Global Information Assurance Certification Paper

GIAC Enterprises

VPN Uses in Small Business

By

Rimbert M. Rivera

Global Information Assurance Certification Information Security Officer

GISO Practical Assignment v.1.1

May 2002

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

INTRODUCTION

Virtual Private Networking (VPN) is a process of securing the connection between a trusted network and another host or network through the encryption of the transmission between them through an untrusted network, commonly, the Internet. VPN is frequently used for connecting mobile users to a company's network and other offices to each other. This paper will describe the GIAC Enterprises (GIACE), a company that uses VPN for these reasons as well as increasing security to the File Transfer Protocol (FTP). FTP was originally designed for transferring files to the general public, e.g., downloading drivers and patches. Because of this, FTP security was not a factor in its design, which is evident in its transmission in clear text of user names and passwords. GIACE uses FTP as their main delivery method to provide their customers with proprietary data – quite the opposite use from its original design. Along with VPN, GIACE increases FTP's level of security through the use of IIS and private IP addressing. Even though FTP lacks built-in security, GIACE values it for its robust and established method of delivery through the Internet.

GIAC ENTERPRISES OVERVIEW

Nature of Business

GIAC Enterprises (GIACE) is a small, privately owned entertainment news organization specializing in the music industry. Based in Washington, DC, their 50 employees are spread out between three other small offices (less than five people) at Chicago, Los Angeles and New York City, as well a number of roaming reporters around the country. They employ mostly well-respected musicians to cover the events and personalities of mainstream American music. What sets GIACE apart is their depth of reporting. Recognizing larger media organizations satisfactorily cover the breadth of the music industry, GIACE focuses on acquiring in-depth stories not of well-established acts, but those who they feel are on the brink of making a huge impact in the U.S. market. In fact, GIACE is becoming known for recognizing the upcoming trends in the nation as GIACE coverage of a rock band usually translates into both critical acclaim and financial success of the act. The reporters accomplish this not through a few hours of interviews, but by spending months, and sometimes years, with the personalities. Due to the recent interest and success of reality shows, the demand for GIACE reports from the bands' loyal following has been growing. The frequency of their reports has been approaching real time as the reporters submit their work almost as soon as history is made. The GIACE customer base is comprised mostly of band fan sites that post GIACE stories to attract fans to their web site. Some of their coverage is also bought by the larger, more traditional news organizations.

IT Infrastructure

GIACE has standardized on manufacturers for their company IT infrastructure as follows: Cisco for network devices, Compaq for servers, and Dell for workstations. They have chosen companies that are well established, recognized as leaders in the industry and dedicated to product support. As for the PC operating system, they have deployed Microsoft Windows exclusively throughout the company. All servers are running NT 4.0 SP6a in an NT domain structure. The workstations and laptops are all running Windows 2000 Professional. GIACE has found that standardizing helps keep support costs lower which leads a higher return on investment. All computers in GIACE are running McAfee's virus protection software, Vshield and VirusScan, as appropriate to their operating systems. They use the grandfather-father-son scheme of backup with the HP DLT8000 tape drive. Please reference Figure 1 - GIACE Network Diagram for a diagram of the GIACE network.

D.C. office internal network

At the DC headquarters, a Cisco Catalyst 6509 switch (24 GB back plane) supplies the 10/100/1000 Mbps backbone of their internal network. The Catalyst 6509 core switch consists of redundant supervisors, redundant power supplies, two 24-port 10/100 Mbps modules and a 16-port 1000 Mbps (gigabit over copper) module. Two Compaq Proliant DL380 (1.4 GHz, 256 MB RAM) act as the Primary and Backup Domain Controller for the NT domain, DoReMi. Two Compaq Proliant DL380 servers (1.4 GHz, 256 MB RAM) are running the Windows Internet Name Service (WINS) and act as Primary and Secondary WINS servers. Two Compaq Proliant DL380 (1.4 GHz, 512 MB RAM) running Microsoft Internet Information Service (IIS) 4.0 serves as the company's corporate web server and as the intranet server. Two Compaq Proliant DL380 1.4 GHz, 512 MB RAM) running IIS 4.0 serves as the company's internal File Transfer Protocol (FTP) server and customer FTP server. Two Compaq Proliant DL760 (Quad 900 MHz, 4 GB RAM) running SQL 7.0 serves serve as the company's database server and application server. A Compaq Proliant DL580 (Dual 900 MHz, 1 GB RAM) running IIS 4.0 and Exchange Server 5.5 serve as the e-mail and Outlook Web Access (OWA) server. All internal servers have an Intel Pro/1000 (gigabit over copper) network interface card (NIC) installed to connect to a port on the 1000 Mbps 16-port module on the Catalyst 6509. Servers at the DMZ have an Intel Pro 10/100 NIC. Users have different models of the Dell Optiplex line and are connected to the 24-port 10/100 Mbps modules running at 100 Mbps. The internal network uses a private IP address space as defined by RFC 1918[1].

