

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

GIAC Certified Firewall Analyst

Practical

v1.6

Mark Gryparis
GCFW Course taken in Denver in June, 2001

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A note on Format and Content:

Instead of writing this paper in an 'academic' format, I decided to cast it in the form of a set of real security documents that one would actually develop and use on the job. It therefore consists of the following sections:

1. **GeF Network Security Policy**

   This is a full-blown policy document, and above and beyond the assignment. But it's actually necessary to have this before the Architecture can be designed)

2. **GeF Network Security Architecture**

   Contains Assignment 1: Security Architecture and Assignment 2: Security Policy.

3. **IP Packet Filtering with Cisco Router ACLs**

   Contains the Security Policy Tutorial section of Assignment 2. Note however, that the explanation of the rules and the services they address is in the GeF Network Security Architecture document.

4. **GeF Outer Firewall Audit Report**

   Contains Assignment 3: Audit your Security Architecture.

5. **Network Perimeter Design Under Fire**

   Contains Assignment 4: Design Under Fire..

© SANS Institute 2000 - 2002, Author retains full rights.

GIAC e-Fortunes

GeF Network Security Policy

v2.3 – 9/1/1

1.0 Purpose and Scope

The purpose of this document is to define and document the Network Security Policy (NSP) of the GIAC e-Fortunes (GeF) division of GIAC Enterprises. This document is one part of an overall GeF Information Security Policy, which includes:

- GeF Network Security Policy — Defines security policies for GeF networks
- GeF Host Security Policy — Defines security policies for GeF hosts and applications
- GeF Physical Security Policy — Defines security policies for the design and use of GeF physical spaces and physical access controls
- GeF Information Release Policy — Defines policies for the release of GeF information through verbal, written and electronic means

For the mapping from Business Plan to this document, see the following documents:

- GeF Business Plan — Defines the GeF Business Objectives
- GeF Network Requirements — Defines those GeF Business Objectives to be met by the GeF Networks, and the operational and functional requirements of the networks
- GeF Network Architecture — Defines the Network Architecture to be implemented to meet those requirements

2.0 Approvals

We, the undersigned, approve and hereby implement this NSP, v2.3. All previous versions of this document are hereby superseded by this document.

_____

Fred F. Flintstone — Date
President and Chief Executive Officer, GIAC e-Fortunes

_____

Barney M. Rubble — Date
Chief Information Officer, GIAC e-Fortunes

3.0 Business Background and Requirements

GeF is a company engaged in the creation of online fortune cookie sayings (FCSs), as well as their direct and wholesale marketing and sales. FCSs come in three varieties: ordinary, insightful and prophetic. Wholesale and direct customers may purchase FCSs individually or in bulk, in whatever variety mix they choose. Prophetic FCSs are created on-site by GeF, using proprietary Divination hardware and software in a process that is a trade secret. Due to the unusual nature of the Divination process, it cannot be patented, and therefore the future business viability of GeF depends on keeping it secret.

GeF's business relationships fall into the following major categories:

Suppliers — GeF has multiple business partners who provide FCSs in quantity in the ordinary and insightful categories. Most of these contractors have SLA agreements for regularly scheduled deliveries of their product. Consequently, WAN links have been established to many of these for electronic delivery. Of the remainder, some

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

suppliers use a VPN connection over the Internet, and others make their deliveries on CD ROM.

Wholesale Customers — GeF has multiple wholesale customers who resell GeF FCSs, who incorporate them into their products, or who integrate them into customized business solutions. GeF has SLAs with many of these for electronic delivery of our product. Consequently, WAN links have been established to many of these, as well, for electronic delivery.

On-line Customers — GeF markets and sells FCSs, individually or in batch, directly to online customers via its Corporate Website, one transaction at a time.

Online Subscribers — GeF markets and sells FCS subscriptions directly to online customers via its Corporate Website. The product subscription is then delivered by Email or by GeF's proprietary MOTD service.

Today, GeF is a small company with about 150 employees, and about 300 nodes. It has obtained a Class C Address, gef.c.net.0 / 24, and its own Domain, gef.com.

4.0 Delegation of Responsibility and Authority

Responsibility is delegated to the GeF **Chief Information Security Officer (CISO)** to do the following:

- Protect the business viability of GeF from harm due to unplanned changes in the Confidentiality, Integrity and Availability of **GeF information** in any form
- Protect the business viability of GeF from harm due to unplanned changes in the Confidentiality, Integrity and Availability of **GeF information systems and technology** that store, process or communicate GeF information in any form
- Constantly monitor the Security, Business and Hacker communities for new risks, threats, trends and developments
- Constantly re-evaluate GeF's Information Security Profile, communicate this status to GeF management, and to advise and make recommendations as needed
- Regularly re-evaluate the NSP and Network Security Architecture (NSA) and all related procedures and policies, and update them as appropriate.
- Be an integral, ground-level participant in all business plans and endeavors

Authority is delegated to the **GeF CISO** to do the following:

- Authoritatively interpret this NSP in every instance of application
- Review and approve/reject all existing aspects of GeF Network Security Architecture, and require remediation where deemed necessary
- Review and approve/reject all proposed changes to the GeF Network Security Architecture, and recommend alternative solutions

The GeF **Network Security Architecture** (NSA) is defined as any and all hardware, software, networks, procedures and employee roles that implement a network security policy.

5.0 Network Security Zones (Zones)

The GeF Network shall be partitioned into multiple Security Zones, each of which is designed to host resources with similar security requirements and/or a similar security profile. Each Zone will have its own set of network security policies

The GeF Network Security Zones are described below:

Zone Name/Net	***Description***
The Internet	The Public Internet. The Network space where a large portion of GeF Customers and Threats reside

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

External DMZ	An (untrusted) DMZ designed to host those resources that are available to GeF customers over the Internet.
Admin DMZ	An (untrusted) DMZ specifically designed to host the following two resources: ▪ **External Mail Server** – The externally available Email Relay ▪ **External/External DNS Server** – The authoritative DNS Server for the gef.com domain.
Employee DMZ	An (untrusted) DMZ specifically designed to host those resources that give GeF employees remote access to the GeF Internal Network, and other resources with a similar level of trust
Partner DMZ	An (untrusted) DMZ specifically designed to host those resources that provide network connectivity with GeF Business Partners, and other resources with a similar level of trust.
General Net	An internal (trusted) network designed to host General GeF Resources
Management Net	An internal (trusted) network designed to host those resources that store and process business-sensitive data that are not GeF Trade Secrets. For example: business plans, marketing plans, budgets, HR-related information
Divination Net	An internal (trusted) network designed to host those resources that store and process GeF Trade Secrets.
Server Net	An internal (trusted) network designed to host those resources that store and process sensitive customer information, products awaiting delivery, and internal network infrastructure resources.

6.0 Network Security Devices (NSDs) and the GeF Security Perimeter

All General and Zone-specific network security policies shall be implemented, enforced, logged and audited by NSDs. Conversely, any device that performs a network security function is categorized an NSD. Some of these devices may be under the primary management of GeF employees that are not members of the Information Security staff, such as System or Network Administrators. Nonetheless, these devices do fall under the purview of Information Security, which has fundamental approval and veto rights over all configuration changes on these devices.

The set of GeF NSDs can include – but is not limited to – the following types:
- Network Cabling
- Network Switches that contain VLANs from different Security Zones
- Network Routers with Access Control Lists (ACLs) or other configuration elements that perform a security function
- Firewalls
- Intrusion Detection Sensors
- Intrusion Detection Analysis Nodes
- DNS Servers
- Email Servers
- Administration and Auditing workstations for any NSD

The **GeF Security Perimeter** is defined to be those NSDs that provide physical or logical connectivity to any network or node outside the defined GeF Network Security Zones.

7.0 General Security Policies

The **External Connectivity Security Policy** is as follows:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- The only external connectivity to GeF networks permitted at any time is that provided by connections that are:
    - GeF CIO-mandated
    - GeF CISO Approved
    - GeF IT Staff installed, operated and maintained
- GeF network Users are not permitted to install or create any other connectivity to or from the GeF networks. This includes, but is not limited to: modems, DSL connections, Cable-TV, wireless, IR, Radio, etc.

The **Network Protocol Security Policy** is as follows:
- TCP/IP shall be supported on all Zones as the standard Layer 3 networking protocol on the GeF Network
- Only TCP/IP shall cross the GeF Security Perimeter in any direction.
- Only TCP/IP shall be used on any DMZ Security Zone. All other Layer 3 protocols will be blocked by NSDs connecting to any DMZ Security Zone. DMZ Security Zones shall be monitored for non-TCP/IP Layer 3 protocols, which shall detected, logged and audited as security incidents.
- Non-TCP/IP Layer 3 networking protocols (AppleTalk, IPX, DECNet, etc.) may be used on Internal networks with the approval of the CISO, and only in the manner approved. In general, the security policies implemented with non-TCP/IP protocols shall be consistent with the letter and spirit of the NSP to the greatest degree that is technically possible with the protocol.

The **IP Addressing Security Policy** is as follows:
- IP Addresses assigned by the IANA to GeF (GeF's "real" IP Addresses) shall only be used by NSDs as NAT and PAT addresses for externally available resources.
- All internal addressing shall be private, using RFC 1918 IP Addresses
- Each Zone shall be assigned a unique private subnet

The **Routing Security Policy** is as follows:
- Only routes to GeF's IANA-assigned IP addresses may be advertised to the Internet
- Only static routes shall be used within any Zone that hosts external network connectivity. NSDs that connect to these Zones must discard and explicitly block all routing protocols
- Every router shall employ anti-spoofing filters

The **DNS Network Security Policy** is as follows:
- The GeF DNS Architecture shall be designed to divulge the minimum necessary information to Business Partners and the Internet
- The GeF DNS Architecture shall be designed to protect internal network users from external threats such as DNS poisoning attacks
- DNS Servers shall be hardened and provide no unnecessary services

The **Email Network Security Policy** is as follows:
- The GeF Email Architecture shall be designed to divulge the minimum necessary information to remote email senders/receivers and to nodes the Internet.
- The GeF Email Architecture shall be designed to protect internal network users from external threats such as Email-borne viruses, worms and trojans.
- Email Servers shall be hardened and provide no unnecessary services

The **Printing Network Security policy** is as follows:
- No print traffic shall be permitted across the GeF Security Perimeter except for business requirements and as explicitly approved by the CISO
- No print traffic shall be permitted to enter or leave a DMZ Zone except as explicitly approved by the CISO
- No host-based print services are permitted on the GeF network. Only network printers with no long-term data storage capability shall be used.
- Print traffic is permitted to cross between Internal Network Zones

The **Microsoft Networking Security Policy** is as follows:
- No Microsoft Networking Protocols shall cross the GeF Security Perimeter in any direction.
- Microsoft Networking Protocols shall not be used within any DMZ, nor shall they enter or leave any DMZ. Exceptions may be granted on a case-by-case basis by the CISO.
- Microsoft Networking Protocols may be used within any Internal Network, but shall not enter or leave any internal network. Exceptions may be granted on a case-by-case basis by the CISO.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Each Internal Network may contain one or more Windows Domains or Active Directories, but no Domain or Active Directory shall span more than one Internal Network

The **Employee Access Security Policy** is as follows:
- Each GeF Employee (or other approved person) shall be assigned to a primary Zone, chosen to best meet their access needs
- Access to additional Zones may be granted to employees whose roles and responsibilities require it
- Some services, such as email
- Each employee with access to a Zone must authenticate to a local resource in the Zone before being granted access to local resources
- Once authenticated, user-based, OS and filesystem-level permissions shall be used to control access to Zone Resources
- No network-level access controls are required within a Zone, although case-by-case exceptions may be mandated by the CISO.

The **Business Partner Access Security Policy** is as follows:
- Business Partners may only access the Partner DMZ and the resources within it
- Business Partners will be blocked from accessing each other's data
- Business Partners will be blocked from accessing each other's remotely-connected resources or networks

The **Internet Access Security Policy** is as follows:
- Nodes on the Internet may only access (inbound) those GeF nodes explicitly designated for this purpose, only using TCP/IP, and only using those services (TCP, UDP, ICMP, Specific ports. etc.) designated, by node, for public access.
- Employee nodes physically residing on an internal (trusted) network, and those remotely connected through the resources in the Employee DMZ may access arbitrary nodes on the Internet (outbound) using HTTP (TCP 80, 8080) and HTTPS (TCP 443). All other types of outbound access to the Internet must be approved and implemented on a case-by-case basis by the CISO.
- Resources located in the External DMZ may access arbitrary nodes on the Internet (outbound) using only TCP/IP, and only using those services (TCP, UDP, ICMP, Specific ports, etc.) required to meet the goals set forth in the GeF Business Plan.

Any type of access or network traffic not explicitly permitted by this policy is prohibited. Exceptions may be granted on a case-by-case basis by the CISO. New requirements that are not addressed can be added to this policy by application to the CISO.

8.0 Security Zone-level Security Policies

The GeF Security Zones Security Policies are defined below:

Zone Name/Net	***Description***

© SANS Institute 2000 - 2002, Author retains full rights.

External DMZ	All Internet-available resources for online purchase shall be hosted in this DMZ ▪ Arbitrary nodes on the Internet may connect to each host in this DMZ for those services intended to be public. All other forms of access will be blocked. ▪ Each node in this DMZ: o Shall be configured only with private (RFC 1918) IP Addresses o Shall – if intended to be available to the Internet – be available to the Internet as a distinct IP Address from GeF's IANA-assigned address pool via NAT or PAT o Shall be hardened o Shall run the minimum number of services required to perform its mission o May be administered remotely from an Internal Network or from the Remote Employee DMZ, but only using encrypted connections. o Shall be backed-up with directly connected hardware – if it is a host. Network devices' configurations shall be backed up over the network to a designated node in the Server Network. o Shall not store sensitive information not required for its operation beyond the time taken to process it. ▪ No user workstations my be hosted in this DMZ ▪ Except for network device backups, all nodes in this DMZ shall be blocked from initiating a connection to any other Zone ▪ Access within the Zone o No network-based access controls are required for communication within this Zone ▪ DNS o Nodes in this Zone shall use the External/External DNS Server in the Admin DMZ for DNS resolution ▪ Email o The only outbound Email permitted from this Zone is that sent from the email-based product delivery resources o No inbound Email is permitted into this Zone ▪ Other Outbound Access from this Zone o Outbound-initiated traffic required for communication between customers and the Corporate Website is permitted into this Zone o Other outbound access from this Zone is permitted only by case-by-case approval by the CISO ▪ Other Inbound Access from this Zone o Inbound-initiated traffic required for customer access and communication to the Corporate Website is permitted into this Zone o Anonymous FTP is permitted to the Corporate FTP drop box o Inbound traffic from approved sources is permitted for Administration o Other inbound access from this Zone is permitted only by case-by-case approval by the CISO Other resources of a similar security profile may be added to this DMZ with the approval of the CISO.

© SANS Institute 2000 - 2002, Author retains full rights.

Admin DMZ	There are two resources hosted in this DMZ: External Email and External DNS
	▪ External Email
	  o The externally-available GeF mail server(s) shall be hosted in this DMZ
	  o The MX record(s) for the gef.com domain shall point to this mail server(s)
	  o Arbitrary nodes on the Internet may connect to this mail server(s) for SMTP. All other forms of access from the Internet shall be blocked.
	  o This mail server(s) may connect to Internal Mail Servers for SMTP. All other forms of access from this servers(s) to the Internal Networks shall be blocked.
	  o This mail server(s) shall be an SMTP relay only – no users may connect to it for any reason
	▪ External DNS
	  o The authoritative DNS server for the gef.com domain shall be hosted in this DMZ
	  o Arbitrary nodes on the Internet may connect to this server(s) for DNS. All other forms of access from the Internet shall be blocked.
	  o All forms of access from this DNS server(s) to the Internal Networks shall be blocked.
	  o No node from any Security Zone shall be permitted to query this DNS Server
	▪ Each node in this DMZ:
	  o Shall be configured only with private (RFC 1918) IP Addresses
	  o Shall – if intended to be available to the Internet – be available to the Internet as a distinct IP Address from GeF's IANA-assigned address pool via NAT or PAT
	  o Shall be hardened
	  o Shall run the minimum number of services required to perform its mission
	  o May be administered remotely from an Internal Network or from the Remote Employee DMZ, but only using encrypted connections.
	  o Shall be backed-up with directly connected hardware – if it is a host. Network devices' configurations shall be backed up over the network to a designated node in the Server Network.
	  o Shall not store sensitive information not required for its operation beyond the time taken to process it.
	▪ No user workstations my be hosted in this DMZ
	▪ Except for email relay and network device backups, all nodes in this DMZ shall be blocked from initiating a connection to any other Zone
	
