



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Auditing Systems, Applications, and the Cloud (Audit 507)"
at <http://www.giac.org/registration/gsna>

Audit of Borderware 6.5 firewall: An Auditor's Perspective

© SANS Institute 2003, Author retains full rights.

John Linehan
GSNA Practical 2.0

Table of Contents

| | |
|---|-----------|
| Introduction..... | 6 |
| Disclaimer | 6 |
| Overview | 6 |
| Terminology | 7 |
| Roles | 8 |
| Assignment 1 – Research in Audit, Measurement Practice and Controls..... | 9 |
| A.1.1- System Identification | 9 |
| Packet Filtering Vs Gateway Technology | 9 |
| Borderware 6.5 Security Architecture | 10 |
| Role of Firewall under audit | 13 |
| Firewall Server Platform..... | 13 |
| Physical Network..... | 13 |
| Logical Network and Information Flow | 14 |
| A.1.2 - Evaluation of Risk to the System | 16 |
| A.1.3- Current State of Practice | 19 |
| Firewall Vendor Information | 19 |
| Certification and Accreditation | 19 |
| Firewall Best Practices..... | 20 |
| Firewall Auditing Practices..... | 22 |
| A.1.4- Improvements on the current state of Practice | 23 |
| Assignment 2 - Creating the Audit Checklist | 24 |
| A.2.1- Policy Documents | 24 |
| Corporate Security Policy | 24 |
| Internet Access Policy | 24 |
| Email Policy | 24 |
| Firewall definition | 24 |
| Firewall Policy | 25 |
| A.2.2- Audit checklist..... | 27 |
| Format of audit checklist | 27 |
| Testing Environment | 28 |
| Control Objectives Group 1 - Policies Procedures and Documentation..... | 32 |
| Control Objectives Group 2 - Physical Access | 40 |
| Control Objectives Group 3 - Redundancy | 42 |
| Control Objectives Group 4 - “Backdoor” Connections | 45 |
| Control Objectives Group 5 - Configurable Services..... | 47 |
| Control Objectives Group 6 - Network Access for Firewall Administration | 63 |
| Control Objectives Group 7 - Firewall Management | 68 |
| Control Objectives Group 8 - Firewall Rule Base and Interfaces | 73 |
| Assignment 3 - Conduct the Audit..... | 91 |
| A.3.2 - Audit Results | 92 |
| Control Objectives Group 1 - Policies Procedures and Documentation..... | 92 |
| Control Objectives Group 2 - Physical Access | 98 |
| Control Objectives Group 3 - Redundancy | 99 |

| | |
|--|------------|
| Control Objectives Group 4 – “Backdoor” Network Connections | 101 |
| Control Objective Group 5 – Configurable Services..... | 103 |
| Control Objectives Group 6 – Network Access for Firewall Administration..... | 117 |
| Control Objectives Group 7 – Firewall Management | 121 |
| Control Objectives Group 8 – Firewall Rule base and Interfaces | 127 |
| A.3.1 - Is the system securable?..... | 141 |
| A.3.3 - Is the system auditable? | 141 |
| Assignment 4 - Follow Up | 143 |
| A.4.1 - Executive summary | 143 |
| A.4.2 - Audit Findings | 144 |
| Audit Finding 1: Change Management Process [CO.1.7] | 144 |
| Audit Finding 2: Firewall Physical Security [CO.2.2] | 146 |
| Audit Finding 3: Firewall Redundancy [CO.3.2]..... | 148 |
| Audit Finding 4: DNS server on external interface [C.O.5.3] | 149 |
| Audit Finding 5: Email Server on Internal and External interfaces [CO.5.3] | 151 |
| Audit Finding 6: Firewall URL filter allows web-based email [CO.5.6] | 153 |
| Audit Finding 7: Internal Remote management Server Security [CO.6.1]..... | 154 |
| Audit Finding 8: Firewall Patch Level [CO.7.1]..... | 156 |
| Audit Finding 9: Additional Servers & Proxies [CO.8.2, 8.9 & 8.10] | 157 |
| Audit Finding 10: IP address ACL on External to SSN WWW Proxy [CO.8.6]..... | 159 |
| Appendices..... | 161 |
| App. 1 – Corporate Documents..... | 161 |
| App. 2 - Interview Questions for IT and Non-IT Personnel | 161 |
| App. 3 – NMAP and Nessus Scan Results | 163 |
| Nmap Scan Report on External Interface | 163 |
| Nessus Scan Report on External Interface | 164 |
| Nmap Scan Report on SSN Interface | 166 |
| Nessus Scan Report on SSN Interface | 167 |
| Nmap Scan report on Internal Interface..... | 167 |
| Nessus Scan Report for Internal Interface..... | 169 |
| External to Internal Nmap Scan | 171 |
| External to Internal Nessus Scan..... | 171 |
| External to SSN Nmap Scan | 172 |
| External to SSN Nessus Scan..... | 172 |
| SSN to Internal Nmap Scan | 173 |
| SSN to Internal Nessus Scan..... | 174 |
| App. 4 – Release Notes for Security Patch 1 | 176 |
| References..... | 178 |

Note: Assignment 2 - *Create the Audit Checklist* - contains tables with checklist items and tests to be performed as well as details on how to perform the tests. These tables are duplicated in Assignment 3 – *Conduct the Audit* - but the actual results (compliant or non-compliant) and comments are included. While this adds to the overall length of the report, it was felt that it allowed the tests results to be easier examined as the reader would not have to constantly refer back to the previous section.

Table of Figures

| | |
|---|-----|
| Fig. 1 Overview of Interaction between Borderware Firewall subsystems..... | 11 |
| Fig. 2: Physical Network Configuration..... | 13 |
| Fig. 3: Internet client accessing SSN web server through HTTP proxy on firewall..... | 15 |
| Fig. 4: Test Environment Setup | 28 |
| Fig. 5: Simple Proxies and Servers access through BWC..... | 47 |
| Fig. 6: BWC Top level menus | 48 |
| Fig. 7: Top level Name Server Configuration Menu | 51 |
| Fig. 8: Top level Email Server Menu | 55 |
| Fig. 9: Sending email from the Firewall SMTP server | 56 |
| Fig. 10: Log Files menu..... | 56 |
| Fig. 11: Internal SMTP Server ACL | 57 |
| Fig. 12: Server Settings in Proxy Server menu | 59 |
| Fig. 13: Server Settings in Proxy Server menu | 65 |
| Fig. 14: Server Settings in Proxy Server menu | 65 |
| Fig. 15: Crypto card configuration for Remote Management Secure Login..... | 67 |
| Fig. 16: Admin menu with Software Updates and Download Patch options | 69 |
| Fig. 17: Alarm Menu | 70 |
| Fig. 18: Servers and Proxies Top Level Menu | 73 |
| Fig. 19: NSLOOKUP on external host using external firewall interface DNS server.... | 105 |
| Fig. 20: Internal SMTP client configuration (1) | 110 |
| Fig. 21: Internal SMTP client configuration(2) | 110 |
| Fig. 22: Email headers on email received by Internet Email account from internal SMTP client bypassing corporate email server | 111 |
| Fig. 23: Firewall external interface relay and email size settings | 111 |
| Fig. 24: External SMTP client configuration (1) | 112 |
| Fig. 25: External SMTP client configuration (2) | 112 |
| Fig. 26: Email headers on email received Internet Email Account from external SMTP client using firewall external interface as a email relay | 112 |
| Fig. 27: Simple WWW proxy enabled | 114 |
| Fig. 28: Squid Proxy disabled..... | 114 |
| Fig. 29: Interfaces enabled for Remote Management | 119 |
| Fig. 30: Remote management authentication | 120 |
| Fig. 31: Installed patches on firewall | 122 |
| Fig. 32: Patches available on Borderware download site..... | 122 |
| Fig. 33: Kiwi Syslog Daemon running on Management Server | 124 |
| Fig. 34: Internal Servers | 128 |
| Fig. 35: External Servers | 130 |
| Fig. 36: Source Address ACL for External to SSM WWW Proxy..... | 133 |
| Fig. 37: Internal to External Proxies | 138 |

List of Tables

| | |
|---|----|
| Table 1: Borderware Firewall Subsystems | 12 |
| Table 2: Hardware configuration of firewall server..... | 13 |
| Table 3: Risks associated with Internet connected firewalls | 17 |
| Table 4: Firewall Best Practices Guide | 20 |
| Table 5: Control Objective Groups | 27 |
| Table 6: Control Objective checklist Sample | 27 |
| Table 7: Configuration of systems for testing | 30 |
| Table 8: Services that should be enabled on each Interface | 73 |
| Table 9: Significant Audit Findings | 91 |

© SANS Institute 2003, Author retains full rights.

Introduction

Disclaimer

This paper presents the findings of an actual audit performed at a client site. All references to the client in question have been deleted. In addition, all public IP addresses have been modified to hide any relationship with the address owner. For the purposes of this report the client will be referred to as *Client Finance Group* or simply “*CFG*”.

Overview

The purpose of this paper is to present the findings of an audit performed on the Borderware 6.5 Firewall Server employed as *CFG*'s Internet gateway. *CFG* is a consulting firm responsible for gathering raw data on behalf of a particular Canadian government department. This information is used to generate reports which are disseminated to specific government departments as well as and industry and education partners.

The organization has recently upgraded its firewall installation from Borderware Firewall Server 6.12 to version 6.5. The newer version, now in production, was installed on new hardware and all configuration settings were migrated from the older installation. All findings are presented from the viewpoint of an external auditor. However I worked very closely with the firewall administrator and had network and physical access to the firewall in his presence. Any tasks requiring root or administrator privileges were performed by the firewall administrator while I observed.

This Borderware 6.5 Firewall Server acts as the Internet and email gateway for *CFG*'s entire network. It separates *CFG*'s production systems from the Internet and acts as the single point of access to and from the network. As such, it is necessary to ensure that it remains as secure as possible based on industry best practices and *CFG*'s corporate security policy while also ensuring that business needs can be met. *CFG* has approximately 250 users of which 200 are located in the same building as the firewall (HQ). The other 50 users connect from regional offices via secure wide area network (WAN).

While this report will reference the larger CGF network architecture and strategies, the main scope of the audit is the Borderware 6.5 Firewall Server itself. This audit will include management, configuration, availability, redundancy and security of the firewall itself as well as the rules employed on the firewall.

Terminology

When referring to the system in question various terms shall be used

1. The **Firewall** is the device (packet filter or gateway) that separates the Internet from the client's production network. As per Borderware's product documentation¹, this may also be referred to as the Firewall Server.
2. The client's production network will generally be referred to as the **internal network**, the **protected network** or the **local area network (LAN)**.
3. When referring to the placement of network devices, servers or workstations, the term **behind the firewall** means on the protected or internal network. The term **in front of the firewall** means on the Internet (unprotected or external) side of the firewall.
4. The client also has a country wide network that connects its regional offices. This network is referred to as the **Wide Area Network (WAN)**. Users who connect from this network are called regional users.
5. As per manufacturer documentation², the term **SSN** (Secure Server Network) is used to refer to the DMZ (De-Militarized Zone) or screened subnet which is hosted off of a 3rd network card on the firewall.
6. As per manufacturer documentation³, the term or **AUX** (Auxiliary network) is used to refer to any subnet hosted off one of the firewall interfaces that is not deemed internal, external or SSN.
7. **ACL** is used to refer to Access Control Lists (either based on user credentials or computer IP address) assigned to resources.
8. The **Borderware Configuration Utility (BWClient.exe or BWC)**⁴ is the windows based utility used to perform Remote Management on the firewall from a computer making a TCP/IP connection to the Remote Management-enabled interface of the firewall.
9. The **Firewall Console** is the actual configuration screen on the firewall itself. This is a menu driven screen and is accessible only when working at the firewall.
10. **Crypto-Card** is the term used by Borderware for the smart card technology used in two-factor authentication for Remote Management.
11. Other terms include the following network protocols and/or services:
 - a. **TCP** – Transmission Control Protocol
 - b. **IP** – Internet Protocol
 - c. **UDP** – User Datagram Protocol
 - d. **FTP** – File Transfer Protocol
 - e. **HTTP** – Hyper Text Transfer Protocol
 - f. **URL** – Uniform Resource Locator (Web site address)
 - g. **WWW** - World Wide Web
 - h. **DNS** – Domain Name Service
 - i. **FQDN** – Fully Qualified Domain Name
 - j. **SMTP** – Simple Email Transfer Protocol
 - k. **SSL** – Secure Sockets Layer
 - l. **SNMP** – Simple Network Management Protocol
 - m. **IPSEC** – Secure Internet Protocol
 - n. **PPTP** – Point to Point Tunneling protocol

- o. **H.232** – protocol used for IP telephony and NetMeeting
- p. **DOS Attack** – Denial of Service
- q. **POP email** – Point of Presence Email
- r. **HSRP** – Hot Standby Routing Protocol

Roles

In this audit report, various parties involved in *CFG's* network are referenced. These are listed below:

IT department (IT): The department responsible for the running of *CFG's* computer systems, network infrastructure, Internet access and helpdesk.

IT Manager: Reports to executive level management and is responsible for the running of the IT department.

Firewall Manager: Responsible for all management of the firewall. This person also manages Internet connectivity issues, WAN connectivity and LAN infrastructure.

Firewall administrator: Responsible for day-to-day administration of the firewall and Internet connectivity. The firewall administrator was the prime contact for this audit. There are two backup firewall administrators who provide only emergency troubleshooting service when on-call. On-call hours for firewall support are 5am to midnight, 7 days per week. The firewall administrators rotate this duty on a weekly basis

Helpdesk manager: Responsible for day-to-day management of Helpdesk

Helpdesk: First point of contact for all user problems relating to all network and computer issues. The helpdesk operates from 7am to 5pm and provides a single (5am to midnight) on-call resource for emergency issues only. This person will perform all preliminary troubleshooting and will notify the on-call firewall administrator if it is determined that a firewall outage is preventing the company from carrying out its mission.

Network Manager: Responsible for all issues regarding WAN and Internet connectivity, perimeter boundaries and control. The same person is designated as Firewall Manager.

ISP: The Internet Service Provider (ISP) is responsible for Internet access. The ISP provides two screening routers (redundant and load balanced over two vendor lines) immediately outside the firewall.

Assignment 1 – Research in Audit, Measurement Practice and Controls

A.1.1- System Identification

The Borderware 6.5 Firewall Server is defined in the manufacturer's product documentation⁵ as a multi-homed firewall. It can be configured with up to 6 network interface cards. It allows for the configuration of an internal (or protected) network, external network, SSN and 3 auxiliary (AUX) networks⁶. The product implements packet filters, circuit level gateways and application level gateways to allow clients to access the Internet.

Packet Filtering Vs Gateway Technology

Before continuing with the discussion of *CFG*'s firewall implementation, a brief discussion on the difference between Packet Filtering firewalls, Application Level Gateways and Circuit Level Gateways will follow:

Packet Filtering Firewall

Packet filtering firewalls drop or allow packets according to source or destination address or port. It is the duty of the firewall administrator to make a list of acceptable and unacceptable computers (IP Addresses) and/or services (Port Numbers). This allows the administrator to filter access at a network or host level but not at a user or application level⁷. The Borderware firewall server monitors each packet destined for all interfaces and filters packets based on whether the source and destination IP addresses and ports are allowed. It also filters out potentially dangerous traffic such as packets with false source IP addresses⁸.

Application Level Gateways

An application level gateway - or proxy firewall - differs from a packet filtering firewall in the way it exercises control on the traffic in an out of the network. It will attempt to enforce integrity in the connection by ensuring that the packets that pass on a particular port actually contain traffic associated with that port⁹. For example, it is possible for a malicious hacker to craft a packet on Port 80 (default port for HTTP requests) that is not necessarily a genuine HTTP request but is in fact a piece of malicious code. A packet filtering firewall would allow this packet to pass through to the internal network if port 80-traffic was allowed to do so but an application level gateway would examine the packet to determine if it really was an HTTP request.

Borderware firewall's application level gateway proxies eliminate direct external connections between the protected internal network and the Internet. The client computer does have control over the Internet host being accessed. For example, enabling the DNS proxy as internal-to-external proxy would allow the clients on the internal network to specify a preferred DNS server on the Internet (at the ISP). The firewall would proxy DNS requests from the client to the ISP DNS server which would see the request as coming from the firewall's external interface and would return resolution to this interface. The firewall would then pass this resolution back to the client.

Circuit Level Gateway

Circuit Level Gateway technology is used in the Borderware firewall to transparently relay outbound connection from hosts on the internal network to hosts on the Internet¹⁰. In the case of Borderware 6.5, as an alternate to using the DNS proxy mentioned above, a DNS zone can be created on the internal interface of the firewall which hosts the DNS records for the internal network. Clients on the internal network specify the internal interface of the firewall server as their preferred DNS server. If the DNS name resolution request is for a resource on the Internet, the firewall forwards the DNS request to a DNS forwarder. The forwarder is usually a DNS server at the ISP and is specified in the DNS properties on the firewall. In addition, while the Internal DNS service can forward queries to the Internet, the external DNS service cannot query the DNS service on the internal interface or any other server on the internal network.

Borderware Servers Vs Proxies

Note: In Borderware terminology, a Server is enabled on a particular interface, e.g. the WWW server running on the internal interface of the firewall would allow users on the protected network to access the web server running on the firewall. Similarly, the DNS server on the SSN would allow SSN hosts to query the Firewall Server's DNS database (which may forward the query to another DNS server).

On the other hand, a Proxy, allows a particular type of traffic to pass through the firewall from, say, the internal network to the external e.g. the WWW proxy enabled as "internal-to-external" would allow an internal host to send a HTTP request directly to the Internet and would allow the reply to pass back to the requesting host. While the proxy allows the internal host to specify the destination host on the Internet, this request is still "proxied" and - to the destination host - will appear to originate from the external interface of the firewall.

The term "Services" will be used to refer generically to either Borderware Servers or Proxies.

Borderware 6.5 Security Architecture

The firewall runs on Intel-based computers or is available as a dedicated appliance¹¹. In the case of the Intel based installation – which is how **CFG** runs Borderware – the product installs as the only software on the computer and runs on Borderware's S-Core¹² technology which is based on a modified and hardened installation of FreeBSD Unix. All direct access to the operating system is disabled and each critical security subsystem functions in a separate domain of execution¹³. The operating system does not permit any direct user logins and all the standard interfaces and features of BSD Unix such as shell access have been removed.

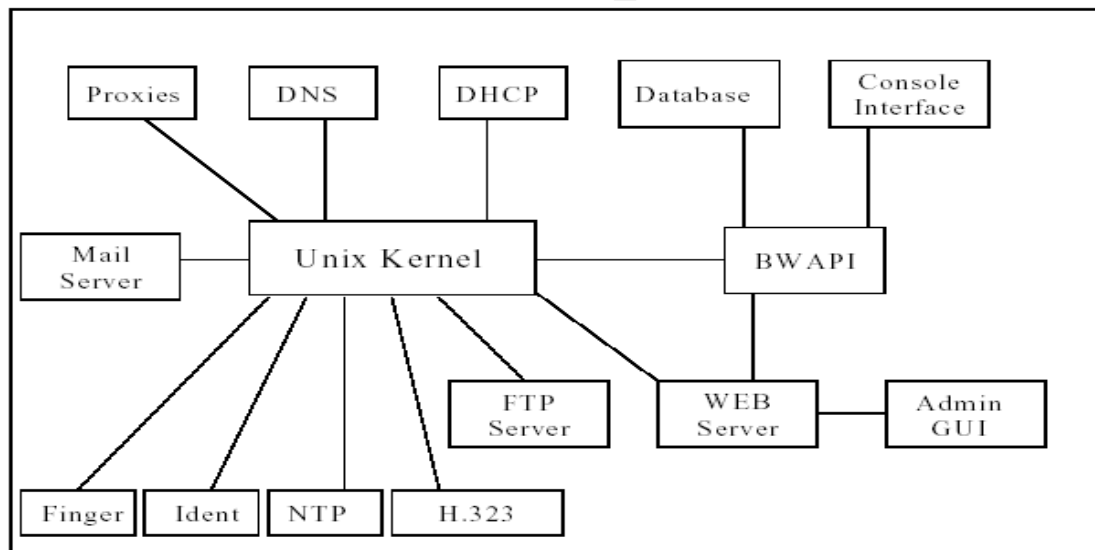
All configuration tasks are performed through the management interface via the firewall console or through the Windows-based Borderware Configuration Utility (BWClient.exe or **BWC**).

Borderware 6.5 Firewall Server provides the following services:

1. Packet Filtering
2. Application Level Gateway (inbound and outbound proxies)
3. Circuit Level Gateway
4. Network Address Translation
5. URL Filtering
6. SMTP Server
7. DNS Server
8. FTP Server
9. Squid Proxy Server
10. HTTP Filter

Figure 1 and Table 1 detail the high level subsystems and how they interact within the Borderware product. This information was taken from the Common Criteria evaluation report ^{(1) 14} completed by the UK government's Communications Electronic Security Group¹⁵. This report details the outcome of the IT security evaluation of Borderware Firewall Server 6.5 running on an Intel platform. The Common Criteria standards and scheme are discussed in more detail under **Certification and Accreditation** in **A.1.3**.

Fig. 1: Overview of Interaction between Borderware Firewall subsystems



¹ Communications Electronic Security Group (CESG),
UKITSec (CESG) Common Criteria Certification Report No. P164 , January 2002
<http://www.cesg.gov.uk/assurance/iacs/itsec/cpl/media/certreps/CRP164.pdf>

Table 1: Borderware Firewall Subsystems

| Subsystems | Description |
|--------------------------------|---|
| BWAPI | Handles requests for firewall management functions from the console interface and the remote Admin GUI (BWC). |
| UNIX Kernel | Provides the environment in which processes and subsystems execute. The process environment provides controlled access to files, the IP stack (which includes the packet filter that discards or redirects packets) and other processes. It is responsible for passing data between proxy and server subsystems and other hosts on the network. |
| Database | Provides a means of information storage and retrieval for other subsystems |
| System Console | Provides a user interface for the firewall administrator to configure and maintain the other subsystems. It is also known as the firewall console interface or simply the firewall console. |
| Admin GUI | Windows 95, 98, NT or Windows 2000 application that allows an administrator to manage the Borderware firewall server from a remote PC. |
| Proxies | Exchanges IP traffic between the firewall's network interfaces. |
| DHCP Client | Provides the firewall with its external IP address and its default route address if the customer does not own an IP address, and requests an IP address from the ISP via DHCP. At CFG , the external address is obtained from the ISP and assigned statically |
| DNS | Provides translation between Internet host names and addresses. It also provides other (PTR, MX etc.) resource records on hosts and domains |
| FTP Server | Provides a secure public file sharing system and allows an administrator to upload and download certain configurations to the firewall. |
| Web Server | Provides 2 distinct services, - access and hosting - on the firewall, i.e. there is a web server hosted on the firewall itself and there is the web proxy that allows clients to send HTTP requests to the Internet. CFG only implements the latter. |
| Email Server | Consists of a Simple Email Transfer Protocol (SMTP) email server and a Post Office Protocol (POP) email server. The SMTP server is used to provide a secure means of passing SMTP email from the Internet to the internal network, and it may be used as a default email gateway to pass email from the internal network to the Internet. The POP email server is used to provide access to user mailboxes held on the firewall. CFG does not utilize the POP email server |
| Finger Server | Implements the finger protocol and provides a static, configurable information message. The finger service does not provide any information about individual users |
| Ident Server | Allows the firewall to process requests for the identity of users on external networks. The firewall does not implement an Ident Client to identify itself or users on the internal network. |
| NTP Server & Client | Provides a reference timestamp to internal machines. The server enables the firewall to be the source of the timestamp; the client allows the firewall to synchronize its system clock with reference sources on the Internet. Currently NTP must be configured via the system console |
| H.323 Proxy | Allows internal users to employ H.323 type protocols such as Microsoft NetMeeting without revealing information about the internal network. This proxy is considered separate from the Proxy subsystem owing to its implementation |

Role of Firewall under audit

In order to audit the Borderware 6.5, it is necessary to look at the role that it plays in the larger network. The following information and diagrams are based on data provided by the network manager and the firewall administrator.

Firewall Server Platform

In the case of **CFG**'s network, the firewall server is installed on a dedicated Compaq Deskpro (Intel Processor) with hardware configuration specified in Table 2.

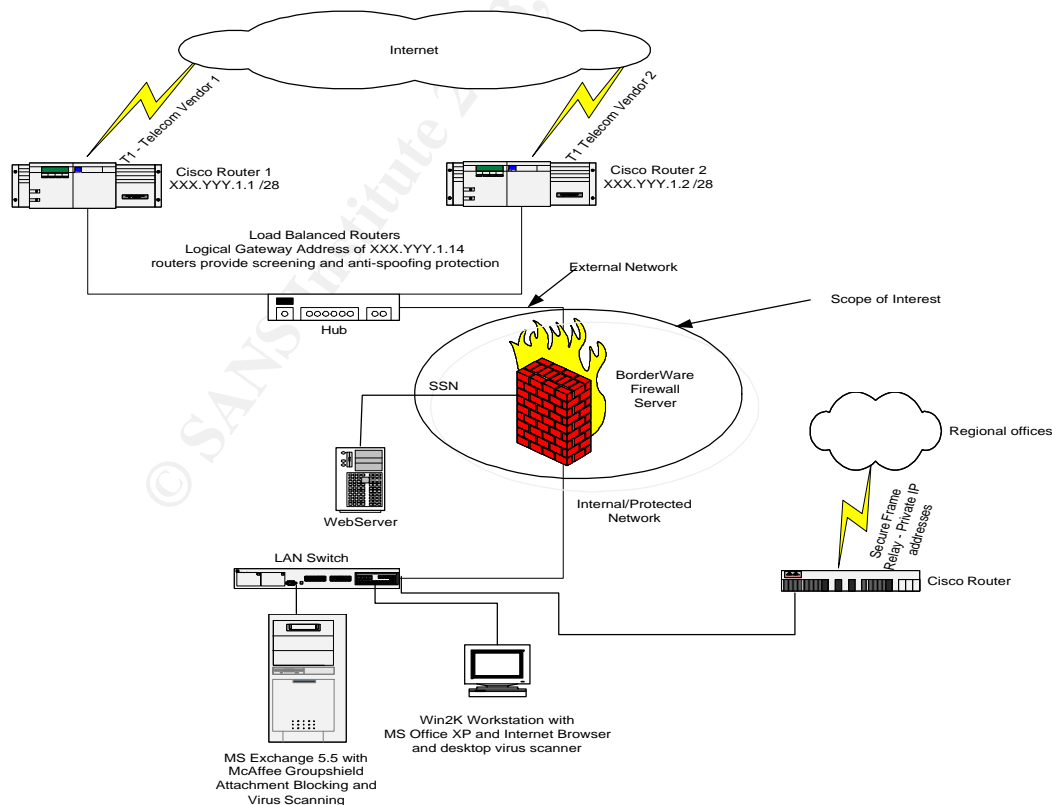
Table 2: Hardware configuration of firewall server

| | |
|-----------------------|--|
| Platform | Compaq Deskpro – Intel Processor |
| Ram | 256MB |
| HDD | 12GB – SCSI |
| Processor | 900Mhz |
| Network Configuration | 3Com 905C 10/100 Network Interface Cards x 3 Internal Interface 172.16.5.1/16 SSN Interface: 10.0.0.1/8 External Interface xxx.yyy.1.9/28 |

Physical Network

The Physical Network Configuration is shown in Figure 2:

Fig. 2: Physical Network Configuration

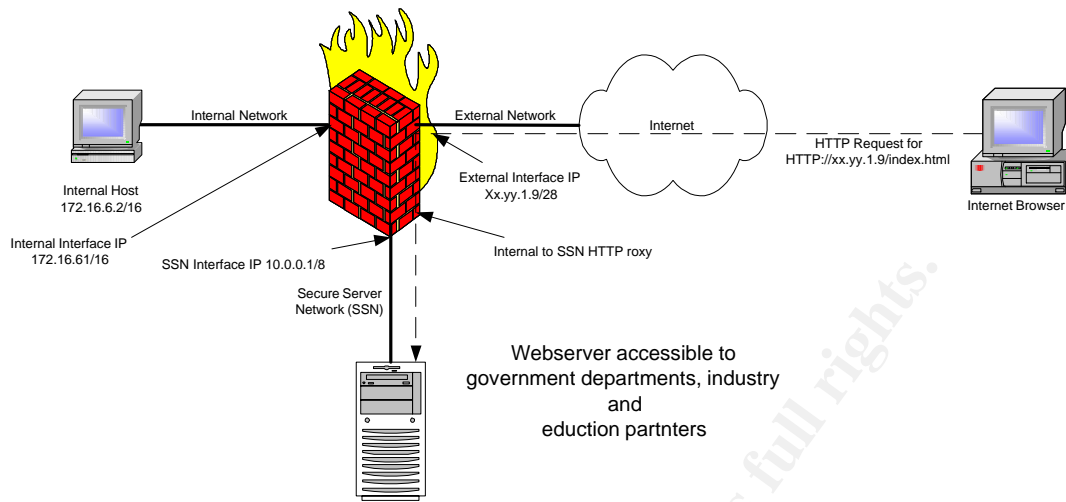


1. This firewall separates **CFG**'s network from the Internet. While the regional users access the Internet via this firewall, they connect to the HQ network via a secure router bypassing the firewall. All production servers are located on the local area network at HQ where a single flat VLAN structure is being used.
2. All users on the internal network are using private IP addressing in the 172.16.0.0/16 range. Regional office users are on the 192.168.x.0/24 subnets and route through the WAN to HQ network resources. The Firewall has a public IP address obtained from the ISP and it performs NAT¹⁶ by transparently mapping the source addresses of outbound connections. In this manner all outbound connections from the protected network appear to come from the firewall's external address.
3. The SSN is hosted off of the 3rd interface of the firewall and uses the 10.0.0.0/8 addressing scheme.
4. The screening routers (provided by the ISP) are outside the firewall. These routers provide load balancing and redundancy through *Hot Standby Routing Protocol* (HSRP). The firewall sees them as having one logical IP address which is specified as its default gateway IP address. Each router connects to a circuit provided by a different access carrier.

Logical Network and Information Flow

1. The firewall acts as **CFG**'s Internet gateway. All Internet requests from clients on the Internal are sent to the relevant (HTTP, FTP etc.) proxy on the firewall and all Internet downloads enter the network through it. The firewall is running Smartfilter¹⁷ URL filtering software which contains a database (automatically downloaded from the vendor) of URL's which may not be accessed from the corporate network.
2. The firewall acts as **CFG**'s email gateway; outgoing email is sent from the corporate email server to the SMTP server on the internal interface of the firewall. The firewall then forwards the email to the destination SMTP server. Incoming email arrives at the SMTP server on the firewall external interface and is sent to the corporate email server on the internal network.
3. Internal hosts are configured with the internal interface of the firewall as their DNS server. If the DNS request is for an Internet resource, the request is forwarded to the DNS server at the ISP. The firewall DNS server hosts the DNS zone for the internal network. If the request is for an internal resource, the DNS server on the internal interface provides resolution without referring to a forwarder. The external ISP also hosts the MX record for corporate email which points to the external interface of the firewall.
4. A single website is hosted on the SSN. This website hosts static HTML pages and is accessed by a number of government, industry and educational partners. This is illustrated in Figure 3. The security employed specifically on the web server is beyond the scope of this audit which is only concerned with the firewall access rules that allow this site to be viewed without compromising network security. Note that the web server in the SSN does not host **CFG**'s public website which is hosted at the ISP.

Fig. 3: Internet client accessing SSN web server through HTTP proxy on firewall



© SANS Institute 2003, Author retains full rights.

A.1.2 - Evaluation of Risk to the System

In order to create the audit checklist and procedures, it is necessary to determine the risks that face the firewall. Considering that the firewall is the single point of access to and from the network, any breach of the firewall security could allow an attacker access to the rest of the network. The security improvement practices section of the Carnegie Mellon Cert Co-ordination Center website¹⁸ states the following:

*“The most common cause of firewall security breaches is a misconfiguration of your firewall system you need to make thorough configuration testing (of the firewall system itself as well as the entire routing, packet filtering, and logging capabilities) one of your primary objectives”.*¹¹

In general terms, the risks associated with any Internet connected firewall can be classified as:

1. Denial of Service due to a (sustained) attack from the Internet or the internal network
2. Unauthorized access to data from internal or external host
3. Unauthorized use of resources by internal or external hosts
4. Reduced availability of the firewall due to any of the above or due to hardware or network failure

Table 3 shows the possible risks that exist for a firewall with interfaces on a protected network as well as the Internet. A risk assessment is an overall analysis of potential vulnerabilities and that may be the cause of loss or harm to the organization¹⁹. As is the case with any risk assessment it is necessary to look beyond the specific vulnerability or threat to evaluate the risk of it being exploited.

Additionally, it is important to note what a firewall cannot protect the network against. A firewall cannot prevent damage done by a network administrator who blatantly violates policy nor will a firewall provide protection against viruses or some Denial of Service (DOS) attacks. The former can only be addressed by employee education and the latter by implementation of compensating controls such as defense-in-depth strategies, virus scanners and screening routers.

¹¹ Carnegie Mellon Software Engineering Institute, CERT Co-ordination Center
Security Improvement Practices
Testing the Firewall System – Why this is important!, May 1, 2001
<http://www.cert.org/security-improvement/practices/p060.html>

Table 3: Risks associated with Internet connected firewalls

| Risk | Likelihood of Occurrence | Potential consequences |
|---|---------------------------------|--|
| 1. Internet attackers gain access to resources on the internal network. | High | <ul style="list-style-type: none"> • Security breach of internal network, servers and resources. • Theft of corporate information • Potential for sensitive data to be revealed to public or passed to malicious entities • Potential downtime if attack involves further malicious attacks on internal servers • Potential for complete loss of primary business function • Damage to reputation and loss of trust from partners and clients. |
| 2. Unnecessary services or proxies on the internal interface of the firewall | High | <ul style="list-style-type: none"> • May allow internal hosts to send unauthorized data to the Internet • Data revealed may be corporate information or may allow network configuration intelligence gathering by external entity leading to security breach, e.g. any network data that contains computer names or internal IP addressing information |
| 3. Unnecessary services or proxies configured on the external interface | High | <ul style="list-style-type: none"> • May allow traffic into the network that is not in accordance with business needs or security policy, e.g. a WWW proxy on the external interface may allow external access to Web servers on the internal network |
| 4. Misconfiguration of built in services allows Internet based attack, e.g. SMTP server | High | <ul style="list-style-type: none"> • If the Firewall allows email spamming through relaying email on its external interface there could be damage to CFG's reputation as its Internet address would be seen as the source of Internet Spam email • Increased potential for DOS attacks from Internet if massive amounts of email are relayed through the external interface |
| 5. Failure to address a known vulnerability allows unauthorized access to firewall or network | High | <ul style="list-style-type: none"> • Possible compromise of data or rules on firewall, or network hosts on internal network • Possible vulnerability to DOS attack |
| 6. Unregulated/unauthorized physical access from internal network | High | <ul style="list-style-type: none"> • Misconfiguration of firewall leading to security breach and/or exposure of corporate and/or network information |
| 7. Unregulated/unauthorized Remote Management access from internal network | High | <ul style="list-style-type: none"> • Misconfiguration of firewall leading to security breach and/or exposure of corporate and/or network information |
| 8. Unregulated/unauthorized Remote Management access from Internet | High | <ul style="list-style-type: none"> • Allow malicious Internet user to access firewall configuration or to "hijack" legitimate session being conducted remotely by system administrator |
| 9. Exposure of firewall to a denial of service attack | High | <ul style="list-style-type: none"> • Loss of primary source of information (Internet and email) and inability to |

| | | |
|---|--------|---|
| from the Internet | | <ul style="list-style-type: none"> communicate with partners. Loss of primary business function, i.e. dissemination of information via email |
| 10. "Backdoor" connections e.g. a system on the protected network has a secondary connection to the Internet via a modem or 3 rd party ISP | High | <ul style="list-style-type: none"> The unauthorized connection will not receive any protection from the firewall and may be a subject of an Internet attack which effectively bypasses the firewall |
| 11. Failure to log firewall events including failure to set alarms, review and retain logs | Medium | <ul style="list-style-type: none"> Administrators may miss trends leading up to full scale Internet based attacks There will be no forensic evidence available in the event of legal action pursued after a security breach |
| 12. Hardware failure | Medium | <ul style="list-style-type: none"> Loss of primary source of information (Internet and email) and inability to communicate with partners. Loss of primary business function, i.e. dissemination of information via email |
| 13. Failure of URL filtering software | Medium | <ul style="list-style-type: none"> Users exposed to inappropriate content on websites. Possible exposure to malicious code. Users denied access to legitimate web content. |
| 14. Inability to recover from any of the above e.g. communications breakdown, no documented procedure, no failover firewall etc. | Medium | <ul style="list-style-type: none"> Damage to reputation |
| 15. Network Failure beyond immediate control e.g. ISP or network carrier | Low | <ul style="list-style-type: none"> Loss of primary source of information (Internet and email) and inability to communicate with partners. Loss of primary business function i.e. dissemination of information via email |

© SANS Institute 2003, Author retains full rights.

A.1.3- Current State of Practice

A number of sources were researched in evaluating the current state of practice for both managing and auditing firewalls. While initial research was conducted at firewall vendors' websites, the bulk was performed through a variety of non-vendor specific Internet and text resources. A general firewall management "best practices" document was derived. Further research was used to examine the current state of auditing practices for firewalls.

Firewall Vendor Information

A firewall is a critical part of any network. A firewall allows users to access resources on both the protected internal network and the Internet. Vendors such as Checkpoint (Firewall-1)²⁰, Cisco (PIX)²¹ and Symantec (Enterprise Firewall)²² claim that their firewall is the best product for the job, combining simplicity of configuration with maximum security and minimum overhead. The Borderware Corporation is no exception with its website highlighting the same features of maximum security, minimal overhead and ease of configuration²³.

*"The **BorderWare Firewall Server** is a comprehensive integrated solution for securing your Internet connection. Built on a hardened operating system, it eliminates vulnerabilities and costs associated with a separate firewall and operating system. The strong defaults and intelligent user interface protects against misconfiguration - a common source of vulnerability - at the same time as providing maximum flexibility for satisfying local requirements. The Borderware Firewall Server offers an integrated, robust and easy to use secure Internet gateway, and provides an ideal solution for both controlling and leveraging Internet access to information, application and systems."*^{III}

Certification and Accreditation

Borderware's website highlights its firewall's acceptance within the security community including accreditation by Canada's Communications Security Establishment [²⁴ ²⁵]. This certification ensures that Canadian government agencies will be more likely to purchase this product since it has received a stamp of approval from Canada's main government accreditation body.

Borderware 6.5 has also received the EAL 4²⁶ assurance level certification from the Common Criteria body [²⁷ ²⁸]. Borderware dedicates a section of its website²⁹ to answering questions on the value of EAL assurance levels and what certification means for the Borderware product.

