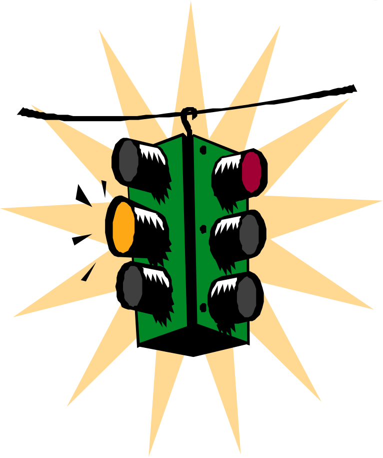
GIAC

CERTIFIED FIREWALL ANALYST



Version 4.0

Richard J. Ednie
February 17 2005

Summary: Companies such as GIAC Enterprises rely greatly on the Internet as a transport for their business to be conducted. Although the Internet offers incredible advantages to organizations and customers alike, it can also be a catalyst for exploitation and negative publicity, ultimately affecting the profitability and sustainability of a business. It is vital that companies do due-diligence in protecting the organization, its' employees, resources, and customers from being affected by malicious attacks from within and across the Internet as a medium. This paper will provide information on a technology that may have impact on the information technology and security industry. Additionally, this paper will provide policies with regard to the administration, operation, and security of GIAC Enterprises processes and network resources, with the goal being to secure the network in an economical and reasonable way focusing on defense-in-depth as much as possible.

Information security is the steps taken to mitigate risks. There are books written on the process to determine risks and how to place an economical mitigation strategy in place. Assuming this process was completed for GIAC Enterprises, it was determined that an appropriate network architecture along with ample security provisions have been planned and, if executed in accordance with this document, will meet the requirement for due-diligence and afford confidentiality, integrity, and availability to the company, employees, business associates, and it's customers.

A firewall is not simply a device but a combination of defense-in-depth protection incorporating a mix of security settings on devices as well as policies and procedures, and user education. All of these things combined can produce a strong and effective firewall protecting against intentional and unintentional damage to an organizations network and its resources. This paper will take all of that into consideration to produce such a firewall posture.

Resources Not Available: This practical, including any configurations and diagrams, was developed without the use of any actual equipment. I was not able to conduct any hands-on with real equipment due to the fact I travel extensively and don't personally administer a network. The content however, is based on my understanding and experience gained through extensive reading and through my work as an auditor of information systems for the Department of Defense. Although I feel I have a good grasp of the various security capabilities available, the configurations throughout this paper were not tested and the syntax shown is my best attempt without testing on actual equipment in a real, or lab, environment.

ASSIGNMENT ONE
VIRTUAL LOCAL AREA NETWORK ACCESS CONTROL LISTS (VACLS) & PRIVATE VLANS (PVLANS)

VLAN INTRODUCTION

Users within organizations can be physically separated from each other and/or from mission critical network resources either by being situated on different floors of a building, housed in different buildings, or even hundreds of miles away. To allow for users to communicate with other users as if they were on the same subnet, and provide transparent local-like communication, virtual LANs can be configured.

A VLAN can be described as basically a number of switch ports physically housed on one or more switches, and commonly assigned to a numbered virtual LAN. An access switch can have 24 ports in use connecting clients and/or servers. A number of these ports can be associated or assigned to a VLAN number. If properly configured, the hosts on the ports assigned to the specific VLAN will be able to communicate with each other at layer two of the Open Systems Interconnect (OSI) model, Media Access Control (MAC) layer. At this point there is no layer three (Network layer) requirement for IP or routing.

Since a typical switched network can span multiple switches, VLANs can be extended among them. In this way users in one building, being supported by one switch, can communicate seamlessly with users in another building physically attached to a different switch. As long as the VLAN assignment is the same on each switch and the switch has a means of connectivity for passing of VLAN data, devices connected to physical ports assigned to this VLAN will not notice any change in operation and will communicate as if they were all on the same switch and/or subnet.

The benefits VLANs provide are many. One of these benefits involves the fact that by creating a VLAN, you have reduced the size of and created one practical broadcast domain. Instead of a broadcast frame having to traverse the entire enterprise network, it will be contained within the assigned VLAN. This helps to reduce unnecessary traffic across the network and minimizes ill use of available bandwidth. Another benefit can be realized with the management of user moves or device relocations. If the VLAN is so configured, a user can physically relocate to another LAN connection without any further change to his or her computer, or to the supporting switch. In a large network with many users, this can add up to a significant savings in time for systems administrators.

There are also problems or concerns when working with VLANs. This paper will limit the discussion to that of security related issues. One of the purposes of a VLAN is to segment the network to keep local user traffic local and restrict or minimize Intra-VLAN communication. Typically in order to establish communications from one VLAN to another, a layer three device such as a router is required.

There are volumes written on VLAN technology and it is beyond the scope of this paper to cover every detail. The purpose of the paper is to discuss VLAN Access Controls (VACLs) and Private VLANs (PVLANs).

VACLs AND PVLANs

VLAN Access Control Lists are applied to control packets at or above layer 3, but on a layer 2 device. Once configured, the VACL is applied to a VLAN or in some cases to a layer 2 interface. Like typical router access control lists, packets are filtered by address, protocol, and/or port and the use of standard and extended lists still apply. Unlike router ACLs, the VACL is processed in hardware and therefore is less taxing on the CPU and ultimately faster to process. However, the layer 2 or layer 3 switch will require an added capability in the form of a policy feature card (PFC), and all switches do not support this.

VACLs, when configured and applied, create a set of match conditions and actions. As with router ACLs, the rule set ends with an implicit deny statement and where a match condition does not exist, the packet is dropped. The VACL can control traffic within a VLAN/subnet and beyond. As previously discussed, the VLAN reduces the size of a broadcast domain and keeps local VLAN traffic local to that VLAN. If you want to further isolate communication within a VLAN, the VACL can accomplish this.

The commands to configure a VACL will vary by operating system. In this example we will assume a Catalyst OS is used. In order to configure and utilize a VLAN ACL, there are three main steps. First you must create the access list, then create a map, and finally apply the access list. The following example establishes an extended named (subnet192) VLAN ACL on VLAN 192 and shows some sample rules:

```
Catalyst (enable)>set security acl ip subnet192 permit 192.168.0.0 0.0.255.255
    host 192.168.10.10
Catalyst (enable)>set security acl ip subnet192 permit icmp any any echo
Catalyst (enable)>set security acl ip subnet192 permit icmp any any echo-reply
Catalyst (enable)>set security acl ip subnet192 deny icmp any any
Catalyst (enable)>set security acl ip subnet192 permit ip 192.168.0.0
0.0.255.255
```

```
    host 192.168.10.20 smtp
Catalyst (enable)>commit security acl ip subnet192
Catalyst (enable)>set security acl ip map subnet192 192
```

Note: Commands one through five establish subnet192 as the extended named ACL and applies some rules. The commit entry moves the ACL from the edit buffer into the ternary content addressable memory (TCAM) of the switch, so that the switch can effectively use the access rule. The final step is to apply this to a particular VLAN. The last command places the ACL and all the configured rules within it onto VLAN 192. In this example the fact that subnet192 (ACL name) and 192 (VLAN) match was intentional. It is entirely optional as long as you follow the numbering scheme for type of ACL.

VLAN ACLs are similar to extended ACLs on a router. Some of those characteristics are:

- A list of permit and deny statements
- Rules checked top down until matched
- End with an implicit deny statement
- One VACL per VLAN
- Filter on source and destination address, and port.

Some additional features, unlike typical router extended ACLs:

- VACL is applied to the entire VLAN vice an interface port
- Not applied in a particular direction – instead they are checked across the bus
- They can filter traffic between devices in a VLAN

Another technology to further limit communication within a VLAN/subnet is with the use of Private VLANs or PVLANs. A PVLAN further segments a broadcast domain, or VLAN, to provide more granular control over the communication/connection processes between hosts in a VLAN. There are three types of PVLANs that can be configured on a switch. These are:

- Promiscuous: The ports configured as such are considered members of the primary VLAN and can communicate with any port in any direction within the PVLAN.
- Isolated: The ports configured here can only communicate to the promiscuous ports. The Isolated VLAN is considered a secondary VLAN.
- Community: These ports are able to communicate amongst each other and the members of the promiscuous ports. This type of port is also considered a secondary VLAN.

The following diagram, taken from *Hardening Network Infrastructure: Bulletproof Your Systems Before You Are Hacked!* by Wesley J. Noonan will help describe the restrictions on communication between devices when a PVLAN is configured. Here you can see that the two servers assigned to VLAN 12 are configured as an isolated VLAN and can only communicate with promiscuous ports in the primary VLAN. We have ports 3/14 and 3/15 configured as promiscuous, assigned to the primary VLAN (VLAN 11). This allows communication in either direction and to any device connected. Not shown here are the uses of community ports, but if required devices assigned to community ports would be able to communicate among themselves and with members of promiscuous ports.

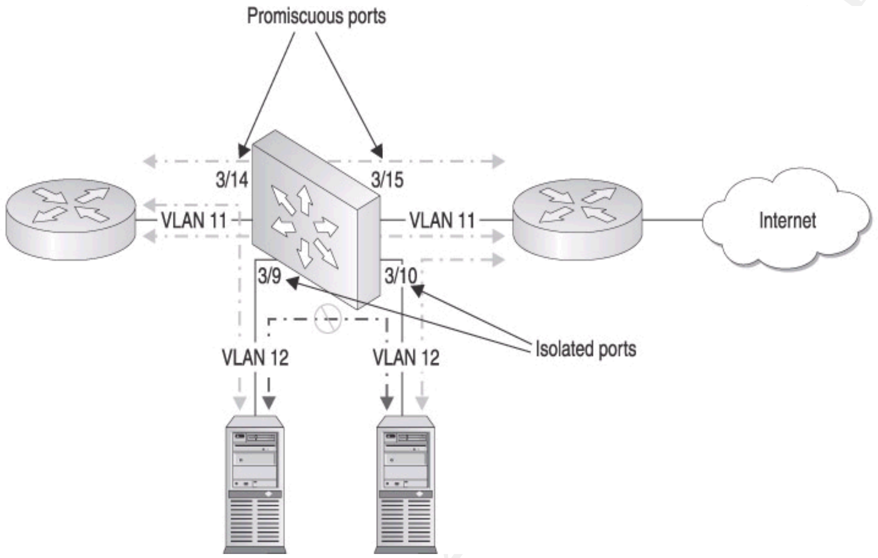


Figure 1: PVLAN diagram

It is important to note that the use of PVLANs require VLAN Trunking Protocol (VTP) *transparent mode* to be configured on the switch. VTP is a CISCO proprietary protocol for maintaining a consistent database of switches trunked together. Transparent mode is one of several modes that configure the switch to not participate in VTP. Since PVLANs are configured on a single switch, they cannot have membership on other switches. Additionally important to note is that PVLANs are limited to certain platforms. Catalyst 6000 and 4000 series are the CISCO products capable of PVLANs at the time of this writing.

To configure PVLANs you must set the switch to *vtp transparent mode*, create a primary VLAN, create isolated and community VLANs, bind the isolated and community VLANs to the primary VLAN, place ports into the isolated and community VLANs, and finally map the isolated and community VLANs to promiscuous ports. The following configuration example assumes a Catalyst operating system on a platform with a multilayer switch feature card (MSFC). VLAN11 is the primary, 12 and 13 are secondary VLANs:

```
Catalyst (enable)>set vtp mode transparent
Catalyst (enable)>set vlan 11 pvlan-type primary
Catalyst (enable)>set vlan 12 pvlan-type isolated
Catalyst (enable)>set vlan 13 pvlan-type community
Catalyst (enable)>set pvlan 11 12
Catalyst (enable)>set pvlan 11 13
Catalyst (enable)>set pvlan 11 12 3/9-10
Catalyst (enable)>set pvlan 11 13 3/2-8,11-23
Catalyst (enable)>set pvlan mapping 11 12 1/2, 15/1
Catalyst (enable)>set pvlan mapping 11 13 1/2, 15/1
Catalyst (enable)>session 15
MSFC_Catalyst>enable
MSFC_Catalyst#config t
MSFC_Catalyst (config)#interface vlan 11
MSFC_Catalyst (config-if)#ip address 192.168.10.1 255.255.255.0
MSFC_Catalyst (config-if)#no shut
MSFC_Catalyst (config-if)#end
MSFC_Catalyst#copy run start
```

DEFENSE IN DEPTH

Applying security is a decision made based on an understanding of the value of the data and the cost of its' loss. Where possible security should be applied in layers. Defense in depth is a way to leverage the security capabilities through layering. Whether it is on a server through the use of registry permissions, passwords, multiple users accounts, or on a firewall where packets are inspected and filtered based on a rule set, defense-in-depth is selective layering of these devices and settings. The thought being, if one layer of security is not strong enough, or fails, another layer may assume responsibility of protection.

VACLs and PVLANs, as previously discussed add to the layering of security within a network.

There are numerous ways a malicious user can attack a network. There are also inherent problems with communication taking place between devices when it is not required or desired. All of these potential risks need to be considered along with the cost of implementation and maintenance against the value of what you are hoping to protect.

IMPACT AND EFFECT

In my experience of conducting network security assessments I have visited many sites and I have yet to see these technologies in use. My suspicion is that most network teams are working hard to maintain what they have and are too undermanned to attempt to implement features that will enhance their security and operation.

The impact to administrators responsible with the day-to-day operation of a network is probably great if attempting to implement this on the fly. Each organization should be aware of these features and consider its' feasibility. The effect to the network overall will be increased security and better use of bandwidth. Depending upon the size and complexity of the network, utilizing these features may be quite daunting when applying them to an existing architecture.

Before implementing any type of configuration or security practice, an organization should weigh the requirement. If the loss of data or network resources wouldn't significantly impact an organization financially or otherwise, it may not be prudent to put security controls at every layer. However, by incorporating varied levels of security into your network, a defense-in-depth posture can be achieved. If one layer of security fails, it is hopeful another security setting or layer will provide the additional protection. If the use of ACLs and Private VLANs are considered appropriate for your switched network, implementing both can aid in providing that defense-in-depth protection.

-

ASSIGNMENT TWO
GIAC ENTERPRISES
SECURITY ARCHITECTURE

Introduction: GIAC Enterprises headquarters is located in Rockledge, Florida and employs 50 personnel. There are 31 employees that operate at the main headquarters, 4 employees at each of the satellite offices located in Canada, Germany, and France, and an additional 7 employees operating out of the Washington D.C. office.

Network overview and access methods: GIAC Enterprises network architecture allows for various methods of access to accommodate the wide range of users, customers, suppliers, and partners.

Users at the headquarters connect to the local area network via 100Meg connections from the desktop to the access switch. User traffic is isolated into a virtual local area network at the access switch. This works to contain broadcast traffic and segregate user data from other data such as management traffic. For access to the Internet, users traverse the CISCO Catalyst 3550 switch. This switch, acting as the premise router, is configured with access controls to control packets entering and leaving the internal network. Additionally there are two redundant CISCO PIX firewalls that provide application layer, stateful inspection of the packets traversing the network. All data entering or leaving the network will be inspected at the firewall. The firewall provides network address translation (NAT) for all internal assets which hides the internal IP addresses of hosts to the outside, untrusted, wide area network. And the PIX515e serves as the VPN termination point for external users, providing an encrypted tunnel across the Internet utilizing IPSec.

Remote users, such as sales personnel, connect back to the headquarters network via a virtual private network (VPN) connection either through a broadband connection or via a dial-up. Each remote user has a laptop with a modem and 10/100Megabit network interface card that they use for this purpose. The laptops, as well as desktops, are a standard configuration from a ghosted image. Each device has the CISCO VPN Client, a personal firewall and anti-virus programs installed.

Satellite offices also utilize the Internet and establish a site-to-site VPN tunnel via IPSec. Each satellite office maintains a small network including user workstations or laptops, a switch, and a CISCO PIX 501 firewall. The Internet connection at each remote site is provided through a Digital Subscriber Line (DSL) service and the Internet is used as a transport back to the headquarters via VPN tunneling. While telecommuting, users can either connect to an available broadband connection in a hotel or their home and establish a VPN connection, or boot their PC into their dial-up profile and utilize their modem for

Internet access where the VPN connection can be initiated. Employees at the satellite offices are primarily charged with maintaining relations with local customers, partners, and suppliers. Additionally, they research new opportunities for expanding the business by making sales pitches to local establishments.

Partners and suppliers utilize the Internet to connect to the public webserver and complete a form to request an account with GIAC Enterprises. Once received the appropriate sales person makes phone contact and discusses the details of the business and reviews agreements for establishing a relationship. Once approved to become a partner or supplier, an account is created to allow the access to the secure webserver. Partners provide translation and resale services and conduct business via secure web connection and email. Suppliers also conduct business in such a manner and provide fortune-cookie sayings based on various order requests.

Customers access GIAC Enterprises through the Internet using HTTP (port 80) to a public web server located in the headquarters demilitarized zone (DMZ). At this point they can access information about the company, review samples of fortune cookie sayings, request secure access, and learn how to conduct business with GIAC Enterprises. If a transaction is required, such as placement of an order, the customer is provided with an Secure Sockets Layer (SSL/port 443) encrypted session. Here they can submit, review, or provide payment for an order. Once the order is received and processed, the customer receives an email notification that the order is available for download. The customer then reconnects to the secure site via HTTPS, and downloads his/her fortune cookie sayings.

The network design for GIAC Enterprises was based on user access requirements, scalability for future growth, security requirements, current support personnel, and budget constraints. Redundancy has been built in where considered necessary. This redundancy aids in ensuring availability in the event of device failure or path disruption. Each remote site has a more basic network and is configured similarly to each other for consistency. The network architecture at the headquarters is depicted below and consists of the following:

a. <u>Internet connectivity</u>: The Headquarters has two redundant connections to the Internet. These include a fractional T1 and DSL.
b. <u>CISCO's CATALYST 3550 12G</u>: There are many options available but the Catalyst 3550 12G was selected as the edge device as it meets the requirements of the small to medium-sized business and offers ample connectivity and security. CISCO is a major player in the network industry and GIAC Enterprises felt comfortable with their products and the ease in administration. This device brings in the Internet connection and through the use of access control lists (ACLs)

applied to the external and internal interfaces, ingress and egress packet-filtering is performed. This provides one layer of the overall defense-in-depth concept to protect the internal network resources from attack as well as from becoming a distributed denial of service platform where internal hosts are used for outbound malicious activity. The ACLs are configured as deny-by-default, permitting only necessary packets in/out. There is an egress filter applied to the internal interface and an ingress filter applied to the external interface. This separation is done primarily to reduce the load on the 3550 CPU, as packets will be checked against the rules at the nearest interface of origin. Additionally there are two of these multi-layer switches installed, for failover, running hot standby routing protocol (HSRP). The Catalyst 3550 12G switch provides:

a. 2 10/100/1000 ports and 10 GBIC-based Gigabit Ethernet ports
b. 1.5 rack unit (RU) stackable, multilayer Gigabit Ethernet switch
c. Delivers full dynamic IP routing and intelligent services to the network edge
d. Enhanced Multilayer Software Image (EMI) installed
e. Ideal for stack aggregation, server aggregation, mini-POP aggregation, or small network cores and backbones

Some additional security measures that are in place on this device include:

- Strong password applied for access (enable secret/MD5).
- Access restricted to out-of-band only (console).
- Individual user accounts applied with various privilege levels.
- All management access logged.
- Idle timeout set to 15 minutes.
- Default services not needed were identified and turned off.
- Physically located in a locked cabinet, and in a secure room with limited access.

c. CISCO PIX 515e is the firewall of choice for GIAC Enterprises Headquarters. For redundancy purposes there are two appliances installed. The 515e security appliance offers stateful, application layer inspection, virtual private networking (VPN), network address translation (NAT), and limited intrusion detection (IDS) capability in a single platform. There are many other features offered by the PIX 515e but only these will be discussed here. Some of the desired features include:

a. Stateful inspection by the 515e prevents unauthorized connections by tracking the state of connections. It adds to the security provided by the Catlyst 3550's packet filtering access control lists, thereby providing another layer of protection ultimately enhancing defense-in-depth.
b. Application and protocol inspection involves looking deeper into

the packet than the layer 3 device can. The 515e “has over two dozen specialized inspection engines for protocols such as HTTP, FTP, SMTP, DNS, SMB, and many more.”

c. The 515e’s VPN capability provides the termination point for tunneled connections across the Internet. This allows use of an open untrusted transport, to pass company sensitive data by providing an encrypted tunnel to clients. The 515e includes an unlimited license of the client VPN software that meets the existing need and allows for future growth.

d. The built-in IDS feature of the 515e is designed for the small to medium-sized business and provides notification of various types of attacks as well as an optional blocking of those attacks. Intrusion detection aids in defense-in-depth by giving site administrators and security personnel an awareness of activity on a network that may be malicious or at least ouside the scope of the network’s normal use. The 515e looks at over 55 different attack signatures and protects against various forms of denial-of-service attacks. Since the IDS is built-in to the firewall, the placement between internal and external resources provides a heads-up to potential attacks coming from the outside, as well as unwitting attacks hosted from the inside such as distributed denial-of-service.

e. Network Address Translation hides internal addresses from external sources by translating a publicly known address to internal host addresses. This provides another layer of defense-in-depth to protect resources.

f. There are three network interface cards (NICs) configured to segment traffic from the external network, the internal network, and the demilitarized zone (DMZ) subnets. One NIC connects to the 3550 edge device, one to an internal switch, and one to a DMZ switch.

Some additional security measures that are in place on this device include:

- Strong password applied.
- Individual user/admin accounts created.
- All access is logged.
- Unneeded services disabled.
- Physically located in a locked cabinet, and in a secure room with limited access.

d. CISCO Catalyst 2950G-48 EI switches have been selected for the access layer where clients, printers, servers and such will connect internally. VLANs internally will be configured to segment the various types of resources improving on bandwidth utilization and maintaining isolation of different types of communication. The placement of the switches will be off of the firewall to provide internal as well as DMZ access.

a. "Cisco Catalyst 2950G-48 is a member of the Catalyst 2950 Series Intelligent Ethernet Switches, and is a fixed-configuration, stackable switch that provides wire-speed Fast Ethernet and Gigabit Ethernet connectivity for midsized networks and the metro access edge. The Catalyst 2950 Series is an affordable product line that brings intelligent services, such as enhanced security, high availability and advanced quality of service (QoS), to the network edge while maintaining the simplicity of traditional LAN switching."
b. There are three switches overall including a DMZ switch off of one NIC of the PIX 515e firewall and two switches (trunked) connected to another NIC of the firewall.
c. The DMZ is created to place publicly accessible servers and avoid external users having to access the internal network.

Some additional security measures that are in place on this device include:

- VLANs created to isolate traffic.
- Unused ports are assigned to an unused VLAN and that VLAN is disabled.
- Strong password applied for access (enable secret/MD5).
- Access restricted to out-of-band only (console).
- Individual user accounts applied with various privilege levels.
- All access logged.
- Idle timeout set to 15 minutes.
- Default services not needed were identified and turned off.
- Physically located in a locked cabinet, and in a secure room with limited access.

e. <u>Microsoft Domain Servers</u>:

a. The network is served through MS Windows 2000 domain controllers and member servers. Some of the services provided include DNS/IIS/SQL/FILE/PRINT.

Some additional security measures that are in place on these devices include:

- Critical patches are applied.
- Unneeded services are disabled.
- Strong password required utilizing ENPASFLT.
- Registry/File permissions tightened.
- Registry/File auditing turned on.

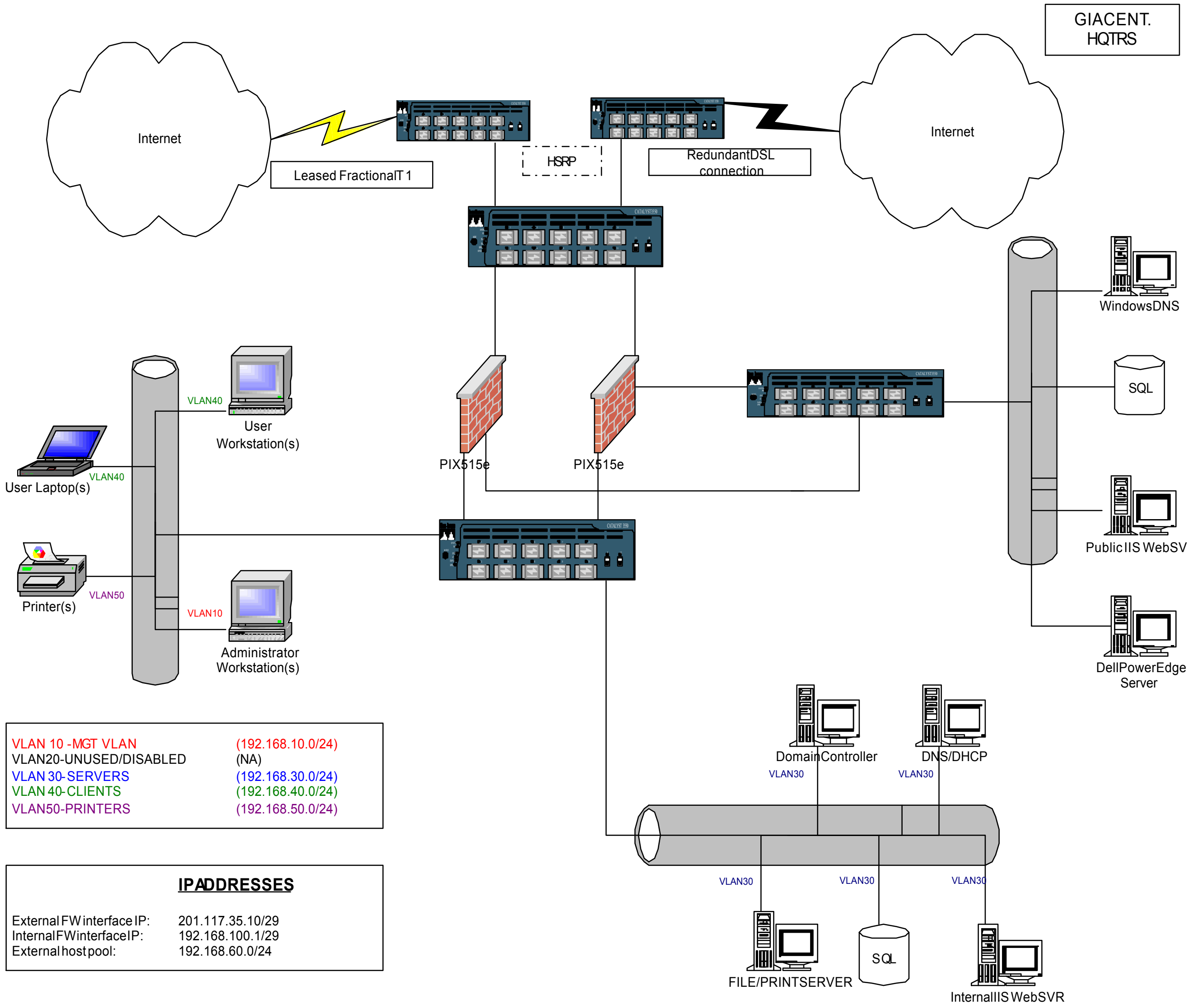
- Password protected screensaver set to launch after 15 minutes of inactivity.
- Servers are physically secured in a locked cabinet.

f. Client workstations:
   a. Running Windows 2000 Professional operating system.
   b. Systems are ghost imaged and include the following basic applications:
      i. Microsoft Office suite
      ii. CISCOs VPN Client software
      iii. Personal Firewall
      iv. Anti-virus
   c. Each user has non-administrative access to their device. One local and domain account is created and provided.

Some additional security measures that are in place on all MS Windows devices include:

- Critical patches are applied.
- Unneeded services are disabled.
- Individual accounts created.
- Strong password required utilizing ENPASFLT.
- Registry/File permissions tightened.
- Registry/File auditing turned on.
- Password protected screensaver set to launch after 15 minutes of inactivity.

The following diagram depicts a representative architecture in place at the headquarters.

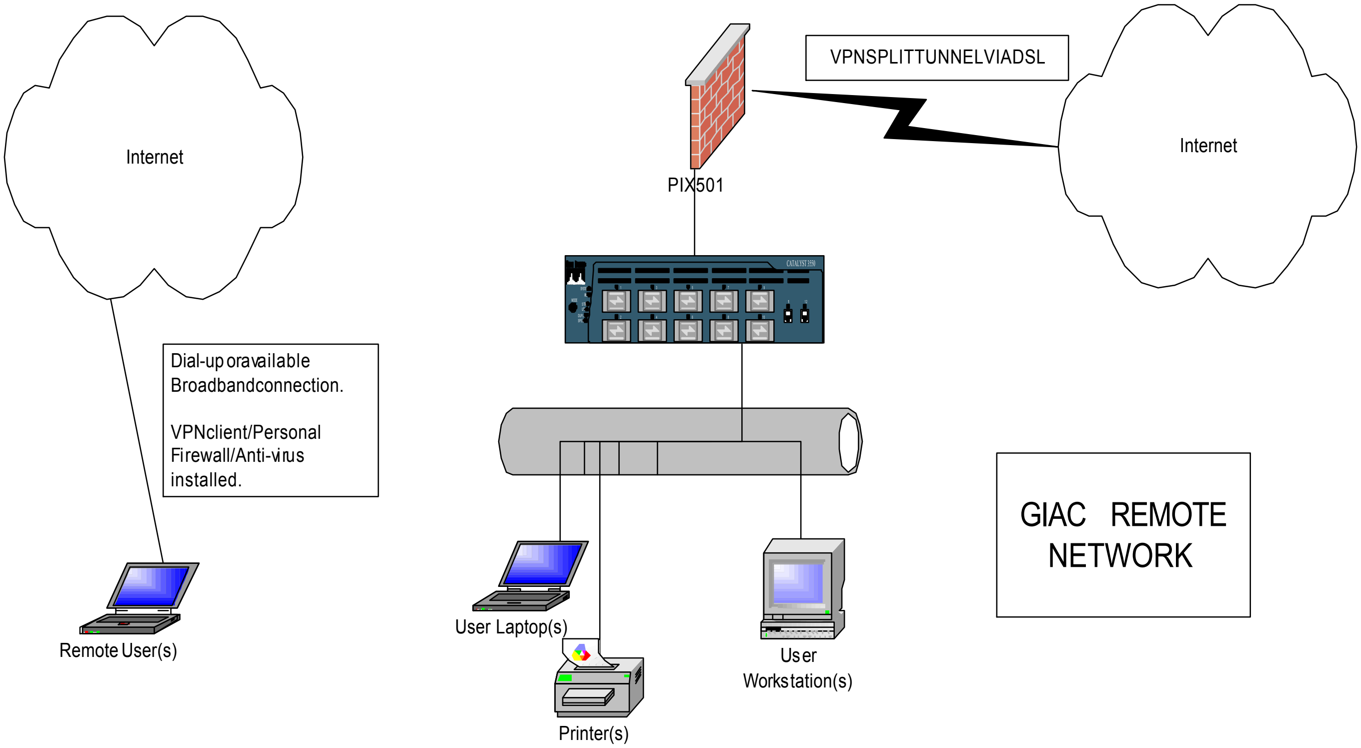


VLAN 10 -MGT VLAN	(192.168.10.0/24)
VLAN20-UNUSED/DISABLED	(NA)
VLAN 30-SERVERS	(192.168.30.0/24)
VLAN 40-CLIENTS	(192.168.40.0/24)
VLAN50-PRINTERS	(192.168.50.0/24)

IPADDRESSES

External FWinterface IP:	201.117.35.10/29
InternalFWinterfaceIP:	192.168.100.1/29
Externalhostpool:	192.168.60.0/24

Each satellite office maintains a DSL connection for access to the Internet. In order for employees to communicate and/or conduct business within GIAC Enterprises, each user will have two profiles configured on their PC. One profile will be for a broadband and one for a dialup connection. The purpose of the dual-boot profile is to isolate the NIC and modem from being active at the same time. In either case the user will utilize the CISCO VPN Client to establish a secure connection to GIAC Enterprises across the Internet. If the employee is operating on the office LAN, the CISCO PIX 501 will provide the appropriate VPN connection.



4. Business Operations. The following subparagraphs describe the various types of groups that require access to GIAC Enterprises network resources whether it is to conduct business, order products, or administer the devices. These groups include: Employees (including internal as well as remote), Customers, Suppliers, Partners, and the general public.

   a. Employees:
      a. Users have dual-profiled computers allowing them to boot to a NIC

activated profile while utilizing broadband, and to a modem only activated profile when dial-up is the only available method of Internet connectity. While in the office users connect to the access switch via 100 Megabit connections. Users are authenticated at the domain level and have non-administrative access to their computer and network resources. Internal communication is controlled through VLAN membership. External communication is routed up to the layer three switch via the firewall and out to the Internet. When an employee is out of the office, he/she logs on locally to their computer and once connected to the Internet via broadband or dial-up launch the VPN client for secure tunneling.

b. Customers may include individuals or established businesses. These customers are geographically dispersed throughout the United States, Canada, and Europe and communicate with GIAC Enterprises via an external web page, which offers a means to research and order our products. These customers are offered a secure means of providing their credit card and other personal information in order to place an order. Forms are provided on the external website and the technology selected for secure processing is 128bit Secure Sockets Layer (SSL).

c. Business partners include suppliers and resellers. Suppliers and resellers, like employees, utilize a VPN connection into the GIAC Enterprise network where they access specific servers for submitting and reviewing fortune cookie sayings. The VPN client software is provided by GIAC Enterprises upon establishment of a business relationship.

d. Business transactions include receiving and filling orders, billing, and shipping. The appropriate department carries out each of these processes. Individuals, such as customers, access the company's website via their individual Internet Service Providers. Most web browsers are supported on the client machines, however when placing an order, the customer is prompted to select secure or non-secure means. If secure is selected, 128bit Secure Sockets Layer (SSL) encryption is required. The public web server is physically located in a demilitarized zone (DMZ). The internal network is configured as a screened subnet through a second network interface housed in the perimeter firewall.

5. Ports/Protocols and filtering.

This section lists the various ports and protocols that will traverse the network. Also shown is the ACL's configured on the premise router to assist in the controlling of packets. The final section of this paper will illustrate the configuration of the firewall. Through a combination of router and firewall rules, and a practice of shutting down unneeded services on individual devices, a defense-in-depth posture will be achieved:

PORT	**PROTOCOL**	**SERVICE**
80	TCP	HTTP
22	TCP	SSH
25	TCP	SMTP
53	TCP,UDP	DNS
123	TCP,UDP	TIME
150	TCP	SQL-NET
443	TCP	HTTPS
500	UDP	ISAKMP
514	UDP	SYSLOG
1521-1535	TCP	SQL*NET

Premise Router

Ingress extended access control lists are placed on the external interface as such:

BLOCKING DDoS PORTS

```
access-list 100 deny tcp any any eq 27665 log
access-list 100 deny tcp any any eq 31335 log
access-list 100 deny tcp any any eq 27444 log
access-list 100 deny tcp any any range 31337-31338 log
access-list 100 deny tcp any any eq 16660 log
access-list 100 deny tcp any any eq 65500 log
access-list 100 deny tcp any any eq 33270 log
access-list 100 deny tcp any any eq 47017 log
access-list 100 deny tcp any any range 6711-6712 log
access-list 100 deny tcp any any eq 6776 log
access-list 100 deny tcp any any eq 6669 log
access-list 100 deny tcp any any eq 2222 log
access-list 100 deny tcp any any eq 7000 log
access-list 100 deny tcp any any eq 2001 log
```

```
access-list 100 deny tcp any any eq 65301 log
```

BLOCKING OF IANA UNALLOCATED AND RESERVED ADDRESSES

```
access-list 100 deny ip 1.0.0.0 0.255.255.255 any log
access-list 100 deny ip 2.0.0.0 0.255.255.255 any log
```

and so on…list is available at http://www.iana.org/assignments/ipv4-address-space

BLOCKING OF RFC 1918 PRIVATE ADDRESSES

```
access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
```

and so on…list is available at http://www.ietf.org/rfc/rfc1918.txt

BLOCKING OF MULTICAST SOURCES AND CLASS “E” RANGES

```
access-list 100 deny ip 224.0.0.0 31.255.255.255 any log
access-list 100 deny ip 240.0.0.0 15.255.255.255 any log
```

BLOCKING OF INTERNAL ADDRESSES FROM ENTERING THE NETWORK

(in this case since we’re using private IP’s internally a rule is already in place)

BLOCKING OF INBOUND ICMP

```
access-list 100 deny ICMP any any log
```

ALLOW IN ALL AUTHORIZED TRAFFIC

(note: no log statement as this would be too much to log) This entry overrides the implicit deny all statement at the end of the filter.

```
access-list 100 permit ip any any
```

Egress extended access control lists are placed on the internal interface as such:

The configuration will include all the ingress rules listed but the rule for allowing legitimate traffic will point to the firewall’s external IP address:

```
! allowing legitimate outbound traffic
access-list 101 permit ip (external firewall IP) any
access-list 101 deny ip any any log
```

ASSIGNMENT THREE
GIAC ENTERPRISES
FIREWALL POLICY

Introduction: The firewall in place at GIAC Enterprises is the CISCO PIX 515e. The purpose of this device is to control network traffic and provide a layer of defense against intentional or unintentional malicious access by internal as well as external individuals and devices. The PIX has been placed in between the external and internal network by connecting the external interface to the premise layer three switch, the internal interface to the internal switch, and a third interface to a switch serving hosts within the DMZ. In addition to providing stateful inspection and application proxying, the PIX is also configured as the network Intrusion Detection System.

Firewall Rules: The PIX is in a deny-all inbound and allow-all outbound by default. I have configured the outbound with an explicit deny all at the end of the outbound rules to override the default condition. Those ports, protocols, and services determined to be required are controlled through the firewall permit access control list statements. In the following sections I will work through the configuration and include explanations of the various output:

Interfaces

By default the PIX has an outside and inside interface with default security zones of 0 and 100. The lower the number the less secure it is. Additional interfaces can be configured to add additional networks. In our case we have a DMZ and have assigned that security level 50. The levels basically control the flow of traffic in that traffic can pass from a higher level to a lower level but not the other way around unless a rule is put in place.

```
nameif ethernet0 outside security0
nameif ethernet1 dmz security50
nameif ethernet2 inside security100
```

Passwords

Passwords assigned for non-privleged and privileged level access:

```
enable password XXXXXXXXXXXX encrypted
passwd XXXXXXXXXXXX encrypted
```

The *nat* command

Network Address Translation is performed by the firewall either statically or dynamically. The purpose of NAT is to translate one address to another. The result is the ability to hide internal addresses from external exposure. It also allows you to limit the number of public IP addresses required as internal addresses can be configured as private iaw RFC1918, with NAT translating these non-routeable addresses to one or many public addresses.

A *show nat* and *show global* command will reveal the configuration in the PIX:

```
PIXA# show nat
nat (inside) 1 192.168.30.0 255.255.255.0 0 0
nat (inside) 2 192.168.40.0 255.255.255.0 0 0
nat (inside) 3 192.168.50.0 255.255.255.0 0 0
PIXA# show global
global (outside) 1 XXX.117.35.1-XXX.117.35.254 netmask 255.255.255.0
global (outside) 2 XXX.117.36.1-XXX.117.36.254 netmask 255.255.255.0
global (outside) 3 XXX.117.37.1-XXX.117.37.254 netmask 255.255.255.0
```

The example above shows three interfaces on the firewall with inside private addresses with their translated IP address range for advertisement to the non-trusted public network.

The *fixup* command

CISCO PIX Adaptive Security Algorithm is the key to providing stateful application inspection of packets. One of the features of the "fixup" command is to force this inspection process. You can also use the command to change the default port assigned to a specific service. In this example I show the default settings of the PIX, and I have not changed them:

```
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol sqlnet 1521
```

Access Control Lists

Since the PIX is CISCO based, the syntax is very similar to IOS. Therefore setting access control lists on the firewall are very much the same as setting them on the router. Traffic can be filtered based on:

- source and/or destination address
- source and/or destination TCP/UDP ports

One key difference between router ACL's is that you can only apply a firewall ACL to filter inbound to the firewall. On a CISCO router, you could put an inbound and an outbound ACL on one interface. That is not the case here.

Another important note deals with the order of rules in the access list. On a PIX access lists rules are checked and action is taken on the first match.

Internal to DMZ

These connections will involve port 80 for browsing, port 25 for mail, port 443 for secure web-browsing, and port 53 for DNS lookup. This access list will be applied to ethernet02 using the *access-group* command.

```
access-list inside permit tcp (internal IP range) (dmz IP) eq 80
access-list inside permit tcp (internal IP range) (dmz IP) eq 25
access-list inside permit tcp (internal IP range) (dmz IP) eq 53
access-list inside permit udp (internal IP range) (dmz IP) eq 53
access-list inside permit tcp (internal IP range) (dmz IP) eq 443
access-list inside deny ip (internal IP range) (dmz IP range) log
```

External to DMZ

These connections will involve port 80 for browsing, port 25 for mail, port 443 for secure web-browsing, and port 53 for DNS lookup. This access list will be applied to ethernet01 using the *access-group* command.

```
access-list outside permit tcp any (dmz IP) eq 80
access-list outside permit tcp any (dmz IP) eq 25
access-list outside permit tcp any (dmz IP) eq 53
access-list outside permit udp any (dmz IP) eq 53
access-list outside permit tcp any (dmz IP) eq 443
access-list outside deny ip any (dmz IP range) log
```

DMZ to Internal

These connections would involve port 66 for SQL*NET, port 25, and port 53. This would be included on the ethernet01 interface.

```
access-list inside permit tcp (dmz IP) (internal IP) eq 66
access-list inside permit udp (dmz IP) (internal IP) eq 66
access-list inside permit tcp (dmz IP) (internal IP) eq 25
access-list inside permit tcp (dmz IP) (internal IP) eq 53
access-list inside permit udp (dmz IP) (internal IP) eq 53
```

PIX VPN CONFIG

The PIX serves as the VPN termination point and utilizes IPSec. IPSec is an open standard that provides data confidentiality, data integrity, and data origin authentication between IPSec peers, in this case between satellite site's and VPN clients. There are basically four steps in configuring IPSec:

- configuring IKE (Internet Key Exchange) for preshared keys
- configuring IPSec
- configuraing NAT
- configuring PIX options

Configure IKE:

Enable ISAKMP (Internet Security Association Key Management Protocol) on the outside interface of each firewall.

```
isakmp enable outside
```

Define IKE policies:

```
isakmp policy 1 authentication pre• share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
```

Configure Pre-shared key and assign peer IP address:

```
isakmp key XXXXXXX  address XXX.45.18.10 netmask 255.255.255.255
```

Configure IPSec

```
access-list 101 permit ip 192.168.0.0 255.255.0.0 XXX.45.18.0 255.255.255.0
crypto ipsec transform• set maxum esp• des esp• md5• hmac
crypto map transam 1 ipsec• isakmp
crypto map transam 1 match address 101
crypto map transam 1 set peer 172.22.112.12
crypto map transam 1 set transform• set maxum
crypto map transam interface outside
```

Configure NAT (The 0 tells the PIX not to NAT VPN traffic identified in ACL 101

```
nat (inside) 0 access• list 101
```

REFERENCES

SANS GIAC: Inside Network Perimeter Security
Stephen Northcutt, Lenny Zeltser; Scott Winters; Karen Kent Frederick; Ronald W. Ritchey

Securing Networks with Private VLANs and VLAN Access Control Lists
http://www.cisco.com/warp/public/473/90.shtml

Virtual LANs: Construction, Operation, and Utilization
Marina Smith, 1998

CISCO Switching Black Book
Sean Odom and Hanson Nottingham, 2001

Deploying Virtual Private Networks with Microsoft Windows Server 2003
Joseph Davies and Elliot Lewis, 2004

CISCO Certified Design Associate
Osborne Certification Press, 2000

CCNP Self-Study CCNP BCRAN Exam Certification Guide 2nd Edition
Morgan/Dennis, 2004

Securing Cisco Routers: Step-by-Step
Wright/Stewart, 2002

Cisco Security Specialists Guide to PIX Firewalls
Vitaly Osipov, 2002