GIAC
CERTIFICATIONS

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 permited 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

Stéphane Grundschober

SANS GSNA

Practical Assignment Version 1.0

September 2001

Auditing Firewall in a Small Office / Home Office environment

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Table of content:

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

1 Assignment 1 – Research in Audit, Measurement Practice and Control

1.1 Introduction

In order to complete this assignment, we will look at a firewall device targeted for Small Office / Home Office (SOHO) users. More specifically, we will study the WatchGuard SOHO product [1] (model WG2510). This device performs stateful packet filtering and Network Address Translation (NAT) for 10 to 50 users.
The following sections will present the current state of firewall auditing, and put it in relation with the specific aspects of a SOHO environment. We will see how we can improve actual checklists, and provide a new method/checklist targeted to SOHO. Assignment 2 will demonstrate its use by performing the audit of the WatchGuard device.

1.2 Current state of practice

The main document describing the methodology and tools for auditing a firewall is the SANS documentation [2]. This document is actually based on Lance Spitzner's document "Auditing your Firewall Setup"[3]. It includes a detailed methodology to perform a complete audit of a firewall. SANS document goes further to include organisational aspects like the verification of the existence of a security policy, of it's implementation, of change control, of system administration authorisation, etc.

Both documents include example of tools used to perform OS vulnerability assessment and to check the rule base of the firewall.

They cover all possible aspects of an architecture (from the simple firewall up to the DMZ and screened subnet). Although this makes the methodology complete, it also makes it complex and difficult to use.

It is very difficult to find other good documents on Internet describing an audit methodology. Among the many sites visited[1], none provided practical and complete information. One single document, found on Fred Cohen and Associates' web site, is the "Management Analytics Firewall Checklist" [4]. Unlike other documents, this one has the form of a checklist. This allows the auditor to go systematically from beginning to end answering simple questions, mostly by "yes" or "no". This checklist covers also most aspects of an audit, from management awareness to technical details.

As far as these methods or checklists provide a methodology to gather the audit information, the evaluation, and especially the decision "passed/not passed" is largely left to the auditor's feeling.

1.3 Need of improvement

An auditor following these methodologies will surely perform an excellent study of his equipment, but will need to do a large amount of work to turn the methodology into the actual audit procedure adapted to his architecture or environment. We would like to have something looking more like a checklist. Unfortunately, once a

[1] http://www.auditnet.org/isaudit.htm , http://www.firewallguide.com , http://www.isaca.org , http://www.securityfocus.com , http://www.securityportal.com , http://www.cert.org , …

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

methodology is turned into a checklist, it is either unusable (too big, too many options), or tied to a specific architecture.

Although both options are not completely satisfying, the second one is still interesting. Indeed, once work has been placed to transform a methodology into a checklist for a specific architecture (like a SOHO environment), this checklist can be reused without problems in the same environment. The challenge is to find an environment which is susceptible to be found at many different places, but doesn't change much. This is the path we will follow in the next section.

By deciding to follow the option of designing a specific checklist for SOHO environment, we will need to adapt the general methodology to the specific aspects of SOHO. Especially, we will have to look at the implication of a small organisation (a couple of computers at most, one Firewall device, no DMZ, one single administrator, …) on various aspects of the methodology. For example, it doesn't make much sense for the Firewall administrator to ask for authorisation to the Chief Information Officer when both are the same person!

1.4 The refined method/checklist

1.4.1 A typical SOHO environment

In order to prepare an adequate audit checklist, we need to define a generic SOHO environment, along with the security policy associated with the firewall.

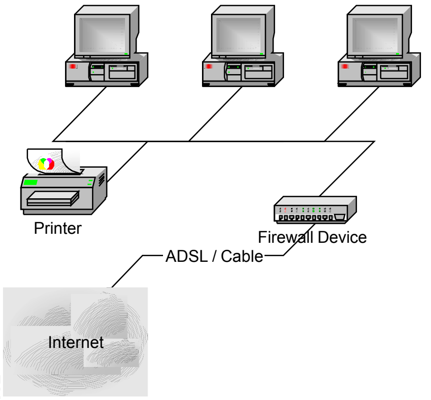


Figure 1: A simple but typical SOHO environment

Figure 1 shows a typical network architecture for SOHO. A couple of PCs (in the meaning of Personal Computer) are connected together, and access the Internet via the Firewall appliance.

In most of the cases, Email and web pages are hosted by the ISP supplying the ADSL or Cable connection. There is therefore no need for a web or mail server within the SOHO network.

The following table describes the various information flow susceptible to be found:

Application	**Protocol**	**Direction** (arrow indicates who initiate the connection; in case of UDP, who sends the first packet)

© SANS Institute 2000 - 2005 Author retains full rights.

Web	http, https	PC -> Internet
Email	pop, imap, smtp	PC -> ISP mail servers
News	nntp	PC -> ISP news server
FTP	ftp	PC -> Internet
File sharing, printing	SMB, Appleshare, …	PC <-> PC
DNS	DNS	PC -> Internet (perhaps relayed/cached by FW)
DHCP (intern)	DHCP	PC -> Firewall
DHCP (extern), PPPoE	DHCP, PPPoE	Firewall -> ISP
Firewall management	http or other	PC -> Firewall

The goal of the firewall is to protect the PCs from external attacks, excluding flooding Denial of Service (DoS), which cannot be avoided. It also provides Network Address Translation (NAT) to hide the PCs behind one external IP address.

