Global Information Assurance Certification Paper

Remote Access VPN – Security Concerns and Policy Enforcement

Michael Stines
GSEC Practical 1.4b – option 1

I. Abstract

With growing numbers of individuals working remotely, telecommuting or traveling with increasing frequency, the traditional business security model continues to evolve. Nearly gone are the days where the remote user may dial directly into a RAS server at the corporate office and access data on the remote network. With the advent of widely available high-speed broadband Internet access coupled with VPN technologies; the secure, clearly defined perimeter many organizations once enjoyed becomes a bit less distinct.

During the evaluation and planning of a VPN solution, it is imperative to understand the associated security risks that are associated with this technology. With the implementation of a remote-access VPN, the concept of providing data confidentiality, integrity and availability must be extended to address the remote VPN client, which has direct access to the parent corporation's protected network resources. This paper serves to review the business reasons for the implementation of remote access VPN, to address security policy considerations, and subsequent enforcement of security policy through the use of a Cisco Concentrator and Zone Labs' Integrity Server. Realizing there are numerous manufacturers marketing diverse methods of VPN implementation, focus will be solely upon the Cisco 3000 Series Concentrator for remote user access; and Zone Labs' Integrity Server for enforcement of policy, thus allowing for specific details to be addressed – rather than paint a broad, general picture.

II. Business Considerations

Today's business needs include access to information. This information may reside on a corporate database, fileserver or intranet. Remote users require a secure, cost effective and expedient method of access to this data. It is these reasons, coupled with the fact that the majority of businesses have already adopted the Internet for business functions, which are responsible for the rapid adoption of VPN technologies by business today. With growth rates predicted to continue through 2004 at an impressive rate of 70 – 80% annually, VPNs have already become a standard for remote access. [1] According to a recent Gartner study of more than 300 companies "…90% of U.S. companies with at least 500 employees and two sites use VPN solutions to provide secure access to home workers. The study also found that 79% of companies use VPNs to connect mobile workers." [2]

The lure of VPN centers on several factors, including cost savings and scalability. Remote access VPNs serve to reduce costs with savings on connection charges and increased productivity. As VPN clients connect to the corporate network via dialup Internet or broadband Internet access, the expenses incurred by supporting dedicated RAS lines and associated long distance charges are diminished. [3] With broadband DSL or cable access becoming increasingly price competitive, high-speed speed remote access becomes a reality. Rather than dialup RAS services that are inherently slow, telecommuters with broadband access have the ability to connect to the corporate office via VPN at speeds that allow them to work in a more productive fashion. Likewise, as increasingly larger numbers of hotels offer high-speed Internet connections, mobile workers are able to work more effectively through the use of remote access VPNs.

Using a selection from the Cisco 3000 Series Concentrator family of products, an organization can satisfy their remote access VPN needs. Included free of charge with the Cisco 3000 Series Concentrator is the VPN Client software. The VPN Client software is used to establish a secure, end-to-end encrypted tunnel to the Concentrator. The client may be pre-configured and deployed in mass. Additionally, VPN access policies and configurations are pushed seamlessly to the client upon successfully connecting with the Concentrator, requiring little user intervention. [4] Cisco offers a range of Concentrator models that can fulfill the needs of the smallest of companies to the major enterprise. With the 3000 Series Concentrator, the latest VPN technology can be used to reduce communications expenses and enhance productivity. Each of the Concentrator models combines the most advanced encryption and authentication techniques available to the market today with high availability, high performance and scalability. Cisco offers five models in their concentrator family: [5]

VPN 3005 Concentrator caters to small- and medium-sized organizations. This model supports up to a full-duplex T1/E1, and up to 100 simultaneous VPN sessions. Encryption is handled via software. This model does not have upgrade capabilities.

VPN 3015 Concentrator offers the same out-of-the-box capabilities as the 3005 model, however the 3015 offers the availability to be upgraded to the 3030 or 3060 models – as dictated by growing business needs.

VPN 3030 Concentrator targets medium to large organizations requiring bandwidth throughput of a full T3/E3, with 50 Mbps maximum performance. The 3030 Concentrator supports a maximum of 1500 simultaneous VPN sessions. SEPs (Scalable Encryption Modules) are available to provide hardware-based acceleration functionality. The 3030's are available in redundant and non-redundant configurations, and can be upgraded to the 3060 model.

VPN 3060 Concentrator is designed for the demands of a large organization. Offering bandwidth capabilities ranging from fractional T3 through full T3/E3 or greater, with 100 Mbps maximum performance. The 3060 Concentrator supports up to 5000 simultaneous VPN sessions, is available in redundant and non-redundant configurations, and can utilize SEP modules for hardware-based acceleration.

VPN 3080 Concentrator supports large enterprise organizations whose demands include the highest level of performance and support for up to 10,000 simultaneous sessions. The 3080 is available only in fully redundant configurations.