	Other resources of a similar security profile may be added to this DMZ with the approval of the CISO.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Remote Employee DMZ	All resources that provide GeF employees (and other approved persons) with remote connectivity to non-public GeF resources shall be hosted in this DMZ. This may include support for the following types of access: ▪ Arbitrary nodes connecting from the Internet using encryption and strong authentication ▪ Arbitrary telephone callers connecting using encryption and strong authentication ▪ Arbitrary wireless (IEEE 802.11) nodes connecting using encryption and strong authentication ▪ Support for other types of access may be added with the approval of the CISO ▪ Once connected, GeF employees (and other approved persons): o Shall be assigned a DHCP IP address from this DMZ's subnet o Can then perform a user-level strong authentication with another NSD that will then grant and enforce access to those Zones and resources permitted to the user. ▪ All remote connectivity resources will authenticate connection attempts to a central authentication server located in this subnet. All communications to/from the authentication server will be encrypted. ▪ Each node in this DMZ: o Shall be configured only with private (RFC 1918) IP Addresses o Shall – if intended to be available to the Internet – be available to the Internet as a distinct IP Address from GeF's IANA-assigned address pool via NAT or PAT o Shall be hardened o Shall run the minimum number of services required to perform its mission o May be administered remotely from an Internal Network or from the Remote Employee DMZ, but only using encrypted connections. o Shall be backed-up with directly connected hardware – if it is a host. Network devices' configurations shall be backed up over the network to a designated node in the Server Network. o Shall not store sensitive information not required for its operation beyond the time taken to process it. ▪ Remote Employee DMZ resources may not provide Business Partners with remote access ▪ No user workstations my be hosted in this DMZ Other resources of a similar purpose and security profile may be added to this DMZ with the approval of the CISO.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Remote Partner DMZ	The following types of resources shall be hosted in this DMZ:
	▪ Product Staging Servers used to:
	  o Stage FCSs to be delivered by GeF to its wholesale customers
	  o Stage FCSs delivered to GeF by its suppliers
	▪ Resources that provide GeF Business Partners with remote connectivity to the Product Staging Servers. This can include support for the following types of access:
	  o Nodes on the far end of a dedicated, point-to-point, encrypted WAN link homed in this DMZ
	  o Arbitrary nodes connecting from the Internet using encryption and strong authentication
	  o Arbitrary telephone callers connecting using encryption and strong authentication
	  o Support for other types of access may be added with the approval of the CISO
	▪ Once connected, GeF Business Partners connecting via Dial-in or VPN from the Internet:
	  o Shall be assigned a DHCP IP address from this DMZ's subnet
	  o May then attempt to authenticate on a Product Staging Server
	▪ GeF Business Partners connecting via a WAN link have direct access to the Product Staging Servers. These servers will require username and password authentication – at a minimum – before granting access to the data they store.
	▪ Each node in this DMZ:
	  o Shall be configured only with private (RFC 1918) IP Addresses
	  o Shall – if intended to be available to the Internet – be available to the Internet as a distinct IP Address from GeF's IANA-assigned address pool via NAT or PAT
	  o Shall be hardened
	  o Shall run the minimum number of services required to perform its mission
	  o May be administered remotely from an Internal Network or from the Remote Employee DMZ, but only using encrypted connections.
	  o Shall be backed-up with directly connected hardware – if it is a host. Network devices' configurations shall be backed up over the network to a designated node in the Server Network.
	  o Shall not store sensitive information not required for its operation beyond the time taken to process it.
	▪ Each WAN Link shall be blocked from accessing each other WAN link
	▪ All nodes in this DMZ shall be blocked from initiating connections that leave this DMZ
	▪ Remote Partner DMZ Resources may not provide Employees with remote access
	▪ No user workstations my be hosted in this DMZ
	
	Other resources of a similar purpose and security profile may be added to this DMZ with the approval of the CISO.

© SANS Institute 2000 - 2002, Author retains full rights.

General Net	This Network will host any and all general resources and nodes that are not explicitly required to reside in another Zone. ▪ Each node in this DMZ: o Shall be configured only with private (RFC 1918) IP Addresses o May not receive inbound connections from the Internet o May not receive inbound connections from any DMZ other than the Remote Employee DMZ o May receive Windows NBT connections form authenticated users connected to the Employee VPN Server o May initiate the following outbound connections ▪ HTTP (TCP 80) and HTTPS (TCP 443) to the Internet ▪ All resources in the External DMZ that are available to the Internet ▪ All internal support resources in the Server Network o May be administered remotely from an Internal Network or from the Remote Employee DMZ, but only using encrypted connections. ▪ Each Server in this DMZ: o Shall be hardened o Shall run the minimum number of services required to perform its mission
Management Net	This Network will host any and all general resources and nodes that are not explicitly required to reside in another Zone. ▪ Each node in this DMZ: o Shall be configured only with private (RFC 1918) IP Addresses o May not receive inbound connections from the Internet o May not receive inbound connections from any DMZ other than the Remote Employee DMZ o May receive Windows NBT connections form authenticated users connected to the Employee VPN Server o May initiate the following outbound connections ▪ HTTP (TCP 80) and HTTPS (TCP 443) to the Internet ▪ All resources in the External DMZ that are available to the Internet ▪ All internal support resources in the Server Network o May be administered remotely from an Internal Network or from the Remote Employee DMZ, but only using encrypted connections. ▪ Each Server in this DMZ: o Shall be hardened o Shall run the minimum number of services required to perform its mission
Divination Net	This Network will host any and all general resources and nodes that are not explicitly required to reside in another Zone. ▪ Each node in this DMZ: o Shall be configured only with private (RFC 1918) IP Addresses o May not receive inbound connections from the Internet o May not receive inbound connections from any DMZ other than the Remote Employee DMZ o May receive Windows NBT connections form authenticated users connected to the Employee VPN Server o May initiate the following outbound connections ▪ HTTP (TCP 80) and HTTPS (TCP 443) to the Internet ▪ All resources in the External DMZ that are available to the Internet ▪ All internal support resources in the Server Network ▪ Whatever additional resources in the Server Network are required for Divination Production o May be administered remotely from an Internal Network or from the Remote Employee DMZ, but only using encrypted connections. ▪ Each Server in this DMZ: o Shall be hardened o Shall run the minimum number of services required to perform its mission

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Server Net	This Network will host any and all general resources and nodes that are not explicitly required to reside in another Zone. ▪ Each node in this DMZ: o Shall be configured only with private (RFC 1918) IP Addresses o May not receive inbound connections from the Internet o May receive connections from DMZ resources that are required for those resources to do their job o May not receive inbound connections from any other DMZ other than the Remote Employee DMZ o May receive Windows NBT connections form authenticated users connected to the Employee VPN Server o May initiate the following outbound connections ▪ HTTP (TCP 80) and HTTPS (TCP 443) to the Internet ▪ All resources in the External DMZ that are available to the Internet ▪ All internal support resources in the Server Network ▪ Whatever additional resources in the Server Network are required for Divination Production o May be administered remotely from an Internal Network or from the Remote Employee DMZ, but only using encrypted connections. ▪ Each Server in this DMZ: o Shall be hardened o Shall run the minimum number of services required to perform its mission

© SANS Institute 2000 - 2002, Author retains full rights.

GIAC e-Fortunes
GeF Network Security Architecture

1.0 Purpose and Scope

The purpose of this document is to define and document the Network Security Architecture of the GIAC e-Fortunes (GeF) division of GIAC Enterprises. It implements the Security Policies defined in the GeF Network Security Policy (NSP) document.

2.0 Approvals

We, the undersigned, approve and hereby implement this NSP, v2.3. All previous versions of this document are hereby superseded by this document.

Fred F. Flintstone — Date
President and Chief Executive Officer, GIAC e-Fortunes

Barney M. Rubble — Date
Chief Information Officer, GIAC e-Fortunes

3.0 Definitions:

Internal Network	A logical network containing trusted nodes
DMZ	De-Militarized Zone. A logical network that is more trusted than the Internet, but not as trusted as an Internal Network
Security Profile	A qualitative vulnerability assessment of a node/resource/object
NAT	Network Address Translation. The technique of using a 1-to-1 translation between public and private network addresses to protect and partially hide private nodes from public ones
PAT	Port Address Translation. The technique of using a 1-to-many translation between public and private network addresses to protect and partially hide private nodes from public ones
Packet Filtering	Packet filtering is a technique of controlling network traffic flowing through a control point. It works by individually evaluating each network packet against a set of rules defined for that control point. Once evaluated, each packet is either permitted to continue to its destination or dropped.
Stateful-inspection	An augmentation of packet-filtering. For those network protocols that have defined connection states (e.g. are 'stateful'), a record is kept of each connection and its current state. Each packet that is an expected part of a known connection is permitted to proceed its destination without going through each filter rule, resulting in a performance increase.
Proxy	A intermediate host, often a firewall, that intercepts, examines and controls network traffic between internal and external nodes in order to protect internal nodes from threats to their confidentiality, integrity and availability

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

NSP	Network Security Policy. The GeF Document that defines the corporate Network Security Policy.
NSA	Network Security Architecture. The GeF Document that defines the corporate Network Security Architecture
NSD	Network Security Device. Any device on the GeF Network that plays a part in the implementation of Security Policy.
MOTD	"Message of the Day." A TCP/IP-based GeF Proprietary network protocol for delivering FCSs to clients running Fortunate, the standalone FCS application, or to other MOTD-enabled applications developed using the MOTD SDK.
MOTD Request	An FCS Request message type used by the MOTD protocol. Sent from client to server on TCP 14140.
MOTD Reply	An FCS Response message type used by the MOTD protocol. Sent from server to client on TCP 14141.
FCS	Fortune Cookie Sayings. The primary GeF product delivered to retail customers vie http, email and MOTD, and to business partners in bulk by FTP.
Prophetic FCS	FCSs created by GeF using a trade secret process that actually prophesize the future.
Divination	The internal GeF name for the trade secret process used to create prophetic FCSs.

4.0 Design Philosophy

The fundamental design philosophy behind this the Network Security Architecture is the following:

- The outermost interface to the Internet shall provide packet-filtering on all traffic
- Externally-available nodes/resources shall be partitioned into groups of similar function and/or security profile
- Each group of externally-available nodes/resources shall be hosted in a dedicated DMZ
- All traffic that comes in from or goes out to the Internet shall be protected with NAT or PAT
- All traffic that comes in from or goes out to the Internet shall be controlled by a stateful-inspection firewall
- All traffic that comes in from the Internet to a DMZ or to an Internal Network shall be proxied
- All traffic flowing between DMZs shall be proxied
- All traffic flowing between a DMZ and an Internal Network shall be proxied
- Internal nodes/resources shall be partitioned into groups of similar function and/or security profile
- All traffic flowing between Internal Networks shall be controlled by a stateful-inspection firewall

© SANS Institute 2000 - 2002, Author retains full rights.

5.0 Network Security Architecture

GeF's Physical Security Architecture is shown below:

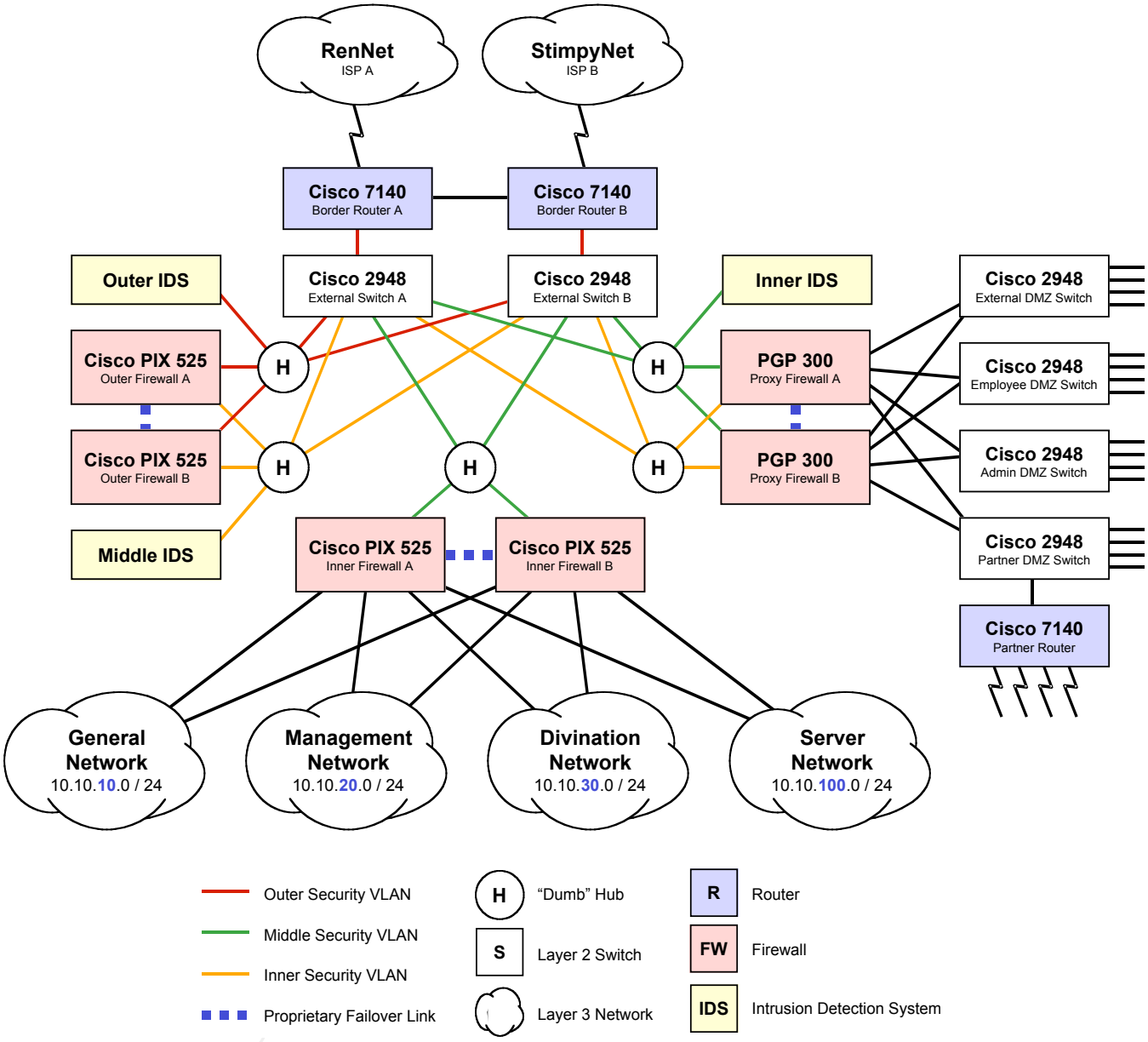


Figure 3.1 – Physical Network Security Architecture

In this diagram

- Each cloud in the diagram represents a Layer 2 Networks each with its own Subnet
- Each white circle labeled "H" represents a "dumb" ethernet hub
- Each white rectangle represents a Layer 2 ethernet switch
- Each blue rectangle represents a router
- Each pink rectangle represents a Firewall, either a Cisco Pix 525 stateful-inspection Firewall, or a PGP e-ppliance 300 proxying firewall (a.k.a. Gauntlet)
- Each yellow rectangle represents a Intrusion Detection System sensor
- Each dashed blue line represents a proprietary Failover link
- Each thin solid line represents a 100BaseT Ethernet connection

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- The thick solid line represents a 1000BaseT Ethernet connection trunking all VALNS between the outer ethernet switches, for automatic failover
- Each thin red solid line represents an 100BaseT connection on the Outer Security VLAN, which lies between the Outer Firewall and the Proxy Firewall
- Each thin yellow solid line represents an 100BaseT connection on the Middle Security VLAN, which lies between the Proxy Firewall and the Inner Firewall
- Each thin Green solid line represents an 100BaseT connection on the Inner Security VLAN

This Physical Network Security Architecture defines the following Logical Network Security Architecture:

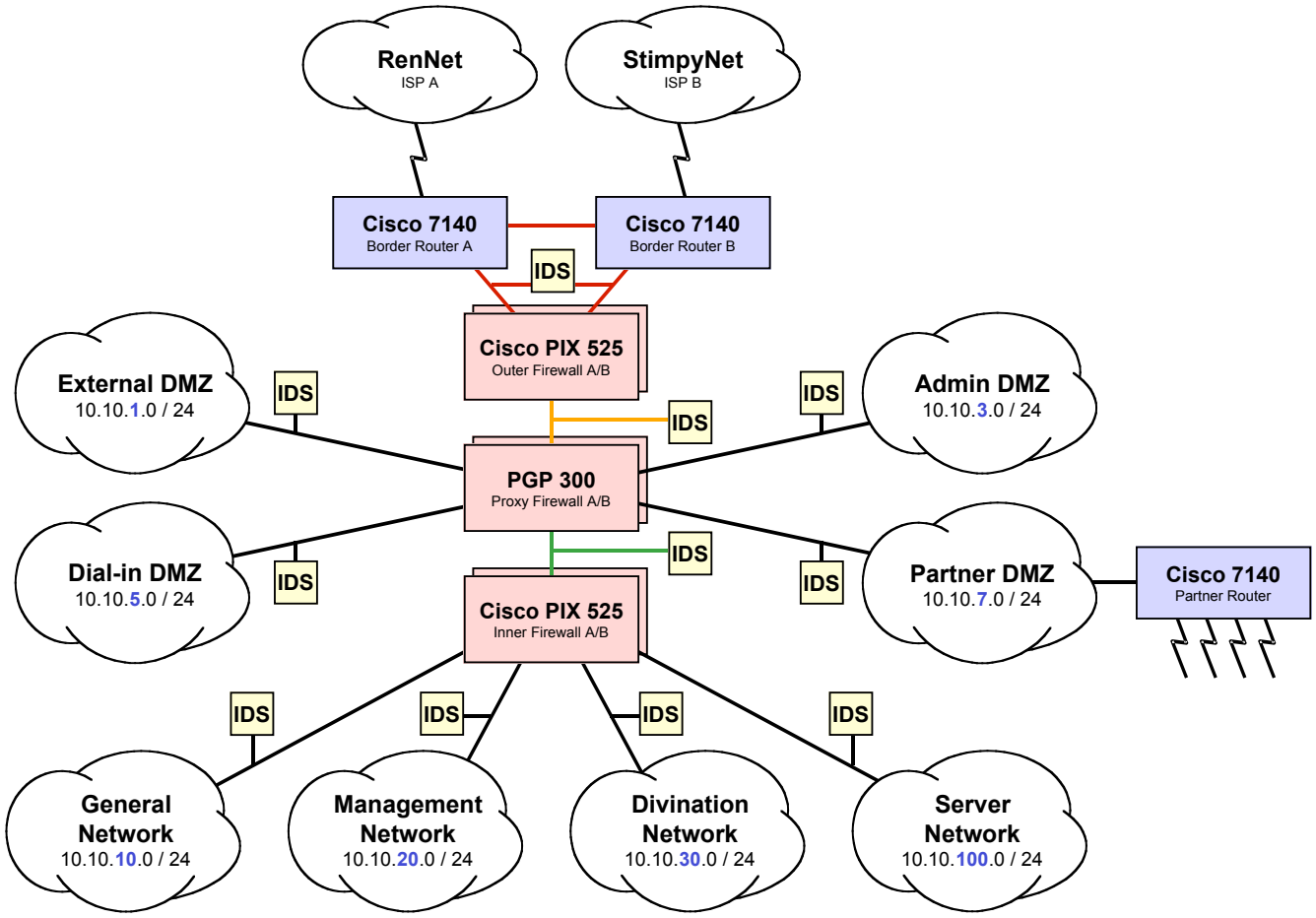


Figure 3.2 – Logical Network Security Architecture

In this diagram:

- Each cloud in the diagram represents a separate Network Security Zone with has its own security policy.
- Each rectangle represents a Network Security Device – a host or networking equipment item that performs a network security function. The security policy for each Zone is implemented by:
  - The Network Security Devices connected to that Zone
  - The configuration of each host in the Zone
  - The configuration of the applications running on each host in the Zone
  - Any manual procedures required in the use or administration of the resources in a Zone. (Note that, although manual procedures may be used to implement security policy, automated means shall be given strong preference in all cases.)
- Each rectangle represents a Network Security Device – a host or networking equipment item that performs a network security function.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Below is an overview of the core Network Security Architecture components and their functions:

- **Dual Internet Connections:** GeF has dual, 10Mb DS-3 ATM connections, each to a separate ISP, RenNet and StimpyNet, whose connections to the Internet are several router hops apart. Should either ISP experience an outage, all inbound Internet traffic will automatically be routed through the other ISP. The router hop separation also provides some natural load balancing between the two ISPs.
- **Dual Border Routers:** Each ISP is connected to a dedicated Cisco 7140 border router.
- **Dual External Switches:** Each border router is connected to a Cisco 2948 ethernet switch. Each switch supports the three special purpose Security VLANs that host no nodes other than security devices.
- **Outer Security VLAN:** Connects, at Layer 2, the Border routers to the outer Firewalls. A single 100BaseT ethernet hub is used to connect the outer interfaces of the two Outer Pix 525 Firewalls to Outer Security VLAN ports on each external switch. This VLAN also hosts an IDS sensor.
- **Dual Outer Firewalls:** Dual Cisco Pix 525 stateful-inspection firewalls in a failover configuration. Their primary purpose is to provide an outer perimeter and to perform NAT/PAT translations between the internal private addresses and the externally available "real" (RFC 1918) IP Addresses.
- **Middle Security VLAN:** Connects, at Layer 2, the outer stateful-inspection Firewalls to the PGP 300 proxying firewalls. A second 100BaseT ethernet hub connects the two inner interfaces of the Outer Pix 525's to a Middle Security VLAN ports on each external switch. A third 100BaseT ethernet hub connects the two outer interfaces of the PGP 300 firewalls to Middle Security VLAN ports on each external switch. This VLAN also hosts an IDS sensor.
- **Dual Proxying Firewalls:** Dual PGP 300 e-ppliance proxying firewalls in a failover configuration. Their purpose is to:
    - Proxy all traffic/services that go between the Internet and the DMZs
    - Proxy all traffic/services that go between the Internet and the Internal Networks
    - Proxy all traffic/services that go between the DMZs
    - Proxy all traffic/services that go between the DMZs and the Internal Networks

Each PGP 300 has six interfaces: an outer, and inner and four for DMZs. The DMZ Interfaces of each PGP 300 are connected to one of four DMZ switches that feed the four DMZs.

- **Inner Security VLAN:** Connects, at Layer 2, the PGP 300 firewalls to the Inner Pix 525 firewalls. A fourth 100BaseT ethernet hub is used to connect the two inner interfaces of the PGP 300 Firewalls to an Inner Security VLAN port on each external switch. A fifth 100BaseT ethernet hub is used to connect the two outer interfaces of the Inner Pix 525 firewalls to an Inner Security VLAN port on each external switch. This VLAN also hosts an IDS sensor.
- **Dual Inner Firewalls:** Dual Cisco Pix 525 stateful-inspection firewalls in a failover configuration. Their primary purpose is to partition the GeF internal networks and control the traffic flowing between them. The inner interfaces of the Inner Pix Firewalls are directly connected to the switches that feed the four GeF internal networks. This single logical firewall therefore acts as the router that connects these four internal networks together and to the outside world.

Note the following:

- In order to protect the Availability of the network, all major network security architecture components have a hot standby configured and ready to take on all traffic in the event of a component failure. The only exceptions are the hubs, which are simple, stable, cheap and plentiful. At least 3 spares are kept on hand at all times.
- Each firewall pair is joined into a single logical firewall via a proprietary fail-over link that instantly informs the backup firewall in the event of a failure of the primary firewall. If a failure is detected in the primary firewall, the backup firewall will automatically take over all functionality. Switch-over latency is low enough so that the vast majority of users should notice no more than a momentary delay.
- "Dumb" hubs are used to connect logical firewall pairs to the ethernet switch for the following reasons:
    - The firewall pairs are in hot-standby configuration and do no load share, therefore no performance would be gained by replacing the hub with separate connections to dedicated switch ports.
    - The firewalls have identical IP addresses, so a switch could be confused by a fail-over event
    - The hubs themselves are cheap and very reliable, so plenty can be kept on hand in case of failure
    - The spare ports on the hubs allow IDS systems (as well as diagnostic tools) to be connected to VLANs without having to mirror ports on a switch.
    - The ease with which devices can be connected to these hubs is a security risk, so the hubs must be protected with appropriate physical security.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

As required by the GeF Network Security Policy (NSP), the GeF Network is partitioned into Security Zones. Each Zone has a unique set of functional requirements based on the resources it contains, and therefore has its own set of security policies. In order to implement these distinct policies by Zone, we do the following:

- The Internet, each DMZ and each Internal Network shall be defined as a separate Security Zone
- All intra-Zone network traffic shall be required to pass through at least one Firewall
- All intra-Zone network traffic shall be monitored by an Intrusion Detection System
- All (non-Internet) external connectivity shall be hosted in a Zone designated as an untrusted DMZ

In order to implement the Zone policies, we will, in this document:

- Describe the purpose of and resources in each Zone (Section 6.0)
- Define the intra-Zone Data Flows (Section 7.0)
- Define the remaining external Data Flows (Section 8.0)
- Define the configuration of each policy-implementing Security Device (Appendices 1-37)

6.0 GeF Security Zones, Purposes and Contents

As defined in the GeF NSP, the nine GeF Security Zones are:

- Internet
- External DMZ
- Admin DMZ
- Employee DMZ
- Partner DMZ
- General Net
- Management Net
- Divination Net
- Server Net

The contents of each Zone are given below:

Internet
Hosts GeF online customers. Also hosts the majority of threats to GeF information security

External DMZ (10.10.1.0 / 24)
An untrusted DMZ designed to host those resources that are addressable and available to GeF customers over the Internet. Hosts the following resources:

- **External Web Servers (Internal: 10.10.1.80-82 / NAT: gef.corp.net.80-82)** – Servers that host the GeF Corporate Website. These servers use http (TCP 80) as a starting point for online customers to purchase FCSs or FCS subscriptions. The Corporate Website uses shopping cart architecture to allow users to select products for purchase, and then transitions to https (TCP 443) once sensitive customer information needs to be entered online. All sensitive customer information captured by the Corporate Website is stored on customer database servers on the Server Network. No sensitive customer information is stored on these Webservers or anywhere else in the External DMZ.
- **FCS Delivery Mail Server (Internal: 10.10.1.26 / NAT: gef.corp.net.26)** – Mail Servers dedicated to the delivery of customer FCSs and FCS Subscriptions via email. These are not used for general gef.com internal email, although email delivery to internal GeF 'customers' is supported.
- **MOTD Servers (Internal: 10.10.1.140-141 / NAT: gef.corp.net.140-141)** – Servers that deliver FCSs and FCS subscriptions to customers via GeF's proprietary MOTD protocol (MOTD Request TCP 14140, MOTD Delivery TCP 14141). This protocol is used to deliver FCSs to users of Fortunate, the standalone FCS application, or to other MOTD-enabled applications developed using the MOTD SDK.
- **FTP Drop Box (Internal: 10.10.1.21 / NAT: gef.corp.net.21)** – An FTP drop box that is available to the Internet and to nodes on the Internal networks

Admin DMZ (10.10.3.0 / 24)
An untrusted DMZ specifically designed to host the following two resources:

- **External Mail Server (Internal: 10.10.3.25 / NAT: gef.corp.net.25)** – The externally available Email Relay. The DNS MX record for the gef.com domain points to this server
- **External/External DNS Server (Internal: 10.10.3.53 / NAT: gef.corp.net.53)** – The authoritative DNS Server for the gef.com domain. Part of the Split/Split DNS architecture – not used by internal users.

© SANS Institute 2000 - 2002, Author retains full rights.

Employee DMZ (10.10.5.0 / 24)

An untrusted DMZ designed to host those resources that give GeF employees remote access to the GeF Internal Network, and other resources with a similar level of trust. Hosts the following resources:

- **Employee Dial-in/VPN Server (Internal: 10.10.5.100 / NAT: gef.corp.net.100)** – A Cisco VPN 3030 remote access server providing employees with both IPSec (3DES, SHA) VPN-protected telephone dial-in access, and IPSec (3DES, SHA) VPN connectivity over the Internet. Fed by a single T-1 for incoming phone connections.
- **Employee Authentication Server (Internal: 10.10.5.65 / NAT: gef.corp.net.65)** – A TACACS+ authentication server dedicated for Employee Dial-in/VPN services. Also provides strong authentication via ACE/SecurID running locally to support one-time passwords for remote administrative access by IT Staff members
- **External/Internal DNS Server (Internal: 10.10.5.153 / NAT: gef.corp.net.153)** – Exclusively handles recursive and iterative DNS queries made by internal nodes.
- **External Syslog Server (Internal: 10.10.5.55 / NAT: gef.corp.net.55)** – Syslog server to which all externally oriented Network Security Devices (NSDs) log their messages. This includes all devices in DMZs, plus the Border Routers, External Switches, Outer Firewalls and Proxying firewalls. Syslog server/clients are custom-configured to use TCP 5555 to send/receive syslog messages.

Partner DMZ (10.10.7.0 / 24)

An untrusted DMZ designed to host those resources that provide network connectivity with GeF Business Partners, and other resources with a similar level of trust. Hosts the following resources:

- **FCS Staging Server (Internal: 10.10.7.20-30 / NAT: none)** – Servers for storing/staging FCS deliveries to/from Business Partners. Support bulk FCS deliveries received by GeF from Suppliers, and sent by GeF to wholesale Customers
- **Point-to-point WAN Links** – WAN Links to those customers and suppliers with whom the volume of transfers merits the cost.
- **Partner Dial-in/VPN Server (Internal: 10.10.7.200 / NAT: gef.corp.net.200)** - A Cisco VPN 3030 remote access server providing Business Partners with both IPSec (3DES, SHA) VPN-protected telephone dial-in access, and IPSec (3DES, SHA) VPN connectivity over the Internet. Fed by a single T-1 for incoming phone connections.
- **Partner Authentication (Internal: 10.10.7.65 / NAT: none)** – A TACACS+ authentication server dedicated for Business Partner Dial-in/VPN services.

General Net (10.10.10.0 / 24)

A trusted internal network designed to host General GeF Resources. Hosts the following resources:

- **The GEF1 NT Master Domain (PAT: gef.corp.net.250)** – A standalone Windows NT Domain containing all the servers, accounts and other resources needed to support all Zone Windows users
- **Writing Staff Nodes (PAT: gef.corp.net.250)** – Windows workstations used by the FCS Writing Staff
- **Editorial Nodes (PAT: gef.corp.net.250)** – Windows workstations used by the FCS Editorial Staff
- **Admin Staff Nodes (PAT: gef.corp.net.250)** – Windows workstations used by the Administrative Staff
- **IT Staff Nodes** (**Internal: 10.10.10.200-240 / NAT: gef.corp.net.220)** – Windows and Unix workstations used by the IT Support Staff
- **Printers** – Network printers available to nodes on all internal networks

Management Net (10.10.20.0 / 24)

A trusted internal network designed to host those resources that store and process business-sensitive data that are not GeF Trade Secrets. For example: business plans, marketing plans, budgets, HR-related information. Hosts the following resources:

- **The IVRYTWR NT Master Domain (PAT: gef.corp.net.251)** – A standalone Windows NT Domain containing all the servers, accounts and other resources needed to support all Zone Windows users
- **Senior Management Staff Nodes (PAT: gef.corp.net.251)** – Windows workstations used by GeF Senior Managers and Executives
- **HR & Financial Staff Nodes (PAT: gef.corp.net.251)** – Windows workstations used by GeF HR and Financial Staff
- **HR & Financial Staff Servers (PAT: gef.corp.net.251)** – Windows and Unix Servers that store and process HR, Financial and other business-sensitive information. For example: payroll applications, PeopleSoft, contracts, etc.
- **Printers** – Network printers available to nodes on all internal networks

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Divination Net (10.10.30.0 / 24)
An trusted internal network designed to host those resources that store and process GeF Trade Secrets. Hosts the following resources:

- **The DIVINE NT Master Domain (PAT: gef.corp.net.252)** – A standalone Windows NT Domain containing all the servers, accounts and other resources needed to support all Domain users
- **Divination Engineer's Nodes (PAT: gef.corp.net.252)** – Unix Workstations used by GeF Divination Engineers to design develop, integrate and the test proprietary GeF Divination hardware and software used in the production Divination Servers
- **Divination Development Servers (PAT: gef.corp.net.252)** – Development Divination Servers used by Divination Engineers to develop the proprietary hardware and software that produces Prophetic FCSs
- **Divination Production Servers (PAT: gef.corp.net.252)** – Production Divination Servers used create Prophetic FCSs to meet customer sales, subscriptions and SLAs
- **Printers** – Network printers available to nodes on all internal networks

Server Net (10.10.40.0 / 24)
A trusted internal network designed to host those resources that store and process sensitive customer information, products awaiting delivery, and internal network infrastructure resources. Hosts the following resources:

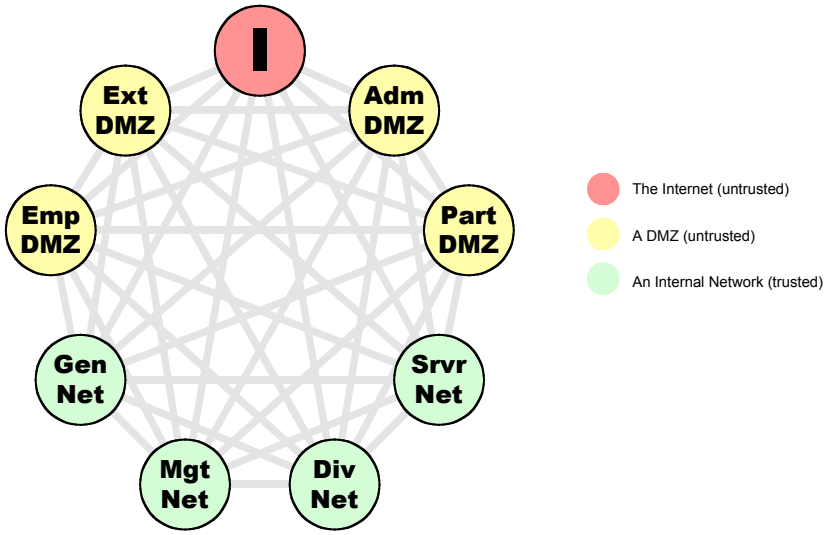
- **The GEF2 NT Master Domain (PAT: gef.corp.net.253)** – A standalone Windows NT Domain containing the servers, accounts and other resources needed to support the Server Net's mission and all Domain users
- **Certificate Servers (PAT: none)** – A standalone Certificate Authority dedicated for GeF internal use
- **Customer Database Servers (PAT: gef.corp.net.253)** – Oracle 8 Database Servers containing all Customer-related information, including Credit Card numbers. All sensitive customer information captured by the Corporate Website is stored here. No sensitive customer information is stored on the Corporate Webservers or anywhere else.
- **FCS Storage Servers (PAT: gef.corp.net.253)** – Servers storing Prophetic FCSs after production is complete, but before the delivery process begins. Note the following:
    - Prophetic FCSs to be delivered via email or the Corporate Website are pulled directly from these servers by the FCS Delivery Mail Server using Certificate-authenticated POP
    - Bulk Prophetic FCSs shipments are moved via FTP from these servers to the FCS Staging Servers in the Partner DMZ
- **Network Management Nodes (PAT: gef.corp.net.253)** – Nodes used by the IT Staff to administer and monitor GeF network devices, hosts and NSDs. All administrative access is done with SSH. Resource health is monitored with ICMP and SNMP, while service availability is monitored using connection attempts directly to listening ports.
- **Internal/Internal DNS Servers (PAT: gef.corp.net.253)** – Internal DNS Servers used exclusively by nodes on the GeF Internal Networks. Recursive and Iterative DNS queries are passed to the External/Internal DNS server in the Employee DMZ
- **Internal Mail Servers (PAT: gef.corp.net.253)** – Mail servers that service users on the GeF Internal Networks. Uses SMTP to communicate with the External Mail Server in the Admin DMZ. All internal Email clients are POP.
- **Internal Syslog Server (PAT: gef.corp.net.253)** – Syslog server to which nodes on the GeF Internal Networks send their messages. Syslog messages from the Internal Pix Firewalls are also sent here. Syslog server/clients are custom-configured to use TCP 5555 to send/receive syslog messages.
- **Printers** – Network printers available to nodes on all internal networks