D.C. office proxy firewall

For greater security and flexibility, GIACE implemented a Checkpoint Firewall-1 proxy firewall to protect the internal network from less trusted networks. The firewall acts as the passage between the DMZ and internal network. It is configured for Network Address Translation (NAT) as the internal network uses private IP space addressing. The firewall access list follows the Principal of Least Privileges[2]:

- The only inbound traffic from the customer FTP server allowed is to the SQL servers.
- The only inbound traffic from the corporate web server allowed is to the programmers' machines. Programmers are the only ones responsible for all GIACE web servers.
- The only inbound traffic from the e-mail server allowed is to the user's machines.
- All traffic outbound is allowed as long as the source IP is part of the

internal network address space to prevent spoofed source IP addresses from reaching the Internet.

This is the only deviation from their Cisco network device standard. By using a different firewall from a different vendor than their stateful inspection firewall, GIACE increases their security by requiring an attacker to compromise two different hardware types and operating systems.

D.C. office Virtual Private Network (VPN) concentrator

To securely connect the three other offices as well as their mobile users to the internal network, GIACE put into service a Cisco VPN 3015 Concentrator. It uses IPSec to securely transmit data over a public network through the use of authentication and encryption. The 3015 Concentrator is connected in parallel to the proxy firewall, between the DMZ and internal network.

D.C. office Demilitarized Zone (DMZ)

The DMZ is provided by a Cisco Catalyst 2900XL 10/100 Mbps switch. The company's web server, FTP server, and e-mail server resides in the DMZ.

D.C. office stateful inspection firewall

To protect from highly untrusted networks (Internet), GIACE employs a Cisco PIX 515 stateful inspection firewall. Since Internet connection speed is important to the GIACE core business, a stateful inspection firewall strikes a good balance between security and performance[3].

D.C. office Internet connection

The Internet Service Provider (ISP) for GIACE is MeMeNet, a well-established Tier 1 provider. MeMeNet supplies GIACE with a full T1 connection. The Customer Premise Equipment (CPE) router is a Cisco 2501. MeMeNet also supplies GIACE with the DNS authority servers for its domain, giace.com.

Satellite office IT infrastructure

All the satellite offices at Chicago, Los Angeles, and New York City, have a similar IT infrastructure as the D.C. headquarters. Their ISP is also MeMeNet with dedicated 56K frame relay lines. The CPE routers are also Cisco 2501 routers, which connect to Cisco Catalyst 2900XL switches that serve as the backbone for the remote LAN. The satellite offices are members of the DoReMi NT domain and each have one Compaq Proliant

DL380 (1.4 GHz, 256 MB RAM) that acts as a backup domain controller (BDC) and primary WINS server for their site. WINS replication is configured to occur between the offsite WINS servers and the primary WINS server at headquarters. The satellite offices use the Exchange Server in D.C. as their mail server.

GIACE Virtual Wide Area Network (WAN)

For cost reasons, GIACE opted not to connect each satellite with a dedicated line to the headquarters in D.C. Instead, the satellite offices use their CPE routers running IPSec to establish a LAN-to-LAN VPN connection with the VPN Concentrator in D.C. Using VPN to create a virtual WAN is a lot more cost effective than dedicated lines because they use Internet connections they already own. Cisco cited cost as a factor in enterprises choosing VPN: "Lower cost than private networks—Total cost of ownership is reduced through lower-cost transport bandwidth, backbone equipment, and operations."[4]

GIACE mobile users

Besides the workers at the headquarters and satellite offices, GIACE also employs "roaming reporters" that comprise the company's mobile users. These reporters are equipped with Dell Latitude laptops. They are provided with adapters that allow them to use their cell phone for their Internet connection, as the reporters are literary on the road for great lengths of time. These roaming reporters use the Cisco VPN Client software to securely connect to the headquarters in D.C. Occasionally, the mobile users connect directly to the internal network of the satellite offices or headquarters to submit their work.