The Common Criteria is directed and endorsed by the governments of Canada, US, UK, France, Germany and Holland³⁰. This standard is designed to be used as a common basis

^{III} Borderware 6.5 Firewall Server website home page
[Http://www.borderware.com/newsite/products/fw/fwserver.html](http://www.borderware.com/newsite/products/fw/fwserver.html)

for evaluation of IT systems' security properties. The Common Criteria group is made up of the following agencies³¹:

1. Communications Security Establishment (CSE) - Canada
2. Service Central de la Sécurité des Systèmes d'Information (SCSSI) - France
3. Bundesamt für Sicherheit in der Informationstechnik (BSI) - Germany
4. Netherlands National Communications Security Agency (NLNCSA)– Netherlands
5. Communications-Electronics Security Group (CESG)– United Kingdom
6. National Institute of Standards and Technology (NIST) – USA
7. National Security Agency (NSA) - USA

Firewall Best Practices

In the paper “Firewall Management and Internet Attacks”, Lowder³² details the benefits of having a firewall. He says that firewalls provide the ability to enforce network standards and policies and to centralize network audit capabilities. His essay provides a set of standards that can be used to develop a comprehensive firewall policy.

The following Internet connected firewalls “best practices” list for was compiled from a number of Internet and text resources [^{33 34 35 36}]. It is meant to be a general best practices list and may or may not be directly relevant to every type of firewall. This list was used in formulating the checklist in **A.2.2**.

Table 4: Firewall Best Practices Guide

| |
|--|
| 1. Use the corporate policy to build the firewall policy and rules, and frequently audit the firewall to ensure that is consistent with this policy. |
| 2. Implement detailed and documented change management processes to ensure all changes to firewall configuration are needed, are performed properly and produce the expected results. |
| 3. Document the firewall configuration (change management should ensure that the document is updated every time the configuration is changed). This will facilitate a timely return to operations in the event of an outage. |
| 4. Perform regular vulnerability assessments to determine vulnerabilities which should be addressed in accordance with industry best practices. In fact, these assessments should be performed to ensure that the number of open ports is kept to a minimum. As a general rule the more open ports there are on a firewall external interface, the more avenues of attack exist for a would-be hacker. |
| 5. Obtain the support of senior management for “political” configuration such as URL filtering or blocking of potentially malicious code such as Java. |
| 6. Determine what servers, proxies and packet filtering rules should be enabled on the internal, external and SSN interfaces. Deny everything by default and then enable only what is necessary to meet business requirements. It is important to note that Borderware 6.5 Firewall Server in its default configuration will allow no traffic to pass between networks. |
| 7. When enabling these services do not confuse inbound and outbound rules, e.g. enabling a POP proxy as external-to-internal would allow users to download POP email from the Internet but allows Internet hosts to access POP servers on the internal network. |
| 8. Understand every rule on the firewall. If the firewall has been “inherited” from a previous administrator, and if a rule (or server or proxy) seems unnecessary, disable it and observe the results. This may be a politically sensitive move but it may well catch an unnecessary and unused service that has potential to compromise the entire network. |
| 9. When enabling packet filtering rules, ensure that the filters are applied correctly, e.g. |

| |
|--|
| packets entering the network must have a destination address of the internal network but a source address of a different network. This also applies to packets leaving the network which must have a source address on the internal network and a destination address on a different network. Additionally, packets entering the network should never have IP addresses on the reserved private range (10.0.0.0, 172.16.0.0., 192.168.0.0) |
| 10. When utilizing complex services that are built into the firewall such as SMTP, HTTP proxy or DNS ensure that the individual security configuration of these services is also addressed |
| 11. When implementing HTTP proxy servers, determine whether they should run transparently or if there is a need for authentication (and the method to be employed, e.g. LDAP, Radius, local authentication) as well as the need for caching on the firewall. |
| 12. Other tools should be used in conjunction with the firewall such as IDS, URL Filters, antivirus software, etc. A screening router outside the firewall, for example, will perform the bulk of the packet filtering tasks as well as anti-spoofing and Denial of Service attack mitigation. |
| 13. To reduce the processor and memory load on the firewall, implement content filtering, VPN, DHCP, authentication software, etc. on separate devices behind the firewall. |
| 14. Note that firewalls cannot prevent attacks that originate inside the network. Implement internal proxy servers with filtering capabilities, screening routers and up to date antivirus solutions to ensure Code-Red style attacks do not originate from inside your network. It may also be possible to implement HTTP filters to detect patterns associated with such attacks. |
| 15. Ensure that all patches from the vendor are complete and up-to-date. Ideally all patches should be tested on a non-production firewall before implementation. When applying patches, evaluate all new exploits carefully to determine if they apply to you, e.g. a new vulnerability relating to SSH in BSD Unix could definitely affect Borderware. However the same vulnerability affecting only Linux may not be of concern. |
| 16. Ensure that Firewall access (physical and network) is closely monitored to ensure that malicious or accidental changes to the configuration can be prevented and controlled. |
| 17. When implementing remote administration or management on the firewall, implement security such as encryption, user and IP address based access control lists and two-factor authentication. |
| 18. Change the administrator credentials from the default and use a complex (mixed-case, non-alphanumeric etc.) password scheme. If possible run the firewall service as a unique user ID instead of as root. |
| 19. Ensure that the firewall is tolerant to failure by implementing redundancy and load balancing (automated failover to an offline system) and battery backup in the event of a power failure. |
| 20. Determine any points in your network that allow traffic to bypass the firewall e.g. remote users dialing up to the network. Determine if these are necessary and if so implement compensating controls. |
| 21. Implement firewall logging and take time to review the logs. They will provide a wealth of forensic data indicating intelligence gathering scans that indicate potential attacks. Ideally the logs will be configured to provide automated alerting when a particular threshold is reached, e.g. a predefined number of a particular type of scan in a given time frame sends and email to the system administrator. Determine who needs to be notified (and who their backup is). Treat the firewall logs as business data and back them up in accordance with the corporate backup policy. |
| 22. Implement a secure remote logging server to make log manipulation more difficult for a would-be hacker. This will prevent any attempt to cover tracks after a successful hack attempt. |

Perhaps the most important point of all is to ensure that the firewall configuration is as simple as possible to avoid confusion.³⁷

Firewall Auditing Practices

There is a host of information available on generic auditing techniques for firewalls. Lance Spitzner, in his paper “Auditing Your Firewall Setup”³⁸, states the importance of setting expectations. This is done through a well defined and detailed policy. It is impossible for a firewall administrator to configure a firewall that balances business needs with security without having a documented policy. When auditing a firewall, the auditor must review the corporate policy and use this to determine the firewall’s performing. While comparisons to industry best practices are very important, business needs must be met. If meeting business needs introduces a security issue then a compensating control must be applied.

Under his Audit Methodology, Spitzner states that once the firewall is physically secure, all interfaces must be scanned to determine open ports. Once open ports have been determined, the integrity of the firewall rules must be established. The rules should allow and deny the traffic that is expected. Implementing port and vulnerability scans from each network segment will determine if the rules governing traffic flow between the segments are performing correctly.

Alan Oliphant provides a comprehensive auditing checklist in his white paper published on the website of The Institute of Internal auditors³⁹. In the same location, Sandy Lindstedt⁴⁰ steps through the audit process referencing a generic firewall audit. While this paper does not present a comprehensive checklist, it does provide an overview of the areas of concern conducting a firewall audit. Other firewall auditing checklists were found at the AuditNet website. It contains documentation, best practices and firewall audit checklists including a generic firewall audit checklist document by Diane Rochette⁴¹.

Research data discussed in the preceding section was used to compile the checklists used in the audit.

© SANS Institute 2003. All rights reserved.

A.1.4- Improvements on the current state of Practice

There is wealth of general information available on firewall management, best practices and auditing. However, I was not able to find any audit checklist and best practices that referred specifically to the Borderware Firewall Server 6.5. In conversation with the Borderware Technical Support desk^{IV}, I was informed that the closest such document was the information on the Borderware Website relating to the EAL 4 assurance levels from the Common Criteria program [Ref 29]. I was also referred to “Common Criteria Report No. P164” [Ref. 14] which documents CESG’s [Ref. 15] (formerly UKITSec) Common Criteria evaluation process for Borderware 6.5 as well as the Security Target Documentation prepared by Borderware [Refs. 2,3,6,13]. The Borderware reference guide [Refs. 1,4,5,8,10,11,12,16,30,36] also offered some basic practices.

In researching the Borderware firewall prior to performing an audit, it was determined that any firewall audit must include the following:

1. Review corporate policy and determine if the firewall meets its needs
2. Review and test the firewall device itself including services running on the firewall
3. Review and test the rule base and filters
4. Review and test the physical access controls
5. Review and test network access controls
6. Review and test the operation of the built-in servers such as HTTP proxy, DNS server, SMTP server, HTTP filters and URL filtering software
7. Review change management procedures
8. Verify whether additional connections to network exist
9. If the firewall is in accordance with the corporate policy, it is important to assess the policy to ensure that its criteria are synonymous with industry best practices.

In addition, the overall firewall architecture relative to hubs, dial-up solutions and other access points to the network must be considered. This document will take available firewall information and present it in a comprehensive audit methodology. It will include a checklist relating the Borderware product to the specific installation at *CFG*. Also included will be recommendations to ensure that *CFG* is getting the most out of its firewall solution in terms of adherence to security best practices while meeting their business needs.

^{IV} 1-877-814-7900, Canadian Technical Support line for Borderware Products

Assignment 2 - Creating the Audit Checklist

A.2.1- Policy Documents

In addition to the best practices discussed in A.1.3, the Firewall IT security policies at *CFG*. These will define expectations in terms of performance of the firewall and its ability to meet the business needs of *CFG*. The policy documents referenced in this report were created by *CFG*'s corporate policy department and had associated procedures that were used to determine the firewall policy and rulebase.

The following policy statements exist in relation to the firewall and Internet access:

Corporate Security Policy

“In terms of network services available to users, throughout *CFG*'s policy document, it shall be assumed that that which is not expressly allowed by the policy must be assumed as denied. All data on *CFG*'s protected network must be treated as corporate information and must be secured and protected as such. IT must take steps to prevent unauthorized access to the network.”

Internet Access Policy

“All *CFG*'s personnel must have access to the Internet resources necessary to carry out their job function. This should involve minimal configuration of the client's Internet browser. While it is not required that users provide authentication to access the Internet, access to racist, sexist, anarchist, violent or otherwise inappropriate websites is not allowed and IT shall implement filters to ensure that these sites are blocked as much as possible. IT must ensure that Internet access is available at all times unless a previous maintenance window has been agreed upon.”

Email Policy

“Users may only access or send email using the corporate email system. All email received must come through the email gateway on the firewall and the corporate email server.”

Firewall definition

The following firewall definition exists in the corporate policies and procedures documentation:

1. The firewall separates the protected network and SSN from the Internet and all traffic between these networks passes through it. It provides a level of security for the *CFG* production systems and ensures that only desired traffic passes through the firewall. In addition, unless *CFG* business needs specially warrant that a service be available it is blocked by the firewall.
2. The firewall allows all users who have logged on to the network to access Internet web pages and download data from Internet servers. This is seamless for users and requires minimal configuration at each user's workstations. The firewall ensures that the security of the network is not compromised while allowing this.

3. The firewall allows users to send and receive Internet email (to and from **CFG.com** address only).
4. The firewall blocks access to inappropriate sites e.g. sexually explicit, anarchist, racist, etc.
5. The firewall can only be managed by authorized personnel (both at the console and from Remote Management workstations)
6. All reasonable steps have been implemented to secure the external interface of the firewall while allowing legitimate services to pass through. The firewall external interface is obscured - for services other than those specifically allowed - to deter potential attackers.
7. The firewall facilitates access from the Internet and internal network to the static web pages in the SSN for a controlled and limited list of government departments as well as specific industry and education partners.
8. The firewall does not allow access to the protected network from the SSN; this is to ensure that in the event of a compromise of the SSN host, access to the protected network will still not be possible.
9. The firewall implements appropriate measures to ensure that an audit trail exists. This would be used in the event of an investigation or forensic analysis.
10. The firewall has the ability to alert the relevant personnel in the event of an attempted security breach.

Firewall Policy

Based on the above corporate policy documents and firewall definition, the following firewall policy exists:

1. The firewall performs Network Address Translation (NAT) ensuring that all traffic leaving the **CFG** protected network appears to originate from the Internet interface of the firewall. All incoming traffic to the **CFG** protected network is directed to the Internet interface of the firewall. Internal hosts use private addressing (172.16.0.0/16 for HQ and 192.168.x.0 in the regional offices). Hosts on the SSN use private IP addressing in the (10.0.0.0/8) range.
2. The Firewall accepts DNS requests for internal and Internet host name resolution from internal network clients and either respond with resolution (for internal hosts) or forwards the request to the ISP's DNS servers. The internal hostnames are not resolvable by hosts outside the firewall.
3. The HTTP application proxy allows users to access Internet content without exposing local systems. It is configured to act in transparent mode (users do not have to authenticate and their browsers will not have to be configured). From the Internet, all HTTP requests appear to come from Internet interface of firewall and all responses are directed to same interface.
4. The FTP application proxy allows users to access Internet FTP content without exposing local systems. All FTP requests appear to come from the Internet interface of the firewall and all responses are directed to same interface.
5. The SMTP service on the firewall acts as the email gateway for the **CFG** network. Outbound email from the corporate server is forwarded to the SMTP server on the firewall. This in turn forwards the email to the destination SMTP server. Inbound

email arrives at the SMTP gateway on the firewall and is forwarded to the corporate email server by firewall. MX records for corporate email are hosted at the ISP and point to the external interface of firewall. The SMTP proxy is not enabled.

6. Incoming HTTP traffic is allowed to access the static web pages on the server in the SSN. These pages are available to a limited number of government, industry and education partners. This list is controlled by implementing an external-to-SSN HTTP proxy utilizing IP address based ACLs. The pages are also be accessible to users on the internal/protected network.
7. The SSN interface permits only HTTP and ICMP replies from the SSN web server to enter the protected network. All services on the SSN interface are disabled.
8. Secure Remote Management is enabled on only the firewall internal interface.
9. ICMP is enabled on the internal interface of the firewall to facilitate connectivity troubleshooting but is not be enabled on the SSN and external interfaces
10. ICMP is enabled as a proxy (internal-to-external and internal-to-SSN) to facilitate troubleshooting when connecting to the Internet or SSN hosts.
11. The firewall logs are reviewed daily. They are configured to raise alarms when attack patterns are detected. These alarms send emails to the administrators' mailboxes. The logs will be backed up with all corporate data and will be stored on a remote logging server.

© SANS Institute 2003, Author retains full rights.

A.2.2- Audit checklist

Format of audit checklist

The audit checklist will contain the following and is divided into Control Objectives Groups (COG) as shown in Table 5.

1. Control objective (CO)
2. Risks associated with this objective
3. Methods for testing compliance

Table 5: Control Objective Groups

| | | |
|--------------|--------------------------------------|---|
| COG1: | Policy, procedures and documentation | Examines the documentation necessary to ensure that all personnel are clear on the policies and procedures to ensure business requirements are met by the firewall. |
| COG2: | Physical Access | Examines physical security of the firewall. |
| COG3: | Redundancy | Examines the firewall tolerance to electrical failure, hardware failure and network failure. |
| COG4: | “Backdoor” connections | Examines whether there are additional devices connecting the protected network to the Internet |
| COG5: | Built in Services | Examines the configuration of the built in engines for SMTP, DNS, NAT, HTTP Proxy and URL filter. |
| COG6: | Network Access | Examines the rules for enabling and securing Remote Management of the firewall. |
| COG7: | Firewall Management | Examines the patch levels and logging practices as well as Support Access settings for vendor troubleshooting |
| COG8: | Rule Base | Examines the servers and proxies enabled on all interfaces to determine how they conform to corporate policy and to industry best practices. |

Each firewall audit checklist item will have the format as shown in Table 6

Table 6: Control Objective checklist Sample

| | | | | |
|---|---------------------------------------|-------------------|------------|-------------------|
| CO.1# – Title of Control Objective | | | | |
| Reference: | | | | |
| Control Objective: | | | | |
| Risk: | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) | | | | |
| b) | | | | |
| Comments | | | | |
| Date: | Completed by: | Signature: | | |
| Note: | | | | |

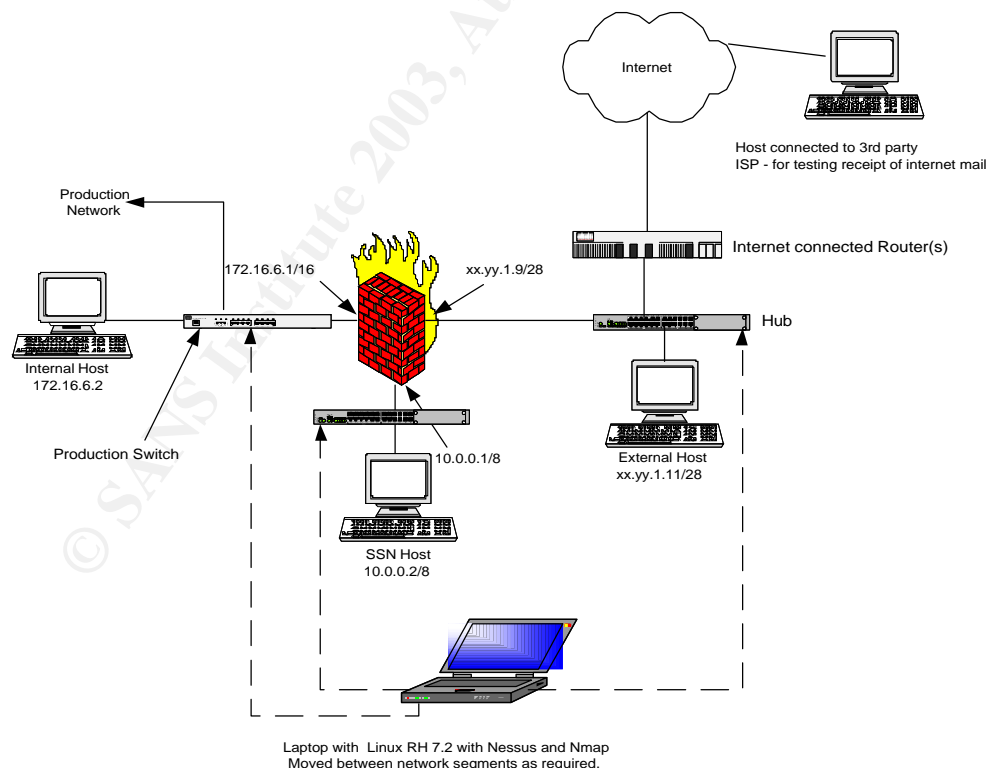
Notes on Control Objective Testing:

1. The method of testing will be **T** (Test), **I** (Interview), **O** (Observation) or **DR** (Document Review)
2. Each test will be listed as either **O** (Objective) or **S** (Subjective)
3. Some control objectives require a number of tests to determine compliance. Failure of any one of these tests will cause the entire control objective to be considered non-compliant.
4. If non-compliance for a particular test makes dependent tests invalid, the dependent tests will be listed as N/A. For example, if particular documentation is found to be non-existence, the document review test will be deemed invalid (N/A).
5. For any control objective that requires subjective testing (documentation review), the first test is generally listed as “Determine whether documentation exists”. The IT manager is responsible for all document management and this determination is generally made in the initial interview when he/she is asked to produce the documentation.

Testing Environment

For the purposes of testing, hosts are implemented on either side of the firewall. Details of the testing environment are discussed below. The test setup configuration is shown in Figure 4.

Fig. 4: Test Environment Setup



1. The internal host and SSN hosts are not actual production systems but are cloned images of these systems. These hosts have protocol analyzing software added to their configuration. This software detects patterns generated using vulnerability assessment tools. They also have BWC installed for the purpose of testing Remote Management capabilities and accessing the firewall configuration.
2. The external host is placed on the hub which connects the screening routers to the external network segment. Effectively, this means that the external host is between the firewall and the Internet screening routers. This system is used to simulate an Internet host. The external host also has protocol analyzing software and BWC installed.
3. The laptop is configured with vulnerability assessment and network scanning tools. These tools are used to scan each firewall interface (and network segment). The laptop is implemented to facilitate a mobile audit/attack host and its IP addressing is reconfigured as it is moved to each network segment.
4. All testing is performed on the actual production firewall with the firewall administrator accessing configuration and tasks that require **Root** privileges. All testing is performed outside of regular production hours during a scheduled maintenance window. For the sake of protecting the clients' identity, the screen shots provided are from an identically configured system with the names changed. In the case where any public IP address owned by **CFG** appears in the screen shot, it will be blanked out to protect the clients' privacy.
5. For the purposes of SMTP testing, a number of different mailboxes and email clients are used. Both the internal and external hosts run Microsoft Outlook Express 6.0 and the internal host is also running Microsoft Outlook XP.
 - a. The internal host's Microsoft Outlook XP application is used to access (and send email from) a mailbox on the corporate email server. In this capacity the system is referred to as the **corporate email client** and the mailbox is referred to as the **corporate mailbox**.
 - b. In the case of the internal host, Microsoft Outlook Express 6.0 is configured to specify the internal interface of the firewall as its SMTP server and is referred to as the **internal SMTP client**. The email account has a bogus domain name and does not have a legitimate POP email server
 - c. In the case of the external host, Microsoft Outlook Express 6.0 is configured to specify the external interface of the firewall its SMTP server, and is referred to as the **external SMTP client**. The email account has a bogus domain name and does not have a legitimate POP email server.
 - d. Email destined for the firewall is sent to postmaster@cfg.com. This is the default mailbox on the firewall.
 - e. It is also necessary to send email to and receive email from an Internet email address. The address stest20@hotmail.com is used as this address and is referred to as the **Internet Email Account**.
6. Any tests that involve accessing an Internet connected system (e.g. reading hotmail to verify receipt) are carried out on a separate stand-alone system connected to the Internet via DSL line from a commercial ISP

Table 7 lists the specific configuration of each system used in the test environment.

Table 7: Configuration of systems for testing

| | |
|----------------------|---|
| Internal Host | <ul style="list-style-type: none"> • Dell GX 240 running Windows 2000 Professional SP2 • Ethereal Protocol analyzer 0.9.7 (to detect incoming traffic patterns from assessment tools) • MS Office XP Suite SP1 (including MS Outlook XP) • MS Outlook Express 6.0 • MS Internet Explorer 6.0 – 128 encryption • MS Outlook XP is used to send email via the corporate email server (MS Exchange 5.5) simulating the internal production systems email clients • MS Outlook Express 6.0 used as an SMTP client in direct testing of the SMTP on firewall internal interface • IP Addressing <ul style="list-style-type: none"> ▪ IP: 172.16.6.11/16 ▪ Default gateway: Firewall internal interface ▪ DNS server: Firewall Internal address |
| External Host | <ul style="list-style-type: none"> • Dell GX 240 running Windows 2000 Professional SP2 • Ethereal Protocol analyzer 0.9.7 (to detect incoming traffic patterns from assessment tools) • MS Office XP Suite SP1 (including MS Outlook XP) • MS Outlook Express 6.0 • MS Internet Explorer 6.0 – 128 encryption • MS Outlook Express 6.0 is used as an SMTP client in direct testing of the SMTP on firewall external interface • IP Addressing <ul style="list-style-type: none"> ▪ IP: xxx.yyy.1.12/28 ▪ Default gateway: xxx.yyy.1.14 ▪ DNS server: ISP DNS server |
| SSN Host | <ul style="list-style-type: none"> • Dell Poweredge 2550 running Windows 2000 Server SP2 • IIS 5.0 • Ethereal Protocol analyzer 0.9.7 (to detect incoming traffic patterns from assessment tools) • MS Outlook Express 6.0 • MS Internet Explorer 6.0 – 128 encryption • IP Addressing <ul style="list-style-type: none"> ▪ IP: 10.0.0.2/8 ▪ Default gateway: Firewall SSN interface ▪ DNS server: Firewall SSN address |
| Laptop | <ul style="list-style-type: none"> • Compaq Evo N6000c running Linux Red Hat 7.2 <ul style="list-style-type: none"> ▪ Nessus vulnerability scanner for Linux V 1.2.5. ▪ Nmap port scanner for Linux V 2.54 ▪ The main purpose of the laptop is to provide a system that can easily be moved around in the test environment. ▪ The laptop also runs as the Nessus server required on the network. ▪ The IP address scheme of laptop varies depending on the segment to which it is connected. It follows that for the SSN, Internal and External hosts (respectively) but the last octet of the Laptop IP address will be one digit higher than the other host on the segment (e.g. when the laptop is on the SSN, its address will be 10.0.0.3) |

Tools used in audit testing

The following tools are to be used in the course of the audit:

Nessus⁴² is a free open-source remote security scanner that can be used to audit a host or network segment to determine whether any vulnerability exists. Nessus runs on *nix based systems (Linux, Unix etc.). It can be downloaded at <http://www.nessus.org/posix.html>. There is also a Win32 version of Nessus (Nessuswx) which runs as a vulnerability assessment tool on a Windows based client. Nessuswx requires a Nessus server running on Linux for authentication. It can be downloaded at <http://www.nessus.org/win32.html>.

Nmap⁴³ is an open source utility for mapping open ports and available services on a given host or range of hosts on a subnet. Like Nessus, Nmap runs on both Linux and Windows systems. Both versions can be downloaded at http://www.insecure.org/nmap/nmap_download.html.

Ethereal 0.9.7⁴⁴ is a freeware network protocol analyzer that can capture and examine network packets. It can be downloaded at <http://www.ethereal.com/distribution/win32/>

All examination of - and changes to - the firewall configuration will be carried out through either the **Firewall Console** or **BWC**. Unless a step specifically states that the item must be examined or configured using the Firewall Console, it is assumed that BWC is the tool that is used.

© SANS Institute 2003, All rights reserved.

Control Objectives Group 1 - Policies Procedures and Documentation

| CO.1 – Corporate Policy on Firewall and Internet access | | | | |
|--|--|--------|------------|------------|
| Reference: Lowder [Ref. 35] and Spitzner [Ref. 38] | | | | |
| Control Objective: To determine the existence of documentation stating corporate policy for Internet and email access. | | | | |
| Risk: Without a corporate policy stating the definition and role of the firewall, administrators will not understand business needs and expectations and will have no guidelines to follow in creation of firewall rules. Ultimately there will be no control over the traffic that enters and leaves the network. There will also be no accountability if business needs are not met due to firewall configuration or if a security breach occurs through the firewall. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Determine whether policy documentation exists | Document exists | I/DR | S | |
| b) Review documentation to determine if it states expectations to be met by firewall | Documentation clearly states business expectations (services allowed) and restrictions (services denied) to be met by firewall | DR | S | |
| c) Determine the firewall administrators level of awareness regarding this documentation | The firewall administrator is aware of document's existence and location | I | S | |
| d) Determine the perceived level of compliance between firewall rules and policy documents and the firewall administrator's understanding of the policy | The firewall administrator states that he is able to equate all firewall rules to policy document stipulations | I | S | |
| Date: | Completed by: | | Signature: | |
| Note: | | | | |

| | | | | |
|--|--|-------------------|------------|-------------------|
| CO.1.2 - Firewall Installation and Configuration Procedures | | | | |
| Reference: COBIT ⁴⁵ | | | | |
| Control Objective: To determine whether, documentation exists detailing installation and configuration steps for the firewall | | | | |
| Risk: In the event of a permanent failure of the firewall, the IT staff must be able to rebuild it on a different computer. Without detailed installation and configuration steps, rebuilding the firewall in a crisis will be more difficult - if not impossible – and the rebuilt firewall will be more likely to deviate from the trusted secure installation. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Determine existence of documentation | Documentation exists | I/DR | O | |
| b) Review Installation steps | Documentation clearly details steps involved in installing Borderware 6.5 from CD or network share | DR | S | |
| c) Review configuration steps | Documentation clearly details all firewall configuration settings necessary to meet CFG's business needs and restrictions | DR | S | |
| d) Review change management references | Documentation references the change management procedures to ensure that the configuration steps are updated every time a change is made on the firewall | DR | S | |
| e) Interview the firewall administrator to determine level of awareness | Administrator is aware of document's existence and location | I | S | |
| Date: | Completed by: | Signature: | | |
| Note: | | | | |

| CO.1.3 - Firewall Backup and Restoration Procedures | | | | |
|---|--|---------------|-------------------|-------------------|
| Reference: COBIT ⁴⁶ | | | | |
| Control Objective: To determine whether documented procedures exist for backup and restoration of the firewall configuration. | | | | |
| Risk: If backups of firewall configuration are not obtained, it will be very difficult to ensure that all rules in place are restored after a hardware failure | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Determine existence of documentation | Document Exists | I/DR | O | |
| b) Review Backup and Restore procedures | Documentation clearly states the requirements and steps for backing up and restoring the firewall configuration as well as the frequency of trial restores | DR | S | |
| c) Interview the firewall administrator to determine level of awareness | Administrator is aware of document's existence and location | I | S | |
| d) Interview the firewall administrator to determine level of agreement and compliance | Administrator agrees with and complies with the procedures in the documentation | I | S | |
| e) Interview the firewall administrator to determine if a backups track configurations changes | Administrator states that a backup is performed every time a change is made to the configuration of the firewall | I | S | |
| Date: | Completed by: | | Signature: | |
| Note: | | | | |

| CO.1.4 – Incident Response | | | | |
|---|---|--------|------------|------------|
| Reference: COBIT ⁴⁷ | | | | |
| Control Objective: To determine the existence of documented policies and procedures, contact lists and priorities relating to firewall related security incidents. | | | | |
| Risk: Without a documented Incident Handling policy and procedure, informatics staff will have no clear direction to follow in the event of a security related incident. Of major importance is the corporate stance on the risk associated with quick recovery in the event of a security breach which may terminate any ongoing network based attack. This may compromise evidence gathering for subsequent prosecution or action. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Determine existence of documentation | Documentation exists | I/DR | O | |
| b) Review Documentation to determine if key points are addressed | Documentation clearly states roles, responsibilities, contact lists and post incident review strategy | DR | S | |
| c) Interview administrator to determine the level of awareness of documentation | Administrator is aware of document's existence and location | I | S | |
| d) Interview administrator to determine the level of understanding of key points | Firewall administrator is clear on the incident response procedures, roles and responsibilities | I | S | |
| e) Interview administrator to determine the level of awareness of corporate priorities regarding incident handling | Firewall administrator is clear on the corporate priorities regarding recovery versus evidence gathering | I | S | |
| f) Interview helpdesk manager to determine the level of level of awareness among helpdesk staff regarding their incident response roles | Helpdesk manager states that helpdesk staff are clear on their role in incident response process, e.g. contacting on-call firewall administrator, etc | I | S | |
| Date: | Completed by: | | Signature: | |
| Note: | | | | |

| | | | | |
|---|---|---------------|-------------------|-------------------|
| CO.1.5 – URL Filter policy | | | | |
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether the method for determining acceptable and unacceptable websites is documented and can be justified to allay fears about “censorship” | | | | |
| Risk: User morale will be affected if there is a perception of censorship or strict enforcement of “corporate-use only” policies in Internet access | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Determine existence of documentation regarding acceptable and unacceptable website usage | Documentation exists | I/DR | O | |
| b) Review Documentation for definition of acceptable websites | Document clearly states what constitutes acceptable and unacceptable web sites | DR | S | |
| c) Review Documentation to determine process for false positives and negatives | Documentation includes steps to deal with false positives and/or false negatives e.g. manual edits to filter database etc | DR | S | |
| d) Interview firewall administrator to determine under what circumstances filter configuration will be edited | Database will be edited on user request subject to verification of site content (that site does not violate policy) in question | I | S | |
| e) Review documentation to determine if consistent process exists for manual edits of filter database | Documentation contains steps (including pre-screening) and process flow for manual editing of database | DR | S | |
| f) Interview sample user to determine level of understanding and acceptance among user community | Users will understand why filter is in place and find it acceptable | I | S | |
| Date: | Completed by: | | Signature: | |
| Note: | | | | |

| | | | | |
|--|---|---------------|-------------------|-------------------|
| CO.1.6 - Firewall administrators contact lists | | | | |
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether an up-to-date list of production and on-call firewall administrators is available to helpdesk personnel and IT managers | | | | |
| Risk: Without an up-to-date contact list of all available personnel with the skills and the authority to access the firewall, it will be impossible to access the necessary resources in a crisis | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Determine existence of documentation | A complete on-call schedule – with full contact details - for firewall administrators exists | DR/I | O | |
| b) Interview firewall administrators to verify contact details are correct and up to date | Firewall administrators agree that contact list details (phone number etc.) are correct and up to date | I | S | |
| c) Interview IT manager and helpdesk manager to determine level of awareness of contact list among helpdesk staff | IT manager and helpdesk manager agree that all IT personnel are aware of document's existence | I | S | |
| d) Interview IT manager to determine if someone (as well as a backup) has been assigned responsibility for list maintenance | IT manager has assigned the task of maintaining the contact list to a full time staff member and a backup | I | S | |
| Date: | Completed by: | | Signature: | |
| Note: | | | | |

| CO.1.7 - Change management Process | | | | |
|---|--|---------------|------------|-------------------|
| Reference: COBIT ⁴⁸ | | | | |
| Control Objective: To determine the existence of a documented change management process to ensure control and awareness of all changes to firewall setup and configuration | | | | |
| Risk: Without a documented change management process, there will be no control over the changes to firewall configuration. Changes will be made without proper justification, authorization or notification process. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Determine existence of documentation | A documented change management process exists | DR/I | O | |
| b) Review documentation to determine policy regarding change process | Documentation will cover process involved in making a change to configuration including who is authorized, who must be notified and who must provide final sign-off | I | S | |
| c) Review documentation to determine policy regarding justification of changes | Documentation will state policy on justification of changes, i.e. does the firewall administrator have to justify these changes to direct management? | DR | S | |
| d) Review documentation to determine policy regarding changes requested by users | Documentation will state process for user requests to change firewall configuration | DR | S | |
| e) Review documentation to determine backup strategy in change management | Documentation will address the fact that backups must be on hand when a change is made and a new backup must be performed once a change is deemed successful | DR | S | |
| f) Interview administrator to determine if backup guidelines from documentation are followed | Administrator will have a copy of the last good backup available when making a change to configuration. Once a change is deemed successful, a new backup will be made. | I | S | |
| g) Interview administrator to determine level of awareness of change management documentation | Administrator is aware of document's existence and location | I | S | |
| h) Interview administrator | Administrators agree | I | S | |

| | | | | |
|---|--|-------------------|--|--|
| to determine level of agreement and compliance with change management documentation | with and comply with the change management process | | | |
| Date: | Completed by: | Signature: | | |
| Note: | | | | |

© SANS Institute 2003, Author retains full rights.

Control Objectives Group 2 - Physical Access

| CO.2.1 - Access to firewall location | | | | |
|---|---|--------|------------|------------|
| Reference: Lowder ⁴⁹ | | | | |
| Control Objective: To determine whether the firewall location is physically secure and that only authorized personnel are allowed to enter the room. | | | | |
| Risk: Unauthorized personnel (or outsiders such as consultants) may be able to access the room and may attempt to logon to the firewall console and/or physically shutdown or disconnect cables/power supply from the firewall. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Interview IT manager and observe firewall location physical security | Access to the room will be secured by code protected lock, swipe card or security guard | O/I | O | |
| b) Observe as IT personnel other than firewall administrators attempt to access the locations | IT personnel will only have access to the firewall location if they are authorized to access the firewall | O | S | |
| c) Observe as non-IT personnel attempt to access the locations | Access will be denied to non-IT personnel | O | S | |
| d) Attempt access to the location (to verify entry restrictions for non-staff/ consultants) | Access will be denied to all non-staff onsite and outside consultants | O | S | |
| Date: | Completed by: | | Signature: | |
| Note: The IT manager must be informed of any attempts to breach security. It is recommended that, where feasible, no-one else in the IT department be informed in order to ensure the integrity of these tests. It may be necessary for the IT manager to enlist the support of a non-IT member of staff as well as the IT personnel necessary to perform these tests. | | | | |

| | | | | |
|--|--|-------------------|------------|-------------------|
| CO.2.2 - Access to Firewall console | | | | |
| Reference: Personal experience | | | | |
| Control Objective: To determine whether the firewall console password is unique and available only to firewall administrators. | | | | |
| Risk: People other than firewall administrators (other IT personnel, non-IT staff, contractors etc.) who do not have appropriate authorization may be able to gain access to the firewall through the console. This could lead to malicious or accidental misconfiguration of the firewall resulting in unavailable services or a security breach | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) To verify the password has been changed from the default, attempt to log in at the firewall console using the default password | The default password should not allow login | T | O | |
| b) Interview the firewall administrator to determine that the console password is unique and complex and is known only to firewall administrator | Firewall administrator states password is unique, complex and is not shared with IT personnel other than firewall administrators | I | S | |
| c) Ask the helpdesk manager to attempt access to the firewall using a standard system administration password | The standard system administration password should not allow login | O/I | O | |
| Date: | Completed by: | Signature: | | |
| Note: The IT manager must be informed of any attempts to breach security. It is recommended that, where feasible, no-one else in the IT department be informed in order to ensure the integrity of these tests. | | | | |

Control Objectives Group 3 - Redundancy

| | | | | |
|--|---|-------------------|------------|-------------------|
| CO.3.1 - Tolerance to electrical failure | | | | |
| Reference: COBIT ⁵⁰ | | | | |
| Control Objective: To determine whether the firewall is able to tolerate electrical shutdown or failure, and whether it shuts down gracefully when utility power fails. | | | | |
| Risk: If the firewall does not shutdown gracefully in event of power failure, there may be corruptions on the hard drive or packets being processed may be lost, e.g. email in the email gateway may not be forwarded, etc. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Examine the firewall physical configuration to determine if it is connected to a UPS | Firewall is connected to utility or building power supply via a UPS | O | O | |
| b) Under the supervision of the firewall administrator, at the firewall console, access the Configure UPS menu under the Misc. menu | UPS Monitor is enabled to ensure graceful shutdown | O | O | |
| c) Disconnect the firewall UPS from the utility power supply | UPS supplies battery power to the firewall | T | O | |
| d) Disconnect the firewall UPS from the utility power supply | Graceful shutdown initiates in time frame specified in UPS monitor | T | O | |
| Date: | Completed by: | Signature: | | |
| Note: Any testing which may cause a firewall outage should be coordinated with the firewall administrator and should be performed under the supervision of the Firewall administrator after business hours. | | | | |

CO.3.2 - Firewall Redundancy

Reference: Lowder⁵¹

Control Objective: To determine whether a failover system is implemented to ensure continued operations in the event of hardware or operating system failure of the firewall.

