sizeable impact on availability of the system should something fail. Also, a lack of logs is catastrophic to any incident investigation effort.

Inspect the IPSO active configuration for `syslog action remote` and verify that the server configured there is an official enterprise syslog server. This server should be used only for collecting logs, it should not be a multipurpose server.

Scoring is Green if a syslog server is configured and that server is a dedicated syslog server. If the server is not dedicated, sore Yellow. Score Red should there be no syslog server defined.

If SNMP is enabled, is it using Version 2c or better? Is the read-only community string set to something other than "public?" Is read-write SNMP access disabled? (Top20)

Remote monitoring of the firewall is important to ensure availability of the system. If the firewalls are not monitored, outages may last longer than they should. If the implementation of this monitoring is not secure, additional risks to availability and confidentiality are introduced into the network.

To test, check the active IPSO configuration file for `snmp community`. This community string should be set to something other than "public." Use **snmpwalk** to probe the firewall using version 1 requests; the firewall should not respond to this request.

Score Green if SNMP is running Version 2c or better with the read-only community string set to other than "public," and the read-write community string is disabled. Score red if SNMP is not running, or is running in version 1, or set with the "public" community string. Otherwise, score yellow.

Is the firewall reporting to a threshold-monitoring and trending system?

This is asked to ensure that metrics of the firewall are being captured and that issues affecting availability, such as resource exhaustion, are reliably detected. Failure to monitor the firewall for health increases the risk of undetected resource issues that may impact availability.

To test, request a copy of the monitoring reports for the firewall.

Score Green if reports from the trending system and the threshold-monitoring system are available for the device. If neither is available, score Red. Otherwise, score Yellow.

Are the logs analyzed for suspicious activity? (SCORE, FISCAM)

This is asked to determine how attempts to violate the security policy would be detected. If logs are not being analyzed and reported on. A successful penetration of the perimeter defenses may go undetected much longer than it normally should. This compounds the impact of a security incident.

To test, request a copy of the analysis reports and the reporting procedure documentation.

Although judging if the analysis is effective is a subjective matter, we objectify it by only measuring if a process exists. The effectiveness of such a policy is out of scope for this audit.

Score Green if reports and procedure documentation are available, Yellow if only reports are available, and Red if reports are not available.

Are the logs retained for 1 year or more, and are they stored safely?

This is asked to ensure that logs are available for investigation and prosecution purposes. Future investigation and prosecution efforts may be put at risk if logs are not retained sufficiently and safely.

Test by requesting a copy of firewall access logs from over twelve and over six months ago.

Score Green if both logs are available, Yellow if the plus-six month logs are available, Red otherwise.

All administrative traffic to the firewall must be encrypted. (Top20)

This step is taken to ensure the confidentiality of administrative credentials. Accounts and passwords used to manage the firewall must not be transmitted in the clear. If this step is not taken, an inside malicious entity could easily gain control of the firewall and alter its policy.

To test, verify that no plaintext protocols are enabled and running on the firewall. These include: FTP, telnet, rlogin, rsh, and HTTP. Verify that these ports are not open by a scan. Verify that the daemons are not running by inspection of the process stack. Verify that these services are not defined in inetd.conf should inetd be running on the firewall. Management traffic between the firewall (enforcement point) and the management module is encrypted and authenticated using Secure Internal Communication (SIC[5].) Access to the Voyager interface should be only by HTTPS, test by attempting to connect via HTTP. Remote command line access to IPSO should be only by SSH, and SSH protocol 1 should not be supported. Test by attempting to connect using protocol 1 or use scanssh[6].

Scoring is Red if any plaintext authentication protocols are detected, Yellow if SSH is running in protocol 1, Green otherwise.

All administrative access to the firewall must use two-factor authentication. (Top20, FISCAM)

Two-factor authentication is used to limit the impact of a compromised password. If this is not used, a leaked password could be used to manage the firewall in an unauthorized manner, exposing the network to further impacts to confidentiality.

To test, have the administration staff demonstrate their log-in procedure, or use the log-in procedure they provide for you to inspect the box (which might not be available to an auditor.) If local passwords are used for authentication, the firewall will fail this test, unless mitigating factors are in place. Such mitigating factors (such as the firewall can only be managed from a server that itself has two-factor authentication) will have to be tested and verified. This makes this question potentially subjective.

Score Green if two-factor authentication is used for all access methods, otherwise Red.

Can the firewall be remotely administered from the outside interface? (ISACA)

This is asked to ensure that the firewall can only be managed from the inside, thus reducing the risk of exposure to external risks. If the firewall is manageable from the outside, this increases the chance that a compromised account/password pair or other authentication credentials will be used against the network.

To test, scan for management ports from the outside interface (TCP 256, 257, 258, 259, 18210, 18211, 18186, 18190, 18191, and 18192,) or attempt to use the management software from the outside. Attempt to connect to Voyager (*i.e.* connect with a browser on HTTP and HTTPS) from the outside. Attempt to log into the command line remotely from the outside.

Score Red if ANY of these connections succeed, Green if all of these ports are blocked in the scan, otherwise Yellow (*i.e.* if some ports are visible, but you can not authenticate through them.)

Is there a periodic "Entitlement Audit?" (FISCAM)

An entitlement audit is a review of accounts on the firewall and firewall manager systems, to verify that the account holders are still employed by the organization and authorized for access to the firewall. This is done to reduce the number of accounts on the system, and to ensure that unused accounts are not still active on the system. Unnecessary accounts offer more account/password pairs that could potentially be discovered by a malicious entity and used to manage the firewall in an unauthorized manner, thus placing confidentiality of the network at risk.

To pass, the administrators must provide documentation of the "entitlement audit" process, and past entitlement audit reports.

Score Green if these documents are present, otherwise Red.

[5] Welch-Abernathy

[6] http://monkey.org/~provos/scanssh/

Are wellness checks in place to ensure that changes to the firewall do not subject the enterprise to a denial of service? (SCORE)

Mistakes happen; the purpose of this question is to ensure that the organization can detect these mistakes before they have measurable impact. Otherwise, the response time to a self-imposed outage will be longer than necessary.

To test, view the process documentation or monitoring reports for the firewall. There should be wellness checks to verify that the firewall is able to pass traffic. For bonus points, critical services should also be tested.

Score Green if the documentation is present, otherwise Red.

Are critical firewall application and underlying OS files protected by file integrity tools? (ISACA)

File integrity tools should be used in order to detect changes made to the firewall application and underlying OS. Otherwise, changes made to the system, planned or otherwise may go undetected. This could delay debugging an issue caused by an accidental change. In the case of malicious change, a lack of file integrity checks could allow a compromised firewall to exist in the network undetected.

To test, the administrators must demonstrate which file integrity tools they are using and provide outputs of the file integrity reports.

Score Green if a tool is in place and reports are available, Yellow if a tool is installed but reports are not actively monitored, Red otherwise.

Is the policy implementation uniform across the entire perimeter? (SCORE)

Consistency is the goal. In a large organization there are many administrators, and often there are independent management structures responsible for sections of an organization's perimeter. If these independent groups are not implementing the perimeter policy uniformly, the organization as a whole is at risk to confidentiality issues, (see appendix 3.)

This is meta-checklist item. To measure, score each enforcement point and aggregate per management group. Compare management groups to one another and calculate their average score of Red, Yellow, or Green.

Scoring is based on uniformity. It's better to have everyone scoring middle ground than a large spread of groups scoring high and low. Score Green if less than 10% of the management groups are below the organizational average, Yellow if less than 25% are, otherwise Red.

Assignment 3

Conducting the Audit

Simply put, conducting the audit involves collecting the system state, evaluating that against the checklist, and reporting to the client. Auditors will request documentation, reports, and configuration files of the system to be audited. Interactive scans are also used to verify that the configuration accomplishes the goals set forth in the security policy. Sometimes interviews are used to collect information. This should be avoided since and results of an audit so rely on objective facts, not how well a given system administrator may present himself or herself in a interview.

Request for Information

The auditor must communicate clearly what is required to complete the audit. The system administrators are busy people doing important work, and wasting their time is a disservice to the organization. Also, if the documentation requirements of the audit are not clearly communicated, the system administrators will show up at the audit unprepared, wasting everyone's time. In addition to clarity, the request must be timely and reasonable. Some requests (like requests for historical log files,) take time and may require the system administrator to go through process to acquire the information. Making incomplete requests for information that arrive at 4:30 on a Friday with close-of-business deadlines are not going to result in an accurate audit. Realistic timelines in requests for information with reminders as deadlines approach will certainly improve the Auditor/System Administrator relationship.

