Global Information Assurance Certification Paper

Auditing the Netscreen-5 Firewall Used as a VPN Gateway

Dan Strom

SANS GCNA Assignment – v. 1.0

August 16, 2001

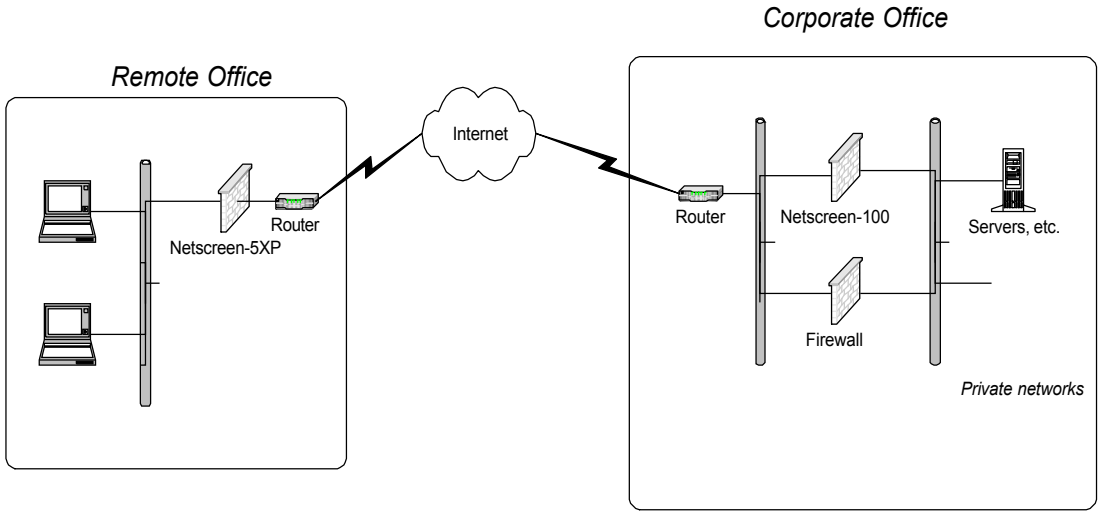
Introduction

Many solutions have been offered to the company having remote offices that need to connect to the corporate networks. In the past the solutions have ranged from asynchronous dial-up to public x.25 networks to frame-relay over the public switched telephone network. Each of these solutions is costly.

Many corporations are now looking to the public Internet as a means of reducing their fixed network cost for connecting their remote offices. Virtual private networks (VPNs) are becoming a standard means for transparently extending the work environment to the remote offices. The security goals for a VPN center around confidentiality of the data and the data transmission. Many corporations are realizing a significant cost savings through replacing their dedicated, private wide area networks with virtual private networks over the public Internet.

The objective of this paper is to present research and application in the audit of a VPN solution. The VPN implementation being audited is a hardware-based, gateway-to-gateway VPN.

Description of the system



The system that is the focus of the audit research and audit application is built upon the Netscreen firewall products. The remote office is configured with a broadband Internet connection. Typically, in a small office this would be DSL, cable, satellite, or wireless. The

Netscreen-5XP acts both as a firewall appliance and VPN gateway. The corporate office would have high-bandwidth Internet connectivity. The Netscreen-100 firewall is dedicated to acting only as a VPN gateway. General Internet connectivity for the corporate network is accomplished thru another firewall.

The scope of this project is limited to the Netscreen-5XP firewall, which also acts as a VPN gateway. The firewall used for general Internet connectivity and the Netscreen-100 are outside the scope of this project.

Certain assumptions will be in force for this project:

1. The ISP connection in the remote office is a cable-TV Internet connection.
2. The router at the remote office is configured and managed by the ISP.
3. The ISP connection at the corporate office has substantially more bandwidth than necessary for the VPN connection. The ISP is a tier-1 provider.
4. The Internet router at the corporate office is configured according to good practice with appropriate ingress and egress filtering.
5. The users in the remote office will have full Internet connectivity in addition to the VPN access to resources at the corporate office.
6. The VPN will be configured with an Autokey IKE tunnel using a preshared secret between the gateways. The tunnel will use ESP with 3DES encryption and SHA-1 authentication. The VPN gateways will be using NAT between the untrusted and trusted interfaces.

Research

Because the NetScreen performs both firewall and VPN functions, both of these functions must be included as a part of the research into the current state of audit practice.