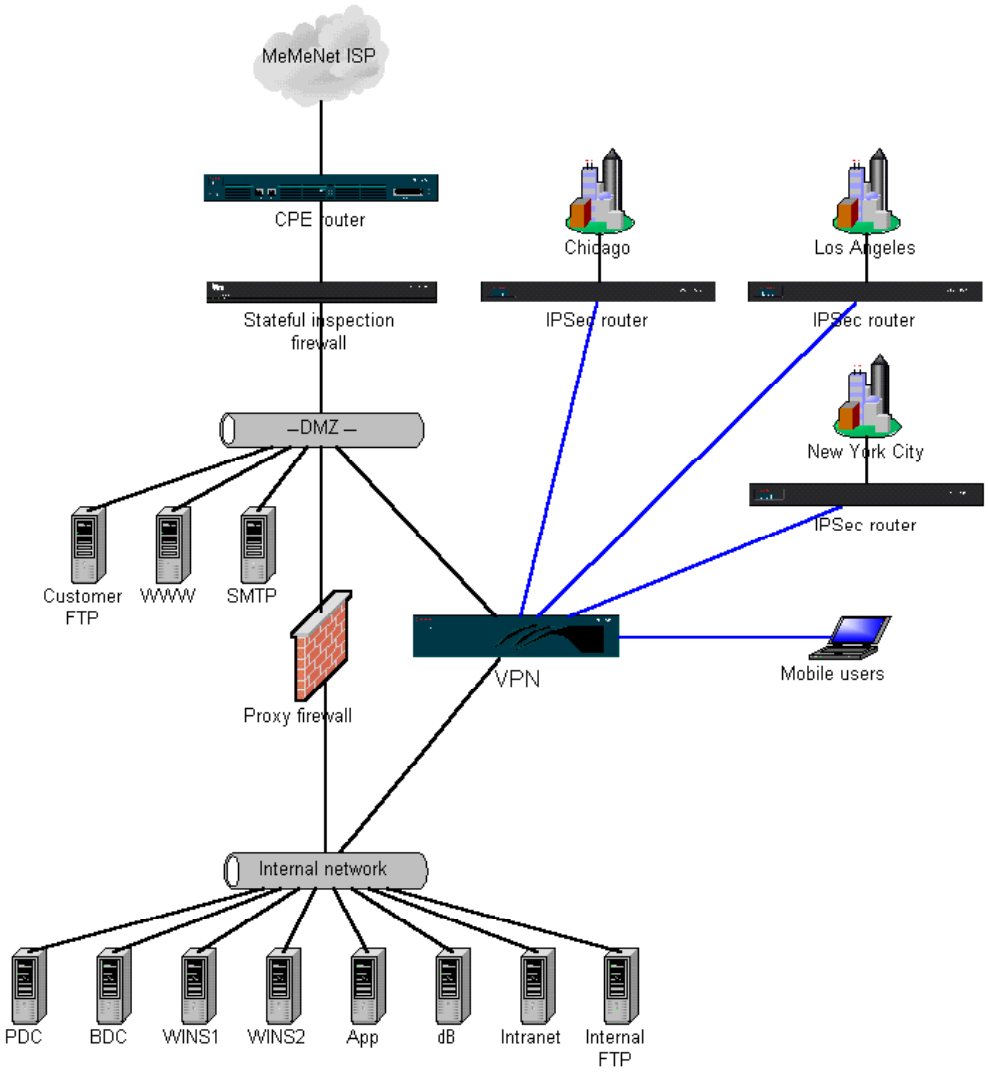

Figure 1 - GIACE Network Diagram

Business Operations

Getting the stories in

GIACE's business operations start from the outside in. The people at the satellite offices and the mobile users gather their information and prepare their report. All reporters use a proprietary, internally developed application to format the story for processing. Once ready, they FTP their story to the internal FTP server at D.C using WS-FTP client software. Since the internal FTP server uses a private IP address, the only way to access it outside the D.C. office is through a VPN connection. This helps secure the FTP server, as well as the transmission of stories as they are encrypted for the VPN tunnel. Stories are uploaded at any time, 24x7.

Processing the stories

The SQL application server detects the new story, parses it, formats it into Extended Markup Language (XML) format, adds additional control fields then sends it to the SQL database for storage. Since the supply and demand for GIACE news coverage is basically 24x7 real time, there is at least one editor in the D.C. office at all times. The editor on duty in the D.C. office uses an internal application to retrieve the story in XML format to prepare them for release. Once edited, the stories are once again stored in the SQL database for release.

Getting the stories out

When the application server detects a finished story, it retrieves it from the SQL database and creates an XML file in the appropriate virtual directories. Many times, the story is released to more than one customer. All this information is also stored in the SQL database. Each GIACE customer is supplied with a user account and password for FTP as well as a virtual directory that only their user account can access. The customers are also supplied with a GIACE-developed FTP reader application. The FTP reader runs on a customer's server and checks GIACE's customer FTP server every five seconds for stories to download. When it finds stories, it downloads the file and then deletes it one at a time until the customer's directory is empty. GIACE's responsibilities end once the files are downloaded to the customer's server.

User Access

Outside of the reporters, other employees support GIACE's standard business functions. GIACE implements the Principal of Least Privileges for user access and delegates only the permissions to groups necessary for

their normal job function. The InfoSec Group is responsible for securing the network infrastructure. As such, they have access to all servers and network devices but only they have access to the firewalls and the VPN concentrator. The Programmers Group is responsible for the SQL database and internal applications that automate the news story processing and control. They are also responsible for the company's public web server and intranet server. This group is the only group that has full access to the application, database and web servers. The Network Group is responsible for the IT infrastructure and the NT domain. They have full access to all switches, hubs, routers, and all servers including domain controllers, WINS servers, and the mail server. The User Support group helps all GIACE employees in all offices as well as all mobile users. They have full access to user workstations only. GIACE also have an executive, administrative and sales group that provide the non-technical business support. These are regular users and have no special access except to their own machines. All employees use e-mail and the Internet to conduct their business. For e-mail, non-mobile users use Microsoft Outlook to connect to the Exchange Server. Mobile users use their dial-up Internet connection to access Outlook Web Access running on the corporate web server.

GIACE'S THREE MOST CRITICAL RISKS

In order to identify the GIACE's three most critical risks, it is necessary to define what risk is in terms of information security. Simply, risk is a vulnerability to an existing threat. Risk does not exist if the combination of both the threat and the vulnerability to the threat is not present. A real world analogy is the risk of being shot when standing in an open field within a sniper's range. The threat is the sniper aiming at you. The sniper is armed and skilled at marksmanship. The vulnerability is being open in the sniper's range. If either one is taken away, then there is no risk. For example, if the sniper is not there or has no ammunition, then there is no threat and hence there is no risk of being shot. On the other hand, if the sniper is armed but you were not standing in the sniper's range or you were well hidden behind a bulletproof obstacle, then you are not vulnerable and hence there is no risk of being shot either.