For example:

```
To: Firewall Administrator/Audit-point-of-Contact
From: Corporate Auditor
Date: February 2nd, 2004
Subject: 2004 Q1 Firewall Audit Warning Order

      We wish to begin the Quarterly Audit of your firewalls on
February 16th, 2004.  In order to make this as smooth as possible we
will require the following on or before the close of business, Friday
February 13th, 2004.

      A Copy of the Firewall policy
      Contents of the following files:
            /config/active
            /etc/inetd.conf
            /var/etc/ipsrd.conf
            /etc/motd
      The following Process and Procedure documents:
            Monitoring firewall synchronicity
            Vulnerability scanning policy and schedule
            Vulnerability resolution procedure and SLA documentation
            Firewall egress/ingress verification procedure with
schedule of scans
            Access log analysis procedure
            Entitlement audit procedure and schedule
            Wellness check procedure
            File integrity check procedure
      The following reports:
            Firewall synchronicity
```

- Recent vulnerability-scan for each interface of the firewall.
- Vulnerability resolution report
- Egress/ingress verification report
- Access log analysis report
- Resource and availability monitoring report
- Entitlement audit report
- Wellness check report
- Fire integrity check report
- The access log from February 16, 2003.
- The access log from September 16, 2003.

Output from the following commands:

- chaprob state
- ps -aux

Output from the resource monitor for the firewall
Output from the threshold monitor for the firewall

At the audit, the system administrator will be expected to demonstrate the log in procedure used to administrate the firewall, and fill in any blanks caused by a lack of documentation.

For February 16th, 2004, the audit team will need access to every switch that the firewall has an interface on. A series of packet scans and tests are planned between 2200 February 16, 2004 and 0200 February 17, 2004.

This type of request for information sent ahead of time, followed by one week, three day, and one day reminder expresses the required level of respect to the system administrator. The expectation of the system administrator is clear, and the interview is kept as short as possible.

Scanning the Firewall

As specified in the audit-warning document, the audit staff needs access to the switches that the firewall has interfaces on. Audit should supply a scanner and sniffer for this procedure, and they should be placed on switch interfaces that are spanned.

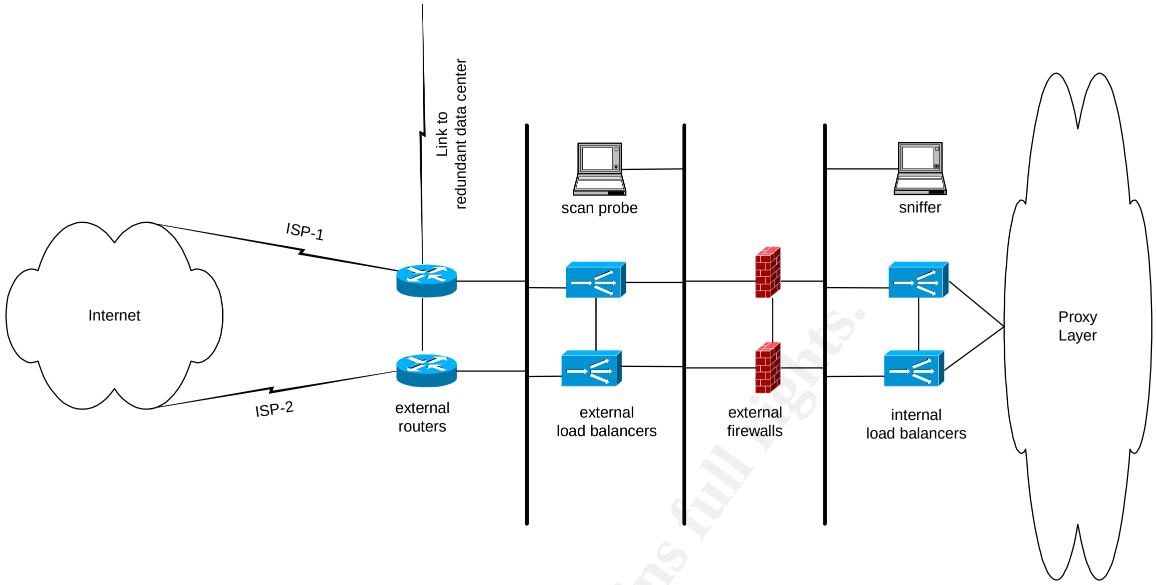


Figure 5: Placement of Scanner and Sniffer for Firewall Testing.

Scans are then executed against and through the firewall. Footprints of the successful scans are plotted and used in the scoring process. Since production traffic will appear in the sniffer captures, the footprinting process should be executed with care and the capture files should be encrypted and not used in any audit report.

Tcpdump[7] is used to capture the session from the inside, and nmap[8] is used to generate the scan packets. The process is fairly simple, a fully negotiate TCP and UDP scan is attempted from the scanning laptop to the following targets: external firewall interface, internal firewall interface, internal DNS server, and internal SMTP server. Nmap itself has an extensive arsenal to scanning tools to throw at the firewall, but for the purposes of this audit, we restrain the scans to simple protocol-abiding behavior. We perform the scan from an organizational IP number, and an external IP number and test the anti-spoofing rules by spoofing an internal IP number. In addition to saving the packet captures on the internal sniffer, the output from the nmap scans are saved.

Here is the nmap output from the scans:

```
Scanner0:~/security_tools/nmap –sT –P0 <external_firewall_interface>

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-02-21 23:30 GMT
All 1659 scanned ports on <external_firewall_interface> are: filtered

Nmap run completed – 1 IP address (1 host up) scanned in 1360.608 seconds

Scanner0:~/security_tools/nmap –sU –P0 <external_firewall_interface>
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-02-22 01:30 GMT
All 1478 scanned ports on <external_firewall_interface> are: filtered

Nmap run completed – 1 IP address (1 host up) scanned in 1778.970 seconds

Scanner0:~/security_tools/nmap –sT –P0 <internal_firewall_interface>

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-02-21 23:58 GMT
All 1659 scanned ports on <internal_firewall_interface> are: filtered

Nmap run completed – 1 IP address (1 host up) scanned in 1360.605 seconds

Scanner0:~/security_tools/nmap –sU –P0 <internal_firewall_interface>
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-02-22 02:02 GMT
```

[7] http://www.tcpdump.org
[8] http://www.insecure.org/nmap/

```
All 1478 scanned ports on <internal_firewall_interface> are: filtered

Nmap run completed – 1 IP address (1 host up) scanned in 1779.026 seconds

Scanner0:~/security_tools/nmap –sU –sT –P0 –S <spoofed_internal_ip> <smtp_server>
<dns_server>
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-02-22 02:35 GMT
All 3137 scanned ports on <smtp_server> are: filtered

All 3137 scanned ports on <dns_server> are: filtered
```

The results for the spoofed IP are to be expected since the results are going to return to the IP that is spoofed, and not to the scanner.

The scanning footprint is produced from the packet captures. The captures are filtered and the output is reduced showing a list of what packets got through. By counting the number of unique source port/destination port pairs per IP we can come up with a ratio of successful to unsuccessful scans.

```
/usr/sbin/tcpdump –n –nn –r capturefile tcp and src <external_scan_ip> or src
<spoofed_internal_ip>| awk ‘{print $2 “ “ $4}’ | ./calc_footprint.pl[9]
<external_scan_ip>:34297 -> <dns_server>: 1659
<spoofed_internal_ip>:41735 -> <smtp_server>: 1659
<spoofed_internal_ip>:41732 -> <smtp_server>: 1659
<external_scan_ip>:34297 -> <smtp_server>: 1659
<external_scan_ip>:34294 -> <smtp_server>: 1659
<external_scan_ip>:34293 -> <smtp_server>: 1659
<spoofed_internal_ip>:41733 -> <smtp_server>: 1659
<external_scan_ip>:34293 -> <dns_server>: 1659
<external_scan_ip>:34296 -> <smtp_server>: 1659
<external_scan_ip>:34294 -> <dns_server>: 1659
<spoofed_internal_ip>:41736 -> <smtp_server>: 1659
<external_scan_ip>:34296 -> <dns_server>: 1659
```

The footprint calculations in this case are trivial, when scanning from the external IP and the spoofed internal IP, 100% of the TCP scan packets passed through the firewall.

```
/usr/sbin/tcpdump –n –nn –nnn –r capturefile udp and udp[4:2] = 8| awk ‘{print $2 “ “
$4}’|./calc_footprint.pl
<spoofed_internal_ip>:41733 -> <smtp_server>: 1250
<external_scan_ip>:34293 -> <dns_server>: 1477
<external_scan_ip>:34294 -> <dns_server>: 1477
<spoofed_internal_ip>:41732 -> <smtp_server>: 1477
<external_scan_ip>:34294 -> <smtp_server>: 1477
<external_scan_ip>:34293 -> <smtp_server>: 1477
```

Here we are interested in only the probes which are 0 length UDP packets.

