Global Information Assurance Certification Paper

Auditing the Checkpoint NG SecureClient (VPN-1 / FireWall-1)
Option 1 - An Auditor's Perspective

John E. Blair

SANS GSNA Assignment – v 2.1
December 3, 2002

Assignment 1

Abstract

The purpose of this paper is to assess the controls of the Checkpoint NG VPN-1 SecureClient as they relate to the connection of mobile users to a corporate network. The SecureClient primary configuration reviewed consists of a broadband connection with a screening router performing NAT (network address translation). Testing from a dial-up connection is also reviewed to verify the SecureClient firewall functionality for another possible client connection configuration.

As part of this assessment, various aspects of the Checkpoint VPN-1 firewall solution must be reviewed. Among these are corporate policies governing VPN connections, enabled services, desktop rule sets pushed to client, authentication and encryption methodologies used and the definition of corporate network resources accessible by remote users.

System Description

This audit reviewed the Checkpoint VPN-1 SecureClient NG FP2 (feature pack 2) VPN solution. This solution provides a secure connection for remote/mobile users to the enterprise network using any IP-based connection and serves as their primary means of connectivity to the enterprise network.

The Windows XP Professional v.5.1 operating system was used on the test client machines. The use of XP is important, since XP provides its own firewall which could interfere with the proper operation of the Checkpoint SecureClient / VPN. A requirement of this VPN implementation is that it not interfere with the users' mobility or LAN functionality, while at the same time it must protect corporate resources through a secure communication channel. The client software connected to a dedicated Checkpoint Firewall-1 NG gateway running on a Nokia 650 appliance. The management and policy servers for this review operate on a Sun 2.8 box running Provider 1 NG FP2.

Evaluation of Risk

The control objectives for this audit fall into two major categories, policy and technical. These two major categories are further refined into client side and

corporate management server / firewall based responsibilities. The following objectives are first ranked by major category, then by the side of the connection that the risk affects (i.e. client or corporate).

Policy risks are those that exist because the enterprise failed to or inadequately defined policies to govern the activity / functionality. This can result in administrators, technicians or even users implementing technology or other solutions without the knowledge, consent or direction of management. Another, perhaps more important, aspect of policies is that they define the legal boundaries and the company's recourse if the policy is violated.

Policy Risks, Probability and Consequences

Procedural / policy risks associated with this audit are as follows. The article Virtual Private Networks (VPN): The Insecure Solution by Simon Jenner[1], serves as the foundation for many items listed below.

Corporate side risks - * *Policies should be kept at a high, general level. Defining the exact technology used and how it is implemented provides too much information for persons intent on disrupting network services.*

- Is there a policy for the technology / functionality being audited?
  Probability: If VPN technology is new to the organization, a policy is unlikely to exist.
  Consequences: Without a policy defining how the organization should implement the technology, it is very difficult to conduct the audit for that specific environment. A best practices approach should be used in this situation.
- Does the policy define the types of traffic allowed and not allowed?
  Probability: Assuming a policy exists, it is likely to define the resources and types traffic permitted.
  Consequences: If a policy does not define the resources / traffic, other unintended traffic or resources may become accessible through the VPN.
- Does the policy reference other corporate security policies where appropriate?
  Probability: Low, based on the time and thoroughness of the Security person assigned to the task.
  Consequences: Policies need to work in unison to provide a complete definition of what is and is not permitted. One policy should not define a particular methodology only to be contradicted by another policy.
- Does the policy define the response procedure to be taken in the event of intrusion or incidence?
  Probability: Low, most policies will not define a response plan. It is possible that the response plan is defined within a departmental procedure, in which case it should be referenced within the policy.
  Consequences: A prepared response plan greatly eliminates the many questions and proposed solutions during an incident. Without a plan of this nature, chaos is the likely result.

- Does the policy specify the level of encryption required for VPN traffic?
  Probability: Low. The policy should not specify the exact type of encryption being used, it should only make a reference to the level of strength (DES, Triple DES, etc.)
  Consequences: If the encryption strength is not defined, future implementations may not incorporate the appropriate encryption methodology resulting in possible data loss, theft, etc.
- Does the policy define the resources available to remote users?
  Probability: High. Since access to resources is a primary purpose to connect to the corporate network.
  Consequences: If specific resources are not defined as VPN accessible, other unintended resources may become accessible through the VPN.
- Does the policy define the authentication methodology to be used to gain access to corporate resources?
  Probability: Low. The policy should reflect the means by which authentication will be performed. Is it a new process, does it follow other company login policies, etc.
  Consequences: Invalid or inappropriate authentication methodologies may be used to authenticate a VPN connection, resulting in inappropriate access to resources.
- Is the policy enforceable?
  Probability: Medium. The policy should specify the action management will take if the policy is not followed.
  Consequences: Without enforcement of the policy, it is of little value. Management must be willing to A) enforcement the policy as defined or B) change the policy to one that can be enforced.
- Does it contain language defining the repercussions for its violation?
  Probability: Medium. The policy should specify the possible outcomes from violating the policy.
  Consequences: Employees / users need to know the repercussions of not following the policy. Without notification of the repercussions, the policy is of little value and cannot be taken seriously.

Client side risks

- Have users read and signed the policy, implying they are aware of the possible results for violating it?
  Probability: High. This is especially true for those companies provided remote access to users who are not employees.
  Consequences: Users should acknowledge that there is a responsibility and potential repercussions that comes from using specific technologies to access company resources.

Technical Risks, Probability and Consequences

Technical risks are those associated with the use of a specific technology. Most of the following risks can be applied to all VPN implementations[2] (Virtual Office: Risk Management, Security, Control and Auditing by Charles H. Le Grand), however, some are specific to the Checkpoint SecureClient implementation. Technology risks tend to have more severe impacts than those associated with procedural risks, since secure policies do not prohibit incidents from occurring and secure system configurations can. Policy violations almost always result in the realization of technical risks.

Consequences from technical risks are many. Attacks and unauthorized access can lead to denial of services, stolen data, public distrust of the company, and inappropriate use of the system (spamming, etc.). Additionally, there is a risk of administrative errors if desktop policies and sites, which are pushed to the client are inappropriately defined it could result in a rule set that inappropriately allows, other networks to access the client machine, the VPN and, ultimately, corporate resources.

Additionally, the users experience should be as simple as possible, yet still accomplish the necessary security and functionality. This can be done through good design practices. By initiating the VPN tunnel, defining sites, automating the connection and controlling the VPN configuration files, the users' experience can be enhanced without affecting security. If users have trouble establishing a VPN connection or have to repeatedly call Technical Support, their experience is not a positive one and they are less likely to support future technology solutions. Also, it is very costly to modify the implemented solutions to accommodate users' desires.

Technology Risks
Corporate Side

- Protection from unauthorized access (hackers cannot get in).
  Probability: Medium. Mis-configuring a client file, leaving a port open, unused service enabled, are likely, easily made mistakes.
  Consequences: Depending on the vulnerability and the exploit used, this could range from taking control of client machine, planting viruses, disrupting service at corporate firewall, etc.
- Minimum network management required (little administration needed).
  Probability: Low. This is true once the connection, accessible network objects, system parameters have been defined.
  Consequences: If administrators have to spend a lot of time resolving VPN issues, the cost of administration may outweigh the benefits.

- Provide secure transport for sensitive content (tunneling / encryption).
  Probability: Low. This is nearly automatic – after system parameters have been defined and tested.

Consequences: If the VPN does not provide a secure channel, it is of no value.

- Centralized management of VPN.
  Probability: Medium. A VPN solution deployed to independent field users must have the ability to be centrally managed because users will not have the expertise to administer it themselves.
  Consequences: Relying on users to administer their own VPN solution is extremely problematic, with hugely increased support costs, additional administration time, etc.
- Provide for recovery and accountability (audit trail).
  Probability: Medium. Recovery must be accurate and easy for the user, additionally accurate and complete logs must be enabled.
  Consequences: If users cannot easily recover from errors, they are likely to demand another communication solution due to unreliability. Without logs to indicate the events that have taken place, troubleshooting is very difficult.
- Reliability / accuracy of rule sets / policies pushed to client.
  Probability: High. This is a manual process, which are more prone to errors.
  Consequences: Checkpoint SecureClient receives configuration files from the host, so an error in any of those files results in each user receiving a bad configuration, which may result in unintended networks gaining access, unauthorized users able to establish connections, etc.
- Authentication of users.
  Probability: High. This is controlled by corporate administrators and is a manual configuration process, thus more error prone.
  Consequences: Unauthorized users able to authenticate through firewall to VPN resources.
- Encryption algorithm used is adequate.
  Probability: Low. This is a management decision, depending on the data traversing the VPN.
  Consequences: If the wrong encryption methodology is selected, it may result in confidential data not being protected at the level dictated by management and is more susceptible to hijacking.
- Encryption Domain definition is accurate.
  Probability: Medium. This becomes more problematic and more difficult to comprehend with the more network objects added to the domain.
  Consequences: This can be a very confusing area for administrators due to the potentially large number of objects in the domain. They may unintentionally allow access to inappropriate resources.
- VPN Session management.
  Probability: Low. This is primarily a usability issue. Users would like their sessions to automatically disconnect after a period of inactivity.
  Consequences: If the VPN session remains enabled for long periods of time, unauthorized users may gain access to corporate resources through the established authenticated VPN session.

Client side

- User impact (ease of use).
  Probability: Low. This is dependent largely on the amount of automation developed to perform various user tasks and the training users receive.
  Consequences: If users have difficulty using the VPN software, technical support costs will likely increase and users will be hesitant in the future to support technology solutions.
- Modification of user files associated with the VPN is ineffective.
  Probability: Low. Configuration files pushed to the client are not intended to be edited by the user.
  Consequences: If users could modify the SecureClient configuration files they could bypass controls designed into the files and place their own machine as well as the corporate network at risk from intrusion and attack.
- Disabling of Windows XP Internet Connection firewall.
  Probability: High. This is setting is a popular Microsoft feature and users will likely have this feature enabled.
  Consequences: With this feature enabled, the VPN may not function or may function will unpredictable and unstable results. This results in the user being unable to conduct business through the VPN.

Research on Current State of Practice

Implementation of this complete Checkpoint VPN solution requires research into both firewall and client software. The current state of practice is described in the following sections three sections, firewall, VPN and client.

Firewall

Firewall audit programs, especially for Checkpoint, are relatively easy to find. A review of www.auditnet.org reveals at least two firewall audit programs, one specifically for Checkpoint. Additionally, it contains numerous links to other sites which also contain helpful audit information http://www.auditnet.org/asapind.htm. While the basic function of a firewall is to stop unwanted traffic while allowing intended traffic to pass, most firewall programs focus significantly on the operating system configuration. For the purposes of this paper, the firewall is reviewed from the perspective of a management server. The operating system the firewall resides on is outside the scope of this review.

Lance Spitzner described it best in "Auditing Your Firewall Setup"[3] when he said "First, you have certain expectations of what your firewall can and cannot do and you want to validate those expectations." He goes on to say, "the first step in auditing is to define what our expectations are, i.e. what do we want our firewall to do"? Following Mr. Spitzner's recommendation, the expectation of the firewall for this audit is that it is primarily a VPN gateway for mobile remote users to connect to the enterprise network.

Lance Spitzner checklist, from "Auditing your firewall setup"[3]

- Disable all unnecessary services. For Checkpoint firewalls, be sure to close administration ports 256, 257, 258 and ICMP, which is open by default.
- Establish a lockdown rule first, with all other rules coming after. For more information on rulebase design, see Mr. Spitzner's article, "Building Your Firewall Rulebase"[4].
- Scan every network segment from every other network segment to verify the traffic going through the firewall is EXACTLY what is allowed.
- Verify authentication and encryption – These are 2 critical elements, especially when the firewall is a VPN gateway.
- Examine the firewall logs – did the firewall detect all the scans? Did it encrypt the correct data and how? This information should all be in the logs.
- TCP and UDP filtering. What packets are (not filtered, and) able to pass through the firewall?

Comments on Spitzner

- Spitzner begins by stating the expectations of the firewall should be defined in a security policy. By auditing to a policy, the auditor has something objective to measure test results against.
- The firewall should follow the profound mantra of security, "everything is denied unless expressly permitted." Scanning the firewall and comparing traffic and filter results will objectively establish whether the firewall is performing as expected.
- Physical security and hardening of the operating system should not be overlooked (though outside the scope of this audit). A breach in either of these areas will effectively render the firewall untrustworthy. Both can be measured objectively through testing. Spitzner recommends other checklists for accomplishing these tasks.

Checklist from Dr. Loye L. Ray[5], courtesy of Dan Strom's SANS GCNA assignment.

- Perform risk analysis, set expectations and goals.
- Verify security policy exists and determine scope.
- Get approval before testing.
- Conduct interviews, review documentation and perform testing.
- Prepare report and prioritize action items.
- Feed findings back into risk analysis – compare to risk acceptance.
- Remember that security is a continuous process.

