Global Information Assurance Certification Paper

SANS GIAC Certified Firewall Analyst (GCFW)
SANS Self Study
March, 2005
GCFW Practical Assignment Version 4.1

Jeff Holland
GCFW, GCIA, GCUX, GCIH, GSEC, CISSP

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Abstract:

The following paper contains three sections that address the requirements for Version 4.1 of the GCFW practical.

Section 1 is a whitepaper based upon the topic GCFW practical wish list topic: "*VLAN ACLs (VACLs) and Private VLANs (PVLANs) and their use in network defense*" as base. Additional discussion and information on VMPS and its use in a small network infrastructure without a Cisco switch that supports the VMPS server function is also included.

Section 2 is a security architecture design and discussion for a small fortune cookie startup company.

Section 3 contains the router and firewall policies for the previous security architecture described in section 2.

Assignment 1: Private VLANs, VLAN ACLs, VMPS and Their Use In Network Defense

Introduction

The following whitepaper is based upon the topic "*VLAN ACLs (VACLs) and Private VLANs (PVLANs) and their use in network defense*" as defined at http://www.giac.org/GCFW_wishlist.php. The intention of this whitepaper is three-fold:

- To discuss what private VLANs and VLAN ACLs are and their use in the role of network defense. A short discussion about their drawbacks will also be presented.

- To briefly discuss the most popular VLAN dynamic port assignment implementation, Cisco's VMPS. Also discussed will be how VMPS, private ACLs and VLAN ACLs can be combined to provide defense-in-depth in network defense.

- To offer a design of the private VLAN/VMPS solution from the standpoint of a remote office that does not have a large Cisco router to act as a VMPS server (such as a Cisco Catalyst 4000 or 6500 switch [1]). Rather, the design will employ the OpenVMPS server solution available at: http://sourceforge.net/projects/vmps and a Cisco Catalyst 2950 XL switch as a VMPS client.

In short, private VLANs allow the segregation of traffic at data-link layer (layer 2) of the OSI model and turn a broadcast segment (also known as a VLAN) into non-broadcast multi-access like segment which helps enforce a trust model for traffic on the same network segment [14]. What this means is that servers in the same VLAN, such as the DMZ, are typically allowed to communicate with each other via ARP and the physical switch they are connected to. By implementing private VLANs, this communication between servers in the same broadcast domain may be controlled more granularly in the switch to enforce access control within the VLAN itself.

VLAN ACLs are ACLs that are configured on a switch in hardware and has no performance effect upon the CPU. They are useful in that when combined with private VLANs, traffic on a secondary VLAN may be filtered and dropped within hardware while not affecting traffic from routers or other switches. For example, traffic that is bound to servers in a DMZ may be allowed, while traffic that initiates from servers may be blocked using VLAN ACLs. This acts to mitigate the risk if these servers are infected with malicious agents and/or are trying to participate in a DoS attack [14].

Cisco's implementation of dynamic port assignment to a VLAN, known as VMPS (VLAN Management Policy Server), is used to dynamically assign a particular switch port to a VLAN based upon the MAC address. This is useful for isolation of consultants and contractors on a network to an isolated VLAN in a firewall service network. By

doing so, consultants may be allowed access to certain VLANs and segments of the network through the use of ACLs on switches and/or the firewall. This also serves to isolate and protect the internal network from malicious agents on consultant laptops, and to protect the consultants themselves from external threats.

Private VLANs

Private VLANs, originally dubbed "Super VLANs" in RFC 3069 (titled "*VLAN Aggregation for Efficient IP Address Allocation"*) , were originally created to allow service providers to segregate hosted servers into their own logical VLAN without having to create numerous physical subnets and perform and maintain lists of complicated variably subnet'ed networks and their associated masks. Instead, servers from multiple customers could be located in the same broadcast domain, in this case a private VLAN, and configured to only talk to the default gateway and not each other.

While the switch market is largely dominated by Cisco, there are other vendors that office private VLAN functionality, such as Foundry Networks switches. However, given the large market share and common familiarity with Cisco, the rest of this paper will focus upon Cisco when discussing the implementation of private VLAN and VLAN ACL technologies. VMPS will also focus solely on Cisco as this is a Cisco proprietary technology.