Firewall Audit

A search for *firewall audit* on www.google.com returned about 52,000 hits. Most of these pages contain information that is not useful in this context. However, several pages did contain information relevant to the security audit of a firewall. None of these dealt specifically with auditing a Netscreen firewall. So, it is important that an audit process be constructed for the Netscreen firewall/VPN gateway.

In response to someone asking for an audit checklist for firewalls, Marcus Ranum is attributed with saying, “If you know what you’re doing when you audit a firewall, you don’t need a checklist. If you don’t know what you’re doing, you do – but then you shouldn’t be taking someone’s money to audit their firewall.”[1] Later in the message thread, Ranum concedes, “As someone reminded me in mail, a checklist is more useful for reminding you what to check, rather than instructing you as to its significance.”[2] Therein lies the true value of the audit checklist – it is a reminder.

Farmer and Venema Checklist

Any audit assumes that the initial configuration of the system is correct. Farmer and Venema in their paper entitled "Improving the Security of Your Site by Breaking Into it"[3] provide this list of 'general suggestions' for improving the security of a system.

- If you cannot turn off the finger service, consider installing a modified finger daemon. It is rarely necessary to reveal a user's home directory and the source of last login.
- Don't run NIS unless it's absolutely necessary. Use NFS as little as possible.
- Never export NFS filesystems unrestricted to the world. Try to export file systems read-only where possible.
- Fortify and protect servers (e.g. hosts that provide a service to other hosts -- NFS, NIS, DNS, whatever.) Only allow administrative accounts on these hosts.
- Examine carefully services offered by inetd and the portmapper. Eliminate any that aren't explicitly needed. Use Wietse Venema's inetd wrappers, if for no other reason than to log the sources of connections to your host. This adds immeasurably to the standard UNIX auditing features, especially with respect to network attacks. If possible, use the loghost mechanism of syslog to collect security-related information on a secure host.
- Eliminate trust unless there is an absolute need for it. Trust is your enemy.
- Use shadow passwords and a passwd command that disallows poor passwords. Disable or delete unused/dormant system or user accounts.
- Keep abreast of current literature (see our suggested reading list and bibliography at the end of this paper) and security tools; communicate to others about security problems and incidents. At minimum, subscribe to the CERT mailing list and phrack magazine (plus the firewalls mailing list, if your site is using or thinking about installing a firewall) and read the usenet security newsgroups to get the latest information on security problems. Ignorance is the deadliest security problem we are aware of.
- Install all vendor security patches as soon as possible, on all of your hosts. Examine security patch information for other vendors - many bugs (rdist, sendmail) are common to many UNIX variants.

Observations and Analysis on Farmer and Venema

- The points in the list that are technical in nature are Unix-centric.
- The security policy is assumed to be known. This is evident in the requirement to eliminate any services that are not explicitly needed. The underlying information security policy is subjective in nature and cannot be measured.
- The services specifically mentioned – finger, NIS, NFS, as well as their state – can be measured objectively through the use of *netstat* at a terminal, and a port scanner such as *nmap*.
- The use of non-administrative accounts on the firewall can be measured objectively.
- The whole issue of trust is subjective in nature. It can be difficult to determine

when there is an absolute need for trust.

- The use of shadow passwords and requirement for strength of passwords can be measured objectively. Shadow passwords can be turned off or on by the system administrator, and the strength of password can be tested with tool like crack.
- This list could be improved upon by suggesting that the firewall be probed and tested from another host using port scan or a vulnerability scanner.
- Although the most of the suggestions given by Farmer and Venema do not have direct corollaries on the Netscreen, the principles ought to be included in the Netscreen audit process.

Farrow Checklist

Rik Farrow, in an article in Network Magazine entitled "Firewall Configuration Done Right"[4] give this list of steps as a way to audit a firewall.

- Acquire a copy of your security policy.
- List permitted services.
- Check the configuration of the firewall to see if it complies with this list of services.
- Correct, if possible, the configuration of the firewall to comply with the policy.
- Check the configuration of the firewall host: Are all security patches installed and unnecessary services disabled?
- Scan your firewall to see what services appear.
- Probe for hosts that should be protected behind the firewall.
- Examine how firewall logs are maintained and see who checks daily reports.

Rik goes on to say that "if you do not have a written security policy, you have failed the audit."