III. Security Concerns

While the potential savings and employee productivity increases that come with a remote-access VPN is significant and attractive to business, advance consideration must be given to the initial efforts required to plan, implement and monitor the technology. These considerations should be documented and addressed within security policy. Additionally, it is recommended by Cisco that security policies be in place prior to the deployment of any security technology. [6] Also supporting the implementation of security policy to address VPN concerns is Russ Cooper of TruSecure, a global leader in managed security services. Cooper's stance is that policies are needed to strengthen security measures and serve as educational resources to users and system administrators. According to Cooper, "What is needed are improved security policies that crack down on sloppy practices, like allowing employees to alter the configuration of company-supplied hardware in order to facilitate file sharing and Web browsing at home". [7]

A cause for concern with the deployment of a remote-access VPN is the diffusion of the existing network perimeter. By allowing access via VPN to the corporate network, an untrusted host is essentially gaining access to the secure intranet. It is important to note that while the VPN connection offers secure connectivity between the client PC and the corporate network, it does not offer personal security features to the client, or protect it from outside attack from sources such as the Internet. The VPN connection is in place to provide data confidentiality and integrity as well as authentication services. Should the remote host be compromised, the attacker could use this compromised system as a means of entry into the corporate network. As many, if not most, end-user PC's have little security measures in place, the end-user PC when connected to the Internet is a much easier target than the corporate network. The unsecured PC is open to password harvesting, infection by virus or worm, could unknowingly serve in a Distributed Denial of Service attack - any of which could conceivably have adverse effects if introduced into the corporate network via VPN connection. [8] To reduce exposure to the corporate network, VPN users should be prevented from opening a VPN session to the corporate office, and leaving the connection

established. This is of particular concern to remote users with broadband Internet access, due to the 'always on' nature of the connection. Security policy should address the VPN session connect time of the VPN clients, and require that a session be terminated after a prescribed period of idle time has elapsed.

IV. THE VPN CLIENT PC AND SECURITY POLICY

In order to lessen the exposure of the corporate network to outside sources, there are a number of matters to consider, and around which fashion security policy. Areas of concern with the VPN client that should be addressed include: the potential hazards of the 'always-on' nature of broadband Internet connections, installation of personal firewalls, antivirus software, and the remote PC itself.

Analysis of the remote VPN client PC begins with considerations made to the PC itself. It is recommended that security policy require the VPN host be company-issued equipment, rather than using the existing users personal property. This eliminates problems associated with mixing business and personal applications, files and activities. Under company ownership it is easier to require the end user to comply with policy, and insist the PC be used only for business-related purposes. As the hardware is company-owned, users are not given administrator account rights on their desktop machines. Controlling user activity as well as checking and maintaining desktop integrity is very difficult (if not impossible) when users have complete control through administrator rights. Company provided hardware also serves to minimize management issues, as the computer should remain relatively static - with no unauthorized software installations, end-user configuration changes or device conflicts to troubleshoot, support calls are consequently reduced.

In addition to requiring all service packs and appropriate hotfixes to be in place, security policy should require that a personal firewall AND antivirus software be installed, operating, and using the most current configuration file(s). A managed antivirus package is highly recommended, such as those marketed by major antivirus vendors such as McAfee, Symantec and Trend Micro, among others. Using a managed antivirus solution allows for a single point of administration and monitoring – allowing for more effective management of the client. In considering a managed antivirus product, the central console should allow an administrator to manage policies and keep servers and workstations updated and properly configured. A managed antivirus product also allows the administrator to lock down client settings to prevent users from changing the prescribed configuration. If a virus is detected, it is automatically repaired and the central console is alerted.

Security policy should require a personal firewall in addition to an antivirus product. As with antivirus software, numerous quality personal firewall products are available from vendors such as Zone Labs, Sygate and Symantec, among

others. While antivirus software can help avoid virus problems on the client, it does not secure against hacker attacks. Firewall software allows inbound access to needed ports, and closes those that are unneeded. Some firewall software products will also monitor outgoing traffic as well; allowing only trusted applications outbound access to the Internet. [9] It is this type software firewall that should be a required by policy. Without the firewall, information stored on the VPN client is subject to compromise. Corporate data, passwords, and proprietary information – all are open for unauthorized access while connected to the Internet. As with antivirus products, managed personal firewalls are available, and highly recommended. Zone Labs, manufacturer of Zone Alarm offers such a solution. Zone Labs Integrity consists of an agent that resides on the client machine, and server - a central management point that allows the administrator to create, monitor and enforce policy from a central console. In addition to serving as a personal firewall, Zone Labs Integrity serves to harden network security by communicating with the Cisco VPN 3000 Concentrator to ensure only trusted VPN client PC's are authenticated and allowed access to the corporate network.

The VPN client's Internet connection is a factor to consider in creation of VPN client security policy. As broadband Internet availability continues to grow and prices become increasingly competitive – it is certain that a number of an organization's VPN clients will be using broadband Internet access. Due to the increased bandwidth available, coupled with the fact the broadband client is 'always on' and will have a static IP, or an IP address that changes infrequently – the broadband client has greater exposure to attack than the dial-up client. It is imperative the broadband client have a personal firewall and antivirus software current and running at all times. Due to the 'always on' nature of broadband access, security policy may require broadband clients to shutdown their machines when not in use. While not exclusive to broadband access, security policy should also limit the idle time of a single VPN session. This is to prevent the VPN user from connecting to the corporate network and leaving the session open and unattended for an extended period of time.

V. Security Policy Enforcement

Means of enforcement of security policy should be a primary consideration throughout the research, test and implementation phases of any security technology. Careful research, review of manufacturer's documentation, questions presented to vendors and manufacturers, and testing of the technology can serve to meet this criteria. Without a method of enforcement, effectiveness of security policy is questionable at best. While audit trails, hardware analysis and security logs should be reviewed regularly; it is a time-intensive process and this alone alerts the administrator to violations and security threats after they have occurred. Without a means of enforcement, the administrator is risking the security of the corporate network by relying upon the remote VPN users to voluntarily comply with policy. As the secure network perimeter is being

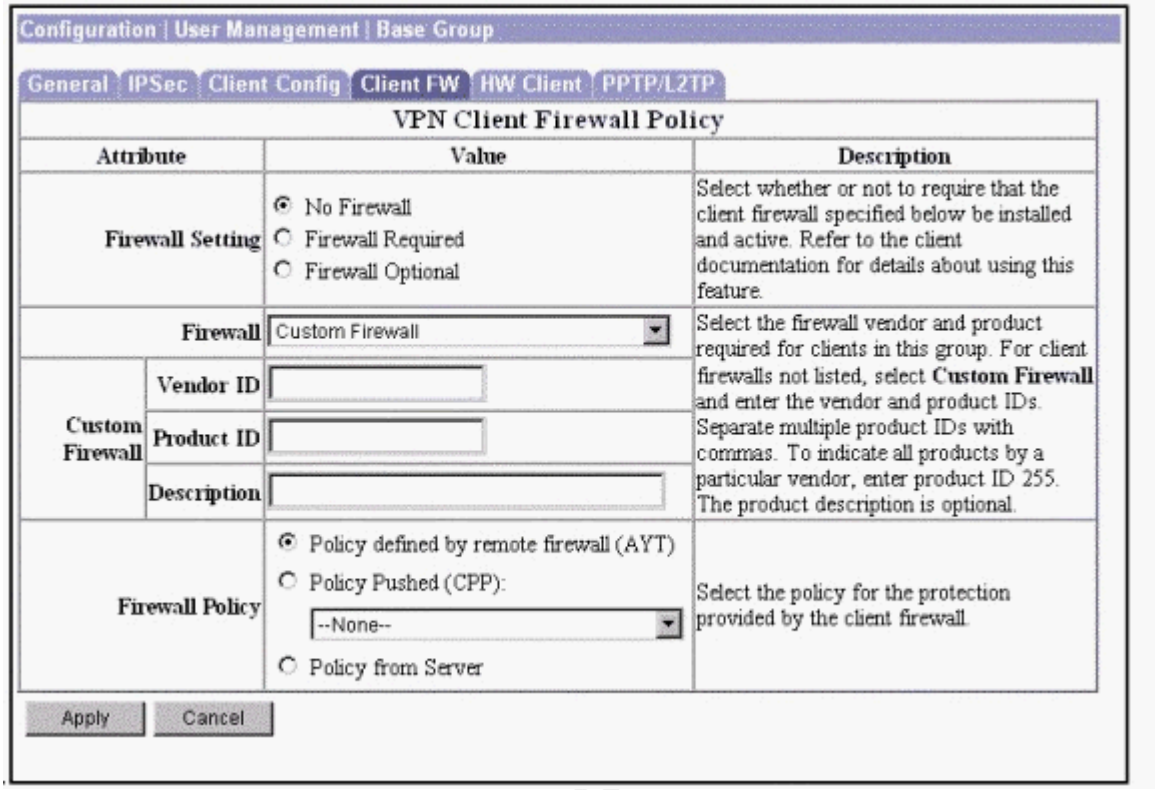
extended to encompass the VPN client, security policy must be enforced in 'real-time' to protect the integrity of both the VPN client and the corporate network.

Having addressed security policy issues that require the VPN client to have antivirus software installed and using the latest update; policy also requires a properly configured personal firewall to be running on the client PC, and also requires a time limit on inactive VPN sessions. How is this to be made obligatory, and remove the responsibility from the VPN user to voluntarily comply with policy? The answer is as stated above – by defining the need and carefully researching solutions available to fulfill this need. The Cisco VPN Concentrator, a managed antivirus package, and Zone Labs Integrity will fulfill the dictated requirements.

Cisco VPN Concentrator

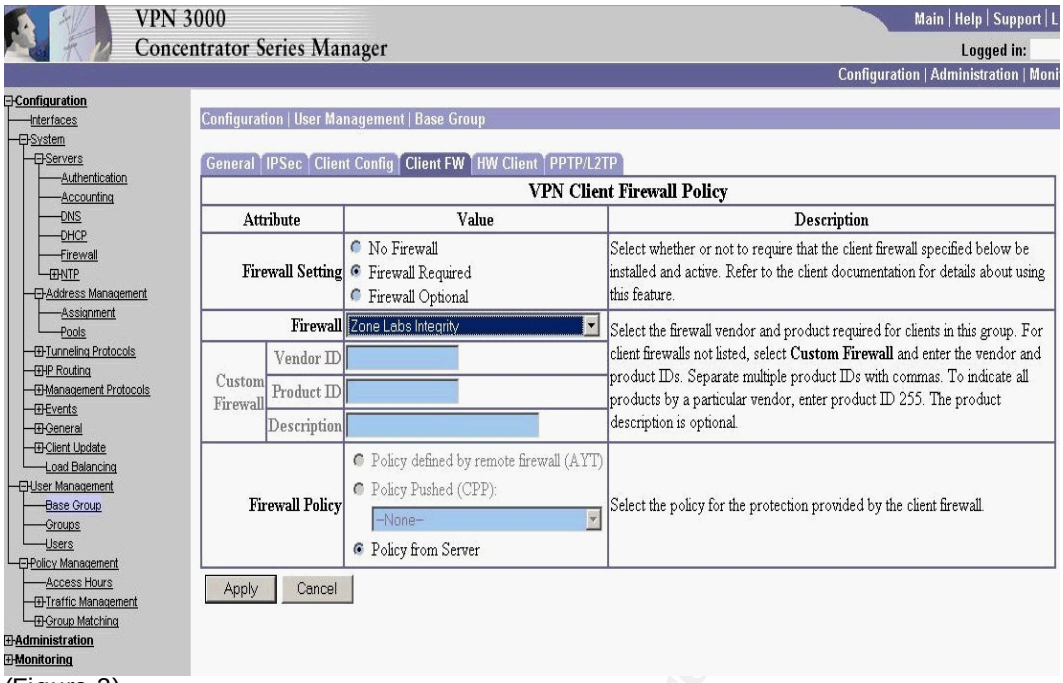
It is with the VPN Concentrator that the remote VPN clients initially communicate. The Concentrator functions as a point of entry into the corporate network, serving to authenticate and authorize access based upon credentials the remote client presents to the Concentrator. The Concentrator in turn, has the ability to audit the remote client to determine if the client meets the prescribed requirements to complete the connection. For ease of administration, the Concentrator allows VPN users to be added to groups. Configuration changes to a group will in turn affect all members of the given group. Additionally, the Concentrator has a default group, named "Base Group". Any manually created groups are subsets of the Base Group, meaning that changes to the Base Group may be universal to all VPN users and groups. When the administrator creates VPN user groups he/she will then determine what values should or should not be inherited from the Base Group. As the overall configuration of the Concentrator is outside the scope of this paper, focus will be upon noted requirements to fulfill security policy.

To require that the VPN client have a personal firewall installed, the administrator selects **Configuration** -> **User Management** -> **Groups** -> **Modify Groups** – **Client FW**, which will present the following selection: (Figure1)



(Figure 1)

By default, the Cisco Concentrator does not require a firewall, and has the additional options of "Firewall Required" and "Firewall Optional". Simply select the "Firewall Required" radio button to require all users in the group to have a personal firewall on the client. Then, in the "Firewall" drop-down selection, choose "Zone Labs Integrity" (Figure 2). At this point the "Policy From Server" radio button becomes automatically selected. This configuration will require that all users in the group have the designated personal firewall installed on the client PC. The Concentrator will drop any session attempting to connect without the required firewall installed and running. Click "Apply" and all configuration changes are saved within the Concentrator.