Risk: Without a failover system, the firewall will have to be rebuilt and reconfigured when it fails. If the firewall failure occurs after regular working hours there could be a significant delay before the new firewall is active.

| Test | Expected Result for Compliance | Method | O/S | Compliance |
|--|---|--------|-----|------------|
| a) At the firewall console access the HALO menu options | High Availability (HALO) clustering is enabled with at least one other firewall in the cluster | O | O | |
| b) If HALO is not configured, interview the firewall administrator to determine the existence of an offline backup firewall | Firewall administrator states that offline backup firewall exists | I | S | |
| c) If HALO is not configured, interview the firewall administrator to determine the existence of documentation detailing the procedure for manual failover to a the offline backup firewall | Documented process exists for manual failover to the offline backup firewall in the event of a failure of the production system | I | S | |
| d) If HALO is not configured, interview the firewall administrator to determine the existence of documentation detailing the procedure for ensuring the offline backup firewall is synchronized with the production system | Documented process exists for ensuring that the offline backup firewall configuration mirrors that of the production system | I | S | |
| e) Examine the offline backup firewall and compare the configuration to that of the production system | Offline backup firewall will have duplicate configuration of production firewall | O | O | |

Date:

Completed by:

Signature:

Note:

| CO.3.3 - Internet Connection Redundancy | | | | |
|---|--|--------|------------|------------|
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether a secondary connection exists from outside the firewall to the ISP | | | | |
| Risk: Without Internet access, the primary business function cannot be carried out. A redundant connection to the Internet (from the external interface of the firewall) will reduce the risk of outage. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Examine architecture documents and interview the network manager determine if there are redundant Internet connections outside the firewall | There are redundant connections from outside the firewall to separate network carriers | I/DR | O | |
| b) Examine architecture documents and interview the network manager to ensure that implementation of redundant Internet connections require no manual intervention on the part of the user or on the part of the Network team | Failover to redundant network carrier is automatic and transparent to users | I/DR | O | |
| c) Under the supervision of the network manager, disconnect one of the Internet connected routers from the hub outside the firewall and determine whether Internet connectivity is still available | It is still be possible to make connections to the Internet from the internal host | T | O | |
| Date: | Completed by: | | Signature: | |
| Note: In performing this test, it would be prudent to schedule it for after regular working hours. If there are multiple Internet connections providing redundant load balanced access to the Internet, it is possible that any load balancing is session-based as opposed to packet-based. This means that any download that has started on a given circuit will complete on that circuit. If this is interrupted that particular download will fail. However new connections can be initiated and they will use the remaining circuit. | | | | |

Control Objectives Group 4 - "Backdoor" Connections

| CO.4.1 - Additional connectivity between protected network and Internet | | | | |
|---|---|---------------|------------|-------------------|
| Reference: Lowder ⁵² | | | | |
| Control Objective: To determine whether the firewall is the single point of connection to the Internet from the protected network. | | | | |
| Risk: It will be impossible to control the volume and type of traffic entering and leaving the network if there is undocumented/unauthorized access points such as modems, other firewalls, systems connected to 3 rd party ISPs, or network drops patched directly to the hub outside the firewall. The firewall cannot protect against traffic that does not pass through it. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Examine architecture documents and interview network manager to determine if there are additional connections between the local protected network and the Internet | There are no connections from the local protected network other than through the firewall | DR/I | S | |
| b) Examine architecture documents and interview network manager to determine if there are additional connections to the Internet from any of the regional offices | There are no connections from the regional office networks other than through the firewall | DR/I | S | |
| c) Examine architecture documents and interview network manager to determine if there are additional connections from protected network systems to the Internet through a 3 rd party ISP | No internal network systems have Internet connections directly to a 3 rd party ISP | DR/I | S | |
| d) Examine architecture documents and interview network manager to determine if there are additional connections from standalone systems to the Internet through a 3 rd party ISP | No standalone systems have Internet connections directly to a 3 rd party ISP | DR/I | S | |
| e) If (d) is non-compliant, interview the network manager to ensure that there is a procedure to ensure that data transfer between systems is controlled and secure and that all data is scanned for viruses before being moved between systems | There are documented procedures and implemented measures to ensure that transfer of data between a stand-alone ISP system and the protected network systems is either expressly forbidden or controlled to ensure all data is free of viruses, etc. | DR/I | S | |

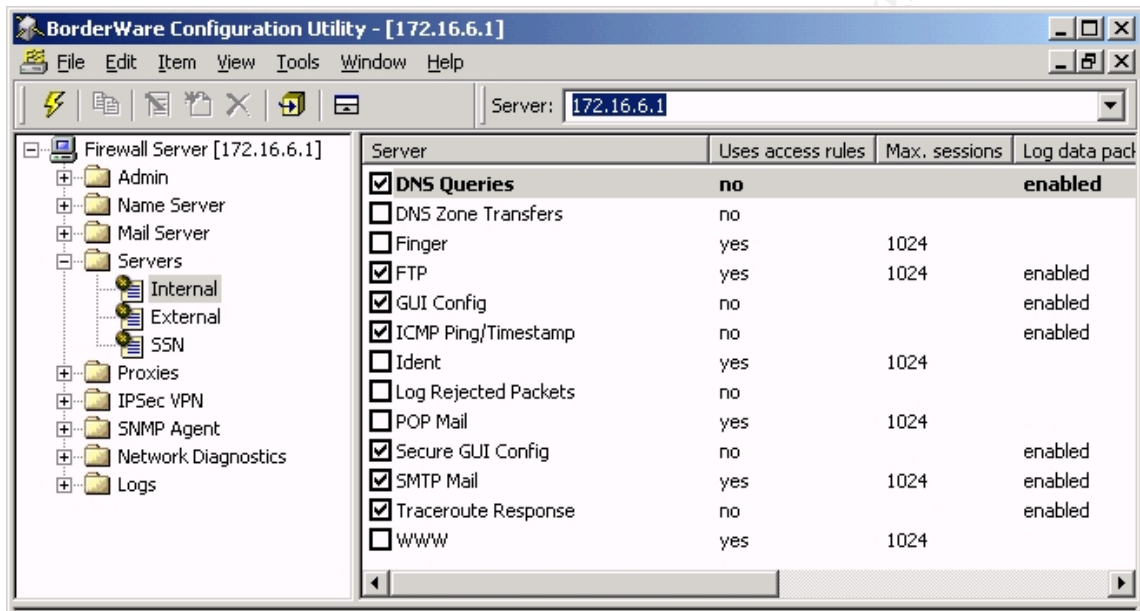
| | | | | | |
|---|--|---|------|-------------------|--|
| f) | Interview network manager and examine results of war-dialing conducted in the most recent overall network security audit to determine if there are modems on the network | There are no modems connected to computers on the internal network | DR/I | S | |
| g) | Conduct an NMAP scan of the entire external subnet range allotted to CFG to determine the devices with "live" Internet connections. | There should be no devices in the subnet range allotted to CFG other than the ISP screening routers and the firewall | T | O | |
| Date: | | Completed by: | | Signature: | |
| <p>Note: The purpose of this audit is to review the security of the Borderware 6.5 Firewall Server in its capacity as Internet and email gateway for CFG's network. The existence of any other Internet connected device will be considered a failing point for this section of the audit. However, if previous security studies have performed vulnerability assessments on these devices and determined they are secure from malicious attacks, this will be considered a compensating control.</p> | | | | | |
| <p>Nmap Syntax: Nmap xxx.yyy.1.0/28</p> | | | | | |

© SANS Institute 2003, Author retains full rights.

Control Objectives Group 5 - Configurable Services

In its simplest installation, Borderware allows services (proxies and/or servers) to be enabled/disabled by a simple check box for each service (See Figure 5). These will be referred to as Simple Proxies or Simple Servers. While access rules (packet filtering, time of day, etc.) can be used to further control these services, there is no detailed configuration available such as user authentication or settings relating specifically to the service offered.

Fig. 5: Simple Proxies and Servers access through BWC



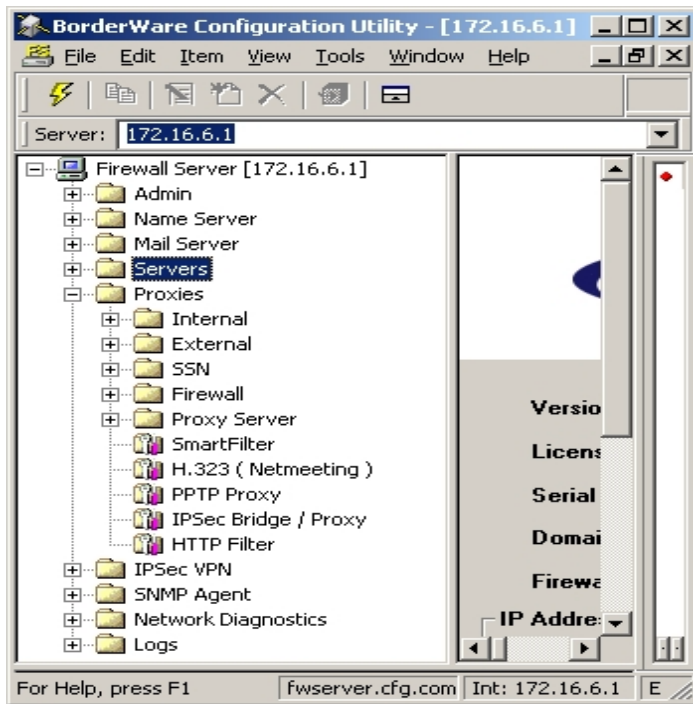
Borderware Firewall Server 6.5 has a number of services which can be configured as individual sub-systems running within the Firewall. While they can be enabled or disabled by the check boxes in the servers or proxies menus, they can be further configured through dedicated menus in BWC - or the firewall console - that allow more detailed control. These services will be audited in COG 5 and the simple services will be examined COG 8.

The following services allow for more detailed configuration

1. NAT (at install only)
2. Name Server (DNS)
3. Email Server (SMTP)
4. Proxy Server
5. Smart Filter (URL Filter)
6. H.323 (Netmeeting)
7. PPTP Proxy
8. IPSEC Bridge/Proxy
9. HTTP Filter
10. IPSEC VPN
11. SNMP Agent

Figure 6 shows the top-level firewall configuration menu with those services that allow more detailed configuration

Fig. 6: BWC Top level menus

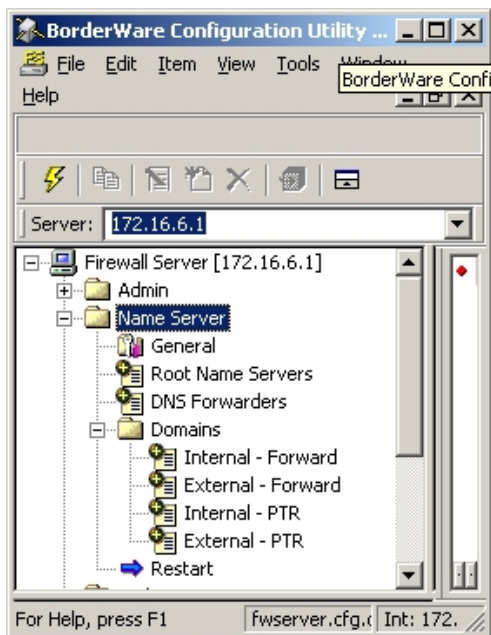


| CO.5.1 - Network Address Translation (NAT) | | | | |
|--|--|--------|------------|------------|
| Reference: Borderware Firewall Server Reference Guide [Ref. 16] | | | | |
| Control Objective: To determine whether the firewall employs Network Address Translation and that the internal and SSN interfaces use private IP addressing schemes. | | | | |
| Risk: If host addresses from the internal or SSN network are exposed directly to the Internet, the chance of a compromise of a host system is increased. The use of private IP addresses on the internal and SSN hosts ensures that they cannot be directly referenced or accessed from the Internet. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC select Admin to examine the configuration of the firewall interfaces | The SSN and protected interfaces are using private IP addressing schemes | O | O | |
| b) In BWC select Admin to examine the configuration of the firewall interfaces. | The external interface of the firewall uses a public IP address | O | O | |
| c) Make a connection (e.g. Ping) from the internal host to the external host. Ensure the external host is running the Ethereal protocol analyzer program and examine the packet capture. | In the packet capture, the source IP address of the ping request (and the destination address for the reply) is the external interface of the firewall | T | O | |
| d) Make an HTTP connection (http://xx.yy.1.9) from the external host to the external interface of the firewall. | HTTP connection is re-directed to the web pages on the SSN server. | T | O | |
| e) From the external host, attempt an HTTP connection (http://10.0.0.2) directly to the SSN web server. Ensure that Ethereal protocol analyzer is running on the SSN web server | This should not be possible as the firewall will not allow connections directly from the external network to resources in the SSN. | T | O | |
| f) Examine the results of the packet capture from (e) | The packet capture will display no packets from the external host | T | O | |
| Date: | Completed by: | | Signature: | |
| Note: | | | | |

| CO.5.2 - Name Server (DNS) | | | | |
|--|---|--------|-----|------------|
| Reference: Borderware Firewall Server Reference Guide ⁵³ | | | | |
| Control Objective: To determine whether the firewall DNS server provides internal and Internet host name resolution to only internal hosts | | | | |
| Risk: <ul style="list-style-type: none"> a) If the DNS server does not perform as expected, internal hosts will be unable to resolve Internet addresses. b) Corporate policy states that DNS resolution can only be performed by firewall. If the DNS proxy is enabled, clients will be able to specify DNS servers on the Internet for resolution. c) Hosts on the Internet must not be able to use the external DNS on the firewall to resolve DNS for internal hosts or for other Internet hosts. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC, click on Internal under Servers and examine the check boxes for each server | DNS Queries are enabled on the internal interface | O | O | |
| b) In BWC select DNS Forwarders under Name Server . (Fig 7 shows the top level DNS Name Server configuration menu.) | The IP address of the DNS forwarder is that of the ISP DNS server address as verified by the firewall administrator | O | O | |
| c) In BWC under Name Server select Domains and then select Internal-Forward | There is a domain hosted on the internal interface | O | O | |
| d) Use NSLOOKUP to resolve DNS for an Internet resource (www.yahoo.com) from the internal host using the internal interface of the firewall as the DNS server for the host | DNS resolution for an Internet host is possible | T | O | |
| e) Use NSLOOKUP to resolve DNS for an Internet resource (www.yahoo.com) from the internal host using the ISP's DNS server as the DNS server for the host | DNS resolution for an Internet host is <u>not</u> possible | T | O | |
| f) Use NSLOOKUP to resolve DNS for an internal host from an internal host using the internal interface of the firewall as the DNS server for the host | DNS resolution for an internal host is possible | T | O | |
| g) Use NSLOOKUP to resolve DNS for an internal host from the external host using the | DNS resolution for an internal host is <u>not</u> possible | T | O | |

| | | | | | |
|---|---------------|--|------------|---|--|
| external interface of the firewall as a DNS server. | | | | | |
| h) Use NSLOOKUP to resolve DNS for an Internet resource (www.yahoo.com) from the external host for using the external interface of the firewall as a DNS server | | DNS resolution for Internet hosts is <u>not</u> possible | T | O | |
| Date: | Completed by: | | Signature: | | |
| Notes: The Nslookup syntax is as follows: | | | | | |
| <ul style="list-style-type: none">• From the command prompt on the Windows 2000 system type nslookup• The default DNS server will be displayed. This can be changed by entering the following command at the ">" prompt: Server IP-address-of new DNS server• To resolve hostnames using this DNS server, type the hostname at the command prompt (>)• The application will return the DNS resolution for the queried host. If the DNS server that was queried is not authoritative for the zone where the queried records are located the application will state that returned data is a "non-authoritative answer" | | | | | |

Fig. 7: Top level Name Server Configuration Menu



| CO.5.3 - Email Server (SMTP) | | | | |
|--|---|--------|-----|------------|
| Reference: Borderware Firewall Server Reference Guide ⁵⁴ | | | | |
| Control Objective: To determine whether the firewall acts as the email gateway for the network relaying email between only the corporate email server and the Internet. | | | | |
| Risk: <ul style="list-style-type: none"> a) If the SMTP gateway does not perform as expected, email access to and from the Internet will be unavailable. b) If the corporate email server is able to specify an Internet SMTP gateway as its forwarder or is allowed to forward directly to the Internet the risk of exposure of email server data on the Internet is increased. c) The external interface of the firewall must not be used as an SMTP relay as this would permit external hosts to relay email through CFG's email server causing it to appear as the root of Spam email. d) The internal interface of the firewall must not accept SMTP email from any email host other than the corporate email server to avoid any instances of internally generated Spam email. e) There must also be limitations on the allowed size of incoming email. This will prevent a possible denial of service attack that could be performed by sending large attachments to a number of people on the network. If the firewall lets through these attachments which are then opened by a number of people simultaneously the corporate email server might experience delays or may even become unavailable. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Servers , examine the enabled servers (check box) under Internal Servers and External Servers | SMTP server is enabled on both Interfaces | O | O | |
| b) In BWC, under Proxies , select Internal and click on Internal to External to examine the enabled proxies | The SMTP proxy is <u>not</u> enabled. | O | O | |
| c) To ensure that the firewall will deliver incoming mail to only the corporate mail server, in BWC, under Mail Server , select Routing . Right-click on the configured internal domain (CFG) and select Modify to examine the Sub-domain mail routing and the Delivery configuration. Figure 8 shows the top level Mail Server menu. | The firewall is configured to only deliver mail destined for the CFG.com domain. All mail will be delivered to the IP address of the Corporate mail server under Deliver Via Host . | O | O | |
| d) To ensure that the corporate mail server will deliver outbound mail to only the firewall Examine its Internet mail configuration | The corporate mail server is configured to send all outgoing SMTP mail to only the firewall | O | O | |
| e) To verify that the corporate mail server can only deliver outbound mail to the firewall, on the mail server, temporarily configure the | This should not be possible as the firewall should not have the SMTP proxy enabled. | O | O | |

| | | | | |
|---|--|----------|----------|--|
| <p>Internet mail connector to deliver mail via DNS (as opposed to delivering via the firewall internal interface). Attempt to send an email from the Corporate Mailbox to the Internet Email Account. (NB: Ensure that the mail server configuration is returned to its previous state immediately after this test)</p> | | | | |
| <p>Test (f), (g) and (h) will verify that SMTP functions on the firewall internal interface</p> | | | | |
| <p>f) To verify that SMTP is configured to send mail from the firewall internal interface to the internal network, in BWC, select Mail Server and under Network Diagnostics, select the check box next to Send Test Mail. Send the test mail to the Corporate Mailbox and verify that the message was received. (see Figure 9)</p> | <p>The mail will be received in the corporate mailbox</p> | <p>T</p> | <p>O</p> | |
| <p>g) To verify that firewall SMTP server is configured to receive mail on the internal interface, from the Corporate Mailbox send an email to postmaster@cfg.com. Examine the firewall mail logs to verify the mail was received by the firewall. (see Figure 10)</p> | <p>In BWC, the mail log under Logs – View Log files will show the email was received by the firewall</p> | <p>T</p> | <p>O</p> | |
| <p>h) To verify that firewall SMTP is configured is to forward mail received on the internal interface to the Internet, send an email from the corporate mailbox to the Internet Mail Account and verify receipt.</p> | <p>The mail will be received by the Internet mail account and the mail headers will show that the mail was sent from the firewall external interface (sender is the corporate mailbox)</p> | <p>T</p> | <p>O</p> | |
| <p>Test (i), (j) and (k) will verify that SMTP functions on the external interface</p> | | | | |
| <p>i) To verify that SMTP is configured to send mail from the external interface, in BWC, select Mail Server and under Network Diagnostics select the check box next to Send Test</p> | <p>The mail will be received by the Internet mail account and the mail headers will show that the mail was sent from the</p> | <p>T</p> | <p>O</p> | |

| | | | | | |
|---|--|---|---|---|--|
| | Mail. Send the test mail to the Internet Mail Account and verify that the message is received. | firewall external interface (sender is the postmaster mailbox) | | | |
| j) | To verify that SMTP is configured to receive mail on the external interface, from the External SMTP Client, send an email to postmaster@cfg.com . | In BWC, the mail log under Logs – View Logfiles will show the mail was received by the firewall | T | O | |
| k) | To verify that SMTP is configured is configured to forward mail received on the external interface to the corporate mail server, send an email from the external SMTP client to the corporate mailbox. | The mail will be received in the corporate mailbox | T | O | |
| Test (l) and (m) will verify that the internal interface can not be used to forward Spam mail generated on the internal network | | | | | |
| l) | To ensure that the Internal SMTP server is configured to receive SMTP mail from only the corporate mail server, In BWC under Servers , select Internal and right click on SMTP Mail in the main window. Select Modify and examine the access rules Click on the Access Rule tab, select Edit and select the Source Addresses tab. | A specific access rule exists for SMTP (as opposed to the initial default rule) and the list of allowed IP addresses should contain only that of the corporate mail server. (See Figure 11) | O | O | |
| m) | To verify the Firewall will not permit internal Spam mail to the Internet, send an email from the Internal SMTP client to the Internet Mail Account. | The mail should not arrive at the Internet mail account's mailbox. If it does, examine the headers to determine whether the message was received from the firewall external interface. | T | O | |
| Test (n) and (o) will verify that the internal interface can not be used to relay Spam mail generated on the Internet | | | | | |
| n) | To ensure that the SMTP server is configured not to relay mail on its external interface, in BWC, under Mail Server , select General and examine the Block Mail Relaying on the External Interface check box | Block Mail Relaying on the External Interface should be selected | O | O | |
| o) | To verify that mail relaying is not permitted on the external interface from the External | The mail should not arrive at the Internet mail | T | O | |

| | | | | | |
|---|--|--|---|-------------------|--|
| interface, from the External SMTP Client, send an email to the Internet Mail Account. | | Internet mail account's mailbox. If it does, examine the headers to determine whether the message was received from the firewall external interface. | | | |
| p) To verify mail size limits, in BWC, under Mail Server , select General and ensure determine whether the Limit mail message size checkbox is selected. | | The box should be selected and the value should be typically no bigger than 2-3mb but that will depend on available bandwidth and capacity of the mail server to deal with large attachments | O | O | |
| Date: | | Completed by: | | Signature: | |
| Note: Any manipulation of configuration settings on either the firewall or the corporate email server should be performed during off hours as part of a regular maintenance window. The IT manager must be informed and all settings must be returned to their previous state. | | | | | |

Fig. 8: Top level Email Server Menu

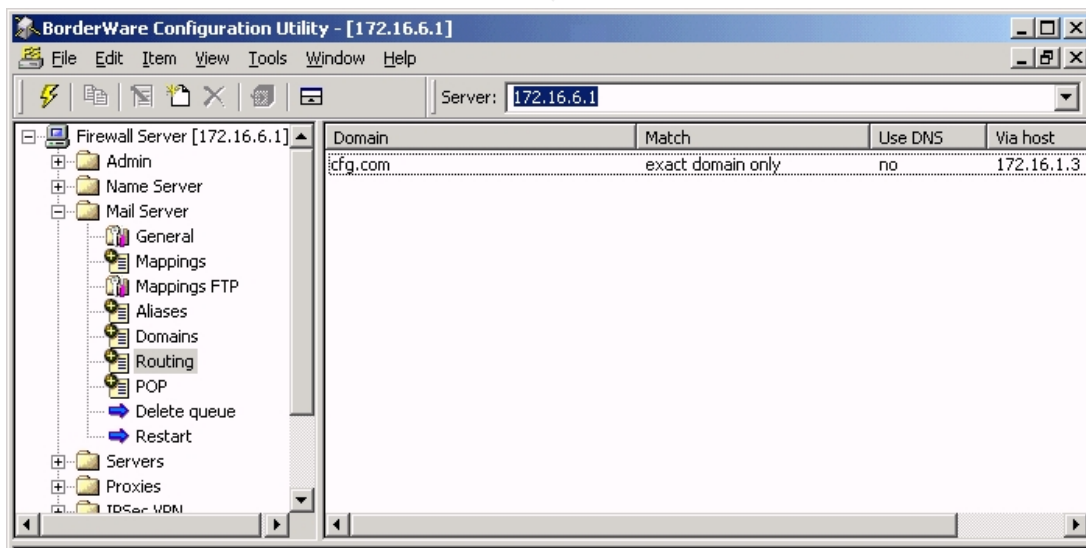


Fig. 9: Sending email from the Firewall SMTP server

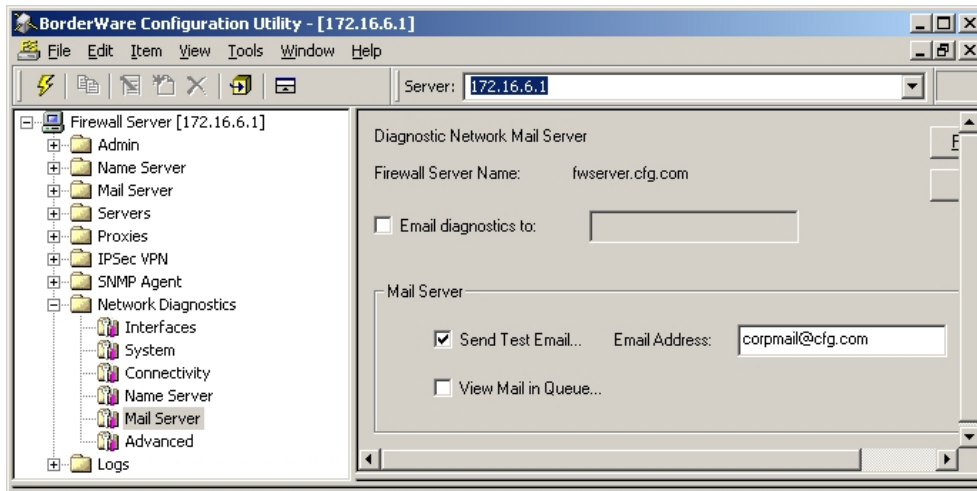


Fig. 10: Log Files menu

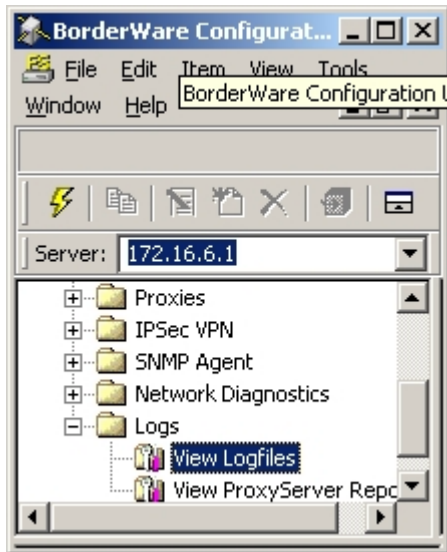
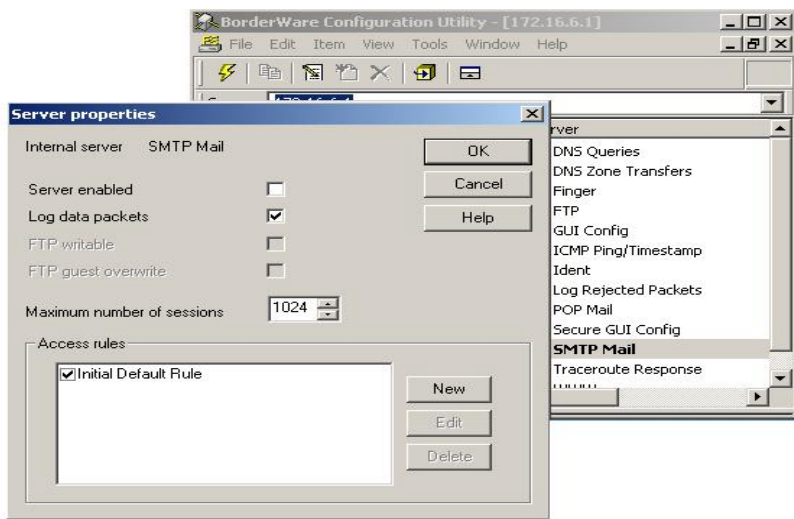
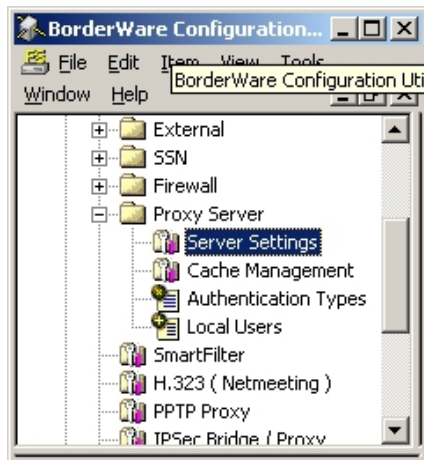


Fig. 11: Internal SMTP Server ACL



| CO.5.4 - Squid Proxy Server (HTTP) | | | | |
|---|---|--------|------------|------------|
| Reference: Borderware Firewall Server Reference Guide ⁵⁵ | | | | |
| Control Objective: To determine whether the firewall acts as a proxy for Internet HTTP requests from internal users without any configuration of the client browser. This objective will also determine that the Squid Proxy Server is used to facilitate caching of web pages and more complete logging* than the simple WWW proxy. | | | | |
| Risk: If the HTTP proxy on the firewall is not configured, Internet access will be unavailable for hosts on the internal network. If clients can pass HTTP requests directly to the Internet, there is a risk of exposure of client systems to the Internet. If only the simple HTTP proxy is used, there will be no caching (which would allow faster access to frequently accessed pages) and logging will be limited. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In the Proxies menu, select Internal and the select Internal-to External and examine the enabled proxies | The WWW proxy is disabled | O | O | |
| b) Under the Proxies menu, select Proxy Server and then select Server Settings (see Figure 12) and examine the proxy server settings under Service | Enable Service check box is selected. Enable with caching is selected in the Internal-to External drop down menu Enable Authentication checkbox is disabled | O | O | |
| c) Under the Proxies menu, select Proxy Server and then select Server Settings (see Figure 13) and examine the proxy server settings under Proxy mode | The transparent check box is enabled under Proxy Mode to ensure users do not need to authenticate or specify the proxy server in their browsers | O | O | |
| d) From the Internal host, attempt to access http://www.sans.org without modifying the browser's default settings. | The site should be accessible | T | O | |
| e) Run Ethereal protocol analyzer on the external host when HTTP requests are made from the internal host to determine the source IP address of HTTP requests | HTTP traffic leaving the network has the external interface of the firewall as its source address | T | O | |
| Date: | Completed by: | | Signature: | |
| Note: * InsideOut Firewall Reporter ⁵⁶ is a Browser based application that is available from Borderware. It allows for complex manipulation of firewall logs and statistics as well as generation of graphical reports. | | | | |

Fig. 12: Server Settings in Proxy Server menu



| CO.5.5 - HTTP Filter | | | | |
|---|--|--------|------------|------------|
| Reference: Personal Experience | | | | |
| Control Objective To determine whether HTTP filtering is enabled with the Code Red and Code Red II file patterns | | | | |
| Risk: If HTTP filters are not enabled, it is possible that the Code Red virus could pass from an HTTP client on the Internet to the web server on the SSN or that infected internal hosts could pass code red attack patterns to the Internet | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC, Examine the HTTP settings under Proxy Server | HTTP Filtering is enabled and the code red file patterns are in the filter list. | O | O | |
| Date: | Completed by: | | Signature: | |
| Note: | | | | |

| CO.5.6 - Smart Filter (URL Filtering Software) | | | | |
|--|---|---------------|------------|-------------------|
| Reference: Borderware Firewall Server Reference Guide ⁵⁷ | | | | |
| Control Objective: To determine whether the URL filtering software meets policy expectations without hindering access to legitimate websites. | | | | |
| Risk: False positives from the filtering software will restrict users from performing legitimate business tasks while false negatives will expose users to inappropriate sites. In addition, false negatives may cause restricted website logs to show access CFG's IP address. (This may be an embarrassment issue as some "hactivist", anarchist, and "cybercrime" websites publish logs showing access from corporate and government addresses) | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) To ensure the service is enabled, in BWC, access the Smartfilter menu under Proxies | The smart Filter Service is enabled | O | O | |
| b) To ensure database downloads occur, under Smartfilter subscription , examine the date of the last download. | The last download of filter database should take place within one week prior to the date of testing | O | O | |
| c) To ensure a manual download is possible, select Download Control List | A manual download of the latest filter database is initiated | T | O | |
| d) From a web browser on the internal host, attempt to access a range of gambling, pornographic, racist, violent, anarchist and sexist websites | Access to sample sites are blocked by the filter a message in the browser window states why this has happened | T | O | |
| e) Interview helpdesk staff and firewall administrators to determine the history of false negatives (unacceptable sites allowed by the URL filter that have warranted manual editing of URL filter database) | Helpdesk personnel report minimum incidents of false negatives | I | S | |
| f) Attempt to access a range of acceptable business related web sites such as government, technology, and university web sites to determine if the filter blocks access or | Browser is granted access to these sites | T | O | |
| g) Interview helpdesk and firewall administrators to determine history of false positives (acceptable sites | Helpdesk personnel will report minimum incidents of false positives | I | S | |

| | | | | |
|--|---|-------------------|---|--|
| blocked by URL filter) that have warranted manual editing of URL filter database | | | | |
| h) From the internal host attempt access to web- based email sites such as www.hotmail.com, etc. | Web based email sites should be blocked by the filter | T | O | |
| Date: | Completed by: | Signature: | | |
| Note: The firewall administrator should be informed before attempting to access a range of blocked sites. If any of the sites are displayed or blocked in an unexpected manner, the administrator should be informed so he can edit the database. | | | | |

© SANS Institute 2003, Author retains full rights.

| CO.5.7 - Additional configurable services that are not mentioned in firewall policy | | | | |
|---|--------------------------------|--------|------------|------------|
| Reference: Product Settings | | | | |
| Control Objective: The following configurable services are not mentioned in the CFG corporate and firewall policies. In accordance with these policies, since these services are not explicitly required they must be disabled. | | | | |
| Risk: Unauthorized services allows unexpected/undesired access to the network from the Internet | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Examine H.323 (Netmeeting) settings | Service is not enabled | O | O | |
| b) Examine PPTP Proxy settings | Service is not enabled | O | O | |
| c) Examine IPSEC Bridge/Proxy settings | Service is not enabled | O | O | |
| d) Examine IPSEC VPN settings | Service is not enabled | O | O | |
| e) Examine SNMP Agent settings | Service is not enabled | O | O | |
| Date: | Completed by: | | Signature: | |
| Note: | | | | |

© SANS Institute 2003, Author retains full rights.

Control Objectives Group 6 - Network Access for Firewall Administration

| CO.6.1 - Remote Management Interfaces on Firewall | | | | |
|---|--|---------------|------------|-------------------|
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether Remote Management is secured and accessible on only the internal interface. | | | | |
| Risk a) It is possible that if Remote Management is allowed on the external interface, that administrator session credentials could be captured or that a session could be hijacked to allow malicious changes to firewall. If it is enabled on the SSN interface, a compromise of the SSN host could allow an attacker to manipulate the firewall to allow access to the internal network from the SSN. b) If encryption is not used for Remote Management sessions, authentication or configuration data for the firewall could be determined by someone running a packet sniffer on the network c) If user-ACLs are not applied to Remote Management settings, anyone who can make a network connection to the firewall interface can perform Remote Management. d) If the credentials used by each administrator are not unique, there will be no accountability for misconfiguration via remote access e) If IP address based ACLs are not applied on the Remote Management interface, a connection can be attempted from any workstation on the network making a brute force password crack (from single or multiple workstations) easier to attempt. Additionally firewall Remote Management may be conducted from a workstation in an area that is not secure or where the credentials could be determined by social engineering methods. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Admin select System Settings and examine the selected interfaces under Remote Management | Only the Internal (Secured) check box is selected. The other check boxes (Internal (unsecured) , External and SSN are not checked (O) | O | O | |
| b) To verify that secure Remote Management is enabled on the internal interface, attempt to initiate an SSL Remote Management (BWC) session from an internal host (check the SSL Encrypted Session box when specifying the server as shown in Figure 13) | Remote management is possible on the Internal interface using SSL | T | O | |
| c) To verify that secure Remote Management is <u>not</u> enabled on the external interface, attempt to initiate an SSL Remote Management (BWC) session from the external host (check the SSL Encrypted | Remote management is not possible on the external interface using SSL | T | O | |

| | | | | |
|----|--|--|---|---|
| | Session box when specifying the server | | | |
| d) | To verify that secure Remote Management is <u>not</u> enabled on the SSN interface, attempt to initiate an SSL Remote Management (BWC) session from the SSN host (check the SSL Encrypted Session box when specifying the server) | Remote management is not possible on the SSN interface using SSL | T | O |
| e) | To verify that Clear Text Remote Management is <u>not</u> enabled on the internal interface, attempt to initiate a clear text Remote Management (BWC) session from the internal host (uncheck the SSL Encrypted Session box when specifying the server) | Remote management is not possible on the Internal interface using clear text | T | O |
| f) | To verify that Clear Text Remote Management is <u>not</u> enabled on the external interface, attempt to initiate a clear text Remote Management (BWC) session from the external host (uncheck the SSL Encrypted Session box when specifying the server) | Remote management is not possible on the SSN interface using clear text | T | O |
| g) | To verify that Clear Text Remote Management is <u>not</u> enabled on the SSN interface, attempt to initiate a clear text Remote Management (BWC) session from the SSN host (uncheck the SSL Encrypted Session box when specifying the server) | Remote management is not possible on the External interface using clear text | T | O |
| h) | At the firewall console, examine the Secure Logins configuration in the Admin menu to determine the specific | There should be one user name for each firewall administrator | O | O |

| | | | | |
|--|--|--|---|------------|
| Admin Users configured for Remote Management (Figure 14) | | | | |
| i) | To verify that user ACLs have been applied, from BWC on the internal host, attempt a Remote Management session bypassing the login screen | It should not be possible to bypass the login screen | T | O |
| j) | To determine if IP address ACLs have been applied, in BWC , under Servers , select Internal Servers , right click Secure GUI Config and select Modify . | The access rules should contain a rule that limits source addresses to particular IP addresses | O | O |
| k) | To verify IP address based ACLs exist, attempt to perform Remote Management from user workstations on the network | It should only be possible to perform Remote Management from specific workstations specified by the firewall administrator | T | O |
| Date: | | Completed by: | | Signature: |
| Note: | | | | |

Fig. 13: Server Settings in Proxy Server menu

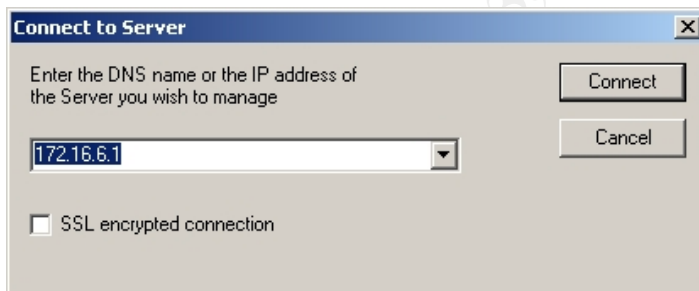
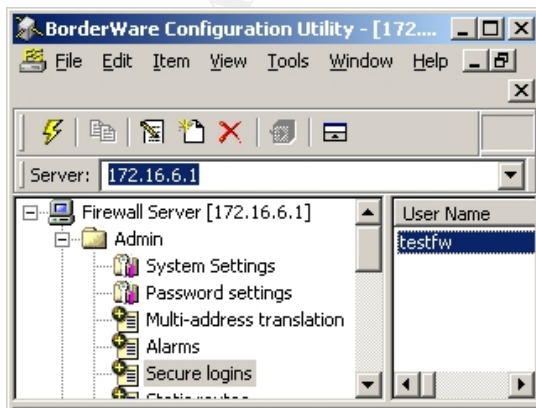
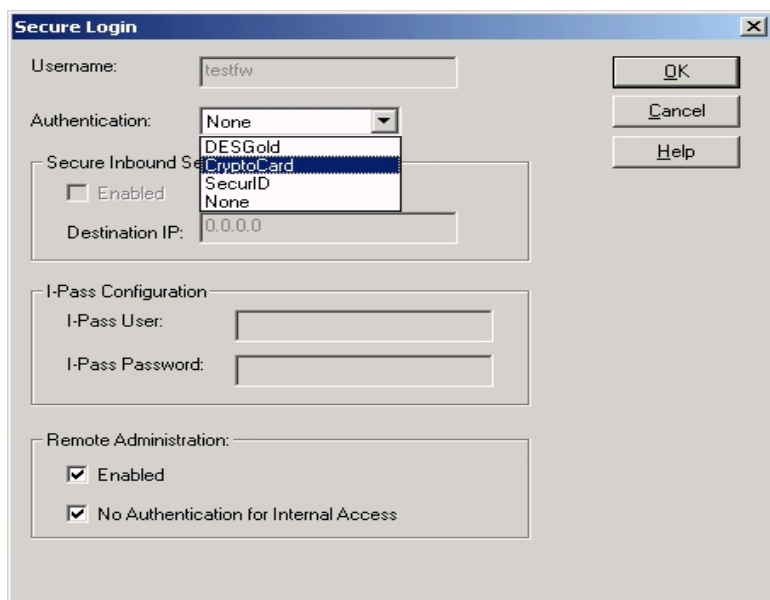


Fig. 14: Server Settings in Proxy Server menu



| | | | | |
|--|---|-------------------|------------|-------------------|
| CO.6.3 - Two factor authentication for Remote Management | | | | |
| Reference: COBIT ⁵⁸ | | | | |
| Control Objective: To determine whether Remote Management is configured to incorporate Crypto-card (smart card) technology to increase security | | | | |
| Risk: If Remote Management authentication is based purely on password credentials, it is more likely to be exploited by a brute force password crack | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC, under the Admin menu, select Secure Logins , double click the configured user account and examine the authentication options to determine if Crypto Card is selected (Figure 15) | Under Authentication in Figure 15 CryptoCard will be listed | O | O | |
| b) Attempt to perform Remote Management from a workstation using only username and password as credentials. | Remote Management using only user name and password will not be possible if the user account requires Cryptocard authentication | T | O | |
| c) Examine the Remote Management workstations to determine if they are equipped with Crypto-card readers | Remote Management workstations will have crypto card readers attached | O | O | |
| Date: | Completed by: | Signature: | | |
| Note: | | | | |

Fig. 15: Crypto card configuration for Remote Management Secure Login

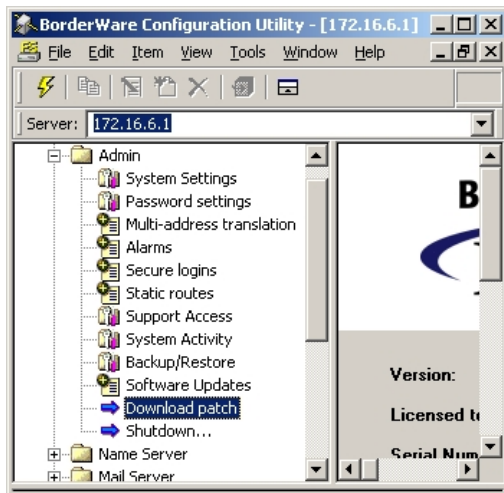


© SANS Institute 2003, Author retains full rights.

Control Objectives Group 7 - Firewall Management

| | | | | |
|--|--|-------------------|------------|-------------------|
| CO.7.1 - Firewall Patches and Fixes | | | | |
| Reference: SANS Course Material ⁵⁹ | | | | |
| Control Objective: To determine whether the firewall has the most recent patches applied | | | | |
| Risk: If the patches and fixes are not up to date the firewall will be subject to exploit via a known vulnerability | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC, select Software Updates in the Admin menu to determine the patches installed on the firewall. From the Download Patch utility in the Admin menu determine the patches available for the firewall (see Figure 16). | All available patches in the Download Patch utility will display as being installed in the Software Updates menu | O | O | |
| b) Examine release notes to determine if outstanding patches are relevant to the configuration employed on this firewall | Any outstanding patches will not be relevant to this particular configuration | DR | O | |
| c) Conduct an interview with the firewall administrator to determine whether a documented procedure and schedule exists for patch downloads and updates. | Documented procedure and schedule exists for patch downloads and updates | I | S | |
| d) Conduct an interview with the firewall administrator to determine whether CFG receives regular notification of new patches from the firewall manufacturer | The firewall manufacturer regular notifies the firewall administrator or new patches | I | S | |
| Date: | Completed by: | Signature: | | |
| Note: | | | | |

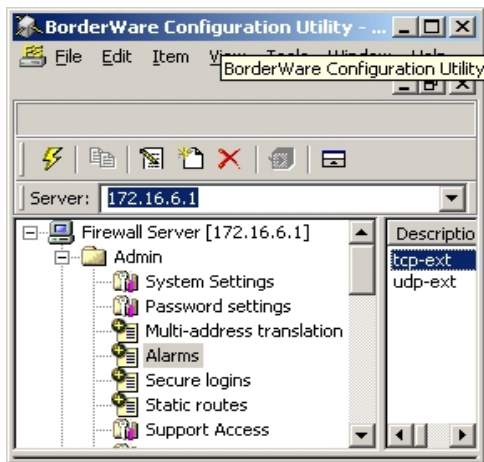
Fig. 16: Admin menu with Software Updates and Download Patch options



| CO.7.2 - Firewall Logging | | | | |
|--|---|---------------|------------|-------------------|
| Reference: SANS Course Material ⁶⁰ | | | | |
| Control Objective: To determine whether all firewall logs are reviewed by the firewall administrator and whether alarm conditions are set so that pagers and/or mailboxes are notified when conditions are met. | | | | |
| Risk: If logs are not reviewed – or if administrators are not notified when alarm conditions are met - potential attack patterns will be missed | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Conduct interviews with firewall administrators to determine if logs are reviewed | Administrator states that logs are reviewed regularly | O | O | |
| b) In BWC, examine Alarms in the Admin menu to determine if alarm conditions are set when attack patterns are generated and if notification is turned on (see Figure 17) | Alarms are enabled on the firewall and the firewall administrators and firewall manager are emailed when an alarm is triggered | I | S | |
| c) From the external host, run NMAP against the external interface of the firewall to determine if alarms are generated | NMAP scans on the external interface cause alarms to appear on the console screen, create entries in the alarm logs and automatically email the firewall administrators | T | O | |
| d) Observe the firewall administrator to determine if alarms are monitored and if action is taken | The firewall administrator observes the attack and examines packets and source IP prior to notifying the firewall manager | O | O | |
| e) Conduct an interview | Documented procedure | I | S | |

| | | | | | | |
|--|--|---|--|--|-------------------|--|
| with the firewall manager to determine if documented procedure exists for when attack patterns are generated in the log file or for when alarms are triggered | | exists to deal with attack patterns determined from log files and alarm notifications | | | | |
| Date: | | Completed by: | | | Signature: | |
| Note: The IT Director and/or the firewall manager should be informed of this audit step to ensure that the incident response plan is not mobilized as a result of these test scans. | | | | | | |
| Nmap Syntax: Nmap xxx.yyy.1.9 (external IP address of the firewall) | | | | | | |

Fig. 17: Alarm Menu



| | | | | |
|---|---|-------------------|------------|-------------------|
| CO.7.3 - Remote Firewall Logging | | | | |
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether firewall logs are written to a remote logging server. | | | | |
| Risk: Writing data to remote logging data helps to mitigate any circumstances where a hacker might modify the logs on the local firewall to cover up a security breach | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC, under Admin , select System Settings and determine the IP address entered for Logging Host under the Syslog field | IP address in Syslog field will be a secure server on the local network running Syslog software | O | O | |
| b) Examine the Syslog server configuration and data to ensure that firewall data is written to the Syslog server | Firewall logs are written to the Syslog server | O | O | |
| Date: | Completed by: | Signature: | | |
| Note: | | | | |

| | | | | |
|--|--|-------------------|------------|-------------------|
| CO.7.4 - Firewall Log Backups | | | | |
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether firewall log data is backed up as business data | | | | |
| Risk: If firewall log data is not backed up, it may not be available at a later date for forensic analysis of attack patterns, or as evidence in any subsequent legal action. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Interview the firewall administrator to determine whether firewall logs are backed up regularly | Administrator states firewall logs are backed up daily with corporate data | I | S | |
| b) Interview the firewall administrator to determine if firewall log backup data is retained in accordance with the corporate backup strategy | Administrator states that firewall log data is retained according to corporate data retention policy | I | S | |
| Date: | Completed by: | Signature: | | |
| Note: | | | | |

| | | | | |
|---|---|-------------------|------------|-------------------|
| CO.7.5– Support Access | | | | |
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether Borderware support access is enabled and under what circumstances it will be enabled. | | | | |
| Risk: While, theoretically, enabling Borderware support access should not be a security risk, it should only be enabled for the purpose of specific troubleshooting by Borderware Technical Support staff. It is possible that if it is left enabled long term, a hacker could attempt to exploit the service to either gain remote access to the server or else cause a disruption of service | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Admin , select Support Access and ensure that the Enable Access box is not checked | Enable Access is not checked | O | O | |
| b) Conduct an interview with the firewall administrator to determine under what circumstance Support Access is enabled | Administrator states that Support Access is enabled only when Borderware Technical Support personnel request and only when this is in response to an issue raised by the firewall administrator at CFG | I | S | |
| c) Contact Borderware Technical Support to determine risks associated with enabling Support Access. | A Borderware technical representative states that the product designers has taken steps to ensure that enabling support access will not compromise the firewall's security | I | S | |
| Date: | Completed by: | Signature: | | |
| Note: Enabling Support Access allows Borderware Technical Support staff to remotely access the firewall configuration for the purpose of troubleshooting and configuration review | | | | |

Control Objectives Group 8 - Firewall Rule Base and Interfaces

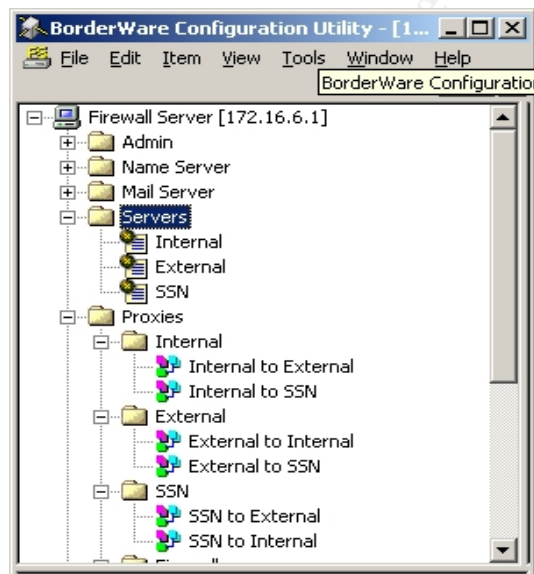
Based on the corporate policy documents in A.2.1., Table 8 was constructed by the auditor. It states the servers and/or proxies that should be enabled on each firewall interface based on the policy stipulations and acts as reference when auditing these interfaces. This table was reviewed by the IT manager prior to creation of the checklist and it was agreed that the services below correspond to the corporate policy stipulations.

Table 8: Services that should be enabled on each Interface

| Servers | Required by policy |
|------------------------------|-----------------------------|
| Internal Servers | SMTP, DNS, Secure GUI, ICMP |
| External Servers | SMTP |
| SSN Server | None |
| Proxies | |
| Internal to External Proxies | HTTP, FTP, ICMP, WWW |
| Internal to SSN Proxies | HTTP, ICMP |
| External to Internal Proxies | None |
| External to SSN Proxies | HTTP |
| SSN to Internal Proxies | None |
| SSS to External Proxies | None |

Refer to Figure 18 for when examining the proxies and servers configured on the firewall.

Fig. 18: Servers and Proxies Top Level Menu



| | | | | |
|---|---|---------------|-------------------|-------------------|
| CO.8.1 – System default as Deny-all | | | | |
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether the firewall defaults to a deny-all state to ensure that services that are not specifically needed are disabled. | | | | |
| Risk: If the default state is anything other than “deny-all” some servers and proxies that are not needed may be left enabled | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Interview firewall administrator to determine criteria for allowing new services or creating new rules | Firewall administrator states that new rules are enabled based on business needs presented to him by the firewall manager | I | O | |
| b) From product documentation and a test install of Borderware Firewall 6.5. determine default state of firewall rules | Default state of firewall rules is to deny all network traffic between network segments | T | S | |
| Date: | Completed by: | | Signature: | |
| Note: | | | | |

© SANS Institute 2003, Author retains full rights.

| CO.8.2 - Servers on Internal Interface | | | | |
|---|---|--------|------------|------------|
| Reference: Personal Experience | | | | |
| Control Objective: To determine that only those servers specified as necessary in the corporate and firewall policy are enabled on the internal interface | | | | |
| Risk: If not all the required servers are enabled, business requirements will not be met whereas additional servers may compromise security or place an unnecessary load on the firewall | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Servers , examine the enabled Internal Servers to ensure that only the required servers are enabled | The following serves should be enabled: <ul style="list-style-type: none">• DNS• Secure GUI Config• ICMP• Traceroute• SMTP | O | O | |
| b) Run Nmap from the Linux system against the internal interface of the firewall to determine open ports. | Only the ports corresponding to the servers in (a) should be open | T | O | |
| c) Run Nessus from the Linux system against the internal interface of the firewall to determine vulnerabilities associated with any open ports or enabled servers | There should be no vulnerabilities associated with open ports or services | T | O | |
| d) To verify that ICMP is running as expected, attempt to Ping and Traceroute from the internal host to internal interface of the firewall. | The Ping command should receive 4 replies from the firewall and the Tracert should show 1 or more "hops" to the destination and indicate Trace Complete at the IP address of the firewall internal interface | T | O | |
| e) Enumerate results of visual examination of servers, Nmap scan results and Nessus scan results | No other servers should be enabled | T | O | |
| Date: | Completed by: | | Signature: | |
| Note: The detailed configuration for DNS, Secure GUI Config, and SMTP are examined separately in CO5.2 , CO6.1 and CO5.3 respectively | | | | |
| NMAP Syntax: From the command prompt on the Linux system connected to the internal network, type the following commands: Nmap -sS -PT -PI -n -O -v -T 3 172.16.6.1 Nmap -sT -PT -PI -n -O -v -T 3 172.16.6.1 Nmap -sA -PT -PI -n -O -v -T 3 172.16.6.1 Nmap -sU -PT -PI -n -O -v -T 3 172.16.6.1 | | | | |

Ping Syntax: Ping *IP_address_of_Internal_Interface*
Tracert Syntax: Tracert *IP_address_of_Internal_Interface*

© SANS Institute 2003, Author retains full rights.

| CO.8.3 - Servers on External Interface | | | | |
|--|---|---------------|-----|------------|
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether only those servers specified as necessary in the corporate and firewall policy are enabled on the external interface. | | | | |
| Risk: If not all the required servers are enabled, business requirements will not be met whereas additional servers may compromise security or place an unnecessary load on the firewall | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Servers , examine the enabled External Servers to ensure that only the required servers are enabled | Only SMTP server should be enabled | O | O | |
| b) Run Nmap from the Linux system against the external interface of the firewall to determine open ports. | Only the ports corresponding to the servers in (a) should be open | T | O | |
| c) Run Nessus from the Linux system against the external interface of the firewall to determine vulnerabilities associated with any open ports or enabled servers | There should be no vulnerabilities associated with open ports or services | T | O | |
| d) As the policy documents specifically deny ICMP on the external interface, this will be tested. To verify that ICMP is disabled, attempt to Ping and Traceroute from the external host to external interface of the firewall. | The Ping command will return Request Timed Out and while Tracert may show 1 or more "hops" to the destination, it will also indicate Request Timed Out and will not indicate Trace Complete | T | O | |
| e) Enumerate results of visual examination of servers, Nmap scan results and Nessus scan results to ensure that no other servers are enabled | No additional servers should be enabled | T | O | |
| Date: | | Completed by: | | Signature: |
| Notes: SMTP is examined separately in CO5.3 NMAP Syntax: Nmap -sS -PT -PI -n -O -v -T 3 xxx.yyy.1.9 Nmap -sT -PT -PI -n -O -v -T 3 xxx.yyy.1.9 Nmap -sA -PT -PI -n -O -v -T 3 xxx.yyy.1.9 Nmap -sU -PT -PI -n -O -v -T 3 xxx.yyy.1.9 Ping Syntax: Ping <i>IP_address_of_Internal_Interface</i> Tracert Syntax: Tracert <i>IP_address_of_Internal_Interface</i> | | | | |

| CO.8.4 - Servers on SSN Interface | | | | |
|--|---|--------|------------|------------|
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether only those servers specified as necessary in the corporate and firewall policy are enabled on the SSN interface. | | | | |
| Risk: If not all the required servers are enabled, business requirements will not be met whereas additional servers on may compromise security or place an unnecessary load on the firewall | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Servers , examine the enabled SSN Servers to ensure that only the required servers are enabled | No Servers should be enabled | O | O | |
| b) Run Nmap from the Linux system against the SSN interface of the firewall to determine open ports. | Only the ports corresponding to the servers in (a) should be open | T | O | |
| c) Run Nessus from the Linux system against the SSN interface of the firewall to determine vulnerabilities associated with any open ports or enabled servers | There should be no vulnerabilities associated with open ports or services | T | O | |
| d) Enumerate results of visual examination of servers, Nmap scan results and Nessus scan results to ensure that no other servers are enabled | No additional servers should be enabled | T | O | |
| Date: | Completed by: | | Signature: | |
| Notes: NMAP Syntax: Nmap -sS -PT -PI -n -O -v -T 3 10.0.0.1 Nmap -sT -PT -PI -n -O -v -T 3 10.0.0.1 Nmap -sA -PT -PI -n -O -v -T 3 10.0.0.1 Nmap -sU -PT -PI -n -O -v -T 3 10.0.0.1 | | | | |

| | | | | |
|---|--|-------------------|------------|-------------------|
| CO.8.5 - External to Internal Proxies | | | | |
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether only those proxies specified as necessary in the corporate firewall policy are enabled as external-to-internal. | | | | |
| Risk: If not all the required proxies are enabled, business requirements will not be met whereas additional proxies may compromise security or place an unnecessary load on the firewall. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Proxies , select External and examine the firewall's External-to-Internal proxies to ensure that only the required proxies are enabled | No external-to-internal proxies should be enabled | O | O | |
| b) Run Nmap from the Linux system against the external interface of the firewall to determine open ports. | Only the ports corresponding to the proxies in (a) should be open | T | O | |
| c) Run Nessus from the Linux system against the external interface of the firewall to determine vulnerabilities associated with any open ports or enabled proxies | There should be no vulnerabilities associated with enabled proxies | T | O | |
| d) Enumerate results of visual examination of proxies, Nmap scan results and Nessus scan results to ensure that no other proxies are enabled | No additional proxies should be enabled | T | O | |
| e) Using Ethereal protocol analyzer on the internal host, capture traffic on the network segment while Nessus and Nmap scan the external interface. | Ethereal protocol analyzer running on the internal host detects no traffic patterns from the external host | T | O | |
| Date: | Completed by: | Signature: | | |
| Notes: NMAP Syntax: Nmap -sS -PT -PI -O -v -T 3 xxx.yyy.1.9 Nmap -sT -PT -PI -n -O -v -T 3 xxx.yyy.1.9 Nmap -sA -PT -PI -n -O -v -T 3 xxx.yyy.1.9 Nmap -sU -PT -PI -n -O -v -T 3 xxx.yyy.1.9 | | | | |

| CO.8.6 - External to SSN Proxies | | | | |
|--|---|---------------|------------|-------------------|
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether only those proxies specified as necessary in the corporate firewall policy are enabled as external-to-SSN. | | | | |
| Risk: If not all the required proxies are enabled, business requirements will not be met whereas additional proxies may compromise security or place an unnecessary load on the firewall. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Proxies , select External and examine the firewall's External-to-SSN proxies to ensure that only the required proxies are enabled | The following external-to-SSN proxies should be enabled: <ul style="list-style-type: none"> WWW | O | O | |
| b) Run Nmap from the Linux system against the external interface of the firewall to determine open ports. | Only the ports corresponding to the proxies in (a) should be open | T | O | |
| c) Run Nessus from the Linux system against the external interface of the firewall to determine vulnerabilities associated with any open ports or enabled proxies | There should be no vulnerabilities associated with enabled proxies | T | O | |
| d) Refer to CO.5.1e for compliance. | All HTTP requests to the external interface are redirected (or proxied) to the SSN web server | T | O | |
| e) To ensure that the external proxy limits access based on source IP address, in BWC, under Proxies , select External and select External-to-SSN proxies and right click on WWW Proxy . Select modify and access rules to ensure that this proxy uses a rule configured specifically for it | There is a rule created specifically for the External to SSN WWW proxy as opposed to the "initial default rule" | O | O | |
| f) Select Edit for the specific rule and select source addresses to examine the IP address ACL | A limited number of IP addresses are allowed to access this proxy as opposed to access being allowed to all source IP addresses | O | O | |
| g) From the command prompt on the internal host use nslookup to determine the domain names associated with the IP addresses in (f) and interview the IT manager to confirm that the IP addresses are those of | All IP addresses in the ACL should be associated with domains who are specifically granted access to the SSN web pages | T | O | |

| | | | | |
|--|--|---|-------------------|--|
| partners who are allowed access to the data on the SSN web server | | | | |
| h) Enumerate results of visual examination of proxies, Nmap scan results and Nessus scan results to ensure that no other proxies are enabled | No additional proxies should be enabled | T | O | |
| i) Using Ethereal protocol analyzer on the SSN host, capture traffic on the network segment while Nessus and Nmap scan the external interface. | Ethereal protocol analyzer running on the SSN host detects only HTTP traffic patterns from the external host | T | O | |
| Date: | Completed by: | | Signature: | |
| Notes: NMAP Syntax: Nmap -sS -P0 -n -O -v -T 3 xxx.yyy.1.9 Nmap -sT -P0 -n -O -v -T 3 xxx.yyy.1.9 Nmap -sA -P0 -n -O -v -T 3 xxx.yyy.1.9 Nmap -sU -P0 -n -O -v -T 3 xxx.yyy.1.9 | | | | |

© SANS Institute 2003, Author retains full rights.

| | | | | |
|--|---|-------------------|------------|-------------------|
| CO.8.7 - SSN to Internal Proxies | | | | |
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether only those proxies specified as necessary in the corporate firewall policy are enabled as SSN-to-internal. | | | | |
| Risk: If not all the required proxies are enabled, business requirements will not be met whereas additional proxies may compromise security or place an unnecessary load on the firewall | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Proxies , select SSN and examine the firewall's SSN-to-Internal proxies to ensure that only the required proxies are enabled | No SSN-to-internal proxies should be enabled | O | O | |
| b) Run Nmap from the Linux system against the SSN interface of the firewall to determine open ports. | Only the ports corresponding to the proxies in (a) should be open | T | O | |
| c) Run Nessus from the Linux system against the SSN interface of the firewall to determine vulnerabilities associated with any open ports or enabled proxies | There should be no vulnerabilities associated with enabled proxies | T | O | |
| d) Enumerate results of visual examination of proxies, Nmap scan results and Nessus scan results to ensure that no other proxies are enabled | No additional proxies should be enabled | T | O | |
| f) Using Ethereal protocol analyzer on the internal host, capture traffic on the network segment while Nessus and Nmap scan the SSN interface. | Ethereal protocol analyzer running on the internal host detects no traffic patterns from the SSN host | T | O | |
| Date: | Completed by: | Signature: | | |
| Notes: NMAP Syntax: Nmap -sS -PT -PI -n -O -v -T 3 10.0.0.1 Nmap -sT -PT -PI -n -O -v -T 3 10.0.0.1 Nmap -sA -PT -PI -n -O -v -T 3 10.0.0.1 Nmap -sU -PT -PI -n -O -v -T 3 10.0.0.1 | | | | |

| CO.8.8 - SSN to External Proxies | | | | |
|--|--|--------|------------|------------|
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether only those proxies specified as necessary in the corporate firewall policy are enabled as SSN-to-external | | | | |
| Risk: If not all the required proxies are enabled, business requirements will not be met whereas additional proxies may compromise security or place an unnecessary load on the firewall | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Proxies , select SSN and examine the firewall's SSN-to-External proxies to ensure that only the required proxies are enabled | No SSN-to-external proxies should be enabled | O | O | |
| b) Run Nmap from the Linux system against the SSN interface of the firewall to determine open ports. | Only the ports corresponding to the proxies in (a) should be open | T | O | |
| c) Run Nessus from the Linux system against the SSN interface of the firewall to determine vulnerabilities associated with any open ports or enabled proxies | There should be no vulnerabilities associated with enabled proxies | T | O | |
| d) Enumerate results of visual examination of proxies, Nmap scan results and Nessus scan results to ensure that no other proxies are enabled | No additional proxies should be enabled | T | O | |
| Date: | Completed by: | | Signature: | |
| Notes: NMAP Syntax: Nmap -sS -PT -PI -n -O -v -T 3 10.0.0.1 Nmap -sT -PT -PI -n -O -v -T 3 10.0.0.1 Nmap -sA -PT -PI -n -O -v -T 3 10.0.0.1 Nmap -sU -PT -PI -n -O -v -T 3 10.0.0.1 | | | | |

| CO.8.9 - Internal to SSN Proxies | | | | |
|---|--|---------------|-------------------|-------------------|
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether only those proxies specified as necessary in the corporate firewall policy are enabled as internal-to-SSN | | | | |
| Risk: If not all the required proxies are enabled, business requirements will not be met whereas additional proxies may compromise security or place an unnecessary load on the firewall | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Proxies , select Internal and examine the firewall's Internal-to-SSN proxies to ensure that only the required proxies are enabled | The following internal-to-SSN proxies should be enabled: <ul style="list-style-type: none"> • WWW • ICMP/Timestamp | O | O | |
| b) Run Nmap from the Linux system against the internal interface of the firewall to determine open ports. | Only the ports corresponding to the proxies in (a) should be open | T | O | |
| c) Run Nessus from the Linux system against the SSN interface of the firewall to determine vulnerabilities associated with any open ports or enabled proxies | There should be no vulnerabilities associated with enabled proxies | T | O | |
| d) From the internal host's Internet browser type http://10.0.0.1 . | The website on the SSN web server is accessible | T | O | |
| e) To verify that ICMP is allowed from the internal network to the SSN, attempt to Ping and Traceroute from the internal host to SSN web server. | The Ping command receives 4 replies from the web server and the Tracert should show 1 or more "hops" to the destination and indicate Trace Complete at the IP of the SSN web server | T | O | |
| f) Enumerate results of visual examination of proxies, Nmap scan results and Nessus scan results to ensure that no other proxies are enabled | No additional proxies should be enabled | T | O | |
| Date: | Completed by: | | Signature: | |

Notes:

NMAP Syntax:

Nmap -sS -PT -PI -n -O -v -T 3 172.16.6.1

Nmap -sT -PT -PI -n -O -v -T 3 172.16.6.1

Nmap -sA -PT -PI -n -O -v -T 3 172.16.6.1

Nmap -sU -PT -PI -n -O -v -T 3 172.16.6.1

Ping Syntax: Ping *IP_address_of_Internal_Interface*

Tracert Syntax: Tracert *IP_address_of_Internal_Interface*

© SANS Institute 2003, Author retains full rights.

| CO.8.10 - Internal to External Proxies | | | | |
|--|--|---------------|------------|-------------------|
| Reference: Personal Experience | | | | |
| Control Objective: To determine whether only those proxies specified as necessary in the corporate firewall policy are enabled as internal-to-external | | | | |
| Risk: If not all the required proxies are enabled, business requirements will not be met whereas additional proxies may compromise security or place an unnecessary load on the firewall | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Proxies , select internal and examine the firewall's internal-to-External proxies to ensure that only the required proxies are enabled | The following internal-to-external proxies should be enabled <ul style="list-style-type: none"> • ICMP/Time-stamp • FTP • WWW** | O | O | |
| b) Run Nmap from the Linux system against the internal interface of the firewall to determine open ports. | Only the ports corresponding to the proxies in (a) should be open | T | O | |
| c) Run Nessus from the Linux system against the internal interface of the firewall to determine vulnerabilities associated with any open ports or enabled proxies | There should be no vulnerabilities associated with enabled proxies | T | O | |
| d) To verify that ICMP is proxied through the firewall from the internal network to the external, from the internal host, attempt to Ping a web site that has enabled ICMP responses (www.yahoo.com). | The Ping command will receive 4 replies from the web site (O). | | | |
| e) To verify that FTP is proxied through the firewall from the internal network to the external, from the Internal host, attempt to establish an FTP session to an Internet FTP site that allows anonymous access such as ftp.nai.com | FTP access should be possible to the site | | | |
| f) Enumerate results of visual examination of proxies, Nmap scan results and Nessus scan results to ensure that no other servers are enabled | No additional proxies should be enabled | T | O | |

| | | | |
|---|----------------------|-------------------|--|
| Comments: | | | |
| Date: | Completed by: | Signature: | |
| Notes: <p>** The WWW proxy should be enabled through the Squid proxy server and should be disabled in the simple proxies menu (See C.O.5.4 for individual testing of the Squid proxy)</p> <p>NMAP Syntax: From the command prompt on the Linux system connected to the internal network, type the following commands: Nmap -sS -PT -PI -n -O -v -T 3 172.16.6.1 Nmap -sT -PT -PI -n -O -v -T 3 172.16.6.1 Nmap -sA -PT -PI -n -O -v -T 3 172.16.6.1 Nmap -sU -PT -PI -n -O -v -T 3 172.16.6.1</p> <p>Ping Syntax: Ping www.yahoo.com</p> <p>FTP Syntax:</p> <ul style="list-style-type: none"> • From the Windows 2000 command prompt type FTP ftp.nai.com and hit Enter • If FTP access is allowed Connected to ftp.nai.com will be displayed and a User: prompt will appear • Type anonymous after the User: prompt and hit Enter • If anonymous access is allowed a Password: prompt will appear • Type an email address at the Password: prompt and hit Enter • Anonymous user logged in should be displayed and the ftp> will be available • Type dir to see the list of directories and/or files • Type get filename to transfer a file from the FTP site to the local hard drive | | | |

© SANS Institute 2003, All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage or retrieval system, without the prior written permission of SANS Institute.

| CO.8.11 – Scan from external host to internal network | | | | |
|---|--|--------|------------|------------|
| Reference: Personal Experience and [Ref.38] | | | | |
| Control Objective: To determine whether the firewall rules allow an external host to directly reference hosts on the internal network | | | | |
| Risk: If the firewall allows an external host to directly reference hosts on the internal network (i.e. specifying the IP address of the internal host), it is possible that an Internet attacker could exploit vulnerabilities on an internal system by directly accessing it without being subject to the firewall rules. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Run Nmap from the Linux system on the external network specifying the internal host IP address and the firewall internal interface IP address as targets. While the NMAP scan is running, the Ethereal protocol analyzer should be running on the internal host | Nmap results yield no information about the internal hosts and the Ethereal protocol analyzer does not capture any packets originating on the external host | T | O | |
| b) Run Nessus from the Linux system on the external network specifying the internal host IP address and the firewall internal interface IP address as targets. While the Nessus scan is running, the Ethereal protocol analyzer should be running on the internal host | Nessus results will yield no information about the internal hosts and the Ethereal protocol analyzer does not capture any packets originating on the external host | T | O | |
| Date: | Completed by: | | Signature: | |
| Notes: Nmap syntax: Nmap -sS -P0 -n -O -v -T3 172.16.6.1-2 In Nessus the target selection window will specify the IP address of both the internal host and the firewall internal interface | | | | |

| | | | | | |
|---|--|---|---------------|-------------------|-------------------|
| CO.8.12 – Scan from external host to SSN | | | | | |
| Reference: Personal Experience and [Ref.38] | | | | | |
| Control Objective: To determine whether the firewall rules allow an external host to directly reference hosts on the SSN. | | | | | |
| Risk: If the firewall allows an external host to directly reference hosts on the SSN (i.e. specifying the IP address of the SSN host), it is possible that an Internet attacker could exploit vulnerabilities on an SSN system by directly accessing it without being subject to the firewall rules. | | | | | |
| Test | | Expected Result for Compliance | Method | O/S | Compliance |
| a) Run Nmap from the Linux system on the external network specifying the SSN host IP address and the firewall SSN interface IP address as targets. While the NMAP scan is running, the Ethereal protocol analyzer should be running on the SSN host | | Nmap results yields no information about the SSN hosts and the Ethereal protocol analyzer does not capture any packets originating on the external host | T | O | |
| b) Run Nessus from the Linux system on the external network specifying the SSN host IP address and the firewall SSN interface IP address as targets. While the Nessus scan is running, the Ethereal protocol analyzer should be running on the SSN host | | Nessus results yields no information about the SSN hosts and the Ethereal protocol analyzer does not capture any packets originating on the external host | T | O | |
| Date: | | Completed by: | | Signature: | |
| Notes: Nmap syntax: Nmap -sS -P0 -n -O -v -T3 10.0.0.1-2 In Nessus the target selection window will specify the IP address of both the SSN host and the firewall SSN interface | | | | | |

| | | | | |
|---|---|--------|------------|------------|
| CO.8.13 – Scan from SSN host to internal network | | | | |
| Reference: Personal Experience and [Ref.38] | | | | |
| Control Objective: To determine whether the firewall rules allow an SSN host to directly reference hosts on the Internal network. | | | | |
| Risk: If the firewall allows an SSN host to directly reference hosts on the internal network (i.e. specifying the IP address of the SSN host), it is possible that a compromised SSN host could be used to exploit vulnerabilities on an internal system by directly accessing it through the firewall. | | | | |
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Run Nmap from the Linux system on the SSN network specifying the internal host IP address and the firewall internal interface IP address as targets. While the NMAP scan is running, the Ethereal protocol analyzer should be running on the internal host | Nmap results yields no information about the internal hosts and the ethereal protocol analyzer will not capture any packets originating on the SSN host | T | O | |
| b) Run Nessus from the Linux system on the SSN network specifying the internal host IP address and the firewall internal interface IP address as targets. While the Nessus scan is running, the Ethereal protocol analyzer should be running on the internal host | Nessus results yields no information about the internal hosts and the ethereal protocol analyzer will not capture any packets originating on the SSN host | T | O | |
| Date: | Completed by: | | Signature: | |
| Notes: Nmap syntax: Nmap -sS -P0 -n -O -v -T3 172.16.6.1-2 In Nessus the target selection window will specify the IP address of both the internal host and the firewall internal interface | | | | |

Assignment 3 - Conduct the Audit

A3.1-Introduction

The following section presents a summary of the audit results. The tests are grouped according to the Control Objectives Groups as specified in the checklist. The format of the data is the same as the checklist tables presented in **A2.2**. In each table the items detailing references, elaboration of control objective, risk and notes that were present in the original checklists have been omitted to avoid unnecessary repetition. However, a comments section has been added to elaborate on areas of non-compliance.

For objective items, output from any tests or configuration screens will be shown. In the case of subjective testing the methods used to evaluate the level of compliance will be discussed. Generally, screen shots are only included to illustrate areas of non-compliance.

The items which reflect the most significant security concerns are listed in Table 9 and are discussed in more detail in **Audit Findings** in **A.4.2**. Greater emphasis will be placed on these items in section **A.3.2, Audit Results**.

Note: This list is not meant to assign an order of importance to these items. The order listed below merely corresponds to the order in which the tests were performed.