Observations and Analysis on Farrow

- The required security policy will be different for each organization and is subjective in nature. The services required should be based on business need.
- Determining if the firewall configuration matches the security policy list is straightforward. Review the rulebase on the firewall and compare with the required services. This is an objective test. To make a more objective analysis of compliance with policy, the firewall should be port scanned by an external host to determine the services that are presented.
- The step of maintaining logs and reviewing reports can only be measured within the context of the implementation of the security policy. The organization ought to create control procedures so that this can be measured objectively.
- This list not only provides for items to check, but also has a process embedded. It should be very useful.

Spitzner Checklist

The white paper "Auditing Your Firewall Setup"[5] by Lance Spitzner gives two

fundamental parts to auditing the firewall setup.

- Audit the firewall
  - Physical security
  - Armor of the operating system
  - Port scan the firewall
- Audit the rulebase
  - Review the validity of rules
  - Test additional services such as virus scanning
- Review the logs
  - Were scans detected?

Observations and Analysis on Spitzner

- Physical security can be measured objectively. Do unauthorized personnel have physical access to the firewall server, the console, or remotely?
- It is interesting to note that Spitzner refers the reader to external sources for checklists to armor the operating system. By using these checklists, this becomes very measurable and objective.
- Scanning the firewall, both port scanning and vulnerability scanning, are objective in nature. Through scanning we get to see what is being offered to the world.
- Auditing of the rulebase and checking the validity of the rules is subjective in that it is dependant upon the subjective information security policy of the organization.
- Testing of the additional services such as virus scanning could become objective through the use of the _____ tool.

Lindstedt Checklist

Sandy Lindstedt presents a more general firewall audit process in her paper "Firewall Audit"[6].

- Logical Security
- System Event Monitoring
- Change Control
- Physical Security

Observations and Analysis on Lindstedt

- According to Lindstedt, this list is intentionally vague. Lindstedt is a consultant and expressed the concern that business secrets would be given away if detail was provided.
- Nonetheless, these general points ought to be addressed in the firewall audit. As presented, they are all subjective in nature.
- This list could be improved greatly with the addition of detail under each of the four audit areas.

Ray Checklist

However, the most detailed security audit checklist came from Dr. Loye L . Ray[7] at the University of Maryland University College. What makes his checklist unique is that it

addresses many of the non-technical aspects of an audit.

- **Before your start**
  - Get management buy-in
  - Perform risk analysis—Know thyself, know the business
    - What is acceptable? Set expectations and goals
  - Draft security policy—Now would be a good time to draft one
- **Preparation**
  - Determine: Type of audit—host, network, firewall
    - Security—heavy, normal, light
    - Perimeter vs internal
    - Scope/scale—Start small and leverage results for more security spending
    - Tools
  - Verify integrity of public domain
  - Obtain network licenses, etc.
  - Schedule and plan for outsourcing
  - Secure your platform/OS
  - Get interdepartmental and location approval
- **Audit**
  - Nontechnical
    - Interview personnel
    - Review documentation—Inventory, topology, emergency procedures, logs
  - Technical
    - Use the great tools currently available, but don't forget your brain—the tools wil not find everything
    - Plan for outages, and schedule audits for off-peak hours
- **Report and post-mortem**
  - Safeguard report and distribution
  - Prepare for data overload and set aside time to read and investigate
  - Be aware that report may rise more questions than it answers
  - Leverage results for a stronger security posture
- **Action**
  - Prioritize action items, set time line, implement
  - Feed findings back into risk analysis, policy—i.e., start all over again
  - Start thinking intrusion/detection…and revisit risk acceptance
  - Remember that security is a continuous process, not a static solution

Observations and Analysis on Ray

- Only Ray specifies that the scope of the audit is important!
- Determining the goals and expectations of the audit is subjective and quite possibly will change from one audit to another.
- This checklist acknowledges that the audit may be different for a internal firewall than for a perimeter firewall.
- The checklist items related to permissions are objective. These will be either yes or no.
- Although not a part of the technical audit, obtaining the licenses for the software will provide the peace of mind required for running an honest business. This can be measured and is an objective item.
- Personnel interviews are subjective. The information received, although truthful,

will be affected by the experiences of the interviewee.
- The information contained in the report created following the audit will be subjective due to the interpretation of the results by the auditor.
-

VPN Audit

In contrast to the information found regarding firewall audits, there seems to be little information specifically related to auditing a VPN. At the time of this writing, audit procedures and checklists for IPSec VPNs have not been found. A searches for *VPN Audit* on www.google.com, www.yahoo.com, and www.altavista.com revealed negligible amounts of useful information on formal VPN audit procedures. However, combining the firewall audit techniques with proper IPSec VPN setup and configuration, one can derive a audit process for the IPSec VPN hosted on the Netscreen 5 firewall.