[9] See Appendix 1 for calc_footprint.pl

Table 2: Inbound Scan Footprint

Source IP	Source Port	Scan Type	Scan Target	Success %
External_scan_ip	34293, 34294, 34296, 34297	TCP	smtp_server	100
External_scan_ip	34293, 34294, 34296, 34297	TCP	dns_server	100
External_scan_ip	34293, 34294	UDP	smtp_server	100
External_scan_ip	34293, 34294	UDP	dns_server	100
Spoofed_internal_ip	41732, 41735, 41736	TCP	smtp_server	100
Spoofed_internal_ip	n/a	TCP	dns_server	0
Spoofed_internal_ip	41732, 41732	UDP	smtp_server	100
Spoofed_internal_ip	n/a	UDP	dns_server	0

The audit team conducts the egress filter tests by generating spoofed traffic from the sniffer, and captures it on the probe system.

Table 3: Egress Scan Results

Source IP	Source Port	Scan Type	Scan Target	Success %
RFC1918	32778, 32779	TCP	external_scan_ip	100
RFC1918	35342, 35343	UDP	external_scan_ip	100

Analyzing the Configuration Files

An auditor could sit down with the configuration files and command output supplied during the request for information phase and score them by hand. Since there are potentially hundreds of firewalls a more automated approach is required. I have created a set of rules to analyze the files and command output requested that works with the RAT[10] tool developed by the Center for Information Security. The rules are available in Appendix 2.

Here is output from the RAT tool for the firewall:

[10] http://www.cisecurity.org/bench_cisco.html

Router Audit Tool report for

audit_test.txt

Audit Date: Mon Feb 23 03:21:10 2004 GMT

Sort Order: importance,passfail,rule,device,instance,line

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number.
5	pass	IPSO - syslog server	audit_test.txt		
5	pass	IPSO - ntp server 3	audit_test.txt		
5	pass	IPSO - ntp server 2	audit_test.txt		
5	pass	IPSO - SNMP RO community string should not be public	audit_test.txt		
5	pass	IPSO - SNMP RO community string set correctly	audit_test.txt		
5	pass	IPSO - RIP should be disabled	audit_test.txt		
5	pass	IPSO - OSPF should be disabled	audit_test.txt		
5	pass	IPSO - IGRP should be disabled	audit_test.txt		
5	pass	IPSO - HTTPS Enabled	audit_test.txt		
5	pass	IPSO - GMT	audit_test.txt		
5	pass	CheckPoint - Synchronization is active - primary	audit_test.txt		
5	pass	CheckPoint - Synchronization is active - secondary	audit_test.txt		
5	FAIL	IPSO - ntp server	audit_test.txt	n/a	2
5	FAIL	IPSO - Telnet Disabled	audit_test.txt	n/a	738
5	FAIL	IPSO - TFTP Disabled	audit_test.txt	n/a	24
5	FAIL	IPSO - HTTP Disabled	audit_test.txt	n/a	118
5	FAIL	IPSO - FTP Disabled	audit_test.txt	n/a	261

Supplied Command Output

The command output and copies of files are below. The contents of /config/active and /var/etc/ipsrd.conf are omitted since they are analyzed by RAT.

```
abcd1[admin]# cphaprob stat

Working mode:   Service

Number     Unique Address  State

1          192.168.200.2   active
2 (local)  192.168.200.1   active


abcd1[admin]# ps -aux
USER       PID %CPU %MEM   VSZ  RSS  TT  STAT STARTED       TIME COMMAND
root     22089  0.0  0.0   464  220  p9  R+    3:18AM    0:00.01 ps -aux
root         1  0.0  0.0   356  192  ??  Is   12Jul03    0:00.02 /sbin/init --
root         2  0.0  0.0     0   20  ??  DL   12Jul03    0:00.00  (pagedaemon)
root         3  0.0  0.0     0   20  ??  DL   12Jul03    0:00.00  (vmdaemon)
root         4  0.0  0.0     0   20  ??  DL   12Jul03   82:42.93  (update)
root        60  0.0  0.0   188  380  ??  Ss   12Jul03    3:29.13 syslogd -6
root        70  0.0  0.1   836  556  ??  Is   12Jul03    0:00.06 /bin/pm
root        89  0.0  0.3  4484 3372  ??  I    12Jul03    0:00.90 /opt/CPshared-50-
03/bin/cprid
root       204  0.0  0.0   160  500  ??  I    12Jul03    0:00.00 /usr/libexec/getty Pc
ttyv0
root       205  0.0  0.0   160  500  ??  I    12Jul03    0:00.00 /usr/libexec/getty Pc
ttyv1
root       206  0.0  0.0   160  500  ??  I    12Jul03    0:00.00 /usr/libexec/getty Pc
ttyv2
root       207  0.0  0.0   160  500  d0  Is+  12Jul03    0:00.00 /usr/libexec/getty
std.9600 ttyd0
root       208  0.0  0.0   160  500  ??  I    12Jul03    0:00.00 /usr/libexec/getty
std.9600 ttync
root       211  0.0  0.3  1920 2940  ??  Is   12Jul03    3:28.03 /bin/xpand
root       212  0.0  0.1   544  840  ??  Is   12Jul03    0:00.49 /bin/ifm /config/active
root       221  0.0  0.1   180  536  ??  Is   12Jul03    0:00.00 /usr/sbin/inetd -n
root       224  0.0  0.2  4328 1864  ??  Ss   12Jul03    4:05.97 /bin/ipsrd -N
root       233  0.0  0.1   320  736  ??  Is   12Jul03  825:10.45 /bin/monitord
root       241  0.0  0.1   352  716  ??  Is   12Jul03    0:00.01 /bin/oamd
root       242  0.0  0.1   268  548  ??  Is   12Jul03    0:44.88 /usr/sbin/cron
root       243  0.0  0.1   204  524  ??  Is   12Jul03    0:00.00 /bin/pccardd
root       244  0.0  0.1   684 1156  ??  Is   12Jul03    0:00.06 /opt/CPshared-50-
03/bin/cpwd
root       245  0.0  0.1   404 1200  ??  Ss   12Jul03    0:21.17 /usr/sbin/sshd-x -D
root       265  0.0  5.5 56348 57348  ??  Ss   12Jul03  113:42.01 cpd
root       266  0.0  2.6 26896 26980  ??  Ss   12Jul03  1383:33.27 /bin/snmpd -f
root       375  0.0  2.7 22012 28156  ??  Ss   12Jul03   21:01.08 /opt/CPfw1-50-
03/bin/cphamcset
root       401  0.0 16.0 175476 167400  ??  Ss   12Jul03  4396:50.88 fwd (fw)
root       423  0.0  3.9 33180 41188  ??  I    12Jul03    3:36.95 in.asessiond 0 (fwssd)
root       424  0.0  3.9 33024 40996  ??  S    12Jul03   11:48.52 in.aufpd 0 (fwssd)
root       426  0.0  4.1 35244 42316  ??  S    12Jul03  122:31.56 mdq 0 (fwssd)
root      9253  0.0  0.1   584  896  ??  S<s  27Jul03   12:37.46 /bin/xntpd
root      7695  0.0  0.2   952 1916  ??  Ss    1Feb04    0:43.55 /bin/httpd -d /web
nobody    7696  0.0  0.1  1044 1136  ??  I     1Feb04    0:00.02 /bin/httpd -d /web
nobody    7697  0.0  0.1  1056 1176  ??  I     1Feb04    0:00.03 /bin/httpd -d /web
nobody   21746  0.0  0.1  1068 1176  ??  I     6:22PM    0:00.04 /bin/httpd -d /web
root     22084  0.0  0.1   516 1140  ??  S     3:18AM    0:00.11 sshd-x: admin@ttyp9
(sshd-x)
root     22085  0.0  0.0   552  424  p9  Ss    3:18AM    0:00.03 -csh (csh)
root         0  0.0  0.0     0    0  ??  DLs  -          0:00.00  (swapper)

abcd1[admin]# cat /etc/motd
IPSO 3.5.1-FCS6 #963: 03.12.2003 021500
abcd1[admin]# cat /etc/inetd.conf
#  This file was AUTOMATICALLY GENERATED
#  Generated by inetd_xlate on Sat Jul 12 01:37:02 2003
#
#  DO NOT EDIT
#
```

Scoring the Firewall

We will use the scan footprint, RAT output, the Firewall Rule Policy, command output, and some of the requested documentation to generate the score for this device.

Is the firewall in a high-availability configuration? Are the members of the "cluster" synchronized?