Comments on Ray

- This article is very focused on the audit process. When reviewing the documentation, it would prove very helpful to be able to match rule base changes to a change control document. Also, documentation within the rule base itself can be checked (if used). Checkpoint provides a column

within the rule base for this purpose, although limited, it is better than nothing and should be used. When there are a lot of rules and networks grouped together it is very difficult to remember who and what the rule is for.

- Policy should dictate what is and what is not allowed within a particular environment. The policy is the standard to which test results can be objectively compared.
- Prior to conducting ANY testing, get management's approval, in writing! Enough said.
- Auditors should strive to adapt and be objective as possible. Technology and its use changes constantly and what is acceptable in one environment may be prohibited in another. Be sure to understand the environment you are auditing.

VPN

In contrast to finding firewall audit programs, VPN audit programs are essentially non-existent. A search for "VPN audit" on www.google.com" led to one audit program. This program was part of a presentation by Lily Shue to the Los Angeles ISACA group entitled, "Security, Audit and Control of VPN"[6] http://www.isacala.org/2002_Spring_Conference/Handouts/S1%20Security%20Audit%20and%20Control%20of%20VPN.pdf. Shue provides a good background of what a VPN is, how it works and the technologies used in deployment.

Another VPN audit program, not displayed in the Google search parameters listed above, is provided by *Simon Jenner*, *"Virtual Private Networks (VPN):" The Insecure Solution*[1]

Checklist from Lily Shue, "Security, Audit and Control of VPN"

- Minimize vulnerability of bridging security and maximize protection of data traversing the Internet.
- Remove all unnecessary services, applications and user accounts from VPN servers.
- Backup, monitoring, policies, performance and compatibility of VPN and enterprise network protocols.

Comments on Shue

- Strong encryption and authentication are of paramount importance. Using a weak encryption algorithm does not provide much security in any environment. Likewise, without strong passwords and procedures to authenticate users initiating the VPN connection, security is nearly worthless. Both of these areas can be tested objectively. Encryption algorithms can be configured/selected and password composition should be a matter of policy and is easy to test.

- The removal of unnecessary services, applications and user accounts from VPN servers should be standard practice. Though testing for these is relatively easy, the question of what is unnecessary may be subjective to many administrators. Generally, if there is no business need or job requirement, it is unnecessary.
- Most of Shue's audit program focuses on the review of documentation, change control, policies and procedures. These elements are certainly a part of every audit however; they do not address the technical aspects. These aspects must be addressed in order to provide a complete security picture.

Checklist from Simon Jenner, "Virtual Private Networks (VPN):" The Insecure Solution[1]

- Was the implemented solution in line with existing security policies?
- Was strong authentication used for user authentication?
- Was a VPN system security policy supplied?
- Does the VPN gateway reside outside the corporate environment?
- Was VPN client security considered?

Comments on Jenner

- Most of Jenner's recommendations are aimed at policy and documentation. While this is important, it does not address the technical aspects needed for a VPN audit.
- Jenner does take client security in to account. This can be easily overlooked. Unfortunately, it is difficult to control clients, especially if the clients are independent users of corporate systems and not remote employees. Independent users would probably have strong opinions about corporate security restrictions being placed on machines they paid for. This is a sensitive area and it should not be overlooked.

Client

The amount of control an enterprise has over remote users depends on the type of users. Are they employees or independent users? If employees, it is much easier to enforce corporate policies. If independent users (think of insurance agents accessing systems at headquarters), then the problem becomes much more complicated. Independent users are likely to resist corporate security considerations far more insistently than an employee. Communication and education are key elements in getting users to understand the need for security. Another, and probably more effective means, is to design security functions into the interfaces used by them. If security tasks can be performed with little interaction from the user, the better the chance security will have the intended affect.

Some responsibilities must be placed on the client side of the solution. Requiring the independent users to have the appropriate hardware, software, and operating system is not unreasonable. The benefits of doing so are easily determined. In

order to take advantage of new functionality, certain minimum standards must be met.

Conclusion

Firewall

Spitzner and Ray both provide valuable insight into what and where to look when auditing the firewall. Spitzner focused more on technical considerations while Ray's leaned more toward policy, procedure and documentation. Together they provide the foundation of the firewall checklist. Additional research within Checkpoint's documentation should supplement this checklist.

VPN

Most of the information consisted of steps taken in nearly every technology audit. Little technical information was presented. Additional checklist steps will have to be derived from Checkpoint documentation and other sources.

Client

Jenner did account for client security, though no suggestions were made as to what to look for or recommend. This is likely due to the nature of remote users. Corporate policies are hard to enforce on independent users and remote employees are often governed by subjective corporate policies. However, in order to provide a consistent service to remote users and ease the administrative overhead involved with that service, certain expectations must be outlined in order to proceed with the design process. These expectations generally consist of upgrades to hardware, software and operating system.

Assignment 2

The following checklist does not include many of the standard steps performed during most I.S. audits, such as software version check, physical security, virus protection etc. Rather, this checklist focuses on steps less obvious and likely not included in a typical VPN audit. While not included here, the standard steps should always be performed. Also, some of the references are original contributions that were not requirements of the corporate VPN implementation project. Project requirements (if used in this report) are noted as such in the reference headings.

Audit Checklist

Item 1 – Verify rule set is pushed to client desktop and is applied successfully.

- *Reference:* Original contribution.
- *Control Objective:* To verify client is running rule set defined by management server and that manually modifying the *local.dt* file does not interfere with the application of the defined network objects and rule set.
- *Risk:* Modification of the *local.dt* file could allow unintended access to the desktop by defining networks outside the encryption domain. Likelihood is

dependent upon curiosity of the remote user, their technical abilities and their own precautions against having their machine compromised (updated anti-virus software, disconnecting from Internet, etc.). The ability to have manual modifications applied to this file could lead to unauthorized access to network resources through a compromised desktop.

- *Compliance:* This is a binary item. The desktop must be running the rule set defined by the management server at all times, not one specified by the user or an attacker.
- *Test:* Step 1 - Manually modify the *local.dt* file on the client desktop. The file is located at *C:/program files/checkpoint/secureremote/policy*.
  Step 2 - Modify one of the *:netobj ipaddr* to an external network IP address. This will allow incoming connections from that external network to the desktop.
  Step 3 - Enable the VPN connection, then submit a port scan from a machine on the external network.
  Step 4 - Go to the SecureClient diagnostics and select *LOG*. The log should indicate all scans from the machine on the external network are being dropped. Additionally, if the PC is rebooted, (causing the VPN client to be reloaded) an error message will be displayed indicating that the Desktop policy files may have been corrupted.
- *Test Type:* This is an objective test.

Item 2 – IP Forwarding Disabled (Internet Connection Sharing)

- *Reference:* Checkpoint Desktop Security Guide NG FP2[7].
- *Control Objective:* Verify that Internet Connect Sharing is disabled for Windows 2000 and XP desktops.
- *Risk:* If Internet Connect Sharing is not disabled, the desktop could become a gateway since SecureClient does not support IP Forwarding. Likelihood of this event is high (especially if user is required to disable this function and assuming attacker gets past screening router, if one exists). A user may also enable Internet Connect Sharing for some other purpose not realizing by doing so, it interferes with the security of the VPN and desktop.
- *Compliance:* This is a binary item. The option is either disabled or it is not.
- *Test:* Step 1 - From the client desktop, select *Control Panel*, then *Administrative Tools>Services.*
  Step 2 - Make sure the services **Internet Connection Sharing** and **Routing and Remote Access** are stopped and not set to automatic (set them to **Manual** or **Disabled**).
  Step 3 – Using **Regedit**, make sure that the following registry value is set to zero.
  HKEY_LOCAL_MACHINE\System\CurrentControSet\Services\Tcpip\Parameters\IpEnableRouter
- *Test Type:* This is an objective test.

Item 3 – VPN Policies for users.

- *Reference:* Virtual Private Networks (VPN): The Insecure Solution by Simon Jenner[1].

- *Control Objective:* Determine if policies governing the use of VPN technology have been defined and acknowledged by the users.
- *Risk:* Without policies to govern the use of a technology, the enterprise has not performed due diligence by informing users of their responsibility for using a corporate resource. This is a relatively low risk item, but one that is easily overlooked and could lead to potential liability claims against the company. A policy does not prevent the loss of company information or negate the user's responsibilities, but it does serve to protect the company from some legal actions and may also help support a claim for insurance purposes in event of an unauthorized access, data loss, etc.
- *Compliance:* This is a binary item. The company has either defined policy regarding the use of the VPN and access to company resources or they have not. Part of this process must include the users' acceptance of the policy in writing.
- *Test:* Obtain VPN user security policy. Verify all remote users have signed their acceptance of the policy and the possible repercussions resulting from its violation.
- *Test Type:* This is an objective test.

Item 4 – User authentication process.
- *Reference:* Original contribution.
- *Control Objective:* Ensure that defined users can enable VPN connection.
- *Risk:* Unauthorized users enable a VPN connection to company resources. The result of this includes data theft, attacks, viruses, etc. The likelihood of this occurring depends on how the authentication process is defined and enforced by the company. It's possible that anyone with access to the desktop could authenticate or it may be limited to a specific group of users without a business need to establish a VPN connection.
- *Compliance:* This is a binary test. The appropriate process is defined correctly and enforced or it is not.
- *Test:* This test assumes an LDAP directory is used for authentication of users. This test could easily be adapted to other architectures.
  Step 1 – Verify the container defined to authenticate remote users (likely named something like - remote / field, etc.).
  Step 2 – Define or obtain a user and password from a different user container within the same LDAP structure.
  Step 3 – Enable the VPN connection from the desktop and attempt to authentication to the management server using the user and password from the container in step 2. The user should not be able to authenticate if the authentication container is accurately defined.
- *Test Type:* This is an objective test

Item 5 – IKE Mode used to authenticate users.
- *Reference:* Excerpt from Checkpoint discussion list[8].

- *Control Objective:* Ensure IKE aggressive mode has not been enabled (note that aggressive mode is disabled by default in NG). The Hybrid mode extension should be used.
- *Risk:* IKE aggressive mode transmits usernames and passwords in clear text. By passing usernames and passwords in clear text, the possibility exists that they will be sniffed or stolen during transmission. The likelihood of this occurring is higher due to the fact that the origin of the transmission is the desktop client. This would result in the possible access of company resources by unauthorized users utilizing a valid username and password.
- *Compliance:* This is a binary test. Hybrid mode is used or it is not.
- *Test:* Step 1 – From the management server (Provider One), launch the *Policy editor.*
  Step 2 – From the displayed rule set, click on the *firewall object (or cluster object* if redundant firewalls are used). When the object is displayed, click on *VPN* to reveal the current configuration settings for IKE.
  Step 3 – Verify the settings adhere to policy or standards for that environment.
- *Test Type:* This is an objective test.

Item 6 – Verify LAN rule exists in SecureClient rule set..
- *Reference:* Original contribution / requirement of project.
- *Control Objective:* To ensure that remote user LAN functionality has not been adversely affected by SecureClient firewall rule set.
- *Risk:* Risk is essentially one of a detrimental user experience. The ability for the user to share local resources and still use the VPN is essential. SecureClient cannot disable the sharing or accessibility of local printers, files, etc. If the user has an unfavorable experience as a result of using SecureClient, support calls and costs are increased and the user is likely to either not use SecureClient or worse, find unapproved alternatives. The likelihood is relatively low if proper design and testing procedures are employed.
- *Compliance:* This is a binary test. LAN functionality is unchanged after the installation and enabling of the SecureClient rule set or it is not.
- *Test:* Step 1 – Obtain the configuration of the SecureClient rule set by going to the *SecureClient Diagnostics screen* and clicking on the *Policy* icon.
  Step 2 – The inbound rule set should have a rule expressly permitting LAN devices.
  Step 3 - Enable VPN connection and attempt to print a file to a LAN printer.
  Step 4 – Share a file from the SecureClient desktop to the LAN. From another PC on the LAN, attempt to access the shared file. If properly configured, both tests should be successful.
- *Test Type:* This is an objective test.

Item 7 – Licensing of SecureClient and Policy Server
- *Reference:* Checkpoint Desktop Security Guide[7].
- *Control Objective:* Ensure compliance with vendor licensing agreements.