(Figure 2)

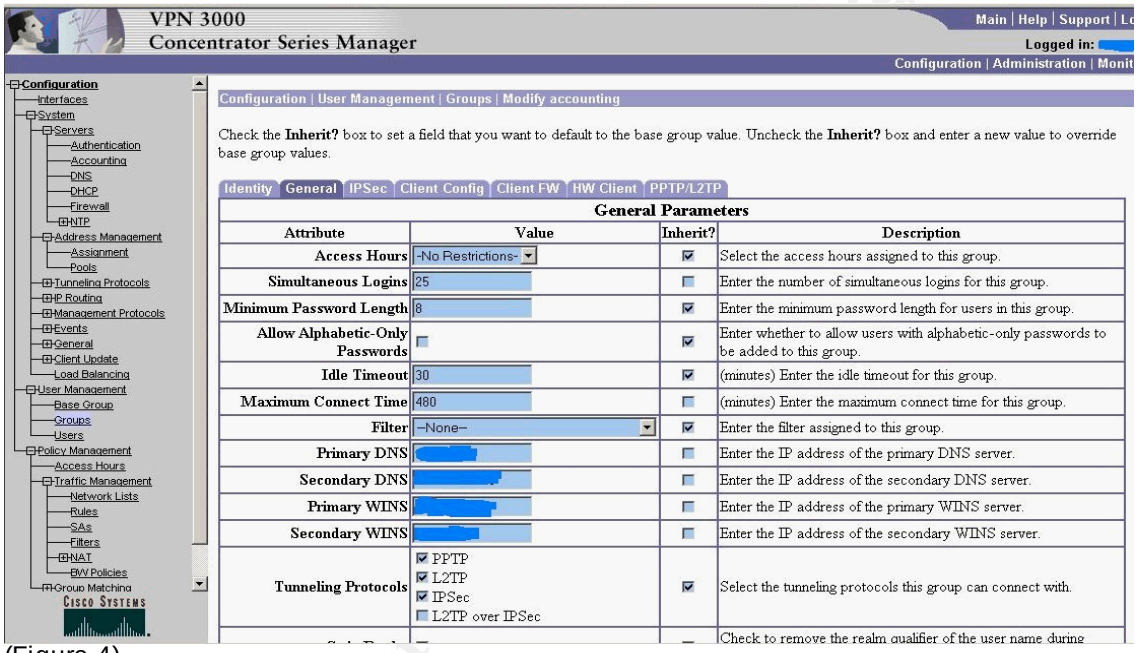
Next, the Integrity Server must be defined within the Concentrator. This may be done by selecting **Configuration** -> **System** -> **Servers** -> **Firewall Server**, which will present the following: (Figure 3)

(Figure 3)

The administrator must then enter the IP address of the Zone Labs Integrity server, thus allowing the Concentrator to communicate with the Integrity Server.

It is the Integrity Server which maintains policies for remote VPN client PCs and monitors connection attempts to ensure policy compliance. Details of the Integrity Server are to follow. Again, click "Apply" and configuration changes are saved within the Concentrator.

Finally, to enforce the security policy requirements of termination of inactive VPN sessions, the administrator must configure the parameters for this to take effect. The "Idle Timeout" attribute may be viewed by selecting **Configuration** -> **User Management** -> **Groups** -> **Modify Group** -> **General**, and the following will be displayed: (Figure 4)



(Figure 4)

The administrator then inputs the timeout value – in minutes. If there is no communication activity on a given VPN session within this time period, the VPN session will be terminated. The user then must re-authenticate with the Concentrator to access the corporate network. Click "Apply" and the configuration changes are saved.

