Interested in learning more about network auditing?

SANS Institute

Security Consensus Operational Readiness Evaluation

This checklist is from the SCORE Checklist Project. Reposting is not permited without express, written permission.

Firewall Checklist

Copyright SANS Institute
Author Retains Full Rights

Firewall Checklist

Prepared by: Krishni Naidu

References:

Top Ten Blocking Recommendations Using Cisco ACL's Securing the Perimeter with Cisco IOS 12 Routers, Scott Winters, August 2000
GIAC Firewall Practical: Implementation of Firewall Filters, Rick Thompson, August 2000
Application Layer Firewalls vs Network Layer Firewalls: Which is the better choice, Keith D. Maxon, August 2000
Top Ten Blocking Recommendations using Ipchains, Paul Tiedemann, August 2000
What is Egress filtering and how can I implement it? Egress Filtering v0.2, Chris Brenton, February 2000
IP Fragmentation attacks on Checkpoint firewalls, James Farrell, April 2001
A comparison of packet filtering vs application level firewall technology, Ernest Romanofski, March 2001
Designing a DMZ, Scott Young, March 2001
The new firewall design question, Jamie R. Blerke, March 2001
Securing your network perimeter by filtering inbound traffic on ACK and Reset bits on Nortel Routers, Oleg Krillov, February 2001
Linux comes of age with stateful firewalling, Greg Hill, February 2001
The desktop modem threat, Joe Livingston, July 2000
DNS Security, Jeff Holland, July 2000
The packet filter: A basic network security tool, Dan Strom, September 2000
Perimeter filtering in a University setting, Elizabeth Mackenzie, September 2000
Protecting your corporate laptops from Hackers, while they are on the road, Darrell Keller, May 2001
Protecting yourself with Norton personal firewall, Mark Greco, May 2001
The Distributed firewall, Daniel Wan, May 2001
A brief taxonomy of firewalls – great walls of fire, Gary Smith, May 2001
Check point firewall-1's stateful inspection, Michael J. Nikitas, April 2001
Stealth firewalls, Brandon Gilespie, April 2001
Firewall network appliance, Craig Simmons, October 2000

Introduction

This checklist should be used to audit a firewall. This checklist does not provide vendor specific security considerations but rather attempts to provide a generic listing of security considerations to be used when auditing a firewall.

Only technical aspects of security are addressed in this checklist. Manual elements like physical protection for the firewall server is not considered.

Prior to using this checklist the following elements should be considered:

- Operating system: This checklist only defines the security items relating the firewall software and not to any security elements of the operating system.
- Port restrictions: A listing of ports to be restricted are highlighted in this checklist. However, prior to recommending that the ports be restricted, the auditor should ensure that the service associated with that port is not used by the business e.g. remote access via telnet. Where such situations exist this checklist attempts to provide alternate security options if the service is needed e.g. use SSH instead of Telnet.
- Modems within the internal network: Modems within the internal network are the biggest threat to subvert a firewall and thus the auditor should ensure that there

are no modems within the internal network. It is senseless performing an audit on the firewall when an even bigger threat exists via the modem. The auditor should perform war dialling to identify any modems within the internal network with tools like phonesweeper.

- Application level firewalls: The inherent nature of application level firewalls require that the operating system be as secure as possible due to the close binding of these two components. Thus, the auditor should ensure that the security on the operating system is secure before evaluating the security offered by the application level firewall.
- Defence in depth: It must be recognised that the firewall implementation is a not an end to itself to provide security. Thus, it is vital that the auditor evaluate the security of the other components like IDS, operating systems, web applications, IIS/Apache, routers and databases. Some organisations have opted for firewall network appliances, which are firewalls loaded onto operating systems which have their security already preconfigured. In such instances, the auditor need only review the security of the firewall configuration instead of the operating system as well.
- Rulesets: This checklist provides a listing of best practice rulesets to be applied. However, the organisational requirements may not need all of the rulesets. For e.g. where an organisation has a need to allow access via the internet to critical servers, the rulesets wound not include a deny rule to that internal IP address for the critical server. Instead it may provide for allow access to HTTP 80 to the critical IP and deny all other traffic to the critical IP. It must be noted that some elements of the recommended rulesets have to be applied irrespective of business requirements e.g. blocking private addresses (RFC1918), illegal addresses, standard unroutables, reserved addresses, etc.
- Laptop users: Most organisations use mobile laptops for telecommuting and on the road sales, etc. This provides a further vulnerability even if the organisation operates a VPN. The hacker could easily gain access to the laptop when it is connected to the internet and download tools to the laptop that can become a problem when the laptop is again connected to the corporate network. In a VPN situation, the hacker with access to the remote station once the tunnel is connected, can access the corporate network. In such a circumstance, it is important for the auditor to determine if laptop usage occurs and to evaluate whether personal firewalls are installed on these laptops prior to usage. This checklist provides a generic set of considerations for personal firewalls, but it does not provide any product specific security recommendations.