According to the RAT tool, the primary and secondary cluster members are in sync. Since testing positive for synchronization requires that synchronization be configured, both tests are satisfied. The firewall scores GREEN for this test.

Does a vulnerability-scan report any vulnerabilities when run from the outside or from the inside?

For this test we accept documentation from the organization's official vulnerability scanner. In this case the document is:

Network Host Assessment Report **Sorted by IP Address 02/10/2004**

This report lists the hosts discovered by Internet Scanner after scanning the network, and for each host, identifies network services, user details, banner details, and vulnerabilities.
Intended audience: This report is intended for security technicians (Security Administrators, Network Administrators,
Workstation Support Engineers, or Helpdesk Support Engineers).
Purpose: For each host, the report provides the IP address, the DNS Name, the operating system type, and the status of the host (reachable or unreachable). The report also provides information about services, users, and banners identified by Internet Scanner.
Related reports: For a brief description of the hosts identified by Internet Scanner after scanning the network, see the Line Management/Host Assessment reports.
Vulnerability Severity: High Medium Low L H M

Session Information

Session Name: firewall-dmz-introutable-mgmt **File Name:** firewall-dmz-introutable-mgmt_20040206_193452.log
Policy: 123456AB-123A-1234-1234-A1A12345A123/12345678
License: Router, Switch, & Firewall 02-06-04
56 **Hosts Scanned:** 56 **Hosts Specified:**
Scan Start: 2/6/2004 8:03:35PM **Scan End:** 2/6/2004 7:34:52PM
Comment:

Status Operating System IP Address {DNS Name}
<firewall_internal_interface> (Unknown OS)   None
<firewall_external_interface> (Unknown OS)   None

Here there are no visible vulnerabilities on either interface so the firewall scores GREEN for this test.

No unnecessary services should be running on the firewall. The following services must not be running on the firewall: FTP, TFTP, telnet, SMTP, POP3, IMAP, rlogin, rsh, HTTP, RPC, DNS, NFS, NIS and any load balancing services. HTTPS is permitted.

The external and internal port scan did not detect any of these services listening. The RAT scan reported that Telnet, FTP, TFTP, and HTTP were enabled. We then consult the output of **ps –aux** and the contents of the inetd.conf file.

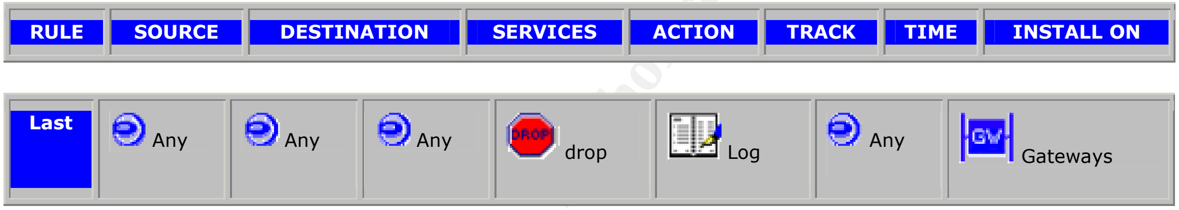
According to the process table, inetd is running, but inetd.conf has no services defined within. This covers all of the services except HTTP. The audit team was unable to make a connection to port 80 from neither inside nor outside of the firewall. The firewall scores GREEN on this test.

No dynamic routing protocols are to be used by the firewall.

RAT tests for the presence of networks using RIP, OSPF, or IRGP in the configuration. For this firewall RAT passes all three protocols. The firewall scores GREEN on this test.

Is there a default-deny cleanup rule that appears at the end of the rule base? Is egress filtering in place? Are spoofed/illegal addresses blocked?

We consult the provided rule base looking for the cleanup rule at the end that enforces the “default deny” policy.

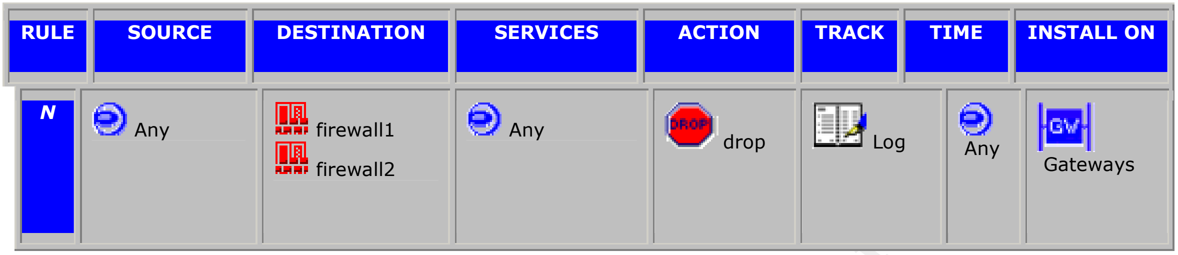


RULE	SOURCE	DESTINATION	SERVICES	ACTION	TRACK	TIME	INSTALL ON
Last	Any	Any	Any	drop	Log	Any	Gateways

The scanning footprint shows that inbound spoofed addresses are not being blocked. The egress footprint also indicates that spoofed addresses are not be blocked outbound. Since two tests failed, the firewall scores RED.

Is the firewall invisible from the outside? Is there a stealth rule present near the top of the policy? The Check Point management ports: 256, 257, 258, 259, 18210, 18211, 18186, 18190, 18191, and 18192 must not be open to the outside. The firewall must not identify itself as such in banners, MOTD files, hostname, or DNS records.

We inspect the rule base, looking for the stealth rule:



RULE	SOURCE	DESTINATION	SERVICES	ACTION	TRACK	TIME	INSTALL ON
N	Any	firewall1 firewall2	Any	drop	Log	Any	Gateways

We consult the results of the external nmap scan of the external and internal firewalls interfaces and see that no ports respond to probes. The /etc/motd file does contain identifying information, like the version and patch level of IPSO, but this is not displayed until authentication over SSH, so this risk is mitigated. The local hostname of the firewall does not contain any identifying strings. The forward DNS name is equivalent to the hostname. The firewall does not have a reverse DNS entry.

We score the firewall GREEN for this test.

Does the firewall effectively cloak assets behind it? Block incoming ICMP echo requests, outgoing echo replies, time exceeded, and destination unreachable except for ICMP type 3/code 4. UDP traceroute should not work through the firewall. Scans using a source port of 53/TCP, 53/UDP, 520/UDP, and TCP/20 should fail. Scans using high source ports should also fail.

From the scanning fingerprint, we see that the firewall fails this test since no TCP nor UDP packets were blocked. The firewall does block all ICMP, but this is not sufficient to protect the servers behind it.

The firewall scores RED on this test.

Is the system set to GMT? Is it using NTP and synchronizing to at least 2 servers?

RAT indicates that the firewall is using GMT and has two out of three internal NTP servers defined.

We score the firewall GREEN for this test.

Is there a syslog server defined? Is the syslog server a dedicated syslog server?

RAT indicates that the firewall is configured to send syslogs to a corporate syslog server.

The firewall is scored GREEN for this test.

If SNMP is enabled, is it using Version 2c or better? Is the read-only community string set to something other than "public?" Is read-write SNMP access disabled?

RAT scores a pass on the Read-Only community string. All attempts to use **snmpwalk** by the audit team resulted in timeouts.

This results in a YELLOW result for the firewall.

Is the firewall reporting to a threshold-monitoring and trending system?
The administration staff could only provide availability monitoring via pings.
Monitoring of the interfaces was available in the team's Cricket[11] system, illustrated by:

Choose a target

Current path: / Firewalls/ abcd1/

Targets that are available:

Name	**Description**
abcd1	class chassis
abcd1 eth1 Ethernet Layer Intel EtherExpress Pro 10/100B [Octets] [UcastPackets] [Errors]	eth1
abcd1 eth2 Ethernet Layer Intel EtherExpress Pro 10/100B [Octets] [UcastPackets] [Errors]	eth2
abcd1 eth3 Ethernet Layer Intel EtherExpress Pro 10/100B [Octets] [UcastPackets] [Errors]	eth3
abcd1 eth4 Ethernet Layer Intel EtherExpress Pro 10/100B [Octets] [UcastPackets] [Errors]	eth4

Neither response is truly sufficient, but they do meet the very minimum requirements for monitoring.

The firewall scores YELLOW on this item.