The next step in identifying the three most critical risks is what makes one risk more critical than another. This is where the value of what is at risk factors in the equation. The higher the value of what is being protected from the risk, the more critical that risk becomes. Using the sniper analogy again, if it is your life that is at risk, your life is of high value and therefore that risk is very critical. If the sniper was aiming at an empty bottle you left in the open field, the empty bottle is of little value to you and therefore the risk is non-critical. The risk to the empty bottle is real, but if both your life and the empty bottle were at risk, the risk to your life is more critical and would require attention before the risk to the bottle.

The relationship to risk between value, threat and vulnerability is nicely summed up in track 9.1 of the SANS ISO Training as follows: "RISK = VALUE x THREAT x VULNERABILITY"[5]. As stated in the document, this is not a strict mathematical formula but a general representation. It does imply that for a risk to be low, all three (value, threat and vulnerability) must be low. Any one of them that is high will increase the risk.

Risk One: Denial of Service

GIACE's "crown jewels" are the acquisition and delivery of their stories of musical acts. GIACE needs to be able to receive the stories from their roaming reporters and satellite offices and then send them successfully to their customers in a timely manner. Without this complete process, there is no financial return for the company and they would go out of business. If the stories do not get to the headquarters from their reporters, then there are no items to sell their customers. Likewise, it does not do the

company any good to have stories without being able to deliver them to their customers. This deals directly with availability, one of the pillars of information security[6].

A Denial-of-Service (DoS) attack or Distributed-Denial-of-Service (DDoS) attack threatens the availability of GIACE to receive and send their stories. Since this process is the "crown jewel" of GIACE, the value of this process is very high. The National Infrastructure Protection Center (NIPC) publishes a bi-weekly report on security issues called CyberNotes. The most recent (as of this writing) covered April 4, 2002 through April 18, 2002 and listed eight vulnerabilities deemed low risk, two deemed medium risk and four that were possible high risk. So the possibility of being vulnerable to DoS attacks is high. As far as existing threat, it is difficult to ascertain DoS attack attempts but NIPC states: "It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high."[7] Though not as recent but still relevant, an eleven month study by the Honeynet Project completed on February 2001 showed a lot of malicious black hat activity[8]. Fortunately, GIACE has done a reasonable job in reducing their vulnerability to DoS types of attack. Their two-tiers of firewalls makes an attack more difficult. The firewalls also provide egress filtering which decreases the likelihood that their machines will participate in a DDoS attack. GIACE's Network Group also does a commendable job in keeping up-to-date with security patches and software fixes for the company. As with most security procedures, there are improvements that can be made.

Decreasing the Denial of Service Risk

- Install host-based firewalls – Part of Defense-in-Depth states that "Layers of defense integrated such that compromise of one layer leads to a layer more difficult to compromise."[9] GIACE's perimeter defense is only one layer. Installing a host-based firewall such as ZoneLab's Zone Alarm or Black Ice Defender will add another layer to GIACE's defense, especially to their critical SQL servers. This can dramatically reduce the risk of a DoS attack should it penetrate the perimeter defense.
- Implement an Intrusion Detection System (IDS) – An IDS can alert of a successful attack and should help in minimizing the effect of the attack. An IDS system with sensors at the internal network, the DMZ and between the CPE router and stateful inspection firewall is the optimum configuration. With this setup, the IDS can not only notify of a successful attack, but also give ample information that the perimeter defense is working as expected.
- Add redundant ISPs – Since GIACE is heavily dependent on their Internet connection for access by reporters and customers, having only one ISP is

a single point of failure. As Eric Cole wrote about network design in helping prevent DoS attacks, "if a company has a mission-critical web site … and there is a single connection with a single router, and the server is running on a single machine – this is not a robust design."[10] By making their headquarters a multi-homed site through the use of the Border Gateway Protocol (BGP), the company can have a hot standby Internet connection if the primary ISP should fail. The secondary ISP needs to be different from the primary ISP and preferably, with a different local loop provider. If the DoS target is the router upstream from the CPE router, then the secondary ISP can be used and the Internet connectivity restored.

- Implement a cluster of FTP and SQL servers – Similar to a single ISP, since FTP is the company's main delivery method to customers, having only one FTP server is another single point of failure. Likewise, SQL servers are used to store stories as well as automate the handling and processing of stories and a cluster of SQL servers will provide higher service availability. If one of the servers is attacked by DoS and files are deleted, the secondary server can be patched and brought online quicker than restoring a server from tape backup.
- Disable unnecessary services on servers – Many DoS attacks are targeted at services that are vulnerable. A logical extension would then be: "running the least amount of services on a machine helps minimize the chance of a successful attack."[11]

Risk Two: Insecure FTP

All data in an FTP session is sent in clear text, including user names and passwords. FTP was not designed for security – it was designed for public access. Unfortunately, the way GIACE uses FTP is quite the opposite: for receiving and transmitting proprietary files – the stories. Microsoft IIS and NT security help somewhat. GIACE is already using virtual directories and NTFS permissioning to prevent customers from accessing each other's files. Even though FTP is not secure natively, there are steps to decrease its vulnerabilities. If an attacker successfully compromised the FTP server, then the stories could be deleted – a form of DoS attack because it affects availability. Even worse, the attacker could change the story's content, which would affect its integrity – another pillar of information security[12]. Depending on the modification, distribution of an unauthorized story can result in legal actions (libel suits), loss of customer confidence, and bad publicity, all of which can lead to financial losses to the company.

Referring again to the risk formula, the threat is relatively low. There have not been many reports regarding FTP servers compromises except for

anonymous logins that have write rights for storing illegal files like illegally-digitized copyrighted movies. GIACE has already disabled anonymous logins to their FTP server. Unfortunately, the other two factors in the risk formula, vulnerability and value are high. Once again, we are dealing with the music stories that are the core product of the company. And, as previously stated, FTP itself is very vulnerable to compromises.

Decreasing the Insecure FTP Service Risk

- Encrypt FTP sessions – Since FTP sessions are normally sent in clear text, the user name and password, as well as the story itself, is vulnerable to unauthorized access through sniffing or man-in-the-middle attacks. There are two ways that GIACE can accomplish this. The first is to run a Secure Shell (SSH) server on the FTP server and have the customers use an SSH client for their FTP sessions. The second, more economical way is to use their existing VPN concentrator, which already encrypts sessions (using 3DES). Since GIACE does not use their FTP server for public access anyway, they should move the FTP server internally with a private IP address. This way, the FTP server can only be accessed via VPN. The client can either establish a LAN-to-LAN or Remote Access VPN tunnel with GIACE.
- Encrypt FTP files – While the files on the FTP server are waiting to be retrieved, they are in clear text format. Should the FTP server be compromised, the integrity of the stories is not guaranteed. Encrypting the files on the FTP server protects them from being modified by either internal or external users. An easy path would be to upgrade the FTP server to Windows 2000 Server and use its native file encryption.
- Limit Access via IP Filtering – GIACE should filter access to their FTP servers by the source IP address of their customers. They should be able to filter down to a few host IP addresses or at least the IP range the customers are using. There are two specific places they can filter: at the firewalls and at the IIS virtual directories. The firewalls include the stateful inspection, application, and host-based firewalls. IIS allows you to deny access to all IP addresses except for one you specified. If VPN is used, filters for tunneled traffic should be applied as well. These steps would follow both Defense In-Depth and the Principle of Least Privileges.

Risk Three: Unprotected Mobile User Laptops

An often-overlooked security hole is the portable computers of the mobile and remote users – out of sight, out of mind. Using VPN for remote access secures the traffic between the remote machine and the secured network, but it does not secure the laptop itself or the network it is connecting to. If a laptop were to be compromised, it can infect the

internal network via the VPN tunnel. All GIAC laptops are setup for a dialup Internet connection but some of them are also taken home which may have a broadband connection. There are also times, when a mobile user, will directly connect to one of the sites' internal network, which also places the network at risk if the laptop was carrying a virus, Trojan or worm. A compromised laptop can lead to unauthorized modifications to a story being distributed, elevated access of the attacker to the GIACE internal network, and DoS attacks, as well as malware (viruses, Trojans, back doors) introduction and proliferation into the GIACE infrastructure. Any of these can lead to the disruption of normal operations and service levels straying from real time. This would lead to customer dissatisfaction and possible loss of revenue.

A compromise of the internal network can also result in the compromise of the integrity and availability to GIACE's stories, which are highly valuable to the company. A laptop hooked up to an always-on Internet connection is exposed to the same threats as corporate machines. In some ways, these home and home office machines are more vulnerable since attackers know they are less likely to be protected and hence, are popular targets. A project of Honeynet.org completed on November 2000, studied real attacks to specifically compromise home machines using broadband access with a worm for the attacker's own purpose[13]. This study gives hard evidence of a real threat. Even using a dial-up connection, the threat is only minimized somewhat, but definitely not eliminated. The laptops are all running an anti-virus package which helps decrease their vulnerability but more should be done. Using the risk formula as a guideline, this combination of factors equates to a critical risk.

Decreasing the Unprotected Mobile User Laptops Risk

- Install personal firewalls – As firewalls are important in the defense of a network, so are personal firewalls to the defense of a host. A personal firewall should be configured with two goals in mind: protection from external attacks and prevention of being enlisted into an attack to others. Many personal firewalls can be easily configured for this including those by Zone Labs, Black Ice, Symantec and McAfee.
- Setup automatic virus updates – Out-of-date anti-virus software is only marginally better than not having one at all. McAfee should be configured to automatically download the newest virus definitions everyday. For mobile users with dial-up only, they should be instructed to update their anti-virus software at the start of their dial-up session for the day.
- Disable shares and delete mapped drives – Since mobile users use an in-house application to transmit their work to headquarters, the need for

shares and mapped drives is low but the vulnerability to attacks is high. CERT has listed exploiting Windows shares as one of the common methods an attacker uses in its Home Network Security advisory[14].

- Disable split tunneling and restrict dual homing – Both split tunneling and dual-homing of laptops in a non-GIACE LAN, e.g., a home network, exposes the laptop to the vulnerabilities of the home network. Most likely, this home network does not have defenses as robust as those implemented in GIACE LANs. Disabling split tunneling is only a matter of a check box in the Cisco VPN Concentrator configuration tool. Restricting dual homing can be done through a company policy.

GIACE VPN POLICY

Since GIACE is so reliant upon their VPN connectivity to establish and assure their business operations, it is important to analyze their current VPN policy for its appropriateness and completeness. This policy applies to their roaming reporters, satellite offices, and business partners. The remote users already follow the policy, but in order to address the Insecure FTP Service risk, this policy must also be enforced to business partners when using FTP.

Current VPN Policy

GIACE's current policy is based on the VPN Policy from the SANS Security Policy Project[15].

Virtual Private Network (VPN) Policy

1.0 Purpose
The purpose of this policy is to provide guidelines for Remote Access IPSec or LAN-to-LAN Virtual Private Network (VPN) connections to the GIACE corporate network.

2.0 Scope
This policy applies to all GIACE employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the GIACE network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

3.0 Policy
Approved GIACE employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to GIACE internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong password phrase.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by GIACE InfoSec Group.
6. All computers connected to GIACE internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (http://www.mcafee.com); this includes personal computers.
7. VPN users will be automatically disconnected from GIACE's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not GIACE-owned equipment must configure the equipment to comply with GIACE's VPN and Network policies.
10. Only InfoSec-approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of GIACE's network, and as such are subject to the same rules and regulations that apply to GIACE-owned equipment, i.e., their machines must be configured to comply with InfoSec's Security Policies.

4.0 Enforcement

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term Definition

IPSec Concentrator - A device in which VPN connections are terminated.

Evaluation of Current VPN Policy

Policy Purpose

The current policy purpose is stated, the "what", but no further information is given to the reason the policy is needed, the "why." Although brevity has its own advantages, the policy would be served better with a description of the risk of not using VPN to connect to the GIACE internal network. It should include that data sent through the Internet unencrypted can be intercepted and easily read. Especially important to protect are the stories that are being transmitted as they are the product the company is providing to their customers.

Policy Background

A background is omitted in the current policy but should be added since this policy directly affects the company's business operations. More

background information can make the importance of this policy's subject clearer. The background should include the three common reasons a VPN connection is used: GIACE's virtual WAN, remote users (reporters), and customer access (secure FTP). It can also reiterate its importance by providing what can happen if this policy did not exist.

Policy Scope

The current scope is well worded and comprehensive. Specific mention of the IPSec concentrator makes it clearer what VPN connections are covered in this policy.

Policy Statement

Up to this point, the policy applied to all three types of GIACE VPN uses. The policy statement needs to be modified on some bullet points to reflect the different requirements of the VPN connection types.

- Item 1 – Regardless of connection type, only authorized users should be able to access the GIACE internal network so this item is appropriate. No changes are necessary.
- Item 2 – For ease of deployment at a lower cost, GIACE opted to use secret keys, which is covered by this item. Requirements for the secret key should be added as follows: minimum 10 character length, with at least one lower case letter, one upper case letter, one numeric character and one special character. Also, the safekeeping of these passwords needs to be specified. The mention of tokens is also fitting as this method may be implemented in the future. In general, policy statements should try to encompass possible future development while still applicable to the current situation, which this item accomplishes.
- Item 3 – This entry requires modification to take into account the needs of the different types of VPN connections. The statement applies only to the mobile users (roaming reporters) and should be specified as such. LAN-to-LAN connections used by satellite offices or customers as well as customers connecting with the VPN software client, need to access their own internal network. In these cases, dual homing is a requirement to connect to their respective (remote) internal networks. The principle of least privileges must be applied between the two network interfaces to only route the minimum necessary traffic for normal operations. Filters must be applied on both ends of the tunnels: at the VPN concentrator and the remote peer (an IPSec device or a computer running the VPN client software)
- Item 4 – Similar to Item 3, this policy as written is appropriate only to the mobile users. For all LAN-to-LAN tunnels and customers using the VPN

client software, split tunneling is a requirement to connect to their respective (remote) internal networks and a filter must be applied between the two network interfaces.

- Item 5 – It is important for a policy to specify the group responsible for implementing the procedures involved. Adding that the set up includes, but not limited to, creating accounts, choosing secret keys and passwords, and assigning internal IP addresses, will add more clarity to this policy.
- Item 6 – Setting policy for another company is not always possible and may cause unnecessary friction between GIACE and its customers. This policy should qualify the statement only for GIACE-owned equipment. GIACE has consciously decided not to have a specific security policy for customers. For customers, a statement that they should follow information security best practices will suffice.
- Item 7 – GIACE's remote users should not need to connect for long periods of time and this policy is appropriate for them. Exceptions need to be made to LAN-to-LAN connections (whether from satellite offices or customers) and customers using the VPN client software because they require a constant connection. On a slow news day, a customer may not have stories to download for long periods but their connection should remain intact.
- Item 8 – Similar to Item 7, all LAN-to-LAN connections and customers using the VPN client software must have unlimited connection times so this needs to be added in the policy. This item is appropriate for non-customer remote users.
- Item 9 – Similar to Item 6, GIACE can only set policy for its own area of authority. This statement applies to GIACE employees, contractors, consultants, temporaries and other GIACE-authorized workers who would like to use their own equipment. Customers' responsibilities for information security are already mentioned in Item 6.
- Item 10 – It is important for security as well as support to control the software used to establish the VPN tunnel. Specifying who has authority of approval is necessary for a clear and effective policy. No changes are necessary.
- Item 11 – This item should be modified to only address GIACE employees and GIACE-authorized workers. It specifies that the InfoSec group must approve the use of non-GIACE machines for VPN use and which policy must be followed in a clear and concise manner.