The configuration of a private VLAN would make use of the following concepts:

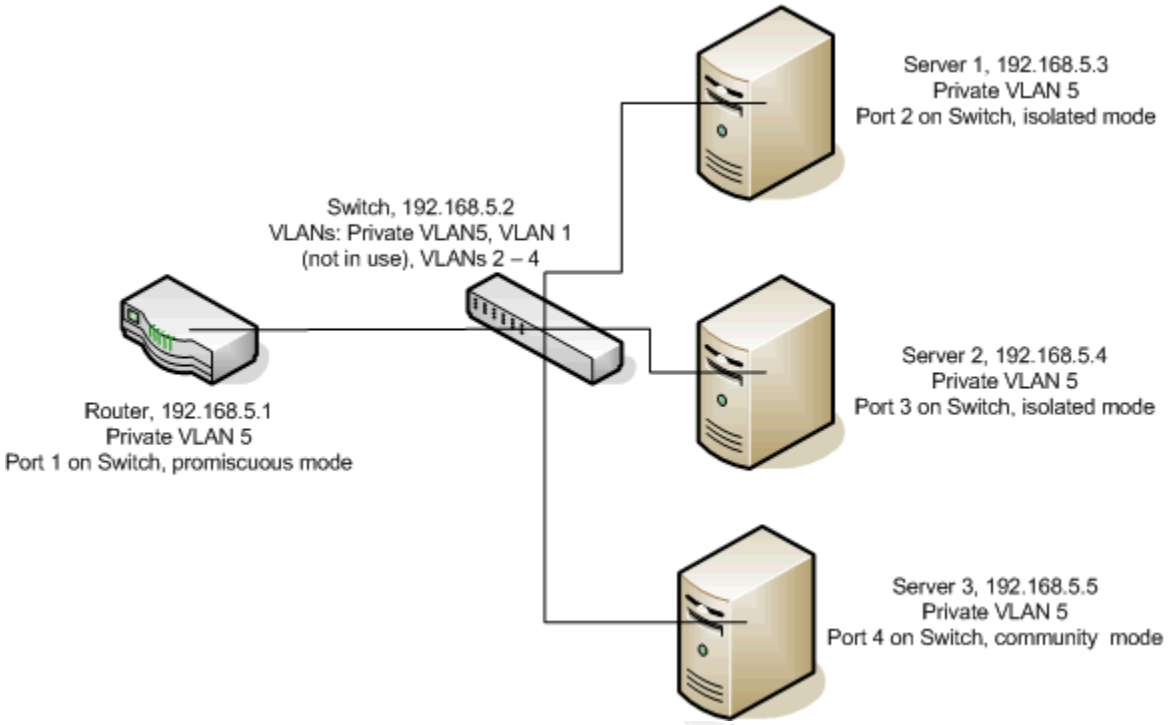
- Each port on the switch assigned to a particular VLAN would be configured as promiscuous, isolated or a community port.

- Promiscuous ports may talk to all other ports on the private VLAN. Ports that serve as the default gateway (often connected to a router or firewall) are typically configured as promiscuous ports.

- Other servers, such as an NTP server or syslog server, may also have their port configured as promiscuous or community. Community ports are ports that can communicate with other ports in the private VLAN, as well as the promiscuous port.

- An isolated port is a port that only communicates with the promiscuous port. Servers that should be isolated from communicating with other servers should be placed on an isolated port.

To illustrate the concept of a private VLAN, consider the network diagram below:



The switch, 192.168.5.2 is configured to have multiple VLANs, one of which is a private VLAN (VLAN 5). For this VLAN, ports 1 – 6 are assigned. The router is plugged into port 1 and this port is set to promiscuous, as the router is the default gateway for the switch and the servers in the VLAN. The servers are plugged into ports 2 – 4 and ports 2 and 3 are set to isolated. This prevents the servers from talking to each other and the server on port 4, but allows them to talk to the router (which is on port 1 and in promiscuous mode). Server 3 is plugged into port 4 and is allowed to talk to all servers in the private VLAN and the router. This server might be on a port set to community mode if it were a time or syslog server for the VLAN (which only the router would be able to communicate with unless another server was added to the VLAN on a community port), whereas servers 1 and 2 might be DMZ servers such as a web and mail server that do not need to communicate and therefore are isolated from each other in case one server is compromised.

This example brings to light where private VLANs play a role in network defense: isolating servers from each other at layer two in the same broadcast domain (or VLAN). Because private VLANs only operate at layer 2, and not at higher layers of the OSI model, VLAN ACLs as well as layer 3 router ACLs should be applied. However, what private VLANs do offer is defense-in-depth, especially in a DMZ firewall service network where there are multiple servers isolated to a single VLAN that perform critical roles. If one server in the VLAN is compromised, the other servers would be protected by the fact that the servers are on isolated private VLAN ports and VLAN ACLs have been applied to the VLAN, and router ACLs have been applied to the VLAN interface for layer 3 defense.

VLAN ACLs

VLAN ACLs offer additional defense to private VLANs by filtering traffic that ingresses and egresses a VLAN interface at both layers 2 and 3. While VLAN ACLs use IOS standard and extended ACLs (again assuming we are focusing on Cisco equipment), VLAN ACLs are not limited to filtering only routed traffic. VLAN ACLs filter IP, IPX and MAC layer traffic on VLAN interfaces, and IP traffic on WAN interfaces (thus achieving filtering at both layers 2 and 3).

There is a hierarchy of filtering rules and functionality that Cisco has implemented with VLAN ACLs, which are as follows [15]:

- All packets that enter a VLAN are check against the VLAN ACL (VACL) when a VACL has been applied to the VLAN

- If a VACL has been applied to VLAN, and an ACL has been applied to a routed interface in the VLAN, packets are checked against the VACL first when entering the VLAN. If the packet is permitted, then it is checked against the ACL before being passed to the routed interface.

- If a packet is being routed to another VLAN, the packet is first compared against the ACL applied to the routed interface. If it is permitted, the packet is then compared against the VACL for the destination VLAN.

- TCP intercepts and reflexive ACLs take precedence over VACLs if they applied to the same interface.

- VACLs and CBAC (Context Based Access Control), which is Cisco's version of a stateful firewall for routers and MSFC cards on switches, cannot be configured on the same interfaces.

- VACLs do not filter IGMP packets.

To configure VACLs, standard and extended IOS ACLs, MAC-layer named ACLs and VLAN access maps are used. These VACL components are briefly described below:

IOS standard and extended ACLs are simply access control lists that are applied to routed interfaces on Cisco routers and VLAN interface on switches with routing modules. Standard ACLs filter only on IP address, and are numbered 1 – 99. Extended ACLs filter on IP address as well as protocol and ports, and are numbered 100 – 199. Note that only one access list may be applied inbound and outbound per interface. Examples of each type of Cisco access list follow:

Standard ACL: `access-list 10 permit 192.168.1.0 0.0.0.255`

Extended ACL: `access-list 101 permit tcp 63.36.9.0 0.0.0.255 any eq 443`
On switches that support Unicast MAC filtering, MAC-layer ACLs are applied to VLAN

interfaces without IP addresses to filter protocol independent traffic (i.e. IPV4, IPV6, IPX, etc), as well as MAC-layer traffic as the traffic ingresses a port. Switches that do not support Unicast MAC filtering only filter on non-IP traffic. Do note that ingress traffic that was permitted or denied by a MAC ACL is treated as MAC-layer traffic when it egresses a port (and therefore IP ACLs cannot be applied to traffic that was inspected by MAC-layer ACLs) [16].

Implementing MAC-layer ACLs on a switch is as simple as follows:

```
Switch(config)# mac access-list extended mac_acl
Switch(config-ext-macl)# permit host 0000.0000.1111 any
Switch(config-ext-macl)# deny host 1111.1111.0000 any
Switch(config-ext-macl)# exit
Switch(config)# interface faste0/2
Switch(config-if)# mac access-group mac_acl in
Switch(config-if)# exit
Switch(config)# wr mem
```

This permits traffic with a MAC address of 0000.0000.1111 and denies traffic with a MAC of 1111.1111.0000 on switch interface fastethernet 0/2.

VLAN access maps are analogous to route-maps on routers and filters traffic into, through and out of a VLAN. The access map uses one or more map sequences, where the specific sequence has a match and action clause. The match clause specifies whether to use an IP, IPX or MAC ACL to apply against the packet, and the action clause clauses specifies whether to drop, forward, forward capture or redirect the packet. Packets that match an ACL entry are permitted and the subsequent ACLs in the sequence are ignored. If a packet does not match an ACL in the map, the packet is checked against the next ACL in the sequence.

Note that an interface (either VLAN or WAN) may only have one access map applied against it, whereas the same access map may be applied to multiple interfaces.

As an example, consider the following VLAN access map configuration that drops all TCP traffic on VLAN 5 and allows all other traffic and uses a layer 3 extended router ACL to do so [17]:

```
Switch(config)# access-list 100 permit tcp any any
Switch(config)# vlan access-map vlan5-map 10
Switch(config-access-map)# match ip address 100
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan access-map vlan5-map 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan filter vlan5-map vlan-list 5
```

In summary then, VACLs provide additional network defense to the use of private VLANs and the isolation of severs using isolated, community and promiscuous ports

by applying layer 3 IP ACLs and layer 2 MAC ACLs to the same VLAN using a VLAN access map structure.

There are drawbacks however to the use of private VLANs and VACLs. Mainly, the drawbacks are related to administration of the configuration of the switches that employ these said technologies, especially when MAC ACLs are used (due to specific MAC addresses being used in ACL statements). However, since private VLANs were designed and make the most sense to deploy in a DMZ subnet, where the architecture should be fairly static, the administration overhead should be minimal after the initial configuration. The same can be said of the configuration and administration of the VACLs. VLAN attacks do exist, one of which is VLAN hopping (where a host spoofs as a switch with ISL or 802.1q trunking enabled to become a member of all VLANs). A full discussion is of this attack is out of scope for this paper, however further information can be found in the following links:

http://www.sans.org/resources/idfaq/vlan.php
http://www.arp-sk.org/doc/bh-us-02-convrey-switches.pdf

VMPS

While private VLANs and VLAN ACLs can protect hosts from each other and filter traffic based on layer 2 MAC and layer 3 IP ACLs, Cisco's dynamic VLAN VMPS functionality adds additional defense by allowing specific hosts to be placed into a specific VLAN based on their MAC. When combining these three defensive technologies, a scenario such as the following is achievable:

Imagine that a consultant is hired and brought in to the internal LAN environment to perform work. To protect the LAN assets and the consultant, the consultant's laptop MAC address is obtained and placed in the VMPS server config. When the consultant plugs their laptop into a network jack (that is patched into a VMPS client switch), they are placed in an isolated VLAN that is located in a firewall service network that protects the consultant from the Internet and the LAN from the consultant. For additional security, the VLAN is configured as a private VLAN with isolated ports (in case there are multiple consultants from multiple companies who are plugged into the same switch), and VLAN ACLs are applied to the VLAN interfaces using access maps as a means of achieving defense-in-depth and to augment the firewall filtering when egressing the firewall service network.

Before discussing a specific implementation of the VMPS portion of this scenario (as is presented in the latter part of this whitepaper), a discussion of what VMPS is and how it works is in order.

VMPS (VLAN Management Policy Server) allows a host to placed dynamically into a specific VLAN based upon the MAC address of the host and the port the host is connected to. As the host moves from one port to another in the organization, the port is dynamically moved to the specific VLAN based upon the MAC. Note that VMPS is a proprietary Cisco

VMPS is implemented using a VMPS server (typically an enterprise Cisco switch, such as a 6000 series) and VMPS clients (typically any Cisco switch, including access-layer switches like the 2900XL and 2950XL models). The VMPS server downloads the VMPS database, typically from a TFTP server, and obtains a list of MAC addresses of hosts that should be placed in a specific VLAN by dynamically placing the switch port in the said VLAN. Additional rules may be applied in the VMPS configuration file, such as which ports should be allowed in a specific VLAN, and whether access should be denied to the host or not.

The following rules apply to VMPS [2]:

- VMPS must be configured before you configure ports as dynamic.

- When a port is configured as dynamic, spanning tree PortFast is enabled automatically for that port. Automatic enabling of spanning tree PortFast prevents applications on the host from timing out and entering loops caused by incorrect configurations.

- If a port is reconfigured from a static port to a dynamic port on the same VLAN, the port connects immediately to that VLAN. However, VMPS checks the legality of the specific host on the dynamic port after a specified period of time.

- Static secure ports cannot become dynamic ports. You must turn off security on the static secure port before it can become dynamic.

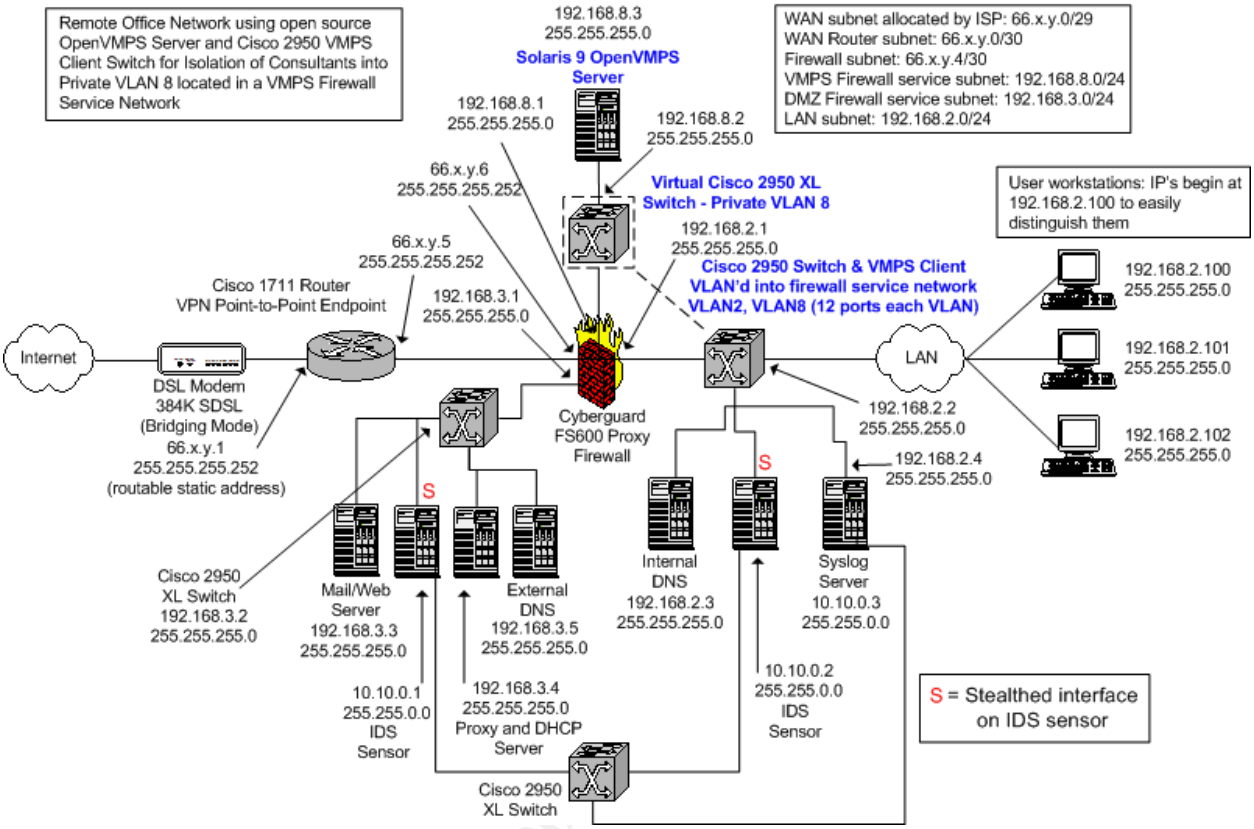
- Static ports that are trunking cannot become dynamic ports. You must turn off trunking on the trunk port before changing it from static to dynamic.

Given this brief explanation of what VMPS is, a specific implementation of VMPS is presented next. Note that VLAN8 in the proceeding section could also be configured as a private VLAN with VACLs as previously discussed to achieve defense-in-depth.

Private VLAN/VMPS Solution for a Small Office Network Using OpenVMPS

The focus on this last section will be upon the use of a private VLAN utilizing Cisco VMPS (VLAN Management Policy Server) to isolate consultants on the internal LAN to an isolated VLAN in a firewall service network. This isolation into a private VLAN will provide protection for the internal LAN from the consultants via ACLs on the firewall, protection from Internet threats and controlled access to the web and internal assets for the consultants.

Network Topology



The topology used in the remote office VMPS solution is show above. Important to note is the LAN switch that has been VLAN'd across the Cyberguard firewall into a firewall service network (12 ports in each VLAN). Normally VLAN'ing across a firewall is not a secure configuration, but given the location of the VLAN into a firewall service network that isolates it from the LAN, Internet and DMZ hosts, mitigates the risk. Also note that the OpenVMPS server will run on an SPARC Ultra5 running Solaris 9. The typical protections, such as a border router that performs ingress/egress filtering and denies inbound traffic that is not explicitly allowed, have been utilized. Similarly, the Cyberguard firewall also employs ACLs to protect all three internal subnets (LAN, DMZ and VMPS firewall service network) and NATs internal private addresses to its public external address (66.x.y.6).

VMPS – VLAN Management Policy Server Functionality Overview

According to Cisco, a VMPS server performs the following specific functions:

"If the assigned VLAN is restricted to a group of ports, VMPS verifies the requesting port against this group. If the VLAN is allowed on the port, the VLAN name is returned to the client. If the VLAN is not allowed on the port and VMPS is not in secure mode, the host receives an "access denied" response. If VMPS is in secure mode, the port is shut down.
<snip…>
If a VLAN in the database does not match the current VLAN on the port and active hosts are on the

port, VMPS sends an access denied or a port shutdown response based on the VMPS secure mode.
<snip…>
When the link comes up, a dynamic port is isolated from its static VLAN. The source MAC address from the first packet of a new host on the dynamic port is sent to VMPS, which attempts to match the MAC address to a VLAN in the VMPS database. If there is a match, VMPS provides the VLAN number to assign to the port. If there is no match, VMPS either denies the request or shuts down the port (depending on the VMPS secure mode setting)." [2]

VMPS – VLAN Management Policy Server (vmpsd)

The VMPS server in this architecture is a Sun Ultra5 running Solaris 9.

```
root@grace:/>uname -a
SunOS grace 5.9 Generic_112233-04 sun4u sparc SUNW,Ultra-5_10
```

The openVMPS server software, vmpsd, should be downloaded from here: http://sourceforge.net/projects/vmps. The software is a compressed tar ball named vmpsd-1.3.tar.gz. Download the file and uncompress and untar it (in this case, to /export/home/downloads/software):

```
root@grace:/export/home/downloads/software> gunzip vmpsd-1.3.tar.gz; tar
-xvf vmpsd-1.3.tar
```

Now build the vmpsd binary:

```
root@grace:/export/home/downloads/software/vmpsd> configure; make; make
install
```

The VMPS server binary (*vmpsd*) is now ready to be configured and started. The config file the vmpsd binary uses is called *vlan.db*. An example of the default vlan.db file is show in Appendix 1 [3].

Note that a tftp server is typically used to store and download the ASCII vmps database file from Cisco switches. Since our OpenVMPS server has the vmps database stored locally, this is not necessary.

As mentioned above, instead of using an enterprise level Cisco switch for the VMPS server, the open-source OpenVMPS software running on a Solaris 9 server will be utilized in the network architecture. The server will open a UDP socket for communications with VMPS clients for searching for MAC address to VLAN mappings.

Below are the options available using the vmpsd binary:

```
root@grace:/export/home/downloads/software/vmpsd>vmpsd -h

Options:
        -a ip       address to bind to (any)
        -d          do not detach, log to stderr also
        -e path     use external program for mac to vlan assignment
                    when/if used with -f, -f is disregarded
        -f file     read VMPS database from file (/etc/vmps.db)
        -l level    set logging level:
                          0x0100 - fatal,
```

```
                        0x0200 - info,
                        0x0400 - warning,
                        0x0800 - debug,
                        0x0001 - system,
                        0x0002 - parser,
                        0x0004 - vqp
        -p port     port to listen on (1589)
```

To start the vmpsd server on UDP port 1589 with the vlan.db configuration file and with the logging syslog level of “warning”, run the following command:

```
root@grace:/export/home/downloads/software/vmpsd> vmpsd -f vlan.db -p 1589 -
l 0x0400
```

Now, to verify the vmpsd binary is listening on UDP port 1589, run a netstat command:

```
root@grace:/export/home/downloads/software/vmpsd> netstat -an | grep 1589

UDP: IPv4
   Local Address         Remote Address     State
-------------------- -------------------- -------
<snip…>
      *.1589                               Idle
<snip…>
```

To configure the vlan.db file for the proposed architecture, changes to the vlan.db file are suggested as follows (changes italicized and in blue text):

!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode { open | secure }
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req { allow | deny }
!
! The default value is allow.

vmps domain *giac-cookies.com*
vmps mode open
vmps fallback *default ! The fallback vlan is default, which is VLAN8 if MAC is not in vlan.db file*
vmps no-domain-req deny

!
!MAC Addresses
!
vmps-mac-addrs
!
! address <addr> vlan-name <vlan_name>

! netreg extension - *default vlan (vlan8) for this MAC*
address 0010.a49f.30e1 vlan-name --DEFAULT--
! disabled - *no access allowed for this MAC*
address 0010.a49f.30e2 vlan-name --NONE--
! vlan *VLAN8* restricted
address 0010.a49f.30e3 vlan-name *VLAN8*

```
! vlan VLAN8 restricted
address 0010.a49f.30e4 vlan-name VLAN8
! vlan VLAN2 unrestricted
address 0010.a49f.30e5 vlan-name VLAN2

!
!Port Groups
!
!vmps-port-group <group-name>
! default-vlan <vlan-name>
! fallback-vlan <vlan-name>
! device <device-id> { port <port-name> | all-ports }

vmps-port-group switch
  default-vlan  VLAN8
  fallback-vlan VLAN8
  device 192.168.8.4 port 0/14
  device 192.168.8.5 port 0/53
  device 192.168.8.6 port 0/64
  device 192.168.8.7 all-ports

!VLAN groups
!
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>

vmps-vlan-group myvlans
  vlan-name VLAN2

!VLAN port Policies
!
!vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
! { port-group <group-name> | device <device-id> port <port-name> }

vmps-port-policies vlan-group myvlans
  port-group switch
```

Each time a new consultant needs access to VLAN8, the vlan.db file on the OpenVMPS server should be updated with their MAC and the vmpsd binary restarted. In addition, access can also be taken away by adding rouge or misbehaving hosts (via their MAC) to the vlan.db file.

VMPS Client Switch

The VMPS client switch needs to be configured on a port-by-port basis to look at the VMPS server to determine if a MAC address of the client plugged into the port should belong to the private VLAN. To configure the switch to be VMPS client, perform the following steps [4]:

While in enable mode in the switch, enter the following to configure ports 0/15 – 0/24 as dynamic ports (ports 0/13 and 0/14 are static ports for the firewall and OpenVMPS server):

```
switch# vmps server 192.168.8.2 primary
switch# conf t
switch(config)# int faste 0/14
switch(config-if)# switchport mode access vlan dynamic
switch(config-if)# end
switch(config)# int faste 0/15
switch(config-if)# switchport mode access vlan dynamic
switch(config-if)# end
<snip…>
switch(config)# int faste 0/23
switch(config-if)# switchport mode access vlan dynamic
switch(config-if)# exit
```

Ports 0/1 – 0/12 are statically assigned to VLAN2 with the following commands:

```
switch# conf t
switch(config)# int faste 0/1
switch(config-if)# switchport mode access vlan 1
switch(config-if)# end
<snip…>
switch(config)# int faste 0/12
switch(config-if)# switchport mode access vlan 1
switch(config-if)# exit
switch(config-if)# wr mem
```

VMPS Security Risks and Mitigations

The following are risks and mitigations involved with the deployment of private VLANs using VMPS are summarized as follows:

Risks	Mitigations	Summary
VLAN'ing across the firewall is inherently dangerous. The switch could be "flooded" and essentially turned into a hub.	The placement of the dynamic VLAN into a firewall service network mitigates the risk from attacks both inside and outside the network by way of access controls on the Cyberguard between the Internet/DMZ and the internal network. Since the firewall service network only contains the VMPS server (which has been sufficiently hardened and only listens on necessary ports, such as 1589/UDP for VMPS and 22/TCP for SSH access by administrators), the risk from attacks from the internal LAN is reduced. Also note that the internal IDS receives alerts from all ports on the internal switch by way of port mirroring.	There is an inherent risk due to VLAN'ing across the firewall, but the risk is mitigated by the network architecture and defense-in-depth.
MAC addresses can be spoofed and VMPS controls can be bypassed.	MAC addresses can be spoofed, however the chance of a consultant spending more time on attacking the local network than working on their assignment is reduced due to the careful screening of consultants hired, monitoring of their progress and careful attention paid to IDS alerts should successful MAC spoofing lead to further attacks.	MAC address spoofing risk is small and mitigated by monitoring consultant performance and IDS alerts.

There are well known attacks and tools for ARP cache poisoning, flooding, VLAN jumping, etc. [5]	The risk from these tools is real and a serious consideration. However, when weighing the convenience of VMPS and the aforementioned defenses against the probability of a consultant attacking the network, using VMPS makes good business sense for GIAC.	Business risk/benefit analysis leads to acceptance of risk from using VMPS given finite staff resources and mitigating defenses through a defense-in-depth inspired architecture.
Network administrators may not have time or be available to make necessary updates to the vlan.db file when needed.	Since the vlan.db files is relatively easy to update, a special group and accounts can be set up on the VMPS server so that help desk personnel can edit the vlan.db file. To mitigate the risk of help desk personnel working on the VMPS server, ssh/scp and symmetric keys can be used to retrieve the vlan.db file and then push it back to the server with changes. A special group/accounts need to be created for this on the VMPS server, the vlan.db file needs its permissions/ownership changed (it's root/other and 644 by default), symmetric keys need to be created and distributed to key help desk personnel, and finally RBAC or sudo should be considered to further enhance security and limit permissions given to the help desk persons.	Lack of administration can be mitigated through technological means and the assistance of help desk personnel.

