Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW)
Practical Assignment
Version 4.1

Submitted By:
Matthew J. Sullivan

Abstract

In this paper, I will be introducing the technology of Private VLANs (PVLANs) and VLAN ACLs (VACLs) and discussing how they can add security to the defense in depth model. I will also discuss the security requirements for a small business, GIAC Enterprises, and look in detail at the security devices that make up their infrastructure. Finally, I will go into even greater detail for two of these devices, the router and firewall, and look at the specifics for the security policy of each device.

Table of Contents

Assignment 1 – Future State of Security Technology

Introduction

Security, in today's networked environments, continues to be a key factor at many different levels. While many physical devices play a part in that role, we are always looking for ways to improve this and provide a more secure infrastructure. With this in mind, I will be presenting a relatively new technology, VLAN ACLs (VACLs) and Private VLANs (PVLANs), which can extend the defense in depth model to layer 2 of the OSI model by providing port-based security between adjacent switch ports within a single VLAN.

In a typical DMZ infrastructure, there are several servers connected to a single switch. Through this switch, connectivity is achieved by end users on the Internet along with outbound access from the server to other resources. However, it is very rare that the servers themselves will ever need to communicate with one another. Typically though, the switch will be configured with a single VLAN for the DMZ network. A firewall will control access into the DMZ segment, but it has no control over communication between servers inside of the DMZ. This is where a Private VLAN can provide additional security, by allowing connectivity outbound for each server to its default gateway, yet preventing communication between the individual servers themselves. In this model, if a DMZ server is compromised, access is not allowed to any of the other DMZ devices. In the following sections, this analysis will go into more detail as to how this is achieved and also discuss how it can aid in the defense in depth model.

As Cisco Systems is the primary vendor of choice in the majority of network infrastructures found throughout the world, I will be focusing specifically on their products and implementation methods.

Private VLANs (PVLANs)

A VLAN on a network is a broadcast domain. All of the hosts on that VLAN can communicate with the other members of the same VLAN. PVLANs allow traffic to be segmented at the data-link layer (layer 2) of the OSI model, creating smaller sub networks within each larger VLAN.

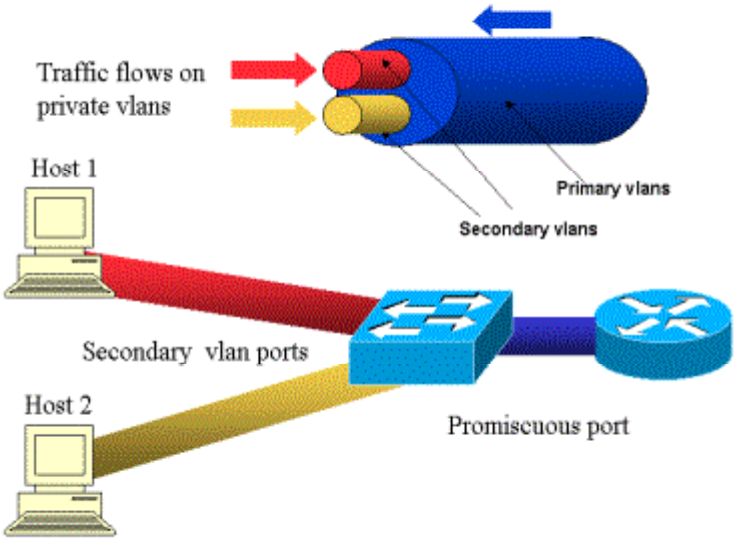
PVLAN ports can be categorized into the following three types [5]:

- Promiscuous: A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN.

- Isolated: An isolated port has complete Layer 2 separation from the other ports within the same PVLAN, but not from the promiscuous ports. PVLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic from the isolated port is forwarded only to promiscuous ports.

- Community: Community ports communicate among themselves and with their promiscuous ports. These interfaces are separated at Layer 2 from all other interfaces in other communities or isolated ports within their PVLAN.

The following diagram shows an example of this [4].



In a PVLAN, promiscuous ports are called the primary VLAN, while community and isolated ports are called secondary VLANs. A PVLAN will only have one primary VLAN, but may have several secondary VLANS.

The above diagram represents the private VLANs as different pipes that connect routers and hosts; the pipe that bundles all the others is the primary VLAN (blue), and the traffic on VLAN blue flows from the routers to the hosts. The pipes internal to the primary VLAN are the secondary VLANs, and the traffic traveling on those pipes is from the hosts towards the router.

The ports where the routers and firewalls are connected are configured as promiscuous so that they can forward traffic to all secondary VLANs. The host devices will be able to reply to these promiscuous ports at a minimum if their port is configured as isolated. In the example, these devices are on separate secondary VLANs and will not be able to communicate with one another.

As of this writing, PVLANs are supported on the following Cisco platforms [4]:

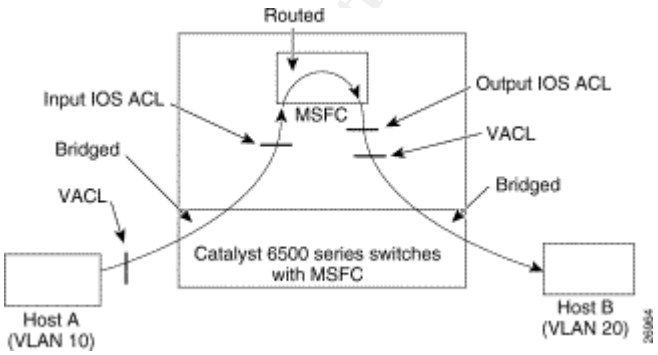
Appendix B.

VLAN ACLs (VACLs)

VLAN access lists work very similar to a normal access list, in that they inspect traffic and can allow or deny packets based on certain criteria. They provide access control for all packets within a VLAN as well as any that are routed into or out of the VLAN. Also, unlike regular ACLs that are configured on a router interface and applied only to routed packets, VLAN access lists apply to all packets.

Another major difference between VACLs and normal access lists is that the VLAN access list is being performed by hardware and therefore has very little impact, if any, on the forwarding rate of the device. A standard access list is software based and can begin to degrade the performance of a router if it is servicing many requests at the same time. As the VACL is working at the data link layer, the screening process is taking place in hardware and will therefore not affect the overall CPU performance of the switch.

VLAN access lists work hand in hand with IOS access lists. Depending on the type of traffic, the comparisons are done to the corresponding list at the appropriate time. The following picture shows the effects of this on routed traffic [2].