Policy Responsibility

The policy does a good job in specifying the responsibility of the users and customers. The role of the InfoSec group is also well defined. Since

security is equally a technical and business issue, a statement that the InfoSec group, Human Resources, and Executive Board are ultimately responsible for all final decisions regarding this policy needs to be added in the Enforcement section.

Policy Action

The Enforcement section of the policy is a good start but more details need to be added. The action on users is already covered. As for customers, the policy needs to include that they are subject to the stoppage of services, should the GIACE authority deem them not abiding by the policy. This includes, but not limited to, disconnecting the VPN tunnel when a network attack is detected and the VPN is found to be involved in the attack. In any case where policy is not satisfactorily followed, the VPN connection will not be restored until the GIACE authority has been given proof of the necessary corrective action taken. The transference of risk is a common practice in business and is a way to managing network security risk[16].

Revised VPN Policy Evaluation

Virtual Private Network (VPN) Policy

1.0 Purpose
The purpose of this policy is to provide guidelines for Remote Access IPSec or LAN-to-LAN Virtual Private Network (VPN) connections to the GIACE corporate network. VPN is a way of securing communication between two IPSec devices through the Internet, an untrusted network, by means of encryption. Without encryption, any communication can be intercepted, read and modified.

2.0 Background
There are three common uses of the GIACE VPN solution: GIACE's virtual WAN, remote users (roaming reporters) and customer access (secure FTP). All three are major participants in GIACE's core business. The virtual WAN supports the normal business operations. Remote users supply the products (stories). Customer access is the method for product delivery. If these are not secured with VPN, the stories can be intercepted, changed or deleted, and can lead to major financial losses to the company.

3.0 Scope
This policy applies to all GIACE employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the GIACE network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

4.0 Policy

Approved GIACE employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs as supplied by GIACE. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and installing the provided software. Further details may be found in the *Remote Access Policy*.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to GIACE internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong password phrase. If using a password phrase, it must be a minimum of 10 characters and must include at least one lower case letter, one upper case letter, one number and one special character. The password phrase must be stored in a physically secure place.
3. For mobile users (GIACE employees) actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped. This does not apply to LAN-to-LAN VPNs and customers using the VPN client software but dual homing is highly recommended with the principle of least privileges applied between the interfaces. For all cases, the appropriate filters must be in place at both ends of the VPN tunnel, at the IPSec concentrator and the remote IPSec device.
4. Dual (split) tunneling is NOT permitted for mobile users; only one network connection is allowed. LAN-to-LAN VPNs and customers using the VPN client software are allowed split tunneling if necessary.
5. VPN gateways will be set up and managed by GIACE InfoSec Group. Set up includes, but not limited to: creation of user accounts and passwords, selection of secret keys, and assignment of an internal IP address.
6. GIACE employees' computers connected to GIACE internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (http://www.mcafee.com); this includes personal computers. Customers are highly recommended to follow information security best practices, especially Defense-in-Depth.
7. GIACE-employed VPN software client users will be automatically disconnected from GIACE's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open. LAN-to-LAN VPNs and customers using the VPN client software are allowed any amount of time of inactivity as required by business operations.
8. The VPN concentrator is limited to an absolute connection time of 24 hours for GIACE employees using the VPN software client. LAN-to-LAN VPNs and

customers using the VPN client software are allowed continuous connectivity as required by business operations.

9. GIACE-employees using computers that are not GIACE-owned equipment must configure the equipment to comply with GIACE's VPN and Network policies.
10. Only InfoSec-approved VPN clients may be used.
11. By using VPN technology with personal equipment, GIACE-employed users must understand that their machines are a de facto extension of GIACE's network, and as such are subject to the same rules and regulations that apply to GIACE-owned equipment, i.e., their machines must be configured to comply with InfoSec's Security Policies.

5.0 Enforcement

The Executive Board, Human Resources and the InfoSec group are ultimately responsible for and have the authority to make final decisions regarding this policy. Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment. Customers are subject to the stoppage of services, should the GIACE authority deem them not abiding by the policy. This includes, but not limited to, disconnecting the VPN tunnel when a network attack is detected and the VPN tunnel is found to be involved in the attack. In any case where policy is not satisfactorily followed, the VPN connection will not be restored until the GIACE authority has been given proof of the necessary corrective action taken.

6.0 Definitions

Term Definition

IPSec Concentrator - A device in which VPN connections are terminated.

VPN PASSWORD/SECRET KEY SELECTION AND SAFEKEEPING PROCEDURE

GIACE uses the Cisco 3015 VPN Concentrator for its VPN needs. This procedure covers how to select a secure password or secret key and how to store it - an important part in setting up a VPN connection. GIACE employees using Cisco's VPN Client software are set up to authenticate using NT authentication and is covered in GIACE's Network Policy. Customers using the software client, on the other hand, are set up with a user account and password stored locally at the VPN Concentrator. For customers and satellite offices with LAN-to-LAN VPN connections, a secret key is used for authentication. Both passwords and secret keys are subject to GIACE's VPN Policy which state that the passwords and secret keys must be a minimum of 10 characters and must contain at least one each of the following: a lower case letter, an upper case letter, a numeric character, and a special character (symbol). The special character is any non-alphanumeric character found in a typical 101-key keyboard which are: !@#$%^&*()_-+=:;"'<>,.?/~`{}[]|\ and the space character.