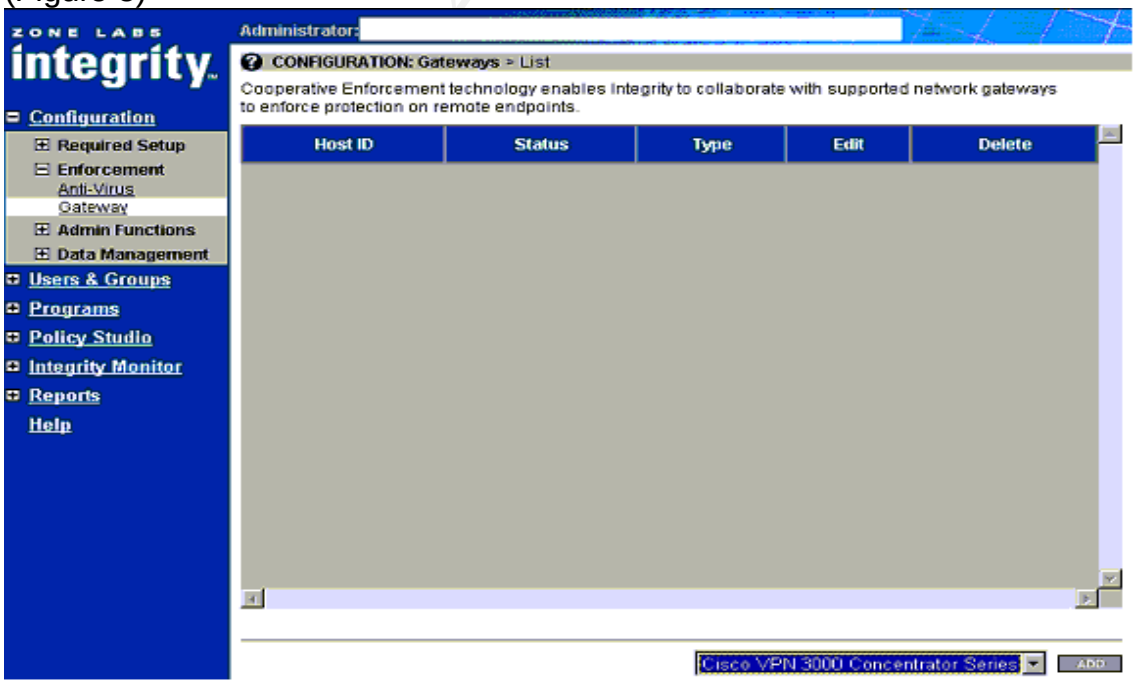
Zone Labs Integrity Server

Although the Cisco Concentrator can be configured to require the VPN client to have a personal firewall installed and functioning, the Concentrator does not verify the configuration of the personal firewall. Zone Labs Integrity fulfills this purpose. The Cisco Concentrator and Zone Labs Integrity work in unison to ensure only trusted VPN clients have access to the corporate network. The Concentrator performs authentication and authorization services when a VPN client attempts to establish a connection. Upon successful authentication, the Integrity Server is responsible for verifying the Integrity Agent is installed, running

and properly configured. The Integrity Server functions as central console for administration of both the Clients and the Server, and offers granular configuration options. Through these operations, the Integrity Server enforces policy and protects the network in depth: [10]

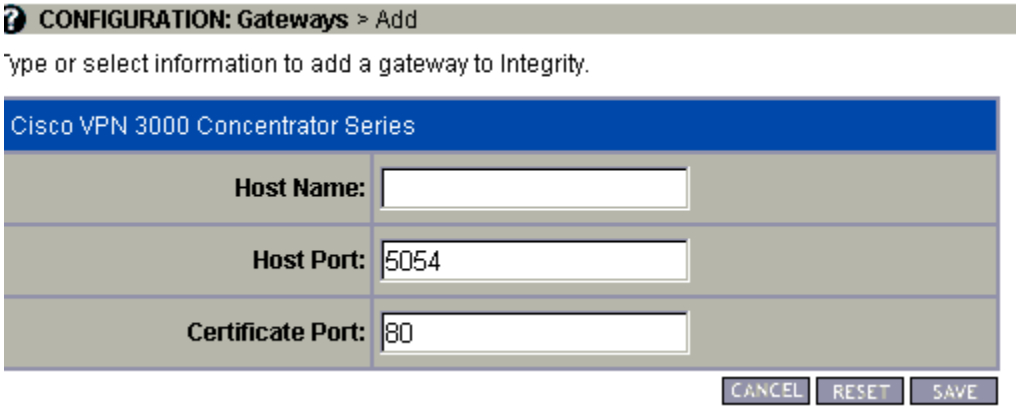
- Maximum Remote Access Protection – hardens network security by cooperating with antivirus and Cisco VPN solutions to insure only trusted PC's access the corporate network.
- Serves as a distributed firewall with application control - blocking hacker attacks by preventing unauthorized connections, both inbound and outbound.
- Web Management Tools – centrally distributes, maintains and administers security policy from a central location
- Policy Lifecycle Management – management tools for the lifecycle of security policy monitoring, creation and enforcement.
- Monitor User Applications – inventory user applications to identify and secure vulnerabilities.

Upon installation, the Integrity server soon begins to fulfill its role in security policy enforcement. The Integrity Server must be configured to communicate with the Cisco Concentrator, VPN groups defined to mirror the groups as they appear within the Concentrator, and policy deployed to the defined groups. As the Concentrator was configured to recognize the Integrity server, likewise the Integrity Server needs to be configured to communicate with the Concentrator [11]. At the main console, the administrator selects **Configuration** -> **Enforcement** -> **Gateway**. The administrator is then presented the following: (Figure 5)



(Figure 5)

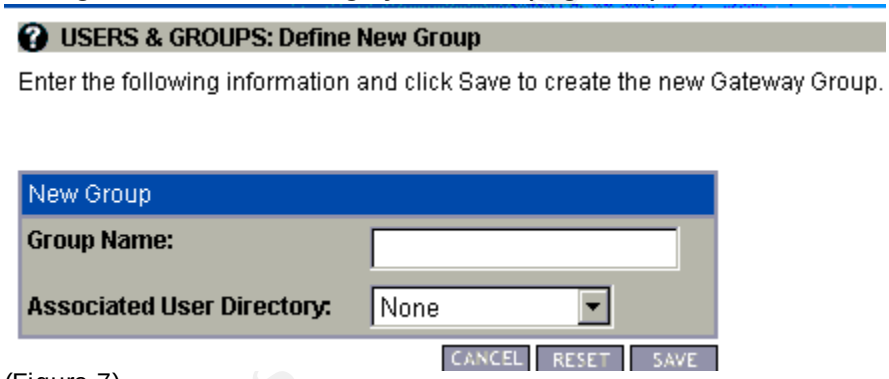
The “Cisco VPN 3000 Concentrator is the default entry in the drop-down menu. By selecting Add, the following is displayed: (Figure 6)