- *Risk:* If the company is out of compliance with licensing agreements, it faces potential fines and restrictions from the vendor and possibly software compliance organizations. Also, the software itself may only allow the connections for which there are licenses, resulting in users being denied access to company resources. For companies that maintain strict procedures to ensure compliance, this is a relatively low risk.
- *Compliance:* This is a binary test. The number of licenses matches the number of users or system configuration or it does not.
- *Test:* Step 1 - Obtain the license agreements for SecureClient and the Policy Server. The SecureClient license is installed on the management server and the Policy Server license is installed on the VPN-enabled firewall module with the policy server installed.
  Step 2 – Compare the SecureClient license list of users, to the number of intended or actual users of SecureClient. The license should match or exceed the number of intended or actual users.
  Step 3 – The policy server license is required for the operation of the Policy Server. If it is not installed, the Policy Server is unavailable and users cannot download policies, which results in an insecure configuration on the desktop.
- *Test Type:* This is an objective test.

Item 8 – PC is still protected by SecureClient firewall if VPN tunnel is disabled.
- *Reference:* Original contribution / requirement of project.
- *Control Objective:* To ensure the desktop client PC is protected by the SecureClient firewall even if the VPN is disabled.
- *Risk:* If the desktop is not protected by the firewall, attackers could compromise the desktop PC, planting trojans, executing malicious code, compromising the VPN connection and potentially gaining access to company resources. The likelihood of this occurring is growing given the popularity of broadband connections and user's general ignorance of security.
- *Compliance:* This is a binary test. The SecureClient firewall will protect the PC from incoming connections (according to its rule set) or it will allow the connections.
- *Test:* Step 1 – Disable the VPN connection, verify SecureClient is enabled.
  Step 2 – Obtain IP address of PC being used (Click on *Start* > *Run* > for program to run enter *winipcfg*) and enter this address in the ShieldsUp box requesting the IP address to be scanned.
  Step 3 – Do a port scan against the client PC to check for possible services to be exploited. Use a commercial tool like ISS Internet Scanner, freeware tools like NMap, or free services such as "Shield's Up" at www.grc.com [9].
  Step 4 – The results of the test should indicate that no ports were accessible, no vulnerabilities were found and that the PC is secured.
- *Test Type:* This is an objective test, assuming reliability of Steve Gibson's product, which has received very good reviews.

Item 9 – Data transmission is encrypted
- *Reference:* Requirement of project.

- *Control Objective:* To verify that data is being encrypted as expected.
- *Risk:* If transmitted data is not encrypted, the VPN is not functioning properly and the potential exists that transmitted data may be intercepted by an attacker. The likelihood of this is relatively low given the configuration methodologies in place. However, if an administrator forgets to select the proper encryption scheme, the VPN may not work at all due to configuration conflicts.
- *Compliance:* This is a binary test, data is being encrypted or it is not.
- *Test:* Step 1 – Establish a VPN connection with firewall.
  Step 2 – With a network analyzer[12] pointed to an address outside the firewall, analyze the data being transmitted to the firewall.
  Step 3 – Select one of the UDP packets being transmitted (for Checkpoint, look for port 259), then in the bottom window of the network analyzer, examine the packet. The data displayed in the bottom window should be in ciphertext and unreadable.
- *Test Type:* This is an objective test.

Item 10 – Screening router configuration…..* *if one is being used.*

- *Reference:* Original contribution / requirement of project.
- *Control Objective:* To ensure the screening router is performing the intended functions of network address translation and other company defined security considerations.
- *Risk:* In a broadband configuration, if the screening router is not accurately performing its functions, the desktop PC can be compromised resulting in disclosure of the PC's actual IP address and facilitate any number of attacks. The likelihood of this occurring is dependent on the administrator's skill set and router configuration. If the router configuration is defined offline, then loaded to the router automatically, the chances of the configuration being accurate is greater because other routers have probably been configured previously with the same batch process. Of course, the chance exists that the configuration is still wrong and now many routers have the same incorrect configuration. This will certainly be noticed quickly once the routers have been deployed to the field and subjected to the wilds of the Internet. Alternatively, if the router configuration has been done manually, there is a higher risk that the configuration is inaccurate, as manual configuration practices have a higher margin of error (people make mistakes).
- *Compliance:* This is a mixed test, because while certain configuration settings are typically considered mandatory for screening routers (filtering set, IP address definitions, passwords encrypted, all unnecessary services disabled, etc.), the actual configuration of the router is dependent on the organization deploying it and that organizations requirements.
- *Test:* Step 1 – Obtain a configuration guideline published by the company for configuring screening routers for remote users. If this document is unavailable, refer to the National Security Agency (NSA) Security Recommendation Guides[10] for a best practice review. This guide is directed

toward Cisco routers, but the information can be applied to other types of routers as well.
Step 2 – Access the router through a network management device, SNMP commands or a network administrator who can download the router configuration. Compare this configuration to the guideline or best practices document, noting any discrepancies.

- *Test Type:* This is an objective test if the router configuration guidelines can be obtained because the actual configuration can be compared to the guideline. The configuration could also be compared to best practices, though those can be subjective because they will not specifically reflect the company's unique I.S. environment.

Item 11 – Unnecessary services disabled on firewall. *Note that this test should be performed for both the host and client firewalls. It is only described from the host perspective here because it is the more relevant test of controls, since the host firewall is responsible for much more activity.

- *Reference:* Lance Spitzner, Auditing your firewall setup[3].
- *Control Objective:* To ensure only necessary ports / services are enabled on the firewall.
- *Risk:* Running unnecessary ports potentially allows an unauthorized user access. Depending on the ports / services enabled, the consequences of this risk can be quite serious. If an attacker can get through the firewall by exploiting a service vulnerability, the internal network may be penetrated. The likelihood of leaving ports /services enabled is fairly high, especially in the Checkpoint environment, since several ports are open by default.
- *Compliance:* This is a mixed test. Though most configurations follow a standard baseline the configuration is truly dependent on the organization and the purpose of the firewall.
- *Test:* Step 1 – If available, obtain the policy defining what type of traffic the firewall is allowed to accept and what traffic should be denied. If no policy exists, verify with administrators the services they think are enabled.
  Step 2 - Using Nmap[11] or some other scan tool, scan the firewall for all tcp, udp and icmp. This scan should be performed from both the internal and Internet sides. The following Nmap command can be used:
  nmap -sT -n -v -r -p1- -P0 -oN nmap-full-80 XXX.XXX.XXX.80
  Step 3 – Based on results of the scan, determine what ports / services need to be disabled, if any, as compared to firewall policy or firewall configuration best practices.
- *Test Type:* This is an objective test if the organization has developed a configuration specifically for a VPN firewall that lists the services enabled, ports open, rule sets to be defined, etc. If not, the test is somewhat subjective, as auditing against best practices will not necessarily consider the unique I.S. environment of the company.

Item 12 – Firewall rule base – host side.

- *Reference:* Lance Spitzner, Auditing Your Firewall Setup[3] and Building Your Firewall Rule Base[4].

- *Control Objective:* To verify the firewall rule base is configured properly and contains a lockdown rule.
- *Risk:* An improperly configured rule base could inadvertently allow unintended access to or through the firewall. Consequences of this are dependent upon the actual improper configuration and the potential cascading effects, if any. For example, a mistake in a network object definition that assigned network groups to multiple rules could severely impact not only the reliability, but the performance of the firewall as well. Outside networks may be allowed access to unauthorized resources, attackers may be able to take control processes, ports, etc. The likelihood of such a mistake being made is relatively high, given the complexity and number of rules defined.
- *Compliance:* This is a conditional test, as compliance is totally dependent upon what the defined rules permit and deny, the number of rules (adds complexity), documentation of rules (often not well documented, leading to unknown / unneeded rules) and the rules position in the rule list. Position is important since rules are processed sequentially from rule 1 to rule xx.
- *Test:* Step 1 – Obtain a copy of the firewall rules from the firewall administrator and evaluate them for appropriateness based on access allowed and prohibited which should be documented in the firewall change control records.
  Step 2 – Define a scan test machine to an IP address outside the firewall (in the DMZ or the firewall's IP address) and a system positioned inside the firewall.
  Step 3 – Using Nmap or some other network scanner, begin scanning every network segment from every other network segment defined to the firewall. The scans will determine what packets can and cannot get through the firewall.
  Step 4 - Based on results of the scan, determine what types of traffic penetrated the firewall and whether or not it that is appropriate. If not, recommend the appropriate rule configuration changes. If rule changes are made, run the scans again to verify the change has the intended affect.
- *Test Type:* This is an objective test if the types of traffic permitted and denied have been defined and or documented by firewall change control records. If not, the test is subjective based on the auditor and administrator's assessment of business need. Also, a procedure for documenting firewall changes should be started immediately.

Item 13 – Logging of firewall traffic.

- *Reference:* Lance Spitzner, Auditing Your Firewall Setup[3], Building Your Firewall Rulebase[4] and Checkpoint's Desktop Security Guide[7]
- *Control Objective:* To ensure logs are created and that the log is correctly recording the appropriate activities.
- *Risk:* Without the log recording firewall actions against traffic, there is no record of events taking place on the firewall. This record provides the one place (assuming log information is not also being written to an external database) to evaluate how the firewall is handling the various forms of traffic it

faces. It also provides a source of information to confirm that the rules are performing as expected. The likelihood of no log being created is remote. The likelihood that the log is not recording the right information is great, especially if the rulebase contains more than 50 rules.

- *Compliance:* The test for log creation is binary. The test for expected information being written to the log is dependent upon the rules defined and the actions associated with those rules.
- *Test:* Tests performed in Item 12 can also be applied to this item. The additional component to this test is to look at the logs and verify that the correct rules are being applied as expected for the intended services, addresses or networks. For instance, suppose a policy stated that no internal outbound FTP traffic was allowed and if detected the firewall should drop the packet, issue an alert and log the event. The rule, however, might be defined to drop only the packet, not to issue an alert or log the event. Therefore, when you issue an FTP request from an internal address, the firewall will drop the packet, but not make a log entry or issue an alert. Your expectation was to receive an alert and to also be able to see the event in the log. Neither happened because the rule was defined incorrectly.
- *Test Type:* This is an objective test. Note, if the firewall has an abundance of rules this is also time consuming.

Item 14 – Attempt to establish VPN connection from a source other than SecureClient NG.

- *Reference:* Original contribution / requirement of project.
- *Control Objective:* To verify that only SecureClient NG VPN connections can be made to firewall.
- *Risk:* Inappropriate connections could be made to the firewall through a different VPN client. By being able to establish a connection with a VPN source other than SecureClient, it may be possible to negate security functionality built into or downloaded to SecureClient. The likelihood of this occurring should be small due to the authentication process and information exchange between SecureClient and the firewall.
- *Compliance:* This is a binary test, the firewall either accepts the connection from a foreign VPN application or it denies it.
- *Test:* Step 1 – Define the firewall address to a VPN application other than SecureClient.
  Step 2 – Attempt to connect to the firewall with this VPN application.
  Examine the firewall log file to verify that connection request was dropped.
- *Test Type:* This is an objective test.

Item 15 – Policies governing VPN solution.

- *Reference:* "Virtual Private Networks (VPN): The Insecure Solution" by Simon Jenner[1].
- *Control Objective:* To ensure effective quality policies are created or updated to reflect a VPN solution.

- *Risk:* Policies are needed to ensure security and business requirements are clearly defined and known to users. Without policies governing the use of a technology implementation, it quickly erodes into a quagmire without clear assignment of responsibility for patches, upgrades, maintenance, standards, etc. Policies should make business sense while defining the parameters the company uses to conduct business.
- *Compliance:* This is a binary observation. Policies have either been updated or created to reflect the VPN solution management intends to provide or they have not.
- *Test:* Step 1 - Contact the security or policy administrator or otherwise find security policies governing remote connections to the corporate network.
  Step 2 – Review these policies for the following types of information.
    a. Firewall policy and procedures - types of traffic allowed through the VPN.
    b. IDS policy and procedures – removing signatures to reduce false positives from VPN traffic.
    c. Router policy – allowing VPN traffic through screening routers.
    d. Internet usage policy – adding remote client details.

  Step 3 – If policies don't exist, then they must be created. If existing policies don't contain content closely related to that listed in Step 2, then it must be added.
- *Test Type:* This is an subjective test, based on company specific information dictated by the business needs.

Item 16 – Firewall change control.

- *Reference:* "Building your firewall rulebase" by Lance Spitzner[4].
- *Control Objective:* To ensure changes made to the firewall rule base are documented, tested and authorized. Additionally, all changes should include a back-out plan in the event problems occur implementing the change.
- *Risk:* Without a proper change control system, unauthorized, untested or unintended changes may be implemented to the production environment. A change control system provides a standardized methodology, ensuring documentation, testing and intent of the change, as well as a back-out plan.
- *Compliance:* This is a binary observation. A change control system exists (incorporating the previously mentioned criteria) or it does not.
- *Test:* Step 1 – Verify the existence and use of a change control system by reviewing firewall change control documentation. If one does not exist, write the recommendation to have one implemented. If the system does exist, proceed to step two.
  Step 2 - Review the firewall logs for changes to the rulebase or firewall configuration itself.
  Step 3 – Through interviews with firewall and change control administrators, acquire the documentation supporting the changes revealed in the logs.
  Step 4 – Verify the changes and identify the following:
    - The person making the change is authorized.

- A brief description of the change itself (due the nature of firewall changes, it is not a good practice to publicize exactly what services/addresses, etc. are being modified).
- Date/Time of change
- Reason for making change
- Approval for the change from appropriate administrators
- Back-out plan is thoroughly documented.

- *Test Type:* This is a subjective test (assuming a change control system is in place), meant to identify the information needed to document changes made to the firewall.

Item 17 – Administrator access.

- *Reference:* "Virtual Office: Risk Management, Security, Control and Auditing" by Charles H. Le Grand[2].
- *Control Objective:* To limit the number of administrators to only those needed to maintain the system and provide for adequate backup coverage.
- *Risk:* Administrators, by the nature of the duties, have a very high level of access. A high number of people with administrator access increases the odds that one of them will abuse this privilege and damage the system.
- C*ompliance:* This is a conditional test. One administrator is not enough (no backup, single point of failure, etc.) and ten administrators is likely too many (too many people with the keys to the kingdom, etc.). This is a best practice test and the auditor should consider the nature and size of the environment being audited.
- *Test:* Step 1 – Obtain a listing of all administrators on the system. To find the administrators defined to the system, performing the following from the management server (Provider 1). Click on the *Administrator icon*. The crowned usernames are administrators. To verify the permissions associated with the administrators (or any other object listed on the Admin page) select the *GUI Client* icon located underneath the *Administrator* icon.
  Step 2 – Based on the size of the environment and the needs of the department (backup & coverage issues, training, number of people available, segregation of duties, etc.), determine the number of appropriate administrators.
  Step 3 – Verify the number of administrators defined does not exceed the appropriate number for that environment.
- *Test Type:* This is a subjective test as appropriate results are dependent upon the company's I.S. environment.

Item 18 – Network redundancy.

- *Reference:* "Virtual Office: Risk Management, Security, Control and Auditing" by Charles H. Le Grand[2].
- *Control Objective:* To ensure the system is designed with appropriate backup resources and is capable of maintaining required availability.
- *Risk:* A system that is unavailable costs the business money and damages its reputation. If users are unable to access or use the system, they cannot

conduct business, which in turn hurts the company. In all likelihood, the system will incur down time at some point for any number reasons, software bug, power disruptions, human error, etc.

- *Compliance:* This is primarily a binary test. However, it is dependent on the need of the system. If the system is deemed critical by management (the business requires the system be available at all times), redundancy considerations must be expanded to include multiple service providers, firewalls and access points, load balancing and immediate support.
- *Test:* Step 1 – Obtain from management the criticality of the system – i.e. how important is the availability of this system to the company? Can it be down for 1 hour a day, 2 days, a week, etc.?
  Step 2 – Ask the network administrators for a diagram of the system/network under review.
  Step 3 - Verify the redundancy of the network and its components. Depending on the criticality of the system, determine if the following are present:
  - At least 2 connectivity / service providers
  - At least 2 paths for traffic into network (fence routers, firewalls, etc.)
  - Load balancing of the heavy traffic components (for performance and fail-over reasons).
  - Availability of support personnel and incident response plans.
- *Test Type:* This is a subjective test, determined by the criticality of the system according to management. The more critical a system, the more avenues of redundancy that must be built in to ensure its availability.

Item 19 – Internal resource access allocation.

- *Reference:* Original contribution / requirement of project.
- *Control Objective:* To ensure that the resources to be accessed by remote users are defined and secured appropriately.
- *Risk:* Resources within the corporate network to be accessed by remote users must be properly secured and defined by policy. If resources are not defined, undesired access may be granted to inappropriate resources, potentially violating confidentiality and intended data security mechanisms. If VPN technology is new to the company, this part of the policy is likely to be overlooked since the focus is on connectivity issues.
- *Compliance:* Defining secured and appropriate resources to be accessed remotely is a binary test. Policies either state the resources to be accessed, level of access allowed and by whom or they do not.
- *Test:* Step 1 – For resource definition, obtain the policies regarding VPN access. Verify if they define the type of user, the level of access allowed and the type of resources that can be accessed through the VPN.
  Step 2 – Review the network and system diagrams to ensure that all paths from the VPN firewall lead to the appropriate systems / resources.
  Step 3 – For the basis of this test, assume only remote users are allowed access and that an LDAP directory provides authentication. Therefore, determine if all remote users are defined to a unique container within the

LDAP directory. Verify that the firewall authenticates only those remote users defined to this container.
Step 4 – Define or acquire a user ID and password from a different container within the LDAP and attempt to authenticate through the VPN and access the resources. If configured appropriately, you should not be able to gain access.

- *Test Type:* These are objective tests. The policy defines the resources and those who are permitted access or it doesn't. If properly defined, only the appropriate users should have access to the resources.

Item 20 – Verification of files and parameters pushed to client.

- *Reference:* Original contribution.
- *Control Objective:* To ensure that the configurations (*local.dt* (*C:/program files/checkpoint/SecureRemote/policy* on the SecureClient PC) and firewall rule set) of the files pushed to the client from the host are accurate and defined appropriately.
- *Risk:* Inaccurate configuration files pushed to the client potentially exposes both the client machines/LAN and corporate network to attack or unauthorized access by permitting networks that should be denied. Given that these files are manually defined and the affect is the entire VPN user base, this is a high risk with high probability.
- *Compliance:* Definition of appropriate resources and networks is a conditional test based on business need of those requiring access. However, once defined it is a binary test to ensure only those resources are accessible.
- *Test:* Step 1 – From the business area responsible for VPN connectivity, obtain the services / resources (including networks, specific IP addresses, etc.) that are permitted for remote access.
  Step 2 – Review the configuration files being pushed to SecureClient by the host gateway / management server. Assuming the resources are defined, they should be the only resources listed in the configuration files.
  Step 3 – Through investigation and interviews determine if a verification process exists to help ensure accuracy of the files. The person creating the file should not be the one who verifies its accuracy.
- *Test Type:* These are objective tests. The resources are defined and stated in a policy / standard or not and a control process for file accuracy exists or it does not.

Item 21 – Management of remote user VPN session.

- *Reference:* Original contribution.
- *Control Objective:* To ensure that the user's VPN session is appropriately controlled / configured and does not expose the user or host to unnecessary risk.
- *Risk:* A user session not properly controlled exposes company resources. The longer an authenticated session is left unattended the more likely it is to be used inappropriately by an unauthorized person to gain access to confidential information or to use the VPN connection for fraudulent activities.

- *Compliance:* This is a conditional test based on criteria management has declared. The session may be controlled according to management's direction, but that may not necessarily be in the best interest of the company.
- *Test:* Step 1 – Obtain from management or the appropriate administrator the session parameters and how this functionality is enforced (elapsed time, period of inactivity, etc.).
  Step 2 – From the management server (Provider One), click on *Policy Editor* à Select *Policy* drop down menu→Select *Global Policies*→*Remote Access*
  Step 3 – Verify that the settings displayed are the right values as determined by policy.
- *Test Type:* This is an objective test, based on management's declarations of how the session should be handled.

Assignment 3

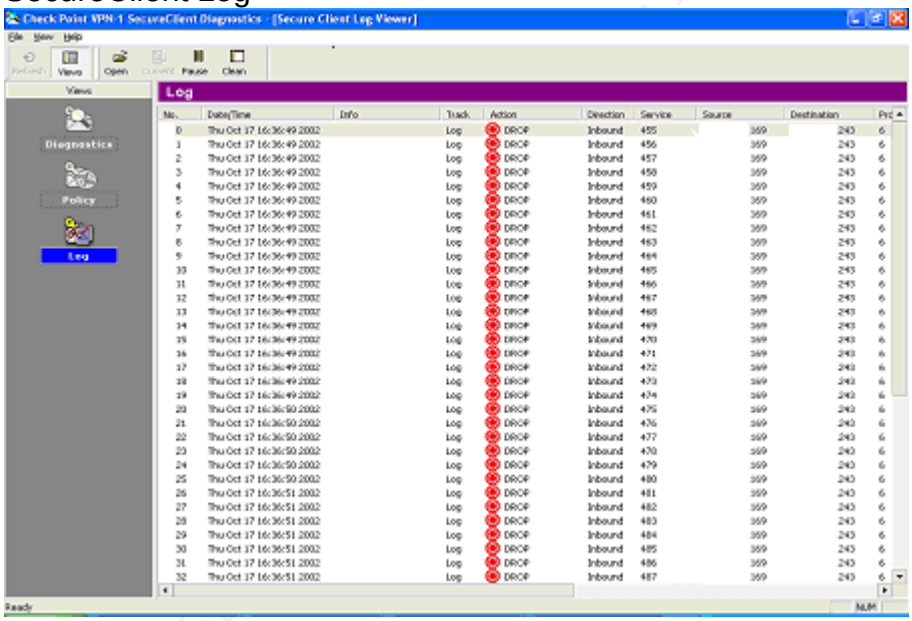
Audit Evidence

Stimulus / Response items 1, 2, 4, 8, 11

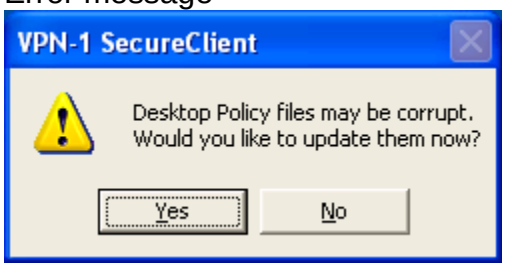
Item 1 – Verify rule set is pushed to client desktop and is successfully applied.
Test result – **PASS**

The *local.dt* (personal firewall rules-client) file has been changed to allow incoming connections from the xxx.xxx.xxx.169 network to the local PC. The following screen print shows a port scan of ports 1-500 originating from a PC with source IP address of xxx.xxx.xxx.169 being dropped by the client firewall. Therefore, attempting to change the *local.dt* file while the personal firewall is loaded has no affect. However, after the PC is rebooted causing the VPN client to be reloaded into memory, an error message is generated indicating the file has been corrupted. The resulting log messages show the machine is not running in secure configuration. For the modified *local.dt* file configuration, refer to Item 21.

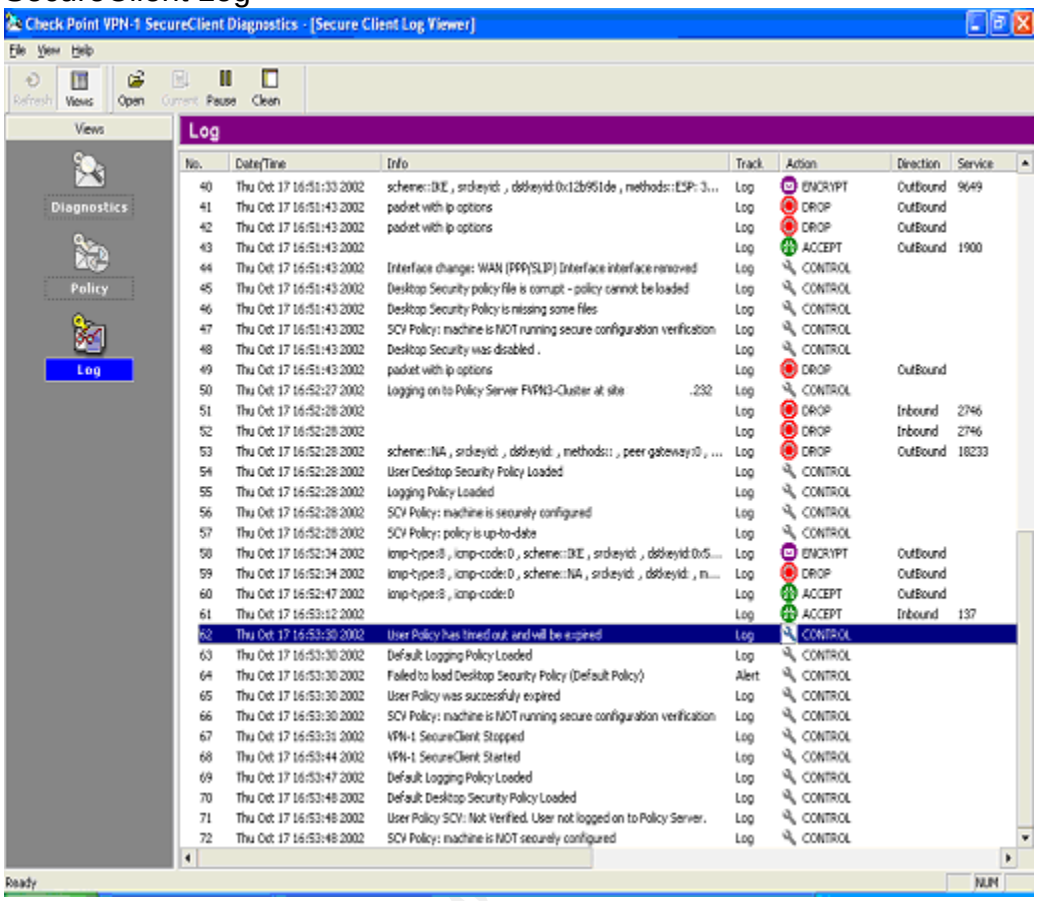
SecureClient Log



Error message

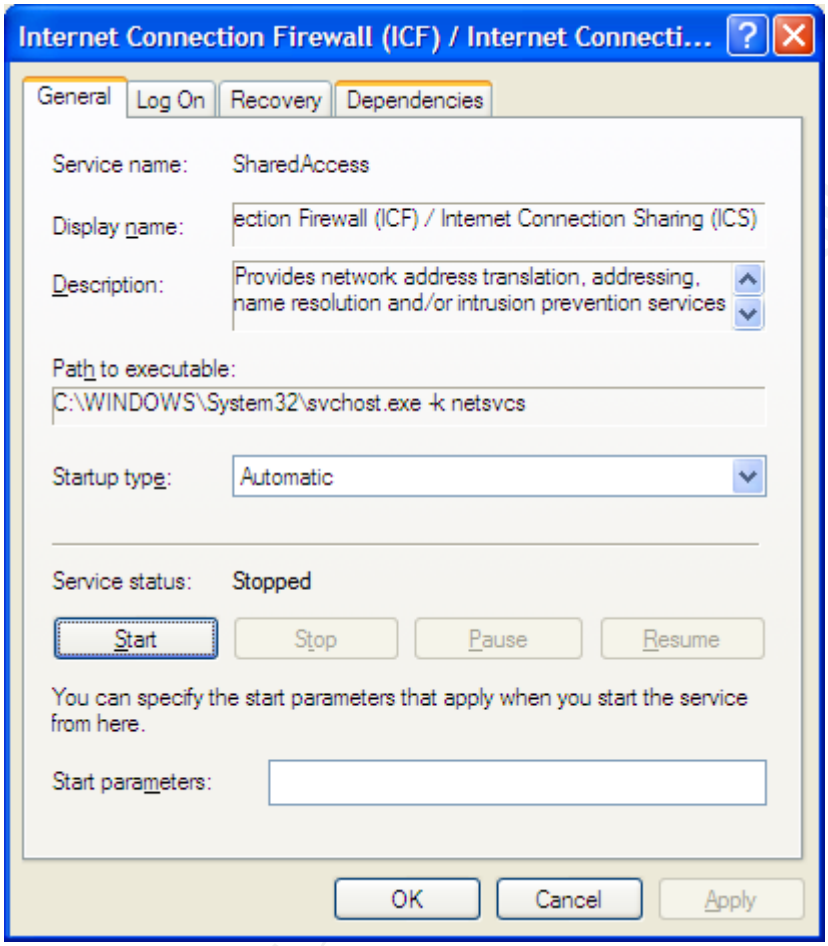


SecureClient Log

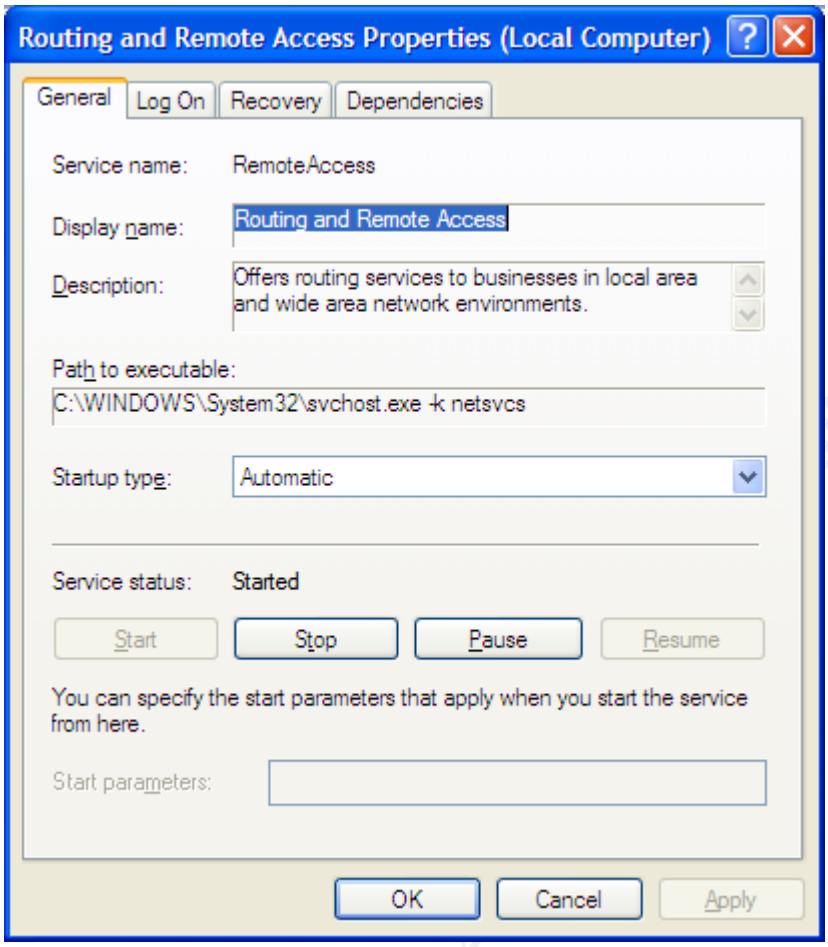


Item 2 – IP Forwarding Disabled (Internet Connection Sharing)
Audit Finding 1 Test result – **FAIL**

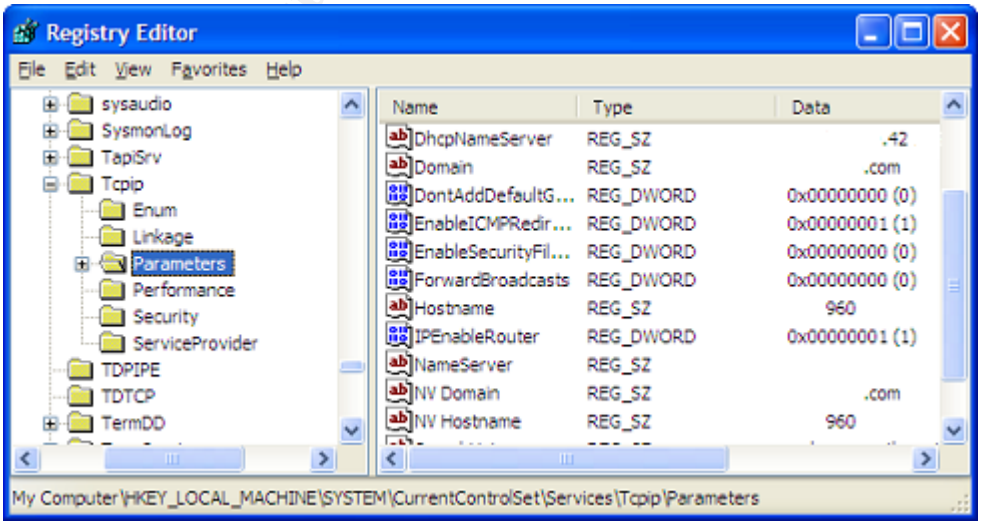
The following screen shows the Internet Connection Firewall configuration window. The *Service Type* is set to automatically start win the machine is booted. Note, in this window, the *Service Status* displays Stopped because there is no activity at the time the window was captured.



Routing and Remote Access screen print showing service is enabled.

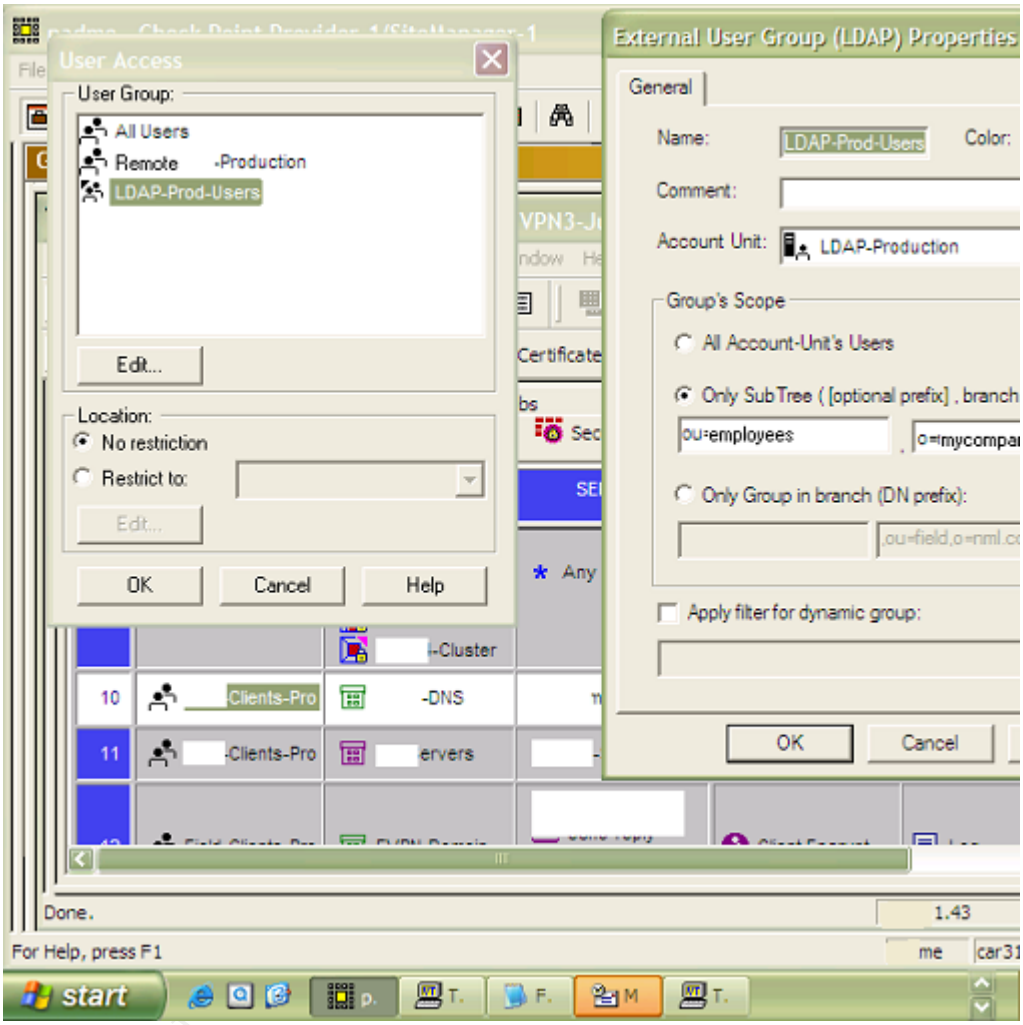


Registry setting confirming that IPEnableRouter is set to one.
HKEY_LOCAL_MACHINE\System\CurrentControSet\Services\Tcpip\Parameters\IpEnableRouter

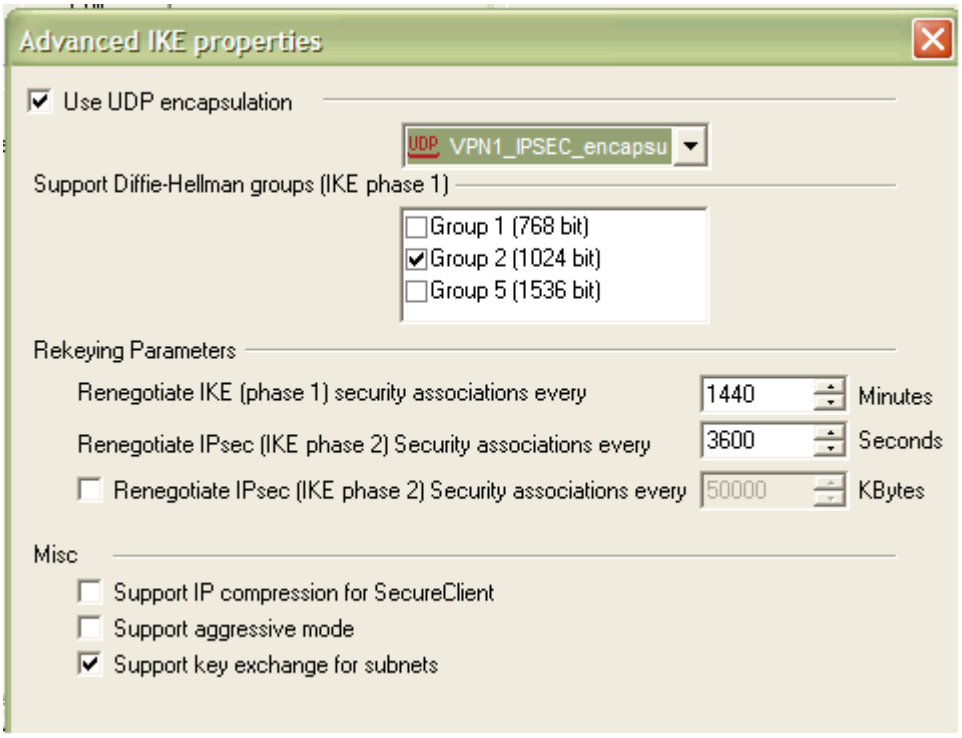


Item 4 – User authentication process. Audit Finding 2
Test result – **FAIL**

The screen print displays an incorrect *ou=employees*. It should display *ou=remote.* Because of this setting, the employee's container can authenticate and access resources through the firewall and the remote users cannot.