7.0 Intra-Zone Data Flows

Now that we know the contents of each Zone, we can determine the Intern-Zone Data Flows. First, we will create a labeling system to identify all possible flows (7.1), then we will document the actual data flows that must occur (7.2 – 7.9).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7.1 All Possible Data Flows



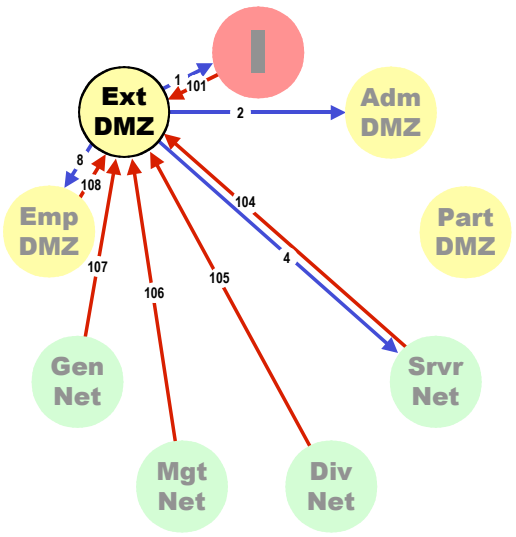
Label	*Zone*	*Direction*	*Zone*
1	Ext DMZ	->	Internet
2	Ext DMZ	->	Adm DMZ
3	Ext DMZ	->	Part DMZ
4	Ext DMZ	->	Srvr Net
5	Ext DMZ	->	Div Net
6	Ext DMZ	->	Mgt Net
7	Ext DMZ	->	Gen Net
8	Ext DMZ	->	Emp DMZ
9	Internet	->	Adm DMZ
10	Internet	->	Part DMZ
11	Internet	->	Srvr Net
12	Internet	->	Div Net
13	Internet	->	Mgt Net
14	Internet	->	Gen Net
15	Internet	->	Emp DMZ
16	Adm DMZ	->	Part DMZ
17	Adm DMZ	->	Srvr Net
18	Adm DMZ	->	Div Net
19	Adm DMZ	->	Mgt Net
20	Adm DMZ	->	Gen Net
21	Adm DMZ	->	Emp DMZ
22	Part DMZ	->	Srvr Net
23	Part DMZ	->	Div Net
24	Part DMZ	->	Mgt Net
25	Part DMZ	->	Gen Net
26	Part DMZ	->	Emp DMZ
27	Srvr Net	->	Div Net
28	Srvr Net	->	Mgt Net
29	Srvr Net	->	Gen Net
30	Srvr Net	->	Emp DMZ
31	Div Net	->	Mgt Net
32	Div Net	->	Gen net
33	Div Net	->	Emp DMZ
34	Mgt Net	->	Gen Net
35	Mgt Net	->	Emp DMZ
36	Gen Net	->	Emp DMZ

Label	*Zone*	*Direction*	*Zone*
101	Ext DMZ	<-	Internet
102	Ext DMZ	<-	Adm DMZ
103	Ext DMZ	<-	Part DMZ
104	Ext DMZ	<-	Srvr Net
105	Ext DMZ	<-	Div Net
106	Ext DMZ	<-	Mgt Net
107	Ext DMZ	<-	Gen Net
108	Ext DMZ	<-	Emp DMZ
109	Internet	<-	Adm DMZ
110	Internet	<-	Part DMZ
111	Internet	<-	Srvr Net
112	Internet	<-	Div Net
113	Internet	<-	Mgt Net
114	Internet	<-	Gen Net
115	Internet	<-	Emp DMZ
116	Adm DMZ	<-	Part DMZ
117	Adm DMZ	<-	Srvr Net
118	Adm DMZ	<-	Div Net
119	Adm DMZ	<-	Mgt Net
120	Adm DMZ	<-	Gen Net
121	Adm DMZ	<-	Emp DMZ
122	Part DMZ	<-	Srvr Net
123	Part DMZ	<-	Div Net
124	Part DMZ	<-	Mgt Net
125	Part DMZ	<-	Gen Net
126	Part DMZ	<-	Emp DMZ
127	Srvr Net	<-	Div Net
128	Srvr Net	<-	Mgt Net
129	Srvr Net	<-	Gen Net
130	Srvr Net	<-	Emp DMZ
131	Div Net	<-	Mgt Net
132	Div Net	<-	Gen Net
133	Div Net	<-	Emp DMZ
134	Mgt Net	<-	Gen Net
135	Mgt Net	<-	Emp DMZ
136	Gen Net	<-	Emp DMZ

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7.2 Data Flows In and Out of the External DMZ

External DMZ contains:
- External Web Servers
- FCS Delivery Mail Server
- MOTD Server
- FTP Drop Box



The Internet (untrusted)
A DMZ (untrusted)
An Internal Network (trusted)

Outbound from the External DMZ:

1. To the Internet:
   a. SMTP (TCP 25) from the FCS Delivery Server to any
   b. MOTD Delivery (TCP 14141) from the MOTD Server to any
2. To the Admin DMZ:
   a. SMTP (TCP 25) from the FCS Delivery Server to the External Email Server
4. To the Server Network:
   a. Oracle (TCP 1525, 1630) from the Web Servers to FCS Storage Servers and Customer Database Servers
8. To the Employee DMZ
   a. DNS (UDP/TCP 53) from any to the Ext/Int DNS Server
   b. Syslog output (on Custom TCP 5555) from any to External Syslog Server

Inbound to the External DMZ

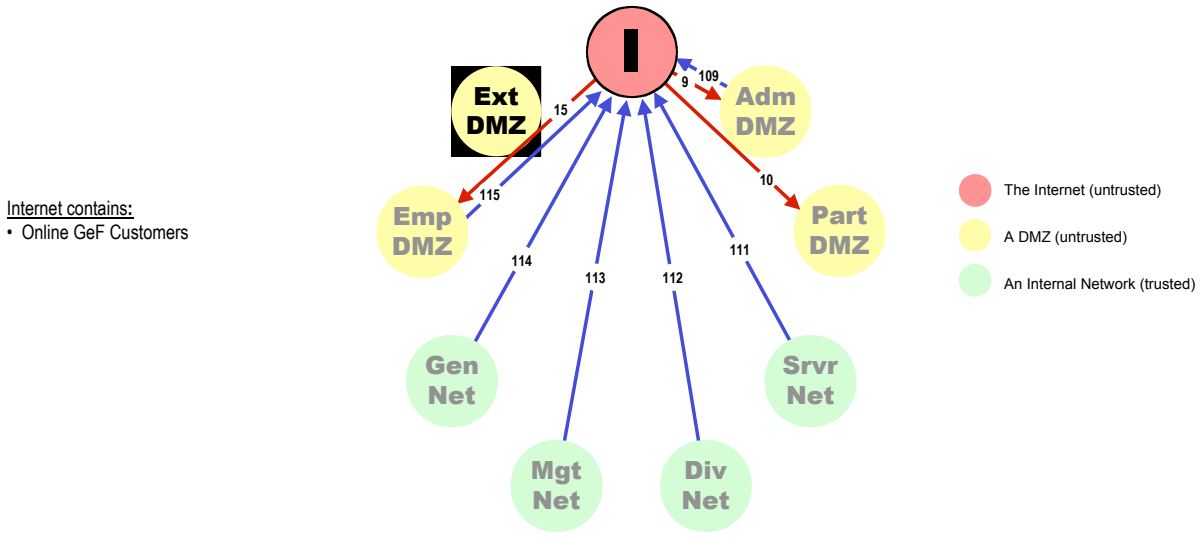
101. From the Internet:
   a. HTTP (TCP 80), HTTPS (TCP 443) from any to the Web Servers
   b. FTP (TCP 20, 21) from any to the FTP Drop Box
   c. MOTD Request (TCP 14140) from any to the MOTD Server
104. From the Server Network:
   a. Connectivity 101
   b. SSH (TCP 22) from any to any
   c. SNMP (TCP 161) from the Network Management Node to any
105. From the Divination Network:
   a. Connectivity 101
106. From the Management Network:
   a. Connectivity 101
107 From the General Network:
   a. Connectivity 101
   b. DNS (UDP/TCP 53) from any to the Ext/Ext DNS Server
   c. SSH (TCP 22) from IT Staff Desktop Workstations to any
   d. SNMP (TCP 161) from IT Staff Desktop Workstations to any
108. From the Employee DMZ:
   a. Connectivity 101
   b. SSH (TCP 22) from authenticated IT Staff users to any
   c. SNMP (TCP 161) from authenticated IT Staff users to any

Intra-Zone ICMP Policy for the External DMZ:

- ICMP Echo Requests permitted inbound from Internal Networks and Employee DMZ only
- ICMP Echo Replies permitted outbound to Internal Networks and Employee DMZ only
- All other ICMP blocked in and out

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7.3 Data Flows In from and Out to the Internet



Inbound from the Internet:

9. To the Admin DMZ:
   a. DNS (UDP/TCP 53) from any to the Ext/Ext DNS Server
   b. SMTP (TCP 25) from any to the External Email Server
10. To the Partner DMZ:
   a. IPSec (UDP 500, IP Proto 50, 51) from any to the Partner VPN Server
15. To the Employee DMZ
   a. IPSec (UDP 500, IP Proto 50, 51) from any to the Employee VPN Server

Outbound to the Internet

109. From the Admin DMZ:
   a. SMTP (TCP 25) from the External Email Server to any
111. From the Server Network:
   a. HTTP (TCP 80, 8080), HTTPS (TCP 443) from any to any
112. From the Divination Network:
   a. HTTP (TCP 80, 8080), HTTPS (TCP 443) from any to any
113. From the Management Network:
   a. HTTP (TCP 80, 8080), HTTPS (TCP 443) from any to any
114. From the General Network:
   a. HTTP (TCP 80, 8080), HTTPS (TCP 443) from any to any
   b. SSH (TCP 22) from IT Staff Desktop Workstations to any
   c. Telnet (TCP 23) from IT Staff Desktop Workstations to any
115. From the Employee DMZ:
   a. HTTP (TCP 80, 8080), HTTPS (TCP 443) from any to any
   b. SSH (TCP 22) from authenticated IT Staff users to any
   c. Telnet (TCP 23) from authenticated IT Staff users to any

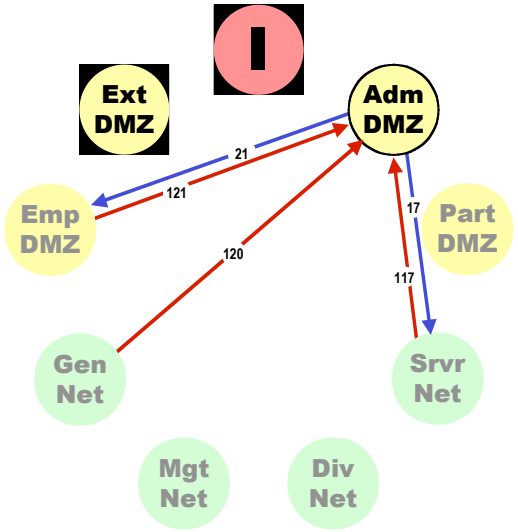
Intra-Zone ICMP Policy for the Internet:

- ICMP Echo Requests permitted outbound to the Internet from IT Staff Desktop Workstations in the General Net
- Following ICMP message types permitted inbound from the Internet to IT Staff Desktop Workstations in the General Net:
  - Echo Reply
  - Unreachable
  - TTL Exceeded
- All other ICMP blocked out to or in from the Internet

© SANS Institute 2000 - 2002, Author

7.4 Data Flows In and Out of the Admin DMZ

Admin DMZ contains:
- External Email Server
- Ext/Ext DNS Server



Outbound from the Admin DMZ:

17. To the Server Net:
    a. SMTP (TCP 25) from the Internal Mail Servers to the External Mail Server
21. To the Employee DMZ:
    a. Syslog output (on Custom TCP 5555) from any to External Syslog Server

Inbound to the Admin DMZ

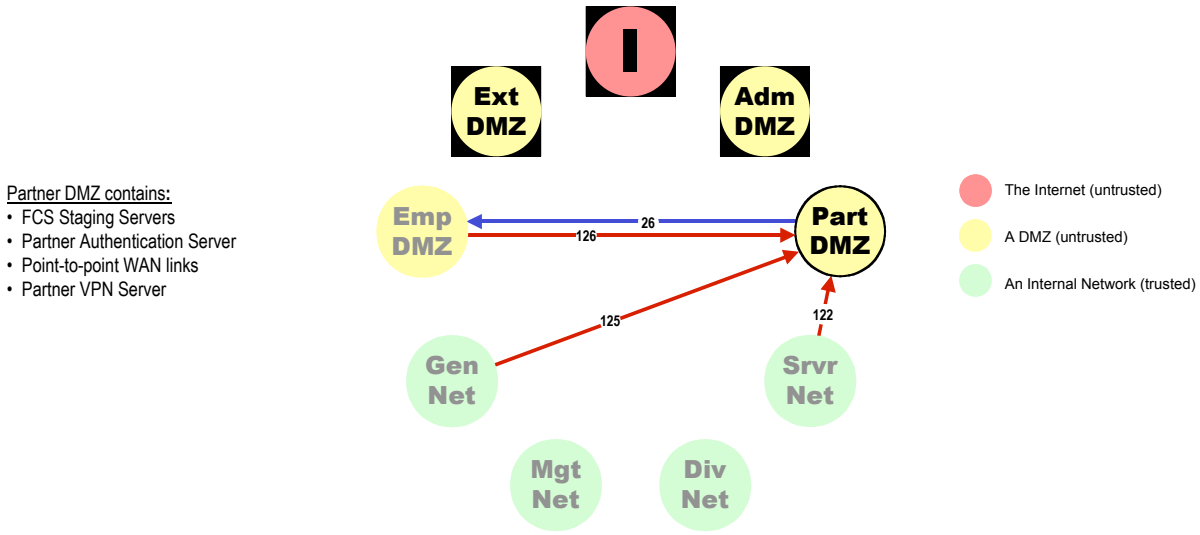
117. From the Server Net:
    a. SMTP (TCP 25) from the Internal Mail Servers to the External Mail Server
    b. SSH (TCP 22) from any to any
    c. SNMP (TCP 161) from the Network Management Node to any
120. From the General Network:
    a. SSH (TCP 22) from IT Staff Desktop Workstations to any
    b. SNMP (TCP 161) from IT Staff Desktop Workstations to any
121. From the Employee Network:
    a. SSH (TCP 22) from authenticated IT Staff users to any
    b. SNMP (TCP 161) from authenticated IT Staff users to any

Intra-Zone ICMP Policy for the Admin DMZ:

- ICMP Echo Requests permitted inbound from Internal Networks and Employee DMZ only
- ICMP Echo Replies permitted outbound to Internal Networks and Employee DMZ only
- All other ICMP blocked in and out

© SANS Institute 2000 - 2002, Author retains full rights.

7.5 Data Flows In and Out of the Partner DMZ



Outbound from the Partner DMZ:

26. To the Employee DMZ:
    a. Syslog output (on Custom TCP 5555) from any to External Syslog Server

Inbound to the Partner DMZ:

122. From the Server Net:
    a. SSH (TCP 22) from any to any
    b. SNMP (TCP 161) from the Network Management Node to any

125. From the General Network:
    a. SSH (TCP 22) from IT Staff Desktop Workstations to any
    b. SNMP (TCP 161) from IT Staff Desktop Workstations to any

126. From the Employee Network:
    a. SSH (TCP 22) from authenticated IT Staff users to any
    b. SNMP (TCP 161) from authenticated IT Staff users to any

Intra-Zone ICMP Policy for the Partner DMZ:

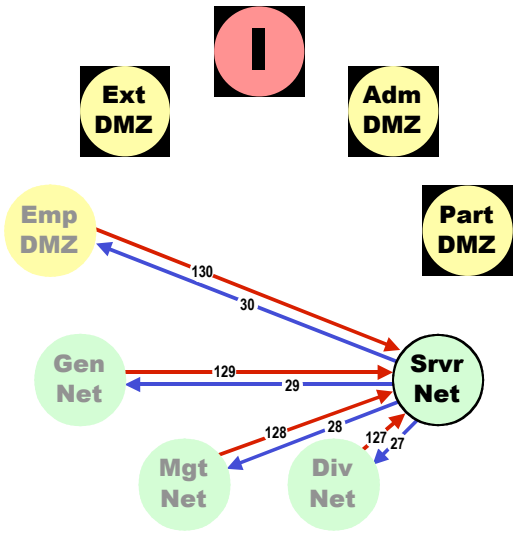
- ICMP Echo Requests permitted inbound from the following:
  - Network Management Node in the Server Net
  - IT Staff Desktop Workstations in the General Net
  - Authenticated IT Staff users from the Employee DMZ
- ICMP Echo Replies, Unreachable and TTL Exceeded messages permitted outbound to the following:
  - Network Management Node in the Server Net
  - IT Staff Desktop Workstations in the General Net
  - Authenticated IT Staff users from the Employee DMZ
- All other ICMP blocked in and out

© SANS Institute 2000 - 2002, Author

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7.6 Data Flows In and Out of the Server Net

Server Network contains :
- **GEF2** NT Master Domain
- Customer Database Servers
- FCS Storage Servers
- Network Management Nodes
- Int/Int DNS Servers
- Internal Mail Servers
- Internal FTP Server
- Internal SYSLOG Server
- Printers



The Internet (untrusted)
A DMZ (untrusted)
An Internal Network (trusted)

Outbound from the Server Net:

27. To the Divination Net:
    a. SSH (TCP 22) from any to any
    b. SNMP (TCP 161) from the Network Management Node to any
28. To the Management Net:
    a. Connectivity 27
29. To the General Net:
    a. Connectivity 27
30. To the Employee Net:
    a. Connectivity 27