(Figure 6)

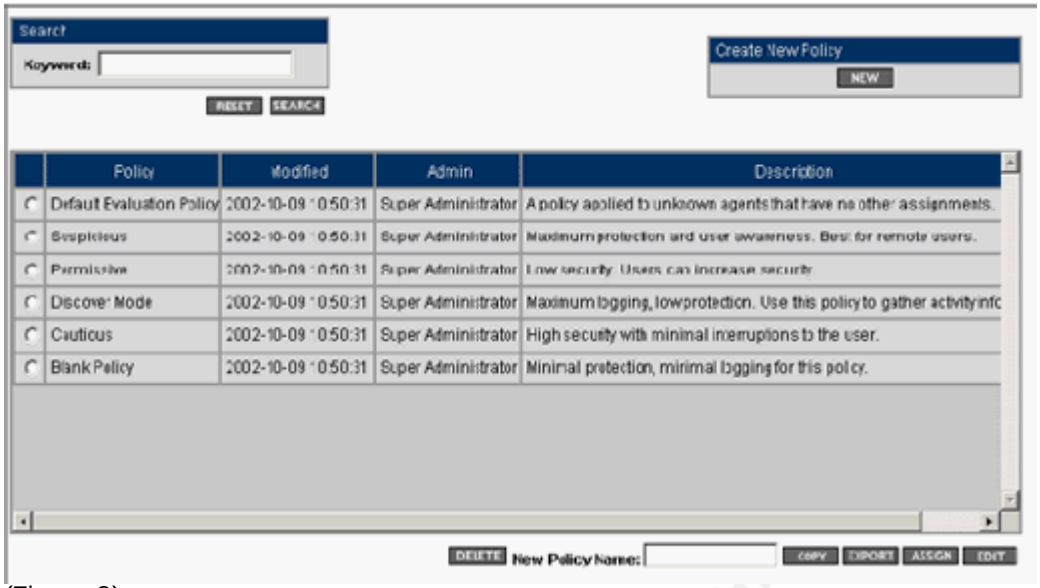
The IP address of the Concentrator is input into the “Host Name” field, the “Host Port” and “Certificate Port” retain their default entries and “Save” is selected.

At this point, selecting **Users & Groups -> Define Gateway Groups** -> **for Gateways** creates groups to mirror those as defined within the Concentrator. Click the ‘Add’ button to define a new group. The group name must be entered precisely as it appears within the Concentrator. Then click ‘Save’ to add the configuration to the Integrity Server: (Figure 7)



(Figure 7)

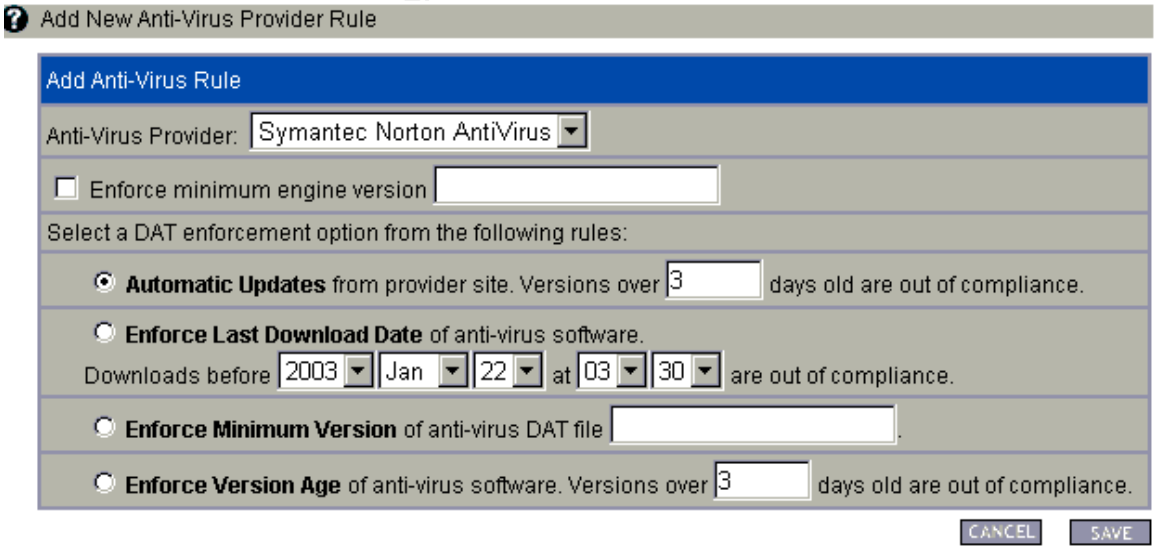
Following group definition, a policy is created, applied to the group and deployed. During installation, policy templates are provided as a method of rapid deployment of policy to VPN clients. Policy may be defined as permissive or restrictive as the administrator likes, and it can automatically block unauthorized connection attempts with no ongoing administration required. Upon successful connection to the corporate network, the Integrity Server automatically pushes the appropriate policy to the Integrity Agent residing on the client PC. Policy templates reside in the “Policy Studio” of the Integrity Server. After logon to the Integrity Server application, the administrator selects **Policy Studio** from the main administrative console window, and is presented with the following: (Figure 8)