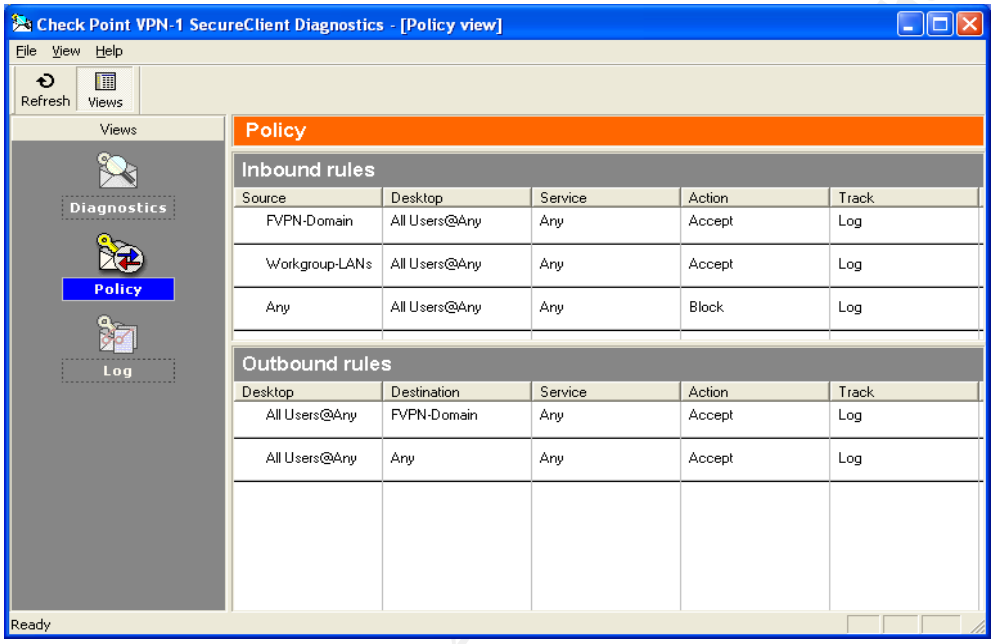


Item 5 – IKE Mode used to authenticate users.
Screen shot of management server showing aggressive mode is not enabled.
Test result – **PASS**



Item 6 – LAN functionality is not affected by VPN.
Test result – **PASS**

The following screen print shows the active rules for inbound and outbound connections for the PC. Rule 2 of the inbound rule set shows all connections from the LAN workgroup are accepted. *Additional tests of printing to a LAN printer from a LAN connected PC and sharing files across the LAN were performed to verify these rules did not interfere with LAN functionality but the results of these tests are difficult portray in this format.



Item 8 – PC is still protected by SecureClient firewall if tunnel is disabled.
Test result – **PASS**

With Personal Firewall disabled (including VPN tunnel), the PC is vulnerable on the Internet without a broadband router with NAT enabled on it. The report below was created on a dial-up connection to the Internet.

Attempting connection to your computer. . .
Shields UP! is now attempting to contact the **Hidden Internet Server** within your PC. It is likely that no one has told you that your own personal computer may now be functioning as an **Internet Server** with neither your knowledge nor your permission. And that it may be serving up all or many of your personal files for reading, writing, modification and even deletion by anyone, anywhere, on the Internet!

Preliminary Internet connection established!
Your computer has accepted an anonymous connection from another machine it knows **nothing** about! (That's not good.) This **ShieldsUP!** web server has been permitted to connect to your computer's highly insecure NetBIOS File and Printer Sharing port (139). Subsequent tests conducted on this page, and elsewhere on this website, will probe more deeply to determine the extent of this system's vulnerability. But regardless of what more is determined, **the presence and availability of some form of Internet Server HAS BEEN CONFIRMED within this machine . . .** and it is accepting anonymous connections!

The phrase you must remember is:
"My port 139 is wide OPEN!"

Remotely connected to your NetBIOS system!
This computer is exposing its internal NetBIOS networking protocol over the Internet. This is called "NetBIOS over TCP/IP" or "NBT" for short. This is a security risk because it gives **anyone in the world** a point of entry to your system. Connecting to your computer is **NOT** something that anyone on the Internet should be allowed to do **. . .** but we've just done it! The following pages provide information about the consequences and your options for increasing your system's security.

Your computer's name is: VD002 / WORKGROUP.
This is an example of some of the information about you and your computer that is leaking out onto the Internet and is openly available to **anyone**. Such information is commonly used as a starting point for guessing your name and/or your passwords and learning more about who you are.

Your computer is exposing NO SHARES to the Internet.
Either your computer has no shared resources (disk drive directories or printers) or they are effectively hidden from external view and attack. This is beneficial for your security because exposed shares can provoke system intrusion. However, allowing unknown persons or software anywhere in the world to connect to your system without your knowledge still affords them the opportunity to poke holes in your system's security.

Also, as you can see below, **significant personal information** is still leaking out of your system and is readily available to curious intruders. Since you do not appear to be sharing files or printers over the TCP/IP protocol, this

system is **relatively secure**. It **is** exposing its NetBIOS names (see below) over the Internet, but it is refusing to allow connections, so it is unlikely that anyone could gain casual entry into your system due to its connection to the Internet.

Disconnecting from your computer. . .

Your System's Internet Connection Security Synopsis:

This system's silent NetBIOS over TCP/IP (NBT) Internet Server is **actively advertising its existence across the Internet** and thus inviting equally silent connection and intrusion into your system. We were just now able to **connect to your computer** and establish a dialog with it, asking for its name and other information. That is the first step in breaking into a system. Automated "hacking tools" already exist to scan the Internet looking for computer targets **exactly** like this one **. . .** and then silently cracking any passwords you may be using to "protect" those resources.

Your system is not exposing ANY shared resources to the Internet. That's very good. But as you can see, the fact that there's a computer here is still completely exposed and dangling out there on the Internet for everyone to see and to cause people to wonder what might be here.

When user authentication occurs, the personal firewall is enforced on the PC. This minimizes the vulnerability of the PC to the Internet. This is not an indication of the presence of a VPN tunnel, merely that the SecureClient Firewall is enforcing the rules. The following test displays the same ShieldsUP! Test previously run without the SecureClient Firewall enabled.

Attempting connection to your computer. . .

Shields UP! is now attempting to contact the **Hidden Internet Server** within your PC. It is likely that no one has told you that your own personal computer may now be functioning as an **Internet Server** with neither your knowledge nor your permission. And that it may be serving up all or many of your personal files for reading, writing, modification and even deletion by anyone, anywhere, on the Internet!

Your Internet port 139 does not appear to exist!

One or more ports on this system are operating in FULL STEALTH MODE! Standard Internet behavior requires port connection attempts to be answered with a success or refusal response. Therefore, only an attempt to connect to a nonexistent computer results in no response of either kind. **But YOUR computer has DELIBERATELY CHOSEN NOT TO RESPOND** (that's very cool!) which represents advanced computer and port stealthing capabilities. A machine configured in this fashion is well hardened to Internet NetBIOS attack and intrusion.

Unable to connect with NetBIOS to your computer.

All attempts to get **any** information from your computer have **FAILED**. (This is **very** uncommon for a Windows networking-based PC.) Relative to vulnerabilities from Windows networking, this computer appears to be **VERY SECURE** since it is **NOT exposing ANY** of its internal NetBIOS networking protocol over the Internet.

The following trace route shows an unsuccessful attempt to find the SecureClient PC. This trace route was run from an outside computer to the SecureClient PC with the firewall enabled.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\vb804>ping aaa.bbb.ccc.51

Pinging aaa.bbb.ccc.51 with 32 bytes of data:

Request timed out.

Ping statistics for aaa.bbb.ccc.51:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
C:\Documents and Settings\vb804>tracert aaa.bbb.ccc.51

Tracing route to 1Cust51.tnt1.milwaukee.wi.da.uu.net [aaa.bbb.ccc.51]
over a maximum of 30 hops:

  1   108 ms    91 ms    92 ms  abc.def.ghi.7
  2    89 ms    90 ms    90 ms abc.def.ghi.1
  3    93 ms    91 ms    93 ms  bc.def.252.41
  4   126 ms    97 ms    97 ms  gbr1-p29.cgcil.ip.att.net [bc.deg.5.154]
  5    99 ms    93 ms    90 ms  gbr4-p00.cgcil.ip.att.net [bc.def.5.218]
  6    91 ms    90 ms    89 ms  ggr1-p370.cgcil.ip.att.net [bc.deg.5.149]
  7    92 ms    93 ms    92 ms  cde.fgh.168.57
  8    93 ms    94 ms    89 ms  0.so-3-1-0.XL2.CHI2.ALTER.NET [abb.ccd.71.97]
  9    95 ms   100 ms    92 ms  0.so-7-0-0.HR2.CHI2.ALTER.NET [abb.ccd.73.49]
 10    95 ms    94 ms    93 ms  160.ATM3-0.DR4.CHI5.ALTER.NET [abb.ccd.65.157]
 11   111 ms   139 ms   100 ms  tnt1.milwaukee.wi.da.uu.net [ee.ff.1.134]
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *     ^C
```

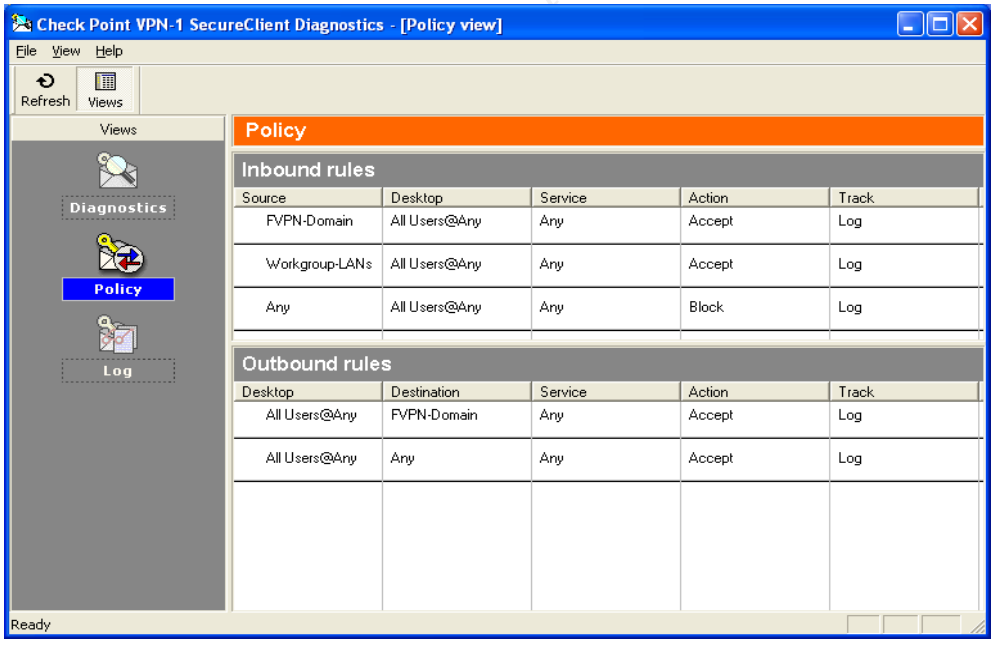
Item 11 – Unnecessary services disabled on firewall. Audit Finding 3
Test result – **FAIL**
The following display from NMAP shows unknown ports open on the corporate firewall.

```
# nmap (V. 3.00) scan initiated Wed Nov 13 12:40:22 2002 as: nmap -sT -n -v -r
-p1- -P0 -oN nmap-full-80 XXX.XXX.XXX.80
Interesting ports on  (XXX.XXX.XXX.80):
(The 65529 ports scanned but not shown below are in state: filtered)
Port            State           Service
264/tcp         open            bgmp
500/tcp         closed          isakmp
18207/tcp       closed          unknown
18231/tcp       open            unknown
18262/tcp       closed          unknown
18264/tcp       open            unknown

# Nmap run completed at Wed Nov 13 13:29:02 2002 -- 1 IP address (1 host up)
scanned in 2920 seconds
```

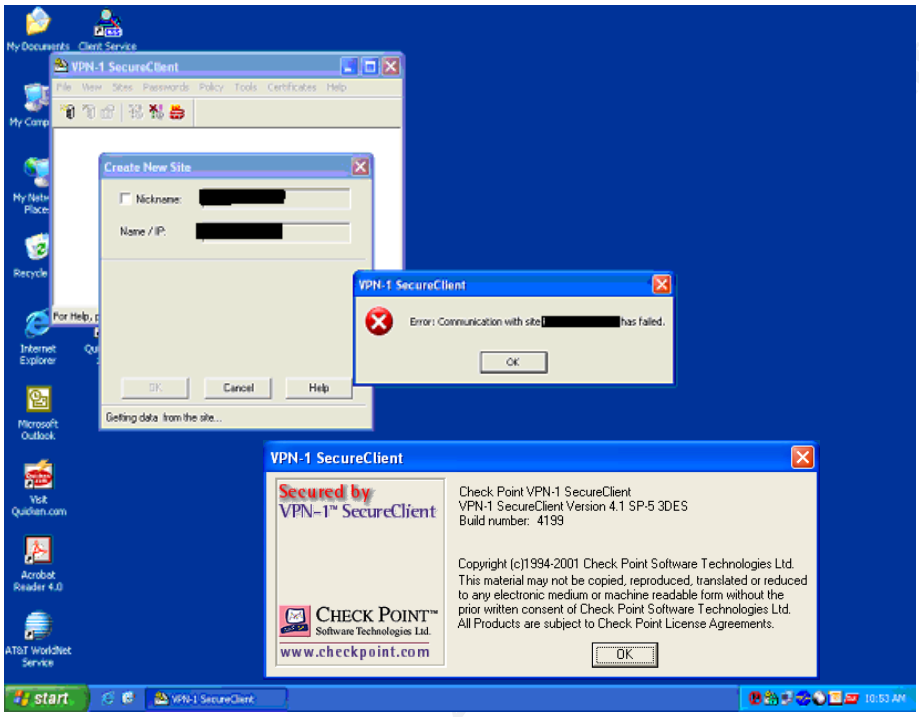
BGMP = Border Gateway Multicast Protocol
ISAKMP = Internet Security Association and Key Management Protocol

The following screen print shows the rule set for the SecureClient. The third rule states that any source, to all users, for any service is blocked and logged. This passes the test.



Item 14 – Attempt to establish VPN connection from application other than SecureClient.
Test result – **PASS**

The following screen prints are the result of trying to attempt with the Checkpoint 4.1 SecureClient to site 208.xxx.xxx.xxx, which is the gateway. The firewall rejects the connection attempt and the authentication window is not displayed. The result is a failed connection attempt.



Item 16 – Firewall change control
Test result – **PASS**
The following test displays a sample change control document. Step 4 of this checklist item listed the following information as needing to be present.
The person making the change is authorized, a brief description of the change itself, date/time of change, reason for change, administrators approval for the change, back-out plan is thoroughly documented.

Change Title: Firewall Changes: Week of 10 June, 2002
Effective Date/Time: 06/13/2002 05:30 PM
Implementer: Firewall admin 1 **Requester:** Firewall admin 1
Main Categories: WAN **Others Affected:** <none>
Change Driver: Client Initiative **Implement. Risk:** Low
Approver: Change Control Board

Change Description
REMOTE CLIENT FIREWALL CHANGE: 1) MSAPPP0340M00 (172.xxx.xxx.xxx) needs FTP PUT/GET access with the Test Network (10.xxx.xxx.0).

Client Impact
Departments Affected By This Change: None
Visual Differences: Client will be enabled to access necessary resources
Login/Logout Or Configuration Files Being Updated: None
Client Impact If Change Results In Problems: Requested access will not be available.
Impact Of Not Implementing The Change: Requested access will not be available.

Planning
Testing Status: Not possible to test **Implementation Plan:** Yes
How long will Imp. take: 00 Hour(s) 10 Minutes
Checkout Plan: Yes there is a plan
Implementation Plan Details: Changes will be staged prior to implementation at 5:30pm
Checkout Plan Details: Client is responsible for checkout after change is implemented.

Infrastructure Impact
Field: Not affected **Business:** Not affected
Remote Offices: Not affected **Remote Clients:** Not affected
Details Regarding the Above Affected Areas:
Hardware Adds\Changes\Deletes: None **Software Adds\Changes\Deletes:**None
Web Sites Affected: None **Systems\Applications Affected:**None
Systems availability during implementation: Available

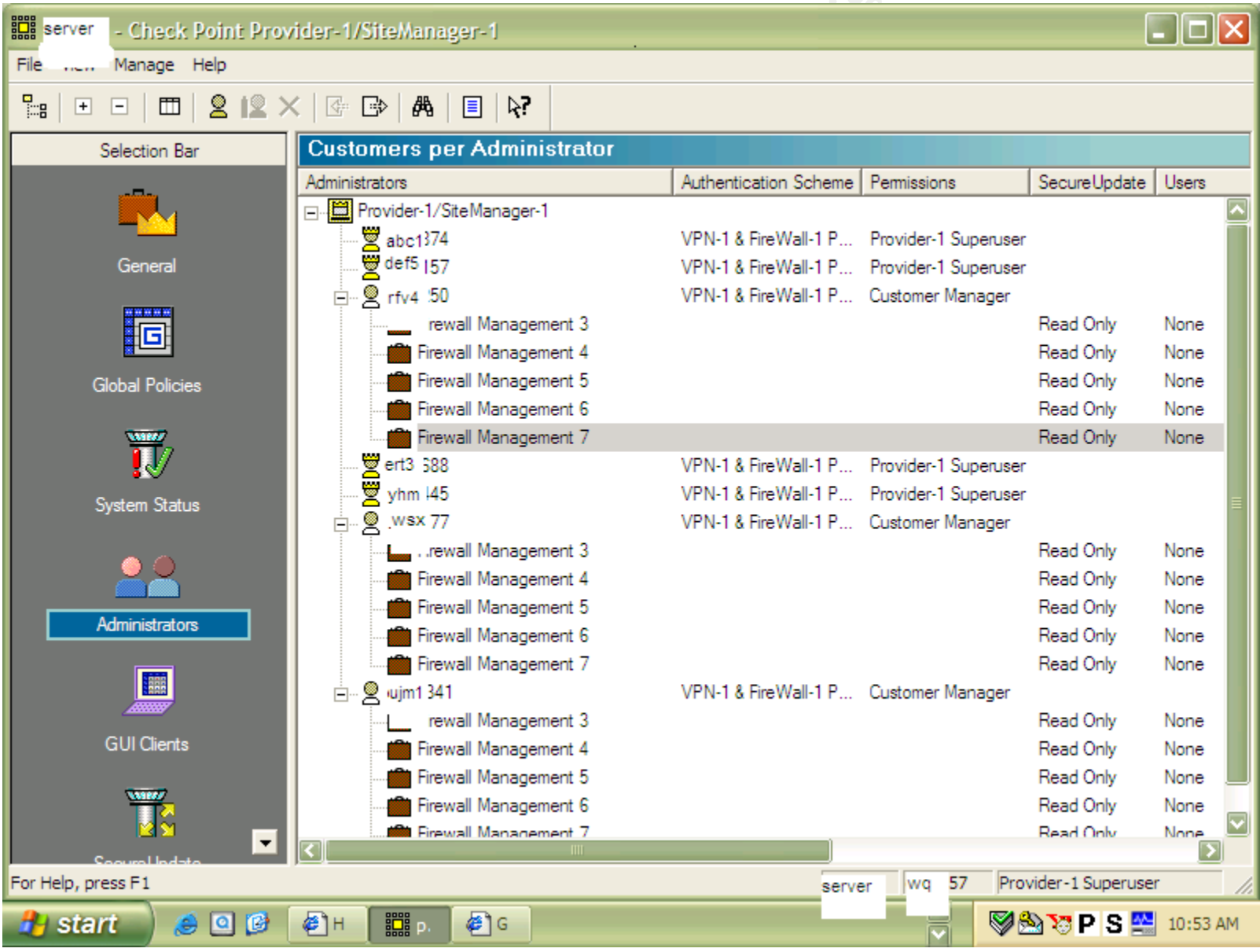
Contacts
Primary Contact: Firewall admin 1 **Pager\Cell\Home Numbers:** 1234
Secondary Contact: Firewall admin 2 **Pager\Cell\Home Numbers:** 3456

Action By Others(Clients, Computer Operations, NSD)
Client Action:none CO Action: none NSD Action: none

Backout
Backout Plan: Yes **Time to Backout:** Hour(s) 10 Minutes
Who will make backout decision: Firewall admin 1
Who will backout and test the systems: Firewall admin 1

Backout Plan Details: Remove requested changes.

Item 17 – Administrator access
Test result – **PASS**
The following screen shot from the management server displays number of administrators. The administrators labeled firewall management / customer manager are groups of users with read only access to the predefined firewall(s). Administrators are indicated by a crown icon and are the true firewall administrators with full permissions. The permissions are defined by clicking on the GUI Clients icon located underneath the Administrators icon. The number of administrators displayed here (4) is appropriate for the environment within which this firewall is defined (4000 + employees and 10,000 remote users).



Item 20 – No verification of files or parameters pushed to client. Audit Finding 4
Test results - **FAIL**

Listed below is a section of a *local.dt* file that contains an error (The file location is *C:/program files/checkpoint/SecureRemote/policy* on the SecureClient PC). The error can be seen in the definition for the *(net-abc.456.0.0) network.* In the *IPADDR* parameter the defined address is for *(abe.456.0.0) not (abc.456.0.0).* This error results in the abe.456 network being allowed access to the client machine. As stated in the other steps of this item, these files should contain information approved by the business area and should be verified by an administrator other than that one who configured the files to ensure accuracy.