Netscreen Checklist

Much information exists regarding the configuration of IPSec VPNs. Since the VPN gateways chosen for this project are Netscreen products, the first place to look for information about the VPN configuration would be the NetScreen Concepts & Examples User's Guide version 2.6.1[8] document. The basic steps (as documented by Netscreen) for configuration are:

1. Enter the address for the remote endpoint of the tunnel in the untrusted address book.
2. Configure the devices at each end of the tunnel with the same options and parameters.
3. Set up incoming and outgoing access policies for VPN traffic to pass bidirectionally through the tunnel.
4. Define the remote gateway and key exchange mode, and specify either a preshared secret or a certificate.
5. Create the autokey IKE VPN entry.

Observations and Analysis on Netscreen

- The setup steps are vague. To arrive at a secure VPN requires knowledge of details that are not a part of the checklist.
- Each of the steps is objective. There are specific and expected values for each item.
- To turn these configuration steps into an audit checklist requires an in-depth understanding of IPSec.

Cisco Checklist

IPSec VPNs may also be implemented using a variety of other vendors products. In the paper entitled Implementing Site-toSite IPSEC VPNs Using Cisco Routers[9], Millie Ives provides this configuration checklist for Cisco routers.

1. Verify that the hardware and software support IPSec, and 3DES encryption.
2. Ensure the IKE feature is enabled.

3. Create filter rule sets to support IKE.
4. Create the IKE policy for the VPN.
5. Configure the IKE parameters such as 3DES encryption, SHA-1 hash, authentication method, and SA lifetime.
6. Create rules for IPSec traffic.
7. Create crypto access lists.
8. Define transform sets.
9. Configure the tunnel interface.
10. Configure crypto map.
11. Apply ctypto map to tunnel interface.

Observations and Analysis on Cisco

- As expected, terminology such as "crypto map" that is Cisco-specific needs to be translated into Netscreen terminology for these items to be useful.
- Steps such as "Ensure IKE is enabled" are objective. It is either *yes* or *no*.
- Other steps can be objectively audited, but how it should be defined is subjective. An example of this is "Create the IKE policy for the VPN."

As can be seen, the setup steps for the Netscreen and Cisco are parallel. The differences arise from the details of the implementation and the product. Corresponding steps can be found for SonicWALL in the SonicWALL VPN User Manual[10] and for CheckPoint[11].

Conclusions

Each of the firewall checklists are general in nature, although may lean more towards a specific firewall. The Spitzner checklist is an example of this, as the paper deals specifically with Checkpoint Firewall-1. The list provided by Farrow gives the most usable framework for creating an audit checklist for the Netscreen 5 firewall/VPN gateway. Work will have to be done to create a suitable checklist that is specific to the Netscreen 5 firewall whose purpose is to be used as a VPN gateway. What follows is a suggested Netscreen 5 audit checklist.

Suggested Audit Checklist

General		
1	Software Version - Objective Ensure that the Netscreen is using the most current version of the operating software. Issue the *get system* command.	By comparing the version of the OS that is returned from the *get system* command with the latest updates on www.netscreen.com, one can easily determine whether this requirement is fulfilled.

2	Administrator Password - Subjective Ensure that the administration account uses a strong password. Issue the *get config* command. The admin password is encrypted.	Because the administration password is encrypted, the auditor must rely upon the owner of the Netscreen to share the password. Then the determination of whether a strong password is in use can be made.
3	Disable telnet and enable SSH – Objective Issue the *get scs* command.	The possible values are either **yes** or **no**.
4	SNMP - Objective Ensure SNMP community strings are not *public* and *private*. Ensure SNMP traps conform to corporate security policy. Issue the *get snmp all* command.	If SNMP is required for management of the Netscreen, then this requirement must be met. If SNMP is n not required, then SNMP must not be enabled.
Firewall		

5	Ingress filtering - Objective
	
	Ensure ingress filters are active
	• Block packets destined for services that are not being offered to the Internet
	• Block illegal addresses – eg 0.0.0.0
	• Block broadcast address – 255.255.255.255
	• Block loopback – 127.0.0.0
	• Block reserved – 240.0.0.0
	• Block RFC1918 addresses
	  o 10.0.0.0 – 10.255.255.255
	  o 172.16.0.0 – 172.31.255.255
	  o 192.168.0.0 – 192.168.255.255
	• Block UDP echo
	• Block ICMP broadcast per RFC2644
	• Block packets from outside the firewall with a source IP address the same as the internal networks.
	• Block source routed packets.
	
	The *set firewall default-deny* command is used by the Netscreen to deny all traffic not specifically allowed by an access rule.
	
	The *set firewall src-route* command block source routed packets.
		This is a Boolean value. To be in spec, the default-deny flag should be set and can be tested using the *get firewall* command. Likewise, the source route flag can be checked with the same command.
		
		This checklist item is required.

6	Block attacks – Objective The Netscreen firewall can automatically block certain kinds of attack. Ensure this is enabled. • Detect SYN Attack • Detect ICMP Flood • Detect UDP Flood • Detect Ping of Death Attack • Detect IP Spoofing Attack • Detect Port Scan Attack • Detect Land Attack • Detect Tear Drop Attack • Detect Address Sweep Attack • Detect Winnuke Attack	These should all be enabled. The *get firewall* command tells whether they are enabled. The values are Boolean.

7	Inbound access rules – Objective If the *get firewall default-deny* command is set, then all traffic not specifically allowed by an access rule is denied. Use the *get policy incoming* command to display these rules.	In the context of the VPN, the only in-bound access rules should be related to the VPN tunnel. These are addressed in the VPN section of the checklist. This step fails if there are any in-bound rules that are not related to the VPN tunnel.
8	Outbound access rules – Objective Use the *get policy outgoing* command	Because one of the assumptions at the beginning of the document is that users on the remote LAN will have full Internet connectivity, the only outbound access rule is to permit any traffic outbound. This rule either exists or does not exist.
9	Logging – Subjective Ensure logging is enabled The Netscreen 5 firewall has a limited amount of RAM for logging. When the log buffer is full, it over-writes from the beginning. It is on by default. The Netscreen 5 has the capability of logging to syslog. In the configuration being used for this study, there is not a syslog server at the remote office. Logging to syslog over the VPN consumes bandwidth.	Depending upon the application and network topology, the syslog option may be either on or off. The default local log is always on.
VPN		

10	Verify the VPN tunnel end-point address – Objective Ensure that the IP configuration for the other end-point of the VPN tunnel is configured accurately. Use the *set address trust <trusted name> <ip address> <subnet mask>* command to specify the address of the trusted side of the Netscreen. Use the *set address untrust <untrusted name> <ip address> <subnet mask>* command to specify the address for the LAN on the other side of the remote gateway. Use the *get address trust* and *get address untrust* commands to return the values.	A thorough knowledge of the topology of the VPN is required to know whether these addresses are correct. An auditor not intimately familiar with the topology must rely on someone else to provide verification of these values.
11	Verify the VPN definition - Objective The VPN definition is where the authentication, encryption, and shared keys are defined for the VPN tunnel. Verify the AutoKey IKE tunnel configuration using the *get ike gateway* command. This returns the VPN tunnel name, the gateway IP, the mode, the encrypted preshare key value, and the IKE phase-1 proposal string. Verify the AutoKey IKE VPN entry using the *get vpn* command. 3DES encryption should be specified for the Encapsulating Security Payload (ESP) and SHA-1 should be the hash for the Authentication Header (AH). The default values for the remainder of the proposal options is sufficient.	The hash algorithm is specified in the organization's security policy. For confidential data being transmitted over the internet, ESP is required so that the source IP, destination IP, and data payload are encrypted. DES encryption is generally considered insufficient for encryption. The AH provides for assurance of integrity of the packet, but does not address confidentiality. Thus both ESP with 3DES and AH are necessary.

12	VPN access rules – Subjective Verify that the rulebase restricts traffic through the VPN tunnel to only what the information security policy allows. Use the *get policy incoming* and *get policy outgoing* commands to check what is allowed.	Compliance with this is completely dependant upon security policy of the organization. Because a VPN essentially extends the working environment to the remote site, it must be specified in the security policy precisely *what* resources may be accessed.
External scans		
13	Port scan the firewall Using nmap, do a *nmap –sS –P0 <ip address of untrusted interface>* to scan for all ports that are available on the external interface. Likewise, do a port scan of the trusted interface.	The Netscreen should block a port scan. If it does, then this step passes.
Report		
14	Prepare report for the audit requestor - Subjective	This step is completely subjective in nature and is simply a result of the audit. It should be prepared with the appropriate audience in mind. If being presented to management, do not overload then with the techno-babble.