Scoring Summary

Table 4: Audit Scoring Summary

Audit Test	Category	Score
Is the firewall in a high-availability configuration?	Availability	GREEN
Does a vulnerability scan show any vulnerabilities?	Vulnerability	GREEN
No unnecessary services are running on the firewall	Vulnerability	GREEN
No dynamic routing protocols are on the firewall	Vulnerability	GREEN
Default deny policy and egress filtering in place	Rule Base	RED
Is the firewall invisible from the outside?	Intelligence Denial	GREEN
Does the firewall effectively cloak assets behind it?	Intelligence Denial	RED
GMT and NTP sync?	Logging	GREEN
Syslogging to dedicated server?	Logging	GREEN
SNMP deployed securely?	Logging	YELLOW
Firewall in threshold and trending systems?	Logging	YELLOW
	Overall	YELLOW

[11] http://cricket.sourceforge.net/

In order to calculate the overall score, we calculate an average per rule category, then average across the aggregate category scores. In this case, Availability is GREEN, Vulnerability is GREEN, Rule Base is RED, Intelligence Denial is YELLOW, and Logging is YELLOW. The average of the overall categories is then YELLOW. This result is fed up into the overall audit to answer the "Is the policy implementation uniform across the entire perimeter?"

Residual Risk

Clearly there is room for improvement for this firewall. There are issues in the Rule Base, Intelligence Denial and Logging categories.

The Rule Base needs to be reconsidered, as it stands it allows any packet in to the DMZ proxy layer, it might not allow sessions to be established, but single-packet attacks could be executed against these resources. This coupled with the policy allowing spoofed internal-IPs into the environment exposes a significant risk to the network availability and confidentiality. During the interview, the administrator indicated that egress and anti-spoofing ingress filters were implemented on the border router, so essentially this risk is mitigated. That may be the case, but the firewall needs to define a perimeter on its own. The costs of upgrading the rule base involve only the manpower required to engineer the rules, test them, and implement them through the corporate implementation process. This would address the issues in the Rule Base and Intelligence Denial categories.

Logging could be improved by using SNMP to monitor more firewall resources. By monitoring CPU, and Memory load, trending may be put to use to predict when the firewall needs a hardware or bandwidth upgrade. The primary issue to address is to get more monitoring of the firewall in the threshold monitor. As it stands, the threshold monitor will alarm when it can no longer ICMP ping the firewall. There should be alarms for CPU and Memory state, as well as a wellness check to test throughput and stat synchronicity. The cost to introduce these measures is also only manpower since the required resources are already in place.

Auditability of the System

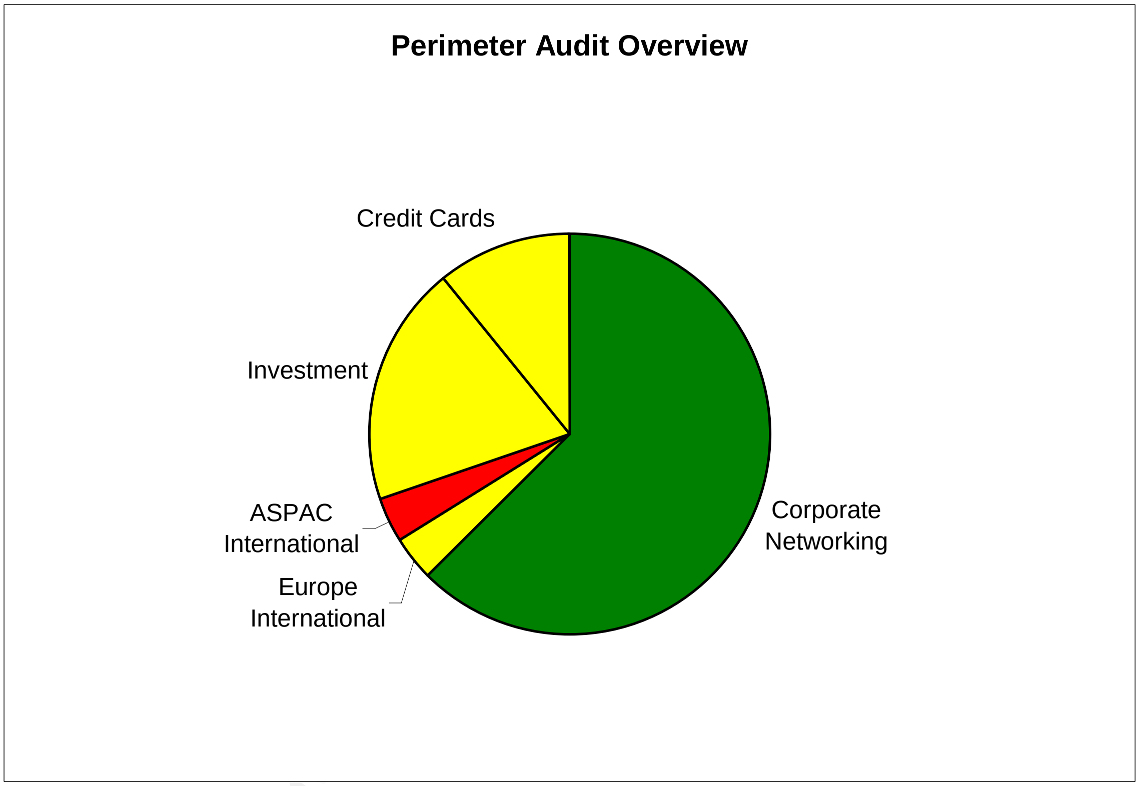
In general, the firewall enforcement point is soundly auditable, even the policies around the management of the firewall can be objectively audited. Very few of the checkpoints in the audit are subjective issues. Effort was focused on defining the checklist items as objectively as possible. The notable exception is the SNMP tests which did not address how the administrators were employing SNMP in their environment. This could have been more accurate had there been a corporate SNMP policy. This illustrates an important lesson: without strong policies, the audit is going to be subjective, and vague, and experience friction when it contacts the system administrators.

Assignment 4

Perimeter Audit Report

Executive Summary

The overall perimeter audit result results



The overall results of the firewall audit for the perimeter firewall abcd1 is: YELLOW

The two major improvement points indicated by the audit are: needed improvements to the firewall rule policy, and the monitoring of the firewall device.

The audit group recommends a rule base review, specifically focusing on reducing the number of external packets that can reach DMZ servers. It is also recommended that anti-spoofing rules be put in place.

The current corporate monitoring system should be leveraged to monitor more metrics on the firewall to manage growth and predict issues.

The costs required to implement these improvements are minimal.

Audit Findings and Exceptions

Audit Test	Category	Score
Is the firewall in a high-availability configuration?	Availability	GREEN
Does a vulnerability scan show any vulnerabilities?	Vulnerability	GREEN
No unnecessary services are running on the firewall	Vulnerability	GREEN
No dynamic routing protocols are on the firewall	Vulnerability	GREEN
Default deny policy and egress filtering in place	Rule Base	RED
Is the firewall invisible from the outside?	Intelligence Denial	GREEN
Does the firewall effectively cloak assets behind it?	Intelligence Denial	RED
GMT and NTP sync?	Logging	GREEN
Syslogging to dedicated server?	Logging	GREEN
SNMP deployed securely?	Logging	YELLOW
Firewall in threshold and trending systems?	Logging	YELLOW
	Overall	YELLOW

Is there a default-deny cleanup rule that appears at the end of the rule base? Is egress filtering in place? Are spoofed/illegal addresses blocked? RED

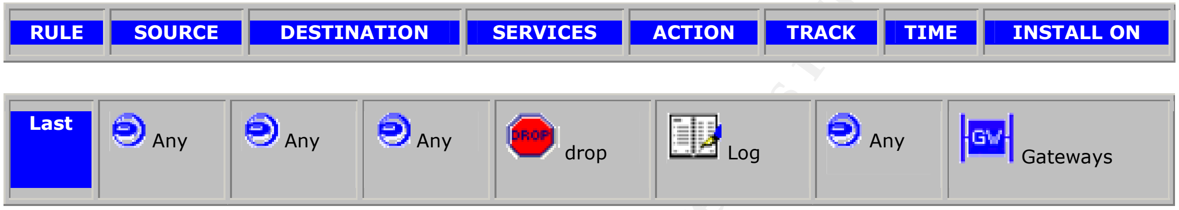
Here the aim is to define a perimeter. With egress and ingress filtering, an inside and an outside are defined. A default-deny policy creates a perimeter that passes only what is explicitly permitted. Failure to define a perimeter places network confidentiality at risk.

If we had asked: “does the firewall form an effective perimeter?” it would have been too vague and subjective of a test. These questions, on the other hand, are definitive, testable, and satisfy the definition of a perimeter.

Inspection of the firewall rule policy is required to determine the presence and location of the default-deny cleanup rule. Egress and spoofing rules are tested via the scanning process. Egress and spoofing rules pass if the network scans to not pass through the firewall.

Scoring is Green if all three tests pass, Yellow if one fails, otherwise Red.