(Figure 8)

It is recommended to copy an existing policy, and make revisions to the newly created copy – thus saving the original in its unchanged condition, should unexpected results arise. Selecting the radio button of the policy to be copied and then click 'Copy' creates the copy. The policy may then be edited by selecting the radio button of the newly created policy and clicking 'edit'.

Security policy should require VPN clients to have anti-virus software installed and current in both engine and dat file. To configure the Integrity Server to audit VPN clients and verify the client meets security policy requirements, edit the newly created policy, select **Client Settings**, and scroll down to **Anti-Virus Cooperative Enforcement** section, click **Add**. (Figure 9)



(Figure 9)

Integrity Server supports McAfee VirusScan, Symantec Norton AntiVirus and Trend Micro PC-cillin. Select the appropriate product in the drop down menu. Input the values of the antivirus minimum engine, select the method of enforcement of minimum dat file required to successfully connect to the corporate network. Click 'Save' and the requirements are saved to policy.

It is now time to assign the policy to the group and deploy the policy to the VPN clients. Policy is assigned within Policy Studio by selecting the radio button of the policy to be deployed, clicking '**Edit'**, selecting the **'Policy Assignments'** folder tab, scroll down to **'Assigned Groups'**, click **'Add or Remove'**, select the group(s) as previously created, click **'add'**, and finally – click **'save'**. At this point the policy is assigned to the group and is ready for deployment. Click **'Deploy Policy'** and the policy is pushed to the Integrity Agent residing on the VPN client PC – and security policy enforcement is under way! Security policy requirements of current antivirus software, properly configured personal firewall, and timeout of inactive sessions are now fully enforced. Voluntary compliance is removed from the user and is now required to successfully connect to the corporate network.

VI. SUMMARY

With the implementation of any new technology, it is imperative to fully consider the associated security risks. The reasons for implementing a remote-access VPN are numerous and sound. However, careful consideration must be given to the risk involved. The Cisco Concentrator and Zone Labs Integrity Server are but one method of many which may be used for successful remote-access VPN implementation and enforcement of security policy. Any organization that currently possesses, or is considering a remote-access VPN solution is strongly encouraged to evaluate the security threat posed by remote workers. If this risk is ignored, there is significant potential for a network security breach and loss of data. The recommendations contained within this paper can assist in a secure and successful implementation of a remote-access VPN.

References:

[1]. Munroe, Courtney. "Internet Growth Fuels IP VPN Growth: Corporate Confidence Increases in Lease Line Alternative" May, 2000
http://www1.worldcom.com/ca/products/internet/uusecure/whitepapers/idcvpn1.pdf

[2]. Greengard, Samuel. "Extended Networks:VPN" March/April 2000
http://business.cisco.com/prod/tree.taf%3Fasset_id=83323&public_view=true&kbns=1.html

[3]. About.com "Introduction to VPN"
http://compnetworking.about.com/library/weekly/aa010701c.htm

[4]. Cisco.com Data Sheet "Cisco VPN Client Data Sheet"
http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_data_sheet09186a008011c35b.html

[5]. Cisco.com Data Sheet "Cisco VPN 3000 Series Concentrator"
http://www.cisco.com/warp/public/cc/pd/hb/vp3000/prodlit/vpn3k_ds.htm

[6]. Convery, Sean; Saville, Roland "Extending the Security Blueprint to Small, Midsize, and Remote-User Networks"
http://www.cisco.com/en/US/netsol/ns110/ns129/ns131/ns128/networking_solutions_implementation_white_paper09186a008009c8a0.shtml

[7]. Roberts, Paul "Secure Twice, Open Once"
CSO Magazine November 2002 (2002): page16

[8]. Murray, Andrew Conry "Securing End Users from Attack"
Network Magazine October 2002 (2002): pages 28 – 32

[9]. Zone Labs Data Sheet "Why do I need a Firewall?"
http://www.zonelabs.com/store/content/catalog/whyFirewall.jsp

[10]. Zone Labs Data Sheet "New Threats, New Solutions: Enterprise Endpoint Security"
http://download.zonelabs.com/bin/media/pdf/IntegrityOverview_final.pdf

[11]. Zone Labs Integrity Document Library "Volume II - Installation and Configuration Guide"
Zone Labs Document 1-0204-0200-2002-12-13