The firewall may also control outgoing connections, allowing only authorised protocols. This may create an additional workload, as it may be necessary to modify regularly the rule base, depending on the various applications installed. This is especially true with the “auto-update” trend in new applications: they connect to their “home” server to see if an update is available. These connections are either http based, or proprietary.

Two choices are at disposition to the FW admin: either filtering outgoing connections, or allow anything out. In the latter case, a software personal firewall on each PC (Zone Alarm for example [5]) is recommended to enforce application control.

Some firewalls include special applications (antivirus), or application layer filtering (URL filtering). In a typical SOHO environment, these features are mostly not present (often for cost reasons).

1.4.2 Checklist

The checklist will try to take the same approach as document [4], but we will remove elements non-relevant to SOHO environment as well as more organisational checkpoints. The goal of the audit checklist is to make a comparison of “what is” to “what should be”, targeted on the firewall box. We will include additional practical (objective) checks from document [2].

Each check will have the following format, describing the type of check to perform, if it is an objective or subjective criteria[2], under which conditions the audited system is in or out of specification, and finally a checkbox indicating if this particular check is passed or not[3].

[2] An objective criteria is the result of tool, command, etc… A subjective criteria is information got from people (interview) or documents (who may not reflect the reality).

[3] Checkbox that will not be used before the actual audit ! (Assignment 2)

© SANS Institute 2000 - 2005 Author retains full rights.

Check	objective subjective
Acceptance criteria	
Comment, command output, …	passed?

1.4.2.1 Basic Firewall Functionality

The control objectives of the firewall is to play the role of “traffic cop”, controlling in- and out-going traffic.	objective subjective
This should be it’s only control objective, i.e. it doesn’t take the role of authentication, authorisation, accounting, etc… (subjective) The Firewall must have two physical interfaces (objective).	
	passed?

The firewall is designed to protect inside systems from exploitation by outside threats.	objective subjective
The specification of the Firewall includes incoming traffic filtering functionality.	
	passed?

The firewall is designed to protect outside systems from exploitation by inside threats.	objective subjective
The specification of the Firewall includes outgoing traffic filtering functionality.	
	passed?

The firewall is designed to protect itself against being used by attackers as a launch point for attacking other systems.	objective subjective
The firewall must be a single purpose box, with limited generic functionality.	
	passed?

The firewall is designed to prevent the corruption or leakage of sensitive information.	objective subjective
The specification of the Firewall must include filtering functionality per host and service. The administrator must know what are sensitive information and what access methods exist within the network.	
	passed?

1.4.2.2 Policy Issues

Effective firewall protection is supported within the SOHO.	objective subjective
Interview with decision makers show a clear support into firewall protection	
	passed?

© SANS Institute 2000 - 2005 Author retains full rights.

Decision makers understand that a firewall is not a magic solutions, and that additional measures have been taken to secure internal systems.	objective subjective
Interview must show this understanding.	
	passed?

The Firewall protection policy identifies the specific assets that the firewall is intended to protect and those are the proper assets.	objective subjective
The network architecture is similar to the one described at point 1.4.1 and the policy specifies similar traffic flow controls.	
	passed?

The policy specifies who is responsible of the firewall and provides the responsible individual with adequate control to carry out the policy.	objective subjective
Check the policy document. Ask the responsible if he/she is the only person who can change something to the firewall.	
	passed?

1.4.2.3 Documentation and change control

Firewall configuration change control process exists.	objective subjective
The document exist	
	passed?

The actual configuration of the firewall is documented, including traffic flows and network architecture.	objective subjective
The document exist and is up-to-date.	
	passed?

Changes to the firewall configuration are done by the responsible only.	objective subjective
Only the responsible knows the management password.	
	passed?

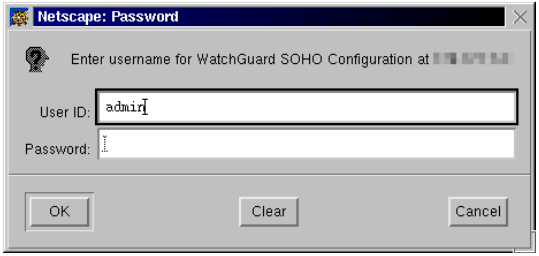
Changes to the firewall configuration are documented.	objective subjective
Change control is implemented as paper or electronic documents.	
	passed?

© SANS Institute 2000 - 2005 Author retains full rights.

A minimum of information must be documented with each change.	objective subjective
Each change control document includes the name of the individual who added/modified a configuration, the date and the reason for the configuration. This is confirmed by looking at the actual documents.	
	passed?

A configuration/rule backup strategy is documented and implemented.	objective subjective
The strategy is implemented and works (has been tested)	
	passed?

1.4.2.4 System Administration

The administration of the firewall is protected by a password.	objective subjective
Connect to the firewall (remote admin) or access the console (local admin) and verify the access control mechanism.	
As an example, the picture on the right shows the access control of the Watchguard SOHO FW.  Netscape: Password Enter username for WatchGuard SOHO Configuration at [redacted] User ID: admin Password: 	passed?

A password policy exists and is followed.	objective subjective
Verify that the admin password complies with the policy. (It will have to be changed at the end of the audit!)	
	passed?

The OS or Firmware of the Firewall has the latest stable patches.	objective subjective
Find the actual patch level of the device and compare it with supplier's information.	
	passed?

Modification of configuration or rules comply with the security policy and documentation.	objective subjective
The administrator confirms to follow the security policy when changing a rule or configuration.	
	passed?

© SANS Institute 2000 - 2005

Author retains full rights.

1.4.2.5 Actual configuration

In this section, we will determine objectively the configuration of the firewall, and check its compliance with the policy and documentation.