Table 9: Significant Audit Findings

| | | |
|-----|----------|---|
| 1. | C.O.1.7 | No change management process or procedure |
| 2. | C.O.2.2 | Access to firewall console and password is not secured |
| 3. | C.O.3.1 | Automate failover is not implemented and offline backup firewall does not duplicate configuration |
| 4. | C.O.5.2 | Firewall external interface responds to DNS queries from Internet hosts |
| 5. | C.O.5.3 | SMTP configuration allows both internal and external sources to router Spam Email |
| 6. | C.O.5.6: | Firewall allows access to webmail products such as hotmail.com etc. |
| 7. | C.O.6.1 | Remote management has not been secured on Internal Interface |
| 8. | C.O.7.2 | Firewall Patches are not up to date |
| 9. | C.O.8.10 | Additional proxies and Servers enabled on the internal interface (FTP Server, POP,SSL Proxy) |
| 10. | C.O.8.6 | External to SSN HTTP proxy does not have IP address ACLs |

A.3.2 - Audit Results**Control Objectives Group 1 - Policies Procedures and Documentation**

| CO.1 – Corporate Policy on Firewall and Internet access | | | | |
|---|--|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Determine whether policy documentation exists | Document exists | I/DR | S | Compliant |
| b) Review documentation to determine if it states expectations to be met by firewall | Documentation clearly states business expectations (services allowed) and restrictions (services denied) to be met by firewall | DR | S | Compliant |
| c) Determine the firewall administrators level of awareness regarding this documentation | The firewall administrator is aware of document's existence and location | I | S | Compliant |
| d) Determine the perceived level of compliance between firewall rules and policy documents and the firewall administrator's understanding of the policy | The firewall administrator states that he is able to equate all firewall rules to policy document stipulations | I | S | Compliant |
| Comments: Policy documents exists and are accessible and known to relevant personnel | | | | |
| Date: | Completed by: | Signature: | | |

| CO.1.2 - Firewall Installation and Configuration Procedures | | | | |
|--|---|---------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Determine existence of documentation | Documentation exists | I/DR | O | Compliant |
| b) Review Installation steps | Documentation clearly details steps involved in installing Borderware 6.5 from CD or network share | DR | S | Compliant |
| c) Review configuration steps | Documentation clearly details all firewall configuration settings necessary to meet CFG's business needs and restrictions | DR | S | Compliant |
| d) Review change management references | Documentation references to the change management procedures to ensure that the configuration steps are updated every time a change is made on the firewall | DR | S | Non-Compliant |

| | | | | |
|---|---|-------------------|---|-----------|
| e) Interview the firewall administrator to determine level of awareness | Administrator is aware of document's existence and location | I | S | Compliant |
| Comments: Ref. (d): While procedures for installation and configuration exist, the steps do not reference change management procedure revision numbers, therefore it is not possible to determine whether the configuration in this documentation is current with the most recent changes. | | | | |
| Date: | Completed by: | Signature: | | |

| CO.1.3 - Firewall Backup and Restoration Procedures | | | | |
|--|--|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Determine existence of documentation | Document Exists | I/DR | O | Non-Compliant |
| b) Review Backup and Restore procedures | Documentation clearly states the requirements and steps for backing up and restoring the firewall configuration as well as the frequency of trial restores | DR | S | N/A |
| c) Interview the firewall administrator to determine level of awareness | Administrator is aware of document's existence and location | I | S | N/A |
| d) Interview the firewall administrator to determine level of agreement and compliance | Administrators agree with and comply with the procedures in the documentation | I | S | N/A |
| e) Interview the firewall administrator to determine if a backups track configurations changes | Administrator states that a backup is performed every time a change is made to the configuration of the firewall | I | S | N/A |
| Comments: Ref. (a): No documents exist for backup and restoration procedures | | | | |
| Date: | Completed by: | Signature: | | |

| CO.1.4 – Incident Response | | | | |
|---|---|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Determine existence of documentation | Documentation exists | I/DR | O | Non-Compliant |
| b) Review Documentation to determine if key points are addressed | Documentation clearly states roles, responsibilities, contact lists and post incident review strategy | DR | S | N/A |
| c) Interview administrator to determine the level of awareness of documentation | Administrator is aware of document's existence and location | I | S | N/A |
| d) Interview administrator to determine the level of understanding of key points | Firewall administrator is clear on the incident response procedures, roles and responsibilities | I | S | N/A |
| e) Interview administrator to determine the level of awareness of corporate priorities regarding incident handling | Firewall administrator is clear on the corporate priorities regarding recovery versus evidence gathering | I | S | Non-Compliant |
| f) Interview helpdesk manager to determine the level of level of awareness among helpdesk staff regarding their incident response roles | Helpdesk manager states that helpdesk staff are clear on their role in incident response process, e.g. contacting on-call firewall administrator, etc | I | S | N/A |
| Comments: Ref (a): No documented incident response procedure exists Ref (e): Firewall administrator is not clear in corporate priorities regarding incident handling | | | | |
| Date: | Completed by: | Signature: | | |

| CO.1.5 – URL Filter policy | | | | |
|---|--|---------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Determine existence of documentation regarding acceptable and unacceptable website usage | Documentation exists | I/DR | O | Compliant |
| b) Review Documentation for definition of acceptable websites | Document clearly states what constitutes acceptable and unacceptable web sites | DR | S | Compliant |
| c) Review Documentation to determine process for false positives and negatives | Documentation includes steps to deal with false positives and/or false negatives | DR | S | Compliant |

| | | | | |
|--|---|-------------------|---|-----------|
| | e.g. manual edits to filter database, etc. | | | |
| d) Interview firewall administrator to determine under what circumstances filter configuration will be edited | Database will be edited on user request subject to verification of site content (that site does not violate policy) in question | I | S | Compliant |
| e) Review documentation to determine if consistent process exists for manual edits of filter database | Documentation contains steps (including pre-screening) and process flow for manual editing of database | DR | S | Compliant |
| f) Interview sample user to determine level of understanding and acceptance among user community | Users will understand why filter is in place and find it acceptable | I | S | Compliant |
| Comments: Ref. (e): Helpdesk has access to a standalone computer that connects to the Internet through a commercial ISP. All websites are examined from this system before being unblocked. Ref. (f): Three sample users were interviewed and asked if they understood how and why particular websites were blocked. The sample users were recommended by the IT manager. | | | | |
| Date: | Completed by: | Signature: | | |

| CO.1.6 - firewall administrators contact lists | | | | |
|---|---|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Determine existence of documentation | A complete on-call schedule – with full contact details - for firewall administrators exists | DR/I | O | Compliant |
| b) Interview firewall administrators to verify contact details are correct and up to date | Firewall administrators agree that contact list details (phone number etc.) are correct and up to date | I | S | Compliant |
| c) Interview IT manager and helpdesk manager to determine level of awareness of contact list among helpdesk staff | IT manager and helpdesk manager agree that all IT personnel are aware of document's existence | I | S | Compliant |
| d) Interview IT manager to determine if someone (as well as a backup) has been assigned responsibility for list maintenance | IT manager has assigned the task of maintaining the contact list to a full time staff member and a backup | I | S | Compliant |
| Comments: Document exists and was verified as up to date | | | | |
| Date: | Completed by: | Signature: | | |

| CO.1.7 - Change management Process | | | | |
|--|--|---------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Determine existence of documentation | A documented change management process exists | DR/I | O | Non-Compliant |
| b) Review documentation to determine policy regarding change process | Documentation will cover process involved in making a change to configuration including who is authorized, who must be notified and who must provide final sign-off | DR | S | N/A |
| c) Review documentation to determine policy regarding justification of changes | Documentation will state policy on justification of changes, i.e. does the firewall administrator have to justify these changes to direct management? | DR | S | N/A |
| d) Review documentation to determine policy regarding changes requested by users | Documentation will state process for user requests to change firewall configuration | DR | S | N/A |
| e) Review documentation to determine backup strategy in change management | Documentation will address the fact that backups must be on hand when a change is made and a new backup must be performed once a change is deemed successful | DR | S | N/A |
| f) Interview administrator to determine if backup guidelines from documentation are followed | Administrator will have a copy of the last good backup available when making a change to configuration. Once a change is deemed successful, a new backup will be made. | I | S | Non-Compliant |
| g) Interview administrator to determine level of awareness of change management documentation | Administrator is aware of document's existence and location | I | S | N/A |
| h) Interview administrator to determine level of agreement and compliance with change management documentation | Administrators agree with and comply with the change management process | I | S | N/A |
| Comments: | | | | |
| Ref. (a): The IT department has no documented change management procedures | | | | |

Ref. (d): There is no procedure for users to request changes to the firewall configuration. Further interviews with the firewall administrator revealed that if a user requests access to a particular service, the administrator will allow or deny it based on his own evaluation of the security risks associated with the service.

Ref. (f): The firewall administrator does not have a copy of the last good backup of configuration on-hand when a change is made to the firewall configuration nor is the firewall configuration backed up after a change is made.

| | | |
|--------------|----------------------|-------------------|
| Date: | Completed by: | Signature: |
|--------------|----------------------|-------------------|

© SANS Institute 2003, Author retains full rights.

Control Objectives Group 2 - Physical Access

| CO.2.1 - Access to firewall location | | | | |
|---|---|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Interview IT manager and observe firewall location physical security | Access to the room will be secured by code protected lock, swipe card or security guard | O/I | O | Compliant |
| b) Observe as IT personnel other than firewall administrators attempt to access the locations | IT personnel will only have access to the firewall location if they are authorized to access the firewall | O | S | Non-Compliant |
| c) Observe as non-IT personnel attempt to access the locations | Access will be denied to non-IT personnel | O | S | Compliant |
| d) Attempt access to the location (to verify entry restrictions for non-staff/ consultants) | Access will be denied to all non-staff onsite and outside consultants | O | S | Compliant |
| Comments: Ref. (a) & (b): Door is protected by code-lock and code is known to all IT department personnel Ref. (d): Non-IT personnel (member of HR attempted access) are not allowed to access the room Ref. (e): I was not able to physically access the room and when I asked a member of helpdesk to allow me to access, I was told that they would have to ask the IT manager. | | | | |
| Date: | Completed by: | Signature: | | |

| CO.2.2 - Access to Firewall console | | | | |
|--|--|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) To verify the password has been changed from the default, attempt to log in at the firewall console using the default password | The default password should not allow login | T | O | Compliant |
| b) Interview the firewall administrator to determine that the console password is unique and complex and is known only to firewall administrator | Firewall administrator states password is unique, complex and is not shared with IT personnel other than firewall administrators | I | S | Non-compliant |
| c) Ask the helpdesk manager to attempt access to the firewall using a standard system administration password | The standard system administration password should not allow login | O/I | O | Non-compliant |
| Comments: Ref. (b) & (c): While the password has been changed from default but it is one of the standard IT administration passwords and is known by the other members of the IT department | | | | |
| Date: | Completed by: | Signature: | | |

Control Objectives Group 3 - Redundancy

| CO.3.1 - Tolerance to electrical failure | | | | |
|--|---|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Examine the firewall physical configuration to determine if it is connected to a UPS | Firewall is connected to utility or building power supply via a UPS | O | O | Compliant |
| b) Under the supervision of the firewall administrator, at the firewall console, access the Configure UPS menu under the Misc. menu | UPS Monitor is enabled to ensure graceful shutdown | O | O | Compliant |
| c) Disconnect the firewall UPS from the utility power supply | UPS supplies battery power to the firewall | T | O | Compliant |
| d) Disconnect the firewall UPS from the utility power supply | Graceful shutdown initiates in time frame specified in UPS monitor | T | O | Compliant |
| Comments: Testing was performed off-hours in a regular maintenance window, replacement firewall was available and configuration of production firewall was backed up beforehand. | | | | |
| Date: | Completed by: | Signature: | | |

| CO.3.2 - Firewall Redundancy | | | | |
|---|---|---------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) At the firewall console access the HALO menu options | High Availability (HALO) clustering is enabled with at least one other firewall in the cluster | O | O | Non-compliant |
| b) If HALO is not configured, interview the firewall administrator to determine the existence of an offline backup firewall | Firewall administrator states that offline backup firewall exists | I | S | Compliant |
| c) If HALO is not configured, interview the firewall administrator to determine the existence of documentation detailing the procedure for manual failover to a the offline backup firewall | Documented process exists for manual failover to the offline backup firewall in the event of a failure of the production system | I | S | Non-complaint |
| d) If HALO is not configured, interview the firewall administrator to determine the existence of documentation detailing the procedure for ensuring | Documented process exists for ensuring that offline backup firewall configuration mirrors that of the production system | I | S | Non-Compliant |

| | | | | |
|---|--|-------------------|---|---------------|
| the offline backup firewall is synchronized with the production system | | | | |
| e) Examine the offline backup firewall and compare the configuration to that of the production system | Offline backup firewall will have duplicate configuration of production firewall | O | O | Non-compliant |
| Comments: Ref. (c): While there is an offline backup firewall for manual failover, there is no documented procedure to perform the failover. Ref. (f): Examination of the offline backup firewall revealed that it was missing one of the service patches (fs65p01, Service Patch 1) installed on the production system. | | | | |
| Date: | Completed by: | Signature: | | |

| CO.3.3 - Internet Connection Redundancy | | | | |
|--|--|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Examine architecture documents and interview the network manager to determine if there are redundant Internet connections outside the firewall | There are redundant connections from outside the firewall to separate network carriers | I/DR | O | Compliant |
| b) Examine architecture documents and interview the network manager to ensure that the implementation of redundant Internet connections requires no manual intervention on the part of the user or on the part of the Network team | Failover to redundant network carrier is automatic and transparent to users | I/DR | O | Compliant |
| c) Under the supervision of the network manager, disconnect one of the Internet connected routers from the hub outside the firewall and determine whether Internet connectivity is still available | It is still be possible to make connections to the Internet from the internal host | T | O | Compliant |
| Comments: Testing was performed off-hours in a regular maintenance window | | | | |
| Date: | Completed by: | Signature: | | |

Control Objectives Group 4 – “Backdoor” Network Connections

| CO.4.1 - Additional connectivity between protected network and Internet | | | | |
|---|---|---------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Examine architecture documents and interview network manager to determine if there additional connections between the local protected network and the Internet | There are no connections from the local protected network other than through the firewall | DR/I | S | Non-Compliant |
| b) Examine architecture documents and interview network manager to determine if there are additional connections to the Internet from any of the regional offices | There are no connections from the regional office networks other than through the firewall | DR/I | S | Compliant |
| c) Examine architecture documents and interview network manager to determine if there are additional connections from protected network systems to the Internet through a 3 rd party ISP | No internal network systems have Internet connections directly to a 3 rd party ISP | DR/I | S | Compliant |
| d) Examine architecture documents and interview network manager to determine if there are additional connections from standalone systems to the Internet through a 3 rd party ISP | No standalone systems have Internet connections directly to a 3 rd party ISP | DR/I | S | Non-Compliant |
| e) If (d) is non-compliant, interview the network manager to ensure that there is a procedure to ensure that data transfer between systems is controlled and secure and that all data is scanned for viruses before being moved between systems | There are documented procedures and implemented measures to ensure that transfer of data between a stand-alone ISP system and the protected network systems is either expressly forbidden or controlled to ensure all data is free of viruses, etc. | DR/I | S | Compliant |
| f) Interview network manager and examine results of war-dialing conducted in the most recent overall network security audit to determine if | There are no modems connected to computers on the internal network | DR/I | S | Compliant |

| | | | | |
|---|---|-------------------|---|-----------|
| there are modems on the network | | | | |
| g) Conduct an NMAP scan of the entire external subnet range allotted to CFG to determine the devices with "live" Internet connections. | There should be no devices in the subnet range allotted to CFG other than the ISP screening routers and the firewall | T | O | Compliant |
| <p>Comments:</p> <p>Ref. (e):</p> <ol style="list-style-type: none"> 1. There are stand-alone systems in the Informatics area and the operations center that connect to the Internet via a commercial high speed Internet provider. 2. All of these systems run locked-down configuration and personnel firewalls. The connection is made through a Linksys (home office) router that has basic firewall capabilities. 3. The systems have static IP addresses on the subnet behind the router. The IP addresses use different subnet IDs than the production network systems. 4. The local administrator password is known only to the IT manager and all removable media in these systems (CDROM, Floppy Disk etc.) have been disabled. 5. There are documented operating procedures stating that no data can be moved between these systems and the production network. <p>Ref. (f): A team of outside security consultants performed war-dialing as part of a recent overall network security review. The network architects were not willing to allow this to be conducted again but they did show me the war-dialing report stating that there are no modem connections from network attached systems</p> | | | | |
| Date: | Completed by: | Signature: | | |

© SANS Institute 2003, Author retains full rights.

Control Objective Group 5 – Configurable Services

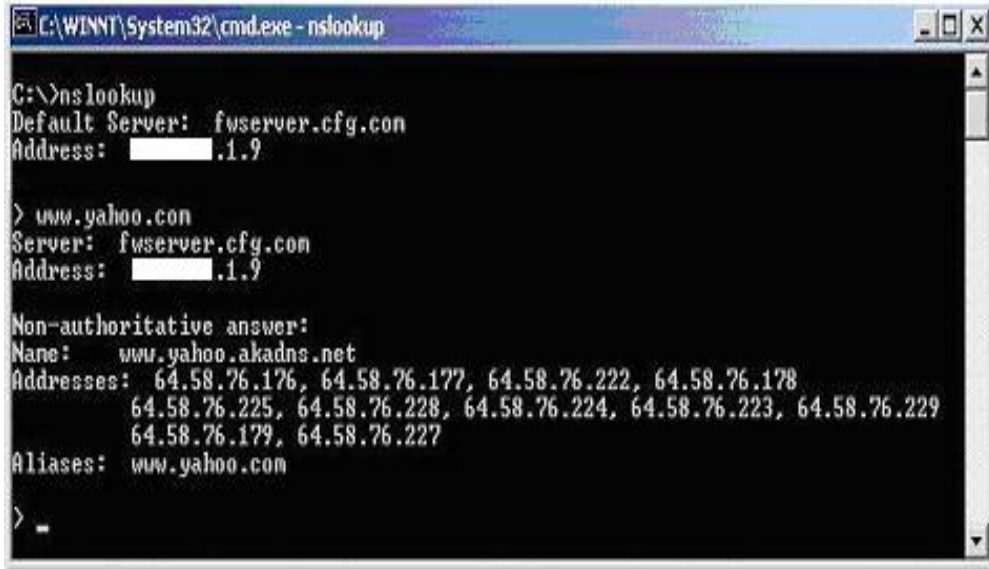
| CO.5.1 - Network Address Translation (NAT) | | | | |
|---|--|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC select Admin to examine the configuration of the firewall interfaces | The SSN and protected interfaces are using private IP addressing schemes | O | O | Compliant |
| b) In BWC select Admin to examine the configuration of the firewall interfaces. | The external interface of the firewall uses a public IP address | O | O | Compliant |
| c) Make a connection (e.g. Ping) from the internal host to the external host. Ensure the external host is running the Ethereal protocol analyzer program and examine the packet capture. | In the packet capture, the source IP address of the ping request (and the destination address for the reply) is the external interface of the firewall | T | O | Compliant |
| d) Make an HTTP connection (http://xx.yy.1.9) from the external host to the external interface of the firewall. | HTTP connection is re-directed to the web pages on the SSN server. | T | O | Compliant |
| e) From the external host, attempt an HTTP connection (http://10.0.0.2) directly to the SSN web server. Ensure that Ethereal protocol analyzer is running on the SSN web server | This should not be possible as the firewall will not allow connections directly from the external network to resources in the SSN. | T | O | Compliant |
| f) Examine the results of the packet capture from (e) | The packet capture will display no packets from the external host | T | O | Compliant |
| Comments: All tests display that NAT is enabled and according to Borderware product documentation [Ref.16] NAT cannot be disabled. | | | | |
| Date: | Completed by: | Signature: | | |

| CO.5.2 - Name Server (DNS) | | | | |
|--|---|---------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC, click on Internal under Servers and examine the check boxes for each server | DNS Queries are enabled on the internal interface | O | O | Compliant |
| b) In BWC select DNS Forwarders under Name Server . (Fig 7 shows the top level DNS Name Server configuration menu.) | The IP address of the DNS forwarder is that of the ISP DNS server address as verified by the firewall administrator | O | O | Compliant |
| c) In BWC under Name Server select Domains and then select Internal-Forward | There is a domain hosted on the internal interface | O | O | Compliant |
| d) Use NSLOOKUP to resolve DNS for an Internet resource (www.yahoo.com) from the internal host using the internal interface of the firewall as the DNS server for the host | DNS resolution for an Internet host is possible | T | O | Compliant |
| e) Use NSLOOKUP to resolve DNS for an Internet resource (www.yahoo.com) from the internal host using the ISP's DNS server as the DNS server for the host | DNS resolution for an Internet host is <u>not</u> possible | T | O | Compliant |
| f) Use NSLOOKUP to resolve DNS for an internal host from an internal host using the internal interface of the firewall as the DNS server for the host | DNS resolution for an internal host is possible | T | O | Compliant |
| g) Use NSLOOKUP to resolve DNS for an internal host from the external host using the external interface of the firewall as a DNS server. | DNS resolution for an internal host is <u>not</u> possible | T | O | Compliant |
| h) Use NSLOOKUP to resolve DNS for an Internet resource (www.yahoo.com) from the external host for | DNS resolution for Internet hosts is <u>not</u> possible | T | O | Non-compliant |

3/6/2003 9:15 AM

| | | | | |
|--|----------------------|-------------------|--|--|
| using the external interface of the firewall as a DNS server | | | | |
| Comments: Ref. (h): From the external host, it was possible to use the DNS server on the external interface of the firewall to query Internet resources. This is displayed in Figure 19. Further testing from a host connected to a 3 rd party ISP revealed that the firewall external interface allows all Internet hosts to issue DNS queries. | | | | |
| Date: | Completed by: | Signature: | | |

Fig. 19: NSLOOKUP on external host using external firewall interface DNS server



```

C:\WINNT\System32\cmd.exe - nslookup

C:\>nslookup
Default Server: fwserver.cfg.com
Address: 1.9

> www.yahoo.com
Server: fwserver.cfg.com
Address: 1.9

Non-authoritative answer:
Name: www.yahoo.akadns.net
Addresses: 64.58.76.176, 64.58.76.177, 64.58.76.222, 64.58.76.178
           64.58.76.225, 64.58.76.228, 64.58.76.224, 64.58.76.223, 64.58.76.229
           64.58.76.179, 64.58.76.227
Aliases: www.yahoo.com

> _

```

| CO.5.3 - Email Server (SMTP) | | | | |
|---|---|---------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Servers , examine the enabled servers (check box) under Internal Servers and External Servers | SMTP server is enabled on both Interfaces | O | O | Compliant |
| b) In BWC, under Proxies , select Internal and click on Internal to External to examine the enabled proxies | The SMTP proxy is <u>not</u> enabled. | O | O | Compliant |
| c) To ensure that the firewall will deliver incoming mail to only the corporate mail server, in BWC, under Mail Server , select Routing . Right-click on the configured internal domain (CFG) and select Modify to examine the Sub-domain mail routing and the Delivery configuration. Figure 8 shows the top level Mail Server menu. | The firewall is configured to only deliver mail destined for the CFG.com domain. All mail will be delivered to the IP address of the Corporate mail server under Deliver Via Host . | O | O | Compliant |
| d) To ensure that the corporate mail server will deliver outbound mail to only the firewall Examine its Internet mail configuration | The corporate mail server is configured to send all outgoing SMTP mail to only the firewall | O | O | Compliant |
| e) To verify that the corporate mail server can only deliver outbound mail to the firewall, on the mail server, temporarily configure the Internet mail connector to deliver mail via DNS (as opposed to delivering via the firewall internal interface). Attempt to send an email from the Corporate Mailbox to the Internet Mail Account. (NB: Ensure that the mail server configuration is returned to its previous state | This should not be possible as the firewall should not have the SMTP proxy enabled. | O | O | Compliant |

| | | | | |
|--|--|---|---|-----------|
| immediately after this test) | | | | |
| Test (f), (g) and (h) will verify that SMTP functions on the firewall internal interface | | | | |
| f) To verify that SMTP is configured to send mail from the firewall internal interface to the internal network, in BWC, select Mail Server and under Network Diagnostics , select the check box next to Send Test Mail . Send the test mail to the Corporate Mailbox and verify that the message was received. (see Figure 9) | The mail will be received in the corporate mailbox | T | O | Compliant |
| g) To verify that firewall SMTP server is configured to receive mail on the internal interface, from the Corporate Mailbox send an email to postmaster@cfg.com . Examine the firewall mail logs to verify the mail was received by the firewall. (see Figure 10) | In BWC, the mail log under Logs – View Logfiles will show the mail was received by the firewall | T | O | Compliant |
| h) To verify that firewall SMTP is configured is to forward mail received on the internal interface to the Internet, send an email from the corporate mailbox to the Internet Mail Account and verify receipt. | The mail will be received by the Internet mail account and the mail headers will show that the mail was sent from the firewall external interface (sender is the corporate mailbox) | T | O | Compliant |
| Test (i), (j) and (k) will verify that SMTP functions on the external interface | | | | |
| i) To verify that SMTP is configured to send mail from the external interface, in BWC, select Mail Server and under Network Diagnostics select the check box next to Send Test Mail . Send the test mail to the Internet Mail Account and verify that the message is received. | The mail will be received by the Internet mail account and the mail headers will show that the mail was sent from the firewall external interface (sender is the postmaster mailbox) | T | O | Compliant |
| j) To verify that SMTP is configured to receive mail on the external | In BWC, the mail log under Logs – View Logfiles will show the | T | O | Compliant |

| | | | | | |
|---|---|---|---|---|---------------|
| | interface, from the External SMTP Client, send an email to postmaster@cfg.com . | mail was received by the firewall | | | |
| k) | To verify that SMTP is configured is configured to forward mail received on the external interface to the corporate mail server, send an email from the external SMTP client to the corporate mailbox. | The mail will be received in the corporate mailbox | T | O | Compliant |
| Test (l) and (m) will verify that the internal interface can not be used to forward Spam mail generated on the internal network | | | | | |
| l) | To ensure that the Internal SMTP server is configured to receive SMTP mail from only the corporate mail server, In BWC under Servers , select Internal and right click on SMTP Mail in the main window. Select Modify and examine the access rules Click on the Access Rule tab, select Edit and select the Source Addresses tab. | A specific access rule exists for SMTP (as opposed to the initial default rule) and the list of allowed IP addresses should contain only that of the corporate mail server. (See Figure 11) | O | O | Non-compliant |
| m) | To verify the Firewall will not permit internal Spam mail to the Internet, send an email from the Internal SMTP client to the Internet Mail Account. | The mail should not arrive at the Internet mail account's mailbox. If it does, examine the headers to determine whether the message was received from the firewall external interface. | T | O | Non-compliant |
| Test (n) and (o) will verify that the internal interface can not be used to relay Spam mail generated on the Internet | | | | | |
| n) | To ensure that the SMTP server is configured not to relay mail on its external interface, in BWC, under Mail Server , select General and examine the Block Mail Relaying on the External Interface check box | Block Mail Relaying on the External Interface should be selected | O | O | Non-compliant |
| o) | To verify that mail relaying is not permitted on the external interface, | The mail should not arrive at the Internet mail account's mailbox. | T | O | Non-compliant |

| | | | | |
|---|--|-------------------|---|---------------|
| from the External SMTP Client, send an email to the Internet Mail Account. | If it does, examine the headers to determine whether the message was received from the firewall external interface. | | | |
| p) To verify mail size limits, in BWC, under Mail Server , select General and ensure determine whether the Limit mail message size checkbox is selected. | The box should be selected and the value should be typically no bigger than 2-3mb but that will depend on available bandwidth and capacity of the mail server to deal with large attachments | O | O | Non-compliant |
| <p>Comments:</p> <p>Ref. (l) & (m): The SMTP server on the internal interface of the firewall does not limit connection based on source IP address. Thus it does not limit the SMTP hosts that can connect to it. A Microsoft Outlook Express client on the internal network configured as in Figure 20 and 21 was able to send email from a bogus email domain to a legitimate Internet Email account. Figure 22 shows the email headers at the recipient.</p> <p>Ref. (n) & (o): The SMTP server on the external interface does not block relaying of email (Figure 23). A Microsoft Outlook Express client on the external network configured as in Figure 24 and 25 was able to send email from a bogus email domain to a legitimate Internet Email account. Figure 26 shows the email headers at the recipient</p> <p>Ref. (o): There are no size limitations configured in the firewall SMTP server (Also shown in Figure 23)</p> | | | | |
| Date: | Completed by: | Signature: | | |

© SANS Institute 2003, Author retains full rights.

Fig. 20: Internal SMTP client configuration (1)

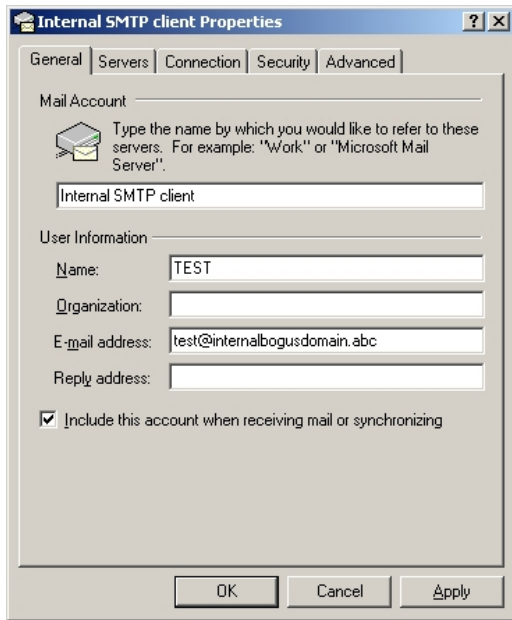
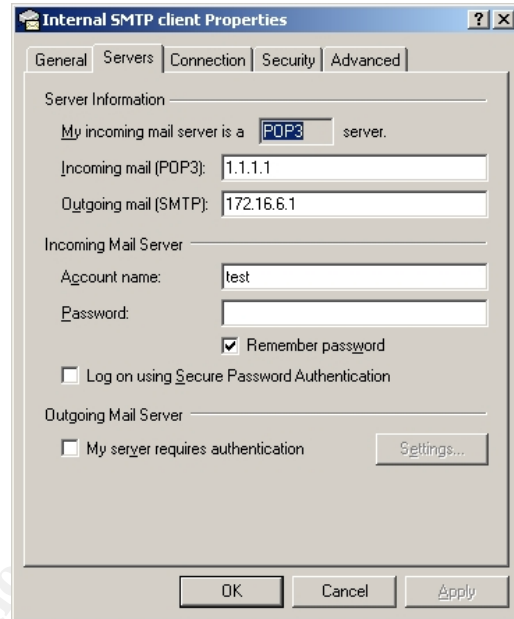


Fig. 21: Internal SMTP client configuration(2)



3/6/2003 9:15 AM

Fig. 22: Email headers on email received by Internet Email account from internal SMTP client bypassing corporate email server

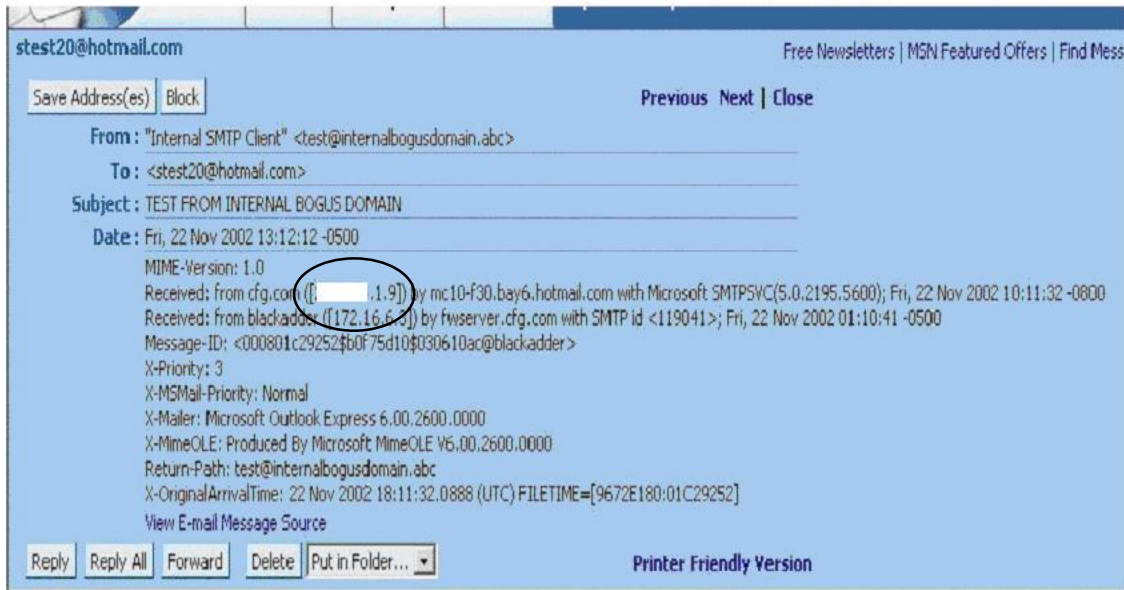
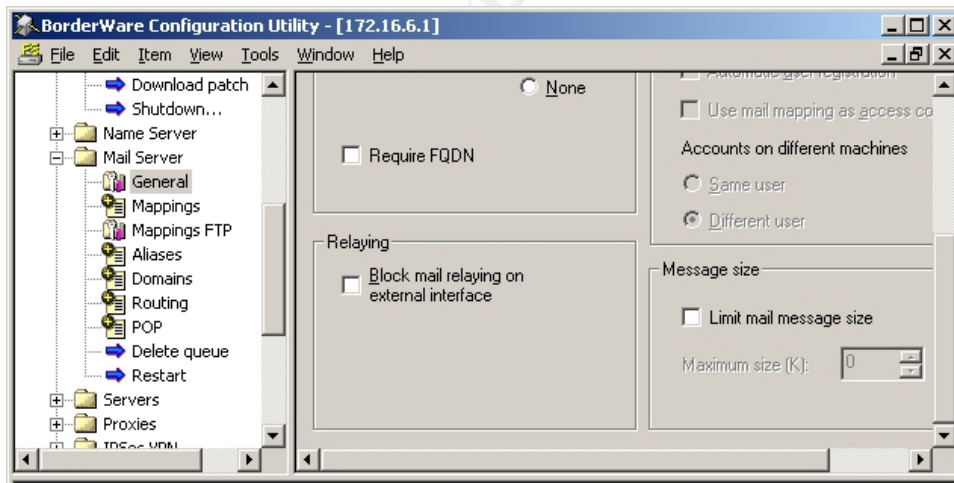
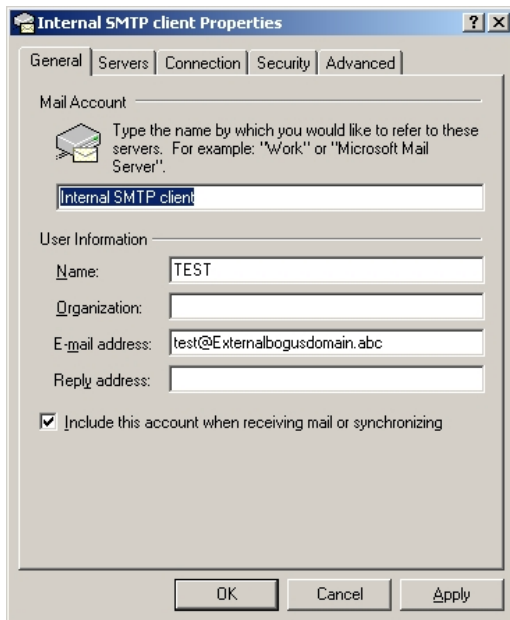
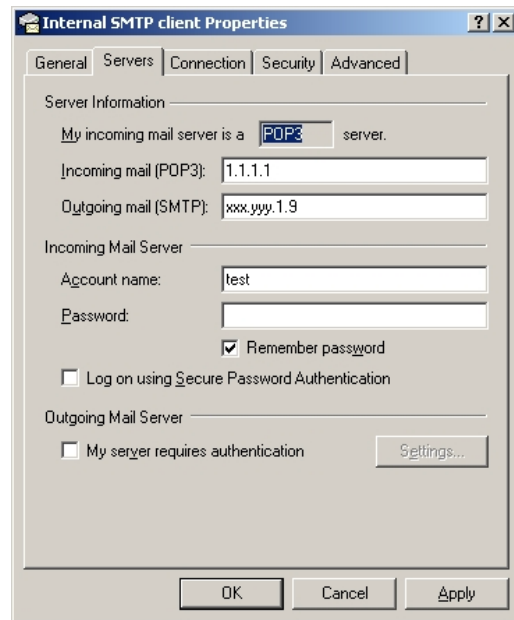
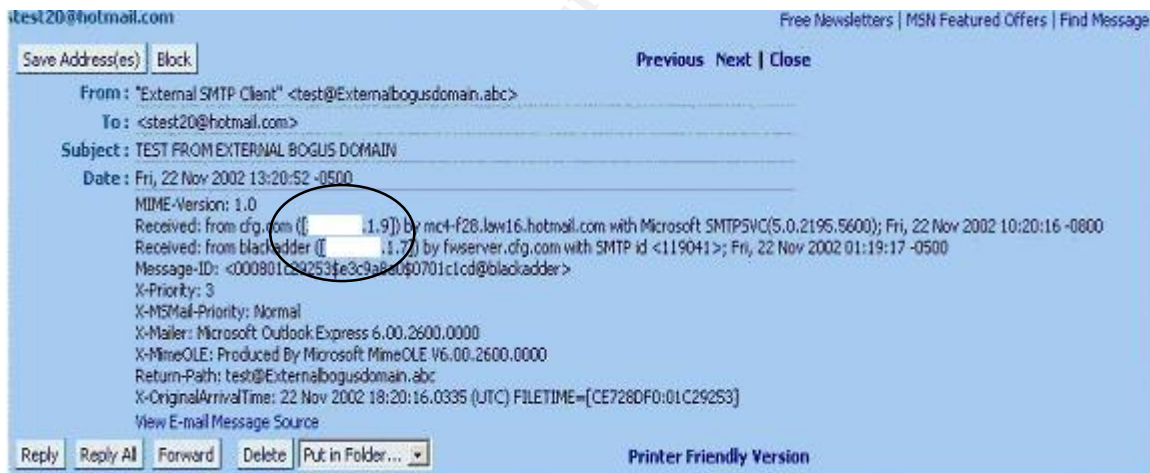


Fig. 23: Firewall external interface relay and email size settings



3/6/2003 9:15 AM

Fig. 24: External SMTP client configuration (1)**Fig. 25: External SMTP client configuration (2)****Fig. 26: Email headers on email received by Internet Email Account from external SMTP client using firewall external interface as a email relay**

| CO.5.4 - Squid Proxy Server (HTTP) | | | | |
|---|---|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In the Proxies menu, select Internal and the select Internal-to External and examine the enabled proxies | The WWW proxy is disabled | O | O | Non-compliant |
| b) Under the Proxies menu, select Proxy Server and then select Server Settings (see Figure 12) and examine the proxy server settings under Service | Enable Service check box is selected. Enable with caching is selected in the Internal-to External drop down menu Enable Authentication checkbox is disabled | O | O | Non-Compliant |
| c) Under the Proxies menu, select Proxy Server and then select Server Settings (see Figure 12) and examine the proxy server settings under Proxy mode | The transparent check box is enabled under Proxy Mode to ensure users do not need to authenticate or specify the proxy server in their browsers | O | O | N/A |
| d) From the Internal host, attempt to access http://www.sans.org without modifying the browser's default settings. | The site should be accessible | T | O | Compliant |
| e) Run Ethereal protocol analyzer on the external host when HTTP requests are made from the internal host to determine the source IP address of HTTP requests | HTTP traffic leaving the network has the external interface of the firewall as its source address | T | O | Compliant |
| Comments: Ref (a), (b) (c): The firewall is configured to use only the simple HTTP proxy enabled as Internal-to-External (see Figure 27). The Squid Proxy server is not being used at all (see Figure 28). While, functionally, this allows the users to access the Internet as required, there will be no opportunity to enable authenticated Internet access and there is no caching of frequently accessed pages to speed up access | | | | |
| Date: | Completed by: | Signature: | | |

Fig. 27: Simple WWW proxy enabled

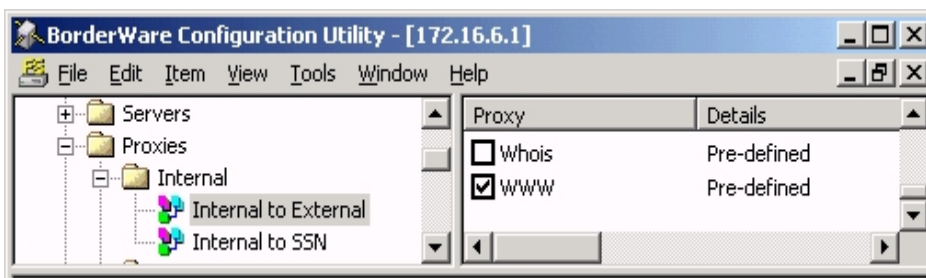
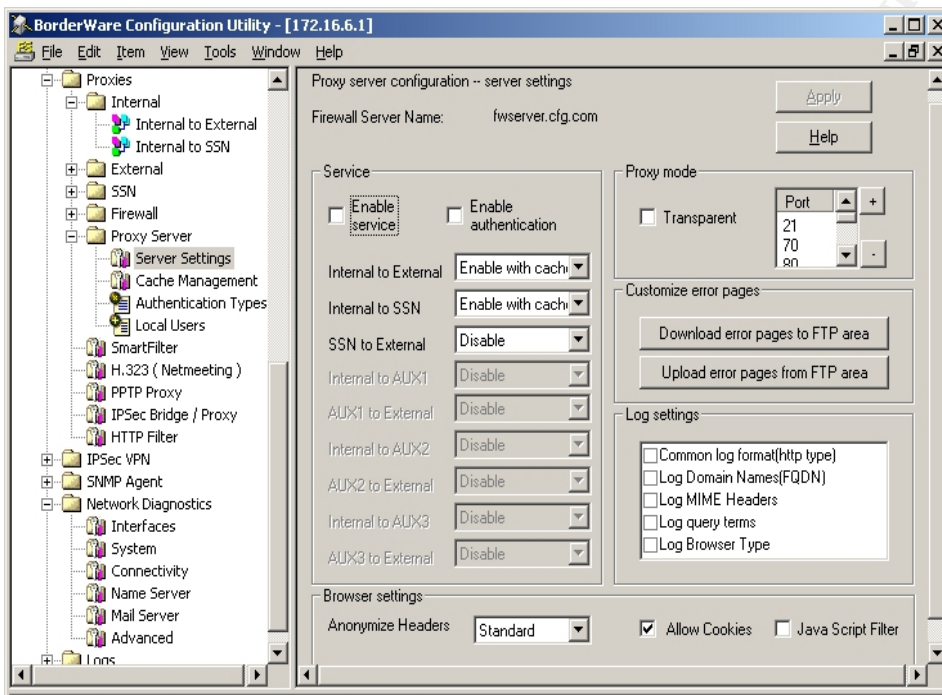