Keeping the passwords and secret keys secure is imperative to continuing GIACE's business operations. Since this information is used to connect to GIACE's internal network, its security must be high. In addition to the requirements in the selection, its safekeeping is also covered in this procedure.

Selecting a Password or Secret Key

For ease of use and increased randomness, use a password generator utility. This procedure outlines the steps using the freeware program Password Generator v.2.0 (Copyright © 1999-2000) by Zero Alpha® (http://www.0a.itgo.com/). A member of the InfoSec Group is responsible for creating a password or secret key as follows:

1. Start the Password Generator application.
2. In the drop-down box, select 10 for password length.
3. Click on the "123" box to include numbers.
4. Click on the "abc" box to include lower case letters.
5. Click on the "ABC" box to include upper case letters.
6. Click on the "!@#" box to include special characters.
7. Click on the Generate button.
8. Check that the password/secret key generated has at least one each of the following: a lower case letter, an upper case letter, a numeric character, and a special character (symbol). If the generated password does not meet the minimum requirements, continue to click the Generate

button until an acceptable phrase is created.
9. Once selected, write it down on paper and submit it, by hand, to the InfoSec Manager for final approval.

Safekeeping the Passwords and Secret Keys

Selecting a hard to guess/crack password is only the first part of securing them. The next part is storing them safely. Unfortunately, we, as human beings, do not have perfect memory. GIACE has consciously decided to store the user names/passwords and remote peer IP address/secret keys combinations in an ASCII (plain text) file for retrieval when necessary. Plain text format was chosen for its compatibility with many operating systems and software applications. This part of the procedure outlines this file's safekeeping.

1. The InfoSec Manager, immediately after approval of a new password or secret key, retrieves the floppy disk from the media safe in his/her locked office.
2. The InfoSec Manager then makes the necessary addition to the password file.
3. The InfoSec Manager also makes a backup copy to another floppy. The backup copy is required in case the password file on the original disk becomes inaccessible.
4. The InfoSec Manager opens the password file on the backup floppy to verify its accessibility.
5. The InfoSec Manager then stores both floppies back in the media safe.
6. The InfoSec Manager then shreds the piece of paper that had the secret combination written on.
7. Members of the Executive Board, Human Resources and the InfoSec Manager knows the combination to the safe as well as having access to the key of the InfoSec Manager office where the safe is located. Should the need arise; any one listed previously can access the password list.

REFERENCES

[1] Rekhter, Y. Moskowitz, B. Karrenberg, D. de Groot, G. J. Lear, E. "Address Allocation for Private Internets." RFC 1918. February 1996. http://www.ietf.org/rfc/rfc1918.txt?number=1918 (April 27, 2002)

[2] Fried, Steven. "9.1 SANS Security Leadership, Part 1". SANS Track 9 – Information Security Officer Training, 2001. 6-12.

[3] Fried, Steven. "9.5 Defense In-Depth". SANS Track 9 – Information Security Officer Training, 2001. 1-21.

[4] Cisco Systems, Inc. "A Primer for Implementing a Cisco Virtual Private Network." Cisco Reference Guides. August 8, 2000. http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21_rg.htm (April 26, 2002)

[5] Fried, Steven. "9.1 SANS Security Leadership, Part 1". SANS Track 9 – Information Security Officer Training, 2001. 1-9.

[6] Fried, Steven. "9.1 SANS Security Leadership, Part 1". SANS Track 9 – Information Security Officer Training, 2001. 1-20.

[7] National Infrastructure Protection Center. "National Infrastructure Protection Center CyberNotes." Issue #2002-48. April 22, 2002. http://www.nipc.gov/cybernotes/2002/cyberissue2002-08.pdf (April 25, 2002). 17.

[8] Honeynet Project. "Know Your Enemy: Statistics." July 22, 2001. http://project.honeynet.org/papers/stats/ (April 25, 2002)

[9] Fried, Steven. "9.5 Defense In-Depth". SANS Track 9 – Information Security Officer Training, 2001. 1-3.

[10] Cole, Eric. Hackers Beware. Indianapolis: New Riders, 2002. 235.

[11] Cole, Eric. Hackers Beware. Indianapolis: New Riders, 2002. 236.

[12] Fried, Steven. "9.1 SANS Security Leadership, Part 1". SANS Track 9 – Information Security Officer Training, 2001. 1-20.

[13] Honeynet Project. "Know Your Enemy: Worms at War." November 9, 2000. http://project.honeynet.org/papers/worm/ (April 30, 2002).

[14] CERT Coordination Center. "Home Network Security." December 5, 2001. http://www.cert.org/tech_tips/home_networks.html (April 30, 2002)

[15] SANS. "VPN Security Policy." The SANS Security Policy Project. http://www.sans.org/newlook/resources/policies/Virtual_Private_Network.doc (April 30, 2002)

[16] Fried, Steven. "9.1 SANS Security Leadership, Part 1". SANS Track 9 – Information Security Officer Training, 2001. 1-8.