There must be no open ports visible from the outside on the firewall itself.

objective
subjective

A tcp syn scan with nmap must show no open ports.

command: `nmap -sS -P0 -O -p 1-65535 -r -T Aggressive xx.xx.xx.xx`

(Syn half-open scan, no ping, OS fingerprinting, all ports, not random order, Aggressive scan speed, xx.xx.xx.xx is the IP address of the Firewall itself on the public side.)

Output example:

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Warning:  No TCP ports found open on this machine, OS detection will be
MUCH less reliable
Interesting ports on  (xx.xx.xx.xx):
Port       State       Service
1/tcp      filtered    tcpmux
2/tcp      filtered    compressnet
3/tcp      filtered    compressnet
4/tcp      filtered    unknown
5/tcp      filtered    rje
6/tcp      filtered    unknown
7/tcp      filtered    echo
8/tcp      filtered    unknown
9/tcp      filtered    discard
10/tcp     filtered    unknown

Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 48 seconds
```

passed?

There must be no open ports visible from the inside on the firewall itself (except the management port).

objective
subjective

A tcp syn scan with nmap must show no open ports (except the management port).

command: `nmap -sS -P0 -p 1-65535 -r -T Aggressive xx.xx.xx.xx`

(Syn half-open scan, no ping, all ports, not random order, Aggressive scan speed, xx.xx.xx.xx is the IP address of the Firewall itself on the private side.)

Output example:

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on  (xx.xx.xx.xx):
(The 5 ports scanned but not shown below are in state: closed)
Port       State       Service
80/tcp     open        http

Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds
```

passed?

© SANS Institute 2000 - 2005 Author retains full rights.

Manual review of the rule base. It must comply to the policy and the traffic flow / architecture diagram.	objective subjective
Use administration commands to get a dump of the rule base. Check if it complies with the authorised traffic (as described in section 1.4.1 for example).	
Example: Output from the management interface of the Watchguard FW.	passed?

```
             Allowed Incoming Services
                No services installed

             Blocked Outgoing Services
                Block TCP requests to port 137 SMB Networking
                Block UDP requests to port 137 SMB Networking
                Block TCP requests to port 1723 PPTP VPN
                Block TCP requests to port 139 SMB Networking
                Block UDP requests to port 138 SMB Networking
                Block protocol 47 requests
                Block UDP port range from port 1 to port 52
                Block UDP port range from port 54 to port 65535
```

Check the correct implementation of the rule base **Outside -> Inside**	objective subjective
Use a tool to generate packets (TCP, UDP, ICMP) from one side of the firewall and tcpdump or another tool to listen for packets on the other side. Anything that goes through must be allowed by the rules and comply with the policy.	
Example of the output of a reporting tool for the ftester [6] tool:	passed?

```
Blocked Services
----------------
< 10.1.227.94:55555 > 10.1.230.118:77 S TCP

Authorised Services
-------------------
10.1.227.94:55555 > 10.1.230.118:78 S TCP
10.1.227.94:55555 > 10.1.230.118:79 S TCP
10.1.227.94:55555 > 10.1.230.118:80 S TCP
10.1.227.94:666 > 10.1.230.118:666 S TCP

Time control:
# Ftestd started on Fri Aug 24 15:43:14 CEST 2001
# Ftest started on Fri Aug 24 15:43:38 CEST 2001
# Ftest stopped on Fri Aug 24 15:43:39 CEST 2001
# Ftestd finished on Fri Aug 24 15:43:40 CEST 2001
```

Check the correct implementation of the rule base **Inside -> Outside**	objective subjective
Use a tool to generate packets (TCP, UDP, ICMP) from one side of the firewall and tcpdump or another tool (ftester [6] for example) to listen for packets on the other side. Anything that goes through must be allowed by the rules and comply with the policy.	
	passed?

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

1.4.2.6 Logging, Detection and Reaction

Verify the logs of the firewall and their effectiveness.	objective subjective
Get a dump of the firewall log, and verify that the previous scans where correctly recorded. It should also include management activities (bad authentication for example).	
	passed?

A log analysis and reaction process exist and is “alive”.	objective subjective
Check the existence of a process to analyse the log. The person responsible must have enough knowledge to recognise unusual situations, and has a reaction plan ready.	
	passed?

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

2 Assignment 2 – Application of Audit Techniques to a Real World System

2.1 Audit

The following pages take the developed checklist, and apply the methodology to the Watchguard Firewall in a typical installation.

In the “Comments” field of each criteria, we use the following color coding:

green: The criteria is fulfilled, the checkbox “passed” can be checked.

purple: The criteria is partially fulfilled, or some items are out of specification. Depending on the gravity of the deviation, the “passed” checkbox may or may not be checked (an explanation is mandatory).

red: The criteria is not fulfilled. The “passed” checkbox is not checked.

Note: The actual IP addresses have been either masked or changed.

2.1.1 Basic Firewall Functionality

The control objectives of the firewall is to play the role of “traffic cop”, controlling in- and out-going traffic.	objective subjective
This should be it’s only control objective, i.e. it doesn’t take the role of authentication, authorisation, accounting, etc… (subjective) The Firewall must have two physical interfaces (objective).	
When interviewing the system administrator, he answered that the role of the firewall was only to block incoming connections, and filter outgoing. By looking at the firewall box itself, we can see two physical Ethernet interfaces (plus a couple of additional ones on the private side)	passed?