Audit consulted the provided rule base looking for the cleanup rule at the end that enforces the “default deny” policy.



RULE	SOURCE	DESTINATION	SERVICES	ACTION	TRACK	TIME	INSTALL ON
Last	Any	Any	Any	drop	Log	Any	Gateways

Inbound Scan Footprint

Source IP	Source Port	Scan Type	Scan Target	Success %
external_scan_ip	34293, 34294, 34296, 34297	TCP	smtp_server	100
external_scan_ip	34293, 34294, 34296, 34297	TCP	dns_server	100
external_scan_ip	34293, 34294	UDP	smtp_server	100
external_scan_ip	34293, 34294	UDP	dns_server	100
spoofed_internal_ip	41732, 41735, 41736	TCP	smtp_server	100
spoofed_internal_ip	n/a	TCP	dns_server	0
spoofed_internal_ip	41732, 41732	UDP	smtp_server	100
spoofed_internal_ip	n/a	UDP	dns_server	0

Egress Scan Results

Source IP	Source Port	Scan Type	Scan Target	Success %
RFC1918	32778, 32779	TCP	external_scan_ip	100
RFC1918	35342, 35343	UDP	external_scan_ip	100

The scanning footprint showed that inbound spoofed addresses are not being blocked. The egress footprint also indicated that spoofed addresses are not be blocked outbound. Since two tests failed, the firewall scored RED.

Does the firewall effectively cloak assets behind it? Block incoming ICMP echo requests, outgoing echo replies, time exceeded, and destination unreachable except for ICMP type 3/code 4. UDP traceroute should not work through the firewall. Scans using a source port of 53/TCP, 53/UDP, 520/UDP, and TCP/20 should fail. Scans using high source ports should also fail. RED

The firewall should only allow connections to explicitly permitted service ports. Packets intended for non-service ports should be denied. This not only denies intelligence to an external/malicious entity, it protects the servers behind the firewall by blocking potentially malicious packets from reaching any unnecessary services that may be running. The risk of not screening the servers exposes the layout of the network to a potential attacker. Unblocked ports can serve as actual attack vectors.

This is measured by scanning through the firewall and capturing the packets that penetrate. The firewall will fail should any of the scan packets leave the internal interface, even if the target server does not reply to the stimulus packet, this is not sufficient to pass. The only exception is for explicitly accepted service ports, *e.g.* allowing scan packets for TCP/80 and TCP/443 to the identified web server farm.

In order to score Green, the firewall must not allow any of the scans to penetrate, should it fail any of the ICMP tests, it will score Yellow—any failure to block the TCP or UDP scans will score Red.

From the scanning fingerprint, we saw that the firewall fails this test since no TCP nor UDP packets were blocked. The firewall did block all ICMP, but this wss not sufficient to protect the servers behind it.

The firewall scored RED on this test.

If SNMP is enabled, is it using Version 2c or better? Is the read-only community string set to something other than "public?" Is read-write SNMP access disabled? YELLOW

Remote monitoring of the firewall is important to ensure availability of the system. If the firewalls are not monitored, outages may last longer than they should. If the implementation of this monitoring is not secure, additional risks to availability and confidentiality are introduced into the network.

To test, check the active IPSO configuration file for `snmp community`. This community string should be set to something other than "public." Use **snmpwalk** to probe the firewall using version 1 requests; the firewall should not respond to this request.

Score Green if SNMP is running Version 2c or better with the read-only community string set to other than "public," and the read-write community string is disabled. Score red if SNMP is not running, or is running in version 1, or set with the "public" community string. Otherwise, score yellow.

5 pass audit_test.txt

IPSO - SNMP RO community string should not be public

5 pass audit_test.txt

IPSO - SNMP RO community string set correctly

RAT scored a pass on the Read-Only community string. All attempts to use **snmpwalk** by the audit team resulted in timeouts, indicating that SNMP is possibly disabled on the firewall. The tests were unable to conclude what version of SNMP was running.

This resulted in a YELLOW result.

Is the firewall reporting to a threshold-monitoring and trending system? YELLOW

This is asked to ensure that metrics of the firewall are being captured and that issues affecting availability, such as resource exhaustion, are reliably detected. Failure to monitor the firewall for health increases the risk of undetected resource issues that may impact availability.

To test, request a copy of the monitoring reports for the firewall.

Score Green if reports from the trending system and the threshold-monitoring system are available for the device. If neither is available, score Red. Otherwise, score Yellow.

The administration staff could only provide availability monitoring of the firewall via ICMP pings.

Monitoring of the interfaces was available in the team's Cricket system, illustrated by:

Choose a target

Current path: / Firewalls/ abcd1/

Targets that are available:

Name	Description
abcd1	class chassis
abcd1 eth1 Ethernet Layer Intel EtherExpress Pro 10/100B [Octets] [UcastPackets] [Errors]	eth1
abcd1 eth2 Ethernet Layer Intel EtherExpress Pro 10/100B [Octets] [UcastPackets] [Errors]	eth2
abcd1 eth3 Ethernet Layer Intel EtherExpress Pro 10/100B [Octets] [UcastPackets] [Errors]	eth3
abcd1 eth4 Ethernet Layer Intel EtherExpress Pro 10/100B [Octets] [UcastPackets] [Errors]	eth4

Neither response was truly sufficient, but they do meet the very minimum requirements for monitoring.

The firewall scored YELLOW on this item.

Existing Risks

While scanning the firewall for the audit, it was discovered that the rule base is not enforcing anti-spoofing rules and it allows a wide window into the DMZ servers. With these two audit exceptions combined, an attacker could craft packets that would enter the DMZ and appear to come from internal network assets. Single packet attacks are not common, but they do exist. Specifically UDP services are vulnerable in such a scenario due to their connectionless nature. DNS used UDP port 53 for its sessions. BIND, a commonly deployed DNS server, has been known to have Buffer Overflows in the past. Such a packet could be spoofed to enter the environment, crash the stack on a vulnerable version of BIND, which instructs the server to open a back door on nearly any port since the firewall is not blocking inbound high ports to the DMZ servers. What this means is that an outside attacker could gain control of the corporate DNS server, and from there enter further into the network, or alter DNS entries to redirect the corporate web page to a compromised server in China, which masquerades as the company's official eCommerce site, and collect confidential customer information.

The other risks found revolve around monitoring and management. The team is not monitoring and analyzing enough information about the health and performance of the firewall. Although this will not lead to security incidents, it will increase the amount of down time experienced by the network this year. This will manifest as delayed restoration of service, and unnecessary outages that could have been avoided had there been advanced warning.

Recommendations

Immediately, we need to establish a true perimeter with the firewall. The current rule configuration allows too much of the constant scanning that exists on today's Internet into the DMZ. This will require a re-engineering of the firewall rules to implement egress-filtering and anti-spoofing rules in the firewall configuration. There are no extra hardware or software costs involved in adding these rules, only the manpower costs to make these changes through the corporate implementation procedure.

The monitoring strategy should be strengthened. There should be more support for monitoring efforts, and more scrutiny of the reports. This will bring the organization out of "fire-fighting mode" and introduce a more proactive environment. Existing tools can be used to accomplish a more robust level of monitoring. Hardware costs should be low if a new, dedicated server is required.

References:

Alberts, Christopher and Audrey Dorofee. "OCTAVE Threat Profiles." Carnegie Mellon Software Engineering Institute, CERT Coordination Center. URL: http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf (February 11, 2004).

General Accounting Office. Federal Information System Controls Audit Manual. GAO/AIMD-12.19.6. January 1999. URL: http://www.gao.gov/special.pubs/ai12.19.6.pdf (February 11, 2004).

Information Systems Audit Control Association. "IS Auditing Procedure, Firewalls, Document #6." URL: http://www.isaca.org/Template.cfm?Section=Standards&Template=/ContentManagement/ContentDisplay.cfm&ContentID=7223 (February 21, 2004).

McClure, Stuart, Joel Scambray and George Kurtz. Hacking Exposed: Network Security Secrets & Solutions. Fourth Edition. New York, NY. McGraw-Hill/Osborne, 2003.

Naidu, Krishni. "S.C.O.R.E. Firewall Checklist." URL: http://www.sans.org/score/checklists/FirewallChecklist.pdf (February 21, 2004).

National Security Agency, Systems and Network Attack Center. "The 60 Minute Network Security Guide (First Steps Toward a Secure Networked Environment.)" July 12, 2002 V1.2. URL: http://www.isaca-utah/org/pdf/sd-7.pdf

SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities (Updated)" Version 4.0 October 8, 2003. URL: http://www.sans.org/top20 (February 21, 2004).

Schneier, Bruce. Secrets & Lies: Digital Security in a Networked World. New York, NY: John Wiley & Sons, Inc., 2000.

Tipton, Harold F. and Micki Krause, editors. Information Security Management Handbook. Fourth edition. New York, NY. Auerbach Publications, 2000.

Welch-Abernathy, Dameon D. Essential Check Point Firewall-1 NG. Boston, MA: Addison-Wesley, 2004.

Appendix 1: Footprint Calculation Scripts

calc_footprint.pl:

```
#!/usr/bin/perl

while (<>) {
      /(\d+.\d+.\d+.\d+).(\d+) (\d+.\d+.\d+.\d+).(\d+)/;
      $key = $1 . “:” . $2 . “ -> “ . $3;
      #scan{$key}++;
}
foreach $index (keys %scan) {
      print “$index: $scan{$index}\n”;
}
```

Appendix 2: RAT Rules for analyzing IPSO active configuration

The active configuration file from IPSO is located in /config/active on the Nokia Security Appliance. Because RAT uses colons in its rule definitions we have to scrub those out of the configuration usually by using **sed** to filter the file thusly: **sed –e 's/:/ /g'**

In order to get RAT to work on a completely new syntax we had to create a new configuration directory. The following modifications had to be made:

1. `fields.txt` was modified to add the IPSOGlobal group to the ConfigRuleContex definition.
2. `contexts.txt` was drastically reduced to be only: `.*:IPSOGlobal:`
3. `common.conf` was modified to contain internal contacts and refer to internal documents.
4. `cis-level-1.conf` had to be built from scratch, it is below, `cis-level-2.conf` was emptied.

Contents of `cis-level-1.conf`[12]:

```
ConfigDataName:NTP_HOST
ConfigDataQuestion:Address of first NTP server
ConfigDataDefaultValue:<ntp_server_1_IP>
ConfigDataHowToGet:Choose an internal NTP server.
ConfigDataDescription:\
|  | The IP address of this router's main NTP server.

ConfigDataName:NTP_HOST_2
ConfigDataQuestion:Address of first NTP server
ConfigDataDefaultValue:<ntp_server_2_IP>
ConfigDataHowToGet:Choose an internal NTP server.
ConfigDataDescription:\
|  | The IP address of this router's main NTP server.

ConfigDataName:NTP_HOST_3
ConfigDataQuestion:Address of first NTP server
ConfigDataDefaultValue:<ntp_server_3_IP>
ConfigDataHowToGet:Choose an internal NTP server.
ConfigDataDescription:\
|  | The IP address of this router's main NTP server.

ConfigDataName:SYSLOG_HOST
ConfigDataQuestion:Address of syslog server
ConfigDataDefaultValue:<syslog_server_1_IP>
ConfigDataHowToGet:Choose a system to receive syslog messages
ConfigDataDescription:\
|  | The IP address of this system that will receive syslog messages.

ConfigDataName:SYSLOG_HOST_2
ConfigDataQuestion:Address of syslog server
ConfigDataDefaultValue:<syslog_server_2_IP>
ConfigDataHowToGet:Choose a system to receive syslog messages
ConfigDataDescription:\
|  | The IP address of this system that will receive syslog messages.

ConfigDataName:SNMP_RO_STRING
ConfigDataQuestion:SNMP Read-only Community String
ConfigDataDefaultValue:<snmp_ro_string>
ConfigDataHowToGet:Choose the Read-only SNMP Community String
ConfigDataDescription:\
|  | The SNMP Read Only Community String

ConfigDataName:SNMP_RW_STRING
ConfigDataQuestion:SNMP Read-write Community String
ConfigDataDefaultValue:<snmp_rw_string>
```