Application

The Audit

Item #1 – Software Version - PASS

```
ns5-> get system
Serial Number: 12345678, Control Number: 00000000
SW Version/Checksum: 2.6.0r3.1/222f2969, HW Version: 2010(0)
Image: ns5[1].2.6.0r, Firewall+VPN, FPGA checksum: 00000000 (0/0)

Date 08/16/2001 21:33:15, Daylight Saving Time enabled
The Network Time Protocol is Disabled
Up 0 hours 28 minutes 23 seconds Since 16 Aug 2001 21:04:52
```

```
System IP: 0.0.0.0, Config Port: 80
User Name: netscreen
interface trust, mode nat, up/half-duplex
  ip 172.22.1.1/255.255.255.0 gateway 0.0.0.0, mac 0010.db0a.8f80
  gateway 0.0.0.0, manage ip *172.22.1.1, mac 0010.db0a.8f80
interface untrust, up/half-duplex
  dhcp disabled
  PPPoE encapsulation disabled
  ip 16.164.237.126/255.255.255.128 gateway 16.164.237.1, mac 0010.db0a.8f81
  gateway 16.164.237.1, manage ip *16.164.237.126, mac 0010.db0a.8f81
ns5->
```

As can be seen from the results of the *get system* command, the version of the software is 2.6.0r3.1. According to the support section of the Netscreen web site, this is the current version.

Item #2 – Administrator Password - FAIL

Because the password is encrypted when displayed via the *get config* command, we cannot directly determine whether the password is strong. Because this Netscreen was configured by one of my co-workers, and that I have administrative access to the firewall, I know the password. Because of this knowledge, I am confident in my judgment that the password is not strong. Thus this test fails.

Item #3 – Disable telnet and enable SSH - FAIL

```
ns5-> get scs
SCS is NOT enabled
SCS status: NOT ready for connections
Key regeneration time: 60 minutes
Current number of SCS connections: 0
ns5->
```

Note that the results of the *get scs* command show that SSH is not enabled. Thus this test fails.

Item #4 – Ingress filtering - PASS

```
ns5-> get firewall
Source Route IP Option Filter:         On
Syn Flood Protection:                  On
  Attack Threshold = 200
  Timeout Value: 20
  Alarm Threshold: 512
  Queue Size: 1024
Tear Drop Protection:                  On
Ping-of-Death Protection:              On
IP Address Spoofing Protection:        On
Land Attack Protection:                On
ICMP Flood Protection:                 Off
  Threshold: 1000
UDP Flood Protection:                  Off
  Threshold: 1000
Port Scan Protection:                  Off
  Threshold: 30000
IP Sweep Protection:                   Off
  Threshold: 30000
Winnuke Attack Protection:             Off
Block Java/ActiveX Component:          Off
Default Packet Deny:                   On
```

```
Log Self:                           Off
--- more ---
Log Self for IKE :                  Off
Log Self for SNMP:                  Off
Bypass others Ipsec:                Off
Bypass non-ip:                      Off
ns5->
```

The results of the *get firewall* command provides the information necessary for this test. Note that **Default Packet Deny** is on and that **Source Route IP Option Filter** is on. These are the values required for ingress filtering on the Netscreen-5 firewall. Thus this test passes.

Item #5 – Block attacks - FAIL

```
ns5-> get firewall
Source Route IP Option Filter:      On
Syn Flood Protection:               On
  Attack Threshold = 200
  Timeout Value: 20
  Alarm Threshold: 512
  Queue Size: 1024
Tear Drop Protection:               On
Ping-of-Death Protection:           On
IP Address Spoofing Protection:     On
Land Attack Protection:             On
ICMP Flood Protection:              Off
  Threshold: 1000
UDP Flood Protection:               Off
  Threshold: 1000
Port Scan Protection:               Off
  Threshold: 30000
IP Sweep Protection:                Off
  Threshold: 30000
Winnuke Attack Protection:          Off
Block Java/ActiveX Component:       Off
Default Packet Deny:                On
Log Self:                           Off
--- more ---
Log Self for IKE :                  Off
Log Self for SNMP:                  Off
Bypass others Ipsec:                Off
Bypass non-ip:                      Off
ns5->
```

Once again, the *get firewall* command is used. Here we can see that **ICMP Flood Protection, UDP Flood Protection, Port Scan Protection, IP Sweep Protection,** and **Winnuke Attack Protection** are all off. The audit requirements specify they are to be on. Thus this step fails.