The firewall is designed to protect inside systems from exploitation by outside threats.	objective subjective
The specification of the Firewall includes incoming traffic filtering functionality.	
From the Watchguard SOHO feature list [1]: “Internet Security: Protect all of your networked computers with dynamic stateful packet filtering firewall technology. Create filter rules based on port and protocol for both in and outbound traffic.”	passed?

The firewall is designed to protect outside systems from exploitation by inside threats.	objective subjective
The specification of the Firewall includes outgoing traffic filtering functionality.	
From the Watchguard SOHO feature list [1]: “Internet Security: Protect all of your networked computers with dynamic stateful packet filtering firewall technology. Create filter rules based on port and protocol for both in and outbound traffic.”	passed?

© SANS Institute 2000 - 2005 Author retains full rights.

The firewall is designed to protect itself against being used by attackers as a launch point for attacking other systems.	objective subjective
The firewall must be a single purpose box, with limited generic functionality.	
The Watchguard SOHO box is a firewall appliance, running on an unknown but probably proprietary and dedicated Operating System. The CPU is a Toshiba TMRP3907.	passed?

The firewall is designed to prevent the corruption or leakage of sensitive information.	objective subjective
The specification of the Firewall must include filtering functionality per host and service. The administrator must know what are sensitive information and what access methods exist within the network.	
Filtering is based on the port (service). Not on the host. This item is therefore only partially compliant. Nonetheless, in a small environment as the one under audit, this may prove to be enough.	passed?

2.1.2 Policy Issues

Effective firewall protection is supported within the SOHO.	objective subjective
Interview with decision makers show a clear support into firewall protection	
Interview of the decision maker (which happens to be also the administrator!) demonstrates the need and will of firewall protection.	passed?

Decision makers understand that a firewall is not a magic solutions, and that additional measures have been taken to secure internal systems.	objective subjective
Interview must show this understanding.	
The interviewed person demonstrates the use of Antivirus, and is aware of the risk related to the use of internet (Outlook clients updated, Internet Explorer patched, ActiveX disabled).	passed?

The Firewall protection policy identifies the specific assets that the firewall is intended to protect and those are the proper assets.	objective subjective
The network architecture is similar to the one described at point 1.4.1 and the policy specifies similar traffic flow controls.	
The policy defines the following allowed traffic in order to protect the internal PCs: Incoming: None Outgoing: DNS, HTTP, HTTPS, FTP, NNTP, POP3, SMTP	passed?

© SANS Institute 2000 - 2005 Author retains full rights.

The policy specifies who is responsible of the firewall and provides the responsible individual with adequate control to carry out the policy.	objective subjective
Check the policy document. Ask the responsible if he/she is the only person who can change something to the firewall.	
The policy does not defines clearly who is responsible. The administrator is implicitly the only person allowed to make changes to the firewall or the network.	passed?

2.1.3 Documentation and change control

Firewall configuration change control process exists.	objective subjective
The document exist	
Such a document does not exist. The process is implicitly known by the administrator and the members of the SOHO.	passed?

The actual configuration of the firewall is documented, including traffic flows and network architecture.	objective subjective
The document exist and is up-to-date.	
The administrator assures us that the firewall is configured correspondingly to the policy. (no specific document)	passed?

Changes to the firewall configuration are done by the responsible only.	objective subjective
Only the responsible knows the management password.	
Indeed, by interviewing the other members of the SOHO, it seems that only the administrator knows the admin password. This may be bad, as this person could be fired or (hopefully not) have a car accident, leading to an unmanageable firewall. On the other hand, the Watchguard box includes a reset procedure (consisting of connecting the two interfaces together and applying power). This will delete any configured rules, but as we have seen, they are not that complicated, and the successor of the administrator will be able to use the firewall again.	passed?

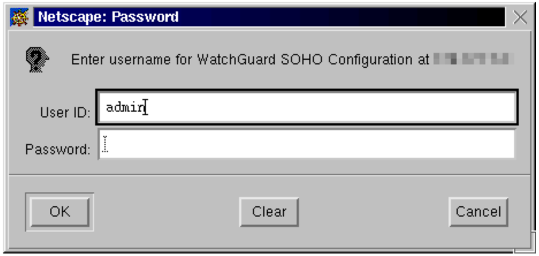
Changes to the firewall configuration are documented.	objective subjective
Change control is implemented as paper or electronic documents.	
The document does not exist. Only some configuration elements are written in a document.	passed?

© SANS Institute 2000 - 2005 Author retains full rights.

A minimum of information must be documented with each change.	objective subjective
Each change control document includes the name of the individual who added/modified a configuration, the date and the reason for the configuration. This is confirmed by looking at the actual documents.	
This information is not present.	passed?

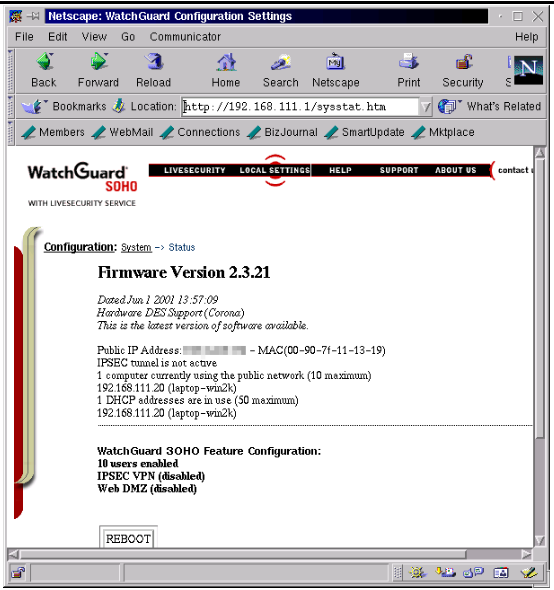
A configuration/rule backup strategy is documented and implemented.	objective subjective
The strategy is implemented and works (has been tested)	
The firewall does not provide a simple interface for exporting the rule configuration. The rules have been once “copy/pasted” in a document, which is susceptible to be used to re-implement the rules.	passed?