[12] Note that `ConfigDefaultVaule` settings have been abstracted to the <value> format. Make appropriate changes for your environment.

```
ConfigDataHowToGet:Choose the Read-write SNMP Community String
ConfigDataDescription:\
|  | The SNMP Read/Write Community String


ConfigClassName:Services Configuration
ConfigClassDescription:Services configuration template
ConfigClassQuestion:Audit configuration for services
ConfigClassSelected:Yes
ConfigClassParentName:Selectable

ConfigClassName:Management Configuration
ConfigClassDescription:Management configuration template
ConfigClassQuestion:Audit configuration for management settings
ConfigClassSelected:Yes
ConfigClassParentName:Selectable

ConfigClassName:Logging Configuration
ConfigClassDescription:Logging configuration template
ConfigClassQuestion:Audit configuration for logging settings
ConfigClassSelected:Yes
ConfigClassParentName:Selectable

ConfigClassName:Routing Configuration
ConfigClassDescription:Routing configuration template
ConfigClassQuestion:Audit configuration for routing settings
ConfigClassSelected:Yes
ConfigClassParentName:Selectable

ConfigClassName:HA Configuration
ConfigClassDescription:HA configuration template
ConfigClassQuestion:Audit configuration for HA settings
ConfigClassSelected:Yes
ConfigClassParentName:Selectable

ConfigRuleName:IPSO - ntp server
ConfigRuleParentName:Services Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Required
ConfigRuleMatch:<code>ntp server <param>$(NTP_HOST)</param></code>
ConfigRuleImportance:5
ConfigRuleDescription:Designate an NTP time server
ConfigRuleReason:Set the NTP server(s) from which you obtain time.\
Obtaining time from a trusted source increases confidence in log data \
and enables correlation of events.
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:Designate an NTP time server
ConfigRuleSelected:yes
ConfigRuleOptional:no
ConfigRuleFix:

ConfigRuleName:IPSO - ntp server 2
ConfigRuleParentName:Services Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Required
ConfigRuleMatch:<code>ntp server <param>$(NTP_HOST_2)</param></code>
ConfigRuleImportance:5
ConfigRuleDescription:Designate a second NTP time server
ConfigRuleReason:Set an additional NTP server(s) from which you obtain time.  Additional
time sources increase the accuracy and dependability of system time.
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:Designate a second NTP time server
ConfigRuleSelected:yes
ConfigRuleOptional:yes
ConfigRuleFix:

ConfigRuleName:IPSO - ntp server 3
ConfigRuleParentName:Services Configuration
ConfigRuleVersion:\.*
```

```
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Required
ConfigRuleMatch:<code>ntp server <param>$(NTP_HOST_3)</param></code>
ConfigRuleImportance:5
ConfigRuleDescription:Designate a third NTP time server
ConfigRuleReason:Set an additional NTP server(s) from which you obtain time.  Additional
time sources increase the accuracy and dependability of system time.
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:Designate a third NTP time server
ConfigRuleSelected:yes
ConfigRuleOptional:yes
ConfigRuleFix:

ConfigRuleName:IPSO - syslog server
ConfigRuleParentName:Logging Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Required
ConfigRuleMatch:<code>syslog action remote <param>$(SYSLOG_HOST)</param></code>
ConfigRuleImportance:5
ConfigRuleDescription:Designate one or more syslog logging servers
ConfigRuleReason:Logs must be collected and retained off-site for 1-year
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:Designate syslog server
ConfigRuleSelected:yes
ConfigRuleOptional:no
ConfigRuleFix:

ConfigRuleName:IPSO - GMT
ConfigRuleParentName:Logging Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Required
ConfigRuleMatch:<code>timezone Etc/Greenwich</code>
ConfigRuleImportance:5
ConfigRuleDescription:Designate one or more syslog logging servers
ConfigRuleReason:For correlation purposes, all servers and network devices must be set to
GMT.
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:Designate syslog server
ConfigRuleSelected:yes
ConfigRuleOptional:no
ConfigRuleFix:

ConfigRuleName:IPSO - Telnet Disabled
ConfigRuleParentName:Services Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Forbidden
ConfigRuleMatch:<code>inetd telnet arg 0 telnetd</code>
ConfigRuleImportance:5
ConfigRuleDescription:Telnet should be disabled on this device
ConfigRuleReason:All administrative traffic must be Encrypted
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:Disable telnet daemon
ConfigRuleSelected:yes
ConfigRuleOptional:no
ConfigRuleFix:

ConfigRuleName:IPSO - TFTP Disabled
ConfigRuleParentName:Services Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Forbidden
ConfigRuleMatch:<code>inetd tftp/udp arg 0 tftpd</code>
ConfigRuleImportance:5
ConfigRuleDescription:TFTP should be disabled on this device
ConfigRuleReason:All administrative traffic must be Encrypted
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:Disable TFTP daemon
ConfigRuleSelected:yes
```

```
ConfigRuleOptional:no
ConfigRuleFix:

ConfigRuleName:IPSO - FTP Disabled
ConfigRuleParentName:Services Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Forbidden
ConfigRuleMatch:<code>inetd ftp arg 0 ftpd</code>
ConfigRuleImportance:5
ConfigRuleDescription:FTP should be disabled on this device
ConfigRuleReason:All administrative traffic must be Encrypted
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:Disable FTP daemon
ConfigRuleSelected:yes
ConfigRuleOptional:no
ConfigRuleFix:

ConfigRuleName:IPSO - HTTP Disabled
ConfigRuleParentName:Services Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Forbidden
ConfigRuleMatch:<code>httpd port 80</code>
ConfigRuleImportance:5
ConfigRuleDescription:HTTP should be disabled on this device
ConfigRuleReason:All administrative traffic must be Encrypted
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:Disable HTTP daemon
ConfigRuleSelected:yes
ConfigRuleOptional:no
ConfigRuleFix:

ConfigRuleName:IPSO - HTTPS Enabled
ConfigRuleParentName:Services Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Required
ConfigRuleMatch:<code>httpd ssl_port 443</code>
ConfigRuleImportance:5
ConfigRuleDescription:Telnet should be disabled on this device
ConfigRuleReason:All administrative traffic must be Encrypted
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:Enable HTTPS daemon
ConfigRuleSelected:yes
ConfigRuleOptional:no
ConfigRuleFix:

ConfigRuleName:IPSO - SNMP RO community string set correctly
ConfigRuleParentName:Services Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Required
ConfigRuleMatch:<code>snmp community <param>$(SNMP_RO_STRING)</param></code>
ConfigRuleImportance:5
ConfigRuleDescription:The SNMP Read-only community string should be set correctly
ConfigRuleReason:To enable remote monitoring
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:Set SNMP RO Community string
ConfigRuleSelected:yes
ConfigRuleOptional:no
ConfigRuleFix:

ConfigRuleName:IPSO - SNMP RO community string should not be public
ConfigRuleParentName:Services Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Forbidden
ConfigRuleMatch:<code>snmp community public</code>
ConfigRuleImportance:5
ConfigRuleDescription:The SNMP Read-only community string should be set correctly
```

```
ConfigRuleReason:To enable remote monitoring
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:Set SNMP RO Community string
ConfigRuleSelected:yes
ConfigRuleOptional:no
ConfigRuleFix:

ConfigRuleName:IPSO - RIP should be disabled
ConfigRuleParentName:Routing Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Forbidden
ConfigRuleMatch:<code>ipsrd import_proto rip proto rip network</code>
ConfigRuleImportance:5
ConfigRuleDescription:Dynamic Routing protocols should be disabled
ConfigRuleReason:To enable remote monitoring
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:Set SNMP RO Community string
ConfigRuleSelected:yes
ConfigRuleOptional:no
ConfigRuleFix:

ConfigRuleName:IPSO - OSPF should be disabled
ConfigRuleParentName:Routing Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Forbidden
ConfigRuleMatch:<code>ipsrd import_proto ospf2ase network</code>
ConfigRuleImportance:5
ConfigRuleDescription:Dynamic Routing protocols should be disabled
ConfigRuleReason:To enable remote monitoring
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:Set SNMP RO Community string
ConfigRuleSelected:yes
ConfigRuleOptional:no
ConfigRuleFix:

ConfigRuleName:IPSO - IGRP should be disabled
ConfigRuleParentName:Routing Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Forbidden
ConfigRuleMatch:<code>ipsrd import_proto igrp network</code>
ConfigRuleImportance:5
ConfigRuleDescription:Dynamic Routing protocols should be disabled
ConfigRuleReason:To enable remote monitoring
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:Set SNMP RO Community string
ConfigRuleSelected:yes
ConfigRuleOptional:no
ConfigRuleFix:

ConfigRuleName:CheckPoint - Synchronization is active - primary
ConfigRuleParentName:HA Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
ConfigRuleType:Required
ConfigRuleMatch:<code>192.168.200.1   active</code>
ConfigRuleImportance:5
ConfigRuleDescription:Firewall should be synchronized with is partner
ConfigRuleReason:To ensure availability
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:State in sync
ConfigRuleSelected:yes
ConfigRuleOptional:no
ConfigRuleFix:

ConfigRuleName:CheckPoint - Synchronization is active - secondary
ConfigRuleParentName:HA Configuration
ConfigRuleVersion:\.*
ConfigRuleContext:IPSOGlobal
```

```
ConfigRuleType:Required
ConfigRuleMatch:<code>192.168.200.2   active</code>
ConfigRuleImportance:5
ConfigRuleDescription:Firewall should be synchronized with is partner
ConfigRuleReason:To ensure availability
ConfigRuleDiscussion:Please see the DMZ configuration standard
ConfigRuleQuestion:State in sync
ConfigRuleSelected:yes
ConfigRuleOptional:no
ConfigRuleFix:

ConfigClassName:BenchmarkGroupOrderLevel1
ConfigClassDescription: Container for Level 1 rule classes in the benchmark
ConfigClassSelected:No
ConfigClassOptional:No
ConfigClassQuestion:Include level 1 in the printed benchmark
ConfigClassParentName:Config Globals
ConfigClassChildrenNeeded:Services Configuration,Logging Configuration,Management
Configuration,Routing Configuration
```

Appendix 3: Diversity and Defense in Depth

The concept of Defense in Depth is central to the corporate security policy. The strategy is to force an attacker to create a chain of events in order to exploit a system. The longer the chain and the more bottlenecks that the attacker must go through in order to penetrate a system, the more secure it is, or so the theory goes.

On September 24, 2003, a report was published that caused all sorts of waves in the security community. "CyberInescurity: The Cost of Monoploy," published by the Computer & Communications Industry Association (CCIA,) asserted that software monopoly was a security threat and raised the specter of a software "monoculture." The report caused a backlash in the community, and one of the authors of the report even lost his job over it.

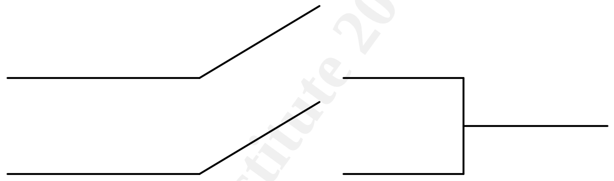
In a case of thesis-antithesis, Mark Burnett published an article on securityfocus.com titled "The Flaw of Security Through Diversification." Claiming that the solution to the threat of monoculture proposed in "CyberInsecurity," that is, risk diversification, is inherently risky and flawed. Marcus Ranum[13] attacks the "CyberInsecurity" report's biological metaphor.

These papers are really arguing about "diversity." "CyberInsecurity" arguing that diversity will reduce catastrophic attacks, Burnett pointing out that more operating systems are more difficult to manage properly.

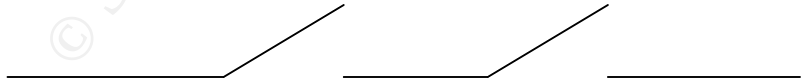
Consider the hypothetical case of a Government Agency using multiple kinds of Web servers. So there are multiple operating systems and HTTP servers each with their own collection of vulnerabilities. Now, if an attacker has more choices of targets, they've just increased the risk of the website being defaced. This is how diversity can harm you.

Now, consider looking at diversity another way. Suppose that our hypothetical Government Agency uses Cisco routers on the perimeter, PIX firewalls behind those, protecting the DMZ, and a CheckPoint solution between the DMZ and the internal network. Now the diverse set of features and vulnerabilities are working together to make much stronger defense.

The attack tree in the first example two major branches: compromise web server configuration one, or compromise web server configuration two. Or to visualize they have two drawbridges to choose from:



In the second example, the attacker would have to cross two drawbridges, on after another. Clearly this route is easier to defend than the former:



Layered diversity is a plus from a security standpoint. Perimeter diversity is a negative. Consider a castle engineer who has the following materials at his disposal: moats, wooden palisades, and stone walls. If he builds a castle with a moat on one side, stone walls on another,

[13] http://www.ranum.com/security/computer_security/rants/monoculture.html

and wooden palisades on the third, you would think his strategy mad. Naturally, you would layer the defenses, perhaps a wooden palisade, surrounding a moat, which surrounds the stone walls.

Let's look at another aspect where diversity can impact security—diversity of management. Continuing to run with the castle metaphor, consider a castle with two gates on opposite sides of the castle. Each gate in managed by a gatekeeper. Now consider that these two gatekeepers have different political views and as a result have differing opinions on who is and who is not a threat to the castle. This clearly could have an ugly outcome.

Diversity of management is not the problem, but the diversity of management policy. As long as the disparate teams are applying the same policy in a consistent manner, there is no additional risk to the organization.

Diversity is not a tool, but a function of the environment. Design around it and use it to your advantage.