Checklist

No.	Security Elements
1.	Review the rulesets to ensure that they follow the order as follows: • anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside) • User permit rules (e.g. allow HTTP to public webserver) • Management permit rules (e.g. SNMP traps to network management server) • Noise drops (e.g. discard OSPF and HSRP chatter) • Deny and Alert (alert systems administrator about traffic that is suspicious) • Deny and log (log remaining traffic for analysis) Firewalls operate on a first match basis, thus the above structure is important to ensure that suspicious traffic is kept out instead of inadvertently allowing them in by not following the proper order.

2.	Application based firewall Ensure that the administrators monitor any attempts to violate the security policy using the audit logs generated by the application level firewall. Alternatively some application level firewalls provide the functionality to log to intrusion detection systems. In such a circumstance ensure that the correct host, which is hosting the IDS, is defined in the application level firewall. Ensure that there is a process to update the application level firewall's vulnerabilities checked to the most current vulnerabilities. Ensure that there is a process to update the software with the latest attack signatures. In the event of the signatures being downloaded from the vendors' site, ensure that it is a trusted site. In the event of the signature being e-mailed to the systems administrator, ensure that digital signatures are used to verify the vendor and that the information transmitted has not been modified en-route. The following commands should be blocked for SMTP at the application level firewall: • EXPN (expand) • VRFY (verify) • DEBUG • WIZARD The following command should be blocked for FTP: • PUT Review the denied URL's and ensure that they are appropriate for e.g. any URL's to hacker sites should be blocked. In some instances organisations may want to block access to x-rated sites or other harmful sites. As such they would subscribe to sites, which maintain listings of such harmful sites. Ensure that the URL's to deny are updated as released by the sites that warn of harmful sites. Ensure that only authorised users are authenticated by the application level firewall.
3.	Stateful inspection Review the state tables to ensure that appropriate rules are set up in terms of source and destination IP's, source and destination ports and timeouts. Ensure that the timeouts are appropriate so as not to give the hacker too much time to launch a successful attack. For URL's • If a URL filtering server is used, ensure that it is appropriately defined in the firewall software. If the filtering server is external to the organisation ensure that it is a trusted source. • If the URL is from a file, ensure that there is adequate protection for this file to ensure no unauthorised modifications. Ensure that specific traffic containing scripts; ActiveX and java are striped prior to being allowed into the internal network. If filtering on MAC addresses is allowed, review the filters to ensure that it is restricted to the appropriate MAC's as defined in the security policy.
4.	Logging Ensure that logging is enabled and that the logs are reviewed to identify any potential patterns that could indicate an attack.
5.	Patches and updates Ensure that the latest patches and updates relating to your firewall product is tested and installed. If patches and updates are automatically downloaded from the vendors' websites, ensure that the update is received from a trusted site.

	In the event that patches and updates are e-mailed to the systems administrator ensure that digital signatures are used to verify the vendor and ensure that the information has not been modified en-route.
6.	Location – DMZ Ensure that there are two firewalls – one to connect the web server to the internet and the other to connect the web server to the internal network. In the event of two firewalls ensure that it is of different types and that dual NIC's are used. This would increase security since a hacker would need to have knowledge of the strengths, weaknesses and bugs of both firewalls. The rulesets for both firewalls would vary based on their location e.g. between web server and the internet and between web server and the internal network.
7.	Vulnerability assessments/ Testing Ascertain if there is a procedure to test for open ports using nmap and whether unnecessary ports are closed. Ensure that there is a procedure to test the rulesets when established or changed so as not to create a denial of service on the organisation or allow any weaknesses to continue undetected.
8.	Compliance with security policy Ensure that the ruleset complies with the organisation security policy.
9.	Ensure that the following spoofed, private (RFC 1918) and illegal addresses are blocked: Standard unroutables • 255.255.255.255 • 127.0.0.0 Private (RFC 1918) addresses • 10.0.0.0 – 10.255.255.255 • 172.16.0.0 – 172.31.255.255 • 192.168.0.0 - 192.168.255.255 Reserved addresses • 240.0.0.0 Illegal addresses • 0.0.0.0 UDP echo ICMP broadcast (RFC 2644) Ensure that traffic from the above addresses is not transmitted by the interface.
10.	Ensure that loose source routing and strict source routing (lsrsr & ssrr) are blocked and logged by the firewall.
11.	Port restrictions The following ports should blocked:

Service	Port Type	Port Number
DNS Zone Transfers	TCP	53
TFTP Daemon	UDP	69
Link	TCP	87
SUN RPC	TCP & UDP	111
BSD UNIX	TCP	512 – 514
LPD	TCP	515
UUCPD	TCP	540
Open Windows	TCP & UDP	2000
NFS	TCP & UDP	2049
X Windows	TCP & UDP	6000 – 6255
Small services	TCP & UDP	20 and below

	Small services	TCP & UDP	20 and below
	FTP	TCP	21
	SSH	TCP	22
	Telnet	TCP	23
	SMTP (except external mail relays)	TCP	25
	NTP	TCP & UDP	37
	Finger	TCP	79
	HTTP (except to external web servers)	TCP	80
	POP	TCP	109 &110
	NNTP	TCP	119
	NTP	TCP	123
	NetBIOS in Windows NT	TCP &UDP	135
	NetBIOS in Windows NT	UDP	137 & 138
	NetBIOS	TCP	139
	IMAP	TCP	143
	SNMP	TCP	161 &162
	SNMP	UDP	161 &162
	BGP	TCP	179
	LDAP	TCP &UDP	389
	SSL (except to external web servers)	TCP	443
	NetBIOS in Win2k	TCP &UDP	445
	Syslog	UDP	514
	SOCKS	TCP	1080
	Cisco AUX port	TCP	2001
	Cisco AUX port (stream)	TCP	4001
	Lockd (Linux DoS Vulnerability)	TCP &UDP	4045
	Cisco AUX port (binary)	TCP	6001
	Common high order HTTP ports	TCP	8000, 8080, 8888
12.	Remote access If remote access is to be used, ensure that the SSH protocol (port 22) is used instead of Telnet.		
13.	File Transfers If FTP is a requirement, ensure that the server, which supports FTP, is placed in a different subnet than the internal protected network.		
14.	Mail Traffic Ascertain which protocol is used for mail and ensure that there is a rule to block incoming mail traffic except to internal mail.		
15.	ICMP (ICMP 8, 11, 3) Ensure that there is a rule blocking ICMP echo requests and replies. Ensure that there is a rule blocking outgoing time exceeded and unreachable messages.		
16.	IP Readdressing/IP Masquerading Ensure that the firewall rules have the readdressing option enabled such that internal IP addresses are not displayed to the external untrusted networks.		

17.	Zone Transfers If the firewall is stateful, ensure packet filtering for UDP/TCP 53. IP packets for UDP 53 from the Internet are limited to authorised replies from the internal network. If the packet were not replying to a request from the internal DNS server, the firewall would deny it. The firewall is also denying IP packets for TCP 53 on the internal DNS server, besides those from authorised external secondary DNS servers, to prevent unauthorised zone transfers.
18.	Egress Filtering Ensure that there is a rule specifying that only traffic originating from IP's within the internal network be allowed. Traffic with IP's other than from the Internal network are to be dropped. Ensure that any traffic originating from IP's other than from the internal network are logged.
19.	Critical servers Ensure that there is a deny rule for traffic destined to critical internal addresses from external sources. This rule is based on the organisational requirements, since some organisations may allow traffic via a web application to be routed via a DMZ.
20.	Personal firewalls Ensure that laptop users are given appropriate training regarding the threats, types of elements blocked by the firewall and guidelines for operation of the personal firewall. This element is essential, since often times personal firewalls rely on user prompt to respond to attacks e.g. whether to accept/deny a request from a specific address. Review the security settings of the personal firewall to ensure that it restricts access to specific ports, protects against known attacks, and that there is adequate logging and user alerts in the event of an intrusion. Ensure that there is a procedure to update the software for any new attacks that become known. Alternatively most tools provide the option of transferring automatic updates via the internet. In such instances ensure that updates are received from trusted sites.
21.	Distributed firewalls Ensure that the security policy is consistently distributed to all hosts especially when there are changes to the policy. Ensure that there are adequate controls to ensure the integrity of the policy during transfer, e.g. IPSec to encrypt the policy when in transfer. Ensure that there are adequate controls to authenticate the appropriate host. Again IPSec can be used for authentication with cryptographic certificates.
22.	Stealth Firewalls Ensure that default users and passwords are reset. Ensure that the firewall is appropriately configured to know which hosts are on which interface. Review the firewall access control lists to ensure that the appropriate traffic is routed to the appropriate segments. A stealth firewall does not have a presence on the network it is protecting and it makes it more difficult for the hacker to determine which firewall product is being used and their versions and to ascertain the topology of the network.
23.	Ensure that ACK bit monitoring is established to ensure that a remote system cannot initiate a TCP connection, but can only respond to packets sent to it.
24.	Continued availability of Firewalls Ensure that there is a hot standby for the primary firewall.