```
: (Field-01-Networks
      :type (group)
      : net-10.2xx.0.0
      : net-10.2xx.0.0
      : net-10.2xx.0.0
      : net-10.2xx.0.0
      : net-10.2xx.0.0
      : net-10.2xx.0.0
      : net-10.2xx.0.0
      : net-10.2xx.0.0
      : net-10.2xx.0.0
      : net-10.2xx.0.0
      : net-10.2xx.0.0
)
: (Field-02-Networks
      :type (group)
      : net-ghj.32.0.0
)
: (net-abc.456.0.0
      :type (network)
     :ipaddr (abe.456.0.0)
:netmask (255.255.0.0)
```

Measuring Residual Risk

The criteria of this audit focused on policies and procedures regarding the use of VPN technology and an examination of the implementation of that technology. The work performed (based on the entire checklist, not just those items listed in Assignment 3) revealed no policies or procedures to govern the use of VPN functionality, either for the remote user or host company. This lack of policies is setting a poor precedent for the future use of technology solutions.

Some consideration must be given to the environment in which this VPN solution resides. The remote users are not company employees, thus, they are not obliged nor inclined to follow corporate procedures. The machines upon which the SecureClient is installed are purchased and owned by the remote users. This further limits the nature of the security solution the company can impose on these users and their machines. While these constraints are understandable, the users should consider the risk to the corporate network. It is a catch-22 situation: in order to create business the company must provide access to its resources to external non-employee users, and the remote users, in order to conduct business on behalf of the company, must have the flexibility to run their own businesses. While it is an unpopular and perhaps an unrealistic point of view, users should be able to understand the company's need for security and should therefore tolerate a few small inconveniences in order to greatly reduce the risk to the company.

The technology piece of the audit went much smoother. Though some software limitations were encountered, for the most part the technology used has the ability to be quite secure, if properly configured. Most of the weaknesses discovered in the technology portion of this audit resulted from inappropriate configurations. Listed below are the significant areas discovered in the course of this audit where residual risk remains.

- IP Forwarding Disabled.
  - As a requirement of the implementation of SecureClient, this setting is to be automatically disabled by the installation package. However, this does not negate the user from enabling the option after installation. This is a very cost effective solution and provides for a much better user experience, provided the user does not enable the option. If the user enables the option, it is likely the VPN session will not work, which will result in calls to Technical Support.
- User Authentication Process
  - This is solely based on accurate configuration of the authentication parameters in the management server. A very inexpensive correction to make should an error be made, however, the magnitude of the error is quite large, since a mis-configuration prohibits the correct group of users from authenticating. A preventive control would be to have the configuration reviewed by a different administrator prior to moving to the production environment.

- Unnecessary services / ports enabled on corporate firewall.
  - Since any open port or enabled service provides some level of risk, completely removing this risk is unrealistic. However, regular scans of the firewall can provide a measure of preventive control by ensuring that only the necessary services / ports are enabled. This is a very inexpensive solution compared to the potentially huge problem of unknown services / ports remaining enabled.
- Accurate file configurations and parameter settings.
  - Since the client is not responsible for the SecureClient, the responsibility of correctly configuring the files and parameters needed to utilize the VPN resides with the VPN/Firewall administrators. The accuracy of these files and settings is critical to the security of the system. To ensure accuracy the company should impose dual verification of the settings. This is a very low cost solution and will significantly improve the accuracy of the files being pushed to the client and the settings required for the secure operation of the VPN.

Overall, the residual risk is well within acceptable tolerances. The additional controls necessary to add greater assurances of file / parameter accuracy are very inexpensive to implement. Additional items not detailed in Assignment 3 where risk remains include:

- VPN Policies – A very easy and inexpensive item to correct.
- Session Management – Not based on amount of inactivity, a limitation of the Checkpoint Software.
- NAT router – If compromised, very dangerous to SecureClient residing behind it. Internal addresses could be revealed resulting in very directed attacks of network resources. Appropriate router configuration and regular independent review of that configuration is likely to prevent significant problems from occurring.
- NG revocation certificate should be created with external interface address to prevent revealing internal address. This is another configuration that should be reviewed by an independent administrator an is very inexpensive. ** Note, this is item is not detailed in Assignment 2 or 3. It is the result of later research but included here for awareness.*

Given the nature of the scope and the controls defined, the work of the audit achieved the desired control objectives.

System Auditability

Based on the objectives of the audit, the system does contain an area that is not realistically auditable. This item is identified below. With this area noted, the remaining portion of the system is auditable once management defines policies governing the use of VPN technology.

- Encryption / tunnel settings are defined by the gateway management server for the firewall. There are several options available (UDP encapsulation, various Diffie-Hellman groups, hybrid mode, etc.). To verify that the actual encryption method selected is actually working is beyond the capabilities of most auditors. However, a mitigating control test can be performed to verify encapsulation/encryption is taking place. A sniffer can be used to view the data passing through the VPN. This will assure the auditor that the traffic between the gateway and client is indeed encrypted.

Assignment 4

Audit Report

Executive Summary

The Checkpoint NG VPN environment consists of Client software (SecureClient) and host software (Checkpoint VPN-1 firewall and associated hardware). This environment provides the primary means of connectivity to corporate resources by remote field users.

The objectives of this audit were to examine the policies and procedures associated with the use of VPN technology and to review the technical configurations for appropriateness and accuracy. Based on these criteria, the control objectives of the audit were met and the VPN system is operating within acceptable risk tolerances except for the items identified below.

A summary of the audit findings are presented below.

- The Windows XP Internet connection sharing is not disabled. This prevents the Checkpoint SecureClient to authenticate to the host gateway.
- User authentication to host resources is inappropriately configured. This allows unauthorized users to establish a VPN connection to the host.
- Unnecessary services and/or ports are open on client and host firewalls. By enabling unneeded services / ports, attackers can utilize these services or ports to launch attacks, resulting in information theft, denial of services, infiltration of remote machines, etc.
- Verification of file / configurations pushed to remote user machines. Errors in the configuration files pushed to client machines by the host could result in unauthorized access to host or client resources by inadvertently enabling access to a foreign/unknown network or specific address.

Audit Findings

Audit Finding 1

Assignment 3 Cross reference = Item 2 – IP Forwarding Disabled (Internet Connection Sharing on Windows XP)

The Internet connection sharing function on the remote client's Windows XP machine was not disabled. Testing revealed that SecureClient does not support IP Forwarding, enabling this option prevents a user from establishing a VPN session with the gateway.

Audit Finding 2

Assignment 3 Cross reference = Item 4 – User authentication process

The LDAP configuration setting for organizational unit was incorrect. The parameter was set to *OU=EMPLOYEES.* It should have been set to *OU=REMOTE.* This setting allows employees to authenticate to the remote user VPN when policy states that only remote users are to access this VPN network.

Audit Finding 3

Assignment 3 Cross reference = Item 11 – Unnecessary services disabled on firewall – host and client

On the host machine, not all unnecessary services / ports were disabled. These services / ports are not being used on the host VPN gateway and should be disabled so an attacker could not exploit them and gain access to the internal network by going through the firewall.

On the client machine, the third inbound rule allows all source addresses access. This restricts nothing and should be changed so that only necessary services are allowed as inbound traffic.

Audit Finding 4

Assignment 3 Cross reference = Item 20 – No verification of files or parameters pushed to client

The *local.dt* file contained an error allowing a specific unauthorized external network access to the client machine. The *local.dt* file is a configuration file pushed to the client from the management server during authentication. Because this file is defined and maintained by the corporate administrators, the client has no control over the contents of this file. Since this file is pushed to all remote clients when they authenticate to the gateway, this error is magnified significantly.

Background / Risk

Item 2 - The Windows XP Internet connection sharing is not disabled. This prevents the Checkpoint SecureClient from authenticating to the host gateway. By not being able to authenticate to the host, the client is unable to conduct

business using the VPN, and therefore the user has a bad experience with the VPN which directly relates to calls to the company support area and damage to company reputation.

Item 4 - User authentication to host resources is inappropriately configured. This allows unauthorized users to establish a VPN connection to the host. By not configuring the authentication parameters correctly, remote users are denied access to resources necessary to conduct business and are thus subject to a poor user experience, resulting in increased calls to the support center and reputational damage. Additionally, by defining the wrong user group to the authentication process, unauthorized users can establish a VPN connection to the host and access all resources defined to remote users. This could result in confidential information being stolen, data loss and fraud.

Item 11 - Unnecessary services and/or ports are open on client and host firewalls. Potential attackers are constantly scanning the Internet looking for machines with vulnerabilities, such as enabled services and ports. By enabling unneeded services / ports, attackers can utilize these services or ports to launch attacks, resulting in information theft (from both the client and host company), denial of services, infiltration of remote machines through Trojan programs, viruses, etc.

Item 20 – Lack of verification of pushed files or parameters to remote user machines. Errors in the configuration files pushed to client machines by the host could result in unauthorized access to host or client resources by inadvertently enabling access to a foreign/unknown network or specific server(s). The accuracy of these configuration files is vital to the success of the VPN. If the files are inaccurate, potential intruders are allowed access to user or host resources, the user's machine is subject to compromise and the host network is at risk from unintended access, depending on the error in the rule set. By granting this access through the rules or configurations, Illegitimate traffic may go undetected for some time, resulting in bigger losses or damage. These losses could be from data corruption / theft, rebuilds of machine(s), support time, administrative resources and the associated costs of each.

Audit Recommendations

Recommendation for Item 2 –Disable Internet Connection Sharing.

This client system setting should be configured appropriately during the installation process of the SecureClient software. The corporate programming staff should routinely develop and test the necessary code to induce the appropriate configuration on behalf of the user. The user should not be expected to understand the necessary system configurations needed to enable the desired results of the software.

Recommendation for Item 4 – Establish a user authentication process.

The parameters defining user authentication should be tested and approved prior to moving to production. Changes should be automatically migrated from the test environment to the production environment, thus eliminating the possibility of manually configuring production machines. If changes cannot be migrated automatically, then a separate administrator should review the configurations for accuracy prior to their implementation.

Recommendation for Item 11 – Disable unnecessary firewall services.

Client – While client requirements dictate no LAN or other functionality be impacted by the use of SecureClient, the firewall rules enabled on the client should be strengthened. The inbound rule set should be hardened to accept only the traffic (TCP/IP, HTTP, etc.) necessary to conduct business. This could possibly be achieved by defining a secondary rule set that is enabled once the VPN connection to the host has been terminated.

Host – All unnecessary services and ports should be disabled on the corporate VPN gateway. Additionally, a port scan tool should be run monthly against the firewall to ensure only the necessary services are enabled.

Recommendation for Item 20 –Verify files or parameters pushed to client.

The files / parameters defining system settings and rule sets that are pushed to remote users should routinely be reviewed, tested and approved prior to pushing to the remote users machines. A procedure / process should be developed where two administrators are required to review and signoff all files being pushed to remote users.

Costs

For the following section company size is assumed to be large with at least 10,000 users, and costs are defined as follows:

Inexpensive: $0 to $10,000
Expensive: $10,000 to $50, 000
Very expensive: > $50, 000

Recommendation for Item 2 – Disable Internet Connection Sharing.

The cost to implement this recommendation is defined by the costs to develop and test this function within the SecureClient installation process, which is probably Inexpensive. Additionally, the costs for implementation of this feature are likely offset by the savings from decreased support desk calls.

Recommendation for Item 4 – Establish a user authentication process.

If an automated process for moving changes between production and test environments must be developed, this is Expensive and likely not worth the investment in relation to this particular risk. The other option of having two administrators review and signoff on all configurations is Inexpensive and is primarily comprised of the administrators' time since it shouldn't take long to verify the accuracy of the configurations.

Recommendation for Item 11 – Disable unnecessary firewall services.
Client – The development of another rule set to be activated by the disconnection of the VPN session is likely Expensive, given that the Checkpoint Software is not currently designed to accommodate such a change. A secondary option of conducting regular port scans, while Inexpensive, is somewhat problematic, since the host company does not own the remote users machines and has little or no say over how they are maintained. It may be possible to establish a contractual arrangement with a third party to perform regular maintenance on the users machines which could possibly include such regular scans.

Host – Conducting regular port scans of the corporate VPN firewall(s) is Inexpensive because very good scanners are available free from the various Internet sites. This should be part of regular network / firewall maintenance procedures.

Recommendation for Item 20 – Verify files or parameters pushed to client.
This recommendation is primarily procedural and Inexpensive, as it is comprised primarily of a limited amount of administrator time. Any cost involved with ensuring the accuracy of these files pales in comparison to the reduced support desk calls and the exposure from inaccurate files.

Compensating controls

Recommendation for Item 2 – Disable Internet Connection Sharing.
If the development cost were deemed prohibitive, one alternative would be to rely on the user to disable this option. A defined procedure explaining how to disable this option would be required along with the support area contact information.

Recommendation for Item 4 – Establish a user authentication process.
If the automated process was considered impractical and the time cost of two administrators was excessive, verification of the administrator's configuration could be reviewed by a junior staff member, whose time is not billed at the same rate.

Recommendation for Item 11 – Disable unnecessary firewall services.

Client – A compensating control to the dual client side rule sets is to have the primary rule set enforce the more restrictive functionality. This option however is likely to be impractical because of the repercussions from the users. Management is unlikely to be willing to force their controls on remote users who are independent of the corporate entity.

Host – I can think of no compensating controls, regular port scans of the corporate VPN firewall(s) should be conducted.

Recommendation for Item 20 – Verify files or parameters pushed to client. Again, as in recommendation 4 above, the best compensating control to the time of two administrators being cost prohibitive is to have the verification of the administrator's configuration performed by a junior staff member.

Sources and Research:

1) Jenner, Simon. "Virtual Private Networks (VPN): The Insecure Solution." February 20 2002. URL: http://www.infosecnews.com/opinion/2002/02/20_02.htm (20 September 2002).

2) Le Grand, Charles H. "Virtual Office: Risk Management, Security, Control and Auditing." URL: http://www.theiia.org/ecm/printfriendly.cfm?doc_id=870 (2 November 2002).

3) Spitzner, Lance. "Auditing your firewall setup." 12 December 2000. URL: http://www.enteract.com/~lspitz/audit.html (5 November 2002).

4) Spitzner, Lance. "Building your firewall rulebase." 26 January 2000. URL: http://www.enteract.com/~lspitz/rules.html (9 November 2002).

5) Ray, Loye. "Security Audit Checklist". – as cited by Dan Strom. "Auditing the Netscreen-5 Firewall used as a VPN gateway." SANS GCNA assignment v. 1.0 August 16 2001.
URL: http://polaris.umuc.edu/~lray/ifsm430/security-audit.htm.

6) Shue, Lily "Security, Audit and Control of VPN." URL: http://www.isaca-la.org/2002_Spring_Conference/Handouts/S1%20Security%20Audit%20and%20Control%20of%20VPN.pdf (October 2002).

7) Checkpoint Desktop Security Guide NG FP2. The Open Group: Checkpoint Technologies. 21 March 2002. 66-67, 120-122.

8) Gibson, Steve ShieldsUp! Tool. URL: http://www.grc.com.

9) National Security Agency Security Recommendation Guides. 24 October 2001. URL: http://www.nsa.gov/snac/cisco (9 November 2002).

10) Nmap by Fyodor. http://www.insecure.org/nmap/. November 2002.

11) Ethereal network analyzer. URL: http://www.ethereal.com. November 2002.

12) Brenton, Chris Mastering network security. Alameda: Network Press. Sybex Inc. 1999. 320-349.

Last Updated: July 25th, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS AUD507 (GSNA) @ Canberra 2017	**Canberra, Australia**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**