Inbound to the Server Net:

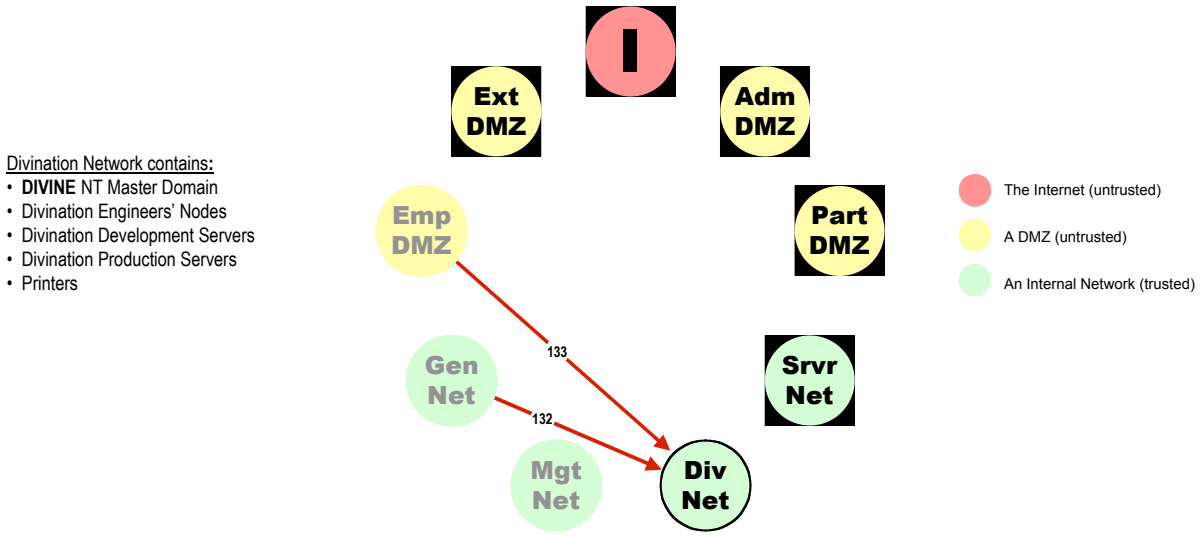
127. From the Divination Net:
    a. DNS (TCP/UDP 53) to the Int/Int DNS Server
    b. POP3 (TCP 110) to the Internal Mail Servers
    c. FTP (TCP 20, 21) to the Internal FTP Server
    c. Syslog output (on Custom TCP 5555) from any to the Internal Syslog Server
    d. Oracle (TCP 1525, 1630) from the Production Divination Servers to FCS Storage Servers
    e. Oracle (TCP 1525, 1630) from any to Customer Database Servers
128. From the Management Net:
    a. Connectivity 127
129. From the General Net:
    a. Connectivity 127
    b. SSH (TCP 22) from IT Staff Desktop Workstations to any
    c. SNMP (TCP 161) from IT Staff Desktop Workstations to any
130. From the Employee Net:
    a. Connectivity 127
    b. SSH (TCP 22) from authenticated IT Staff users to any
    c. SNMP (TCP 161) from authenticated IT Staff users to any
    d. Windows Connectivity (TCP/UDP 135,137-139, 445, TCP 1213) from authenticated IT Staff users to any

Intra-Zone ICMP Policy for the Server Net:

- ICMP Echo Requests permitted inbound from the following:
    - IT Staff Desktop Workstations in the General Net
    - Authenticated IT Staff users from the Employee DMZ
- ICMP Echo Replies, Unreachable and TTL Exceeded messages permitted outbound to the following:
    - IT Staff Desktop Workstations in the General Net
    - Authenticated IT Staff users from the Employee DMZ
- All other ICMP blocked in and out

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7.7 Data Flows In and Out of the Divination Net



Inbound to the Divination Net:

132. From the General Net:
   a. SSH (TCP 22) from IT Staff Desktop Workstations to any
   b. SNMP (TCP 161) from IT Staff Desktop Workstations to any

133. From the Employee Net:
   a. SSH (TCP 22) from authenticated IT Staff users to any
   b. SNMP (TCP 161) from authenticated IT Staff users to any
   c. Windows Connectivity (TCP/UDP 135,137-139, 445, TCP 1213) from authenticated IT Staff users to any

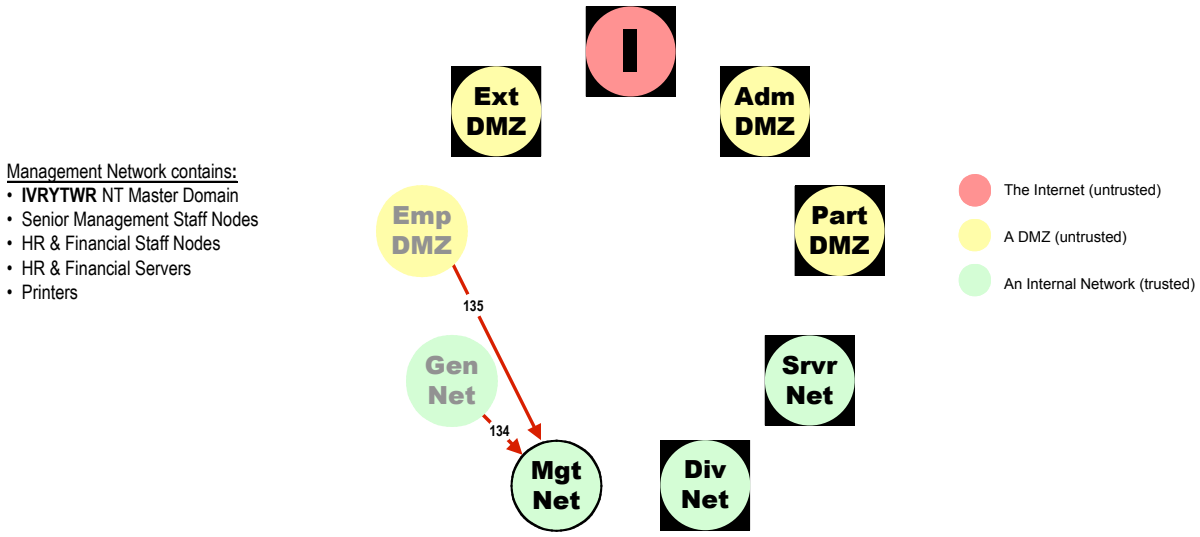
Intra-Zone ICMP Policy for the Divination Net:

- ICMP Echo Requests permitted inbound from the following:
  - IT Staff Desktop Workstations in the General Net
  - Authenticated IT Staff users from the Employee DMZ
- ICMP Echo Replies, Unreachable and TTL Exceeded messages permitted outbound to the following:
  - IT Staff Desktop Workstations in the General Net
  - Authenticated IT Staff users from the Employee DMZ
- All other ICMP blocked in and out

© SANS Institute 2000 - 2002 Author

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7.8 Data Flows In and Out of the Management Net



Inbound to the Management Net:

134. From the General Net:
    a. SSH (TCP 22) from IT Staff Desktop Workstations to any
    b. SNMP (TCP 161) from IT Staff Desktop Workstations to any
135. From the Employee Net:
    a. SSH (TCP 22) from authenticated IT Staff users to any
    b. SNMP (TCP 161) from authenticated IT Staff users to any
    c. Windows Connectivity (TCP/UDP 135,137-139, 445, TCP 1213) from authenticated IT Staff users to any

Intra-Zone ICMP Policy for the Management Net:

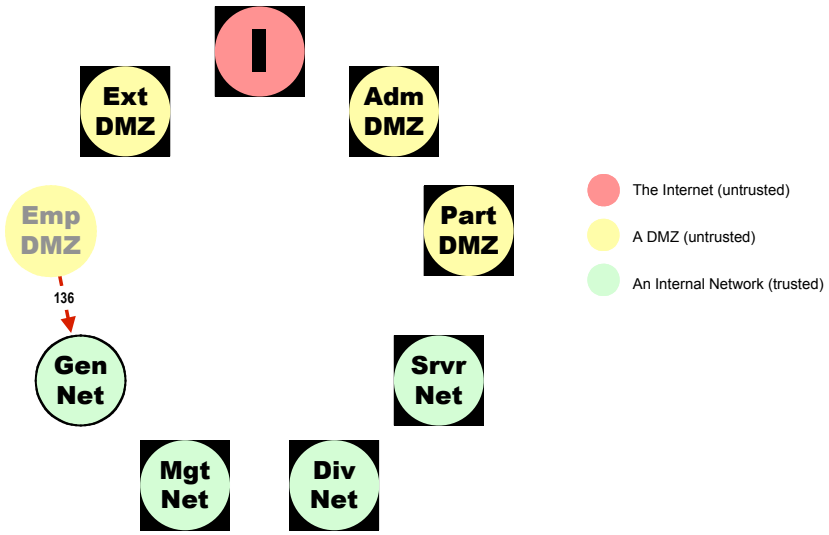
- ICMP Echo Requests permitted inbound from the following:
    - IT Staff Desktop Workstations in the General Net
    - Authenticated IT Staff users from the Employee DMZ
- ICMP Echo Replies, Unreachable and TTL Exceeded messages permitted outbound to the following:
    - IT Staff Desktop Workstations in the General Net
    - Authenticated IT Staff users from the Employee DMZ
- All other ICMP blocked in and out

© SANS Institute 2000 - 2002 Author

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7.9 Data Flows In and Out of the General Net

General Network contains:
- **GEF1** NT Master Domain
- Writing Staff Nodes
- Editorial Staff Nodes
- Admin Staff Nodes
- IT Staff Nodes
- Printers



Inbound to the General Net:

136. From the Employee Net:
   a. SSH (TCP 22) from authenticated IT Staff users to any
   b. SNMP (TCP 161) from authenticated IT Staff users to any
   c. Windows Connectivity (TCP/UDP 135,137-139, 445, TCP 1213) from authenticated IT Staff users to any

Intra-Zone ICMP Policy for the Management Net:

- ICMP Echo Requests permitted inbound from the following:
  - IT Staff Desktop Workstations in the General Net
  - Authenticated IT Staff users from the Employee DMZ
- ICMP Echo Replies, Unreachable and TTL Exceeded messages permitted outbound to the following:
  - IT Staff Desktop Workstations in the General Net
  - Authenticated IT Staff users from the Employee DMZ
- All other ICMP blocked in and out

© SANS Institute 2000 - 2002 Author

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

8.0 Other External Connectivity Security Architectures

Employee Dial-in Access:
In addition to the direct VPN connectivity from the Internet already described, the GeF Employee VPN Server provide GeF employees with access to IPSec (3DES, SHA) VPN-protected telephone and ISDN dial-in access.

To dial-in over a telephone line, employees must use the Cisco VPN Client for Windows and authenticate to a TACACS+ server. IT Staff members, because of their greater privileges on GeF networks and hosts, must authenticate to the ACE Server with one-time passwords using a SecurID token. ISDN connectivity is supported using call-back functionality and CHAP.

Business Partner Dial-In Access:
In addition to the direct VPN connectivity from the Internet already described, the GeF Partner VPN Server provide specific GeF Business Partners with access to IPSec (3DES, SHA) VPN-protected telephone and ISDN dial-in access.

To dial-in over a telephone line, Business Partners must use the Cisco VPN Client for Windows and authenticate to a TACACS+ server. ISDN connectivity is supported using call-back functionality and CHAP.

Business Partner WAN Links:
For those Business Partner connections that have high throughput and/or SLA requirements, dedicated point-to-point WAN Links have been implemented. These Links all terminate in the Cisco 7140 Partner Router. ACLs are implemented on this router to:

- Permit well-defined access to designated FCS Staging Servers in the Partner DMZ
- Block all other access – especially access from one WAN link to another

IPSec tunnels (3DES, SHA), terminating at the 7140 Partner Router, are implemented to secure these WAN links.

To support this configuration, the FCS Staging Servers are configured to support connectivity via non-anonymous FTP and Authenticated MOTD Protocol only. No general accounts are provided, and all general access services, such as rsh and telnet, are disabled. In addition, these servers are hardened and kept up-to-date on all security-relevant patches.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix 1 – RenNet Border Router – Security Configuration

```
hostname fred
```
Nondescript node name to make intelligence gathering more difficult

```
service timestamps debug uptime
service timestamps log uptime
```
Enables the timestamping of debugging and log messages. Needed to correlate security events of Interest detected by multiple NSDs

```
service password-encryption
```
Encrypts router passwords in memory

```
aaa group server tacacs+ tacserver
  server gef.corp.net.56
aaa authentication login auth.group group tacacs+ enable
login authentication auth.group
enable secret 5 <password >
```
Require user-level authentication from the TACACS+ server gef.corp.net.56. Also configure a secret password in case of TACACS+ server unavailability. The Secret password will be kept in secure escrow until needed.

```
banner motd ^C
********************  WARNING  ********************
All access to this system is limited to authorized use by network administrator
employees of GIAC e-Fortunes and no one else.

Unauthorized access is prohibited by Public Law 99-474, (The Computer Fraud and
Abuse Act of 1986) and can result in administrative, disciplinary and/or criminal
proceedings.

This system is the property of GIAC e-Fortunes and is intended for use by
authorized individuals only.  Use of this computing system is subject to monitoring
by system and security personnel.  If any such monitoring reveals evidence of
criminal activity, system personnel shall be obliged to provide such evidence to
law enforcement officials.

Use of this system constitutes a consent to monitoring at all times.
********************  WARNING  ********************
^C
```
Login banner that covers you from a legal POV.

```
no tcp small services
no udp small services
no ip http server
```
Disable unneeded services: router-based web server as well as echo, chargen, discard, etc.

```
logging gef.corp.net.55
logging source-interface FastEthernet 0/0
logging trap 4
logging on
```
Log error events from Syslog level 1 (emergencies) to level 4 (warnings) to the External Syslog server via the NAT-translated IP address gef.corp.net.55. Source address is that of interface FastEthernet 0/0

```
interface FastEthernet0/0
 ip address gef.corp.net.1 255.255.255.0
 ip access-group 101 in
 duplex full
 speed 100
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
interface FastEthernet0/1
 no ip address
 shutdown

interface ATM1/0
 no ip address
 no atm ilmi-keepalive
 pvc 0/16 ilmi

interface ATM1/0.173 point-to-point
 ip address ren.corp.net.122 255.255.255.240
 ip access-group 102 in
 pvc cvn77 0/101
  vbr-nrt 1544 1544 10
  encapsulation aal5snap

interface ATM2/0
 no ip address
 shutdown
 no atm ilmi-keepalive
```

Interface configuration:

- FastEthernet 0/0: Internal interface connected to the Outer Security VLAN. Assigned a "real" IP address. Access-list 101 applied inbound – from the Outer Security VLAN into the router.
- FastEthernet 0/1: Disabled
- ATM 1/0.173: Subinterface of ATM 1/0. External interface connected to RenNet. Access List 102 applied inbound – from RenNet into the router.
- ATM 2/0: Disabled

Access list 101: Outbound to the Internet: Into FastEthernet 0/0 – the Inside interface

```
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 permit tcp any any established
access-list 101 permit tcp host gef.corp.net.26 any eq 25
access-list 101 permit tcp gef.corp.net.240 0.0.0.15 any eq 80
access-list 101 permit tcp gef.corp.net.240 0.0.0.15 any eq 443
access-list 101 permit tcp host gef.corp.net.25 any eq 25
access-list 101 permit udp host gef.corp.net.153 any eq 53
access-list 101 permit tcp host gef.corp.net.153 any eq 53
access-list 101 permit udp host gef.corp.net.53 eq 53 any
access-list 101 permit tcp host gef.corp.net.140 any eq 14141
access-list 101 permit tcp host gef.corp.net.141 any eq 14141
access-list 101 permit tcp host gef.corp.net.21 any eq 20
access-list 101 permit udp host gef.corp.net.100 any eq 500
access-list 101 permit 50 host gef.corp.net.100 any
access-list 101 permit 51 host gef.corp.net.100 any
access-list 101 permit udp host gef.corp.net.200 any eq 500
access-list 101 permit 50 host gef.corp.net.200 any
access-list 101 permit 51 host gef.corp.net.200 any
access-list 101 permit tcp host gef.corp.net.220 range 22-23
access-list 101 permit icmp host gef.corp.net.220 echo
access-list 101 deny   any any log
```

Rule Order Logic for access-list 101:

1. Drop all packets from the 10 network. This will block and log any internal, privately-addressed packets that have somehow managed to get through to this router. This must be before any permit statements, or privately-addressed packets that meet the criteria of the permit would be missed.
2. Permit access to those external services that are intended to be available to internal nodes. Rule Order in this section is based on observed traffic levels by service

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. Block everything else

Line-by- line description of the access-list 101:

access-list 101 deny ip 10.0.0.0 0.255.255.255 log
Block and log outbound packets purporting to come from the 10 network. They could be spoofed or they could be somehow "leaking" from an internal network

access-list 101 permit tcp any any established
Permit TCP packets for established sessions

access-list 101 permit tcp host gef.corp.net.26 any eq 25 (FCS SMTP)
Permit outbound SMTP connections from the FCS Delivery Mail Server

access-list 101 permit tcp gef.corp.net.240 0.0.0.15 eq 80
access-list 101 permit tcp gef.corp.net.240 0.0.0.15 eq 443
Permit outbound HTTP and HTTPS connections from the PAT addresses of internal nodes

access-list 101 permit tcp host gef.corp.net.25 any eq 25
Permit outbound SMTP connections from the Corporate Mail Server

access-list 101 permit udp host gef.corp.net.153 any eq 53
access-list 101 permit tcp host gef.corp.net.153 any eq 53
Permit outbound DNS requests from the External/Internal DNS Server

access-list 101 permit udp host gef.corp.net.53 eq 53 any
Permit outbound UDP-based DNS responses from the External/External DNS Server

access-list 101 permit tcp host gef.corp.net.140 eq 14141
access-list 101 permit tcp host gef.corp.net.141 eq 14141
Permit outbound MOTD Replies from the MOTD Servers.

access-list 101 permit tcp host gef.corp.net.21 any eq 20
Permit outbound FTP Data connections from the FTP Dropbox.

access-list 102 permit udp host gef.corp.net.100 eq 500
access-list 102 permit 50 host gef.corp.net.100 any
access-list 102 permit 51 host gef.corp.net.100 any
Permit outbound IPSec traffic from the Employee VPN Server. UDP 500 is for IKE, IP Protocols 50 and 51 are for tunnel mode (ESP) and transport mode (AH) IPSec services, respectively.

access-list 102 permit udp host gef.corp.net.200 eq 500
access-list 102 permit 50 host gef.corp.net.200 any
access-list 102 permit 51 host gef.corp.net.200 any
Permit outbound IPSec traffic from the Business Partner VPN Server. UDP 500 is for IKE, IP Protocols 50 and 51 are for tunnel mode (ESP) and transport mode (AH) IPSec services, respectively.

access-list 101 permit tcp host gef.corp.net.220 range 22-23
Permit outbound SSH and Telnet from the PAT address used by IT Staff members.