Fig. 28: Squid Proxy disabled



| CO.5.5 - HTTP Filter | | | | |
|---|--|-------------------|-----|------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC, Examine the HTTP Filter (see Figure 6) settings under Proxy Server | HTTP Filtering is enabled and the code red file patterns are in the filter list. | O | O | Compliant |
| Comments: Http filters for Code Red are enabled | | | | |
| Date: | Completed by: | Signature: | | |

| CO.5.6 - Smart Filter (URL Filtering Software) | | | | |
|--|---|---------------|------------|---|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) To ensure the service is enabled, in BWC, access the Smartfilter menu under Proxies | The smart Filter Service is enabled | O | O | Compliant |
| b) To ensure database downloads occur, under Smartfilter subscription , examine the date of the last download. | The last download of filter database should take place within one week prior to the date of testing | O | O | Compliant |
| c) To ensure a manual download is possible, select Download Control List | A manual download of the latest filter database is initiated | T | O | Compliant |
| d) From a web browser on the internal host, attempt to access a range of gambling, pornographic, racist, violent, anarchist and sexist websites | Access to these sample sites is blocked by the filter and a message in the browser window states why this has happened. <ul style="list-style-type: none"> • http://come.to/anarchy • www.bingo.com • www.sexist.com | T | O | <ul style="list-style-type: none"> • Compliant • Non-compliant • compliant |
| e) Interview helpdesk staff and firewall administrators to determine the history of false negatives (unacceptable sites allowed by the URL filter that have warranted manual editing of URL filter database) | Helpdesk personnel will report minimum incidents of false negatives | I | S | Non-compliant |
| f) Attempt to access a range of acceptable business related web sites such as government, technology, and university web sites to determine if the filter blocks access or | Browser is granted access to these sample sites: <ul style="list-style-type: none"> • www.canada.gc.ca • www.uottawa.ca • www.nortelnetworks.com | T | O | <ul style="list-style-type: none"> • Compliant • Compliant • Compliant |
| g) Interview helpdesk and firewall administrators to | Helpdesk personnel report minimum incidents of false negatives | I | S | Compliant |

| | | | | |
|---|--|-------------------|---|---------------|
| determine history of false positives (acceptable sites blocked by URL filter) that have warranted manual editing of URL filter database) | | | | |
| h) From the internal host attempt access to web-based email sites such as www.hotmail.com, etc. | Browser is granted access to these sites | T | O | Non-compliant |
| Comments: Ref (a): Service is enabled and download took place within the last week Ref. (d): Some sites that are deemed unacceptable by corporate policy were accessible from the internal network. Ref. (e): Helpdesk reports that no calls have been received to request a site to be blocked but did report that in the case of the large majority of pornographic Spam email that gets through to users, any web site links in the Spam are allowed for a short period of time (until the URL filter updates its database). These sites are then usually manually blocked. Ref. (f) & (g): While all legitimate sites attempted were allowed by the filter, Helpdesk reports that approximately 1% of support calls are to unblock sites that are deemed acceptable by corporate policy Ref. (g): Internal network users are allowed to send and receive free web-based email such as hotmail. | | | | |
| Date: | Completed by: | Signature: | | |

| CO.5.7 - Additional configurable services that are not mentioned in firewall policy | | | | |
|--|---------------------------------------|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Examine H.323 (Netmeeting) settings | Service is not enabled | O | O | Compliant |
| b) Examine PPTP Proxy settings | Service is not enabled | O | O | Compliant |
| c) Examine IPSEC Bridge/Proxy settings | Service is not enabled | O | O | Compliant |
| d) Examine IPSEC VPN settings | Service is not enabled | O | O | Compliant |
| e) Examine SNMP Agent settings | Service is not enabled | O | O | Compliant |
| Comments: As per policy requirements, none of the above services are enabled or configured | | | | |
| Date: | Completed by: | Signature: | | |

Control Objectives Group 6 – Network Access for Firewall Administration

| CO.6.1 – Security of Remote Management Interfaces on Firewall | | | | |
|---|--|---------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Admin select System Settings and examine the selected interfaces under Remote Management | Only the Internal (Secured) check box is selected. The other check boxes (Internal (unsecured) , External and SSN are not checked (O) | O | O | Non-compliant |
| b) To verify that secure Remote Management is enabled on the internal interface, attempt to initiate an SSL Remote Management (BWC) session from an internal host (check the SSL Encrypted Session box when specifying the server as shown in Figure 13) | Remote management is possible on the Internal interface using SSL | T | O | Compliant |
| c) To verify that secure Remote Management is <u>not</u> enabled on the external interface, attempt to initiate an SSL Remote Management (BWC) session from the external host (check the SSL Encrypted Session box when specifying the server) | Remote management is not possible on the external interface using SSL | T | O | Compliant |
| d) To verify that secure Remote Management is <u>not</u> enabled on the SSN interface, attempt to initiate an SSL Remote Management (BWC) session from the SSN host (check the SSL Encrypted Session box when specifying the server) | Remote management is not possible on the SSN interface using SSL | T | O | Compliant |
| e) To verify that Clear Text Remote Management is <u>not</u> enabled on the internal interface, attempt to initiate a clear text Remote Management (BWC) session from the internal host (uncheck the SSL Encrypted Session box when specifying the server) | Remote management is not possible on the Internal interface using clear text | T | O | Non-Compliant |
| f) To verify that Clear Text | Remote | T | O | Compliant |

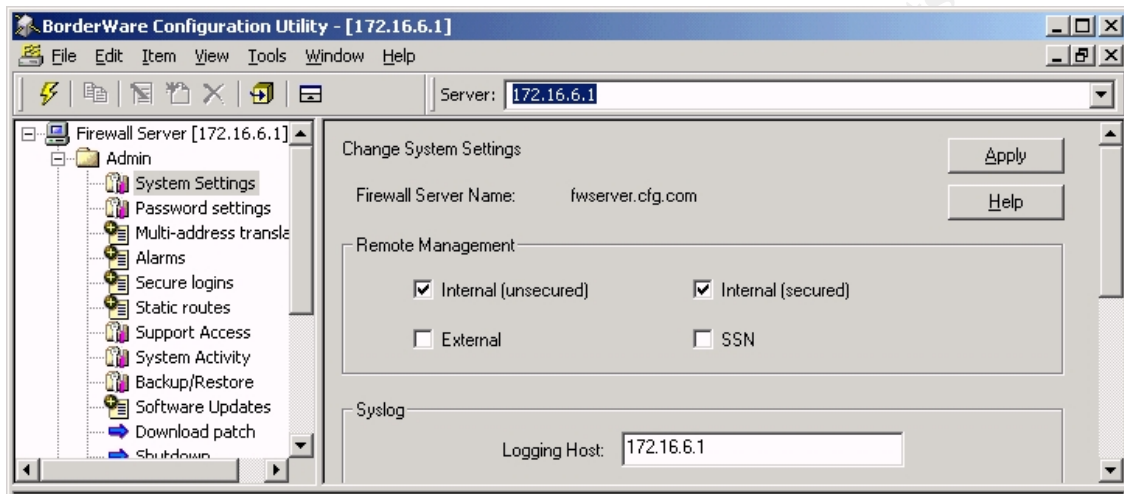
| | | | | | |
|--|--|--|---|---|---------------|
| | Remote Management is <u>not</u> enabled on the external interface, attempt to initiate a clear text Remote Management (BWC) session from the external host (uncheck the SSL Encrypted Session box when specifying the server) | management is not possible on the SSN interface using clear text | | | |
| g) | To verify that Clear Text Remote Management is <u>not</u> enabled on the SSN interface, attempt to initiate a clear text Remote Management (BWC) session from the SSN host (uncheck the SSL Encrypted Session box when specifying the server) | Remote management is not possible on the External interface using clear text | T | O | Compliant |
| h) | At the firewall console, examine the Secure Logins configuration in the Admin menu to determine the specific Admin Users configured for Remote Management (Figure 14) | There should be one user name for each firewall administrator | O | O | Non-Compliant |
| i) | To verify that user ACLs have been applied, from BWC on the internal host, attempt a Remote Management session bypassing the login screen | It should not be possible to bypass the login screen | T | O | compliant |
| j) | To determine if IP address ACLs have been applied, in BWC , under Servers , select Internal Servers , right click Secure GUI Config and select Modify . | The access rules should contain a rule that limits source addresses to particular IP addresses | O | O | Non-Compliant |
| k) | To verify IP address based ACLs exist, attempt to perform Remote Management from user workstations on the network | It should only be possible to perform Remote Management from specific workstations specified by the firewall administrator | T | O | Non-compliant |
| Comments: Ref. (a) & (e): Remote Management is enabled on only the internal interface. It has been enabled so that it can be accessed using clear text as well as SSL (Figure 29). Ref (c) & (f): According to Borderware Product Documentation ⁶¹ Remote Management is not possible from the external network or the Internet without some form of encryption based on a hardware token such as Crypto Card or SecureID. Ref. (g): Only one Remote administration user account has been created and each firewall | | | | | |

administrator uses the same credentials. According to the Borderware Technical Support, multiple remote administration accounts can be created but they must all use the Admin password configured at install (also used for direct access to firewall console)

Ref. (f): There are no IP address-based ACLs assigned to the Remote management server on the internal interface and the option to do so is grayed out. According to Borderware Technical Support, it is not possible to assign this sort of ACL to either secure or clear text Remote Management

| | | |
|--------------|----------------------|-------------------|
| Date: | Completed by: | Signature: |
|--------------|----------------------|-------------------|

Fig. 29: Interfaces enabled for Remote Management

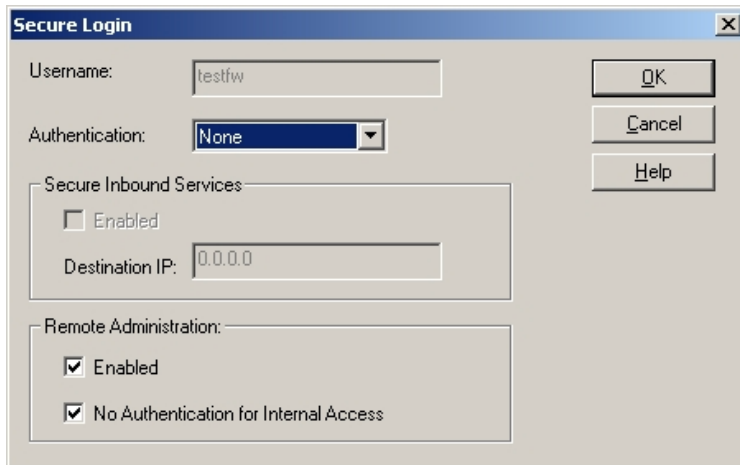


CO.6.3 - Two factor authentication for Remote Management

| Test | Expected Result for Compliance | Method | O/S | Compliance |
|--|---|--------|-----|---------------|
| a) In BWC, under the Admin menu, select Secure Logins , double click the configured user account and examine the authentication options to determine if Crypto Card is selected (Figure 15) | Under Authentication in Figure 15 CryptoCard will be listed | O | O | Non-compliant |
| b) Attempt to perform Remote Management from a workstation using only username and password as credentials. | Remote Management using only user name and password will not be possible if the user account requires Cryptocard authentication | T | O | Non-compliant |
| c) Examine the Remote Management workstations to determine if they are equipped with Crypto-card readers | Remote Management workstations will have crypto card readers attached | O | O | Non-compliant |
| Comments: Ref. (a): Authentication for Remote Management is based only on username and password | | | | |

| | | |
|-----------------------------|----------------------|-------------------|
| credentials (see Figure 30) | | |
| Date: | Completed by: | Signature: |

Fig. 30: Remote management authentication



Control Objectives Group 7 – Firewall Management

| CO.7.1 - Firewall Patches and Fixes | | | | |
|--|--|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC, select Software Updates in the Admin menu to determine the patches installed on the firewall. From the Download Patch utility in the Admin menu determine the patches available for the firewall (see Figure 16). | All available patches in the Download Patch utility will display as being installed in the Software Updates menu | O | O | Non-compliant |
| e) Examine release notes to determine if outstanding patches are relevant to the configuration employed on this firewall | Any outstanding patches will not be relevant to this particular configuration | DR | O | Non-compliant |
| f) Conduct an interview with the firewall administrator to determine whether a documented procedure and schedule exists for patch downloads and updates. | Documented procedure and schedule exists for patch downloads and updates | I | S | Non-compliant |
| g) Conduct an interview with the firewall administrator to determine whether CFG receives regular notification of new patches from the firewall manufacturer | The firewall manufacturer regular notifies the firewall administrator or new patches | I | S | Compliant |
| Comments: Ref. (a): There were 2 available patches (URLfilter and fs65s01) that had not been installed on the firewall (see Figure 31 and 32). | | | | |
| Date: | Completed by: | Signature: | | |

Fig. 31: Installed patches on firewall

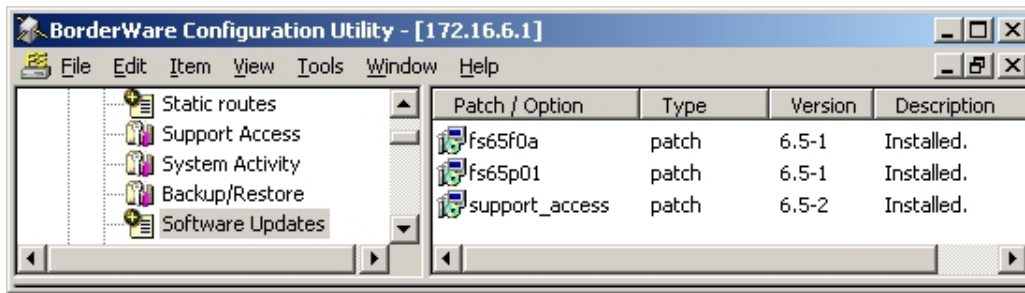
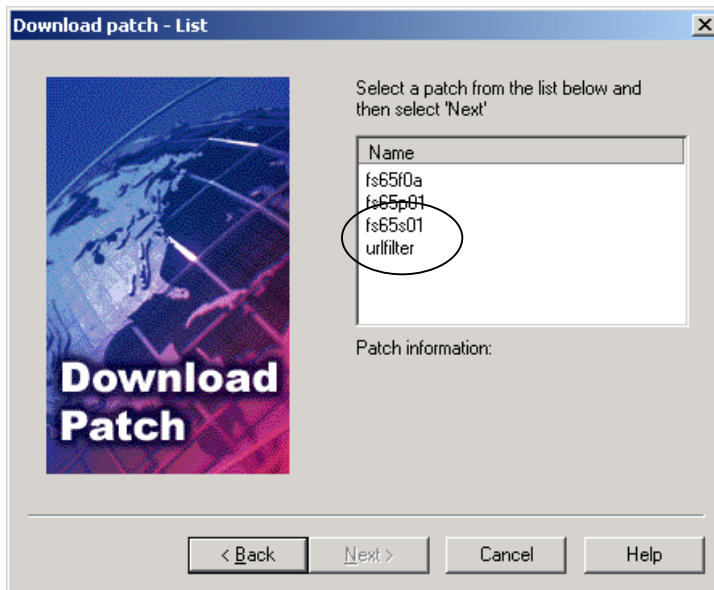


Fig. 32: Patches available on Borderware download site.



| CO.7.2 - Firewall Logging and alarms | | | | |
|---|---|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Conduct interviews with firewall administrators to determine if logs are reviewed | Administrator states logs are reviewed regularly | O | O | Compliant |
| b) In BWC, examine Alarms in the Admin menu to determine if alarm conditions are set when attack patterns are generated and if notification is turned on (see Figure 17) | Alarms are enabled on the firewall and the firewall administrators and firewall manager are emailed when an alarm is triggered | I | S | Compliant |
| c) From the external host, run NMAP against the external interface of the firewall to determine if alarms are generated | NMAP scans on the external interface cause alarms to appear on the console screen, create entries in the alarm logs and automatically email the firewall administrators | T | O | Compliant |
| d) Observe the firewall administrator to determine if alarms are monitored and if action is taken | The firewall administrator observes the attack and examines packets and source IP prior to notifying the firewall manager | O | O | Compliant |
| e) Conduct an interview with the firewall manager to determine if documented procedure exists for when attack patterns are generated in the log file or for when alarms are triggered | Documented procedure exists to deal with attack patterns determined from log files and alarm notifications | I | S | Non-compliant |
| Comments: Ref. (e): There are no documented procedures to deal with potential attacks indicated in the log files or by the alarm system. Ref. (b) & (d): Alarm notification is enabled to email all firewall administrators and the helpdesk when unused ports are accessed more than 6 times in 8 minutes. By running generic Nmap scans on the external interface, emails were sent to the firewall administrator and helpdesk mailboxes. The firewall administrators then contacted the firewall manager to report potential attack patterns. | | | | |
| Date: | Completed by: | Signature: | | |

| CO.7.3 - Remote Firewall Logging | | | | |
|--|---|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC, under Admin , select System Settings and determine the IP address entered for Logging Host under the Syslog field | IP address in Syslog field will be a secure server on the local network running Syslog software | O | O | Compliant |
| b) Examine the Syslog server configuration and data to ensure that firewall data is written to the Syslog server | Firewall logs are written to the Kiwi Syslog server | O | O | Compliant |
| Comments: | | | | |
| Ref (a): The firewall logs to the Kiwi Syslog server (See Figure 33) | | | | |
| Date: | Completed by: | Signature: | | |

Fig. 33: Extract from Kiwi Syslog Daemon log running on Management Server

| | | | | | |
|---------------------|---------------------|------------|----------------------|--------|----------|
| 2002-10-13 00:06:09 | Kernel.Critical | 172.16.6.1 | /kernel: ipfw: 41069 | Deny | UDP |
| 172.16.1.3:3505 | 172.16.255.255:1100 | in via xl1 | | | |
| 2002-10-13 00:06:09 | Kernel.Critical | 172.16.6.1 | /kernel: ipfw: 41069 | Deny | UDP |
| 172.16.1.1:1579 | 172.16.255.255:1100 | in via xl1 | | | |
| 2002-10-13 00:06:09 | Kernel.Critical | 172.16.6.1 | /kernel: ipfw: 41069 | Deny | UDP |
| 172.16.1.22:1121 | 172.16.255.255:1100 | in via xl1 | | | |
| 2002-10-13 00:06:09 | Kernel.Critical | 172.16.6.1 | /kernel: ipfw: 41069 | Deny | UDP |
| 172.16.10.2:2633 | 172.16.255.255:1100 | in via xl1 | | | |
| 2002-10-13 00:06:10 | Kernel.Critical | 172.16.6.1 | /kernel: ipfw: 41069 | Deny | UDP |
| 172.16.5.27:1033 | 172.16.255.255:1100 | in via xl1 | | | |
| 2002-10-13 00:06:10 | Kernel.Critical | 172.16.6.1 | /kernel: ipfw: 11002 | Accept | ICMP:8.0 |
| 172.16.7.0 | 172.16.6.1 | in via xl1 | | | |
| 2002-10-13 00:06:10 | Kernel.Critical | 172.16.6.1 | /kernel: ipfw: 11002 | Accept | ICMP:8.0 |
| 172.16.7.0 | 172.16.6.1 | in via xl1 | | | |
| 2002-10-13 00:06:10 | Kernel.Critical | 172.16.6.1 | /kernel: ipfw: 41069 | Deny | UDP |
| 172.16.10.1:3577 | 172.16.255.255:1100 | in via xl1 | | | |
| 2002-10-13 00:06:12 | Kernel.Critical | 172.16.6.1 | /kernel: ipfw: 41069 | Deny | UDP |
| 172.16.1.3:3505 | 172.16.255.255:1100 | in via xl1 | | | |
| 2002-10-13 00:06:12 | Kernel.Critical | 172.16.6.1 | /kernel: ipfw: 41069 | Deny | UDP |
| 172.16.1.1:1579 | 172.16.255.255:1100 | in via xl1 | | | |
| 2002-10-13 00:06:12 | Kernel.Critical | 172.16.6.1 | /kernel: ipfw: 41069 | Deny | UDP |
| 172.16.1.22:1121 | 172.16.255.255:1100 | in via xl1 | | | |
| 2002-10-13 00:06:12 | Kernel.Critical | 172.16.6.1 | /kernel: ipfw: 41069 | Deny | UDP |
| 172.16.10.2:2633 | 172.16.255.255:1100 | in via xl1 | | | |
| 2002-10-13 00:06:13 | Kernel.Critical | 172.16.6.1 | /kernel: ipfw: 11002 | Accept | ICMP:8.0 |
| 172.16.9.0 | 172.16.6.1 | in via xl1 | | | |
| 2002-10-13 00:06:13 | Kernel.Critical | 172.16.6.1 | /kernel: ipfw: 11002 | Accept | ICMP:8.0 |
| 172.16.9.0 | 172.16.6.1 | in via xl1 | | | |
| 2002-10-13 00:06:13 | Kernel.Critical | 172.16.6.1 | /kernel: ipfw: 41069 | Deny | TCP |
| 172.16.103.6:4373 | 172.16.6.1:53 | Syn in | | | |

| CO.7.4 - Firewall Log Backups | | | | |
|--|--|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Interview the firewall administrator to determine whether firewall logs are backed up regularly | Administrator states firewall logs are backed up daily with corporate data | U | S | Compliant |
| b) Interview the firewall administrator to determine if firewall log backup data is retained in accordance with the corporate backup strategy | Administrator states that firewall log data is retained according to corporate data retention policy | I | S | Compliant |
| Comments: Ref. (a): The firewall log files are backed up weekly and the Kiwi Syslog files which are on a management server are backed up nightly with other data on that server | | | | |
| Date: | Completed by: | Signature: | | |

| CO.7.5 – Support Access | | | | |
|---|---|---------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Admin , select Support Access and ensure that the Enable Access box is not checked | Enable Access is not checked | O | S | Compliant |
| b) Conduct an interview with the firewall administrator to determine under what circumstance Support Access is enabled | Administrator states that Support Access is enabled only when Borderware Technical Support personnel request and only when this is in response to an issue raised by the firewall administrator at CFG | I | S | Compliant |
| c) Contact Borderware Technical Support to determine risks associated with enabling Support Access. | A Borderware technical representative states that the product designers has taken steps to ensure that enabling support access will not compromise the firewall's security | I | S | Compliant |
| Comments: Ref. (b): Support access is enabled only when requested by Borderware Technical Support. Ref. (c): According to Borderware Technical Support, Support Access allows Remote Management of the firewall to be performed by Borderware Personnel. Support Access is protected by RSA host authentication, SSH encryption, passwords and IP address ACLS that only allow access to specific Borderware corporate hosts. Other than enabling or disabling it, the support access configuration is inaccessible from the Borderware administration utilities | | | | |

(console and BWC). Nessus vulnerability scans and NMAP port scans on the external interface with Support Access enabled did not reveal any additional vulnerabilities or open ports.

| | | |
|--------------|----------------------|-------------------|
| Date: | Completed by: | Signature: |
|--------------|----------------------|-------------------|

© SANS Institute 2003, Author retains full rights.

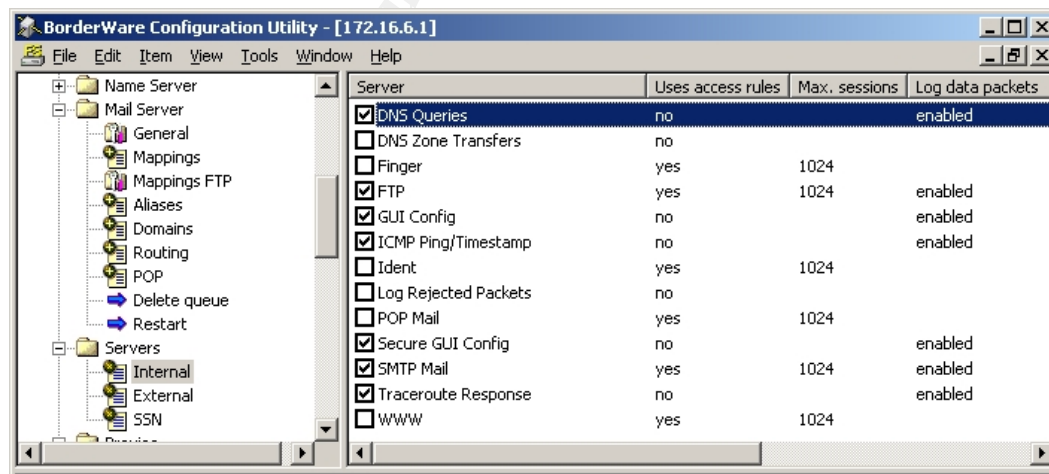
Control Objectives Group 8 – Firewall Rule base and Interfaces

| CO.8.1 - System default as Deny-all | | | | |
|--|---|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Interview firewall administrator to determine criteria for allowing new services or creating new rules | Firewall administrator states that new rules are enabled based on business needs presented to him by the firewall manager | I | O | Compliant |
| b) From product documentation and a test install of Borderware Firewall 6.5. determine default state of firewall rules | Default state of firewall rules is to deny all network traffic between network segments | T | S | Compliant |
| Comments: Ref. (b): As a test, a default installation of Borderware 6.5 was performed on an offline system. It was determined that the default state is to allow no traffic between any of the attached network segments. | | | | |
| Date: | Completed by: | Signature: | | |

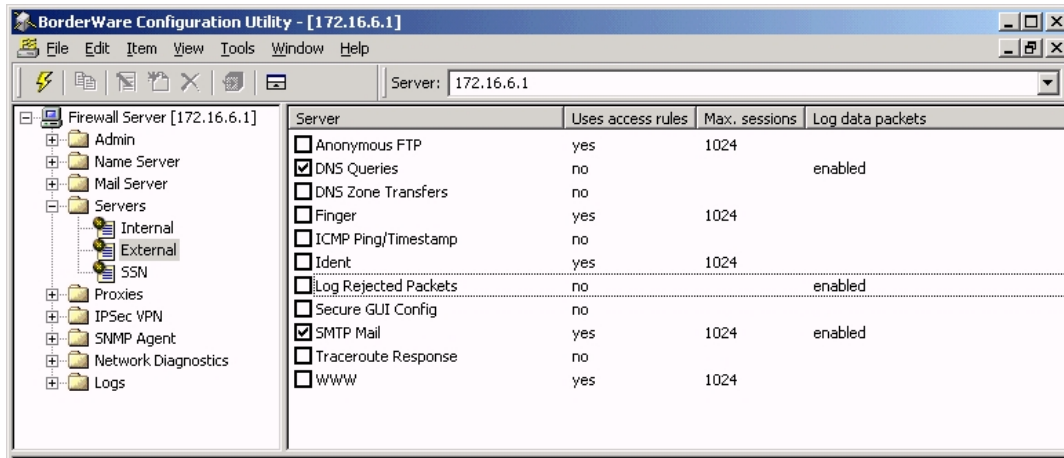
| CO.8.2 - Servers on Internal Interface | | | | |
|---|--|---------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Servers , examine the enabled Internal Servers to ensure that only the required servers are enabled | The following serves should be enabled: <ul style="list-style-type: none"> • DNS • Secure GUI Config • ICMP • Traceroute • SMTP | O | O | Compliant |
| b) Run Nmap from the Linux system against the internal interface of the firewall to determine open ports. | Only the ports corresponding to the servers in (a) should be open | T | O | Non-compliant |
| c) Run Nessus from the Linux system against the internal interface of the firewall to determine vulnerabilities associated with any open ports or enabled servers | There should be no vulnerabilities associated with open ports or services | T | O | Non-compliant |
| d) To verify that ICMP is running as expected, attempt to Ping and Traceroute from the internal host to internal interface of the firewall. | The Ping command should receive 4 replies from the firewall and the Tracert should show 1 or more "hops" to the destination and | T | O | Compliant |

| | | | | |
|---|---|-------------------|---|---------------|
| | indicate Trace Complete at the IP address of the firewall internal interface | | | |
| e) Enumerate results of visual examination of servers, Nmap scan results and Nessus scan results | No other servers should be enabled | T | O | Non-compliant |
| Comments: Ref. (b): Nmap port scans found the following unauthorized ports on the internal interface corresponding to servers (See Appendix 3 for full NMAP Scan results) i) TCP port 441 ii) TCP Port 21 Ref. (c): Nessus vulnerability scans on the internal interface reported vulnerabilities as follows (See Appendix 3 for full Nessus Scan results): i) The firewall internal interface allows recursive queries to be performed. Since this is the Internal DNS server and it is supposed to either respond to DNS queries or else forward them to the Internet, this issue can be ignored ii) The firewall internal interface answers to an ICMP timestamp request which could allow a hacker to determine the date set on the firewall and thus circumvent time-based security. iii) The firewall internal interface is using non-random IP address IDs which could allow someone running a packet sniffer to determine whether a packet is a reply to an existing request or a session initiation. Ref. (e): Examination of the internal servers found the following unauthorized servers enabled (see Figure 34): i) GUI Config (Clear text Remote Management) ii) FTP Server | | | | |
| Date: | Completed by: | Signature: | | |

Fig. 34: Internal Servers



| CO.8.3 - Servers on External Interface | | | | |
|--|---|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Servers , examine the enabled External Servers to ensure that only the required servers are enabled | Only SMTP server should be enabled | O | O | Compliant |
| b) Run Nmap from the Linux system against the external interface of the firewall to determine open ports. | Only the ports corresponding to the servers in (a) should be open | T | O | Non-compliant |
| c) Run Nessus from the Linux system against the external interface of the firewall to determine vulnerabilities associated with any open ports or enabled servers | There should be no vulnerabilities associated with open ports or services | T | O | Non-compliant |
| d) As the policy documents specifically deny ICMP on the external interface, this will be tested. To verify that ICMP is disabled, attempt to Ping and Traceroute from the external host to external interface of the firewall. | The Ping command will return Request Timed Out and while Tracert may show 1 or more "hops" to the destination, it will also indicate Request Timed Out and will not indicate Trace Complete | T | O | Compliant |
| e) Enumerate results of visual examination of servers in Nmap scan results and Nessus scan results to ensure that no other servers are enabled | No additional servers should be enabled | T | O | Non-Compliant |
| Comments: Ref. (c): Nessus detected DNS on the external interface responds to recursive queries for Internet resources from external hosts. (See Appendix 3 for full Nessus Scan results) Ref. (e): DNS appears as an unauthorized server on the external interface (see Figure 35) | | | | |
| Date: | Completed by: | Signature: | | |

Fig. 35: External Servers

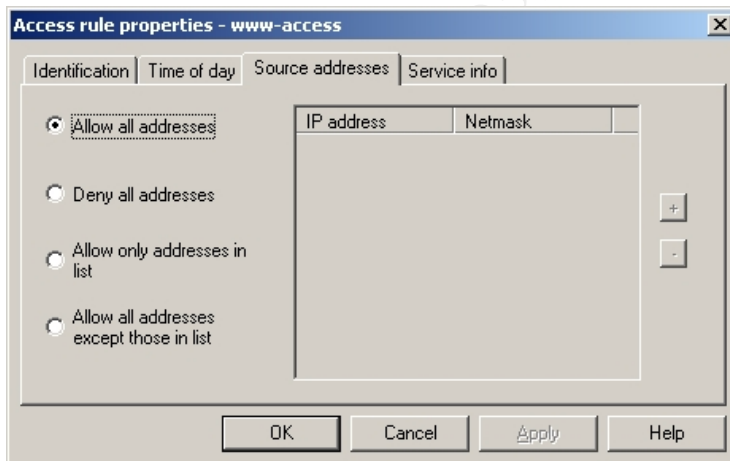
| CO.8.4- Servers on SSN Interface | | | | |
|--|---|-------------------|-----|------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Servers , examine the enabled SSN Servers to ensure that only the required servers are enabled | No Servers should be enabled | O | O | Compliant |
| b) Run Nmap from the Linux system against the SSN interface of the firewall to determine open ports. | Only the ports corresponding to the servers in (a) should be open | T | O | Compliant |
| c) Run Nessus from the Linux system against the SSN interface of the firewall to determine vulnerabilities associated with any open ports or enabled servers | There should be no vulnerabilities associated with open ports or services | T | O | Compliant |
| d) Enumerate results of visual examination of servers, Nmap scan results and Nessus scan results to ensure that no other servers are enabled (O) | No additional servers should be enabled | T | O | Compliant |
| Comments: As per corporate policy there are no servers enabled on the SSN interface | | | | |
| Date: | Completed by: | Signature: | | |

| CO.8.5 - External to Internal Proxies | | | | |
|---|--|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Proxies , select External and examine the firewall's External-to-Internal proxies to ensure that only the required proxies are enabled | No external-to-internal proxies should be enabled | O | O | Compliant |
| b) Run Nmap from the Linux system against the external interface of the firewall to determine open ports. | Only the ports corresponding to the proxies in (a) should be open | T | O | Compliant |
| c) Run Nessus from the Linux system against the external interface of the firewall to determine vulnerabilities associated with any open ports or enabled proxies | There should be no vulnerabilities associated with enabled proxies | T | O | Compliant |
| d) Enumerate results of visual examination of proxies, Nmap scan results and Nessus scan results to ensure that no other proxies are enabled | No additional proxies should be enabled | T | O | Compliant |
| e) Using Ethereal protocol analyzer on the internal host, capture traffic on the network segment while Nessus and Nmap scan the external interface. | Ethereal protocol analyzer running on the internal host detects no traffic patterns from the external host | T | O | Compliant |
| Comments: As per corporate policy there are no external-to-internal proxies running on the firewall | | | | |
| Date: | Completed by: | Signature: | | |

| CO.8.6 - External to SSN Proxies | | | | |
|--|---|---------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Proxies , select External and examine the firewall's External-to-SSN proxies to ensure that only the required proxies are enabled | The following external-to-SSN proxies should be enabled: <ul style="list-style-type: none"> WWW | O | O | Compliant |
| b) Run Nmap from the Linux system against the external interface of the firewall to determine open ports. | Only the ports corresponding to the proxies in (a) should be open | T | O | Compliant |
| c) Run Nessus from the Linux system against the external interface of the firewall to determine vulnerabilities associated with any open ports or enabled proxies | There should be no vulnerabilities associated with enabled proxies | T | O | Compliant |
| d) Refer to CO.5.1e for compliance. | All HTTP requests to the external interface are redirected (or proxied) to the SSN web server | T | O | Compliant |
| e) To ensure that the external proxy limits access based on source IP address, in BWC, under Proxies , select External and select External-to-SSN proxies and right click on WWW Proxy . Select modify and access rules to ensure that this proxy uses a rule configured specifically for it | There is a rule created specifically for the External to SSN WWW proxy as opposed to the "initial default rule" | O | O | Compliant |
| f) Select Edit for the specific rule and select source addresses to examine the IP address ACL | A limited number of IP addresses are allowed to access this proxy as opposed to access being allowed to all source IP addresses | O | O | Non-compliant |
| g) From the command prompt on the internal host use nslookup to determine the domain names associated with | All IP addresses in the ACL should be associated with domains who are specifically granted access to the | T | O | N/A |

| | | | | |
|--|--|-------------------|---|-----------|
| the IP addresses in (f) and interview the IT manager to confirm that the IP addresses are those of partners who are allowed access to the data on the SSN web server | SSN web pages | | | |
| h) Enumerate results of visual examination of proxies, Nmap scan results and Nessus scan results to ensure that no other proxies are enabled | No additional proxies should be enabled | T | O | Compliant |
| i) Using Ethereal protocol analyzer on the SSN host, capture traffic on the network segment while Nessus and Nmap scan the external interface. | Ethereal protocol analyzer running on the SSN host detects only HTTP traffic patterns from the external host | T | O | Compliant |
| Comments: Ref. (f) & (g): While an access rule has been created specifically for the external to SSN WWW proxy, it does not limit access by IP address (See Figure 36). Thus this WWW proxy can be used by any Internet host. | | | | |
| Date: | Completed by: | Signature: | | |

Fig. 36: Source Address ACL for External to SSM WWW Proxy



| CO.8.7 - SSN to Internal Proxies | | | | |
|---|---|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Proxies , select SSN and examine the firewall's SSN-to-Internal proxies to ensure that only the required proxies are enabled | No SSN-to-internal proxies should be enabled | O | O | Compliant |
| b) Run Nmap from the Linux system against the SSN interface of the firewall to determine open ports. | Only the ports corresponding to the proxies in (a) should be open | T | O | Compliant |
| c) Run Nessus from the Linux system against the SSN interface of the firewall to determine vulnerabilities associated with any open ports or enabled proxies | There should be no vulnerabilities associated with enabled proxies | T | O | Compliant |
| d) Enumerate results of visual examination of proxies, Nmap scan results and Nessus scan results to ensure that no other proxies are enabled | No additional proxies should be enabled | T | O | Compliant |
| g) Using Ethereal protocol analyzer on the internal host, capture traffic on the network segment while Nessus and Nmap scan the SSN interface. | Ethereal protocol analyzer running on the internal host detects no traffic patterns from the SSN host | T | O | Compliant |
| Comments: As per corporate policy there are no SSN-to-internal proxies running on the firewall | | | | |
| Date: | Completed by: | Signature: | | |