Item #6 – Inbound access rules - PASS

```
ns5-> get policy incoming
 pid  direction  source      destination         service     action      stlc
10001 incoming   AAALAN      WANLAN              ANY         Tunnel      --X-
10002 incoming   AAADNS      WANLAN              ANY         Tunnel      --X-
ns5->
```

The *get policy incoming* command is used to audit the inbound access rules. For the usage of this firewall, there should be no inbound rules other than what are

used for the VPN tunnel. That is the case here. The test passes.

Item #7 – Outbound access rules - PASS

```
ns5-> get policy outgoing
 pid  direction  source       destination          service     action      stlc
    6 outgoing   WANLAN       MNH                  ANY         Permit      --X-
    1 outgoing   WANLAN       AAALAN               ANY         Tunnel      --X-
    7 outgoing   WANLAN       WAN_Access           ANY         Tunnel      --X-
    3 outgoing   Inside Any   Outside Any          ANY         Permit      ----
ns5->
```

Policy 6 is specified to force a particular application to traverse the Internet rather than the VPN. Policies 1 and 7 are for the VPN tunnel. Policy 3 allows full Internet connectivity for the users on the remote LAN. The test passes.

Item #8 – Verify the VPN tunnel end-point address - PASS

```
ns5-> get address trust
Trusted Individual Addresses:
Name                 Address         Netmask         Flag  Comments
Inside Any           0.0.0.0         0.0.0.0           02  All Trusted Addr
WANLAN               172.22.1.0      255.255.255.0     00

ns5-> get address untrust
Untrusted Individual Addresses:
Name                 Address         Netmask         Flag  Comments
Outside Any          0.0.0.0         0.0.0.0           03  All Untrusted Addr
Dial-Up VPN          255.255.255.255 255.255.255.255   03  Dial-Up VPN Addr
AAALAN               172.16.0.0      255.255.0.0       01
AAADNS               16.182.17.3     255.255.255.255   01
AAAEmail             16.135.49.192   255.255.255.248   01
AAADNS2              172.16.1.12     255.255.255.255   01
MNH                  16.135.49.197   255.255.255.255   01

Untrusted Group Addresses:
Group Name       Group Member Count              Comment
  WAN_Access              4
  WAN_DNS                 2

ns5->
```

Using the *get address trust* and *get address untrust* commands, we can see the VPN tunnel IP address information. The definitions of the tunnel end-points are accurate according to the topology of the VPN. The test passes.

Item #9 – Verify the VPN definition - FAIL

```
ns5-> get ike gateway
Id Name            Gateway IP      Mode Preshr Key       Proposals
-- --------------- --------------- ---- ---------------- ---------------
 0 KAAALANVPN       16.164.237.14   Main t0lr21zq         pre-g2-des-md5
  Total Gateways: 1
ns5-> get vpn
Name            Gateway         Mode RPlay Proposals       Monitor  Use Cnt
--------------- --------------- ---- ----- --------------- -------  -------
BBBAAALAN       AAALANVPN       tunl No    nopfs-esp-des-md5 off      4
  Total VPN Auto: 1

Name            Gateway         Local SPI   Remote SPI  Algorithm  Monitor
Total Manual VPN 0
ns5->
```

Testing this item requires both the *get ike gateway* command and the *get vpn* command. The results are seen above. The audit checklist specifies that 3DES encryption and SHA-1 hash are to be used. This test fails.

Item #10 – VPN access rules -

```
ns5-> get policy incoming
 pid  direction  source       destination          service     action      stlc
10001 incoming   AAALAN       WANLAN               ANY         Tunnel      --X-
10002 incoming   AAADNS       WANLAN               ANY         Tunnel      --X-
ns5-> get policy outgoing
 pid  direction  source       destination          service     action      stlc
    6 outgoing   WANLAN       MNH                  ANY         Permit      --X-
    1 outgoing   WANLAN       AAALAN               ANY         Tunnel      --X-
    7 outgoing   WANLAN       WAN_Access           ANY         Tunnel      --X-
    3 outgoing   Inside Any   Outside Any          ANY         Permit      ----
ns5->
```

The *get policy incoming* and *get policy outgoing* commands were used for a previous step in the audit. However, here we focus on the traffic crossing the VPN. What is allowed across the VPN is purely a function of the information security policy of the organization. The organization using this VPN requires the access rules listed above. The test passes.

Evaluation of the Audit

This audit checklist was built specifically for the Netscreen-5 firewall in the VPN context of a particular organization. There are many options and settings on the Netscreen-5 that were not evaluated and were assumed to have the default settings.

The section on actually testing the Netscreen-5 for vulnerabilities is weak. Time should be taken to develop a thorough test through port scanning, "firewalking", and response to denial of service attacks. I was unable to sufficiently audit these with the tools at my disposal. This is an area that should be expanded upon.

The section of the audit where information is taken directly off the command line interface of the Netscreen-5 is sufficient for the requirements of the organization performing the audit.

Future Work

The audit process for the Netscreen-5 firewall could be improved in at least these areas:

1. Include an audit of the VPN design and topology.
2. Several of the subjective tests require knowledge of the information security policy. Many times there is a gap between what is specified in the security policy document and what is actually required for the organization. So, just comparing against the existing security policy *may* leave gaps in the audit. I would like to see the subjective steps expanded to include a review of the security policy against

current business requirements.

3. Processes surrounding the administration of the device were omitted from the audit process. Who configures the Netscreen? Who is responsible for reviewing the logs? Who came up with the passwords? How can we make sure that the passwords used are sufficiently strong?
4. This checklist does not take into account the reason for conducting the audit. An audit resulting from a security breach would be more in-depth than an audit initiated as a curiosity.
5. Several settings on the Netscreen-5 ought to be included in the audit checklist even though they are not specifically related to the VPN.

Sources

The Packet Filter: A Basic Network Security Tool, Dan Strom, September 2000, http://www.sans.org/infosecFAQ/firewall/packet_filter.htm.

Firewalk: Can Attackers See Through Your Firewall, David Irby, December 2000, http://www.sans.org/infosecFAQ/firewall/firewalk.htm.

IPSec, Johan Allard, July 1999, http://www.networkmagazine.com/article/printableArticle?doc_id=DCM20000509S0082.

Security Audit Checklist, Loye Ray, http://polaris.umuc.edu/~lray/ifsm430/security-audit.htm.

Auditing Firewalls: A Practical Guide, Bennett Todd, 1998, http://www.itsecurity.com/papers/p5.htm.

Firewall Audit's from Bedgood.net!, http://bedgood.net/fwaudit.cfm.

Audits from Hell, Carole Fennelly, March 1999, http://www.itaudit.org/forum/networkmanagement/f206nm.htm.

Firewall Audit, Sandy Lindstedt, June 1999, http://www.itaudit.org/forum/networkmanagement/f212nm.htm.

Auditing Your Firewall Setup, Lance Spitzner, September 1999, http://www.enteract.com/~lspitz/audit.html.

Firewall Configuration Done Right, Rik Farrow, December 1998, http://www.networkmagazine.com/article/NMG20000515S0047.

Improving the Security of Your Site by Breaking Into It, Dan Farmer and Wietse Venema, http://www.fish.com/security/admin-guide-to-cracking.html.

[1] http://www.securityportal.com/list-archive/firewall-wizards/1998/Mar/0051.html
[2] http://www.securityportal.com/list-archive/firewall-wizards/1998/Mar/0058.html
[3] http://www.fish.com/security/admin-guide-to-cracking.html
[4] http://www.networkmagazine.com/article/NMG20000515S0047
[5] http://www.enteract.com/~lspitz/audit.html
[6] http://www.itaudit.org/forum/networkmanagement/f212nm.htm
[7] http://polaris.umuc.edu/~lray/ifsm430/security-audit.htm
[8] http://www.netscreen.com/support/downloads/C&E.pdf
[9] http://www.sans.org/infosecFAQ/encryption/IPSEC_VPNs.htm
[10] ftp://ftp.sonicwall.com/pub/info/VPN-021301.pdf
[11] Checkpoint Virtual Private Networks (supplied as PDF on the Checkpoint FW1/VPN1 CD)