Access List 102: Inbound from the Internet: Into ATM1/0.173 – the Outside interface

```
access-list 102 deny ip gef.corp.net.0 0.0.0.255 any log
access-list 102 deny ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny ip 172.16.0.0 0.15.255.255 any log
access-list 102 deny ip 192.168.0.0 0.0.255.255 any log
access-list 102 permit tcp any any established
access-list 102 permit tcp any host gef.corp.net.80 eq 80
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
access-list 102 permit tcp any host gef.corp.net.81 eq 80
access-list 102 permit tcp any host gef.corp.net.82 eq 80
access-list 102 permit tcp any host gef.corp.net.80 eq 443
access-list 102 permit tcp any host gef.corp.net.81 eq 443
access-list 102 permit tcp any host gef.corp.net.82 eq 443
access-list 102 permit tcp any host gef.corp.net.140 eq 14140
access-list 102 permit tcp any host gef.corp.net.141 eq 14140
access-list 102 permit tcp any host gef.corp.net.21 eq 21 log
access-list 102 permit tcp any host gef.corp.net.25 eq 25
access-list 102 permit udp any host gef.corp.net.53 eq 53
access-list 102 permit tcp any host gef.corp.net.53 eq 53
access-list 102 permit udp any eq 53 host gef.corp.net.153
access-list 102 permit udp any host gef.corp.net.100 eq 500
access-list 102 permit 50 any host gef.corp.net.100
access-list 102 permit 51 any host gef.corp.net.100
access-list 102 permit udp any host gef.corp.net.200 eq 500
access-list 102 permit 50 any host gef.corp.net.200
access-list 102 permit 51 any host gef.corp.net.200
access-list 102 permit icmp any host gef.corp.net.220 echo-reply
access-list 102 permit icmp any host gef.corp.net.220 net-unreachable
access-list 102 permit icmp any host gef.corp.net.220 host-unreachable
access-list 102 permit icmp any host gef.corp.net.220 port-unreachable
access-list 102 permit icmp any host gef.corp.net.220 ttl-exceeded
access-list 102 deny   any any log
```

(Note that no inbound SMTP connections are allowed to the FCS Email server – only outbound FCS Email deliveries are allowed.)

Rule Order Logic for access-list 102:

4. Drop all spoofed packets: This must be before any permit statements, or spoofed packets that meet the criteria of the permit would be missed.
5. Permit access to those services that are intended to be externally available. Rule Order in this section is based on observed traffic levels by service:
6. Block everything else

Line-by- line description of the access-list 102:

```
access-list 102 deny ip gef.corp.net.0 0.0.0.255 log
```
Anti-spoofing filter: Block and log inbound packets spoofing the 'internal' address space

```
access-list 102 deny ip 10.0.0.0 0.255.255.255 log
access-list 102 deny ip 172.16.0.0 0.15.255.255 log
access-list 102 deny ip 192.168.0.0 0.0.255.255 log
```
Anti-spoofing filter: Block and log inbound packets from private addresses

```
access-list 102 permit tcp any any established
```
Permit TCP packets for established sessions

```
access-list 102 permit tcp any host gef.corp.net.80 eq 80
access-list 102 permit tcp any host gef.corp.net.81 eq 80
access-list 102 permit tcp any host gef.corp.net.82 eq 80
access-list 102 permit tcp any host gef.corp.net.80 eq 443
access-list 102 permit tcp any host gef.corp.net.81 eq 443
access-list 102 permit tcp any host gef.corp.net.82 eq 443
```
Permit inbound HTTP and HTTPS connections to the External Webservers

```
access-list 102 permit tcp any host gef.corp.net.140 eq 14140
access-list 102 permit tcp any host gef.corp.net.141 eq 14140
```
Permit inbound MOTD Requests to MOTD Servers

© SANS Institute 2000 - 2002, Author retains full rights.

access-list 102 permit tcp any host gef.corp.net.21 eq 21 log
Permit and log inbound FTP connections to the FTP Dropbox

access-list 102 permit tcp any host gef.corp.net.25 eq 25
Permit inbound SMTP connections to the Corporate Email Server

access-list 102 permit udp any host gef.corp.net.53 eq 53
access-list 102 permit tcp any host gef.corp.net.53 eq 53
Permit inbound DNS queries to the External/External DNS Server

access-list 102 permit udp any eq 53 host gef.corp.net.153
Permit return UDP-based DNS traffic to the External/Internal DNS Server

access-list 102 permit udp any host gef.corp.net.100 eq 500
access-list 102 permit 50 any host gef.corp.net.100
access-list 102 permit 51 any host gef.corp.net.100
Permit inbound IPSec connections to the Employee VPN Server UDP 500 is for key exchange (IKE), IP Protocols 50 and 51 are for tunnel mode (ESP) and transport mode (AH) IPSec services, respectively.

access-list 102 permit udp any host gef.corp.net.200 eq 500
access-list 102 permit 50 any host gef.corp.net.200
access-list 102 permit 51 any host gef.corp.net.200
Permit inbound IPSec traffic to the Business Partner VPN Server. UDP 500 is for IKE, IP Protocols 50 and 51 are for tunnel mode (ESP) and transport mode (AH) IPSec services, respectively.

access-list 102 deny any any log
Block and log all other packets. Logging this will create large volumes of logs, but is necessary for correlating events of interest across the network.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix 5 – Primary Outer Firewall Configuration
(Security-irrelevant lines omitted)

```
nameif ethernet0 outside security0
```
Name interface ethernet0 “outside” and assign it the lowest security level – 0.

```
nameif ethernet1 inside security100
```
Name interface ethernet1 “inside” and assign it the highest security level – 100.

```
nameif ethernet2 intf3 security5
nameif ethernet3 intf3 security10
nameif ethernet4 intf4 security15
nameif ethernet5 intf5 security20
```
Give arbitrary names to the remaining interfaces and give them intermediate security levels.

```
enable password gEoZ6VTV./88w.GV encrypted
passwd dU.46nSuJ4gjLhLt encrypted
```
Passwords are stored in encrypted form.

```
hostname barney
```
Nondescript hostname to confound intelligence gathering.

```
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
```
Enable the Pix “mini-proxies” for those services we use.

```
no fixup protocol h323 1720
no fixup protocol rsh 514
no fixup protocol sqlnet 1521
no fixup protocol sip 5060
no fixup protocol skinny 2000
```
Enable the Pix “mini-proxies” for those services we don’t use.

```
interface ethernet0 auto
interface ethernet1 auto
```
Enable interfaces ethernet1 and ethernet2.

```
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
```
Shutdown unused interfaces.

```
ip address outside gef.corp.net.2 255.255.255.0
```
Assign public address to outside interface.

```
ip address inside 10.10.201.1 255.255.255.0
```
Assign private address from outer security VLAN to inside interface.

```
ip address intf2 127.0.0.1 255.255.255.255
ip address intf3 127.0.0.1 255.255.255.255
ip address intf4 127.0.0.1 255.255.255.255
ip address intf5 127.0.0.1 255.255.255.255
```
Assign bogus addresses to remaining interfaces.

```
failover active
failover timeout 0:00:00
failover poll 15
failover ip address outside gef.corp.net.222
failover link ethernet0
failover replicate http
```
Enable failover to the secondary Outer Pix firewall using the outside interface.

© SANS Institute 2000 - 2002, Author retains full rights.

```
failover ip address intf1 0.0.0.0
failover ip address intf2 0.0.0.0
failover ip address intf3 0.0.0.0
failover ip address intf4 0.0.0.0
failover ip address intf5 0.0.0.0
```

Disable failover on the remaining interfaces.

```
nat (inside) 1 10.10.1.0 255.255.255.0
static (inside,outside) gef.corp.net.80 10.10.1.80 netmask 255.255.255.255
static (inside,outside) gef.corp.net.81 10.10.1.81 netmask 255.255.255.255
static (inside,outside) gef.corp.net.82 10.10.1.82 netmask 255.255.255.255
static (inside,outside) gef.corp.net.140 10.10.1.140 netmask 255.255.255.255
static (inside,outside) gef.corp.net.141 10.10.1.141 netmask 255.255.255.255
static (inside,outside) gef.corp.net.21 10.10.1.21 netmask 255.255.255.255
global (outside) 1 gef.corp.net.101 netmask 255.255.255.255
```

Assign static NAT mappings for externally available servers hosted on the External DMZ (Web, MOTD and FTP servers.) Create PAT address (gef.corp.net.101) for FCS Mail Delivery server and any other nodes that may be placed there.

```
nat (inside)3 10.10.3.0 255.255.255.0
static (inside,outside) gef.corp.net.25 10.10.3.25 netmask 255.255.255.255
static (inside,outside) gef.corp.net.53 10.10.3.53 netmask 255.255.255.255
global (outside) 3 gef.corp.net.103 netmask 255.255.255.255
```

Assign static NAT mappings for externally available servers hosted on the Admin DMZ (Corp Email and External/External DNS server.) Create PAT address (gef.corp.net.103) for any other nodes that may be placed there.

```
nat (inside) 5 10.10.5.0 255.255.255.0
static (inside,outside) gef.corp.net.100 10.10.5.100 netmask 255.255.255.255
global (outside) 5 gef.corp.net.105 netmask 255.255.255.255
```

Assign static NAT mappings for externally available servers hosted on the Employee DMZ (Employee VPN server.) Create PAT address (gef.corp.net.105) for any other nodes that may be placed there.

```
nat (inside) 7 10.10.7.0 255.255.255.0
static (inside,outside) gef.corp.net.200 10.10.5.200 netmask 255.255.255.255
global (outside) 5 gef.corp.net.107 netmask 255.255.255.255
```

Assign static NAT mappings for externally available servers hosted on the Partner DMZ (Partner VPN server.) Create PAT address (gef.corp.net.107) for any other nodes that may be placed there.

```
nat (inside) 10 10.10.10.0 255.255.255.0
global (outside) 10 gef.corp.net.110 netmask 255.255.255.255
```

Create PAT address (gef.corp.net.110) for use by nodes in the General Network.

```
nat (inside) 20 10.10.20.0 255.255.255.0
global (outside) 20 gef.corp.net.120 netmask 255.255.255.255
```

Create PAT address (gef.corp.net.110) for use by nodes in the Management Network.

```
nat (inside) 30 10.10.30.0 255.255.255.0
global (outside) 30 gef.corp.net.130 netmask 255.255.255.255
```

Create PAT address (gef.corp.net.110) for use by nodes in the Divination Network.

```
nat (inside) 100 10.10.100.0 255.255.255.0
global (outside) 100 gef.corp.net.101 netmask 255.255.255.255
```

Create PAT address (gef.corp.net.110) for use by nodes in the Server Network.

```
access-list acl.inbound deny ip gef.corp.net.0 255.255.255.0 any
access-list acl.inbound deny ip 10.0.0.0 255.0.0.0 any
access-list acl.inbound deny ip 172.16.0.0 255.240.0.0 any
access-list acl.inbound deny ip 192.168.0.0 255.255.0.0 any
access-list acl.inbound permit tcp any host gef.corp.net.80 eq 80
access-list acl.inbound permit tcp any host gef.corp.net.81 eq 80
access-list acl.inbound permit tcp any host gef.corp.net.82 eq 80
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
access-list acl.inbound permit tcp any host gef.corp.net.80 eq 443
access-list acl.inbound permit tcp any host gef.corp.net.81 eq 443
access-list acl.inbound permit tcp any host gef.corp.net.82 eq 443
access-list acl.inbound permit tcp any host gef.corp.net.140 eq 14140
access-list acl.inbound permit tcp any host gef.corp.net.141 eq 14140
access-list acl.inbound permit tcp any host gef.corp.net.21 eq 21
access-list acl.inbound permit tcp any host gef.corp.net.25 eq 25
access-list acl.inbound permit udp any host gef.corp.net.53 eq 53
access-list acl.inbound permit tcp any host gef.corp.net.53 eq 53
access-list acl.inbound permit udp any eq 53 host gef.corp.net.153
access-list acl.inbound permit udp any host gef.corp.net.100 eq 500
access-list acl.inbound permit 50 any host gef.corp.net.100
access-list acl.inbound permit 51 any host gef.corp.net.100
access-list acl.inbound permit udp any host gef.corp.net.200 eq 500
access-list acl.inbound permit 50 any host gef.corp.net.200
access-list acl.inbound permit 51 any host gef.corp.net.200
access-list acl.inbound permit icmp any host gef.corp.net.220 echo-reply
access-list acl.inbound permit icmp any host gef.corp.net.220 net-unreachable
access-list acl.inbound permit icmp any host gef.corp.net.220 host-unreachable
access-list acl.inbound permit icmp any host gef.corp.net.220 port-unreachable
access-list acl.inbound permit icmp any host gef.corp.net.220 ttl-exceeded
access-list acl.inbound deny   any any
access-group acl.inbound in interface outside
```

Create access list that mirrors access-list 102 on the Border Router, and apply it to the outside interface.

```
access-list acl.outbound deny ip gef.corp.net.0 255.255.255.0 any
access-list acl.outbound permit tcp host 10.10.1.26 any eq 25
access-list acl.outbound permit tcp host 10.10.1.240 eq 80
access-list acl.outbound permit tcp host 10.10.1.240 any eq 443
access-list acl.outbound permit tcp host 10.10.3.25 any eq 25
access-list acl.outbound permit udp host 10.10.5.153 any eq 53
access-list acl.outbound permit tcp host 10.10.5.153 any eq 53
access-list acl.outbound permit udp host 10.10.3.53 any eq 53
access-list acl.outbound permit tcp host 10.10.1.140 any eq 14141
access-list acl.outbound permit tcp host 10.10.1.141 any eq 14141
access-list acl.outbound permit udp host 10.10.5.100 any eq 500
access-list acl.outbound permit 50 host 10.10.5.100 any
access-list acl.outbound permit 51 host 10.10.5.100 any
access-list acl.outbound permit udp host 10.10.7.200 any eq 500
access-list acl.outbound permit 50 host 10.10.7.200 any
access-list acl.outbound permit 51 host 10.10.7.200 any
access-list acl.outbound permit tcp host 10.10.10.220 any range 22-23
access-list acl.outbound permit icmp host 10.10.10.220 any echo
access-list acl.outbound deny   any any
access-group acl.outbound in interface inside
```

Create access list that mirrors access-list 101 on the Border Router, and apply it to the inside interface. Note that on this side, we see the private addresses of the resources.

```
aaa-server TACACS+ protocol tacacs+
aaa-server joey protocol tacacs+
aaa-server joey (inside) host 10.10.5.55 porkpie timeout 20
```

Use the TACACS+ server in the remote Employee DMZ to authenticate administrative logins.

```
no snmp-server location
no snmp-server contact
snmp-server enable traps
snmp-server community GeFMeBaby
snmp-server host 10.10.100.165
```

Change the community string to something other than “public”, and permit SNMP traps/queries to/from the Network Management station in the Server Network.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

floodguard enable

Enables the reclamation of resources in the event of an resource-draining attack

ssh 10.0.0.0 255.0.0.0 inside
ssh timeout 5

Permit ssh connection attempts from all internal nodes (limited by IP address at the Proxy firewall).

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix 26 – Partner Router VPN Configuration
(VPN-irrelevant lines omitted)

Below is the portion of the Partner Router configuration that specifies the VPN to one specific business partner: Quimby Predictions, Inc.

```
crypto isakmp policy 9
 encr 3des
 hash md5
 authentication pre-share
 group 2
```

Define ISAKMP policy #9 with the following parameters:

- Use 3DES encryption algorithm to protect confidentiality during the IKE phase
- Use SHA hash algorithm to protect integrity during the IKE phase
- Use pre-shared secret key strings for Phase 2 of IKE
- Use Group 2 Diffie-Hellman for Main Mode exchange

crypto isakmp key <*shared_secret*> **address 192.168.88.1**

Specify the shared-secret key string, and the IP address of the device that terminates the far end of the VPN tunnel

crypto ipsec transform-set 3des-md5 esp-3des esp-md5-hmac

Define the set of encryption algorithms to be used by IPSec, called the transform-set. In this case we're using 3DES and MD5-hmac

```
crypto map toquimby 25 ipsec-isakmp
 set peer 192.168.88.1
 set transform-set 3des-md5
 match address 10
```

Create a crypto map called "toquimby" that defines

- The IP address of the device that terminates the far end of the VPN tunnel
- The transform-set to be used
- The access-list that defines the near-end IP addresses that may traverse the link

access-list 10 permit ip 10.10.7.0 0.0.0.255 any

Define access-list 10 to include source addresses from the Partner DMZ only

```
interface ATM1/0.173 point-to-point
 ip address 192.168.88.2 255.255.255.0
 pvc cvn77 0/101
 vbr-nrt 1544 1544 10
 encapsulation aal5snap
 crypto map toquimby
```

Apply the "toquimby" crypto map to the appropriate interface.