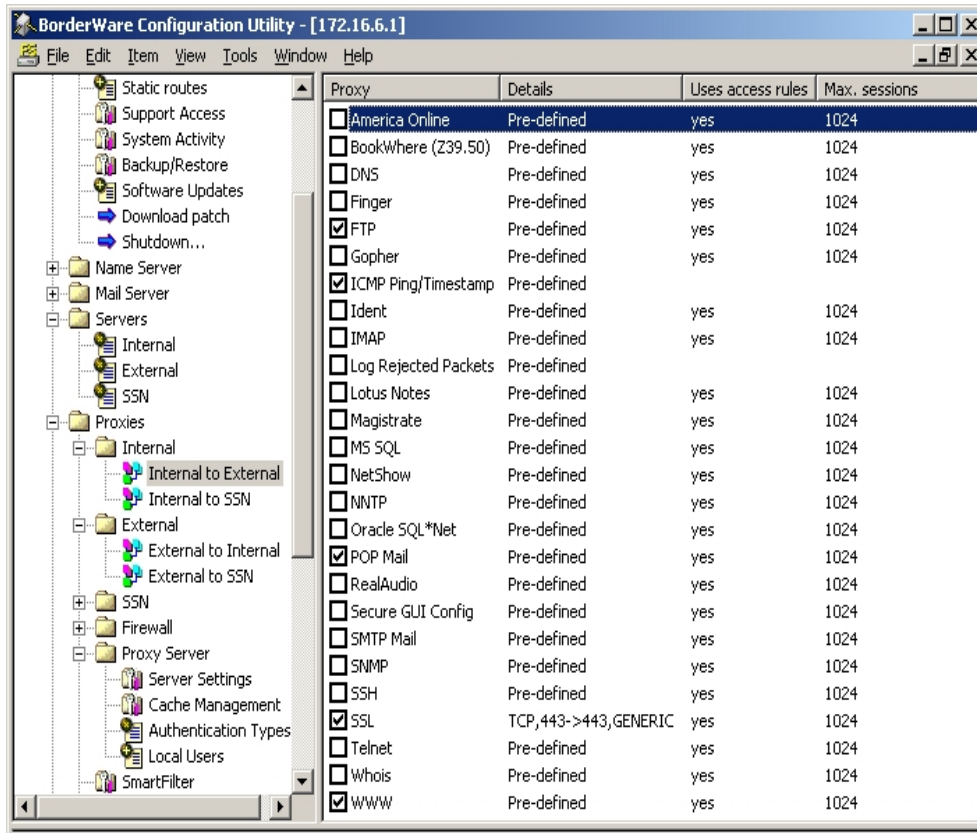
| CO.8.8 - SSN to External Proxies | | | | |
|---|--|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Proxies , select SSN and examine the firewall's SSN-to-External proxies to ensure that only the required proxies are enabled | No SSN-to-external proxies should be enabled | O | O | Compliant |
| b) Run Nmap from the Linux system against the SSN interface of the firewall to determine open ports. | Only the ports corresponding to the proxies in (a) should be open | T | O | Compliant |
| c) Run Nessus from the Linux system against the SSN interface of the firewall to determine vulnerabilities associated with any open ports or enabled proxies | There should be no vulnerabilities associated with enabled proxies | T | O | Compliant |
| d) Enumerate results of visual examination of proxies, Nmap scan results and Nessus scan results to ensure that no other proxies are enabled | No additional proxies should be enabled | T | O | Compliant |
| Comments: As per corporate policy there are no SSN-to-internal proxies running on the firewall | | | | |
| Date: | Completed by: | Signature: | | |

| CO.8.9 - Internal to SSN Proxies | | | | |
|--|--|---------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Proxies , select Internal and examine the firewall's Internal-to-SSN proxies to ensure that only the required proxies are enabled | The following internal-to-SSN proxies should be enabled: <ul style="list-style-type: none"> • WWW • ICMP/Timestamp | O | O | Compliant |
| b) Run Nmap from the Linux system against the internal interface of the firewall to determine open ports. | Only the ports corresponding to the proxies in (a) should be open | T | O | Compliant |
| c) Run Nessus from the Linux system against the SSN interface of the firewall to determine vulnerabilities associated with any open ports or enabled proxies | There should be no vulnerabilities associated with enabled proxies | T | O | Compliant |
| d) From the internal host's Internet browser | The website on the SSN web server is accessible | T | O | Compliant |

| | | | | |
|--|--|-------------------|---|-----------|
| type http://10.0.0.1 . | | | | |
| e) To verify that ICMP is allowed from the internal network to the SSN, attempt to Ping and Traceroute from the internal host to SSN web server. | The Ping command receives 4 replies from the web server and the Tracert should show 1 or more "hops" to the destination and indicate Trace Complete at the IP of the SSN web server | T | O | Compliant |
| f) Enumerate results of visual examination of proxies, Nmap scan results and Nessus scan results to ensure that no other proxies are enabled | No additional proxies should be enabled | T | O | Compliant |
| Comments: Only the Internal-to-SSN proxies required by corporate policy are enabled | | | | |
| Date: | Completed by: | Signature: | | |

| CO.8.10 - Internal to External Proxies | | | | |
|---|--|--------|-----|---------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) In BWC under Proxies , select internal and examine the firewall's internal-to-External proxies to ensure that only the required proxies are enabled | The following internal-to-external proxies should be enabled <ul style="list-style-type: none"> • ICMP/Time-stamp • FTP • WWW** | O | O | Compliant |
| b) Run Nmap from the Linux system against the internal interface of the firewall to determine open ports. | Only the ports corresponding to the proxies in (a) should be open | T | O | Non-Compliant |
| c) Run Nessus from the Linux system against the internal interface of the firewall to determine vulnerabilities associated with any open ports or enabled proxies | There should be no vulnerabilities associated with enabled proxies | T | O | Non-Compliant |
| d) To verify that ICMP is proxied through the firewall from the internal network to the external, from the internal host, attempt | The Ping command will receive 4 replies from the web site (O). | | | Compliant |

| | | | | |
|--|---|-------------------|---|---------------|
| to Ping a web site that has enabled ICMP responses (www.yahoo.com). | | | | |
| e) To verify that FTP is proxied through the firewall from the internal network to the external, from the Internal host, attempt to establish an FTP session to an Internet FTP site that allows anonymous access such as ftp.nai.com | FTP access should be possible to the site | | | Compliant |
| f) Enumerate results of visual examination of proxies, Nmap scan results and Nessus scan results to ensure that no other servers are enabled | No additional proxies should be enabled | T | O | Non-Compliant |
| Comments: Ref. (b): Nmap port scans found the following unauthorized ports on the internal interface corresponding to servers (See Appendix 3 for full NMAP Scan results): i) TCP port 109 (Pop Email) ii) TCP port 110 (Pop Email) iii) TCP port 443 (This port is also open to allow for secure Remote administration, which is authorized by policy) Ref. (c): Nessus detected DNS on the external interface is able to perform recursive queries which may make the server vulnerable to cache poisoning attacks from the Internet (See Appendix 3 for full Nessus Scan results) Ref. (f): NMap, Nessus scans and visual inspection (see Figure 37) of the Internal to external proxies revealed the following unauthorized proxies i) POP ii) SSL | | | | |
| Date: | Completed by: | Signature: | | |

Fig. 37: Internal to External Proxies

© SANS Institute 2003,

| CO.8.11 – Scan from external host to internal network | | | | |
|---|--|-------------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Run Nmap from the Linux system on the external network specifying the internal host IP address and the firewall internal interface IP address as targets. While the NMAP scan is running the Ethereal protocol analyzer should be running on the internal host | Nmap results will yield no information about the internal hosts and the ethereal protocol analyzer does not capture any packets originating on the external host | T | O | Compliant |
| b) Run Nessus from the Linux system on the external network specifying the internal host IP address and the firewall internal interface IP address as targets. While the Nessus scan is running the Ethereal protocol analyzer should be running on the internal host | Nessus results will yield no information about the internal hosts and the ethereal protocol analyzer does not capture any packets originating on the external host | T | O | Compliant |
| Comments: When attempting to scan internal addresses from the external host, the scans returned no usable information about the systems, and the protocol analyzer on the internal system captured no traffic from the external system. | | | | |
| Date: | Completed by: | Signature: | | |

| CO.8.12 – Scan from external host to SSN | | | | |
|--|--|---------------|------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Run Nmap from the Linux system on the external network specifying the SSN host IP address and the firewall SSN interface IP address as targets. While the NMAP scan is running the Ethereal protocol analyzer should be running on the SSN host | Nmap results will yield no information about the SSN hosts and the ethereal protocol analyzer does not capture any packets originating on the external host | T | O | Compliant |
| b) Run Nessus from the Linux system on the external network specifying the SSN host IP address and the firewall SSN interface IP address as targets. While the Nessus scan is running the Ethereal | Nessus results will yield no information about the internal hosts and the ethereal protocol analyzer does not capture any packets originating on the external host | T | O | Compliant |

3/6/2003 9:15 AM

| | | | | |
|---|----------------------|--|-------------------|--|
| protocol analyzer should be running on the SSN host | | | | |
| Comments: When attempting to scan SSN addresses from the external host, the scans returned no usable information about the systems, and the protocol analyzer on the SSN system captured no traffic from the external system. | | | | |
| Date: | Completed by: | | Signature: | |

| CO.8.13 – Scan from SSN host to internal network | | | | |
|--|---|---------------|-------------------|-------------------|
| Test | Expected Result for Compliance | Method | O/S | Compliance |
| a) Run Nmap from the Linux system on the SSN network specifying the internal host IP address and the firewall internal interface IP address as targets. While the Nmap scan is running the Ethereal protocol analyzer should be running on the internal host | Nmap results will yield no information about the internal hosts and the ethereal protocol analyzer does not capture any packets originating on the SSN host | T | O | Compliant |
| c) Run Nessus from the Linux system on the SSN network specifying the internal host IP address and the firewall internal interface IP address as targets. While the Nessus scan is running the Ethereal protocol analyzer should be running on the internal host | Nessus results will yield no information about the internal hosts and the ethereal protocol analyzer does not capture any packets originating on the SSN host | T | O | Compliant |
| Comments: When attempting to scan internal addresses from the SSN host, the scans returned no usable information about the systems, and the protocol analyzer on the internal system captured no traffic from the SSN system. | | | | |
| Date: | Completed by: | | Signature: | |

A.3.1 - Is the system securable?

The configuration of the Borderware Firewall at **CFG**, deviates from corporate policies and industry best practices. The individual areas of concern are addressed in more detail in **Audit Findings** in **A.4.2**

While the business needs are met, there are extra services enabled on the firewall that do not conform to policy. These services thus introduce unwanted traffic flow in and out of the protected network. Vulnerability assessment tools did find weaknesses in the system but with the exception of a DNS issue on the external interface and an inability to secure access to Remote Management, these were due to configuration issues as opposed to inherent security flaws. For example, the SMTP server was misconfigured in a manner that could potentially allow Spam email to be relayed to the Internet from both the internal and external network.

While reconfiguring the firewall will remove the risks in the short term, it is felt that the bulk of the threats uncovered would be mitigated by addressing the root cause. In this case, it is felt that **CFG** needs to focus on implementation of a change management process, a more controlled document management program and closer observation of the policies and procedures.

The costs associated with improving the security of the firewall are minimal for the configuration changes. It is estimated that it would take one to two days to remove the extra servers and proxies, and tighten up network and physical access security. The issues relating to redundancy would take a little longer to address, but assuming the hardware and appropriate licensing were available, it would only be a matter of three to five days of the administrator's time. This would be time well spent as in the event of a firewall failure, automated failover would greatly reduce the downtime and work involved in reconfiguring the replacement.

The larger tasks are those associated with the documentation. The corporate policy and the associated firewall definition and policy need to be re-addressed to determine if business needs have changed. Procedure documentation needs to be created to ensure configuration control, data availability, improved reaction and restoration capability in the event of a security incident or an outage. It is estimated that it could take 60-80 person hours to create documentation for change management, backup procedures, and incident response. As regards the policy documents, this may take longer as the business needs will have to be re-examined at senior management level.

A.3.3 - Is the system auditable?

Policy documents exist at **CFG** against which the system can be audited. However the system deviates from best practice and does not utilize its security potential to the fullest. For example, the policy requirements regarding Internet access state that the users should be able to access the Internet with no configuration at their systems. This is achieved with

the existing firewall rules but more complex configuration (caching options, authentication and Java script blocking) have been overlooked in both policy and configuration.

While editing the configuration of a device may deem it secure or insecure (at that particular moment in time), the value of doing is limited without change control and strict policy adherence.

Appropriately addressed was the degree to which the firewall configuration deviated from business needs. It was possible to determine which required services were not available and which services - not required by policy - were enabled. Issues such as the security of the screening routers outside the firewall, the security of corporate servers (the email and SSN web servers) and client workstation security were not considered.

Areas that could not be appropriately addressed included subjective areas such as the actual level of day-to-compliance with documented procedure. While there seemed to be awareness of the policy documentation, the configuration of the firewall indicated that the policy was not followed. Again, the root cause is not the policy document itself, but the lack of a change management process.

The audit process itself was quite effective in determining weaknesses in the firewall's configuration; however, some core security issues can not be remedied due to limitations of the product. These include the inability to secure Remote Management with IP address-based access controls and unique credentials, as well as the inability to use the internal DNS server for Internet resolution without allowing recursive queries on the external interface.

© SANS Institute 2003. All rights reserved. For research purposes only.

Assignment 4 - Follow Up

A.4.1 - Executive summary

This audit examined the configuration of a Borderware 6.5 Firewall Server installed as *CFG*'s email and Internet gateway. This firewall acts as the single point of traffic flow between *CFG*'s protected network and the Internet. As such it is vital to the day-to-day functioning of the organization. It is managed by the Firewall administrator who reports to the Firewall Manager in a 10-person IT department (includes helpdesk personnel and server administrators.)

All objectives of the audit were achieved with no questions left unanswered. Certain steps were omitted such as war dialing to verify that no modem connections existed. This had been performed previously by 3rd party security auditors.

The firewall itself defaults to a secure configuration, however in *CFG*'s implementation, unnecessary services had been enabled on the internal interface allowing unauthorized traffic out of the protected network and the subsequent replies back in. In addition, critical services running on the firewall (DNS and SMTP) displayed some serious security vulnerabilities. The latter was due to misconfiguration of the SMTP server and how it handles email relaying on all interfaces and the former was one of the few features inherent to the system that affected security.

Also of concern was the physical and network security governing access to device. The ability of all members of the IT department to access the firewall both physically and from any workstation using generic credentials makes it very difficult to control changes made to the firewall.

System redundancy is also an issue. Automated failover to a redundant firewall is not employed, and the manual failover system requires greater diligence on the part of the firewall team. In a situation where there is unregulated access and uncontrolled configuration changes, the likelihood of the firewall ceasing to function is increased and thus the need for a fast replacement becomes all the more important.

While for the most part the above are easily remedied (or at least compensated for) it is felt that these errors in configuration are a symptom of a more fundamental issue within *CFG* regarding adherence to existing policies, and the lack of change management processes and accountability.

A.4.2 - Audit Findings

The following points represent the 10 most critical issues that must be addressed:

Audit Finding 1: Change Management Process [CO.1.7]

Overview: Currently there is no change management process in existence for the firewall. This was largely a subjective item and all findings were determined directly in an interview with the IT manager and confirmed in the interview process with the firewall administrator. Subsequent interviews revealed that if a change is required (or if a service is requested), the firewall administrator evaluates the change including the security risks involved and chooses to allow or deny based on that evaluation.

The feeling within the IT department is that, given the small size of the department, there are clear communications between the Firewall team and the other IT personnel. The firewall administrator added that when changes are made to the firewall, the helpdesk is notified by email of the change and any effect it will have on user access.

Background/Risk: The lack of a change management process is the root cause of the configuration issues found on the firewall (discussed in the subsequent pages) and could also be the cause of a failure to react properly in a crisis.

Additional services were found on the firewall and they are discussed in **Audit Finding 9: Additional Servers & Proxies** below. The administrator stated the reasons that they were enabled and that the firewall manager and helpdesk had been notified. While it was found that, in general, the administrator's judgment was sound on these issues, there is no process for ensuring control and authorization of these changes. There is also no process to ensure that the last good firewall configuration backup is available when changes are made. Additionally, it was determined in the interview process (CO.1.3) that after a change is made and the system is determined to be stable and working as expected, the configuration is not backed up immediately.

Audit Recommendations: The additional services that have been enabled on the firewall may be justified and needed. But if this is the case, the IT manager, in consultation with senior management, needs to revisit the business requirements and thus re-address the firewall policy. The lack of a change management process for the firewall may be a symptom of the larger corporate change management philosophy. This may need to be addressed at a broad level before being implemented in the IT department.

It is recommended that the firewall administrator be directed to ensure that all changes to the firewall configuration are communicated to IT management in advance and that all changes are held pending approval. Once changes are implemented there should be a due process that ensures that this information as well as any consequences arising out of such changes is available to the helpdesk and server teams.

Any user request for changes to the firewall policy should not be made directly to the firewall administrator. Instead someone in an information management role (the office of the CIO) should receive this request. It should be a formal business case and, if deemed appropriate, the IT department should examine the methods for facilitating this request through the firewall.

The change management process must be extended to cover reboots (as part of regular maintenance) and implementation of vendor patches. Every change made to the firewall must be communicated clearly to the helpdesk so they know how to react and where to direct the department's energies in the event of a significant outage.

While the implementation of documented procedures is a corrective control, it will not be effective if they are not adhered to. Preventative controls could be implemented to limit the ability of the administrator to edit the configuration. Since this is an administrator's exact job description, this would be a self-defeating task.

Costs: The cost involved in revamping a change management procedure is significant. In addition to the 40 person-hours (approximately) necessary to create the documentation, there are sensitive areas to be addressed such as a perceived loss of control on the part of the firewall administrator. Further, there may be political fallout if user requests are not met in a timely fashion.

At the outset, the change management process may be perceived as extra work (e.g. justification of changes, submission for approval, approval process, etc.) for all concerned parties. The feeling is that in a small department, verbal communication is sufficient. However, once the department starts to grow, that will not be scalable.

There will also be associated costs in retraining of all concerned IT personnel. In addition to the firewall administrator having to follow process for justification and approval, the helpdesk and server staff will need to be trained to determine how to track and access this process. This will ensure that any ill-effects on user productivity arising out of the change are documented and recorded

Compensating Controls: In the absence of full implementation of a change management process, the IT manager needs to ensure that the firewall administrator still follows a process for approval and justification. It can be as simple as explaining why a change has to be made in an email to both the helpdesk and the firewall managers. The firewall manager can then reply with approval and an explanation to all IT personnel as to what the perceived effects on the users will be.

Audit Finding 2: Firewall Physical Security [CO.2.2]

Overview: The firewall console user name and password is known to all IT employees. The helpdesk manager was able to logon to the firewall (CO2.2c) using a standard administration password. Additionally, as determined in the interview process in (CO2.1), physical access to the firewall location is granted to all IT personnel. Thus all members of the IT department, even the most junior of staff, can log on to the firewall console and make significant changes that could cause a complete cessation of regular business function.

Background/Risk: The justification of this situation is that the same credentials are used for Remote Management which is used to access the URL filter controls and database. Since helpdesk personnel perform the majority of tasks requiring manual manipulation of the database it was deemed necessary to allow them to have these credentials. This represents an inherent limitation in the Firewall server itself. According to Borderware Technical Support, the same password is used for console login as well as for all remote administration accounts, thus access to the console cannot be controlled without affecting remote administration.

Of larger concern is the fact that these credentials are the same as those used for all server and network administration tasks. It is the standard administrator password at **CFG**. The net effect is that any member of the IT department can log on directly to the firewall console and perform any task that can be accessed including shutting down the firewall, manipulation of interface configuration or editing of rules and filters.

Audit Recommendations: The ideal situation would be to ensure that the firewall console password is known only to the firewall administrators and that the firewall console is left in a locked-down state. The former is not an option as helpdesk personnel need these credentials to perform remote administration, so it is recommended to physically secure the firewall console by moving it to a locked room that only authorized staff can access. This does not change that fact that all IT personnel can still access the firewall from the Remote Management interface (which allows full administration of the firewall), this is discussed in more detail under **Audit Finding 7: Internal Remote Management Server Security** below.

Costs: The cost of moving the firewall to a secure room (that only authorized firewall administrators can access) will be both the dollar value of construction (rates vary from city to city) as well as downtime (1 hour) while the firewall is moved. As with all process changes that are perceived as removing previously held rights of key personnel, there may be some resistance among the IT staff. This is natural and should be addressed as openly and honestly as possible. The point is not to demote or take responsibility from anybody but to ensure that maximum control is retained by those who are ultimately responsible for the firewall's operation.

Compensating Controls: If physically securing the firewall is not feasible, the password should be changed to limit access to the console. As mentioned, this will affect

the ability for the helpdesk to perform Remote Management. However, if the desire is to lock down access to the firewall, perhaps the rights to access it should also be limited and the firewall administrator should take over the helpdesk tasks that are currently performed on the firewall.

© SANS Institute 2003, Author retains full rights.

Audit Finding 3: Firewall Redundancy [CO3.2]

Overview: Examination of the Firewall Console revealed that Borderware High Availability Clustering (HALO) has not been enabled. In the event of a failure of the firewall itself, there will be no automated failover to a backup system. By way of compensation, there is an offline backup firewall (for manual failover) in place. While examination of this system and comparison to the production firewall revealed duplicate configuration, it did not have the same software updates (security patches etc.) installed (CO.3.2b & e).

Background/Risk: The risk associated with this situation is twofold. Without automated failover to a backup firewall, in the event of an unrecoverable failure of the production system, there will be no communications between the protected network and the Internet until a duplicate system is manually put in place. If on the other hand an offline backup firewall (no automated failover) does not exist, in the event of a failure of the production system there will be no communications between the protected network and the Internet until a duplicate system is manually built on suitable hardware. Such hardware may not be immediately available. Additionally, installation of a duplicate system in an emergency will invariably result in a misconfigured system.

Audit Recommendations: It is recommended that duplicate hardware and licensing are purchased and that a firewall cluster is configured using the HALO option in the firewall console. This firewall cluster's virtual IP address will ensure that Internet access will not be interrupted as there will be an automatic failover to the duplicate firewall in the event of a system failure.

Costs: The costs of implementing HALO are fairly significant. In addition to the purchase of hardware for the failover system, the licensing costs are also effectively doubled. Additionally there will be significant time (approximately 40-60 personnel-hours) spent on configuration and testing of the clustered servers.

Compensating Controls: In the absence of budget or time to configure licensing and hardware for firewall server clustering, a duplicate licensed copy should be kept available offline. Borderware allows its clients to implement an offline backup firewall. A suitable license can be downloaded free of charge at the Borderware⁶² website. This license presents a lower cost alternative for firewall redundancy. The backup firewall is configured with the exact same IP addressing information as the production system allowing for a simple substitution in the event of failure of the production system. If this method is employed it is of extreme importance to:

1. Ensure the device is never live on the network at the same time as the production device as this will cause IP addressing conflicts
2. Ensure that patch level and rules employed on the backup server are identical stage to the production server.

Audit Finding 4: DNS server on external interface [C.O.5.3]

Overview: Nessus Scans on the external interface of the firewall revealed that the external DNS server is enabled and can be used by Internet hosts to perform queries for Internet resources. This was tested by configuring the external host to use the external firewall interface as its DNS server and then submitting queries for Internet resources. In all cases (e.g. www.yahoo.com – see figure 19) the firewall replied as a non-authoritative server with name-to-IP address resolution for the host.

Background/Risk: Testing of Internet access from the internal network and consultation with Borderware Technical Support revealed that when using DNS in the manner employed at *CFG*, the external DNS server must be enabled to ensure that Internet resolution is possible from the Internal network. Since the firewall forwards the DNS queries to the ISP DNS server as UDP (a connectionless protocol which does not remember the state of a network session) traffic, the response can not come back into the network as a reply to an already initiated session. Instead it must be initiated from the outside by the ISP DNS server. Hence DNS queries must be enabled on the external interface to allow the ISP DNS server to return the DNS response to the firewall.

There are two issues with this. The first is the increased potential for DNS cache poisoning⁶³ attacks where misleading DNS entries received from remote DNS servers are stored in the DNS cache. In theory, it is possible that if a resource can query a DNS server, it can cause that server to obtain DNS records from Internet DNS servers that contain bogus Internet host records. This data would be stored in cache. This could then cause legitimate users to obtain these false results when issuing queries against that server. According to Borderware Technical Support, the likelihood of any issues arising from DNS cache poisoning are remote, as there is complete separation between the external and internal DNS engines on the firewall. In addition, even if the external DNS cache did get corrupted, since *CFG* hosts all its public records at the ISP, no one should ever query the external interface for DNS resolution anyway.

Another possibility is a primitive Denial of Service attack where multiple DNS queries are sent from a number of hosts to the firewall external interface simultaneously. According to Borderware Technical Support, the number of CPU cycles used in responding to a DNS query is minimal. In order to affect the running of the server, an unfeasibly large amount of DNS queries would have to be submitted to the server at the exact same instance.

Audit Recommendations: It is recommended that measures be taken to ensure that the ability for remote Internet hosts to query the external interface of the firewall be removed. Ideally, this would involve merely un-checking the *DNS Queries* external server. However this is not possible given *CFG*'s DNS implementation. Since the ISP's DNS server is the only Internet host that needs to initiate DNS sessions with the firewall, the next logical step is to enable access controls on the external DNS server specifying the only allowed IP address as that of the ISP DNS server. However, examination of the

product and conversation with Borderware Technical Support reveals that this is also not possible.

Costs: Since all recommended avenues of removing this concern are blocked by either business needs or product limitations, a number of compensating controls will have to be looked at. These are addressed below.

Compensating Controls: The most immediate fix available involves a certain amount of re-engineering of the current DNS architecture and may create different security vulnerabilities. It is possible to enable the DNS proxy on the firewall and ensure that the internal hosts specify the ISP DNS server as their DNS server. This will remove the external DNS server from the firewall but will open a proxy from the internal network to the external for DNS traffic. It is possible that a malicious hacker could exploit this proxy port.

It may also be feasible to approach the ISP and ask for a rule to be entered in their router configuration to ensure that all DNS traffic initiated on the Internet and directed to the firewall external interface is screened out by the router unless its source IP address is that of the ISP DNS server. This is the recommended approach as it does not require any reconfiguration of hosts on the internal network and does not introduce any new open ports on the firewall.

© SANS Institute 2003, Author retains full rights.

Audit Finding 5: Email Server on Internal and External interfaces [CO.5.3]

Overview: The SMTP server on both the internal and external interfaces will accept SMTP email from any SMTP host and will forward this email to the destination. This could cause the firewall to be seen as the source of “Spam” email on the Internet

Background/Risk: The SMTP server has not been configured to **Block Relaying on the External Interface** (See figure 23). From an external email client, it was possible to specify the firewall’s external interface as the outgoing email server. With this configuration it was possible to send email from a bogus source email address to a legitimate Internet email address. When the email was received by the Internet account, the headers were examined and the external interface of the firewall was seen as the source of the email (see figure 26 where the IP addresses of the firewall external interface and the SMTP client are obscured to protect the client’s identity).

The SMTP server on the Internal Interface of the firewall has not been configured with IP address ACLs (Access Control Lists) to accept outgoing email from only the corporate email server. From an email client on the internal network, it was possible to send email to an Internet email account using the firewall internal interface as the outgoing email server. When the email was received by the Internet account, the headers were examined and the external interface of the firewall was seen as the source of the email (See figure 22 where the actual external IP address of firewall is obscured to protect client’s identity).

It is possible that an attacker (or perhaps a malicious/curious user on the internal network) could send bulk email from bogus source addresses to legitimate email accounts on the Internet. In both cases, the email headers show the firewall external interface as the source of the email. This could cause the email recipients to blame *CFG* for distributing Spam email and could be damaging to the company’s reputation.

Audit Recommendations: Enable IP address access controls to ensure that the SMTP server on the internal interface of the firewall accepts SMTP email from only the corporate email server. This ensures that all email must be sent from legitimate corporate email clients.

Ensure that the “Block Relaying on the External Interface” is enabled to ensure that external hosts cannot specify the firewall’s external interface as their server for outgoing email.

Costs: The costs in configuring the external interface to block relaying are minimal and should really be no more than selecting a check box.

3/6/2003 9:15 AM

As regards the Internal SMTP server, the ACL will involve determining the IP address of the corporate email server and ensuring that this is the only server allowed to send email to the firewall.

Compensating Controls: If there are business requirements that demand email relaying on the external interface (perhaps a partner hosted web server that allows email alerts or queries to be sent from its web pages via the firewall) then strict IP address-based ACLs should be employed to ensure that only specific SMTP hosts are allowed to relay email through the firewall.

The same situation applies to the Internal SMTP server. Again, it should be locked down with IP address-based ACLs to ensure that only the corporate email server (and perhaps email enabled web servers) can send email via the internal interface

© SANS Institute 2003, Author retains full rights.

Audit Finding 6: Firewall URL filter allows web-based email [CO.5.6]

Overview: Simple testing revealed that it is possible to access free web based email such as <http://www.hotmail.com> and <http://mail.yahoo.com> from internal hosts.

Background/Risk: The *CFG* network employs a layered defense against virus attacks. There are strict attachment-blocking policies employed on the email server and email clients. There is also virus scanning software running on both the email server and on the client computers. Allowing access to free web based email from the internal network allows users to circumvent these “defense-in-depth” mechanisms. It allows users to receive dangerous attachments (executables, batch files, script files) - that would otherwise be blocked at the corporate email server. It is also possible that users will receive virus infected files that would otherwise be scanned and blocked at the email server. (It is more difficult to keep multiple desktop virus scanners up to date than one email server and, as such, all virus infected files should be blocked at the email server). Web-based email allows virus infected files to arrive right at the clients’ desktop without any perimeter scanning. If this happens, the safety of the network is dependent on each client system being 100% up to date with its virus scanning software. Additionally, while some web-based email servers do perform server-side virus scanning, *CFG* does not want to be in the situation where the security of its network and the integrity of its virus defense strategy hinges on the diligence of any 3rd party that relies on Spam email and advertising for its revenue.

Audit Recommendations: It is recommended to block access to all web-based email sites unless any such site is implemented and controlled by *CFG* and is required on the on the protected network.

Costs: The costs associated with this are onerous in terms of keeping up to date with the multitude of free web based email sites that exist in the world. There will also be a reaction from the user community who may have become accustomed to sending personal emails on lunch breaks or after hours. This may be seen as management implementing a “crack-down” on personal use of Internet resources.

Compensating Controls: If blocking free web based email sites is not an option, it might be feasible to investigate (and thoroughly test) web based email sites which provide virus detection at the server. Users could be encouraged to use these sites. If *CFG* continues to allow access to all free web based email sites, it will have to make significant investment in a system for centralizing control of its desktop virus scanners. This would include automatic push of virus scanner updates and the ability to generate reports and statistics on the state of virus detection software versions across the network.

Audit Finding 7: Internal Remote management Server Security [CO.6.1]

Overview: Examination of the Remote Management settings (CO.6.1a) revealed that both “Secured” and “Unsecured” Remote Management are enabled on the firewall internal interface (figure 29). Using the Windows-based Borderware configuration utility from a host on the internal network, it was possible to remotely manage the firewall using both encrypted and clear text sessions (CO.6.1b & CO.6.1e). The Remote Management capability on the internal interface is not configured with an IP address based access control list (CO.6.1j & CO.6.1k). In addition, it is configured with only one set of user credentials that is known to all IT personnel (CO.6.1h).

Background/Risk: By allowing Remote Management to be performed using clear-text sessions, it is possible that someone running a packet sniffer on the internal network could determine the user credentials or valuable information about the firewall configuration.

Since there are no IP address based access control lists employed for Remote Management, any workstation on the internal network can be used to remotely access and administer the firewall. Assuming someone was a packet sniffer or protocol analyzer software on the internal network that allowed the clear text login credentials to be captured, they could remotely administer the firewall without having to be in the dedicated (secure, controlled access) IT area.

Since the firewall is configured with only one Remote Management account, with credentials known to all members of the IT department, there can be no accountability among those authorized to make changes to the firewall. There is also no way to prevent those who are not authorized to access the firewall from doing so.

Audit Recommendations: It is recommended that only Secure Remote Management (SSL) be allowed on only the internal interface of the firewall and that more granular user and IP address-based access control lists be applied.

Costs: There is no significant cost associated with configuring Remote Management to accept only SSL connections. There is minimal overhead on the session once SSL is enabled and the configuration requires selection of one check box.

While the other issues discussed above should, in theory, be easily remedied, according to Borderware Technical Support it is not possible to implement IP address based ACLs for Secure Remote Management. Nor is it possible to create totally unique credentials for Remote Management. When the firewall is first installed, a password is created and this password is used by all Remote Management user accounts.

Compensating Controls: Since the above recommendations are hampered by technical limitations of the product itself, other approaches have to be explored. It is recommended that a 4th network interface card be installed on the firewall to create an auxiliary (Aux)

network. By placing a limited number of hosts on the network segment that connects to this interface, the number of Remote Management workstations can be limited. In addition, Remote Management tasks should not be assigned to helpdesk personnel. Responsibility for these tasks should be reassigned to the dedicated firewall team and the console/Remote Management password should be changed to something known only by that team.

© SANS Institute 2003, Author retains full rights.

Audit Finding 8: Firewall Patch Level [CO.7.1]

Overview: Examination of the service patches and fixes on the firewall demonstrate that not all relevant patches have been applied.

Background/Risk: There are two available patches that have not been applied to the firewall. These are the URLFilter patch to upgrade the web site filter from Smartfilter to Surfcontrol and Service Patch 1 (fs65s01). This is illustrated in figures 31 and 32.

The absence of the URLFilter patch does not present a major security concern as this is simply an upgrade from one web filtering product to another. However, it should be noted that Borderware is encouraging its customers to complete this upgrade and will be withdrawing support for Smartfilter in the next year.

The absence of fs65s01 is concern as it contains fixes to ensure improved access to clustering options, better operation of the WWW and email proxies as well as a correction for a security flaw inherent to the encryption daemon running on the firewall. The release notes for fs65s01 are in Appendix 4.

Audit Recommendations: In the short term, it is recommended to update the patches. However, this does not address the larger issue of ensuring that patches remain up to date. It is recommended that the firewall administrator approach the vendor to arrange a subscription or automated notification on publication of a new service patch or fix.

Costs: As regards the immediate issues, download and install of the missing patches should not take more than one hour. However, this will only remedy the situation in the short term. Generally speaking, services that provide notification on release of a new patch or fix are free of charge once the product has been purchased. In fact the Borderware Support Center website provides a link⁶⁴ that allows sign-up for an automatic notification service on release of firewall updates.

Compensating Controls: In the absence of any notification service from the product manufacturer, the firewall administrator needs to document a procedure specifying a schedule for accessing the download site and installing patches and updates.

Audit Finding 9: Additional Servers & Proxies [CO8.2, 8.9 & 8.10]

Overview: Examination of the configuration and port scans (Appendix 3) on the firewall's internal interface revealed that servers and proxies not required by policy are enabled. The enabled service is FTP, while the enabled proxies are SSL and POP.

Background/Risk: The FTP (File Transfer Protocol) service is enabled (figure 34) to allow uploads of vendor patches to the firewall prior to installation. It is justifiable that FTP would be enabled on the internal interface for this purpose. The FTP service is protected by the firewall administrator credentials.

SSL (Secure Sockets Layer) is enabled as a proxy on the internal interface (figure 37) and allows users to take part in encrypted sessions with remote web servers. This is usually the protocol used to add a layer of security to any password protected transaction such as online banking. Enabling the SSL internal-to-external proxy should theoretically not be a major security concern, however it is not required by policy and should be therefore denied.

The POP (Post Office Protocol) proxy represents a significant security issue (figure 37). Most commercial ISPs implement POP email. Effectively, each email sent to a user is transferred as a file from the email server to the user's local hard drive. This usually means that when a user downloads email, it is removed from the email server saving space on the server. POP email does not allow the mobility that can be achieved with web based email as each workstation must be specifically configured to point to the ISP's SMTP and POP servers. The major concern is that most ISPs do not run virus scanning on their email server. Thus allowing POP email downloads through the firewall could effectively allow a transfer of a virus infected file from the ISP email server directly to a local workstation hard drive. POP email presents the same risk as web-based email and allows incoming email to completely circumvent defense-in-depth strategies.

Audit Recommendations: In the short term, it is recommended to disable all services that are not expressly required by the corporate policy. While a business case can be made for FTP (to facilitate patch updates on the firewall) and SSL (to allow users to engage in secure online transactions), it is recommended that these be enabled only after a complete policy review by senior management. Additionally, penetration testing and vulnerability assessment should be conducted on the firewall with these services enabled.

POP email on the other hand should be disabled immediately. There is no business case to justify letting email from third party email servers access the client computers directly. The corporate policy states that users may only access email addressed to their *user@cfg.com* address and a POP email proxy on the firewall specifically allows violation of this.

In the long term, it is recommended that change management procedures are addressed. It should be determined why these services were enabled. In the case of the FTP server, the

administrator saw a justifiable need to allow it but someone may have requested SSL and POP proxies. In addition to addressing change management issues within the IT department, the users should be informed of the process to be followed when requesting access to a particular service through the firewall.

Costs: The short term cost is mainly the time it will take to disable these services. It should be noted that disabling the FTP service will affect the administrator's ability to perform security updates.

The cost associated with disabling SSL may be political. Users may argue that banking on line using this protocol saves time as they do not have to physically leave the office and are thus more productive. There may also be morale issues with the users feeling that management is implementing another "crack down" on personal use of Internet resources.

Disabling the POP email proxy may cause some complaints from the users and will require the support of senior management. Users are most likely not aware of the dangers of allowing an ISP's POP email into the network and will resent losing the ability to read personal email on personal time such as lunch, after hours, etc.

The larger cost here will be the time spent re-addressing the policy documents which has to be an ongoing process between the corporate policy makers, the IT manager and senior management. It is also recommended that if anything is added to the list of allowed services in the policy documents, vulnerability assessment and penetration test be conducted on the firewall. The latter will take approximately 60-80 person hours for completion and report submission.

Compensating Controls: For FTP, as mentioned, disabling it fully may not be a viable solution but perhaps the firewall administrator should consider enabling it only when firewall updates take place, disabling immediately afterward.

SSL needs to be addressed at the policy level. The question is whether the policy allows users to perform personal tasks such as banking online. If not, the proxy should be disabled. It is important to note that many legitimate business-related websites offer subscription or password protected services that use SSL for added security. If disabling SSL affects the ability for users to perform legitimate business tasks, the policy will have to be revised to compensate for this.

The only real compensating control for POP email is to ensure that all desktop virus scanners are 100% up to date and that the POP servers that users connect to employ virus scanning. It would be good if these servers limited the size of attachments to avoid the situation where users downloading attachments from their personal email accounts on remote POP email server tie up all of the available corporate bandwidth.

Audit Finding 10: IP address ACL on External to SSN WWW Proxy [CO8.6]

Overview: The external-to-SSN WWW proxy is supposed to allow only a limited number of partners to access the SSN website from the Internet. Currently it is not configured to limit access based on IP address (figure 36) and anyone with an Internet connection can access the proxy.

Note: The individual security, authentication and authorization on the web server itself are beyond the scope of this work.

Background/Risk: Allowing and denying access to a website using IP address based access controls is only one step in the overall web server security process. However it is a fairly significant one. Currently, the access control list on the external to SSN web proxy is configured to allow access from all IP addresses. This means that any system that is on the Internet can make an HTTP connection to the external interface of the firewall and be redirected to the web server in the SSN. While it is assumed that there are authentication controls on this server, omission of the ACL on the proxy allows a would-be hacker to get one step closer to the data in the SSN.

Audit Recommendations: It is recommended that, in addition to strict controls on the web server itself, IP address based access controls be employed on the WWW proxy. Partners wishing to access these web pages will have to supply their department's public IP address information to *CFG* and, after verification, this would be added to the list of allowed IP addresses.

Costs: It should not take more than a few minutes to create an access control list to deny access based on IP address. The real work will be in getting each partner to supply the IP address information as the contact person will have to get this information for their relevant IT or infrastructure groups. Once this data is obtained, it will have to be manually entered into the "allowed" list on the appropriate firewall access rule.