2.1.4 System Administration

The administration of the firewall is protected by a password.		objective subjective
Connect to the firewall (remote admin) or access the console (local admin) and verify the access control mechanism.		
The access to the administration functions (through a web browser) is protected by a userid and password, both defined by the user.	 Netscape: Password Enter username for WatchGuard SOHO Configuration at [redacted] User ID: admin Password: 	passed?

A password policy exists and is followed.	objective subjective
Verify that the admin password complies with the policy. (It will have to be changed at the end of the audit!)	
The policy is implicit, and the administrator uses a password of 8 characters including numbers and special characters.	passed?

© SANS Institute 2000 - 2005 Author retains full rights.

The OS or Firmware of the Firewall has the latest stable patches.	objective subjective
Find the actual patch level of the device and compare it with supplier's information.	
 Netscape: WatchGuard Configuration Settings Location: http://192.168.111.1/sysstat.htm Configuration: System -> Status **Firmware Version 2.3.21** *Dated Jun 1 2001 13:57:09* *Hardware DES Support (Corona)* *This is the latest version of software available.* Public IP Address: [redacted] - MAC(00-90-7f-11-13-19) IPSEC tunnel is not active 1 computer currently using the public network (10 maximum) 192.168.111.20 (laptop-win2k) 1 DHCP addresses are in use (50 maximum) 192.168.111.20 (laptop-win2k) **WatchGuard SOHO Feature Configuration:** **10 users enabled** **IPSEC VPN (disabled)** **Web DMZ (disabled)** REBOOT File Edit View Go Communicator Help Back Forward Reload Home Search Netscape Print Security Bookmarks What's Related Members WebMail Connections BizJournal SmartUpdate Mktplace WatchGuard SOHO WITH LIVESECURITY SERVICE LIVESECURITY LOCAL SETTINGS HELP SUPPORT ABOUT US contact The firmware version is 2.3.21, but the Watchguard web site (https://www.watchguard.com/support/sohoresources.asp) indicates version 2.4.16 as the latest one.	passed?

Modification of configuration or rules comply with the security policy and documentation.	objective subjective
The administrator confirms to follow the security policy when changing a rule or configuration.	
Interviewing the administrator indicates that he tries to follow the policy when changing rules. For example, he opened lately (outgoing) an additional port (8888) in order to access an external web-proxy, but refused to open the firewall for Peer to Peer communicating software.	passed?

2.1.5 Actual configuration

In this section, we will determine objectively the configuration of the firewall, and check its compliance with the policy and documentation.

There must be no open ports visible from the outside on the firewall itself.	objective subjective
A tcp syn scan with nmap must show no open ports. command: `nmap -sS -P0 -O -p 1-65535 -r -T Aggressive xx.xx.xx.xx` (Syn half-open scan, no ping, OS fingerprinting, all ports, not random order, Aggressive scan speed, xx.xx.xx.xx is the IP address of the Firewall itself on the public side.)	

© SANS Institute 2000 - 2005 Author retains full rights.

```
# Nmap (V. nmap) scan initiated 2.53 as: nmap -sS -P0 -O -p 1-65535 -n -r -
T Insane -oN external_nmap.txt --host_timeout 9000000 10.1.225.174
Warning:  No TCP ports found open on this machine, OS detection will be
MUCH less reliable
All 65535 scanned ports on  (10.1.225.174) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
# Nmap run completed at Thu Sep 13 20:46:01 2001 -- 1 IP address (1 host
up) scanned in 4024 seconds
```

passed?

There must be no open ports visible from the inside on the firewall itself (except the management port).

objective
subjective

A tcp syn scan with nmap must show no open ports (except the management port).

command: `nmap -sS -P0 -p 1-65535 -r -T Aggressive xx.xx.xx.xx`

(Syn half-open scan, no ping, all ports, not random order, Aggressive scan speed, xx.xx.xx.xx is the IP address of the Firewall itself on the private side.)

```
# Nmap (V. nmap) scan initiated 2.53 as: nmap -sS -P0 -O -p 1-65535 -n -r -
T Insane -oN internal_nmap.txt --host_timeout 9000000 192.168.111.1
Interesting ports on  (192.168.111.1):
(The 65531 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
53/tcp     filtered    domain
80/tcp     open        http
1080/tcp   open        socks

TCP Sequence Prediction: Class=truly random
                         Difficulty=9999999 (Good luck!)
No 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:
TSeq(Class=TR)
T1(Resp=Y%DF=N%W=C00%ACK=S++%Flags=AR%Ops=)
T2(Resp=Y%DF=N%W=C00%ACK=S%Flags=AR%Ops=)
T3(Resp=Y%DF=N%W=C00%ACK=S++%Flags=AR%Ops=)
T4(Resp=Y%DF=N%W=C00%ACK=S%Flags=AR%Ops=)
T5(Resp=Y%DF=N%W=C00%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=C00%ACK=S%Flags=AR%Ops=)
T7(Resp=Y%DF=N%W=C00%ACK=S++%Flags=AR%Ops=)
PU(Resp=N)


# Nmap run completed at Sun Sep  9 20:04:05 2001 -- 1 IP address (1 host
up) scanned in 1058 seconds
```

This scan shows port 80 and 21 open. Although the HTTP port (80) is known to be the management port, Watchguard's documentation does not mention the FTP port (21). We suspect it is used for firmware update, or other administration purposes.

Port 1080 (socks) is on the other hand not expected. This is indeed an internal SOCKS Proxy, which is enabled by default. As it is not in the policy, this criteria is not passed.

passed?

© SANS Institute 2000 - 2005 Author retains full rights.

Manual review of the rule base. It must comply to the policy and the traffic flow / architecture diagram.

objective
subjective

Use administration commands to get a dump of the rule base. Check if it complies with the authorised traffic (as described in section 1.4.1 for example).

```
Allowed Incoming Services
No services installed

Blocked Outgoing Services
Block TCP port range from port 8889 to port 65535
Block TCP port range from port 26 to port 79
Block TCP port range from port 1 to port 19
Block TCP port range from port 23 to port 24
Block TCP port range from port 120 to port 442
Block TCP port range from port 81 to port 108
Block TCP port range from port 111 to port 118
Block TCP port range from port 444 to port 8079
Block TCP port range from port 8081 to port 8887
Block UDP port range from port 54 to port 65535
Block UDP port range from port 1 to port 52
```

The Watchguard rules configuration is an “allow by default” for outgoing connections. The administrator blocked everything except ports:

TCP: 20 (ftp data), 21 (ftp), 22 (ssh), 25 (smtp), 80 (http), 109 (pop-2) , 110 (pop-3), 119 (nntp), 443 (https), 8080 (http), 8888 (http)

UDP: 53 (DNS)

Except port 22 and 109, everything complies with the policy. Nonetheless, because of these two open ports, the criteria is not passed.

passed?

Check the correct implementation of the rule base **Outside -> Inside**

objective
subjective

Use a tool to generate packets (TCP, UDP, ICMP) from one side of the firewall and tcpdump or another tool to listen for packets on the other side. Anything that goes through must be allowed by the rules and comply with the policy.

We used ftester [6].

ftest.conf:

```
10.1.227.94:1025:10.1.225.174:80::ICMP:3:5
10.1.227.94-94:53-53:10.1.225.174:1-65535:A:TCP
10.1.227.94-94:53-53:10.1.225.174:1-65535:U:UDP
```

Result: No packet has been forwarded on the private network.

Note: 10.1.225.174 is the external address of the firewall. We cannot use an internal addresses, as the Watchguard box is doing Network Address Translation (NAT). On the other hand, an “incoming” rule would forward ports on a specific internal address.

10.1.227.94 is the address of an external host we are using for the tests.

passed?

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Check the correct implementation of the rule base **Inside -> Outside**	objective subjective
Use a tool to generate packets (TCP, UDP, ICMP) from one side of the firewall and tcpdump or another tool (ftester [6] for example) to listen for packets on the other side. Anything that goes through must be allowed by the rules and comply with the policy.	
We used ftester [6].	passed?

ftest.conf:

```
192.168.111.20:1025:10.1.227.94:80::ICMP:3:5
192.168.111.20-20:53-53:10.1.227.94:1-65535:A:TCP
192.168.111.20-20:53-53:10.1.227.94:1-65535:U:UDP
stop_signal=192.168.111.20:666:10.1.227.94:22:S:TCP
```

Result:

```
# Ftestd started on Fri Sep 7 13:58:51 CEST 2001
10.1.225.174 > 10.1.227.94 ICMP 3 5
10.1.225.174:29050 > 10.1.227.94:20 A TCP
10.1.225.174:29050 > 10.1.227.94:21 A TCP
10.1.225.174:29050 > 10.1.227.94:22 A TCP
10.1.225.174:29050 > 10.1.227.94:25 A TCP
10.1.225.174:29050 > 10.1.227.94:80 A TCP
10.1.225.174:29050 > 10.1.227.94:109 A TCP
10.1.225.174:29050 > 10.1.227.94:110 A TCP
10.1.225.174:29050 > 10.1.227.94:119 A TCP
10.1.225.174:29050 > 10.1.227.94:443 A TCP
10.1.225.174:29051 > 10.1.227.94:8080 A TCP
10.1.225.174:29051 > 10.1.227.94:8888 A TCP
10.1.225.174:29052 > 10.1.227.94:53 UDP
(10.1.225.174:29053 > 10.1.227.94:22 S TCP) -> stop signal
# Ftestd finished on Fri Sep 7 14:21:11 CEST 2001
```

This test confirms the manual analysis of the rule set. Except port 22 and 109, the other ports are allowed by the policy.

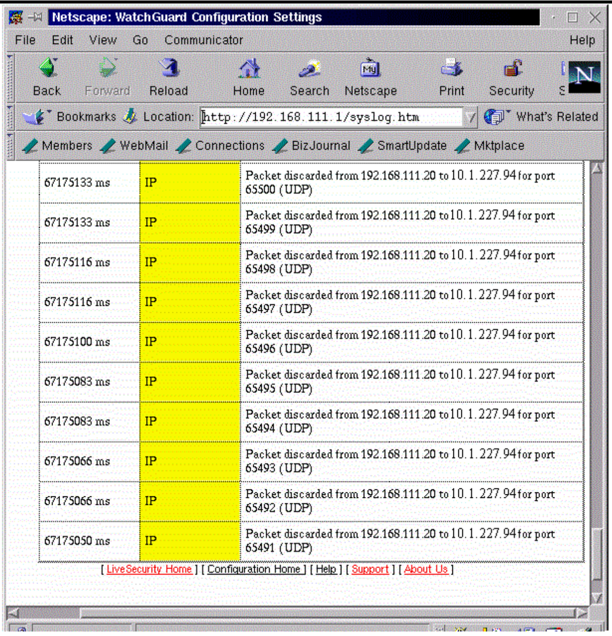
One interesting aspect is the fact that the packets where generated with an Ack only (no previous Syn): this lead to the conclusion that the firewall is **not** a stateful firewall (to the contrary of the description on Watchguard’s web site), i.e. it doesn’t look for a normal three-way handshake. In the same way, ftp data connections (port 20) are apparently allowed without a corresponding ftp command connection (port 21).

ICMP messages are also allowed, but it is not specified (as allowed or blocked) in the policy. This is clearly a deficiency of the policy.

Note: 10.1.227.94 is the address of an external host we are using for our tests. 10.1.225.174 is the external address of the firewall (the firewall is doing NAT).

© SANS Institute 2000 - 2005 Author retains full rights.

2.1.6 Logging, Detection and Reaction

<table>
<tr><td colspan="2">Verify the logs of the firewall and their effectiveness.</td><td>objective
subjective</td></tr>
<tr><td colspan="3">Get a dump of the firewall log, and verify that the previous scans where correctly recorded. It should also include management activities (bad authentication for example).</td></tr>
<tr><td>
Netscape: WatchGuard Configuration Settings
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security
Bookmarks Location: http://192.168.111.1/syslog.htm What's Related
Members WebMail Connections BizJournal SmartUpdate Mktplace
<table>
<tr><td>67175133 ms</td><td>IP</td><td>Packet discarded from 192.168.111.20 to 10.1.227.94 for port 65500 (UDP)</td></tr>
<tr><td>67175133 ms</td><td>IP</td><td>Packet discarded from 192.168.111.20 to 10.1.227.94 for port 65499 (UDP)</td></tr>
<tr><td>67175116 ms</td><td>IP</td><td>Packet discarded from 192.168.111.20 to 10.1.227.94 for port 65498 (UDP)</td></tr>
<tr><td>67175116 ms</td><td>IP</td><td>Packet discarded from 192.168.111.20 to 10.1.227.94 for port 65497 (UDP)</td></tr>
<tr><td>67175100 ms</td><td>IP</td><td>Packet discarded from 192.168.111.20 to 10.1.227.94 for port 65496 (UDP)</td></tr>
<tr><td>67175083 ms</td><td>IP</td><td>Packet discarded from 192.168.111.20 to 10.1.227.94 for port 65495 (UDP)</td></tr>
<tr><td>67175083 ms</td><td>IP</td><td>Packet discarded from 192.168.111.20 to 10.1.227.94 for port 65494 (UDP)</td></tr>
<tr><td>67175066 ms</td><td>IP</td><td>Packet discarded from 192.168.111.20 to 10.1.227.94 for port 65493 (UDP)</td></tr>
<tr><td>67175066 ms</td><td>IP</td><td>Packet discarded from 192.168.111.20 to 10.1.227.94 for port 65492 (UDP)</td></tr>
<tr><td>67175050 ms</td><td>IP</td><td>Packet discarded from 192.168.111.20 to 10.1.227.94 for port 65491 (UDP)</td></tr>
</table>
[LiveSecurity Home] [Configuration Home] [Help] [Support] [About Us]</td><td>We can see on the log output messages about discarded packets.
Unfortunately, only the latest 100 events are recorded. Moreover, some time dependant functions of the firewall generate additional events. After one or two hours, all suspicious events are "pushed" out of the log file.</td><td>passed?</td></tr>
</table>

A log analysis and reaction process exist and is "alive".	objective subjective
Check the existence of a process to analyse the log. The person responsible must have enough knowledge to recognise unusual situations, and has a reaction plan ready.	
Due to the limited functionality of the log system on the Watchguard firewall, the administrator is using the log only for debugging purposes. A reaction plan is not defined.	passed?

© SANS Institute 2000 - 2005

Author retains full rights.

2.2 Evaluation of the audit checklist

Based on the practical experience of section 2.1, we can now evaluate this new audit checklist and methodology. More specifically, we will first review the areas:

- with good coverage
- overlooked
- which cannot be covered

Finally, we will try to summarise how effective this checklist is in auditing a SOHO Firewall.

2.2.1 Areas with good coverage

The management aspects related to the utilisation of a Firewall as a mean of protection seems to be correctly addressed by this audit. This is especially true for a small SOHO environment, where the network architecture and management issues are much simplified. On the other hand, proper documentation should not be left as a "nice to have" item… This is reflected in this audit checklist, where we can see a couple of questions oriented at discovering the understanding level of the managers and administrators about the technology and it's correct use. Additionally, proper documentation is controlled with questions about policy and change control.

From the practical trial of this audit checklist, we can see that these questions are pertinent (some are correctly answered in this specific example, others are clearly showing weaknesses in the processes), without being overwhelming.

The rule auditing part contains the basic steps of comparison between the "should be"-state and the "is"-state. We consider it enough for this environment, although some exotic aspects could be better analysed (see also next section).

2.2.2 Areas overlooked

The main overlooked area is the auditing of applications and application level filtering.

Indeed, we could design a suite of tests in order to check the resilience of the management interface. In this particular case, it was a web application. We could have tested the internal web server for possible Denial of Service attacks, weaknesses in the authentication mechanisms, parameters manipulations in the web forms, etc… In the same way, the internal FTP server could present vulnerabilities. These vulnerabilities may lead to an access on the operating system. (This threat is mitigated by the fact that the firmware is running on an unusual CPU with an unknown Operating System, making the design of buffer overflow especially difficult).

Other proxy applications (like the socks proxy) should be the subject of testing. Unfortunately, this may render the checklist much more complex and difficult to design (which goes against our design goal for this checklist), as every product will have different proxy functionality. The resulting checklist will cover only with difficulties major options of such SOHO firewalls. It would be better to include pointers to additional checklists (for application auditing), and request the auditor to

© SANS Institute 2000 - 2005 Author retains full rights.

check the applications appropriate to his/her actual system.

Application level filtering is not checked. For example, we could design a test where we try to establish an FTP-data connection without the prior FTP-command connection (and commands). Or we could try to establish HTTP connections, without proper HTTP semantic. As we have seen in this practical example, the Watchguard device does not do such application level checks (we where able to extract this information from the "rules scan", without designing specific test for this feature). If a device would claim such high-level filtering, we should have tests to proof such claims. On the other hand, these devices, because of their customer target, are designed to be cheap: high-level filtering requires much more CPU, Memory and development. It is therefore less likely to find high-level filtering in these devices, lessening the impact of the lack of specific tests in this audit.

Finally, we could have more detailed filter rules audit checks. In the actual checklist, we just ask to create packets from one side of the firewall, and look if they get on the other side. We could be more specific, and try more packet's configuration: some trying to follow normal three-way handshake (ACK following a SYN), some other more exotic packets (SYN-FIN in one, fragmented packets, various ICMP ones). In our case (Watchguard), as the device is stateless (an ACK goes through even if no previous SYN has been seen), this makes less sense. But other devices may present more complex behaviour, and it should be addressed.

2.2.3 Areas which cannot be covered

Many of these devices are "embedded" devices [7]. They have usually a proprietary operating system, running on less known CPUs. They do not provide access to the operating system (no shell prompt), and are designed to fulfil only their firewall task.

It is therefore not possible to evaluate the configuration of the operating system, and we have to rely on the vendor's diligence to provide patches when vulnerabilities are discovered. On the other hand, as these devices are designed from the ground up as firewall appliance, we can expect them to be well designed. We can also expect no unneeded services running as a side effect of running on low resources (CPU, Memory).

In the same way, we cannot audit the hardware itself: crash recovery, hardware weaknesses (encryption keys available to a hardware analyser), etc.

2.3 Directions for future work

As we have seen throughout Section 2, our actual checklist, although not perfect, constitutes a nice background to build better versions. One aspect to keep in mind is the design goal of this checklist: keep it simple. If we want this checklist to be used by administrators of SOHO networks, which are probably not security professionals, it has to be simple enough and at the same time covers essential aspects of the operations of a firewall.

Still, we can think about the following improvements:

2.3.1 Better guidelines in auditing the filtering rule

We could improve the actual checklist by detailing a procedure to correctly check

© SANS Institute 2000 - 2005 Author retains full rights.

the filtering rules. This would include the recommendation of one or two specific tools, along with typical configurations probing exhaustively the filtering rules.

2.3.2 Exotic packet penetration tests

We could add some tests with exotic packets (fragmented, etc…) in order to test the quality of the filtering (especially if it is stateful).

2.3.3 Application tests

We should include some basic tests for a set of typical applications that may be found on such devices. The management application is to be considered (web server, ftp server, …). The main difficulty will be to determine the relevant applications, without making the checklist too complex.

2.3.4 Additional architectures

The considered architecture is very simple. Although this architecture is probably the most common one in a SOHO environment, it is possible that more complex architectures are implemented (providing an FTP or HTTP server to the Internet). The consequences on the checklist must be evaluated, and appropriately addressed.

2.3.5 Computer assisted audit

One solution to avoid the complexity of the checklist for the end-user, is to design a small tool to assist the auditor. The tool would ask the auditor specific questions about the architecture, require some tests to be performed, and appropriately “switches” sections of the checklist “on”. For example, a section testing a web management interface would be seen by the end-user only if he previously indicated that such an interface exists.

The evaluation of the results of the audit would be facilitated, and the possibility to record baseline configuration is one of the many additional features allowed by the use of such a tool.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

3 References

[1] WatchGuard, “WatchGuard Technologies Product Line”, 2001. URL: http://www.watchguard.com/products/soho_features.asp (13 Aug. 2001)

[2] Northcutt, Stephen. Track 7 – Auditing Information Systems, Volume 7.3 Auditing Routers and Firewall. SANS Institute, 2001

[3] Spitzner, Lance. “Auditing your Firewall Setup”, 12 December 2000. URL: http://www.enteract.com/~lspitz/audit.html (13 Aug. 2001)

[4] Management Analytics. “Management Analytics Firewall Checklist”, 1995. URL: http://www.all.net/books/audit/Firewall/manal/index.html (13 Aug. 2001)

[5] Zone Labs, “ZoneAlarm”, 2001. URL: http://www.zonelabs.com/products/index.html (13 Aug. 2001)

[6] Barisani, Andrea. “Ftester-0.1.tar.gz”,Firewall Tester, v.0.1, 2001. URL:

http://sole.infis.univ.trieste.it/~lcars/ftester (13 Aug. 2001)[4]

[7] “Embedded Systems Programming”, URL: http://www.embedded.com (13 Aug 2001)

© SANS Institute 2000 - 2005, Author retains full rights.

[4] In the mean time, Andrea took some of my improvements for version 0.2

© SANS Institute 2000 - 2005 Author retains full rights.