© SANS Institute 2000 - 2002, Author retains full rights.

IP Packet Filtering with Cisco Router ACLs:
A Tutorial for new Network Administrators

Applying the theory

Packet filtering is a technique of controlling network traffic flowing through a control point. It works by individually evaluating each network packet against a set of rules defined for that control point. Once evaluated, each packet is then either permitted to continue to its destination or dropped.

In most real-world network implementations:
- The control point is a router's interface
- The set of rules used to filter packets at a router interface is called an Access Control List (ACL)
- ACLs are implemented in two steps:
  - First the ACL is created as an ASCII list in the router's configuration file, in which each rule is a single line. Since a router may contain many ACLs, each ACL is given a unique numerical label. All rules belonging to a single ACL share the same label.
  - Then the ACL is applied to a router's interface as either **inbound** or **outbound** on that interface. If applied as inbound, each packet **entering** the router at that interface is evaluated. If applied as outbound, each packet **exiting** the router at that interface is evaluated. The choice of inbound vs. outbound is critical, since ACLs applied in the wrong direction will not work as intended.

Cisco ACLs

Cisco supports many types of ACLs for many Layer 2 and 3 Network Protocols, such as IP, IPX, AppleTalk, Ethernet, etc. This tutorial will only focus on ACLs for controlling IP traffic. Note that advanced features such as dynamic ACLs, and ACLs that filter based on precedence or Type of Service (TOS) will not be discussed.

Cisco defines two major categories of IP ACLs: Regular and Extended. Regular ACLs:
- Are labeled with an access list number between 1-99
- Can control traffic based on source and/or destination IP Address only

Extended ACLs:
- Are labeled with an access-list-number between 100-199
- Can control traffic based on:
  - IP Protocol type of the packet
  - Source and/or destination IP Address
  - Source and/or destination ICMP Message Type
  - Source and/or destination UDP Port
  - Source and/or destination TCP Port

Cisco ACL Rule Syntax

Each rule in a Regular ACL has the following general syntax:

access-list <*label*> <*action*> **ip** <*src-ip*> <*src-mask*> <*dst-ip*> <*dst-mask*> *[<log>]*

- **Access-list** Required keyword that defines this line as a rule in an access-list
- **Label** Required decimal label between 1-99
- **Action** Required value of either **permit** or **deny**
- **IP** Required keyword that defines the type of packet being
- **Src-IP** Source IP address in the packet being evaluated
- **Src-Mask** Selection mask that, together with the src-ip can define a single source IP address or a range of possible source IP address, just like a subnet mask. Note however, that the "bits are

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

flipped" in an ACL mask, as compared to a subnet mask. A 0-bit means "match this bit", and a 1-bit is a wildcard.

- **Dst-IP** Destination IP address in the packet being evaluated.
- **Dst-Mask** Selection mask that, together with the dst-ip can define a single destination IP address or a range of possible destination IP address, just like a subnet mask. Note however, that the "bits are flipped" in an ACL mask, as compared to a subnet mask: a 0-bit means "match this bit", and a 1-bit is a wildcard.
- **Log** Optional action to create a log entry every time this rule is matched

Each rule in an Extended ACL has the following general syntax:

access-list <*label*> <*action*> <*IP-protocol*> <*src-ip*> <*src-mask*> <*src-op/port*> <*dst-ip*> <*dst-mask*> <*dst-op/port*> *[<log>]*

- **Access-list** Required keyword that defines this line as a rule in an access-list
- **Label** Required decimal label between 100-199
- **Action** Required value of either **permit** or **deny**
- **IP-Protocol** Required decimal value of this packet's IP protocol
- **Src-IP** Source IP address in the packet being evaluated
- **Src-Mask** Selection mask that, together with the src-ip can define a single source IP address or a range of possible source IP address, just like a subnet mask. Note however, that the "bits are flipped" in an ACL mask, as compared to a subnet mask: a 0-bit means "match this bit", and a 1-bit is a wildcard.
- **Src-Op/Port** May only be used when the IP protocol type has defined ports, such as TCP and UDP. Decimal values and operands can be combined to resulting any of the following:
  - A specific port within this IP protocol, using a decimal value
  - A specified range of ports within this IP protocol, using the syntax
    - **lt** <*port-number*> (less than)
    - **gt** <*port-number*> (greater than)
    - **eq** <*port-number*> (equal to),
    - **neq** <*port-number*> (not equal to)
    - **range** <*port-number*>-<*port-number*> (inclusive range)
- **Dst-IP** Destination IP address in the packet being evaluated.
- **Dst-Mask** Selection mask that, together with the dst-ip can define a single destination IP address or a range of possible destination IP address, just like a subnet mask. Note however, that the "bits are flipped" in an ACL mask, as compared to a subnet mask. A 0-bit means "match this bit", and a 1-bit is a wildcard.
- **Dst-Op/Port** May only be used when the IP protocol type has defined ports. Decimal values and operands can be combined identically to the Src-Op/Port
- **Log** Optional action to create a log entry every time this rule is matched

When certain IP protocol are specified, the name of the protocol may be used as a keyword instead of its decimal value, for instance:

- icmp (IP protocol 1)
- tcp (IP protocol 6)
- udp (IP protocol 17)

With ICMP, the ICMP message types may be specified, for instance:

- echo (ping request)
- echo-reply (ping reply)
- net-unreachable
- ttl-exceeded

Also, the following syntax shortcuts are available in both forms:

- When specifying a single IP address as either source or destination IP address, you may substitute the IP/Mask pair with the syntax: **host <ip_address>**
- Instead of specifying a completely wildcard mask (255.255.255.255), you may substitute the IP/Mask pair with the word **any**

Here're some examples of rule syntax in Regular ACLs:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

access-list 2 permit ip 10.10.10.1 0.0.0.0 15.15.15.1 0.0.0.0
access-list 2 permit ip host 10.10.10.1 15.15.15.1 0.0.0.0
access-list 2 permit ip 10.10.10.1 0.0.0.0 host 15.15.15.1
access-list 2 permit ip host 10.10.10.1 host 15.15.15.1
These four functionally identical rules will each permit any IP packet from 10.10.10.1 to 15.15.15.1

access-list 10 deny ip 5.5.5.5 0.0.0.0 0.0.0.0 255.255.255.255
access-list 10 deny ip 5.5.5.5 0.0.0.0 any
access-list 10 deny ip host 5.5.5.5 any
These three functionally identical rules will each deny any IP packet from 5.5.5.5 to any host

access-list 50 permit ip 5.5.5.5 0.0.0.0 15.15.15.0 0.0.0.255
access-list 50 permit ip host 5.5.5.5 15.15.15.0 0.0.0.255
These two functionally identical rules will each permit any IP packet from 5.5.5.5 to any host with an IP address between 15.15.15.0 and 15.15.15.255

access-list 17 deny ip host 5.5.5.5 15.15.64.0 0.0.15.255
These two functionally identical rules will each deny any IP packet from 5.5.5.5 to any host with an IP address between 15.15.64.0 and 15.15.79.255 inclusive

access-list 85 deny ip any any
Block any (every) packet

Here're some examples of rule syntax in Extended ACLs:

access-list 101 permit udp host 10.10.10.1 15.0.0.0 0.255.255.255 eq 53
Permit any UDP packet with a destination port of 53 (DNS) from 10.10.10.1 to any node on the 15.0.0.0 Class A network

access-list 150 deny tcp host 10.10.10.1 range 6000-6100 15.0.0.0 0.255.255.255
Deny any TCP packet with a source port value between 6000 to 6100 inclusive (X Windows) from 10.10.10.1 to any node on the 15.0.0.0 Class A network

access-list 199 deny tcp any any gt 1023
Deny any TCP packet with a destination port value greater than 1023

access-list 172 deny icmp any 192.168.10.0 0.0.0.255 echo
Deny all ping requests destined for the 192.168.10.0 Class C network

access-list 172 permit 50 any host 20.1.1.17
Permit any IP Protocol 50 packet (IPSec ESP) destined for 20.1.1.17

When the IP protocol being matched is TCP, the special syntax **established** may be used in an extended ACL rule to match all packets in an already-established TCP session:

access-list 25 permit tcp 10.20.30.0 0.0.0.255 any eq 25 established
Permit all TCP Port 25 packets (SMTP) originating from the 10.20.30.0 Class C network that do not have the SYN bit set.

Building ACLs from rules

Packets are evaluated by ACLs as follows:
- Each packet going through a router interface is evaluated against the ACL that applies in that direction (if one exists in that direction.)
- Each packet is evaluated against each rule in the ACL, one rule at a time, from the first rule to the last. Therefore the order of the rules in the ACL is paramount.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- If the parameters of the packet being evaluated match the parameters defined in the rule, then "the rule is matched," and the action defined in that rule is executed: to either **permit** the packet to continue to its destination or to **deny** the packet from doing so – a.k.a "drop the packet."
- If the end of the ACL list is reached without matching a single rule, the packet is dropped. This feature is called the "implicit deny-all" at the end of each Cisco ACL.

There are two different kids of ACLs you can build:

- Default-deny: Everything not specifically permitted is denied
- Default-permit: Everything not specifically denied is permitted. Note that the implicit deny-all feature of Cisco ACLs requires one to explicitly add a **permit any any** rule at the end to get a default-permit ACL.

Real-world Example: RenNet Border Router ACL

Now let's consider access-list 102 from the RenNet Border Router. It consists of the following 27 rules in the order given:

```
access-list 102 deny ip gef.corp.net.0 0.0.0.255 any log
access-list 102 deny ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny ip 172.16.0.0 0.15.255.255 any log
access-list 102 deny ip 192.168.0.0 0.0.255.255 any log
access-list 102 permit tcp any any established
access-list 102 permit tcp any host gef.corp.net.80 eq 80
access-list 102 permit tcp any host gef.corp.net.81 eq 80
access-list 102 permit tcp any host gef.corp.net.82 eq 80
access-list 102 permit tcp any host gef.corp.net.80 eq 443
access-list 102 permit tcp any host gef.corp.net.81 eq 443
access-list 102 permit tcp any host gef.corp.net.82 eq 443
access-list 102 permit tcp any host gef.corp.net.140 eq 14140
access-list 102 permit tcp any host gef.corp.net.141 eq 14140
access-list 102 permit tcp any host gef.corp.net.21 eq 21 log
access-list 102 permit tcp any host gef.corp.net.25 eq 25
access-list 102 permit udp any host gef.corp.net.53 eq 53
access-list 102 permit tcp any host gef.corp.net.53 eq 53
access-list 102 permit udp any eq 53 host gef.corp.net.153
access-list 102 permit udp any host gef.corp.net.100 eq 500
access-list 102 permit 50 any host gef.corp.net.100
access-list 102 permit 51 any host gef.corp.net.100
access-list 102 permit udp any host gef.corp.net.200 eq 500
access-list 102 permit 50 any host gef.corp.net.200
access-list 102 permit 51 any host gef.corp.net.200
access-list 102 permit icmp any host gef.corp.net.220 echo-reply
access-list 102 permit icmp any host gef.corp.net.220 net-unreachable
access-list 102 permit icmp any host gef.corp.net.220 host-unreachable
access-list 102 permit icmp any host gef.corp.net.220 port-unreachable
access-list 102 permit icmp any host gef.corp.net.220 ttl-exceeded
access-list 102 deny   any any log
```

The first four lines are called anti-spoofing filters. They protect against packets that come into from RenNet with spoofed (faked) source addresses. Here we protect against packets claiming to be from gef.corp.net.0 even as they come in from the outside, and any of the RFC 1597-defined private IP addresses. These anti-spoofing filters must come before any permit statements to be effective, because a spoofed packet might still match a permit statement and be allowed through.

The fifth line permits all TCP traffic from already established sessions. This will allow, for instance, internal users who initiate connections to external websites to receive their return traffic.

Lines 6 through 26 define the traffic that is explicitly permitted in from RenNet. They permit:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- External users to connect to our web servers (gef.corp.net.80, 81 & 82 on TCP 80)
- External users to submit MOTD requests to our MOTD servers (gef.corp.net.140 & 141 on TCP 14140)
- External users to connect to our FTP Dropbox (gef.corp.net.21 on TCP 21)
- External mail servers to send mail to our Corporate Email Server (gef.corp.net.25 on TCP 25)
- External nodes to query our External/External DNS Server (gef.corp.net.53 on UDP and TCP 53)
- Employees to connect to the Employee VPN server from the Internet (gef.corp.net.100 on UDP 500, and IP 50 and 51.)
- Business Partners to connect to the Partner VPN server from the Internet (gef.corp.net.200 on UDP 500, and IP 50 and 51.)
- Specific ICMP reply message types to the IT Staff's workstations

And finally, line 26 is an explicit deny-all rule. Although this line is redundant to the implicit deny-all at the end of all ACLs, putting it in explicitly allows us to specify the log option to log all hits on this rule.

The final step is to apply this access list inbound to the outer interface of the router, which is done as follows:

```
access-group 102 in interface ATM1/0.173
```

Testing the Rules

Let's pick three rules form this ACL and discuss how we would test them:

Rule to Test: **`access-list 102 deny ip gef.corp.net.0 0.0.0.255 any log`**

To test this anti-spoofing rule, we'd need to:

- Pick a host/service that is available from the Internet, for instance, a corporate Webserver
- Configure the IDS on the External DMZ to look for packets coming from gef.corp.net.0 (although it really should already be configured this way…)
- Use a tool such as nmap to send a spoofed packet to port 80 on the Webserver, and see if the packet is picked up by the IDS. To do this with nmap, the syntax would be:

```
nmap –v –sS –p80 –P0 –Dgef.corp.net.100 gef.corp.net.80
```

Rule to Test: **`access-list 102 permit tcp any any established`**

This one's easy to test. Simply go to any host on an Internet Network and try to hit a website on the Internet. If this rule is absent or incorrect, you will never get any TCP packets back from the website you tried to hit.

Rule to Test: **`access-list 102 deny any any log`**

This one's also easy to test. Simply go to your handy @home test node, and try to make any connection to a host that's available (via a static NAT mapping) on a service that is not explicitly allowed, like an FTP connection to the External Mail server on the Server Net. If this rule is working, it will generate a syslog entry when it catches this packet. To do this with nmap, the syntax would be:

```
nmap –v –sS –p21 –P0  gef.corp.net.25
```

© SANS Institute 2000 - 2002, Author retains full rights.

GIAC e-Fortunes
GeF Outer Firewall Audit Report - Q3 2001

This document describes the approach, plan and results of the quarterly audit of the outer firewall for Q3 2001.

Objective

The goal of this audit is to assess the overall security posture of the outer firewall with respect to internet-based threats, and to determine how well it implements its firewall security policy. After examining the Network Security Architecture (NSA) document, it was determined that the firewall security policy to be verified is:

1. Only the following addresses in gef.corp.net.0 network should be reachable from the Internet, and only on the specified ports:
   1.1. Web servers at gef.corp.net.80, 81 & 82 on TCP 80 and 443
   1.2. MOTD Servers at gef.corp.net.140 & 141 on TCP 14140
   1.3. FTP Server at gef.corp.net.21 on TCP 21
   1.4. Email server at gef.corp.net.25 on TCP 25
   1.5. DNS Server at gef.corp.net.153 on TCP and UDP 53
   1.6. DNS Server at gef.corp.net.53 on UDP 53 only (UDP responses to queries from the Ext/Int Server)
   1.7. Employee VPN server at gef.corp.net.100 on UDP 500 (IKE) and IP 50 & 51 (IPSEC)
   1.8. Employee VPN server at gef.corp.net.100 on UDP 500 (IKE) and IP 50 & 51 (IPSEC)
2. Nothing on gef.corp.net should respond to unsolicited ICMP
3. Only the IT staff nodes, PATted to gef.corp.net.220, can send ICMP out, and only ICMP echo requests
4. Only the IT staff nodes, PATted to gef.corp.net.220, can receive ICMP, and only the following ICMP message types:
   4.1. Echo-reply
   4.2. Net-unreachable
   4.3. Host-unreachable
   4.4. Port-unreachable
   4.5. TTL-exceeded
5. All other connection attempts should be blocked

Test Plan

Policies being verified	***Verification Test***	***Test Results if properly implemented***
1, 2, 3, 4, 5	A. Perform a pingsweep of the entire gef.corp.com.0 Class C network	Nothing should answer
1.1 – 1.8	B. Perform a TCP and UDP portscan of the entire gef.corp.com.0 Class C network	Only the following nodes should be listening: B1. Web servers at gef.corp.net.80, 81 & 82 on TCP 80 and 443 B2. MOTD Servers at gef.corp.net.140 & 141 on TCP 14140 B3. FTP Server at gef.corp.net.21 on TCP 21 B4. Email server at gef.corp.net.25 on TCP 25 B5. DNS Server at gef.corp.net.53 on TCP and UDP 53 B6. DNS Server at gef.corp.net.53 on UDP 53 only (UDP responses to queries from the Ext/Int Server) B7. Employee VPN server at gef.corp.net.100 on UDP 500 (IKE) and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

		IP 50 & 51 (IPSEC) B8. Employee VPN server at gef.corp.net.100 on UDP 500 (IKE) and IP 50 & 51 (IPSEC)
3, 4	C. Ping and traceroute to a "known good" Internet node from selected IT staff nodes D. Ping and traceroute to a "known good" Internet node from a node in each DMZ and Internal Network	

Verification Test Results

All test were conducted either from or to weebairn.home.com – connected to the Internet via the tester's @home.com cable modem connection.

A. Pingsweep of entire network

Tool used: **nmapNT 2.53 SP1**
Command executed: **nmapnt -sP gef.corp.net.***
Intended effect: Ping each IP access in the range gef.corp.net.0/24
Output:

```
Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
Based on nmap by fyodor@insecure.org ( www.insecure.org/nmap/ )
```

Nmap run completed – 256 IP addresses (0 hosts up) scanned in 8 seconds

Evaluation: No host answered to ping, as per policy

B. Perform a TCP and UDP portscan of the entire gef.corp.com.0 Class C network

Tool used: **nmapNT 2.53 SP1**
Command executed: **nmapnt -sS -P0 -p "1-65535" gef.corp.net.***
Intended effect: Perform a TCP SYN scan on all TCP ports at all IP addresses in gef.corp.net.0/24
Output:

```
Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
Based on nmap by fyodor@insecure.org ( www.insecure.org/nmap/ )
```

Interesting ports on www1.gef.com (gef.corp.net.80):
(The 65533 ports scanned but not shown below are in state: closed)

Port	State	Service
80/tcp	open	http
443/tcp	open	https

Interesting ports on www2.gef.com (gef.corp.net.81):
(The 65533 ports scanned but not shown below are in state: closed)

Port	State	Service
80/tcp	open	http
443/tcp	open	https

Interesting ports on www3.gef.com (gef.corp.net.82):
(The 65533 ports scanned but not shown below are in state: closed)

Port	State	Service
80/tcp	open	http
443/tcp	open	https

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Interesting ports on motd1.gef.com (gef.corp.net.140):
(The 65534 ports scanned but not shown below are in state: closed)

Port	State	Service
14140/tcp	open	unknown

Interesting ports on motd2.gef.com (gef.corp.net.141):
(The 65534 ports scanned but not shown below are in state: closed)

Port	State	Service
14140/tcp	open	unknown

Interesting ports on ftp.gef.com (gef.corp.net.21):
(The 65534 ports scanned but not shown below are in state: closed)

Port	State	Service
21/tcp	open	ftp

Interesting ports on extmail.gef.com (gef.corp.net.25):
(The 65534 ports scanned but not shown below are in state: closed)

Port	State	Service
25/tcp	open	smtp

Interesting ports on ns.gef.com (gef.corp.net.53):
(The 65534 ports scanned but not shown below are in state: closed)

Port	State	Service
53/tcp	open	dns

Nmap run completed – 256 IP addresses (8 hosts up) scanned in 1hr 35min 16sec

Evaluation: No host answered on a TCP port that was disallowed by policy

Command executed: `nmapnt –sU –P0 –p "1-65535" gef.corp.net.*`
Intended effect: Perform a UDP port scan on all TCP ports at all IP addresses in gef.corp.net.0/24
Output:

```
Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
EEye Digital Security ( http://www.eEye.com )
Based on nmap by fyodor@insecure.org ( www.insecure.org/nmap/ )
```

Interesting ports on ns.gef.com (gef.corp.net.53):
(The 65534 ports scanned but not shown below are in state: closed)

Port	State	Service
53/udp	open	dns

Interesting ports on sparky.gef.com (gef.corp.net.153):
(The 65534 ports scanned but not shown below are in state: closed)

Port	State	Service
53/udp	open	dns

Nmap run completed – 256 IP addresses (2 hosts up) scanned in 1hr 22min 40sec

Evaluation: No host answered on a UDP port that was disallowed by policy. Was unable to test full connectivity to the VPN servers because we were unable to find a tool that could scan IP Protocols 50 and 51.

C. Ping and traceroute to a "known good" Internet node from selected IT staff nodes

Tested from: Windows 2000 workstation quimbyrw.gef.com (10.10.10.127)
Command & Output:

```
Pinging weebairn.home.com [home.com.17.250] with 32b of data:

Reply from home.com.17.250: bytes=32 time=80ms TTL=128
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Reply from home.com.17.250: bytes=32 time=86ms TTL=128
Reply from home.com.17.250: bytes=32 time=83ms TTL=128
Reply from home.com.17.250: bytes=32 time=96ms TTL=128

Ping statistics for home.com.17.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 80ms, Maximum =  96ms, Average =  86ms
```

Tested from: Windows 2000 workstation quimbyrw.gef.com (10.10.10.127)
Command & Output:

```
tracert weebairn.home.com

Tracing route to weebairn.home.com [home.com.17.250]
over a maximum of 30 hops:

  1   <10 ms   <10 ms   <10 ms  fred.gef.com [gef.corp.net.1]
  1   <10 ms   <10 ms   <10 ms  ren052-s1-rj2.int.ren.net [ren.net.1.238]
  1   <10 ms   <10 ms   <10 ms  rengw-atm5-3.int.ren.net [ren.net.44.2]
  1   <10 ms   <10 ms   <10 ms  usc-e2-q9q.uu.net [uu.net.240.3]
  1   <10 ms   <10 ms   <10 ms  igw5.home.com [home.com.199.102]
  1   <10 ms   <10 ms   <10 ms  weebairn.home.com [home.com.17.250]

Trace complete.
```

D. Ping and traceroute to a “known good” Internet node from a node in each DMZ and Internal Network

Tested from: The command line at External DMZ node www1.gef.com (10.10.1.80)
Command & Output:

```
ping weebairn.home.com
Pinging weebairn.home.com [home.com.17.250] with 32b of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for home.com.17.250:
      Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds
      Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Tested from: The command line at External DMZ node www1.gef.com (10.10.1.80)
Command & Output:

```
tracert weebairn.home.com

Tracing route to weebairn.home.com [home.com.17.250]
over a maximum of 30 hops:

  1    fred.gef.com [gef.corp.net.1] reports: Destination net unreachable.

Trace complete.
```

The same commands were executed from each of the following nodes, resulting in identical output:

- External DMZ node www1.gef.com (10.10.1.80)
- Admin DMZ node extmail.gef.com (10.10.3.25)
- Employee DMZ node joey.gef.com (10.10.5.65)
- Partner DMZ node tacky.gef.com (10.10.7.65)
- General Network node smithwt.gef.com (10.10.10.172)

SANS Institute 2000 - 2002, Author retains full rights.

- Management Network node rollinsh.gef.com (10.10.20.88)
- Divination Network node squidhead.gef.com (10.10.30.22)
- Server Network node gef2dc2.gef.com (10.10.100.6)

Conclusions

The Outer Firewall is properly implementing the firewall security policy, and has passed that audit

© SANS Institute 2000 - 2002, Author retains full rights.

Network Perimeter Design
UNDER FIRE…

Locked onto Target

The network I chose to attack was that designed by Christine Schuetz in her GCFW Practical dated 8/15/00 (http://www.sans.org/y2k/practical/Chris_Schuetz.doc). Her design is for an internal firewall that protects a computer lab from the rest of the internal network.

Below is the network security archtecture:

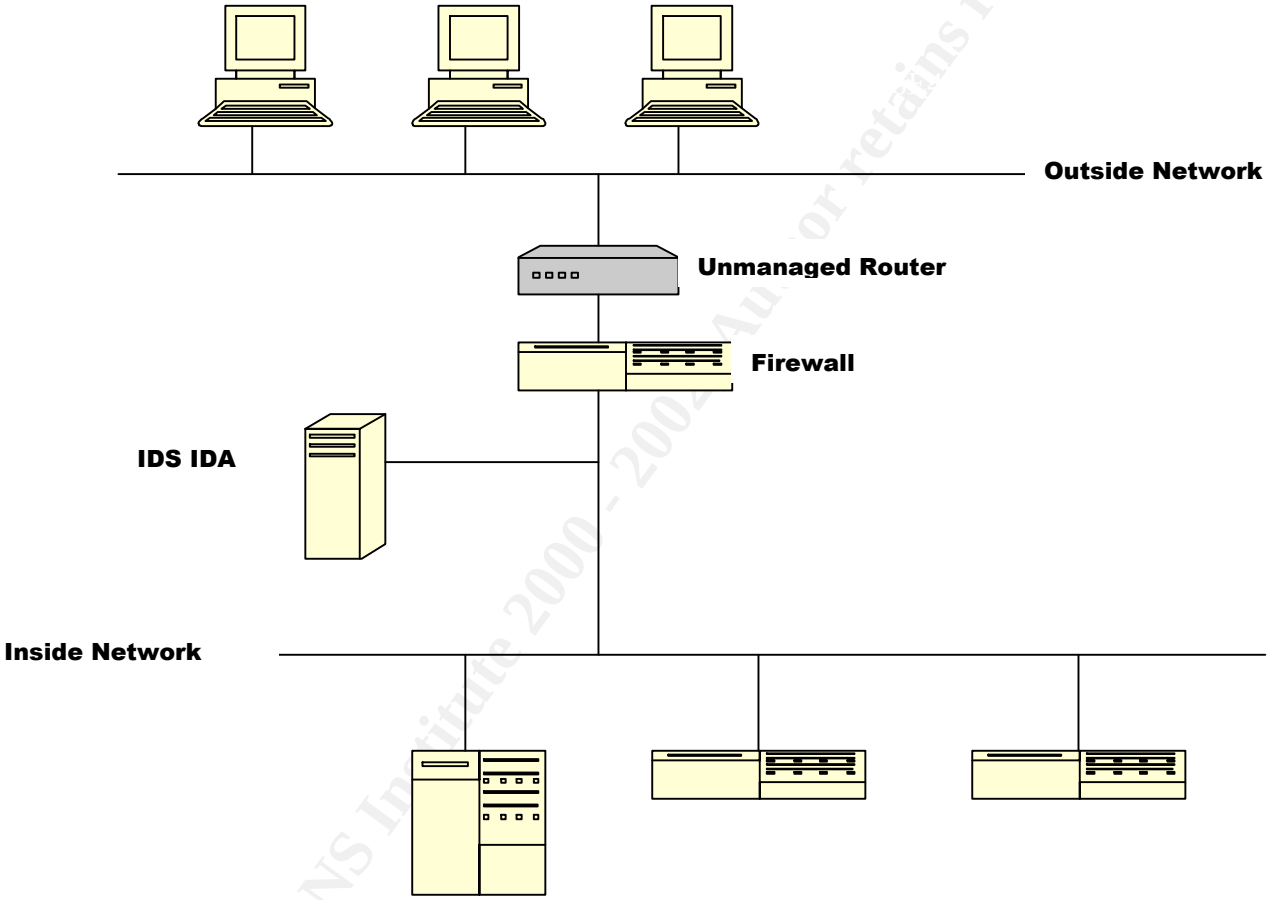


Figure 1 Network Design

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

And here is the firewall's rulebase:

No.	Source	Destination	Service	Action	Track	Install On	Time
1	Any	Any	WinNB	drop		secfw	Any
2	sec_lab_net	External_SecDNS DNS_1 DNS_2	domain-udp	accept		secfw	Any
3	External_SecDNS	Internal_DNS	domain-udp	accept	Long	secfw	Any
4	Internal_DNS	External_SecDNS	domain-tcp	accept	Long	secfw	Any
5	sec_lab_net	mail_svr	smtp	accept	Long	secfw	Any
6	Any	sec_lab_net	echo-request	drop	Long	secfw	Any
7	sec_lab_net	Any	dest-unreach time-exceeded echo-reply	drop	Long	secfw	Any
18	sec_lab_net	Any	icmp-proto	accept	Long	secfw	Any
19	Any	sec_lab_net	icmp-proto	accept	Long	secfw	Any
10	CS_NTwkst secfw	secfw CS_NTwkst	FW1_log FW1_mgmt FW1	accept	Long	secfw	Any
11	sec_lab_net sec_wkhm	sec_wkhm sec_lab_net	ssh	accept	Long	secfw	Any
12	Any	Any	Any	drop	Long	secfw	Any

Figure 09 Complete Rule Base

The critical points of the design are:

- The perimeter simply consists of a Sparc5 workstation running CheckPoint Firewall-1 v4.0
- The router connecting the firewall to the rest of the internal network is not under her control, so we have no knowledge or control over the ACLs put in place there
- An NFR intrusion detection system monitors the connection to the firewall's inside interface
- The firewall security policy can be summarized as:
    - All Windows NetBIOS traffic is blocked in both directions
    - Lab nodes may directly query internal, non-Lab DNS servers located outside the lab perimeter
    - A Lab-internal DNS server can communicate with an internal DNS server located outside the lab perimeter
    - No nodes outside the lab can ping lab nodes, nor can the following types of ICMP message exit the lab perimeter: destination unreachable, ttl-exceeded, echo reply
    - Lab nodes can ping nodes outside the lab
    - An internal lab node is configured to administer the firewall on proprietary CheckPoint ports
    - An external node is permitted to SSH into the lab across its perimeter
    - All other connection attempts are denied

Three possible attacks against the Firewall itself

Three possible attacks against this Checkpoint Firewall-1 are:

1. **Checkpoint Fragmentation DoS**: (http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html) Check Point FireWall-1 4.0 contains a special mechanism for logging certain IP fragmentation reassembly events to the console in real-time. During an IP fragmentation attack, this logging functionality consumes all available CPU resources, resulting in a frozen firewall – an effective denial of service.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Checkpoint has made new 4.0 kernels and Service Packs available that remove this vulnerability. However, an interim workaround is to enter the following command at the Firewall-1 command line:

$FWDIR/bin/fw ctl debug -buf

This immediately disables console logging. Then this line can be added to the $FWDIR/bin/fw/fwstart file so that console logging is automatically disabled upon boot-up.

2. **Username Information Giveaway**: (CVE-2000-1032): The client authentication interface for Check Point Firewall-1 4.0 and earlier generates different error messages for invalid usernames versus invalid passwords. This allows remote attackers to identify valid usernames on the firewall.

3. **File Overwrite Vulnerability**: (http://archives.neohapsis.com/archives/bugtraq/2001-09/0051.html) authenticated users of the CheckPoint Firewall-1 GUI are able to save arbitrary files on the firewall system, regardless of their permissions (read-only, monitor, user-edit and so on). All versions of FW-1 appear to be vulnerable.

On order to attempt the Checkpoint Fragmentation DoS against the Lab firewall, one would simply download the source code for jolt2, compile it on a Linux machine and run it against the firewall with the following command:

jolt2 <target ip_address>

The result would be that the Checkpoint firewall would become unusable

Denial of Service Attack

If the zombie master of 50 compromised cable modem/DSL computers were to target this perimeter using, say, a TCP SYN Flood, what would the result be? Well, 50 machines would be enough to eat up most or all available resources on the firewall, resulting in an effective DoS.

However, there are two things the firewall admin could do to minimize the impact of such an attack:

- **External ACLs**: The Lab admin could beg the Admin of the Internal network outside the Lab perimeter to put in ACLs blocking the sources of these IP addresses. However, if they're randomly spoofed addresses, this won't be effective.
- **SYNDefender**: Firewall-1 has a feature call SYNDefender that, when enabled, can act as a SYN gateway to intercept half-open sessions. With SYNDefender enabled, the session between the firewall and the internal node would not be initiated until the half-open session between the external node and the firewall was completed/fully opened. However, when SYNDefender's maximum number of half-open sessions is reached, the half-open sessions are dropped by the firewall – and the host was never touched. This will defeat the TCP SYN Flood attack
- **Other Flood Guards**: Today, many network devices, especially Cisco routers (see the **ip tcp intercept** family of commands that exist in IOS 12.1 and later), have mechanisms for "proxying" and controlling the number of half-open connections that are permitted to exist at a given time. If there is such a device on the internal network outside the lab perimeter, the Lab admin could beg the Admin to enable this feature.

Given that this is an internal firewall, however, one would hope that the administrator of the internal network outside the Lab perimeter would already have such measures in place to protect his/her network. If so, the risk of the attack making it as far as the lab firewall would be very low.

There's at least one path in…

There's a trust relationship between the Lab's DNS server and the internal DNS outside the lab perimeter. This is a vector that a BIND worm, such as Lion, could use to get past the Lab firewall.

From a SANS Security advisory written by Matt Fearnow of SANS and William Stearns or the Dartmouth Institute for Security Technology studies (http://www.sans.org/y2k/lion.htm), we know the following:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- The Lion worm spreads between DNS servers vulnerable to a buffer overflow in the Transaction Signature (TSIG) handling code. This includes Linux systems running BIND versions 8.2, 8.2-P1 and 8.2.20Px. BIND versions 8.2.3-REL and BIND 9 are not vulnerable.
- Lion generates random Class B addresses to look for vulnerable servers.
- Once it finds a vulnerable server, it exploits the system using the expoit called “name” and then installs the t0rn rootkit
- Once it has “taken root”, Lion then:
    - Kills syslogd to disable system logging
    - Emails /etc/passwd, /etc/shadow and some network settings to huckit@china.com
    - Deletes /etc/hosts.deny, potentially weakening TCP wrappers
    - Installs backdoor root shells at TCP 60008 and 33567 by inserting a line into /etc/inetd.conf
    - Installs a trojaned version of ssh on TCP 33568
    - Installs a trojaned version of login
- In addition, the t0rn rootkit replaces many binaries to hide itself.

The NFR intrusion detection system in this security architecture will catch Lion in transit across the perimeter.

Lion can be detected using on an infected host the lionfind script developed by William Stearns, which is available at http://www.sans.org/y2k/lion.htm. Snort can also detect Lion in transit with the following rule:

```
alert UDP $EXTERNAL any -> $INTERNAL 53
  (msg:"IDS482/named-exploit-tsig-infoleak";
  content: "|AB CD 09 80 00 00 00 01 00 00 00 00 00 00 01 00 01 20 20 20 20 02 61|";)
```

© SANS Institute 2000 - 2002, Author retains full rights.