Compensating Controls: IP address based controls on the external to SSN proxy are a fundamental security step that should not be overlooked. It is important to stress that these controls should not be the only security employed. Allowing access based on source IP address serves to obscure the existence of the web server from the view of a would-be hacker and would eliminate the bulk of the risk associated with opportunistic or "script-kiddy" attacks. A determined attacker will be able to manipulate their source IP address headers to get around this first security hurdle. However, implementing tighter authentication and authorization controls on the web server itself as well as, possibly, a PKI based solution would greatly add to the security of the website data.

If *CFG* is not prepared to implement IP address based access controls, then the data in the SSN is potentially reachable (at least up to the point where a user is presented with a login screen or other security measure employed on the web server) by any host on the Internet. If *CFG* wants to make this information available to all Internet users regardless

of source IP, the company will have to consider greatly increased security measures to ensure the site is not vulnerable to malicious attacks. This will include a full study of revised architecture design, including layered screened subnets and total physical separation of the network segment with the web server from the production network.

© SANS Institute 2003, Author retains full rights.

Appendices

App. 1 – Corporate Documents

The following documents were examined as part of this audit:

1. Corporate Security policy
2. Internet Access policy
3. Email usage policy
4. Firewall definition
5. Firewall policy

App. 2 - Interview Questions for IT and Non-IT Personnel

Firewall Administrator

1. Are you aware of the existence and location of the corporate policy relating to the firewall and Internet access?
2. In your opinion, does the firewall in its current state comply with this policy?
3. Are you aware of the existence and location of documentation pertaining to installation and configuration of the Borderware firewall?
4. Are you aware of the existence and location of documentation pertaining to backup and restoration procedures for the Borderware firewall?
5. Do you follow these procedures when performing backups and/or restoration of the firewall configuration?
6. Is a backup performed every time a change is made to the firewall configuration?
7. Are you aware of the existence and location of documentation pertaining to incident response procedures for the Borderware firewall?
8. Are you clear on the roles and responsibilities of IT personnel regarding the incident response procedures?
9. Are you aware of the corporate priorities regarding incident handling?
10. Under what circumstances is the URL filter database edited?
11. Are firewall administrators' contact details correct and up to date in contact list?
12. Are change management guidelines followed when performing backups of firewall configuration?
13. Are you aware of the existence and location of documentation pertaining to change management procedures for the Borderware firewall?
14. Do you agree with and comply with the change management procedures for the Borderware firewall?
15. Is the firewall console password unique and known only to firewall administrators?
16. Does a duplicate offline backup firewall exist?
17. Is there documentation detailing the procedure for manual failover to the offline backup firewall?
18. Is there documentation detailing the procedure for ensuring the offline backup firewall is synchronized with the production firewall?
19. Is there a procedure and schedule for downloads of firewall patches and updates?

20. Does **CFG** receive regular notifications from the firewall vendor regarding patches and updates?
21. Does a documented procedure exist for when firewall logs or alarms demonstrate attack patterns?
22. Is firewall log data backed up and retained according to the corporate backup strategy?
23. Under what circumstances is Borderware Support Access enabled?

IT Manager

- 1) Can you produce the following documentation?
 - a) Corporate Policy on Firewall and Internet Access
 - b) Firewall Installation and Configuration Procedures
 - c) Firewall backup and restoration procedures
 - d) Incident response/handling procedures
 - e) URL filtering policy
 - f) Firewall administrators contacts lists
 - g) Change management process
- 2) What physical security is applied to the location of the firewall?
- 3) Has someone been assigned the task of maintaining the firewall administrators contact list?

Helpdesk Manager

1. Are helpdesk personnel aware of their roles in the incident handling procedure?
2. Are helpdesk personnel aware of firewall administrators contact list?
3. Can you access the firewall using one of your standard administration passwords?

Network Manager

1. Do additional connections to the Internet exist from any computers (either stand-alone or on the network) in the local or regional offices?
2. If there are stand-alone systems connected to the Internet via a 3rd party ISP, is there a procedure to ensure data transfer between the systems is secure and does not compromise the security of the production network?
3. Did war-dialing determine if any modems were active on network systems?

Sample User

1. Are you aware of the existence of a URL filter (allows or denies access to public websites based on content) on the **CFG** network?
2. Do you understand how this works?

App. 3 – NMAP and Nessus Scan Results

Nmap Scan Report on External Interface

```
nmap (V. 2.54BETA22) scan initiated Mon Nov 11 14:10:32 2002 as:
nmap -sA -PT -PI -n -O -v -oN nmap-ext-A xxx.yyy.1.9
Warning: OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
Interesting ports on (xxx.yyy.1.9):
(The 1537 ports scanned but not shown below are in state: filtered)
Port      State      Service
20/tcp    UNfiltered  ftp-data
25/tcp    UNfiltered  smtp
80/tcp    UNfiltered  http
54320/tcp UNfiltered  bo2k
65301/tcp UNfiltered  pcanywhere
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=2.54BETA22%P=i386-redhat-linux-gnu%D=11/11%Time=3DD00163%O=-1%C=-1)
T5(Resp=N)
T6(Resp=Y%DF=N%W=0%ACK=0%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=N)
# Nmap run completed at Mon Nov 11 14:13:39 2002 -- 1 IP address (1 host up)
scanned in 187 seconds

#nmap (V. 2.54BETA22) scan initiated Mon Nov 11 13:55:06 2002 as:
nmap -sS -PT -PI -n -O -v -oN nmap-ext xxx.yyy.1.9
Interesting ports on (xxx.yyy.1.9):
(The 1538 ports scanned but not shown below are in state: filtered)
Port      State      Service
25/tcp    open       smtp
80/tcp    open       http
54320/tcp closed     bo2k
65301/tcp closed     pcanywhere

No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=2.54BETA22%P=i386-redhat-linux-gnu%D=11/11%Time=3DCFFDC0%O=25%C=54320)
TSeq(Class=TR%IPID=I%TS=U)
T1(Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=M)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=M)
T4(Resp=Y%DF=N%W=0%ACK=0%Flags=R%Ops=)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=0%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=N)
TCP Sequence Prediction: Class=truly random
                        Difficulty=9999999 (Good luck!)
IPID Sequence Generation: Incremental
Nmap run completed at Mon Nov 11 13:58:08 2002 -- 1 IP address (1 host up)
scanned in 182 seconds

nmap (V. 2.54BETA22) scan initiated Mon Nov 11 14:08:50 2002 as:
nmap -sT -PT -PI -n -O -v -oN nmap-ext-T xxx.yyy.1.9
Interesting ports on (xxx.yyy.1.9):
(The 1538 ports scanned but not shown below are in state: filtered)
Port      State      Service
25/tcp    open       smtp
80/tcp    open       http
```

```

54320/tcp  closed      bo2k
65301/tcp  closed      pcanywhere

No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=2.54BETA22%P=i386-redhat-linux-gnu%D=11/11%Time=3DD000DE%O=25%C=54320)
TSeq(Class=TR%IPID=I%TS=U)
T1(Resp=Y%DF=Y%W=402E%ACK=S+++Flags=AS%Ops=M)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=402E%ACK=S+++Flags=AS%Ops=M)
T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=N%W=0%ACK=S+++Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=N)

TCP Sequence Prediction: Class=truly random
                        Difficulty=9999999 (Good luck!)
IPID Sequence Generation: Incremental
# Nmap run completed at Mon Nov 11 14:11:26 2002 -- 1 IP address (1 host up)
scanned in 156 seconds

# nmap (V. 2.54BETA22) scan initiated Mon Dec  9 13:07:24 2002 as:
nmap -sU -P0 -n -O -v -T3 -oN nmapudpx xxx.yyy.1.9
Warning: OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
All 1453 scanned ports on (xxx.yyy.1.9) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=2.54BETA22%P=i386-redhat-linux-gnu%D=12/9%Time=3DF4E393%O=-1%C=-1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)
# Nmap run completed at Mon Dec  9 13:40:19 2002 -- 1 IP address (1 host up)
scanned in 1975 seconds

```

Nessus Scan Report on External Interface

| Nessus Scan Report | |
|--|---------------------------|
| This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats. | |
| Scan Details | |
| Hosts which where alive and responding during test | 1 |
| Number of security holes found | 0 |
| Number of security warnings found | 1 |
| Host List | |
| Host(s) | Possible Issue |
| xxx.yyy.1.9 | Security warning(s) found |

| Analysis of Host | | |
|--|---------------------------------|---|
| Address of Host | Port/Service | Issue regarding Port |
| xxx.yyy.1.9 | domain (53/udp) | Security warning(s) found |
| Security Issues and Fixes: xxx.yyy.1.9 | | |
| Type | Port | Issue and Fix |
| Warning | domain (53/udp) | <p>The remote name server allows recursive queries to be performed by the host running nssusd.</p> <p>If this is your internal nameserver, then forget this warning.</p> <p>If you are probing a remote nameserver, then it allows anyone to use it to resolve third parties names (such as www.nessus.org). This allows hackers to do cache poisoning attacks against this nameserver.</p> <p>Solution : Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it). If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf</p> <p>If you are using another name server, consult its documentation.</p> <p>Risk factor : Serious CVE : CVE-1999-0024</p> |

This file was generated by [Nessus](#), the open-sourced security scanner.

© SANS

Nmap Scan Report on SSN Interface

```
# nmap (V. 2.54BETA22) scan initiated Mon Nov 25 13:25:56 2002 as:
nmap -sA -P0 -n -O -v -T3 -oN nmapssnA 10.0.0.1
Warning: OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
All 1542 scanned ports on (10.0.0.1) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=2.54BETA22%P=i386-redhat-linux-gnu%D=11/25%Time=3DE27584%O=-1%C=-1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)
# Nmap run completed at Mon Nov 25 14:09:56 2002 -- 1 IP address (1 host up)
scanned in 2640 seconds
```

```
# nmap (V. 2.54BETA22) scan initiated Mon Nov 25 13:25:56 2002 as:
nmap -sA -P0 -n -O -v -T3 -oN nmapssnA 10.0.0.1
Warning: OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
All 1542 scanned ports on (10.0.0.1) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=2.54BETA22%P=i386-redhat-linux-gnu%D=11/25%Time=3DE27584%O=-1%C=-1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)
# Nmap run completed at Mon Nov 25 14:09:56 2002 -- 1 IP address (1 host up)
scanned in 2640 seconds
```

```
# nmap (V. 2.54BETA22) scan initiated Mon Nov 25 13:25:19 2002 as:
nmap -sT -P0 -n -O -v -T3 -oN nmapssnT 10.0.0.1
Warning: OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
All 1542 scanned ports on (10.0.0.1) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=2.54BETA22%P=i386-redhat-linux-gnu%D=11/25%Time=3DE27255%O=-1%C=-1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)
# Nmap run completed at Mon Nov 25 13:56:21 2002 -- 1 IP address (1 host up)
scanned in 1862 seconds
```

```
# nmap (V. 2.54BETA22) scan initiated Tue Dec 10 09:46:37 2002 as:
nmap -sU -P0 -n -O -v -T3 -oN nmapudpS 10.0.0.1
Warning: OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
All 1453 scanned ports on (10.0.0.1) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=2.54BETA22%P=i386-redhat-linux-gnu%D=12/10%Time=3DF60604%O=-1%C=-1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)
# Nmap run completed at Tue Dec 10 10:19:32 2002 -- 1 IP address (1 host up)
scanned in 1975 seconds
```

Nessus Scan Report on SSN Interface

| Nessus Scan Report | | |
|--|-----------------------------|--|
| This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats. | | |
| Scan Details | | |
| Hosts which where alive and responding during test | 1 | |
| Number of security holes found | 0 | |
| Number of security warnings found | 0 | |
| Host List | | |
| Host(s) | Possible Issue | |
| 10.0.0.1 | Security note(s) found | |
| [return to top] Analysis of Host | | |
| Address of Host | Port/Service | Issue regarding Port |
| 10.0.0.1 | general/tcp | Security notes found |
| Security Issues and Fixes: 10.0.0.1 | | |
| Type | Port | Issue and Fix |
| Informational | general/tcp | The remote host is considered as dead - not scanning |

This file was generated by [Nessus](#), the open-sourced security scanner.

Nmap Scan report on Internal Interface

```
# nmap (V. 2.54BETA22) scan initiated Mon Nov 25 12:50:26 2002 as:
nmap -sA -PT -PI -n -O -v -T3 -oN nmapIntA 172.16.6.1
Warning: OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
Interesting ports on (172.16.6.1):
(The 1530 ports scanned but not shown below are in state: filtered)
Port      State      Service
20/tcp    UNfiltered  ftp-data
21/tcp    UNfiltered  ftp
25/tcp    UNfiltered  smtp
80/tcp    UNfiltered  http
109/tcp   UNfiltered  pop-2
110/tcp   UNfiltered  pop-3
441/tcp   UNfiltered  decvms-sysmgmt
442/tcp   UNfiltered  cvc_hostd
443/tcp   UNfiltered  https
8080/tcp  UNfiltered  http-proxy
54320/tcp UNfiltered  bo2k
65301/tcp UNfiltered  pcanywhere

Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo (V=2.54BETA22%P=i386-redhat-linux-gnu%D=11/25%Time=3DE2639F%O=-1%C=-1)
T5 (Resp=N)
```


3/6/2003 9:15 AM

```

T6 (Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7 (Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU (Resp=N)

# Nmap run completed at Mon Nov 25 12:53:35 2002 -- 1 IP address (1 host up)
scanned in 189 seconds

# nmap (V. 2.54BETA22) scan initiated Mon Nov 25 12:48:38 2002 as:
nmap -sS -PI -PT -n -O -v -T3 -oN nmapIntS 172.16.6.1
Interesting ports on (172.16.6.1):
(The 1531 ports scanned but not shown below are in state: filtered)
Port      State      Service
21/tcp    open       ftp
25/tcp    open       smtp
80/tcp    open       http
109/tcp   open       pop-2
110/tcp   open       pop-3
441/tcp   open       decvms-sysmgt
442/tcp   open       cvc_hostd
443/tcp   open       https
8080/tcp  open       http-proxy
54320/tcp closed     bo2k
65301/tcp closed     pcan anywhere

No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo (V=2.54BETA22%P=i386-redhat-linux-gnu%D=11/25%Time=3DE26337%O=21%C=54320)
TSeq (Class=TR%IPID=I%TS=U)
T1 (Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=M)
T2 (Resp=N)
T3 (Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=M)
T4 (Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T5 (Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6 (Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7 (Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU (Resp=N)
TCP Sequence Prediction: Class=truly random
                        Difficulty=9999999 (Good luck!)
IPID Sequence Generation: Incremental
# Nmap run completed at Mon Nov 25 12:51:51 2002 -- 1 IP address (1 host up)
scanned in 193 seconds

# nmap (V. 2.54BETA22) scan initiated Mon Nov 25 12:49:34 2002 as:
nmap -sT -PI -PT -n -O -v -T3 -oN nmapIntT 172.16.6.1
Interesting ports on (172.16.6.1):
(The 1531 ports scanned but not shown below are in state: filtered)
Port      State      Service
21/tcp    open       ftp
25/tcp    open       smtp
80/tcp    open       http
109/tcp   open       pop-2
110/tcp   open       pop-3
441/tcp   open       decvms-sysmgt
442/tcp   open       cvc_hostd
443/tcp   open       https
8080/tcp  open       http-proxy
54320/tcp closed     bo2k
65301/tcp closed     pcan anywhere

No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo (V=2.54BETA22%P=i386-redhat-linux-gnu%D=11/25%Time=3DE26347%O=21%C=54320)
TSeq (Class=TR%IPID=I%TS=U)

```

```
T1 (Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=M)
T2 (Resp=N)
T3 (Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=M)
T4 (Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T5 (Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6 (Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7 (Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU (Resp=N)

TCP Sequence Prediction: Class=truly random
                        Difficulty=9999999 (Good luck!)
IPID Sequence Generation: Incremental

# Nmap run completed at Mon Nov 25 12:52:07 2002 -- 1 IP address (1 host up)
scanned in 153 seconds

# nmap (V. 2.54BETA22) scan initiated Mon Dec 9 13:51:00 2002 as:
nmap -sU -PT -PI -n -O -v -T3 -oN nmapudpI 172.16.6.1
Warning: OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
All 1453 scanned ports on (172.16.6.1) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo (V=2.54BETA22%P=i386-redhat-linux-gnu%D=12/9%Time=3DF4E67E%O=-1%C=-1)
T5 (Resp=N)
T6 (Resp=N)
T7 (Resp=N)
PU (Resp=N)
# Nmap run completed at Mon Dec 9 13:52:46 2002 -- 1 IP address (1 host up)
scanned in 106 seconds
```

Nessus Scan Report for Internal Interface

| Nessus Scan Report | |
|--|---------------------------|
| This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats. | |
| Scan Details | |
| Hosts which were alive and responding during test | 1 |
| Number of security holes found | 0 |
| Number of security warnings found | 3 |
| Host List | |
| Host(s) | Possible Issue |
| 172.16.6.1 | Security warning(s) found |
| Analysis of Host | |
| | |

| | | |
|---------------------------------------|-------------|---------------------------|
| 172.16.6.1 | general/tcp | Security warning(s) found |
| Security Issues and Fixes: 172.16.6.1 | | |
| | | |

host sent a packet in reply to another request. This may be used for portscanning and other things.

Solution : Contact your vendor for a patch
Risk factor : Low

This file was generated by Nessus, the open-sourced security scanner. External to Internal Nmap Scan

External to Internal Nmap Scan

```
# nmap (V. 2.54BETA22) scan initiated Fri Nov 22 14:04:57 2002 as:
nmap -sS -P0 -n -O -v -T3 -oN nmapx-I 172.16.6.1-2
Warning: OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
All 1542 scanned ports on (172.16.6.1) are: filtered
Too many fingerprints match this host for me to give an accurate OS
guess
TCP/IP fingerprint:
SInfo (V=2.54BETA22%P=i386-redhat-linux-gnu%D=11/22%Time=3DDE894A%O=-
1%C=-1)
T5 (Resp=N)
T6 (Resp=N)
T7 (Resp=N)
PU (Resp=N)

Warning: OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
All 1542 scanned ports on (172.16.6.2) are: filtered
Too many fingerprints match this host for me to give an accurate OS
guess
TCP/IP fingerprint:
SInfo (V=2.54BETA22%P=i386-redhat-linux-gnu%D=11/22%Time=3DDE92F1%O=-
1%C=-1)
T5 (Resp=N)
T6 (Resp=N)
T7 (Resp=N)
PU (Resp=N)
# Nmap run completed at Fri Nov 22 15:26:25 2002 -- 2 IP addresses (2
hosts up) scanned in 4888 seconds
```

External to Internal Nessus Scan

Nessus Scan Report

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details

| | |
|-----------------------------------|----------------|
| during test | |
| Number of security holes found | 0 |
| Number of security warnings found | 0 |
| Host List | |
| Host(s) | Possible Issue |

This file was generated by Nessus, the open-sourced security scanner.

External to SSN Nmap Scan

```
# nmap (V. 2.54BETA22) scan initiated Fri Nov 22 12:34:20 2002 as:
nmap -sS -P0 -n -O -v -T3 -oN nmapx-s 10.0.0.1-2
Warning: OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
All 1542 scanned ports on (10.0.0.1) are: filtered
Too many fingerprints match this host for me to give an accurate OS
guess
TCP/IP fingerprint:
SInfo (V=2.54BETA22%P=i386-redhat-linux-gnu%D=11/22%Time=3DDE74C2%O=-
1%C=-1)
T5 (Resp=N)
T6 (Resp=N)
T7 (Resp=N)
PU (Resp=N)

Warning: OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
All 1542 scanned ports on (10.0.0.2) are: filtered
Too many fingerprints match this host for me to give an accurate OS
guess
TCP/IP fingerprint:
SInfo (V=2.54BETA22%P=i386-redhat-linux-gnu%D=11/22%Time=3DDE7E51%O=-
1%C=-1)
T5 (Resp=N)
T6 (Resp=N)
T7 (Resp=N)
PU (Resp=N)

# Nmap run completed at Fri Nov 22 13:58:25 2002 -- 2 IP addresses (2
hosts up) scanned in 5045 seconds
```

External to SSN Nessus Scan

| |
|--|
| Nessus Scan Report |
| This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats. |
| Scan Details |

| | | |
|--|------------------------|--|
| Hosts which where alive and responding during test | 2 | |
| Number of security holes found | 0 | |
| Number of security warnings found | 0 | |
| Host List | | |
| Host(s) | Possible Issue | |
| 10.0.0.2 | Security note(s) found | |
| 10.0.0.1 | Security note(s) found | |
| [return to top]Analysis of Host | | |
| Address of Host | Port/Service | Issue regarding Port |
| 10.0.0.2 | general/udp | Security notes found |
| Security Issues and Fixes: 10.0.0.2 | | |
| Type | Port | Issue and Fix |
| Informational | general/udp | For your information, here is the traceroute to 10.0.0.2 : xxx.yyy.1.1 xxx.yyy.1.225 aaa.bbb.16.9 aaa.bbb.28.25 ? |
| Analysis of Host | | |
| Address of Host | Port/Service | Issue regarding Port |
| 10.0.0.1 | general/udp | Security notes found |
| Security Issues and Fixes: 10.0.0.1 | | |
| Type | Port | Issue and Fix |
| Informational | general/udp | For your information, here is the traceroute to 10.0.0.1 : xxx.yyy.1.1 xxx.yyy.1.225 aaa.bbb.16.9 aaa.bbb.28.25 ? |

This file was generated by Nessus, the open-sourced security scanner.

SSN to Internal Nmap Scan

```
# nmap (V. 2.54BETA22) scan initiated Mon Nov 25 09:04:55 2002 as:
nmap -sS -P0 -n -O -v -T3 -oN nmapS-I 172.16.6.1-2
Warning: OS detection will be MUCH less reliable because we did not
```

```

find at least 1 open and 1 closed TCP port
All 1542 scanned ports on (172.16.6.1) are: filtered
Too many fingerprints match this host for me to give an accurate OS
guess
TCP/IP fingerprint:
SInfo (V=2.54BETA22%P=i386-redhat-linux-gnu%D=11/25%Time=3DE2382D%O=-
1%C=-1)
T5 (Resp=N)
T6 (Resp=N)
T7 (Resp=N)
PU (Resp=N)

Warning: OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
All 1542 scanned ports on (172.16.6.2) are: filtered
Too many fingerprints match this host for me to give an accurate OS
guess
TCP/IP fingerprint:
SInfo (V=2.54BETA22%P=i386-redhat-linux-gnu%D=11/25%Time=3DE241BC%O=-
1%C=-1)
T5 (Resp=N)
T6 (Resp=N)
T7 (Resp=N)
PU (Resp=N)

# Nmap run completed at Mon Nov 25 10:29:00 2002 -- 2 IP addresses (2
hosts up) scanned in 5045 seconds

```

SSN to Internal Nessus Scan

| Nessus Scan Report | |
|--|------------------------|
| This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats. | |
| Scan Details | |
| Hosts which where alive and responding during test | 2 |
| Number of security holes found | 0 |
| Number of security warnings found | 0 |
| Host List | |
| Host(s) | Possible Issue |
| 172.16.6.2 | Security note(s) found |
| 172.16.6.1 | Security note(s) found |
| Analysis of Host | |
| | |
| | |
| | |

| Address of Host | Port/Service | Issue regarding Port |
|---------------------------------------|--------------|--|
| 172.16.6.2 | general/tcp | Security notes found |
| Security Issues and Fixes: 172.16.6.2 | | |
| Type | Port | Issue and Fix |
| Informational | general/tcp | The remote host is considered as dead - not scanning |
| Analysis of Host | | |
| Address of Host | Port/Service | Issue regarding Port |
| 172.16.6.1 | general/tcp | Security notes found |
| Security Issues and Fixes: 172.16.6.1 | | |
| Type | Port | Issue and Fix |
| Informational | general/tcp | The remote host is considered as dead - not scanning |

This file was generated by Nessus, the open-sourced security scanner.

© SANS Institute 2003, All Rights Reserved

App. 4 – Release Notes for Security Patch 1

BorderWare Firewall Server 6.5

Service Patch 1

Release Notes, May 13 2002

Features:

HALO:

- 1 There is now a top level menu on the Firewall console to allow for easier access and configuration of HALO (High Availability Option).
- 2 The ability to specify an email address so that changes in status messages are sent to this address has been added. This option can be found under the "Advanced" menu for HALO configuration.
- 3 A new item to the "Interface" dialogue called "Enable carrier detect" has been added. This option allows you to disable/enable carrier detects for each interface on the Firewall. Most customers should leave this option enabled. This option should be disabled only in rare instances such as when a Firewall NIC does not handle carrier detects properly.
- 4 The maximum failover interval has been increased to 300 seconds.

ICMP Redirects

- 1 The ability to ignore ICMP redirects has been added to the Firewall. When ICMP Redirects are ignored, the Firewall will NOT change its routing when it is issued an ICMP redirect from a router. The Firewall will continue to send the packets to the route listed in its routing table. This option can be found on the Firewall console under *Misc -- Configure ICMP redirect*.

Corrections:

- 1 **Automatic Tape Backup:** After installing Feature Pack A, the nightly tape backups would no longer work. This has been corrected.
- 2 **Proxy Server:**
 - a) The Proxy Server has been updated to address a problem that would occur when accessing certain URLs that would cause the Proxy Server to stop processing web requests until it was restarted.
 - b) JavaScript filter debug logging has been now disabled.
 - c) The Proxy Server will no longer start twice on boot up.
 - d) The Proxy Server has been patched to address FreeBSD Security Advisory SA-02:19 - "Squid heap buffer overflow in DNS handling".
- 3 **FTP Proxy:** For inbound passive mode FTP connections, the Firewall will now correctly handle IP address checks performed by internal FTP servers.
- 4 **Access Rules:** Access rules can now be applied to proxies without requiring the proxy to be restarted.

3/6/2003 9:15 AM

- 5 **SNMP:** The SNMP daemon has been upgraded to version 4.2.3 to address FreeBSD Security Advisory SA-02:11 - "Ucd-snmp/net-snmp remotely exploitable vulnerabilities".
- 6 **SSH:** The SSH daemon has been patched to address FreeBSD Security Advisory SA-02:13 - "OpenSSH contains exploitable off-by-one bug".
- 7 **SMTP Email Proxy:** Previously the Internal to External SMTP proxy did not work when the Internal to SSN SMTP proxy was enabled. This has been corrected.
- 8 **Web access** will no longer stop if SmartFilter is unable to do a reverse lookup on an IP address.

Dependencies: Feature Pack A (fs65f0a.pf)

Exclusions: none

© SANS Institute 2003, Author retains full rights.

References

The following texts are referred to throughout the document. Where applicable the relevant URL is included. The date in (brackets) refers to the date that the URL was accessed for the purposes of this document. Please note that the Internet is dynamic in nature and while all URLs were active and valid at the time of access, no responsibility can be taken by the author if these links have subsequently become invalid.

¹ Borderware Firewall Server, Reference Guide, Revision B, July 2000

Introducing the Firewall Server, Pg. 7

<http://www.borderware.com/products/fw/reference-guide.pdf> (Dec 11, 2002)

² Security Target for BorderWare Firewall Server 6.5, January 2002

Features, Pg. 9

http://www.cesg.gov.uk/assurance/iacs/itsec/cpl/media/sectarg/borderware6_5.pdf (Dec 7, 2002)

³ Security Target for BorderWare Firewall Server 6.5, January 2002

Features, Pg. 9

http://www.cesg.gov.uk/assurance/iacs/itsec/cpl/media/sectarg/borderware6_5.pdf (Dec 7, 2002)

⁴ Borderware Firewall Server, Reference Guide, Revision B, July 2000

Administering Firewall Server, BWClient, Pg. 25

<http://www.borderware.com/products/fw/reference-guide.pdf> (Dec 11, 2002)

⁵ Borderware Firewall Server, Reference Guide Revision B, July 2000

Introducing the Borderware Firewall Server, Pg. 7

<http://www.borderware.com/products/fw/reference-guide.pdf> (Dec 11, 2002)

⁶ Security Target for BorderWare Firewall Server 6.5, January 2002

Features Pg. 9-10

http://www.cesg.gov.uk/assurance/iacs/itsec/cpl/media/sectarg/borderware6_5.pdf (Dec 7, 2002)

⁷ Lowder, Lt Jeffrey L., Firewall Management and Internet Attacks, Information Security Management Handbook 4th Edition, Chapter 7, Auerbach, 2000, Packet Filtering, Pg. 120

⁸ Borderware Firewall Server, Reference Guide Revision B, July 2000

Packet Filtering Pg. 9

<http://www.borderware.com/products/fw/reference-guide.pdf> (Dec 11, 2002)

⁹ Lowder, Lt Jeffrey L., Firewall Management and Internet Attacks, Information Security Management Handbook 4th Edition, Auerbach, 2000, Chapter 7, Application Level Gateways, Pg. 121

¹⁰ Borderware Firewall Server, Reference Guide Revision B, July 2000

Security Architecture, Circuit level Gateways P.10

<http://www.borderware.com/products/fw/reference-guide.pdf> (Dec 11, 2002)

¹¹ Borderware Security Server Appliance Home Pg.

<http://www.borderware.com/products/hardware/index.html/> (Dec 5, 2002)

¹² Borderware Firewall Server, Reference Guide Revision B, July 2000

Security Architecture, Operating System Platform, Pg. 9

<http://www.borderware.com/products/fw/reference-guide.pdf> (Dec 11, 2002)

- ¹³ Security Target for BorderWare Firewall Server 6.5, January 2002
Security Target Overview, Pg. 7
http://www.cesg.gov.uk/assurance/iacs/itsec/cpl/media/sectarg/borderware6_5.pdf (Dec 7, 2002)
- ¹⁴ Communications Electronic Security Group (CESG/UKITSec), Common Criteria Certification Report No. P164, January 2002
Product security Architecture Pg.26-29
<http://www.cesg.gov.uk/assurance/iacs/itsec/cpl/media/certreps/CRP164.pdf> (Dec 10, 2002)
- ¹⁵ Website of the Communications Electronic Security Group (CESG),
<http://www.cesg.gov.uk/> (Dec, 10 2002)
- ¹⁶ Borderware Firewall Server, Reference Guide Revision B, July 2000
Network Address Translation (NAT), Pg. 10
<http://www.borderware.com/products/fw/reference-guide.pdf> (Dec 11, 2002)/
- ¹⁷ Smartfilter URL filtering software home page
<http://www.securecomputing.com/index.cfm?skey=85> (Dec 11, 2002)
- ¹⁸ Carnegie Mellon Software Engineering Institute, CERT Co-ordination Center
Security Improvement Practices
Testing the Firewall System – Why this is important!, May 2001
<http://www.cert.org/security-improvement/practices/p060.html> (Dec 11, 2002)
- ¹⁹ Hoelzer, Dave. Auditing Principles and Concepts, Version 1.1a
SANS Audit Track 7, Section 7.1., How Does Auditing Help?, Risk Assessment, Pg. 57
- ²⁰ Checkpoint Firewall-1 website home page
<http://www.checkpoint.com/products/protect/firewall-1.html> (Dec 11, 2002)
- ²¹ Cisco PIX 500 Series Firewalls website home page
<http://www.cisco.com/warp/public/cc/pd/fw/sqfw500> (Dec 11, 2002)
- ²² Symantec Enterprise Firewall 7.0 (Formerly Raptor Firewall) website home page
<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=47> (Dec 11, 2002)
- ²³ Borderware 6.5 Firewall Server website home page
<http://www.borderware.com/newsite/products/fw/fwserver.html> (Dec 11, 2002)
- ²⁴ Press Release: Borderware Firewall Server V6.5 placed on CSE approved security products list, May 2002
<http://www.borderware.com/news/cselist.html> (Dec 1, 2002)
- ²⁵ Communications Security Establishment (CSE) ITS Pre-qualified Product List, Nov 2002
http://www.cse-cst.gc.ca/en/services/industrial_services/products/borderware.html (Dec 1, 2002)
- ²⁶ Common Criteria Assurance Levels - Overview
<http://www.commoncriteria.org/epl/AssuranceLevel/index.html> (Dec 1, 2002)
- ²⁷ Common Criteria website and information about the Common Criteria initiative
<http://www.commoncriteria.org/docs/aboutus.html> (Dec 1, 2002)

-
- ²⁸ Information on the Borderware Firewall Server V6.5's Common Criteria Evaluation
<http://www.commoncriteria.org/ccc/epl/productType/epldetail.jsp?id=81> (Dec 1, 2002)
- ²⁹ Frequently Asked Questions on Borderware Firewall Servers's EAL4 Certification, January 2000
<http://www.borderware.com/news/eal4faq.pdf> (Dec 11, 2002)
- ³⁰ Borderware Firewall Server, Reference Guide Revision B, July 2000
Certification, Pg. 8
<http://www.borderware.com/products/fw/reference-guide.pdf> (Dec 11, 2002)
- ³¹ Common Criteria for Information Technology Security Evaluation,
Introduction and General Model Part 1, Version 2.1 August 1999,
Foreword, Legal Notice Pg. II
<http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF> (Dec 1, 2002)
- ³² Lowder, Lt Jeffrey L., Firewall Management and Internet Attacks, Information Security Management Handbook 4th Edition, Auerbach, 2000, Chapter 7, Benefits of Having a Firewall, Pg. 116
- ³³ Robinson, Chad. Best Practices for Firewall Deployments, October, 2002
<http://www.csoonline.com/analyst/report563.html> (Dec 11, 2002)
- ³⁴ SANS, "The Twenty Most Critical Internet Security Vulnerabilities (Updated) The Experts' Consensus"
Version 2.504, May 2, 2002,
Section G5 (Not filtering packets for correct incoming and outgoing addresses)
Section G4 (Large number of open ports)
Section G6 (non-existent or incomplete logging)
http://www.sans.org/top20/top20_Oct01.htm (Dec 1, 2002)
- ³⁵ Lowder, Lt Jeffrey L., Firewall Management and Internet Attacks, Information Security Management Handbook 4th Edition, Auerbach, 2000, Chapter 7, Developing a Firewall Policy and Standards, Pg. 122
- ³⁶ Borderware Firewall Server, Reference Guide Revision B, July 2000
Thinking about Security, Pg. 22
<http://www.borderware.com/products/fw/reference-guide.pdf> (Dec 11, 2002)
- ³⁷ SANS Course Materials, Auditing the Perimeter, Version 1.0
SANS Audit Track 7, Section 7.2., Auditing Firewalls, The Next Step, Pg. 136
- ³⁸ Spitzner, Lance Auditing your Firewall Setup, December 2000
<http://www.spitzner.net/audit.html> (Nov 31, 2002)
- ³⁹ Oliphant, Alan, "IT Auditing Without Pain - The Internet - Part 10 – Firewalls"
The Institute of Internal Auditors (THEIIA) website, Vol #5, April, 2002
<http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=430> (Nov 29, 2002)
- ⁴⁰ Lindstedt, Sandy "Firewall Audit, Vol. # 2 June, 1999"
The Institute of Internal Auditors (THEIIA) website, April 2002
<http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=179> (Nov 29, 2002)
- ⁴¹ Rochette, Diane. "Audit of Internet Firewall Audit Program" January 2000
<http://www.auditnet.org/docs/firewall%20audit%20program.txt> (Dec 1, 2002)
- ⁴² Nessus website with downloads and documentation
<http://www.nessus.org/intro.html> (Dec 1, 2002)

⁴³ Website with downloads and documentation for NMAP
<http://www.insecure.org/nmap/index.html> (Dec 1, 2002)

⁴⁴ Website containing download and documentation for Ethereal
<http://www.ethereal.com> (Dec 1, 2002)

⁴⁵ COBIT, 3rd Edition, Control Objectives, July 2000
DS9.2, Configuration Baseline

⁴⁶ COBIT, 3rd Edition, Control Objectives, July 2000
DS11.23-DS11.26, Managing Data

⁴⁷ COBIT, 3rd Edition, Control Objectives, July 2000
DS10.1-10.5, Managing Problems and Incidents & DS5.11, Incident Handling

⁴⁸ COBIT, 3rd Edition, Control Objectives, July 2000
AI6.1-6.6, Manage Changes

⁴⁹ Lowder, Lt Jeffrey L., Firewall Management and Internet Attacks, Information Security Management Handbook 4th Edition, Auerbach, 2000, Chapter 7, Firewall Evaluation Criteria, Physical Security, Pg. 119

⁵⁰ COBIT, 3rd Edition, Control Objectives, July 2000,
DS12.6 Uninterruptible Power Supply

⁵¹ Lowder, Lt Jeffrey L., Firewall Management and Internet Attacks, Information Security Management Handbook 4th Edition, Auerbach, 2000, Chapter 7, Firewall Contingency Planning, Pg. 127-128

⁵² Lowder, Lt Jeffrey L., Firewall Management and Internet Attacks, Information Security Management Handbook 4th Edition, Auerbach, 2000, Chapter 7, Limitations of the firewall, Point 2, Pg. 117

⁵³ Borderware Firewall Server, Reference Guide Revision B, July 2000
Using the DNS Server, Pg. 29-33
<http://www.borderware.com/products/fw/reference-guide.pdf> (Dec 11, 2002)

⁵⁴ Borderware Firewall Server, Reference Guide Revision B, July 2000
Using the Email Server, Pg. 33-35
<http://www.borderware.com/products/fw/reference-guide.pdf> (Dec 11, 2002)

⁵⁵ Borderware Firewall Server, Reference Guide Revision B, July 2000
Proxy Server, Pg. 46-49
<http://www.borderware.com/products/fw/reference-guide.pdf> (Dec 11, 2002)

⁵⁶ InsideOut Firewall Reporter website Home Page
<http://www.borderware.com/products/fw/insideout.html> (Dec 13, 2002)

⁵⁷ Borderware Firewall Server, Reference Guide Revision B, July 2000
Smartfilter, Pg. 45-46
<http://www.borderware.com/products/fw/reference-guide.pdf> (Dec 11, 2002)

⁵⁸ COBIT, 3rd Edition, Control Objectives, July 2000
DS5.14, Transaction Authorization

⁵⁹ SANS Course Materials, Auditing the Perimeter, Version 1.0

SANS Audit Track 7, Section 7.2., Auditing Firewalls II, Patches Pg. 204

⁶⁰ SANS Course Materials, Auditing the Perimeter, Version 1.0
SANS Audit Track 7, Section 7.2., Auditing Firewalls II, Logs and Alerts Pg. 240-247

⁶¹ Borderware Firewall Server, Reference Guide Revision B, July 2000
Authentication, Pg. 27
<http://www.borderware.com/products/fw/reference-guide.pdf> (Dec 11, 2002)

⁶² Borderware License Activation Server website
<http://igate.borderware.com/activate.spl> (Dec 1, 2002)

⁶³ Carnegie Mellon Software Engineering Institute,
CERT Co-ordination Center Vulnerability Note #VU109475, August, 2002
<http://www.kb.cert.org/vuls/id/109475> (Dec 1, 2002)

⁶⁴ Borderware Support Center
<http://dgsupport.borderware.com/login.spl> (Dec 1, 2002)

© SANS Institute 2003, Author retains full rights.