For routed/Layer 3-switched packets, the ACLs are applied in the following order:

1. VACL for input VLAN

2. Input IOS ACL

3. Output IOS ACL

4. VACL for output VLAN

VACLs are available on the Catalyst 6000 series running CatOS 5.3 or later. They also require a Policy Feature Card (PFC).

Known Limitations

While we have seen that PVLANs and VACLs can provide additional security features to a network design, there are a few limitations that those using the technology should be aware of. The first is in the handling of the Internet Control Messaging Protocol (ICMP), specifically with fragments. By default, Cisco hardware is programmed to explicitly permit fragments, as it views fragments and echo-replies to be the same. So we must add an entry in our VLAN access list to drop echo replies. To correct this issue, we can add a line in our VACL to explicitly drop any ICMP fragment traffic:

Deny ICMP any any fragment

Another issue to be aware of is that while PVLANs work at the data link layer, they do not provide protection from other layer 3 (network) devices such as routers and firewalls. This is because firewalls and routers are plugged into the promiscuous port of the switch and can route traffic across VLANs. To correct this problem, we need to be sure that we have properly defined our VLAN access lists and explicitly allowed only that traffic that we want to pass though the correct ports.

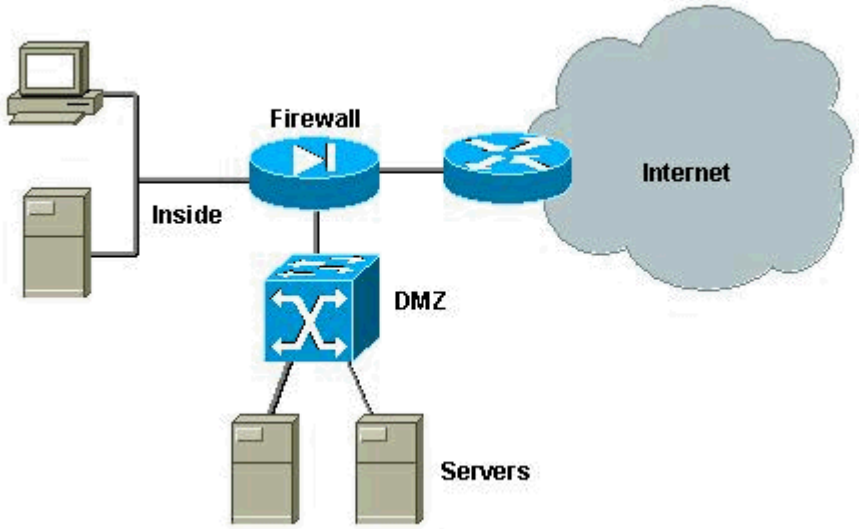
For example, even if two servers belong to two different secondary VLANs or to the same isolated VLAN, there is still a way an attacker can make them communicate to each other. If one of the servers is compromised and then configured by a hacker in such a way that the traffic for the same subnet is sent to the router, the router will direct the traffic back on the same subnet, thus defeating the purpose of the PVLANs. Therefore, we need to configure a VLAN access list on the primary VLAN such that:

- Allow all traffic whose source is the router itself
- Deny traffic with source and destination on the same network
- Allow all other traffic

By doing this, the ACL will allow outbound traffic from the servers as long as it is not destined to any other server on the same VLAN.

DMZ Example

To give a better understanding of how this all comes together, we can use the following picture of a typical DMZ [2].



While no two DMZs are alike, for this example we will assume that the DMZ servers do not need to communicate with one another. Using the defense in depth principles, we can harden the border router ACLs, tighten firewall rules, and place NIDS in the infrastructure. However, in a typical environment, without PVLANs and VACLs, if one of these servers is compromised, an intruder would now be free to start launching attacks against other hosts on the same network space.

To take the defense in depth model one layer deeper, we can place each of the servers off of an isolated switch port inside of the DMZ. We can also create a VLAN access list on the switch to drop ICMP fragments and prevent traffic routing between the same subnet. To take the safety level even further, we can create our VLAN access lists to allow only those ports specifically needed for the application running on the server.

Benefits

While the threat of having a server compromised and used to launch attacks against other devices on the same network space has been around for a long time, there have been very few solutions available to fight it. One idea would be to dedicate a firewall port for each server, but this would be very expensive, not very scalable, and make routing and firewall policies very complex. Also, because most firewalls are software based, the time and CPU load for making these decisions is much higher.

By using this setup, we are mitigating the risk of having a DMZ server compromised and then allowing access from one server to another. This does, however, increase the complexity of our network. It also requires that engineers have experience both configuring these technologies and in troubleshooting communication problems, should they be found.

My recommendation is that, while not widely used in networks today, I believe that we will begin to see an increased use in this technology over the coming years. While defense in depth works to protect systems from being compromised, this technology can increase that safety level by insuring that even if a system is compromised, the infected system is limited into what it can do and is isolated from the rest of the network.

Assignment 2 – Security Architecture

Introduction

GIAC Enterprises is a small business which markets fortune cookie sayings to customers worldwide. GIAC employs fifty people with the majority in or near its head office and the remainder located in or near the four regional satellite offices geographically distributed around the world. All of GIAC enterprises sales are done via the Internet.

Access Requirements and Restrictions

Customers

This user group will be making purchases of fortunes through the Web architecture setup in the GIAC DMZ. To allow customers access to this, they will be granted http access for viewing web pages along with https for secure transactions and payments. We will also allow this group to query DNS records and send email to GIAC enterprise employees. Should additional access be required by a customer, it will be handled on a case by case basis, at the discretion of Information Security management.

Source	Destination	Port(s) / Protocol	Description
Customers	Web Server	TCP/80 (HTTP) TCP/443 (HTTPS)	Customer access to web server
Customers	SMTP Relay	TCP/25 (SMTP)	Allow customers to send email
Customers	DNS Server	UDP/53 (DNS)	Allow customer access to DNS records

Suppliers

This group of users will be supplying GIAC enterprises with fortune cookie sayings. To facilitate the transfer of sayings in a secure manner, we will allow outside suppliers SFTP access to a secure server in the GIAC DMZ. Username and passwords will be supplied as needed and re-approved every 90 days. There will be strict requirements for passwords and every 90 days the password will need to be changed.

Source	Destination	Port(s) / Protocol	Description
Suppliers	SSH Server	TCP/22 (SSH)	Supplier access to SSH server
Suppliers	SMTP Relay	TCP/25 (SMTP)	Allow suppliers to send email
Suppliers	DNS Server	UDP/53 (DNS)	Allow supplier access to DNS records

Partners

This group will consist of external companies that translate and resell fortunes throughout the world. Each of these connections will be allowed secure access over https to a web server in the GIAC DMZ. Each partner will have a unique login name with password, which follows the username and password standard defined by GIAC Enterprises. After logging in to the website, the partners will be allowed to access the fortunes database to download fortunes which they have access to. We will also allow this group to query DNS records and send email to GIAC enterprise employees.

Source	Destination	Port(s) / Protocol	Description
Partners	Web Server	TCP/80 (HTTP) TCP/443 (HTTPS)	Partner access to web server
Partners	SMTP Relay	TCP/25 (SMTP)	Allow Partners to send email
Partners	DNS Server	UDP/53 (DNS)	Allow Partner access to DNS records

GIAC Internal Employees

Internal employees of GIAC, located at either the headquarters or satellite offices will be given basic access to perform their daily job functions. This will

include http, https, and ftp access through the firewall to the Internet. Other users, based on job function will be given additional access as needed. For instance, SSH will be opened up from internal networks into the GIAC DMZ for server administrators and support personnel. This will allow for remote administration and configuration changes as needed. If additional access is required by individuals or business groups, it will be handled on a case by case basis, at the discretion of Information Security management.

All satellite offices will have site-to-site VPN connections which feed through the main office. This way we will provide secure, encrypted connections between offices and then manage all firewall rules on a single gateway cluster.

Source	Destination	Port(s) / Protocol	Description
Internal Employees	Internet	TCP/80 (HTTP) TCP/443 (HTTPS) TCP/21 (FTP)	Employee access to Internet resources
Internal Employees	Internal Mail server	TCP/25 (SMTP)	Allow employees to send and receive email
Internal Employees	Internal DNS Server	UDP/53 (DNS)	Allow employees access to DNS records
Internal Employees	SSH Server	TCP/22 (SSH)	Allow employees access to administer and update secure server

GIAC Remote Users

To support the needs of remote users, GIAC Enterprises will provide a Checkpoint NG VPN client to users on an as needed basis. This will allow connectivity from outside connections over the Internet. To support these connections, we will need to open up ports for IKE negotiation and also to allow topology requests from remote users.

By using Checkpoint's NG VPN client we will also be installing a personal firewall on each remote computer. This will provide additional safety for remote users as they will have access to needed resources but will also provide a layer of security on the remote desktop.

Source	Destination	Port(s) / Protocol	Description
Any	VPN Gateway	UDP 500 / IKE	Key negotiation
Any	VPN Gateway	TCP 500 / IKE	Key Negotiation
Any	VPN Gateway	TCP 264	Topology requests

Any	VPN Gateway	TCP 18231	Policy Server logon
Any	VPN Gateway	UDP 18234	Tunnel Test

General Public

This group will consist of all other users who access the GIAC website. We will allow connections over http to the main web server. We will also allow this group to query DNS records and send email to GIAC enterprise employees.

Source	Destination	Port(s) / Protocol	Description
General Public	Web Server	TCP/80 (HTTP) TCP/443 (HTTPS)	General access to web server
General Public	SMTP Relay	TCP/25 (SMTP)	Allow public to send email
General Public	DNS Server	UDP/53 (DNS)	Allow public access to DNS records

Security Components and Defense in Depth

I*P Addressing Scheme*

While the overall security of a network is incorporated into a number of different physical devices, in addition the IP addressing scheme used plays a very crucial role. GIAC Enterprises has taken this into consideration when designing the layout of their network. As such, all internal networks will use non-routable, RFC 1918 compliant, 10.X.X.X network segments.

Specifically, GIAC Enterprises has broken up this Class A network space to be used for different functions across the business. All remote offices will be given a Class C network in the 10.1.X.X IP address range. By using a class C network, 254 hosts, it will provide enough addresses for current needs while accommodating any future expansion at these sites.

For the corporate network, we will use addresses in the 10.2.X.X IP address range. DHCP clients will be given addresses in the 10.2.1.0 /23 network range. We will also use 10.2.90.X /23 for a server network. By separating these networks we will ease the routing functionality, improve network performance, and provide an additional layer of security by keeping users and servers on different networks.

By using non-routable addresses internally, we will need to provide NAT, Network Address Translation, on our outbound gateway. By doing this, we have secured our perimeter in a number of ways:

(1) Traffic leaving the network will always be translated behind the IP address of our Internet Gateway. To an outside company, all network requests will appear to be coming from the same IP address. This will conceal the true IP addressing scheme and makeup of the internal networks.

(2) As we are using non-routable and RFC 1918 compliant addresses, no one outside of the company will be able to make direct connections to any inside resources.

An additional network that GIAC will also use is the 172.16.1.X/24 network space. This will be used for the NIDS deployment. This network will be completely isolated from the rest of the company and will only include the NIDS sensors and syslog server for collecting data.

Border Router

This device will separate GIAC Enterprises from the Internet, and is the first piece in the layered architecture we will incorporate into our security design. While a router's primary function is to direct packets, it also aids in defense in depth by blocking traffic destined to and from certain network address ranges. The specifics of the policy will be discussed in detail in Section 3. I will briefly touch on some of these as they relate to defense in depth.

To incorporate security onto our border router, we will use ACL's (Access Control Lists) to provide ingress (incoming) and egress (outgoing) traffic filters. There are pros and cons to this approach that need to be looked at. A definite benefit is that we can block incoming and outgoing traffic from a number of source addresses that should not be communicating on the Internet. For example, we would never receive a request from a 10.X.X.X network address. If we did it is more than likely spoofed and possibly a DoS attempt. As such we will put in filters to drop all traffic to and from 10.0.0.0/8, 172.16.0.0/16 and 192.168.0.0/16.

To prevent any spoofing of the GIAC Enterprise network space, there will be an ingress filter to drop any traffic from the 68.219.25.0/24 network range. In the same regards, there will be an egress filter to only allow outbound traffic from the 68.219.25.0/24 network range. This will prevent any mis-configurations or leaking of IP addresses to the Internet.

Another access list, which will be created and applied to both inbound and outbound interfaces, deals with critical services that should not be leaving

or entering the network. While outbound traffic should be dropped by the firewall, this will compliment that policy and prevent any unwanted traffic from reaching the Internet. Included in this access list will be commonly used Windows ports, TCP and UDP 135 – 139 and 445. Also included in this list will be UDP 69 (tftp), UDP 161 (snmp), UDP 162 (snmp-trap), and UDP 514 (syslog). Along with this, we will filter out all source routing packets and a number of specific ICMP types and codes.

As for the router itself, we will use a Cisco 2801 running the latest version of IOS code, 12.3(10). We will be using a single T1 line which will terminate on the router. This will serve as a potential single point of failure but we will work with the service provider to get an SLA put in place to make sure that the uptime achieved is in the 99% category. We also feel that the additional complexity of adding a second link with redundancy is more than is currently needed.

To prevent any unwanted access to the router itself, an access list will be defined that only allows connections from a small subnet of the internal network. To monitor the device we will use SNMP but again by defining the specific source in an access list and only after changing the SNMP "public" password. Finally, to incorporate additional safety, we will not use any routing protocols. Because we only have one routable network address range, our routing entries will be quite small on this device and easy to maintain.

Firewall

While the border router begins the process of dropping unwanted traffic, the primary security device for doing this function is the firewall. On this device, we will setup rules to allow only that traffic that we deem as necessary and safe, with a cleanup rule at the bottom of the rule set to drop all other traffic. While the specifics of the rules will de discussed later in this paper, I will briefly touch on those that relate to defense in depth.

GIAC Enterprises has chosen to use Checkpoint SecurePlatform NG R55 with the latest hotfix which is currently HFA-12. By going with a Checkpoint installation we are using an industry standard and also leveraging the knowledge of the current staff. While a more expensive solution than other options available, we feel that the ease of management and the ability to run the operating system on a well known, less expensive piece of hardware will make up for this cost difference.

GIAC Enterprises will use the Compaq DL320 G4 model for its hardware architecture. By doing so, we are able to use hardware that supports both fiber and copper connections, which allows us to meet business needs and expand as needed. These devices also come with built-in RAID controllers which will prevent outages for hard drive problems.

As GIAC Enterprises relies heavily on its web presence for sales, we have chosen to implement a high availability pair of gateways to limit the amount of downtime in case of hardware failure. While this adds increased cost, we feel it is a necessity for the business environment. To add increased security, we will setup this environment in what Checkpoint refers to as a "distributed" environment. This means that we will also have a separate management station on the internal server network that maintains policies and logs for the gateways.

The firewalls physically will be placed between the border router and the internal network, with a separate interface for the DMZ network. By using this design, we are adhering to defense in depth and gain a few key benefits:

(1) We can inspect all traffic entering our network from the Internet and allow/deny as we see fit.

(2) We can limit all traffic leaving GIAC Enterprises accordingly with our stance of deny all; we can make sure that only valid traffic is allowed out.

(3) If our border should be compromised or allow unwanted traffic in from the Internet, the firewall will also inspect the traffic and allow or deny it based on the current policy

Again, as an additional safety measure, the firewall will not run a routing protocol but will contain static routes for the required networks. Due to the relatively small size of the network and segregated layout, the maintenance of the routing tables will be fairly easy to maintain.

VPN

GIAC Enterprises has chosen to implement two different types of VPN technology in their layered architecture. We will use site-to-site VPN tunnels, terminating on the firewall gateway for remote sales offices. This will provide for a central rule base for managing traffic while also ensuring that all traffic is encrypted between the headquarters and remote offices. At the remote offices their will be a Cisco 2811, which includes an onboard VPN encryption card to offset the CPU requirements needed for this type of traffic. This model will be running the latest IOS code, 12.3(10), and while more than adequate to handle the needs of the remote offices, it is fairly inexpensive.

We will also employ Checkpoint remote user VPN for home users, which will also terminate on the firewall gateway. Due to the relative small size of the company and workforce, the decision was made to use the existing gateway, instead of purchasing additional hardware and software. This will add some additional complexity to the firewall rule base and increased CPU utilization for

the firewall, but by purchasing the correct hardware upfront, we can prevent this from becoming an issue.

As discussed earlier, by using the Checkpoint remote user VPN solution, we get the added benefit of a personal firewall on each remote desktop. We can also control the policy through the firewall management interface and make changes that are propagated during the login process. Another benefit to this solution is what Checkpoint refers to as “Office mode”. Each user, after authentication to the gateway, is given a virtual IP address from a pool of addresses defined on the gateway. This corrects problems seen from users at home or in hotels, when trying to connect from behind a NAT device that uses the same network address space as found inside of GIAC Enterprises. For authentication of remote users, GIAC will assign a username and password, which meets the requirements of the password standards and follows the same guidelines as all other passwords. While we would ideally like to have 2-factor authentication, the additional cost and administration does not seem justified.

IDS

Once traffic has passed through the router and firewall, we are relatively sure it has come from a valid host and is destined to an allowed network address. However, we have not inspected the traffic to verify what it is doing and make sure that it is not malicious. This is where our Network Intrusion Detection Systems (NIDS) will play a vital role in our security architecture as they form the third layer in our defense in depth model. These devices will use known patterns to try and identify potential attacks against systems and when found, will either reset the connection and/or trigger an alert.

GIAC Enterprises has chosen to use SNORT v2.3 for its NIDS deployment. We will also use Intrusion SecureNet IDS taps which will be placed inline between the firewall gateway and the DMZ network. We have chosen this location to protect the servers on this network from malicious attacks and also to look for any unusual traffic, either inbound or outbound. Another set will be placed between the firewall gateway and the internal network. This will monitor the traffic directly to and from GIAC employees and alert for any anomalies or suspicious events.

One of the reasons for choosing SNORT is that it is widely used and has a large support base. We can also leverage the existing knowledge of our current support staff. The product itself is also freeware, which makes it very cost effective to the company.

For the hardware platform of the NIDS sensor, we will again use Compaq DL 320 G4 models. These will be running Fedora Core 3 along with the latest patches. These sensors will be placed on a private IP address network

172.16.1.X/24 which will tie into a central syslog server for collecting log data.

Vulnerability Assessment

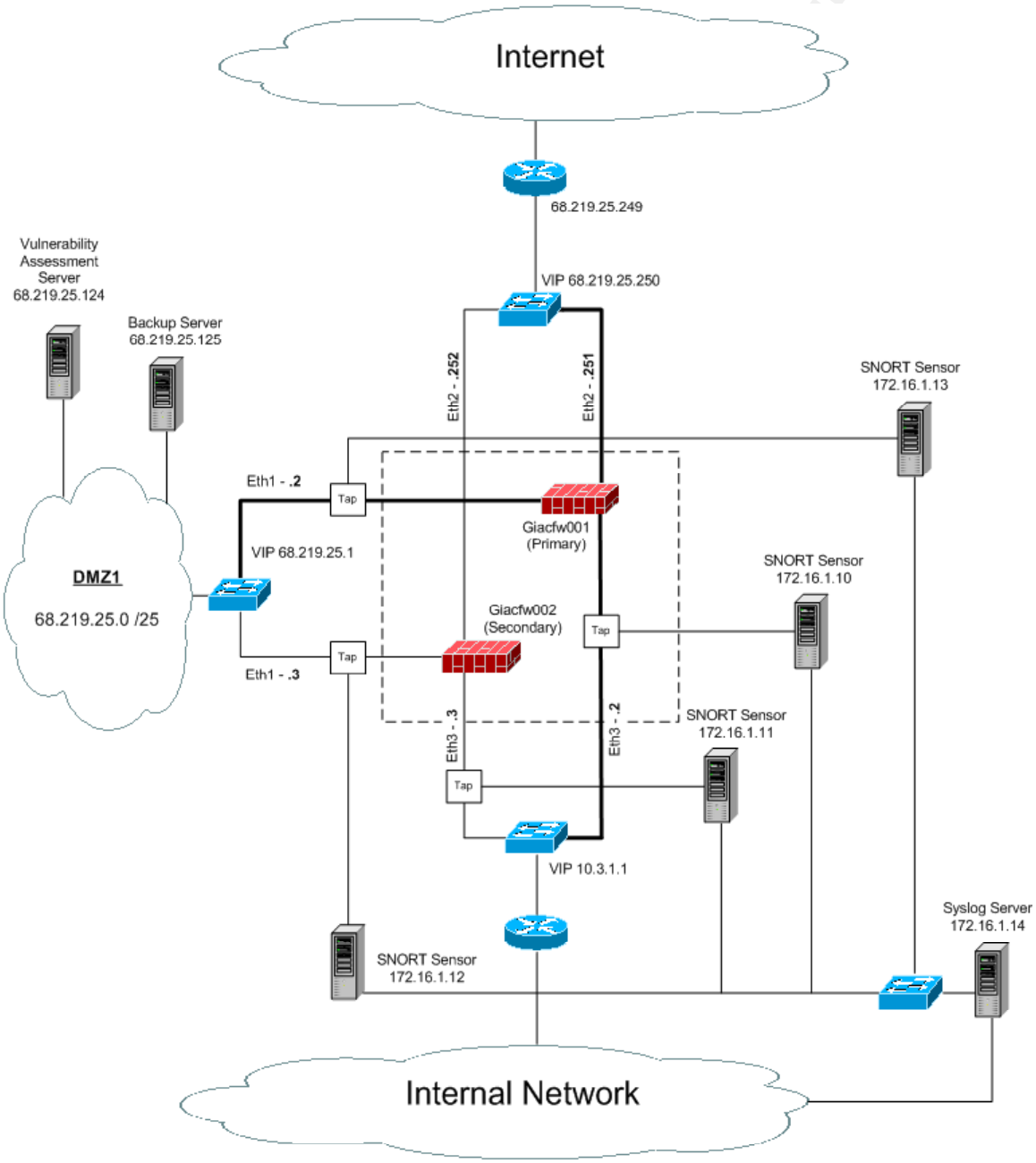
By placing servers on the DMZ network and creating firewall rules to allow traffic to these devices, we are making ourselves susceptible to an attack. Even with the devices in our security architecture that we have previously reviewed to protect our DMZ systems, we could still become victim to a virus attack or have a server compromised. Also, with the influx of new patches being released by software vendors and the increased number of attacks that exploit these vulnerabilities, it is imperative that our DMZ systems are patched in a timely manner.

As such, GIAC Enterprises will deploy a Linux system, running Fedora Core 3, along with the latest version of Nessus, 2.2.3 to perform weekly vulnerability scans of the entire DMZ network. These systems will then be patched accordingly. GIAC Information Security will also maintain a standard secure OS build to be deployed to systems which need to be placed into the DMZ network. These practices will also be used on internal application servers to prevent vulnerabilities from being found and exploited.

Disaster Recovery

While everything we have discussed so far deals with protecting systems, the final piece of our defense in depth model is in place to provide recovery from any potential loss of data. As GIAC relies heavily on its server infrastructure for everyday business functionality, we cannot accept the risk of potential downtime due to the loss of data or system failure. Therefore, incremental backups will be performed on all servers during the week, with full backups taking place over the weekends. For recovery purposes in the case of a large disaster, a copy of all the weekly full backups will be stored off site for a one year timeframe. GIAC Enterprises has chosen to use Legato as its software of choice for backups and recovery. While a more expensive solution, we feel the cost is justified by the superiority of the product and the experience level of the staff.

Network Diagram



Assignment 3 – Router and Firewall Policies

General Security Stance

GIAC Enterprises has taken many factors into account when designing the policies of the filtering router and firewall gateway. We will base our policies around a general stance of denying all traffic and allowing only that which is needed. We also have specifically ordered the rules, to optimize the performance and utilization of these devices.

In addition, we have taken into account the fact that traffic must pass through both the router and firewall when either entering or leaving the network. The policies therefore complement one another and can correct any issues where unwanted protocols or ports are making it through one of these devices. As both devices are being monitored, we will keep watch of traffic patterns and make changes accordingly. We will also audit and review the policies on both devices in accordance with the security standards for the company, which will occur every 90 days.

Border Router Configuration

Ingress ACL

Action	Protocol	Source	Destination	Port	Description
Deny	IP	10.0.0.0/8	Any	Any	RFC 1918 Private Network
Deny	IP	192.168.0.0/16	Any	Any	RFC 1918 Private Network
Deny	IP	172.16.0.0/12	Any	Any	RFC 1918 Private Network
Deny	IP	68.219.25.0/24	Any	Any	GIAC DMZ Network
Deny	IP	127.0.0.0/8	Any	Any	Loopback Network
Deny	IP	0.0.0.0/8	Any	Any	Historic Broadcast
Deny	IP	169.254.0.0/16	Any	Any	Link Local Networks
Deny	IP	224.0.0.0/4	Any	Any	Class D Multicast
Deny	IP	240.0.0.0/5	Any	Any	Class E Reserved
Deny	IP	248.0.0.0/5	Any	Any	Unallocated
Deny	IP	255.255.255.255/32	Any	Any	Broadcast
Deny	IP	Any	68.219.25.149	Any	Drop all traffic destined to the router
Deny	TCP	Any	Any	135-139, 445	Microsoft Ports
Deny	UDP	Any	Any	135-139, 445	Microsoft Ports
Deny	TCP	Any	Any	23, 111, 512 -514, 2049, 6000-6063	Unix Ports
Deny	UDP	Any	Any	111, 2049, 6000-6063	Unix Ports
Deny	UDP	Any	Any	69, 161, 162, 514	SNMP, syslog, and TFTP
Permit	IP	Any	68.219.25.0/25	Any	Allow access to GIAC DMZ

Permit	IP	Any	68.219.25.250/32	Any	Allow access to NAT address of GIAC DMZ firewalls
Deny	IP	Any	Any	Any	Drop all other traffic

The first rule in our ingress filter is to drop any traffic with a private source address as defined by RFC 1918. Packets crossing the Internet should not be using these addresses so it is either a mis-configured system or a spoofed IP address. Either way, we can simply drop this traffic at the border router as we know it is not valid. Along with private IP addresses, we are also filtering out other invalid networks that would never make a legitimate request. We are also dropping any attempts to access the router directly from the Internet.

The next few lines of our ACL deal with traffic over well-known TCP and UDP ports that will never be used for legitimate requests from the Internet and will be denied as well. These include Windows specific ports such as Netbios and Microsoft directory services, along with TFTP, SNMP and Syslog.

The rules have been ordered is a specific way such that all invalid source addresses will first be eliminated. Secondly, we will look for well known TCP and UDP ports that should not be entering the network and eliminate all these requests. Finally, if the request is from a valid source address over a valid port, we will validate that it is destined to the GIAC DMZ and allow it through. Any other requests will match the final rule and be dropped.

Egress ACL

Action	Protocol	Source	Destination	Port	Description
Deny	IP	10.0.0.0/8	Any	Any	RFC 1918 Private Network
Deny	IP	192.168.0.0/16	Any	Any	RFC 1918 Private Network
Deny	IP	172.16.0.0/12	Any	Any	RFC 1918 Private Network
Deny	IP	68.219.25.0/24	Any	Any	GIAC DMZ Network
Deny	IP	127.0.0.0/8	Any	Any	Loopback Network
Deny	IP	0.0.0.0/8	Any	Any	Historic Broadcast
Deny	IP	169.254.0.0/16	Any	Any	Link Local Networks
Deny	IP	224.0.0.0/4	Any	Any	Class D Multicast
Deny	IP	240.0.0.0/5	Any	Any	Class E Reserved
Deny	IP	248.0.0.0/5	Any	Any	Unallocated
Deny	IP	255.255.255.255/32	Any	Any	Broadcast
Allow	UDP	68.219.25.250	68.219.25.249	161, 162	SNMP Monitoring of Router
Allow	ICMP	68.219.25.250	68.219.25.249	Any	ICMP Monitoring of Router
Allow	IP	68.219.25.250	68.219.25.249	23	Administration of Router
Deny	IP	Any	68.219.25.149	Any	Drop all traffic destined to the router
Deny	TCP	Any	Any	135-139, 445	Microsoft Ports
Deny	UDP	Any	Any	135-139, 445	Microsoft Ports
Deny	TCP	Any	Any	23, 111, 512 -514, 2049, 6000-6063	Unix Ports
Deny	UDP	Any	Any	111, 2049, 6000-6063	Unix Ports
Deny	UDP	Any	Any	69, 161, 162, 514	SNMP, syslog, and TFTP
Permit	IP	68.219.25.0/25	Any	Any	Allow access out of GIAC DMZ

Permit	IP	68.219.25.250	Any	Any	Allow access outbound for NAT address of firewalls
Deny	IP	Any	Any	Any	Drop all other traffic

To prevent the leaking of internal networks, the first rule in our egress filter will be to drop all traffic from RFC 1918 private networks. We will also prevent any requests from other invalid networks from reaching the Internet. Next, working in conjunction with the firewall gateway, we will allow for remote administration and monitoring of the router from the internal network. Any other attempts to access the router directly will be dropped. We will also drop all traffic using well known TCP and UDP ports again. By adding these rules to the router, we can assure that we have two layers protecting our network boundary to prevent these services from ever reaching the Internet. Lastly, we will confirm that the request is from a valid GIAC network space and allow this traffic outbound. Any other traffic will then be dropped.

The firewall gateway should prevent most of this traffic from ever reaching the router. However, by using this design method, we will be assuring ourselves that a firewall mis-configuration has not taken place and if it does, no vital information will be leaked.

The ordering of these rules is again very important. We first want to eliminate any invalid network requests from reaching the Internet. Then we want to allow only a select IP address access to the router and drop any other attempts. Next, we will filter out any unwanted TCP and UDP ports. Finally, if it passes all these tests, and is from a valid GIAC address space, we will allow it outbound. By changing the ordering of the rules, we could allow many unwanted requests out to the Internet.

In addition to the access lists, GIAC will also be turning off IP source routing and the Cisco discovery protocol.

Firewall Configuration

General Rules

Action	Protocol	Source	Destination	Port	Description
Allow	TCP	Security Network	GIAC Firewalls	22, 443	Allow Security administrators access to firewall gateways
Allow	ICMP	Security Network	GIAC Firewalls	Any	Allow Security administrators to ping and traceroute to firewall gateways
Allow	TCP	Firewall Management Server	GIAC Firewalls	256, 258, 18191, 18192, 18208, 18210	Allow for management of firewall devices
Allow	TCP	GIAC Firewalls	Firewall Management Server	257, 18191, 18210, 18264	Allow firewalls to send logs to management server
Allow	UDP	10.2.90.90	GIAC Firewalls	161, 162	Allow remote monitoring of firewalls over SNMP

Allow	ICMP	10.2.90.90	GIAC Firewalls	Any	Allow ICMP monitoring of firewalls
Deny	IP	Any	GIAC Firewalls	Any	Drop all traffic destined to the firewalls themselves

The first step in configuring the firewall rule set is to turn off all implied rules (See Appendix A). This will prevent any unwanted access being gained through the firewall and will allow GIAC to achieve its goal of only allowing traffic that is needed to pass through the device.

As for the rules, we will begin by explicitly defining a select set of IP addresses which can access the firewall gateways over SSH and HTTPS for remote administration and troubleshooting. On the internal network of GIAC Enterprises, we will reserve a small set of IP addresses to be used by the router and firewall administrators for this purpose. We will also allow them ICMP and traceroute for basic connectivity testing.

As I stated earlier, there will be a firewall management server that will be used for logging and administration of the firewall policies. The next two rules will allow the communication to take place over the appropriate ports both to and from the firewalls. Next, we have added two rules for monitoring of the firewalls directly. There will be a single source on the internal network with access over SNMP and ICMP to confirm that the firewalls are operational and to gather statistics about traffic flow. Finally, we have added a rule to drop any other traffic destined for the firewalls themselves.

Looking at this policy, its order is very important. We have explicitly defined a few sources which can access the firewalls directly and then we have denied all other requests. Rule # 7 must be last in the sequence or else requests to the devices will be denied.

Inbound Rules

Allow	TCP/UDP	Any	68.219.25.8	53	Internet access to external DNS server
Allow	TCP	Any	68.219.25.9	80, 443	Internet access to http(s) server
Allow	TCP	Any	68.219.25.10	22	Internet access to SSH server
Allow	TCP	Any	68.219.25.11	25	Internet access to external SMTP server
Allow	TCP	Any	68.219.25.250	500, 264, 18231, 18234	VPN access for remote users
Allow	UDP	Satellite Office Net Headquarters Net	Satellite Office Net Headquarters Net	500	Site to Site VPN connections
Allow	TCP	68.219.25.11	10.2.90.91	25	Allow external mail relay to talk to internal mail server
Allow	TCP/UDP	68.219.25.8	10.2.90.92	53	Allow external DNS server to communicate with internal DNS server
Allow	TCP	GIAC Firewalls	Any	21	Allow for updating of code on firewalls

Allow	TCP	GIAC Firewalls	Any	Any	Allow connectivity test from firewall gateways
Deny	TCP	Any	Any	113, 139	Drop specific ports and do not log them
Deny	UDP	Any	Any	67, 137, 138	Drop specific ports and do not log them
Deny	IP	Any	Any	Any	Drop all other traffic

Our inbound rules give protection to those systems in the GIAC DMZ and also provide connectivity for remote offices and users. In building our rule set, we are using the GIAC security stance to only allow traffic as needed. Therefore, we have only opened up specific ports to specific destinations.

In our first rule, we allow users on the Internet access to GIAC's external DNS server. In the following rules, we have opened the corresponding service on the appropriate server. We have also setup a rule to allow encrypted communication to take place between each remote office and the firewall gateway. Finally, we have allowed the external SMTP and DNS servers to communicate with their corresponding internal servers.

The ordering of these rules is less important than the previous set of rules. The final rule of the firewall policy is a "deny all" to any remaining traffic and must be placed last in the group. Because the rules are matched sequentially from top to bottom, we would want to monitor traffic and place the most frequently used rules higher in the rule set. In this rule set, we have explicitly allowed only specific traffic and all other patterns will be dropped. This is in contrast to the border router where we eliminated unwanted traffic and allowed what was valid. Here we are taking the opposite approach.

Outbound Rules

Allow	UDP	10.2.90.90	68.219.25.249	161, 162	SNMP Monitoring of Router
Allow	ICMP	10.2.90.90	68.219.25.249	Any	ICMP Monitoring of Router
Allow	TCP	GIAC Internal Networks	Any	80, 443, 21	Allow internal users outbound access over ftp and http(s)
Allow	TCP	GIAC Internal Networks	68.219.25.0/25	22	SSH access into GIAC DMZ for admin of servers
Allow	TCP	10.2.90.91	Any	25	Allow internal mail server to send outbound SMTP
Deny	TCP/UDP	10.2.90.92	Any	53	Allow internal DNS server to make external DNS requests
Allow	TCP	GIAC Firewalls	Any	21	Allow for updating of code on firewalls
Allow	TCP	GIAC Firewalls	Any	Any	Allow connectivity test from firewall gateways
Deny	TCP	Any	Any	113, 139	Drop specific ports and do not log them
Deny	UDP	Any	Any	67, 137, 138	Drop specific ports and do not log them
Deny	IP	Any	Any	Any	Drop all other traffic

The final piece of our rule set permits systems internal to GIAC Enterprises access to the GIAC DMZ and also the Internet. Our first rule allows for the monitoring of the border router by an internal server. This corresponds

with the ACL in place on the router itself. Next, we have a rule in place to allow employees outbound access over HTTP(S) and FTP to the Internet. Third, we have given internal employees SSH access to the GIAC DMZ for remote administration. To provide additional security, we have added the next rules so that only the internal SMTP and DNS servers are allowed to talk outbound over their respective ports. We have also added rules to allow connectivity directly from the firewalls. This includes ICMP and traceroute, along with FTP for doing code updates. Finally, the last rules deal with dropping traffic. To prevent un-necessarily large log files, we will first drop and not log traffic over specific well-known ports. We will then drop all other requests and log them.

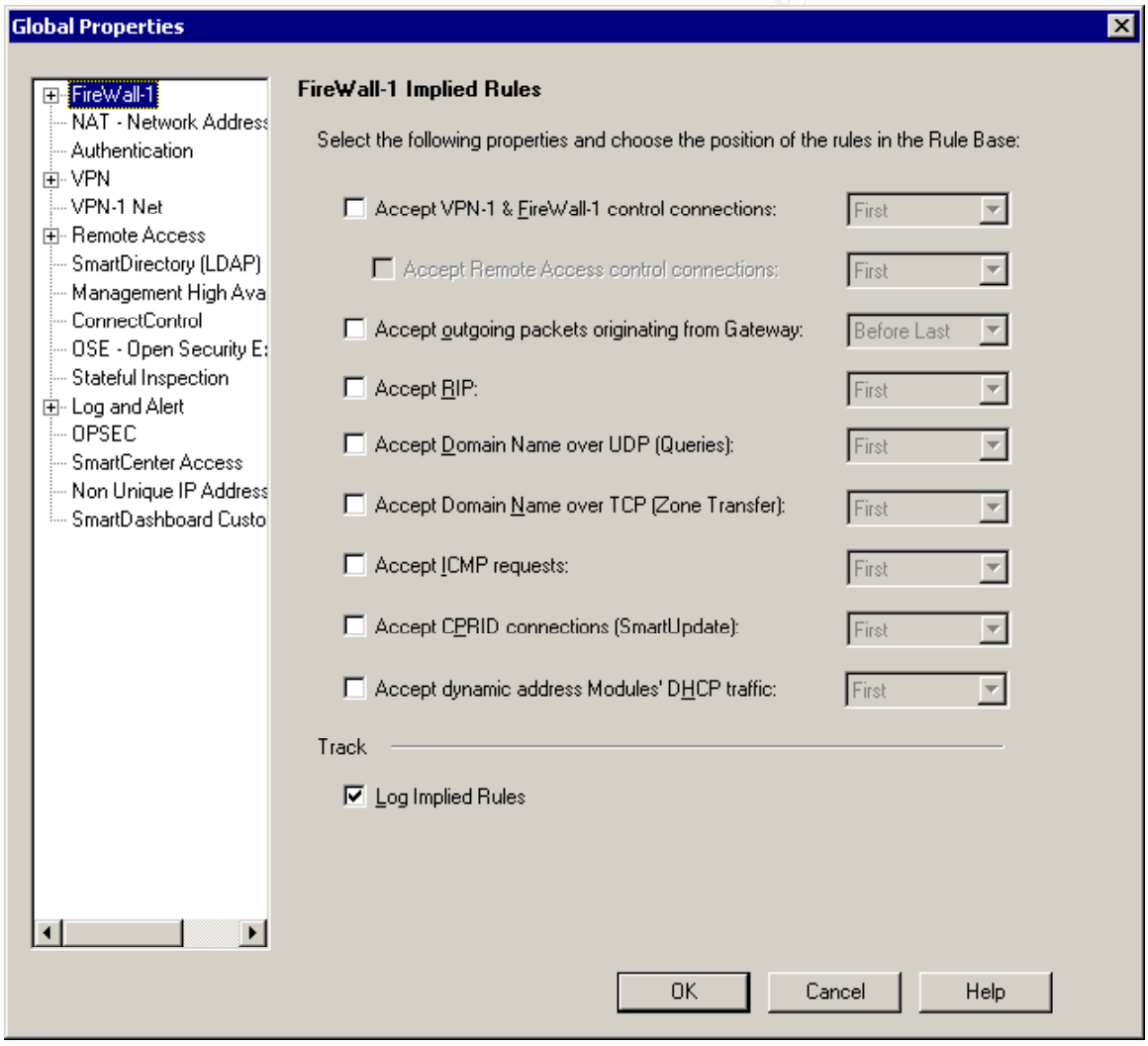
NAT Rules

Original Packet		Translated Packet	
Source	Destination	Source	Destination
68.219.25.0/24	Any	= Original	= Original
GIAC Internal Networks	Any	68.219.25.250	= Original

In this policy, we will only NAT those connections initiated from the internal GIAC network. These we will perform hide NAT on using the IP address of 68.219.25.250. All connections initiating from the GIAC DMZ network will not have NAT translations as they are Internet routable.

Appendix

A.



B.

Catalyst Platform	Software Version	Isolated VLAN	PVLAN Edge (Protected Port)	Community VLAN
Catalyst 6500/6000 - CatOS on Supervisor and Cisco IOS® on MSFC	5.4(1) on Supervisor and 12.0(7)XE1 on MSFC	Yes	N/A	Yes
Catalyst 6500/6000 - Cisco IOS® System software	12.1(8a)EX, 12.1(11b)E1	Yes	N/A	Yes
Catalyst 5500/5000	Not Supported	-	-	-
Catalyst 4500/4000 - CatOS	6.2(1)	Yes	N/A	Yes
Catalyst 4500/4000 - Cisco IOS	12.1(8a)EW	Yes	N/A	12.2(20)EW
Catalyst 3550	12.1(4)EA1	No	Yes	Not Currently Supported
Catalyst 2950	12.0(5.2)WC1, 12.1(4)EA1	No	Yes	Not Currently Supported
Catalyst 2900XL/3500XL	12.0(5)XU (on 8MB switches only)	No	Yes	No
Catalyst 2948G-L3 / 4908G-L3	Not Supported	-	-	-
Catalyst 1900	Not Supported	-	-	-
Catalyst 8500	Not Supported	-	-	-

Catalyst 3560	12.2(20)SE - EMI	Yes	12.1(19)EA1	Yes
Catalyst 3750	12.2(20)SE - EMI	Yes	12.1(11)AX	Yes
Catalyst 3750 Metro	12.1(14)AX	No	Yes	No
Catalyst 2940	12.1(13)AY	No	Yes	No
Catalyst 2948G/2980G	6.2	Yes	N/A	Yes
Catalyst 2955	12.1(6)EA2	No	Yes	No
Catalyst 2970	12.1(11)AX	No	Yes	No

Bibliography

1. Cisco Systems "Understanding and Configuring Private VLANs"
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_18a/config/pvlans.htm

2. Cisco Systems "Catalyst 6500 Series MSFC (12.x) & PFC Configuration Guide"
http://www.cisco.com/en/US/products/hw/switches/ps700/products_command_reference_chapter09186a008007f2ae.html#17907

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

4. Cisco Systems "Private VLAN Catalyst Switch Support Matrix"
http://www.cisco.com/warp/public/473/63.html

5. Cisco Systems "Private VLANs (PVLANs)
http://www.cisco.com/en/US/tech/tk389/tk814/tk840/tech_protocol_home.html

6. SANS Institute "Track 2 – Firewalls, Perimeter Protection and Virtual Private Networks (2.4 Defense-In-Depth)" The SANS Institute, 2004

7. SANS Institute "Track 2 – Firewalls, Perimeter Protection and Virtual Private Networks (2.6 Network Design and Assessment)" The SANS Institute, 2004

8. SANS Institute "Track 2 – Firewalls, Perimeter Protection and Virtual Private Networks (2.2 Packet Filters)" The SANS Institute, 2004

9. SANS Institute "Track 2 – Firewalls, Perimeter Protection and Virtual Private Networks (2.3 Firewalls)" The SANS Institute, 2004

10. Network Working Group "RFC 1918 - Address Allocation for Private Internets" http://www.faqs.org/rfcs/rfc1918.html