Last Updated: April 26th, 2024

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Autumn Australia 2024	Sydney, NSW, AU	May 06, 2024 - May 11, 2024	Live Event
SANS Rome May 2024	Rome, IT	May 06, 2024 - May 11, 2024	Live Event
SANS Security West 2024	San Diego, CAUS	May 09, 2024 - May 14, 2024	Live Event
SANS Dubai May 2024	Dubai, AE	May 11, 2024 - May 16, 2024	Live Event
SANS ICS Europe 2024 Munich	Munich, DE	May 12, 2024 - May 18, 2024	Live Event
SANS Cloud Singapore 2024	Singapore, SG	May 13, 2024 - May 24, 2024	Live Event
SANS Doha May 2024	Doha, QA	May 18, 2024 - May 23, 2024	Live Event
SANS Leadership & Cloud Security - Crystal City 2024	Arlington, VAUS	May 20, 2024 - May 24, 2024	Live Event
SANS Amsterdam May 2024	Amsterdam, NL	May 20, 2024 - Jun 01, 2024	Live Event
SANS SEC530 Canberra 2024	Canberra, ACT, AU	May 27, 2024 - Jun 01, 2024	Live Event
SANS Cyber Defence Thailand 2024	Bangkok, TH	May 27, 2024 - Jun 01, 2024	Live Event
SANS Philippines SEC504 2024	Manila, PH	May 27, 2024 - Jun 01, 2024	Live Event
SANS Summer Dunes 2024	Riyadh, SA	Jun 01, 2024 - Jun 06, 2024	Live Event
SANS Muscat June 2024	Muscat, OM	Jun 01, 2024 - Jun 06, 2024	Live Event
SANS Munich June 2024	Munich, DE	Jun 03, 2024 - Jun 08, 2024	Live Event
SANS Miami 2024	Coral Gables, FLUS	Jun 03, 2024 - Jun 15, 2024	Live Event
SANS Madrid June 2024	Madrid, ES	Jun 10, 2024 - Jun 15, 2024	Live Event
SANS Paris June 2024	Paris, FR	Jun 10, 2024 - Jun 15, 2024	Live Event
SANS ICS Security Summit & Training 2024	Orlando, FLUS	Jun 16, 2024 - Jun 24, 2024	Live Event
SANS Tbilisi June 2024	Tbilisi, GE	Jun 17, 2024 - Jun 22, 2024	Live Event
SANS Rocky Mountain Summer 2024	Denver, COUS	Jun 17, 2024 - Jun 22, 2024	Live Event
SANS Warsaw June 2024	Warsaw, PL	Jun 17, 2024 - Jun 22, 2024	Live Event
SANS Cyber Defence Japan 2024	Tokyo, JP	Jun 17, 2024 - Jun 29, 2024	Live Event
SANS Zurich June 2024	Zurich, CH	Jun 24, 2024 - Jun 29, 2024	Live Event
SANS Cyber Defence Australia 2024	Canberra, ACT, AU	Jun 24, 2024 - Jul 06, 2024	Live Event
SANS San Antonio 2024	San Antonio, TXUS	Jun 24, 2024 - Jun 29, 2024	Live Event
SANS London July 2024	London, GB	Jul 01, 2024 - Jul 06, 2024	Live Event
SANSFIRE 2024	Washington, DCUS	Jul 15, 2024 - Jul 20, 2024	Live Event
SANS Amsterdam July 2024	Amsterdam, NL	Jul 15, 2024 - Jul 20, 2024	Live Event
SANS Pen Test Hackfest Europe Summit & Training - Amsterdam 2024	Amsterdam, NL	Jul 21, 2024 - Jul 27, 2024	Live Event
SANS Baltimore Spring 2024	OnlineMDUS	Apr 28, 2024 - May 03, 2024	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced