



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

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

## Interested in learning more?

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

John Dietrich

GSNA Practical Assignment Version 2.1 (amended July 5, 2002)

Option 1

Auditing A Checkpoint VPN-1 Mobile User Virtual Private Network  
(VPN)

From An Independent Auditor's Point Of View

February 11, 2003

## **Overview**

This paper will document the methodology used to perform a risk based audit of a CheckPoint 4.1 VPN-1 mobile user VPN solution and present the audit results at both a detailed and executive level. In developing an audit methodology for this specific mobile user VPN audit, a review of the current best practices was conducted the results of which are also documented. The reader can take away from this paper a checklist to be used to audit other CheckPoint VPN-1 mobile user VPN environments.

The company name and IP addresses have all been sanitized. 'Acme Corporation' will be used to represent the company being audited.

## **Assignment 1 - Research in Audit, Measurement Practice, and Control**

### ***System to be audited***

The focus of this audit is a CheckPoint VPN-1 version 4.1 mobile user VPN solution that uses the CheckPoint SecureClient 4.1 mobile user VPN client. As shown in Figure 1 below, the Acme Corporation has deployed the VPN-1 gateway in parallel to the corporate Firewall. This places additional importance on ensuring it is configured securely since the VPN traffic will not be inspected by the corporate firewall resulting in the CheckPoint VPN-1 gateway performing both Firewall and VPN duties.

In addition to the corporate VPN, Acme Corporation also allows mobile users to gain access to corporate resources (particularly email) via Citrix remote client and Microsoft Outlook Web Access. The scope of this audit is limited to the CheckPoint VPN configuration but the other remote access solutions will be a factor in discussing the risks associated with the system.

The VPN-1 server is running on a Windows 2000 platform. The VPN client is supported by Acme Corporation only on the Windows 2000 Professional

platform. The majority of mobile users use high-speed Internet access (cable or DSL) so the client side portion of this audit was conducted using a high-speed cable connection. It is important to note that the two firewalls in the diagram are not being used to create a DMZ but each is a distinct entry point into the Acme network and each is configured and maintained without regard to the other.

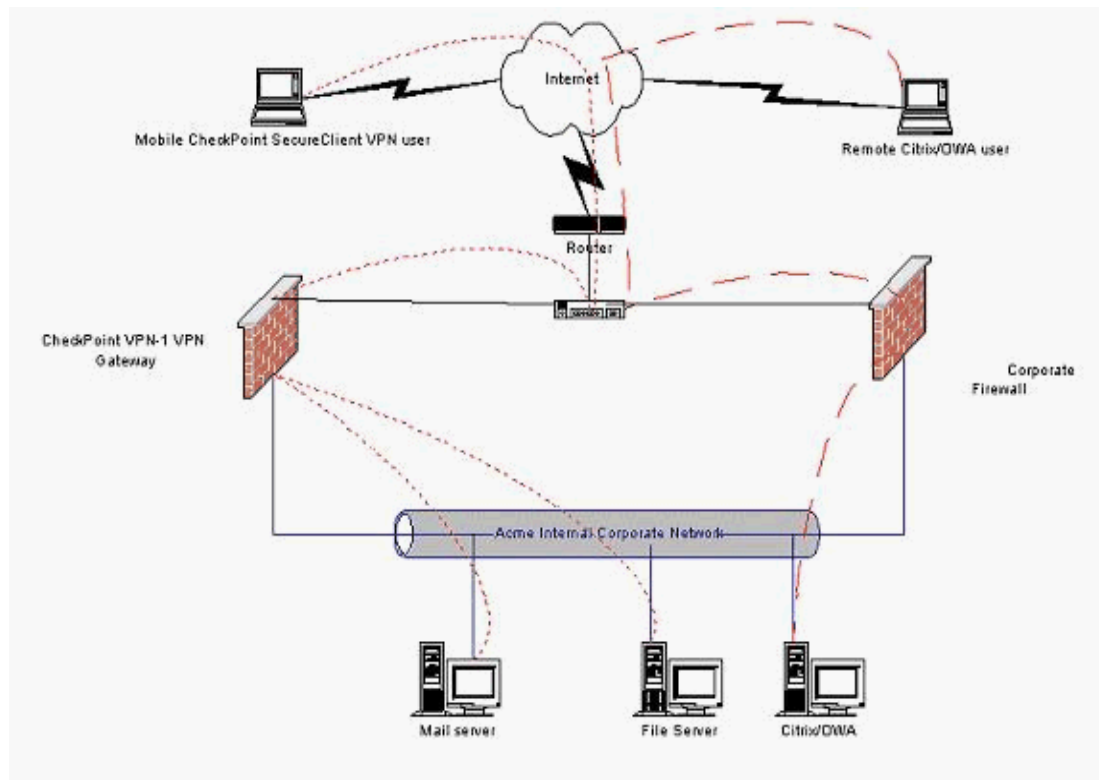


Figure 1 Acme Corporation Remote Access Design

Short-dashed red lines indicate VPN traffic, long-dashed red lines indicate Citrix ICA or SSL (OWA) traffic

### ***Evaluation of the risk to the system***

There are risks associated with both the VPN gateway and client configurations. Acme Corporation has a 'typical' mix of business servers on its internal network (they do not have a secret formula or credit card information stored on the network) so they take the stance that the likely attacker will be a competitor or disgruntled current/former employee. The following table summarizes the risks faced by Acme Corporation's VPN solution:

Risk#	What can go wrong	Likelihood of Issue/Exploit occurring	Consequences of Issue/Exploit
1.	VPN gateway allows unintended traffic to pass into the internal network due to misconfiguration of CheckPoint rules or Windows Operating system.	Medium	High - Potential compromise of the internal network
2.	Virus or Trojan on mobile user laptop	Medium	Severe - Potential compromise of the internal network
3.	Cracker gains internal information provided by VPN gateway	Low	Low – Information gathering to be used in a later attack
4.	Lack of strong passwords allow Cracker to impersonate valid user	High	Severe – Definite compromise of the internal network
5.	Unable to determine who did what in the event of a compromise Event correlation.	High	Medium – lack of audit trail makes tracking of intruder or malicious user difficult. Prosecution effort weakened, more damage done to network or more information stolen.
6.	VPN Gateway or Client is compromised due to lack of applied system patches	Medium	High - Potential compromise of the internal network and or client machine
7.	Theft or loss of client laptop	High	High - Potential compromise of the internal network and or client machine

8.	Lack of High Availability and scalability can cause VPN outage	Medium	Low – Other remote access solutions provide similar functionality
9.	Lack of centralized account management can result in incorrect network access being granted	High	High - Potential compromise of the internal network.
10.	Lack of vendor support results in patches and upgrades not being applied	Medium	High - Potential compromise of the internal network.
11.	A hacker can capture data and decrypt it because a low level of encryption is used	Medium	High - Potential compromise of the internal network.
12.	Shared Operating System accounts allow helpdesk users to modify CheckPoint management accounts to allow for Read/Write access.	High	High - Potential compromise of the internal network.
13.	Mobile VPN user laptop provides direct access back into the corporate network for a hacker.	High	High - Potential compromise of the internal network.

14.	Because of the location within the network of the VPN gateway, unencrypted VPN traffic is not subject to additional Firewall inspection/filtering	High	Medium – Potential compromise of the internal network.
15.	No filtering on the Internet router allows non-VPN traffic to reach the VPN server.	High	Low – If the Gateway is configured properly, it will drop the traffic.

### ***Current state of practice***

Research to determine existing resources to be used to help conduct an audit of a CheckPoint mobile user VPN revealed very little specific detailed information. While VPNs are widely deployed in many organizations, there does not seem to be an abundance of information regarding checklists to be used to audit VPN configurations. Even information from the Virtual Private Network Consortium (<http://www.vpnc.org>) was not directly applicable. Troubleshooting guides and manuals provide the most detailed 'how-to' procedures. These need to be used together with higher-level standards and best practices to arrive at an acceptable audit methodology and checklist.

A good starting point when reviewing security issues is the British Standards 7799 (BS7799 and also ISO17799). The standard says to include the following in the development of a formal policy for mobile computing and teleworking:

... requirements for physical protection, access controls, cryptographic techniques, back-ups, and virus protection. This policy should also include rules and advice on connecting mobile facilities to networks and guidance on the use of these facilities in public places.

It is important that teleworking is both authorized and controlled by management... (BS7799 section 9.8)

A good alternative/supplement to the BS7799 standard is the publicly available Request for Comments: 2196 Site Security Handbook. This guidebook provides some advice for remote connections that apply to VPN connections.

The components of a good security policy include:

- An Access Policy which defines access rights and privileges to protect assets from loss or disclosure by specifying acceptable use guidelines for users, operations staff, and management.
- An Accountability Policy which defines the responsibilities of users, operations staff, and management. It should specify an audit capability, and provide incident handling guidelines.
- An Authentication Policy which establishes trust through an effective password policy, and by setting guidelines for remote location authentication and the use of authentication devices.
- An Availability statement which sets users' expectations for the availability of resources. It should address redundancy and recovery issues, as well as specify operating hours and maintenance down-time periods.

#### Architecture recommendations:

- Firewalls are not always, or even typically, a single machine. Rather, firewalls are often a combination of routers, network segments, and host computers.
- Firewalls are typically thought of as a way to keep intruders out, but they are also often used as a way to let legitimate users into a site. There are many examples where a valid user might need to regularly access the "home" site while on travel to trade shows and conferences, etc. Access to the Internet is often available but may be through an untrusted machine or network. A correctly configured proxy server can allow the correct users into the site while still denying access to other users.
- The current best effort in firewall techniques is found using a combination of a pair of screening routers with one or more proxy servers on a network between the two routers.
- Most firewalls provide logging which can be tuned to make security administration of the network more convenient. Logging may be centralized and the system may be configured to send out alerts for abnormal conditions. It is important to regularly monitor these logs for any signs of intrusions or break-in attempts.

#### Security Services and Procedures:

- When using cryptography products, like PGP, take care to determine the proper key length and ensure that your users are trained to do likewise. As technology advances, the minimum safe key length continues to grow.

- Given today's networked environments, it is recommended that sites concerned about the security and integrity of their systems and networks consider moving away from standard, reusable passwords.
- Portable hosts are a particular risk. Make sure it won't cause problems if one of your staff's portable computer is stolen.
- All logins, whether successful or unsuccessful should be logged. However, do not keep correct passwords in the log.

An article entitled "Management Strategies Best Practices For VPN Implementation" by Browne, Lewis, Hamilton, and Weaver provides a high-level checklist of sorts for VPN deployment. These areas are relevant to this audit:

- The VPN gateway location in the network.
- External authentication services recommendation.
- Client operating system strategy
- The assignment of IP addresses to remote access VPN users.
- Logging requirements
- VPN gateway redundancy design

Aside from VPN specific resources, the individual underlying components of the VPN solution have more information available about them. Checklists on Firewall, Windows 2000 and Personal Firewall configurations. An excellent resource for this information is NIST

(<http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf> NIST Special Publication 800-41 January 2002 Guidelines on Firewalls and Firewall Policy).  
<http://www.auditnet.org/docs/CheckpointFirewall.txt> and SANS ([www.sans.org](http://www.sans.org))

## Assignment 2 –Create an Audit Checklist

The following checklist was developed from existing high-level checklists, technical manuals and personal experience. It covers an audit of a CheckPoint VPN-1 mobile user VPN. Both the client and server will be audited. Specific risks are mapped back to the risk matrix in Assignment 1.

Audit Step 1.	Security Policy for VPN/Remote access
Control Objective	The documentation and communication of a corporate security policy and the existence of standards for the deployment and use of VPN Remote access.
Reference	BS7799 (Section 3), NIST (Pub SP 800-41, SP 800-47, SP 800-46), RFC 2196 (section 2.2)



Risk	Without a formal policy, inconsistent settings may be applied. Business objectives may not be met. Risks # 1,5
Compliance	A formal policy exists or it does not. Are there written procedures and is there an acceptable use policy? Is the policy communicated to the user community?
Testing	Obtain the policy from IT or HR and interpret the policy to determine if existing configuration supports it. Consider all undocumented and documented procedures that may exist in place of a formal policy. Sample user community to determine policy awareness level.
Objective/Subjective	Subjective- review and interpretation of the policy, communication of policy to user community.

Audit Step 2.	Physical Security
Control Objective	Unauthorized physical access to the VPN gateway server must be protected.
Reference	BS7799 (Section 7), RFC 2196 (section 4.5.1)
Risk	Without proper security, access to the box would allow a person to attempt password guessing, ability to create/modify CheckPoint user accounts, booting from floppy, or accidental/ intentional denial of service. Very high likelihood. Risks #5
Compliance	While different levels of security are possible depending on business requirements, a basic level of security (e.g. server is behind a locked door and is password protected) needs to exist to achieve compliance: Server is locked in a room with restricted access. Logs are kept of server access. Server is in a locked rack and is password protected.
Testing	Observe precautions in place by asking to visit the server room. Record steps that a visitor is required to go through to get access (e.g. Sign log book) Attempt to access the server and record controls on server access (e.g. Locked rack, password protected screen)
Objective/Subjective	Objective – Server access must be limited to authorized personnel, behind a locked door and password protected.

Audit Step 3.	License and Support
Control Objective	The VPN gateway and clients must be properly licensed and covered under technical support and software maintenance
Reference	BS7799 (Section 10), NIST (SP 800-40 Section 5), CheckPoint User Center
Risk	Access to critical patches may depend on a valid support contract. Phone support may be needed if in-house support is lacking. Eval versions of software should not be in production. Could result in denial of service if eval expires. Risks # 10, 6
Compliance	The software is registered and covered under software maintenance and licensed for the correct number of users as shown in the CheckPoint User Center. The level of technical support required is dependent on business requirements.
Testing	<p>Visit the CheckPoint User Center <a href="https://usercenter.checkpoint.com">https://usercenter.checkpoint.com</a> have the administrator log in using the appropriate credentials to view the registered product list.</p> <p>Run FW printlic command from VPN-1 /bin directory. The output will look like:</p> <pre>Host      Expiration Features 10.1.1.1  Never    cpvp-vsc-100-v41 CK-xxxxxxx 10.1.1.1  Never    CPVP-VEE-U-3DES-MODULE-V41 CPVP-VEE-U-3DES-MGMT-V41</pre> <p>Indicating a 100 user SecureClient license (cpvp-vsc-100) and Enterprise Edition VPN-1 server (CPVP-VEE-U-3DES)</p> <p>Run FW ver command from VPN-1 /bin directory (Run the command once with the -k switch and once without any switches as the build number may vary slightly). The output will look like:</p> <pre>This is Check Point VPN-1(TM) &amp; FireWall-1(R) Version 4.1 Build 41514 [VPN + DES + STRONG]</pre> <p>A good site to visit to determine what build number equates to what service pack is:</p> <p><a href="http://www.phoneboy.com/fom-serve/cache/377.html">http://www.phoneboy.com/fom-serve/cache/377.html</a></p> <p>Compare what is installed on the server to what the User</p>

	Center reports.
Objective/Subjective	Objective – Must have registered software and have software maintenance

Audit Step 4.	Performance and Scalability
Control Objective	The system must perform within manufacture's suggested limits and be able to scale to support additional VPN users.
Reference	CheckPoint FireWall-1 Performance Tuning Guide, CheckPoint Administration Guide (Chapter 19), Server manufacturer's specifications
Risk	Business objectives may not be met if the server can't handle additional VPN users or support more simultaneous users. Risks # 8
Compliance	Is Hardware sufficient to support current and future VPN users? Business requirements will determine when a VPN Accelerator Card or faster CPU would be needed. Best practice performance enhancement settings should be made.
Testing	<p>Operating System Enhancements - check that the following settings have been made:</p> <ul style="list-style-type: none"> <li>• NT memory strategy set to "Maximize Throughput for Network Applications"</li> <li>• Unneeded services and drivers are disabled (See OS hardening test too).</li> </ul> <p>Services: Alerter, Computer Browser, DHCP client, Messenger, Server, Task Scheduler  Devices: Parallel, ParPort, ParVdm, Serial, WINS Client  The Netbios Interface and Wins Client (TCP/IP) unbound from the network bindings.</p> <ul style="list-style-type: none"> <li>• Performance boost for foreground applications should be disabled.</li> <li>• Pagefile optimized with a fixed size page file of at least 2 times the amount of RAM available on a another (preferably dedicated) disk drive.</li> <li>• Tuning TCP/IP registry values to improve network performance. <ul style="list-style-type: none"> <li>▪ Parameters that affect the IP forwarding performance:</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>▪ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\ForwardBufferMemory = 296960</li> </ul> <p>REG_DWORD, multiple of 256, default 74240. Buffer the IP allocates to store packet data in the router queue. The default value is enough for 50 1480-byte packets.</p> <ul style="list-style-type: none"> <li>▪ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\NumForwardPackets = 200</li> </ul> <p>REG_DWORD, default 50. Number of IP headers allocated for router queue. Should be at least as large as ForwardBufferMemory / IP data size of the network.</p> <ul style="list-style-type: none"> <li>▪ Increasing these two parameters can have significant effect on throughput especially with 'slow' policies.</li> <li>▪ Other TCP/IP stack parameters:</li> <li>▪ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize</li> </ul> <p>REG_DWORD, default 8760 for Ethernet. Larger TCP receive window size will improve performance over high-speed networks. For highest efficiency should be even multiple of TCP Maximum Segment Size (MSS).</p> <ul style="list-style-type: none"> <li>▪ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\MaxFreeTcbs = 0xFA0</li> </ul> <p>REG_DWORD, default 2000, timewait table size</p> <p>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\MaxHashTableSize = 0x400</p> <p>REG_DWORD, default 512, TCB hash table size</p>
--	---

	<p>FireWall-1 System Enhancements - check that the following settings have been made:</p> <ul style="list-style-type: none"> <li>Expand the VPN-1 memory pool a good rule of thumb number for busy firewall memory allocation parameter is 16MB. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\FW1\Parameters \Memory = 16000000</li> <li>Increase the connection table limit to 50000 (default 25000). With that number of connections it is also important to increase the table hash size to 65536 (default 8192) for faster lookups. Insufficient connection table size leads to connections being dropped and serious performance degradation. Adequate hashing noticeably improves performance. In \$FWDIR/lib/table.def file, 'connections' value: connections = ... limit 50000 hashsize 65536</li> </ul> <p>Windows Performance monitor should be run to check CPU utilization during a period of normal VPN usage. The hardware spec that affects VPN-1 performance by far the most is processor speed.</p> <p>128 MB of RAM is a minimum for a high performance firewall system.</p>
Objective/Subjective	Objective – CPU utilization over the course of a normal usage period is not maxed out, CheckPoint performance recommendations have been implemented.

Audit Step 5.	Firewall Rule base
Control Objective	Functionality of the VPN Gateway's Firewall settings must be configured appropriately and simply to block all non-VPN traffic.
Reference	BS7799 (Section 9), NIST(Pub SP 800-41), CheckPoint Manual
Risk	Focus on VPN functionality may cause admin to overlook Firewall functionality. Could result in compromise of internal servers. Risks # 1, 5

Compliance	Make sure only desired VPN traffic is allowed in and out of the VPN-1 Gateway. VPN-1 log should show all non-VPN traffic is dropped.
Testing	<ul style="list-style-type: none"> <li>• Review the rule base and Firewall Properties page for misconfiguration and complexity. Only VPN related rules should be necessary.</li> <li>• Check against corporate security policy.</li> <li>• Scan Firewall for open ports (using a tool like Fscan) – look for non-VPN related open ports.</li> <li>• Attempt to use the VPN-1 server as an outbound gateway from an internal workstation by setting the default gateway to be the internal address of the VPN-1 server.</li> </ul>
Objective/Subjective	Objective – Standard best practice firewall rules in place (e.g. Drop all as a last rule). Firewall blocks all non-VPN traffic.

Audit Step 6.	VPNAccess
Control Objective	The VPN Gateway's rule configuration and properties configuration must allow only encrypted access by authenticated users.
Reference	BS7799 (Section 9), NIST (Pub SP 800-46 section 7), CheckPoint manual
Risk	Determine if access is undermined by other Firewall rules. Are proper restrictions in place to prevent information gathering. Risks # 3, 1
Compliance	Make sure only authorized users have access to VPN resources and there is no rule allowing non-VPN access to the same resources. PING test should fail if there is non-authenticated VPN connection.
Testing	<p>Check for the existence of rules that have the Action 'Client Encrypt' look for valid destinations to test access to. These VPN rules should be the first rules in the rulebase. Attempt to ping a resource with and without an authenticated VPN connection.</p> <p>Under the Desktop Security Tab of the Firewall Properties page The option to 'Respond to Unauthenticated Topology Requests' should be unchecked.</p> <p>Attempt to setup a client without using a known account to see what information can be acquired (topology download).</p>

Objective/Subjective	Subjective- Review of rules against security policy. Objective – Authenticated users should be the only ones allowed to obtain topology information and access to VPN resources.
----------------------	---

Audit Step 7.	Operating System Hardening
Control Objective	The VPN Gateway's operating system must be hardened and maintained to prevent system compromises.
Reference	NIST (SP 800-43), SANS, CheckPoint FireWall-1 Performance Tuning Guide
Risk	Unneeded services, as defined by CheckPoint and a combination of best practices (See SANS) and business requirements (A subjective assessment), should be disabled otherwise they invite attack. Risks # 5, 6
Compliance	Has a hardening standard been followed when building the VPN-1 server. Determine what services are running. At least the following should be stopped: Alerter, Computer Browser, DHCP client, Messenger, Server, Task Scheduler. NetBIOS should not be bound to the external interface.
Testing	Run the Netstat –an command. Run IPCONFIG /ALL command. List all Services from Control Panel -> Services. Request server build documentation look for standards (NT security templates used etc).
Objective/Subjective	Objective – Only essential services should be running, documented server build should exist.

Audit Step 8.	VPN User Account Management
Control Objective	Proper account management procedures must be in place to ensure appropriate VPN access is granted.
Reference	BS7799, NIST(Pub SP 800-46 section 7), CheckPoint Manual, Management Strategies Best Practices For VPN Implementation
Risk	Unwanted user may be given access accidentally. Risk is high without centralized management in place. Total compromise of resources might result. Risks # 9
Compliance	Is the user database maintained on the VPN-1 Gateway or is it centralized elsewhere. Policy in place to add/remove users. Only users with valid Corporate Windows 2000 Domain accounts should have a CheckPoint VPN account created
Testing	List current users allowed VPN access (Manage>Users in

	the Policy Editor). By comparing the CheckPoint User Database against the Windows 2000 Domain user database, accounts in the CheckPoint database but not in the Windows 2000 database are suspect. HR needs to confirm status of users . Look for policy to support account creation/removal.
Objective/Subjective	Objective – look for unauthorized users in user database and look for centralized management (e.g. RADIUS)

Audit Step 9.	Virus Protection for Mobile User
Control Objective	Mobile user's desktop machines must be protected with the corporate standard Anti-Virus software.
Reference	BS7799 (Section 8), NIST (SP 800-46)
Risk	Compromise of a client machine with a Trojan might allow access to the corporate network by an unauthorized user. Client machine could become a participant in a Denial of service attack. Risks # 2
Compliance	Is there a corporate antivirus strategy and policy. Are updates pushed to all mobile VPN users.
Testing	Check client configuration to determine if policy is being followed. Test that the Anti-Virus software: <ul style="list-style-type: none"> <li>• Initializes with the boot of the operating system</li> <li>• Runs in the background and automatically scans all incoming files</li> <li>• Automatically updates virus signatures on a weekly basis. If this option is unavailable, then the signatures should be updated manually on a weekly basis.</li> <li>• Attempts to recognized unknown or "mutated" viruses not contained in the virus signature database file.</li> </ul>
Objective/Subjective	Objective – Are patterns up-to date on client machine?

Audit Step 10.	Log Settings
Control Objective	VPN traffic must be logged and logs must be maintained and reviewed.
Reference	BS7799 (Section 8.4), NIST, CheckPoint manual, Management Strategies Best Practices For VPN Implementation



Risk	Without proper logs, troubleshooting, auditing and incident response is very difficult. Intruders could go undetected allowing free reign in the corporate network. Risks # 5
Compliance	Determine if logging is enabled on both the OS and the VPN-1 software. Is there evidence of log reviews and maintenance? What rules require logging can be subjective based on business requirements but VPN and Drop ALL rules should almost always be logged.
Testing	Inspect the rules to see where logging is enabled. Confirm that all implied rules are logged under the Security Policy tab of the Policy Properties in the Policy Editor. Generate traffic to match each rule to see that it is logged. For Client Encrypt rules, use the VPN Client and attempt to access internal resources. For the Drop ALL rule, use Ping and Telnet to try to connect to an internal resource. For any other rule that allows or denies a specific type of traffic, use the appropriate client or Telnet on the port that is open (Telnet Port#) to generate traffic to match the rule. Run the AT command to see if the CheckPoint logswitch command is scheduled to run in order to roll the log. Ask for a high-level report. On the client, temporary log files can be made by creating Fwenc.log for tracking SecuRemote actions and Sr.log for tracking packets blocked by SecureClient Policy.
Objective/Subjective	Objective – Is logging enabled, reviewed and maintained?

Audit Step 11.	Laptop physical protection
Control Objective	Mobile user's laptops must be protected from theft or data loss.
Reference	BS7799 (Section 9.8), NIST, RFC 2196 (section 4.5.1)
Risk	A stolen laptop with cached credentials would allow total access to corporate resources. Risks # 7
Compliance	Theft itself can't be completely prevented but at least the use of a power on BIOS password and file encryption should be employed. Login credentials should not be cached although this is a subjective business requirement decision.
Testing	Look for corporate policy guidelines, inspect a laptop by booting it up. Is a BIOS password enabled? Does the Windows Operating System auto-login? Under the Passwords option in the SecureClient VPN software is Single Sign On Configured and enabled?
Objective/Subjective	Objective – Are power on passwords and encryption in place? Is Single Sign On enabled

Audit Step 12.	High Availability / Disaster recovery
Control Objective	A High Availability / Disaster recovery strategy must be in place to prevent loss of VPN service.
Reference	BS7799, NIST, CheckPoint manual
Risk	Business objectives may not be met if there is an outage of the VPN service. Users may lose productivity. Many single points of failure increase risk. Risks # 8
Compliance	Review policy regarding high availability, are there multiple policy servers and VPN entry points? The existence of multiple Internet connections and at least a cold spare server. The level of High availability in all components is a subjective business requirement.
Testing	If more than one VPN gateway exists, Attempt to access VPN services from more than one Gateway. Pull the plug on one gateway to determine fail over behavior while laptop is PINGing a resource via the VPN. Confirm current Firewall is backed up and a cold spare server is identified and compatible for a restore.
Objective/Subjective	Objective – Does fail over work – Is there a Disaster recovery plan and cold spare server?

Audit Step 13.	Patch Level
Control Objective	Current and compatible Patch levels of OS, CheckPoint Server and VPN client software must be maintained.
Reference	BS7799 (section 10), NIST (SP 800-40)
Risk	Unpatched software and operating systems are classic entry points for hackers. There is a high risk of an exploit of an unpatched server. Risks # 6, 10
Compliance	Look for the latest revisions of all software components of the VPN solution
Testing	Perform FW ver on the gateway, Look at the Help – About menu option in the CheckPoint client, issue the Winver command in the Windows Operating system
Objective/Subjective	Objective – Patches are at manufactures specified current level

Audit Step 14.	Accountability
Control Objective	VPN users entering the internal network must be identifiable by IP address using Network Address Translation.

Reference	BS7799, CheckPoint Manual, Management Strategies Best Practices For VPN Implementation
Risk	If users are allowed access without a known IP address it will be difficult to spot VPN user activities and to restrict use based on IP address. Risks # 5, 1, 4
Compliance	Are VPN users assigned a known range of addresses when they are granted VPN access.
Testing	<p>Confirm that IP Pool NAT is enabled under the IP Pool NAT tab of the Policy Properties in the Policy Editor.</p> <p>Under Manage-&gt;Network Objects in the Policy Editor, Confirm the Address range in the object containing the IP Nat Pool. Make sure the range can accommodate the licensed number of users. Start a VPN session and check the Log to see that the VPN client's source address is translated to an address in the NAT Pool.</p>
Objective/Subjective	Objective – Are VPN users identifiable by IP address on the internal network by being NATed to a Pool address.

Audit Step 15.	Encryption
Control Objective	Appropriate encryption level and settings must be in use for VPN connections
Reference	BS7799 (section 10), NIST (SP 800-46), CheckPoint Virtual Private Networks manual (Chapter 9)
Risk	Unless the highest level of encryption is used, it may be possible for a hacker to capture data and decrypt it. This is a medium risk due to the effort involved but the compromise could be significant. Reliance on pre-shared secrets and usernames is not as secure as certificates because they can be guessed. Risks # 11

Compliance	<p>Is 3DES encryption in use? Are pre-shared secrets or certificates in use?</p> <p>Authentication: For IKE encryption (The only type recommended), The SecuRemote Client and VPN-1 server authenticate each other by verifying that the other party knows the pre-shared secret, which is the user's password (as defined in the Authentication tab of the user's IKE Properties) OR the user checks Use Certificate, enters an Entrust profile file name and a Password to access the certificate. The SecuRemote Client authenticates itself to the VPN-1 server by using its certificate. The VPN-1 server verifies the certificate against a certificate revocation list (CRL). The VPN-1 server authenticates itself by sending the SecuRemote Client its certificate and a copy of a valid CRL signed by the Certificate Authority.</p> <p>Key Exchange: Once the user has been authenticated, the SecuRemote Client and VPN-1 server exchange encryption keys, in preparation for encrypting the actual connection. The method of key exchange depends on the encryption scheme used: FWZ or IKE.</p> <p>Connection: After encryption keys have been exchanged, the connection begins. The connection is encrypted according to the encryption scheme used: FWZ or IPsec (for IKE).</p>
Testing	On the VPN client, confirm Tools->Encryption Scheme has IPsec selected. Check the VPN properties of the Firewall object and edit the IKE settings. Review the CheckPoint log to verify that the setup of the VPN connection uses 3DES IPSEC. If possible, capture VPN traffic with a packet sniffer to confirm that it is indeed encrypted.
Objective/Subjective	Objective – 3DES encryption should be the only level supported. IKE should be used instead of FWZ

Audit Step 16	VPN Administration
Control Objective	Least amount of access is granted to the VPN Gateway for users to perform job duties, accounts are not shared.
Reference	BS7799 (section 8)

Risk	Make sure access levels are appropriate for the job. Write access is not needed for the helpdesk to view log files. Unintended changes to the system could occur. Risks # 5, 12
Compliance	Users should have only the appropriate power at both an Operating system and VPN-1 level necessary to perform their job. Each user has their own individual account.
Testing	<p>Look for segregation of duties and appropriate level of privilege for the job.</p> <p>List all CheckPoint GUI client IPs and Users. Verify that all IP addresses that are allowed GUI access have a business need.</p> <p>List all management accounts in Windows and confirm each account has the appropriate level of privilege for the job and that shared accounts are not in use.</p> <p>Verify read only accounts cannot make unexpected changes by trying to create a new object and try to install a policy from the CheckPoint Policy Editor.</p>
Objective/Subjective	Objective – Accounts are not shared and access levels are appropriate.

Audit Step 17.	Personal Firewall
Control Objective	The VPNclient's personal Firewall settings must be enforced on the mobile user's desktop
Reference	BS7799, NIST, CheckPoint Manual
Risk	A VPN client machine must have protection from unauthorized inbound access. If compromised, a mobile VPN user laptop would provide direct access back into the corporate network. Risk is very high for Cable/DSL 'always on' connections. Risks # 13
Compliance	Is the personal firewall policy set to disallow all inbound connections? Attempts to access the corporate network will fail if the personal firewall is disabled.
Testing	<p>Check that the personal firewall blocks inbound connections by scanning the client with a port scanner (e.g. Shields Up).</p> <p>Disable the Firewall client on the Mobile user laptop by selecting the Policy option and then select 'Disable Policy' and attempt to access the corporate network (PING a host)</p>

Objective/Subjective	Objective – Scan shows all connections are blocked, VPN Gateway disallows connections if personal firewall disabled.
----------------------	--

Audit Step 18	Documentation
Control Objective	Network and VPN documentation must be maintained.
Reference	BS7799, NIST, RFC 2196
Risk	Lack of documentation makes change control impossible. Alternate paths around the VPN-1 Gateway could exist. Risks # 5
Compliance	Are documents reviewed on a scheduled basis and kept up to date via a change control process?
Testing	Confirm current diagram exists. Compare documented rulebase with production rulebase and note discrepancies. Review change control logs to find last change made to VPN-1 Server.
Objective/Subjective	Objective – Current documents are produced

Audit Step 19.	VPN Design
Control Objective	The VPN Gateway must physically be located on the corporate infrastructure so as not to compromise security.
Reference	BS7799 (section 9), NIST (SP 800-41), Management Strategies Best Practices For VPN Implementation, RFC 2196 (section 3.3)
Risk	Locating the VPN gateway in a position on the network that allows traffic to by-pass the firewall can allow for unintended access. Risks # 14
Compliance	Is there a justification for the design and location of the VPN gateway? Is the unencrypted VPN traffic subject to Firewall inspection?
Testing	Review network diagram to look for alternate access points into the corporate network. Use Traceroute to confirm VPN traffic enters via the VPN-1 gateway. Confirm the range of NAT pool address is routed back to the VPN-1 Gateway on the internal network.
Objective/Subjective	Subjective- Determine design justification Objective- Determine VPN traffic is routed into and out of the VPN gateway.

Audit Step 20.	Router Configuration
Control Objective	The Internet router must be configured to screen non-VPN traffic out.
Reference	SANS, NIST, RFC 2196 (section 3.3)
Risk	Proper ingress and egress filtering allow the router to screen non-VPN traffic before it reaches the VPN server. Risks # 15
Compliance	Is the router configured to screen non-VPN traffic destined for the VPN Gateway?
Testing	Send VPN and Non-VPN traffic to/from the VPN Gateway and examine the router logs to see what was allowed. Use the VPN client to establish a normal VPN session. Confirm via the router log and/or Access control list that it allows the key exchange to take place and passes the encrypted traffic. Use Telnet to try to connect to the VPN-1 Gateway directly and confirm via the router log and/or Access control list that it blocks the connection Confirm Best practice Egress/Ingress Filters are in place in the Access control list.
Objective/Subjective	Objective – Unwanted traffic is dropped.

### Assignment 3 – Audit Evidence

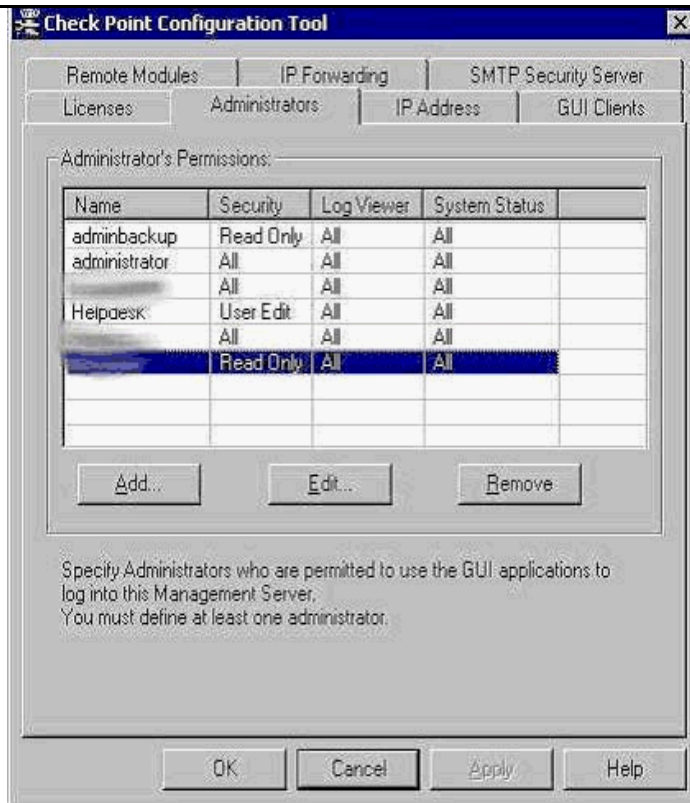
#### **Conduct the audit**

12 of the 20 checklist items are presented here including five Stimulus Response Test Items:

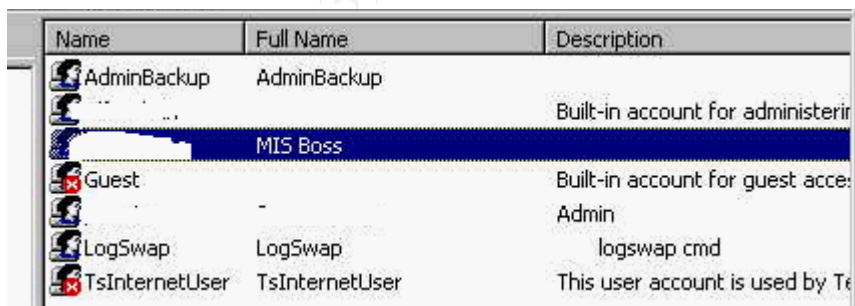
Audit Step 16	Test 1 VPN Administration
Control Objective	Least amount of access is granted to the VPN Gateway for users to perform job duties, accounts are not shared.
Testing	Look for segregation of duties and appropriate level of privilege for the job. List all CheckPoint GUI client IPs and Users. Verify that all IP addresses that are allowed GUI access have a business need.  List all management accounts in Windows and confirm each account has the appropriate level of privilege for the job and that shared accounts are not in use.  Verify read only accounts cannot make unexpected changes by trying to create a new object and try to install a policy from the CheckPoint Policy Editor.

## Findings

### Fail

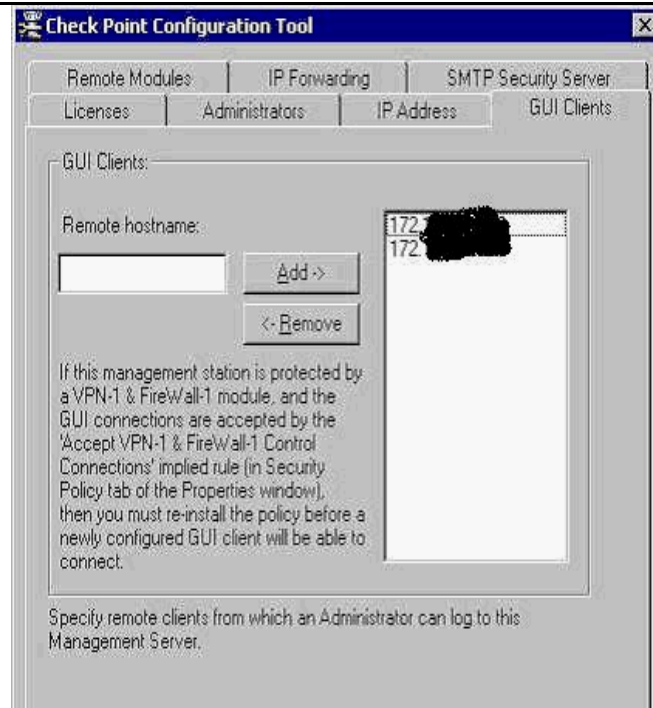


Accounts are created based on job function, which is good. Shared accounts like 'Helpdesk' should be avoided



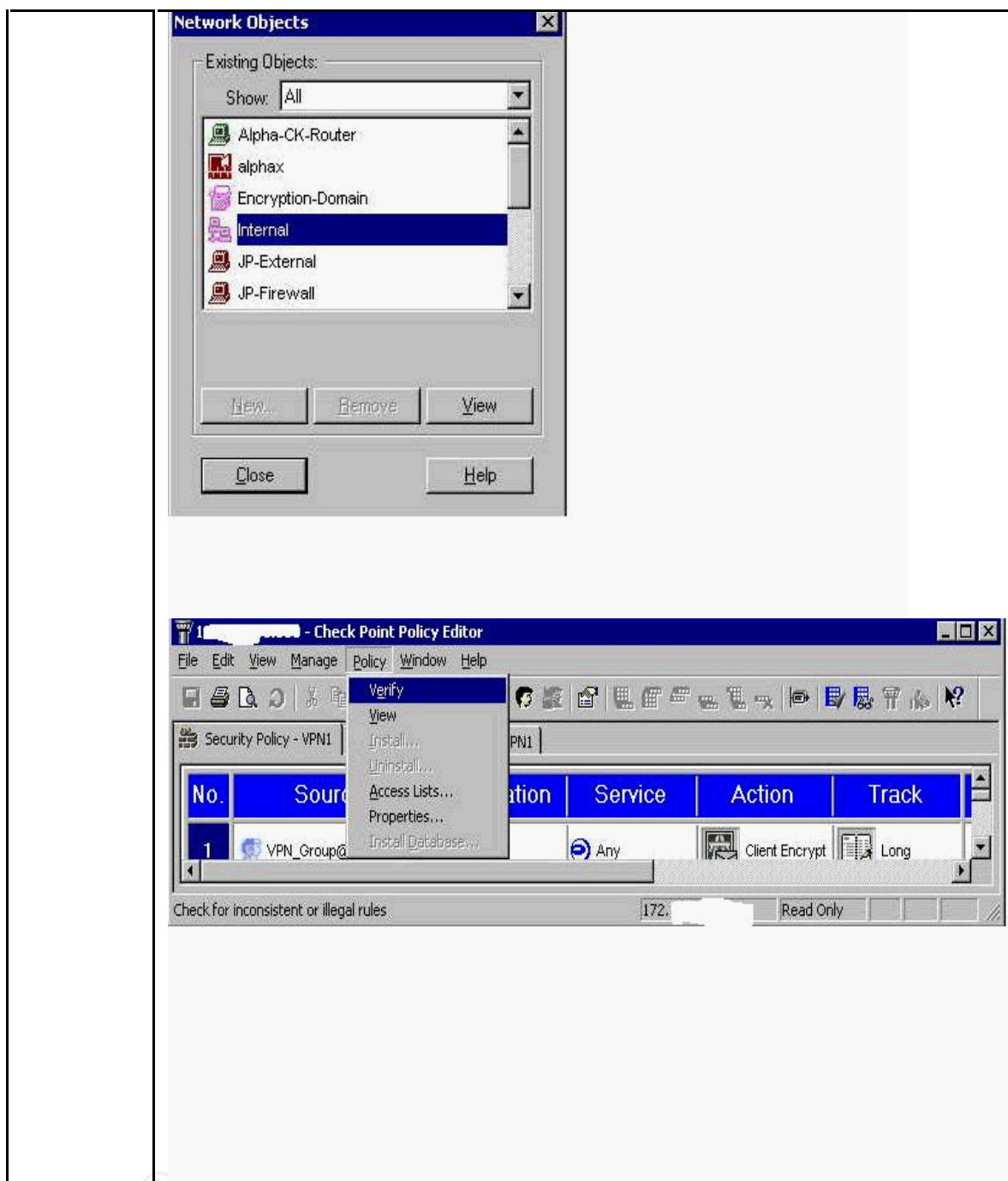
Limited windows accounts created but all have administrator access. Can easily change all CheckPoint user accounts.





The above screen shot shows that only two internal remote workstations are allowed GUI (management) access to the VPN-1 Server.

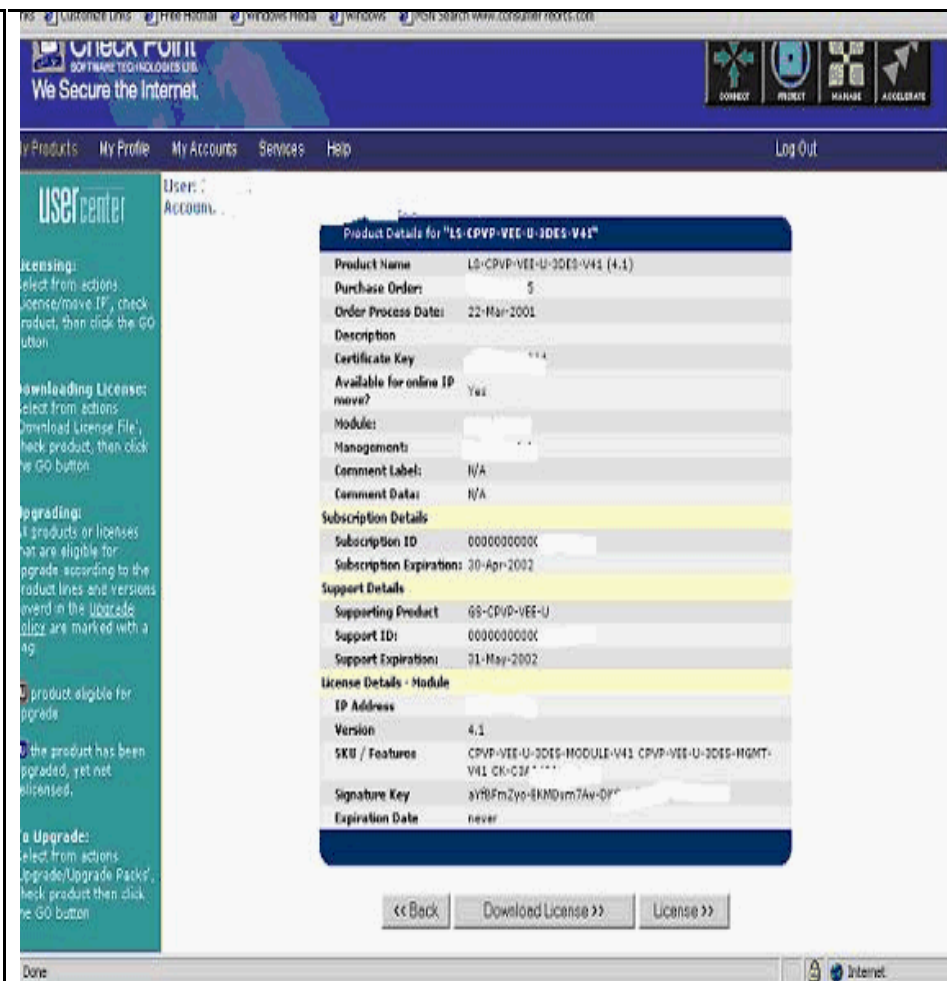
The following 2 screen shots show that while logged into the VPN-1 Management console as the Read-Only Adminbackup user, the option to remove or create new network objects is not available and the option to install/uninstall a policy or database is not available.



Audit Step 3	Test 2. License and Support
Control Objective	The VPN gateway and clients must be properly licensed and covered under technical support and software maintenance
Testing	Visit the CheckPoint User Center <a href="https://usercenter.checkpoint.com">https://usercenter.checkpoint.com</a> have the administrator log in using the appropriate credentials to view

	<p>the registered product list.</p> <p>Run FW printlic command from VPN-1 /bin directory. The output will look like:</p> <pre>Host          Expiration Features 10.1.1.1      Never      cpvp-vsc-100-v41 CK-xxxxxxx 10.1.1.1      Never      CPVP-VEE-U-3DES-MODULE-V41 CPVP-VEE- U-3DES-MGMT-V41</pre> <p>Indicating a 100 user SecureClient license (cpvp-vsc-100) and Enterprise Edition VPN-1 server (CPVP-VEE-U-3DES)</p> <p>Run FW ver command from VPN-1 /bin directory (Run the command once with the -k switch and once without any switches as the build number may vary slightly). The output will look like:</p> <pre>This is Check Point VPN-1(TM) &amp; FireWall-1(R) Version 4.1 Build 41514 [VPN + DES + STRONG]</pre> <p>Compare what is installed on the server to what the User Center reports.</p>
--	---

Fail



Software subscription expired April 30, 2002 and Tech support expired May 31, 2002

### Results of FW printlic:

This is Check Point VPN-1(TM) & FireWall-1(R) Version 4.1 ( 4Dec2002 21:02:14)

(printing license embedded in fw-1 kernel module)

Host      Expiration      Features

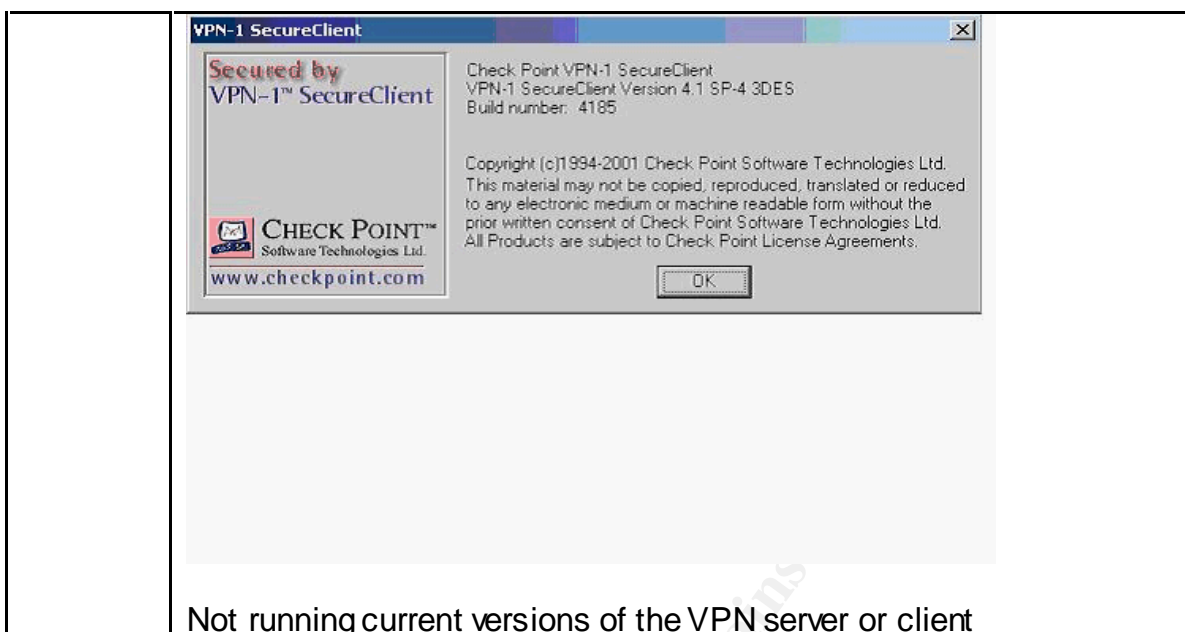
x.x.x.x      Never      cpvp-vsc-100-v41 CK-1E1xxxxxx4

x.x.x.x      Never      CPVP-VEE-U-3DES-MODULE-V41 CPVP-VEE-U-3DES-MGMT-V41 CK-C3xxxxxxx4

100 user license for SecureClient is not registered in User Center but both Gateway and SecureClients are set to Never expire

### Results of FW ver:

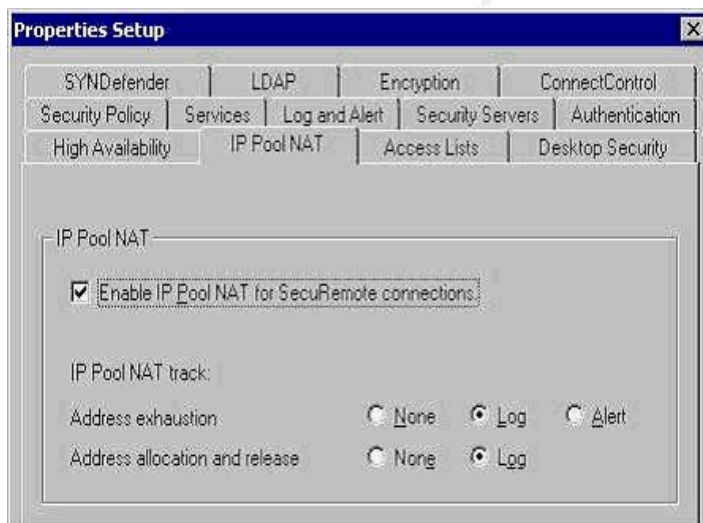
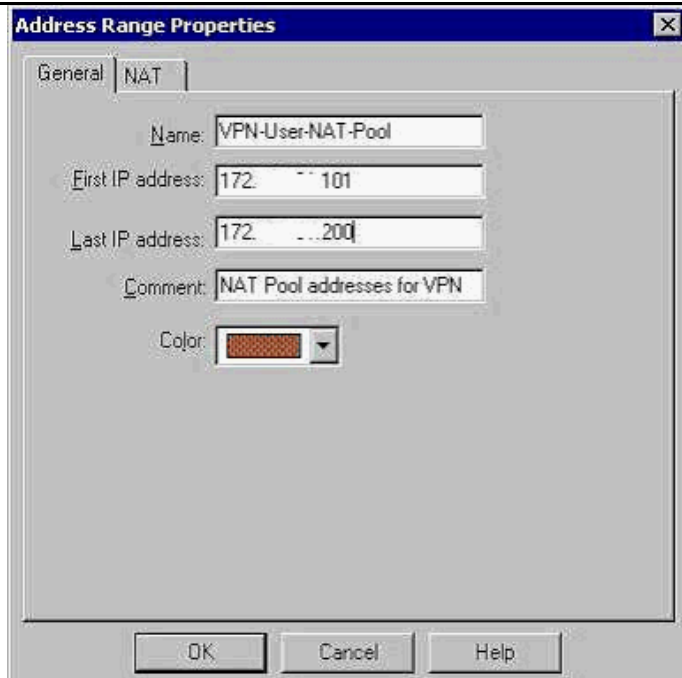
This is Check Point VPN-1(TM) & FireWall-1(R) Version 4.1 Build 41514 [VPN + DES + STRONG]



Audit Step 14	Test 3 Accountability
Control Objective	VPN users entering the internal network must be identifiable by IP address using Network Address Translation.
Testing	<p>Confirm that IP Pool NAT is enabled under the IP Pool NAT tab of the Policy Properties in the Policy Editor.</p> <p>Under Manage-&gt;Network Objects in the Policy Editor, Confirm the Address range in the object containing the IP Nat Pool. Make sure the range can accommodate the licensed number of users. Start a VPN session and check the Log to see that the VPN client's source address is translated to an address in the NAT Pool.</p>

## Findings

PASS



100 addresses are set aside for VPN users (100 user license for SecureClient is installed).



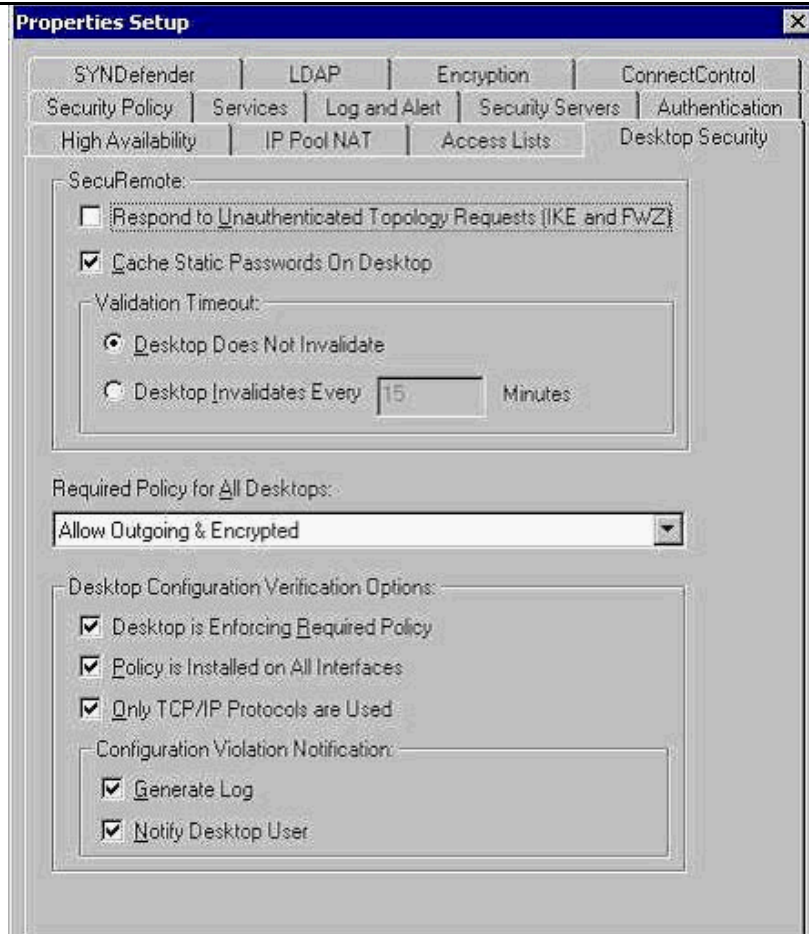
The log file shows my test VPN connection being assigned a translated source address (XlateSrc) of 172.x.x.144 which is part of the NAT pool range.

Audit Step 6	Test 4 VPN Access
Control Objective	The VPN Gateway's rule configuration and properties configuration must allow only encrypted access by authenticated users.
Testing	<p>Check for the existence of rules that have the Action 'Client Encrypt' look for valid destinations to test access to.</p> <p>These VPN rules should be the first rules in the rulebase.</p> <p>Attempt to ping a resource with and without an authenticated VPN connection.</p> <p>Under the Desktop Security Tab of the Firewall Properties page The option to 'Respond to Unauthenticated Topology Requests' should be unchecked.</p> <p>Attempt to setup a client without using a known account to see what information can be acquired (topology download).</p>

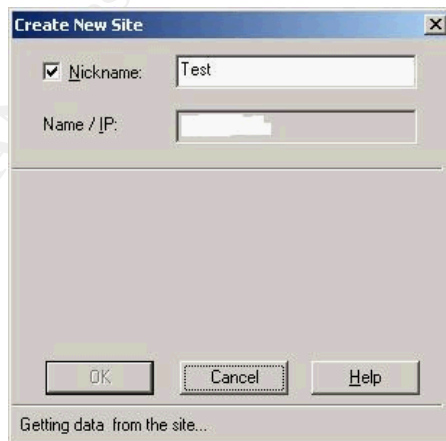


## Findings

PASS



Configuration of server does not allow a user to obtain the topology without authenticating.



Attempt to create a new site and download the Topology...



Topology is not transferred – instead the VPN Login screen is presented.

Results of PING test from authenticated VPN client:

```
C:\>ping InternalServer
```

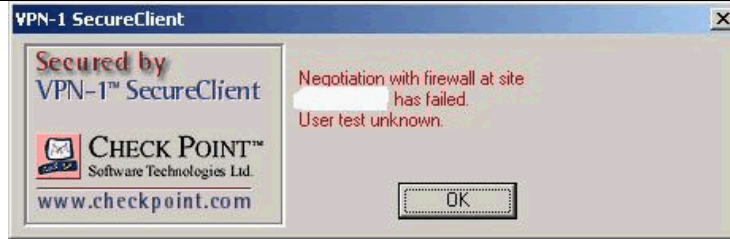
Pinging InternalServer [172.x.x.x] with 32 bytes of data:

```
Reply from 172.x.x.x: bytes=32 time=301ms TTL=127
Reply from 172.x.x.x: bytes=32 time=20ms TTL=127
Reply from 172.x.x.x: bytes=32 time=50ms TTL=127
Reply from 172.x.x.x: bytes=32 time=40ms TTL=127
```

Ping statistics for 172.x.x.x:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 20ms, Maximum = 301ms, Average = 102ms

Results of PING test from un-authenticated VPN client:



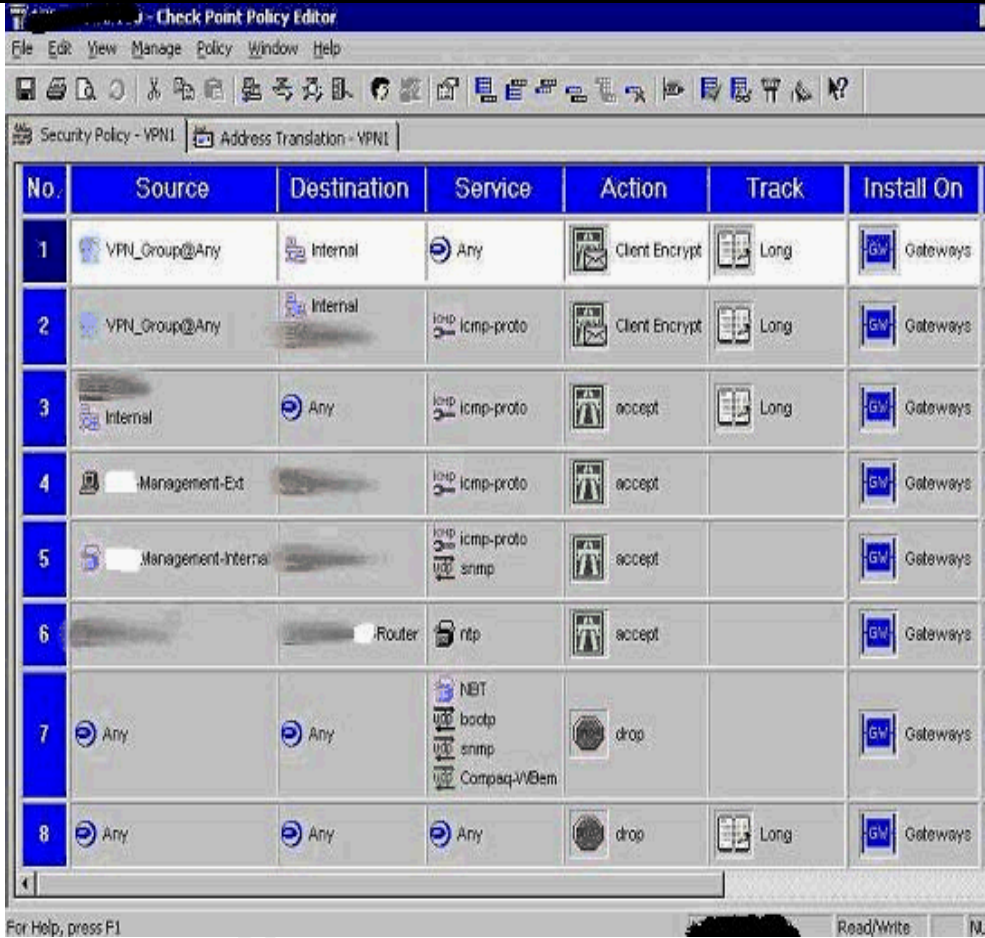
C:\>ping InternalServer

Pinging InternalServer [172.x.x.x] with 32 bytes of data:

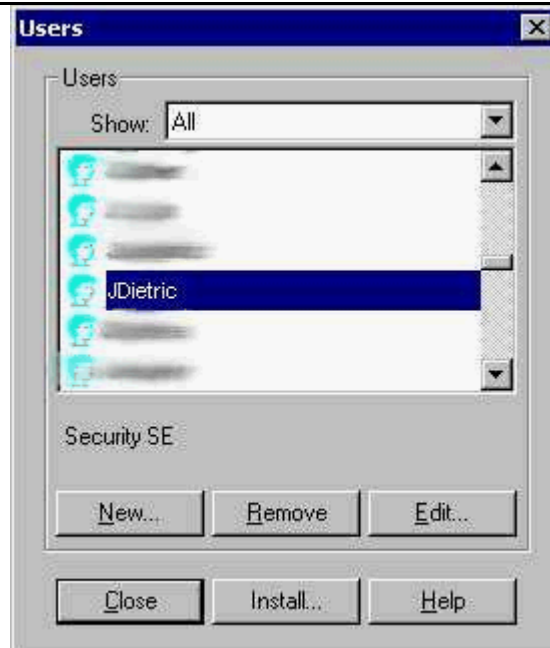
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.

Ping statistics for 172.x.x.x:

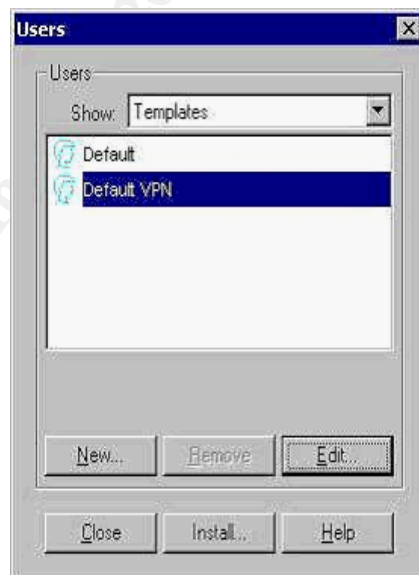
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms

	 <p>Client Encrypt rules are at the top of the rulebase and limit the source to the VPN user group.</p>
--	--

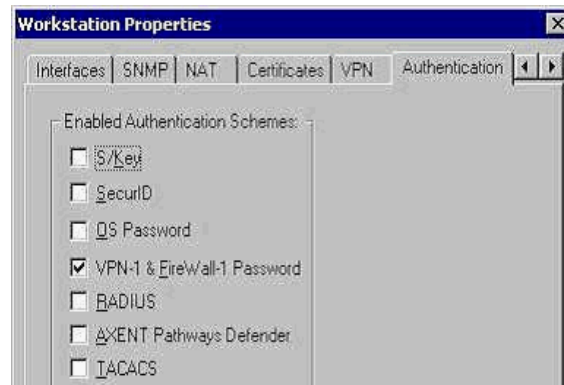
Audit Step 8	Test 5 VPN User Account Management
Control Objective	Proper account management procedures must be in place to ensure appropriate VPN access is granted.
Testing	List current users allowed VPN access (Manage->Users in the Policy Editor). By comparing the CheckPoint User Database against the Windows 2000 Domain user database, accounts in the CheckPoint database but not in the Windows 2000 database are suspect. HR needs to confirm status of users . Look for policy to support account creation/removal.
Findings	
FAIL	



Active accounts discovered that belong to fired employees. Only users with valid Corporate Windows 2000 Domain accounts should have a CheckPoint VPN account created. By comparing the CheckPoint User Database against the Windows 2000 Domain, the accounts that were in the CheckPoint database but not in the Windows 2000 database were suspect and confirmed to be terminated employees by HR.



Use of templates to create users.



Only VPN-1 accounts being used which de-centralizes account management which is bad.





Accounts are valid 24 hours a day



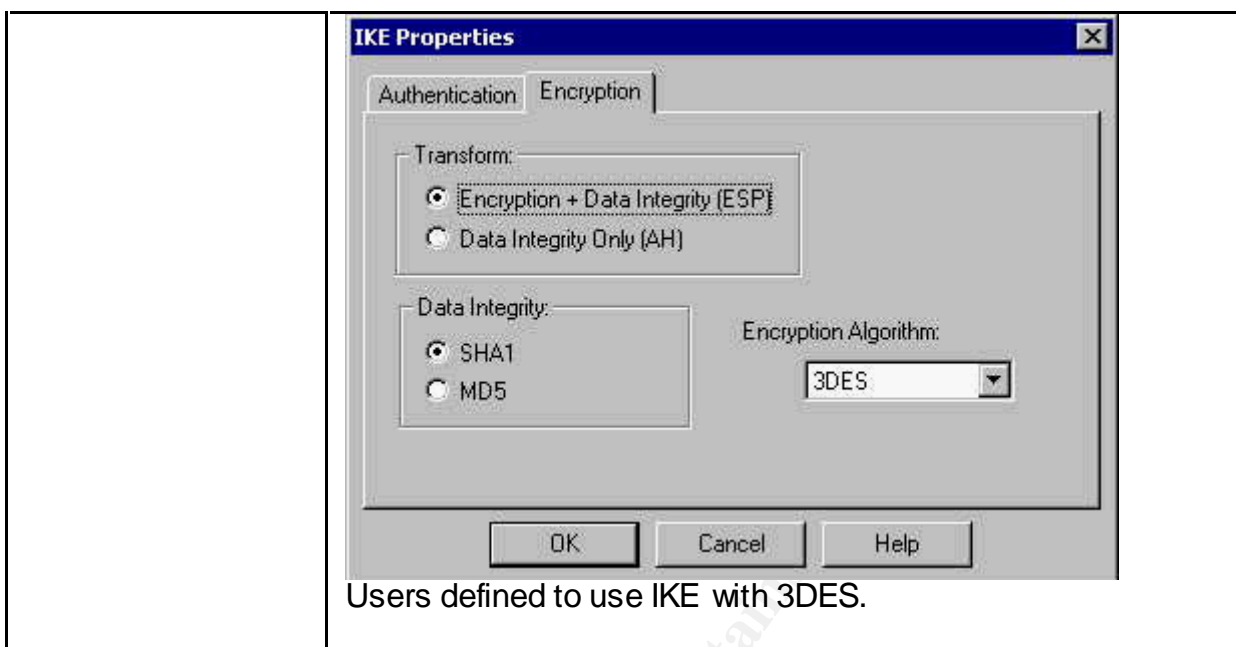
All accounts can go to/from anywhere.



Lack of token-based authentication. No policy governing password creation and maintenance.







Audit Step 15	Test 6 Encryption
Control Objective	Appropriate encryption level and settings must be in use for VPN connections
Testing	On the VPN client, confirm Tools->Encryption Scheme has IPSec selected. Check the VPN properties of the Firewall object and edit the IKE settings. Review the CheckPoint log to verify that the setup of the VPN connection uses 3DES IPSEC. If possible, capture VPN traffic with a packet sniffer to confirm that it is indeed encrypted.

## Findings

Pass

Check Point Log Viewer - [fw.log]

File Edit View Select Window Help

Log

Product	Info.
VPN...	scheme: IKE methods: Combined ESP, 3DES + SHA1
VPN...	scheme: IKE methods: Combined ESP, 3DES + SHA1
VPN...	len 328
VPN...	len 328
VPN...	reason: Client Encryption: Authenticated by Pre-shared secret scheme: IKE methods: 3DES, IKE, SHA1
VPN...	IKE Log: Phase 1 [TCP] completion: 3DES/SHA1/Pre shared secrets Negotiation ID: a0645115ee40f0c4-255599aeb51740d5
VPN...	scheme: IKE methods: Combined ESP, 3DES + SHA1 (phase 2 completion) for host: 192.1 and for subnet: 0.0.0.0 (mask= 0.0.0.0)
VPN...	reason: unknown established TCP packet
VPN...	len 48
VPN...	scheme: IKE methods: Combined ESP, 3DES + SHA1
VPN...	scheme: IKE methods: Combined ESP, 3DES + SHA1
VPN...	scheme: IKE methods: Combined ESP, 3DES + SHA1
VPN...	scheme: IKE methods: Combined ESP, 3DES + SHA1
VPN...	scheme: IKE methods: Combined ESP, 3DES + SHA1
VPN...	len 104
VPN...	len 69
VPN...	scheme: IKE methods: Combined ESP, 3DES + SHA1
VPN...	scheme: IKE methods: Combined ESP, 3DES + SHA1
VPN...	scheme: IKE methods: Combined ESP, 3DES + SHA1
VPN...	scheme: IKE methods: Combined ESP, 3DES + SHA1
VPN...	scheme: IKE methods: Combined ESP, 3DES + SHA1
VPN...	scheme: IKE methods: Combined ESP, 3DES + SHA1

For Help, press F1

logview.fw 172 NUM

172 Check Point Log Viewer - [fw.log]

File Edit View Select Window Help

Log

Type	Action	Service	Source	Destination	Proto.	Rule	S_Port	User	SrcKeyID	DstKeyID
log	key install				ip	0			0x3312c734	0x3544
log	drop	domain-udp	172.1		udp	8	1075			
log	decrypt	nbdetagram	192.1	172.1	udp	1	nbdetagram	J.Dietric	0x3312c734	
log	drop	bootpc	172.1	255.255.255.255	udp	8	bootpc			
log	drop	bootpc	172.1	255.255.255.255	udp	8	bootpc			
log	decrypt	nbdetagram	192.1	172.1	udp	1	nbdetagram	J.Dietric	0x3312c734	
log	decrypt	nbdetagram	192.1	172.1	udp	1	nbdetagram	J.Dietric	0x3312c734	
log	drop	14000	172.1	255.255.255.255	udp	8	14000			
log	drop	domain-udp	172.1		udp	8	1075			
log	decrypt	nbdetagram	192.1	172.1	udp	1	nbdetagram	J.Dietric	0x3312c734	
log	decrypt	nbdetagram	192.1	172.1	udp	1	nbdetagram	J.Dietric	0x3312c734	
log	decrypt	nbdetagram	192.1	172.1	udp	1	nbdetagram	J.Dietric	0x3312c734	
log	decrypt	domain-udp	192.1	172.1	udp	1	3622	J.Dietric	0x3312c734	
log	decrypt	1026	192.1	172.1	tcp	1	3623	J.Dietric	0x3312c734	
log	decrypt	1026	192.1	172.1	tcp	1	3625	J.Dietric	0x3312c734	
log	drop	bootpc	172.1	255.255.255.255	udp	8	bootpc			
log	drop	bootpc	172.1	255.255.255.255	udp	8	bootpc			
log	drop	domain-udp	172.1		udp	8	1075			
log	drop	bootpc	172.1	255.255.255.255	udp	8	bootpc			
log	drop	bootpc	172.1	255.255.255.255	udp	8	bootpc			
log	drop	domain-udp	172.1		udp	8	1075			
log	drop	14000	172.1	255.255.255.255	udp	8	14000			

For Help, press F1

logview.fw 172 NUM

172.16.1.1 - Check Point Log Viewer - [fw.log]

File Edit View Select Window Help

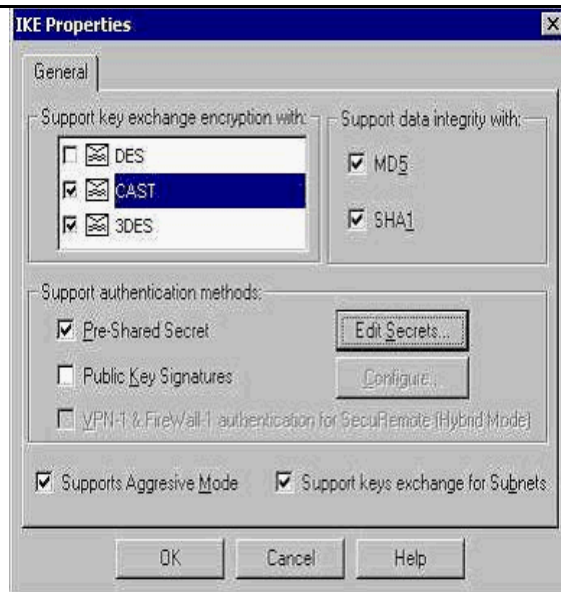
Log

XlateSrc	XlateDst	XlateS..	XlateD..	Product	Info.
172.16.1.1	172.16.1.1	1075	domain-udp	VPN-1 & FireWall-1	scheme: IKE methods: Combined ESP, 3DES
172.16.1.1	172.16.1.1	nbdatagram	nbdatagram	VPN-1 & FireWall-1	len 60
172.16.1.1	172.16.1.1	nbdatagram	nbdatagram	VPN-1 & FireWall-1	scheme: IKE methods: Combined ESP, 3DES
172.16.1.1	172.16.1.1	nbdatagram	nbdatagram	VPN-1 & FireWall-1	len 328
172.16.1.1	172.16.1.1	nbdatagram	nbdatagram	VPN-1 & FireWall-1	len 328
172.16.1.1	172.16.1.1	nbdatagram	nbdatagram	VPN-1 & FireWall-1	scheme: IKE methods: Combined ESP, 3DES
172.16.1.1	172.16.1.1	nbdatagram	nbdatagram	VPN-1 & FireWall-1	scheme: IKE methods: Combined ESP, 3DES
172.16.1.1	172.16.1.1	nbdatagram	nbdatagram	VPN-1 & FireWall-1	len 104
172.16.1.1	172.16.1.1	1075	domain-udp	VPN-1 & FireWall-1	len 69
172.16.1.1	172.16.1.1	nbdatagram	nbdatagram	VPN-1 & FireWall-1	scheme: IKE methods: Combined ESP, 3DES
172.16.1.1	172.16.1.1	nbdatagram	nbdatagram	VPN-1 & FireWall-1	scheme: IKE methods: Combined ESP, 3DES
172.16.1.1	172.16.1.1	nbdatagram	nbdatagram	VPN-1 & FireWall-1	scheme: IKE methods: Combined ESP, 3DES
172.16.1.1	172.16.1.1	3622	domain-udp	VPN-1 & FireWall-1	scheme: IKE methods: Combined ESP, 3DES
172.16.1.1	172.16.1.1	3623	1026	VPN-1 & FireWall-1	scheme: IKE methods: Combined ESP, 3DES
172.16.1.1	172.16.1.1	3625	1026	VPN-1 & FireWall-1	scheme: IKE methods: Combined ESP, 3DES
172.16.1.1	172.16.1.1	nbdatagram	nbdatagram	VPN-1 & FireWall-1	len 328
172.16.1.1	172.16.1.1	nbdatagram	nbdatagram	VPN-1 & FireWall-1	len 328
172.16.1.1	172.16.1.1	1075	domain-udp	VPN-1 & FireWall-1	len 60
172.16.1.1	172.16.1.1	nbdatagram	nbdatagram	VPN-1 & FireWall-1	len 328
172.16.1.1	172.16.1.1	nbdatagram	nbdatagram	VPN-1 & FireWall-1	len 328
172.16.1.1	172.16.1.1	1075	domain-udp	VPN-1 & FireWall-1	len 69
172.16.1.1	172.16.1.1	nbdatagram	nbdatagram	VPN-1 & FireWall-1	len 104

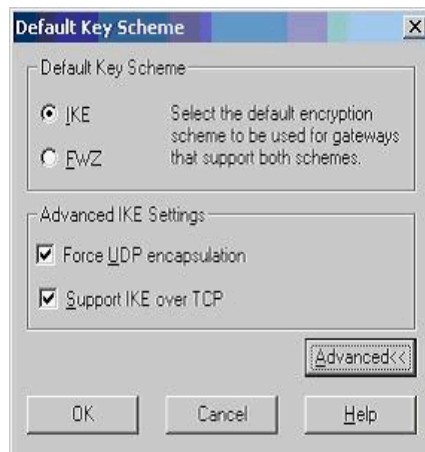
For Help, press F1

logview.fw

Log Files confirm proper encryption in use during a VPN session.



On the VPN-1 Gateway 3DES is supported



The VPN client is using IKE

Audit Step 17	Test 7 Personal Firewall
Control Objective	The VPN client's personal Firewall settings must be enforced



Encrypted

C:\>ping 172.x.x.x

Pinging 172.x.x.x with 32 bytes of data:

Reply from 172.x.x.x: bytes=32 time=120ms TTL=128

Reply from 172.x.x.x: bytes=32 time=10ms TTL=128

Reply from 172.x.x.x: bytes=32 time=80ms TTL=128

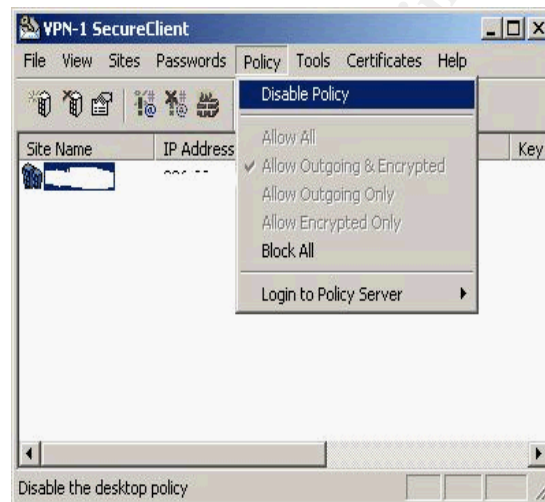
Reply from 172.x.x.x: bytes=32 time=20ms TTL=128

Ping statistics for 172.x.x.x:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 10ms, Maximum = 120ms, Average = 57ms



Disable policy on desktop and try PING again.

C:\>ping 172.x.x.x

Pinging 172.x.x.x with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 172.x.x.x:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),



	<p>Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</p> <p>Without Policy, VPN connection not allowed.</p>
--	--

Audit Step 7	Test 8 Operating System Hardening																																																																																																																																		
Control Objective	The VPN Gateway's operating system must be hardened and maintained to prevent system compromises.																																																																																																																																		
Testing	Run the Netstat -an command. Run IPCONFIG /ALL command. List all Services from Control Panel -> Services. Request server build documentation look for standards (NT security templates used etc).																																																																																																																																		
Findings	Services Started or Disabled (from Administrative Tools -> Services): <table><tr><th>Name</th><th>Description</th><th>Status</th><th>Startup Type</th><th>Log On As</th></tr><tr><td colspan="5">-----Services that are Disabled or Manual -----</td></tr><tr><td>Alerter</td><td>Notifies selected users and computers of administrative alerts.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Application Management</td><td>Provides software installation services such as Assign, Publish, and Remove.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>ClipBook</td><td>Supports ClipBook Viewer, which allows pages to be seen by remote ClipBooks.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Compaq System Shutdown Service</td><td>Shuts down the system in the event of overheating or loss of cooling in response to commands from the Compaq Integrated System Management Controller driver.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Computer Browser</td><td>Maintains an up-to-date list of computers on your network and supplies the list to programs that request it.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>DHCP Client</td><td>Manages network configuration by registering and updating IP addresses and DNS names.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Distributed File System</td><td>Manages logical volumes distributed across a local or wide area network.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Distributed Link Tracking Client</td><td>Sends notifications of files moving between NTFS volumes in a network domain.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Distributed Link Tracking Server</td><td>Stores information so that files moved between volumes can be tracked for each volume in the domain.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Distributed Transaction Coordinator</td><td>Coordinates transactions that are distributed across two or more databases, message queues, file systems, or other transaction protected resource managers.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Fax Service</td><td>Helps you send and receive faxes.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>File Replication</td><td>Maintains file synchronization of file directory contents among multiple servers.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Indexing Service</td><td>Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Internet Connection Sharing</td><td>Provides network address translation, addressing, and name resolution services for all computers on your home network through a dial-up connection.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Intersite Messaging</td><td>Allows sending and receiving messages between Windows Advanced Server sites.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>IPSEC Policy Agent</td><td>Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Kerberos Key Distribution Center</td><td>Generates session keys and grants service tickets for mutual client/server authentication.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>License Logging Service</td><td></td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Logical Disk Manager Administrative Service</td><td>Administrative service for disk management requests.</td><td>Manual</td><td>LocalSystem</td><td></td></tr><tr><td>Messenger</td><td>Sends and receives messages transmitted by administrators or by the Alerter service.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Net Logon</td><td>Supports pass-through authentication of account logon events for computers in a domain.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>NetMeeting Remote Desktop Sharing</td><td>Allows authorized people to remotely access your Windows desktop using NetMeeting.</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Network DDE</td><td>Provides network transport and security for dynamic data exchange (DDE).</td><td>Disabled</td><td>LocalSystem</td><td></td></tr><tr><td>Network DDE DSDM</td><td>Manages shared dynamic data exchange and is used by Network DDE.</td><td>Manual</td><td>LocalSystem</td><td></td></tr></table>	Name	Description	Status	Startup Type	Log On As	-----Services that are Disabled or Manual -----					Alerter	Notifies selected users and computers of administrative alerts.	Disabled	LocalSystem		Application Management	Provides software installation services such as Assign, Publish, and Remove.	Disabled	LocalSystem		ClipBook	Supports ClipBook Viewer, which allows pages to be seen by remote ClipBooks.	Disabled	LocalSystem		Compaq System Shutdown Service	Shuts down the system in the event of overheating or loss of cooling in response to commands from the Compaq Integrated System Management Controller driver.	Disabled	LocalSystem		Computer Browser	Maintains an up-to-date list of computers on your network and supplies the list to programs that request it.	Disabled	LocalSystem		DHCP Client	Manages network configuration by registering and updating IP addresses and DNS names.	Disabled	LocalSystem		Distributed File System	Manages logical volumes distributed across a local or wide area network.	Disabled	LocalSystem		Distributed Link Tracking Client	Sends notifications of files moving between NTFS volumes in a network domain.	Disabled	LocalSystem		Distributed Link Tracking Server	Stores information so that files moved between volumes can be tracked for each volume in the domain.	Disabled	LocalSystem		Distributed Transaction Coordinator	Coordinates transactions that are distributed across two or more databases, message queues, file systems, or other transaction protected resource managers.	Disabled	LocalSystem		Fax Service	Helps you send and receive faxes.	Disabled	LocalSystem		File Replication	Maintains file synchronization of file directory contents among multiple servers.	Disabled	LocalSystem		Indexing Service	Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.	Disabled	LocalSystem		Internet Connection Sharing	Provides network address translation, addressing, and name resolution services for all computers on your home network through a dial-up connection.	Disabled	LocalSystem		Intersite Messaging	Allows sending and receiving messages between Windows Advanced Server sites.	Disabled	LocalSystem		IPSEC Policy Agent	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.	Disabled	LocalSystem		Kerberos Key Distribution Center	Generates session keys and grants service tickets for mutual client/server authentication.	Disabled	LocalSystem		License Logging Service		Disabled	LocalSystem		Logical Disk Manager Administrative Service	Administrative service for disk management requests.	Manual	LocalSystem		Messenger	Sends and receives messages transmitted by administrators or by the Alerter service.	Disabled	LocalSystem		Net Logon	Supports pass-through authentication of account logon events for computers in a domain.	Disabled	LocalSystem		NetMeeting Remote Desktop Sharing	Allows authorized people to remotely access your Windows desktop using NetMeeting.	Disabled	LocalSystem		Network DDE	Provides network transport and security for dynamic data exchange (DDE).	Disabled	LocalSystem		Network DDE DSDM	Manages shared dynamic data exchange and is used by Network DDE.	Manual	LocalSystem	
Name	Description	Status	Startup Type	Log On As																																																																																																																															
-----Services that are Disabled or Manual -----																																																																																																																																			
Alerter	Notifies selected users and computers of administrative alerts.	Disabled	LocalSystem																																																																																																																																
Application Management	Provides software installation services such as Assign, Publish, and Remove.	Disabled	LocalSystem																																																																																																																																
ClipBook	Supports ClipBook Viewer, which allows pages to be seen by remote ClipBooks.	Disabled	LocalSystem																																																																																																																																
Compaq System Shutdown Service	Shuts down the system in the event of overheating or loss of cooling in response to commands from the Compaq Integrated System Management Controller driver.	Disabled	LocalSystem																																																																																																																																
Computer Browser	Maintains an up-to-date list of computers on your network and supplies the list to programs that request it.	Disabled	LocalSystem																																																																																																																																
DHCP Client	Manages network configuration by registering and updating IP addresses and DNS names.	Disabled	LocalSystem																																																																																																																																
Distributed File System	Manages logical volumes distributed across a local or wide area network.	Disabled	LocalSystem																																																																																																																																
Distributed Link Tracking Client	Sends notifications of files moving between NTFS volumes in a network domain.	Disabled	LocalSystem																																																																																																																																
Distributed Link Tracking Server	Stores information so that files moved between volumes can be tracked for each volume in the domain.	Disabled	LocalSystem																																																																																																																																
Distributed Transaction Coordinator	Coordinates transactions that are distributed across two or more databases, message queues, file systems, or other transaction protected resource managers.	Disabled	LocalSystem																																																																																																																																
Fax Service	Helps you send and receive faxes.	Disabled	LocalSystem																																																																																																																																
File Replication	Maintains file synchronization of file directory contents among multiple servers.	Disabled	LocalSystem																																																																																																																																
Indexing Service	Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.	Disabled	LocalSystem																																																																																																																																
Internet Connection Sharing	Provides network address translation, addressing, and name resolution services for all computers on your home network through a dial-up connection.	Disabled	LocalSystem																																																																																																																																
Intersite Messaging	Allows sending and receiving messages between Windows Advanced Server sites.	Disabled	LocalSystem																																																																																																																																
IPSEC Policy Agent	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.	Disabled	LocalSystem																																																																																																																																
Kerberos Key Distribution Center	Generates session keys and grants service tickets for mutual client/server authentication.	Disabled	LocalSystem																																																																																																																																
License Logging Service		Disabled	LocalSystem																																																																																																																																
Logical Disk Manager Administrative Service	Administrative service for disk management requests.	Manual	LocalSystem																																																																																																																																
Messenger	Sends and receives messages transmitted by administrators or by the Alerter service.	Disabled	LocalSystem																																																																																																																																
Net Logon	Supports pass-through authentication of account logon events for computers in a domain.	Disabled	LocalSystem																																																																																																																																
NetMeeting Remote Desktop Sharing	Allows authorized people to remotely access your Windows desktop using NetMeeting.	Disabled	LocalSystem																																																																																																																																
Network DDE	Provides network transport and security for dynamic data exchange (DDE).	Disabled	LocalSystem																																																																																																																																
Network DDE DSDM	Manages shared dynamic data exchange and is used by Network DDE.	Manual	LocalSystem																																																																																																																																

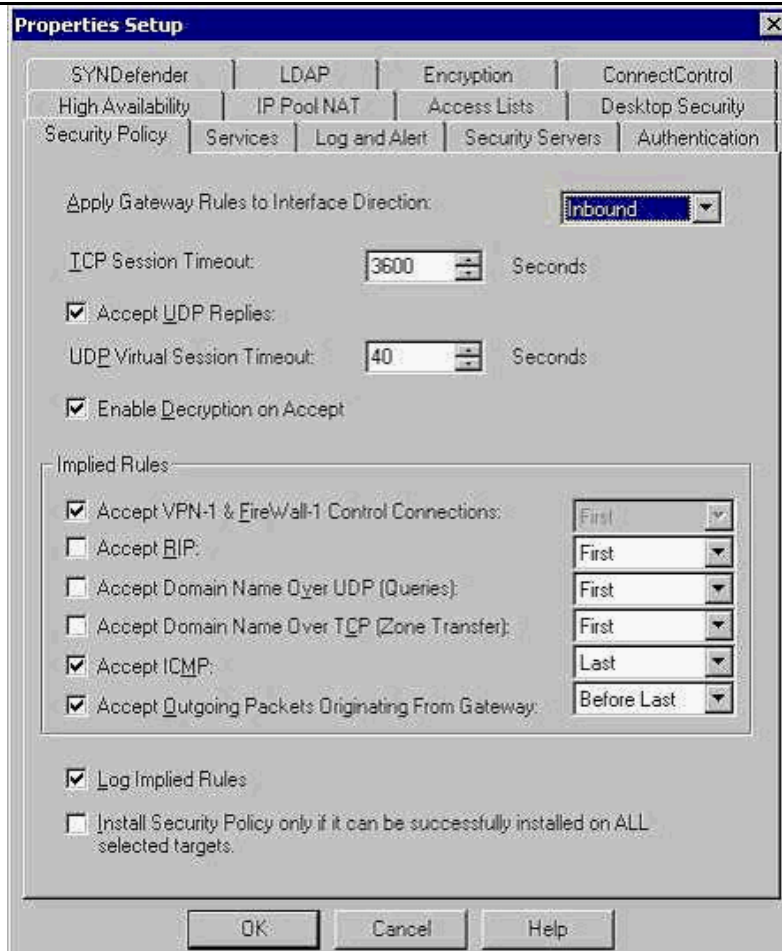
NT LM Security Support Provider	Provides security to remote procedure call (RPC) programs that use transports other than named pipes.	Disabled	LocalSystem
Performance Logs and Alerts	Configures performance logs and alerts.	Manual	LocalSystem
Print Spooler	Loads files to memory for later printing.	Disabled	LocalSystem
QoS RSVP	Provides network signaling and local traffic control setup functionality for QoS-aware programs and control applets.	Disabled	LocalSystem
Remote Access Auto Connection Manager	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.	Disabled	LocalSystem
Remote Access Connection Manager	Creates a network connection.	Disabled	LocalSystem
Remote Procedure Call (RPC) Locator	Manages the RPC name service database.	Manual	
Remote Registry Service	Allows remote registry manipulation.	Disabled	LocalSystem
Routing and Remote Access	Offers routing services to businesses in local area and wide area network environments.	Disabled	LocalSystem
RunAs Service	Enables starting processes under alternate credentials	Disabled	LocalSystem
Server	Provides RPC support and file, print, and named pipe sharing.	Disabled	LocalSystem
Smart Card	Manages and controls access to a smart card inserted into a smart card reader attached to the computer.	Disabled	LocalSystem
Smart Card Helper	Provides support for legacy smart card readers attached to the computer.	Disabled	LocalSystem
SNMP Trap Service	Receives trap messages generated by local or remote SNMP agents and forwards the messages to SNMP management programs running on this computer.	Manual	LocalSystem
TCP/IP NetBIOS Helper Service	Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.	Disabled	LocalSystem
Telephony	Provides Telephony API (TAPI) support for programs that control telephony devices and IP based voice connections on the local computer and, through the LAN, on servers that are also running the service.	Disabled	LocalSystem
Telnet	Allows a remote user to log on to the system and run console programs using the command line.	Disabled	LocalSystem
Terminal Services	Provides a multisession environment that allows client devices to access a virtual Windows 2000 Professional desktop session and Windows-based programs running on the server.	Disabled	
Uninterruptible Power Supply	Manages an uninterruptible power supply (UPS) connected to the computer.	Disabled	LocalSystem
Utility Manager	Starts and configures accessibility tools from one window	Disabled	
Windows Installer	Installs, repairs and removes software according to instructions contained in .MSI files.	Disabled	LocalSystem
Windows Management Instrumentation	Provides system management information.	Manual	
Workstation	Provides network connections and communications.	Disabled	LocalSystem
-----Services that are Started -----			
Check Point ELA Proxy		Started	Automatic LocalSystem
Check Point VPN-1 / FireWall-1		Started	Automatic LocalSystem
COM+ Event System	Provides automatic distribution of events to subscribing COM components.	Started	
Compaq Foundation Agents	Compaq Foundation Agents	Started	Automatic LocalSystem
Compaq NIC Agents	Compaq NIC Agents	Started	Automatic LocalSystem
Compaq Remote Monitor Service		Started	Automatic LocalSystem
Compaq Storage Agents	Compaq Storage Agents	Started	Automatic LocalSystem
DNS Client	Resolves and caches Domain Name System (DNS) names.	Started	Automatic LocalSystem
Event Log	Logs event messages issued by programs and Windows. Event Log reports contain information that can be useful in diagnosing problems. Reports are viewed in Event Viewer.	Started	Automatic LocalSystem
Event Log Watch		Started	Automatic LocalSystem
Logical Disk Manager	Logical Disk Manager Watchdog Service	Started	Automatic LocalSystem
Network Connections	Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.	Started	Manual LocalSystem
Plug and Play	Manages device installation and configuration and notifies programs of device changes.	Started	Automatic LocalSystem
Protected Storage	Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services, processes, or users.	Started	Automatic LocalSystem
Remote Procedure Call (RPC)	Provides the endpoint mapper and other miscellaneous RPC services.	Started	Automatic LocalSystem
Removable Storage	Manages removable media, drives, and libraries.	Started	Automatic LocalSystem
Security Accounts Manager	Stores security information for local user accounts.	Started	Automatic LocalSystem
SNMP Service	Includes agents that monitor the activity in network devices and report to the network console		



	<p>workstation. Started Automatic LocalSystem</p> <p>System Event Notification Tracks system events such as Windows logon, network, and power events. Started Automatic LocalSystem</p> <p>Notifies COM+ Event System subscribers of these events. Started Automatic LocalSystem</p> <p>Task Scheduler Enables a program to run at a designated time. Started Automatic LocalSystem</p> <p>Windows Management Instrumentation Driver Extensions Provides systems management information to and from drivers. Started Automatic LocalSystem</p> <p>Windows Time Sets the computer clock. Started Automatic LocalSystem</p> <p><b>Results of fscan (fscan x.x.x.x -bp 1-65535) issued from the Internet against the external address of the VPN-1 Server shows only CheckPoint Services - VPN ports open.</b></p> <p>Scan started at Tue Dec 8 01:20:47 2002</p> <p>x.x.x.x 264/tcp</p> <p>x.x.x.x 265/tcp</p> <p>x.x.x.x 500/tcp</p> <p><b>Results of 'ipconfig /all' command issued on the VPN-1 Server:</b></p> <p>Windows 2000 IP Configuration</p> <p>Host Name . . . . . : acme</p> <p>Primary DNS Suffix . . . . . :</p> <p>Node Type . . . . . : Hybrid</p> <p>IP Routing Enabled. . . . . : Yes</p> <p>WINS Proxy Enabled. . . . . : No</p> <p>Ethernet adapter Internal:</p> <p>Connection-specific DNS Suffix . : </p> <p>Description . . . . . : 3Com EtherLink XL 10/100 PCITX NIC (3C905B-TX)</p> <p>Physical Address. . . . . : 00-10-4B-xx-xx-AC</p> <p>DHCP Enabled. . . . . : No</p> <p>IP Address. . . . . : 172.x.x.x</p> <p>Subnet Mask . . . . . : 255.x.x.x</p> <p>Default Gateway . . . . . :</p> <p>DNS Servers . . . . . : 172.x.x.x</p> <p>172.x.x.x</p> <p>Primary WINS Server . . . . . : 172.x.x.x</p> <p>Secondary WINS Server . . . . . : 172.x.x.x</p> <p>Ethernet adapter External:</p> <p>Connection-specific DNS Suffix . : </p> <p>Description . . . . . : Compaq NC3120 Fast Ethernet NIC</p> <p>Physical Address. . . . . : 00-80-5F-xx-xx-98</p> <p>DHCP Enabled. . . . . : No</p> <p>IP Address. . . . . : 2.x.x.x</p> <p>Subnet Mask . . . . . : 255.255.255.0</p> <p>Default Gateway . . . . . : 2.x.x.x</p> <p>DNS Servers . . . . . : 2.x.x.x</p> <p>2.x.x.x</p>
--	---

Audit Step 5	Test 9. Firewall Rule base
Control Objective	Functionality of the VPN Gateway's Firewall settings must be configured appropriately and simply to block all non-VPN traffic.
Testing	<ul style="list-style-type: none"> <li>Review the rule base and Firewall Properties page for mis-configuration and complexity. Only VPN related rules should be necessary.</li> <li>Check against corporate security policy.</li> <li>Scan Firewall for open ports (using a tool like Fscan) – look for</li> </ul>

	<p>non-VPN related open ports.</p> <p>Attempt to use the VPN-1 server as an outbound gateway from an internal workstation by setting the default gateway to be the internal address of the VPN-1 server.</p>
Findings	
PASS	



ICMP should not be enabled and an explicit rule for control connections should be created. Consider adding a 'stealth rule' to drop or reject any non-VPN traffic directed to the VPN-1 Gateway directly.

Results of fscan show VPN ports open.

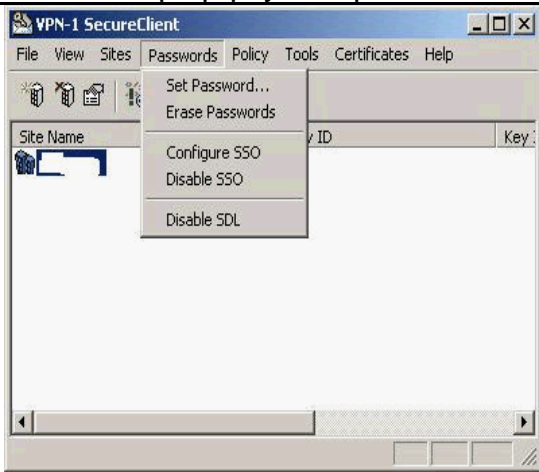
Scan started at Tue Dec 8 01:20:47 2002

x.x.x.x 264/tcp

x.x.x.x 265/tcp

x.x.x.x 500/tcp

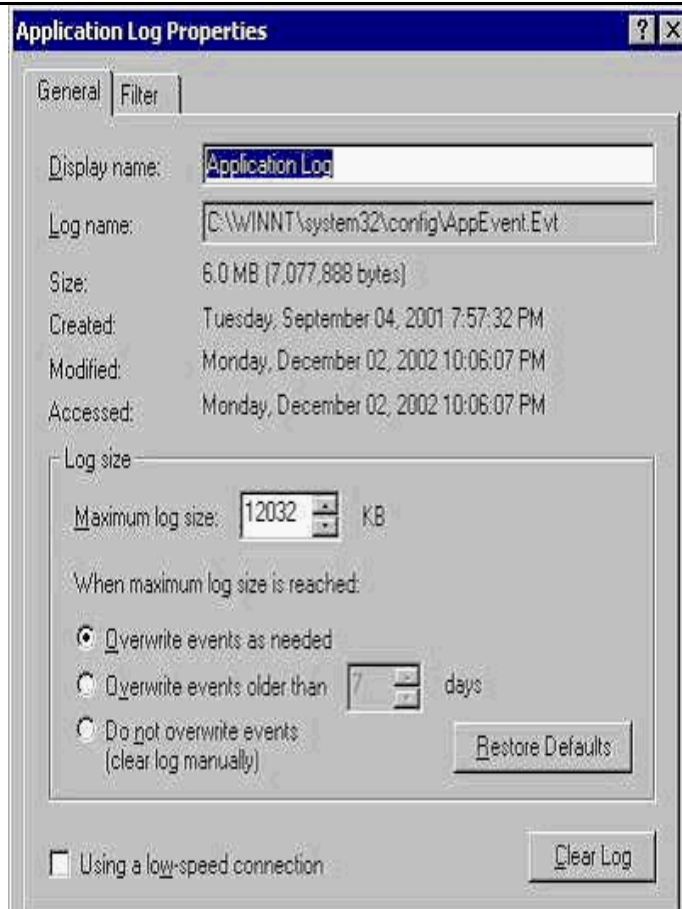
Audit Step 11.	Test 10 Laptop physical protection
Control Objective	Mobile user's laptops must be protected from theft or data loss.
Testing	Look for corporate policy guidelines; inspect a laptop by booting it up. Is a BIOS password enabled? Does the Windows Operating System auto-login? Under the Passwords option in the SecureClient VPN software is Single Sign On Configured and enabled?

Audit Step 11.	Test 10 Laptop physical protection
Findings	 <p>Single Sign On is enabled.</p> <p>Not BIOS power-on password set.</p> <p>Last logon name and domain displayed when logging into laptop.</p>
FAIL	

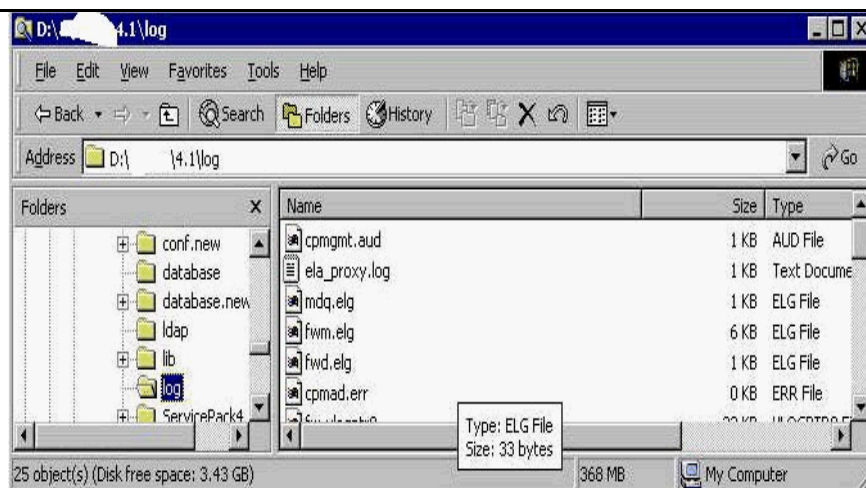
Audit Step 10	Test11 Log Settings
Control Objective	VPN traffic must be logged and logs must be maintained and reviewed.
Testing	<p>Inspect the rules to see where logging is enabled.</p> <p>Confirm that all implied rules are logged under the Security Policy tab of the Policy Properties in the Policy Editor.</p> <p>Generate traffic to match each rule to see that it is logged.</p> <p>For Client Encrypt rules, use the VPN Client and attempt to access internal resources. For the Drop ALL rule, use Ping and Telnet to try to connect to an internal resource.</p> <p>Run the AT command to see if the CheckPoint logswitch command is scheduled to run in order to roll the log. Ask for a high-level report.</p> <p>On the client, temporary log files can be made by creating Fwenc.log for tracking SecuRemote actions and Sr.log for tracking packets blocked by SecureClient Policy.</p>

## Findings

PASS



Windows 2000 logs are set to 12 MB each to allow for reasonable growth.



VPN-1 Server Log directory has adequate free space (3.43 GB).

Check Point Log Viewer - [fw.log]

	Time	Inter.	Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S...
2	19:29:04	EL9...		log	drop	14000	172.	255.255.255.255	udp	8	1
2	19:30:21	EL9...		log	drop	domain-udp	172.		udp	8	1
2	19:31:47	N10...		log	drop	1026	192.	172.1	tcp	0	2
2	19:32:21			log	drop	domain-udp	172.		udp	8	1
2	19:33:14	N10...		log	drop	1026	192.	172.	tcp	0	2
2	19:34:04	EL9...		log	drop	14000	172.	255.255.255.255	udp	8	1
2	19:34:11	EL9...		log	drop	bootpc	172.	255.255.255.255	udp	8	b
2	19:34:11	EL9...		log	drop	bootpc	172.	255.255.255.255	udp	8	b
2	19:34:21	EL9...		log	drop	domain-udp	172.		udp	8	1
2	19:35:55	EL9...		log	drop	bootpc	172.	255.255.255.255	udp	8	b
2	19:35:55	EL9...		log	drop	bootpc	172.	255.255.255.255	udp	8	b
2	19:36:21	EL9...		log	drop	domain-udp	172.		udp	8	1
2	19:38:21	EL9...		log	drop	domain-udp	172.		udp	8	1
2	19:39:04	EL9...		log	drop	14000	172.	255.255.255.255	udp	8	1
2	19:40:21	EL9...		log	drop	domain-udp	172.		udp	8	1
2	19:41:43	EL9...		log	drop	bootpc	172.1	255.255.255.255	udp	8	b
2	19:41:43	EL9...		log	drop	bootpc	172.1F	255.255.255.255	udp	8	b
2	19:42:21	EL9...		log	drop	domain-udp	172.1		udp	8	1
2	19:43:16	EL9...		log	drop	bootpc	172.	255.255.255.255	udp	8	b
2	19:43:16	EL9...		log	drop	bootpc	172.	255.255.255.255	udp	8	b
2	19:44:04	EL9...		log	drop	14000	172.1	255.255.255.255	udp	8	1
2	19:44:21	EL9...		log	drop	domain-udp	172.1		udp	8	1



	<p>Search for dropped traffic in log to see matches on Rule 8</p> <p>fwenc.log file header from client machine:</p> <p>Running VPN-1 SecuRemote Version 4.1 SP-4 3DES Build number: 4185; Windows 2000 version Using Entrust Toolkit version: EntrustIPSec Negotiator(tm) Toolkit 5.1.100.361 SDL enabled SSO enabled</p> <p>AT command shows no scheduled jobs. Manual log rotation is required – no documented procedure to ‘roll’ log.</p>
--	---

Audit Step 19	Test 12 VPN Design
Control Objective	The VPN Gateway must physically be located on the corporate infrastructure so as not to compromise security.
Testing	Review network diagram to look for alternate access points into the corporate network. Use Traceroute to confirm VPN traffic enters via the VPN-1 gateway. Confirm the range of NAT pool address is routed back to the VPN-1 Gateway on the internal network.
Findings  FAIL	<p>No good design justification for placing the VPN gateway in parallel with the corporate firewall (see figure 1). The Corporate Firewall should be protecting all network traffic. Network diagram was available but no policy document was available to support the current design.</p> <p>C:\&gt;tracert InternalHost</p> <p>Tracing route to InternalHost [172.x.x.x] over a maximum of 30 hops:</p> <pre> 1  30 ms  30 ms  30 ms  x.x.x.x (VPN Server) 2  30 ms  30 ms  10 ms  InternalHost [172.x.x.x]</pre> <p>Trace complete.</p> <p>Traceroute Indicates traffic entering the Corporate network via the VPN gateway.</p>

## ***Measure Residual Risk***

A good deal of residual risk exists with the VPN system as it exists today. Lack of policy and procedures coupled with out of date and unsupported software will lead to system compromise.

Test 1 revealed the use of shared administrative accounts that make accountability difficult to enforce. Access to the Server itself is too widespread allowing a user to modify their CheckPoint administrative privileges. This issue can be corrected by assigning all administrators unique accounts in both Windows and CheckPoint, limiting the number of users that can log onto the VPN-1 Windows server console. This change of procedure would have a minimal impact in terms of cost or additional resources.

Test 5 showed that because there is no policy governing VPN user account creation and deletion old user accounts continue to be active on the VPN-1 Server. This threat can be mitigated by synchronizing the account creation/removal process with the creation/removal of Windows Domain accounts. This change of procedure would have a minimal impact in terms of cost or additional resources.

Test 2 shows out of date software that is no longer covered under software maintenance or technical support. Given that CheckPoint will not be supporting or enhancing this version in the near future, the decision to upgrade or discontinue use needs to be made. As new security weaknesses are discovered, there will not be patches available. To correct this threat, a significant investment must be made in terms of cost and resources.

Test 10 revealed that mobile user's laptops are not protected from unauthorized access if they are stolen. To remedy this, procedures and guidelines need to be developed and communicated. This will consume some resources but go a long way to safeguarding company resources if a laptop with cached VPN credentials is compromised. The risk of theft, however, is very difficult to prevent.

Test 12 points out that the current network architecture that places the VPN server in parallel with the corporate firewall has no justification. A more secure solution would be to place the VPN server on the DMZ of the production Firewall. This will allow the corporate Firewall to inspect and log all VPN traffic after it is decrypted. It also removes a direct access point into the corporate network. To remediate this threat will take little cost but will result in downtime and the need for high-end resources.



Most of the control objectives were met to some extent but to correct all the problems discovered will take significant high-end resources and money. Given the other remote access methods in production at Acme Corporation, the question must be asked why the CheckPoint VPN needs to be left in production at all.

***Is the system auditable?***

The CheckPoint VPN-1 Gateway and client system is auditable by following the checklist outlined above. If there are additional requirements to audit CheckPoint internal communications or SecureClient interaction with the Windows 2000 TCP/IP stack then the checklist would have to be expanded to attempt to address these issues. In some cases, however, the only method to audit some manufacturer features would be inquiry. The more subjective areas of the audit involving corporate policy prove to be more difficult to audit since many procedures are not written down.

## **Assignment 4 – Audit Report or Risk Assessment**

### ***AUDIT REPORT - FOR INDEPENDENT AUDITORS***

#### ***Executive summary***

The audit of Acme Corporation's CheckPoint VPN-1 Gateway has revealed many vulnerabilities but many of them can be mitigated by taking simple and inexpensive steps. Two of the more costly and time consuming findings include: The technology in production today is not covered under maintenance and the location of the gateway on the network in parallel with the corporate firewall should be reconsidered.

Many procedural changes would go a long way to improving the security of the VPN solution in place today. Better account management is the most pressing need as many old accounts were discovered still active on the VPN gateway.

A review of the other Remote access solutions in place should occur to be sure security and business needs are being met by offering three different methods for remote users to retrieve email.

Most of the Audit Objectives were met. There were no audit steps that did not at least partially meet the objectives with the exception of the placement of the VPN server on the Network.

#### ***Audit findings***

Test 1 of assignment 3: FAIL: There is use of shared administrative accounts (accounts like 'Helpdesk' and AdminBackup as shown in the screen shots). Access to the Server itself is too widespread with many users sharing the AdminBackup password.

Test 2 of assignment 3: FAIL: shows out of date software that is no longer covered under software maintenance or technical support. Both the production server and client are not up to date with patches.

Test 3 of assignment 3: PASS: All 100 potential VPN users are able to get an address from the Network Address Translation Pool issued by the VPN server when the VPN session is established. The VPN User is logged with the Translated Source address.

Test 4 of assignment 3: PASS: VPN rules are configured according to CheckPoint best Practices by being located at the top of the rulebase and limited to a source of VPN users group. If the client does not authenticate with a valid

user account, the topology of the corporate site can not be downloaded from the server.

Test 5 of assignment 3: FAIL: Old user accounts continue to be active on the VPN-1 Server. Users are created with templates. No procedure governs creation/removal of accounts or selection of user passwords.

Test 6 of assignment 3: PASS: Clients use IKE with 3DES IPsec encryption to establish a VPN connection. The connection is logged by the VPN server and shows the method used. Shared secrets are used in place of Certificates.

Test 7 of assignment 3: PASS: The personal Firewall on the client has to be enabled in order for access to internal resources to be allowed. By disabling the desktop policy access to internal resources is not allowed.

Test 8 of assignment 3: PASS: The Windows operating system that the VPN-1 server has been installed on is hardened to at least the best practice standards offered by CheckPoint. The majority of services have been disabled including the Server and Workstation services. A port scan from the Internet reveals only 3 VPN ports open on the VPN server.

Test 9 of assignment 3: PASS: The VPN-1 Server is configured to only allow VPN traffic into/out of the corporate network with the exception of PING traffic. This is confirmed by a port scan.

Test 10 of assignment 3: FAIL: Mobile user's laptops are not protected from unauthorized access if they are stolen. Cached VPN credentials are used for Single sign on.

Test 11 of assignment 3: PASS: Logging is enabled correctly, there is no formal review process. Logs are used reactively not proactively. No job scheduled to roll the logs on a regular basis.

Test 12 of assignment 3: FAIL: The current network architecture that places the VPN server in parallel with the corporate firewall has no justification.

### ***Background/risk***

Test 1 of assignment 3: VPN administration procedures have risks to Acme Corporation in that there are shared accounts in use resulting in loss of accountability. Administrators can make changes without being tracked. The Windows accounts have administrative rights. The Helpdesk can log into Windows and then change the access rights on the CheckPoint accounts. They can then modify access and rules on the VPN Server. This could result in a total compromise of the internal network.

Test 2 of assignment 3: The lack of support and software maintenance is a growing risk as CheckPoint moves to 'end of life' version 4.1 within a year. A decision needs to be made to renew or abandon the product. As the system ages, new exploits can be discovered that will not have fixes. New functionality in the VPN client is not available without an upgrade.

Test 5 of assignment 3: Old user accounts continue to be active on the VPN-1 Server. Users are created with templates. No procedure governs creation/removal of accounts or selection of user passwords. VPN User account management has proved to be difficult because the VPN users are maintained in a local CheckPoint database. There are no procedures in place to clean up old or unused accounts. Therefore terminated employees still have access to the VPN system.

Test 10 of assignment 3: Mobile user's laptops are not protected from unauthorized access if they are stolen. Cached VPN credentials are used for Single sign on.

Test 11 of assignment 3: Although logging is enabled correctly, there is no formal review process. Logs are used reactively not proactively. No job scheduled to roll the logs on a regular basis. The log files can grow to a large size and be difficult to archive. These logs are one of the only ways to detect abuses of the VPN system since no other Intrusion detection system is in place.

Test 12 of assignment 3: The current network architecture that places the VPN server in parallel with the corporate firewall has no justification. The design of the VPN gateway is a risk in that rules created on the corporate firewall have no impact on VPN users. Keeping the Corporate firewall in sync with the VPN server might prove difficult. Hackers have two Gateways to try to attack instead of just one. A compromise in either one will result in penetration of the corporate network.

### ***Audit recommendations***

At the heart of many of the above risks is the lack of policy governing the administrator's actions. The creation of detailed policy would be a good first step. Identifying roles and responsibilities would also benefit the organization.

Test 1 of assignment 3: A procedure should be created that eliminates the convenient shared administrator accounts currently in use. Administrators should be accountable for all actions. Accounts on the VPN-1 Server at the Operating System level do not have to match those of the CheckPoint Administration GUI (i.e. there are too many users with Windows Console access).

Test 2 of assignment 3: Software maintenance and support should be budgeted for each year to keep critical servers covered. The ability to get upgrades and patches is critical. The need for technical support might not be as critical if there is in-house expertise.

Test 5 of assignment 3: A procedure that governs the creation/removal of VPN user accounts and selection of user passwords should be developed. VPN User account management has proved to be difficult because the VPN users are maintained in a local CheckPoint database. The use of a central database for users and / or the introduction of token / certificate based authentication would better control who can access the Acme corporate network via VPN.

Test 10 of assignment 3: A policy governing the use of Mobile user laptops should be developed to limit unauthorized access to the corporate network if they are stolen. The use of Cached VPN credentials used for Single sign on needs a business justification.

Test 11 of assignment 3: A log review process should be developed for all security devices at a minimum. Management level reports would help detect unauthorized users of the VPN system.

Test 12 of assignment 3: The current network architecture that places the VPN server in parallel with the corporate firewall has no justification. Acme Corporation should try to create a network design with a minimum of entry points from the Internet. The development of a review process before devices are placed on the production network would also help prevent the 'evolution' of insecure temporary solutions that become permanent.

### **Costs**

The big cost will be to pay for the lapsed support and maintenance of the CheckPoint software. Other costs will be measured in the amount of time it takes to adjust to new procedures.

Test 1 of assignment 3: This procedural change will have minimal impact on resources.

Test 2 of assignment 3: CheckPoint charges a fixed percentage of the cost of the software for maintenance and support. They will charge an additional fee for the lapse in coverage.

Test 5 of assignment 3: The procedural change will have minimal impact on resources. The move to token / certificate based authentication will involve significant effort and cost.

Test 10 of assignment 3: This procedural change will have minimal impact on resources.

Test 11 of assignment 3: The cost of reporting software or 'home-grown' code. Ongoing support and maintenance needs to be factored in.

Test 12 of assignment 3: The cost of redeploying the VPN server on a DMZ subnet protected by the corporate firewall will be small – just the labor to design and reconfigure and test. Ideally the mobile users will just have to update their VPN site information.

### ***Compensating controls***

If Acme Corporation does not want to pay to keep up with support on the VPN-1 gateway, one control that can easily be put in place is to position the VPN-1 gateway behind the corporate firewall. This will offer additional protection for the un-patched VPN-1 Gateway but it is not a long-term solution. In the long term, if the cost is too high to upgrade, the existing Citrix solution may prove to be a more secure and reliable solution.

## References

Ruangkrai, Rangsiphol *Checkpoint Firewall-1 Audit*,  
<http://www.giac.org/GSNA.php>

Nelson, Paul *Checkpoint Firewall-1 Audit* <http://www.giac.org/GSNA.php>

Strom, Dan *Auditing the Netscreen-5 Firewall Used as a VPN Gateway* August 16, 2001 <http://www.giac.org/GSNA.php>

Spitzner, Lance *Auditing Your Firewall Setup* December 12, 2000  
<http://www.spitzner.net/audit.html>

Tu, James *SANS GSNA – Practical Assignment* (Version 2.0) June 2002  
*Auditing a Nokia 440 Check Point Firewall-1 Firewall: An Auditor's Perspective*

Browne, Brian; Lewis, Cindy; Hamilton, Rich; Weaver Woody *Management Strategies Best Practices For VPN Implementation* March 2001 issue of *Business Communications Review*, pp. 24–30  
<http://www.bcr.com/bcmag/2001/03/p24.asp>

Gibbons, Ryan *VPN-1 SecureClient – Check Point's Solution for Secure Intranet Extension*, April 9, 2002 <http://rr.sans.org/encryption/securedclient.php>

Virtual Private Network Consortium <http://www.vpnc.org/>

British Standards Institution (as BS 7799)  
<http://www.bspsi.com/17799>

National Institute of Standards and Technology  
<http://csrc.nist.gov/publications/nistpubs/>

- SP 800-46 Security for Telecommuting and Broadband Communications, September 2002
- SP 800-47 Security Guide for Interconnecting Information Technology Systems, September 2002
- SP 800-41 Guidelines on Firewalls and Firewall Policy, January 2002
- SP 800-40 Procedures for Handling Security Patches, September 2002
- SP 800-43 Systems Administration Guidance for Windows 2000 Professional, November 2002

Wack, John; Cutler\*, Ken; Pole\*, Jamie *NIST Special Publication 800-41 C O M P U T E R S E C U R I T Y* January 2002 Guidelines on Firewalls and Firewall Policy Recommendations of the National Institute of Standards and Technology <http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf>

Request for Comments: 2196 - Site Security Handbook  
<http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2196.html>

*CheckPoint Security Courseware VPN-1 for the Security Professional*  
CheckPoint 2000 Edition

*Check Point™ Virtual Private Networks*  
Part No.: 700057 January 2000

*Check Point™ VPN-1/FireWall-1® Administration Guide*  
Part No.: 71300002410 July 1999

How to Troubleshoot SecuRemote Problems by Creating a Fwenc.log File  
Solution ID: **47.0.1537649.2530505** Revised Date: **11/15/2001**  
<http://www.checkpoint.com/>

FireWall-1 Performance Tuning Guide  
<http://www.checkpoint.com/>

McClure, Stuart; Scambray, Joel; Kurtz, George *Hacking Exposed – Network Security Secrets and Solutions* (Third Edition) p. 482, 489-490, 494-495