Assignment 2: Security Architecture

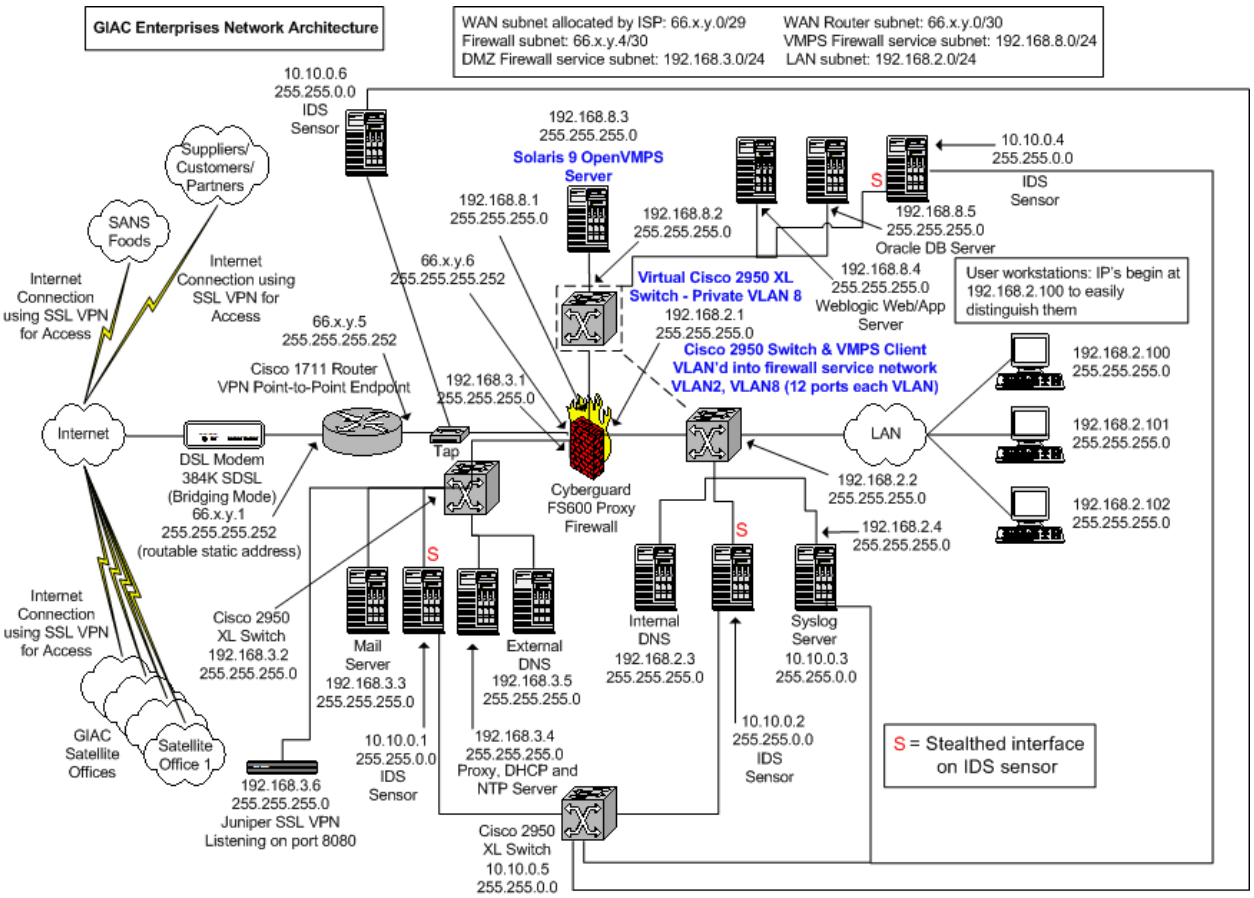
Introduction

The following security architecture is that of a remote office, GIAC Enterprises, which markets fortune cookies worldwide. Currently, the office is in its startup phase and is a subsidiary of its parent corporation, SANS Foods.

Because it is a remote office, an expensive high-speed line (such as a fractional T1) is not needed nor is there budget for it. A 384K symmetric DSL (SDSL) line with a small subnet containing static, routable IPs will be used. In addition, there was limited budget for expensive high-end hardware, so equipment that is appropriate for a remote office (which is often handed down from the parent corporation) was utilized. This type of equipment often means small 24-port switches, Sun Ultra5 and Ultra60 servers, PC's running Linux, etc. Where applicable, such as the Weblogic web/app server and Oracle database, internal tape drives exist for backups. Backups of other data utilize a CD/DVD burner on an internal host and data is transferred there via SFTP/SCP.

Architecture Diagram

The following diagram depicts the network topology of GIAC Enterprises:



Customer Interaction

Customers access GIAC Enterprises for online catalog browsing and purchases on the GIAC Enterprises web server using HTTP (80/TCP) and HTTPS (443/TCP). General browsing of the web/app server is done over port 80, whereas orders and any private customer data is done over an SSL-encrypted connection using port 443. In addition, 53/UDP is open for name resolution of the domain giac-enterprises.com domain to the web/app server. 53/TCP is not open to external entities as they have no need for zone transfers between themselves and GIAC Enterprises, and query responses 512 bytes and larger are indicative of malicious activity and are not allowed. All other ports/protocols are denied to customers, which is in line with the “deny what is not explicitly allowed” access policy on the GIAC firewall.

Source	Destination	Port(s)/Protocol	Description
Customer	Web/App Server in firewall service network	80/TCP (HTTP) 443/TCP (HTTPS)	Customer access to web/app sever to view online catalog and/or order cookies.
Customer	Mail Server in DMZ Firewall Subnet	25/TCP (SMTP)	E-mail sent from customer to GIAC Enterprises.
Customer	External DNS Server in DMZ Firewall Subnet	53/UDP (DNS queries)	Name resolution for GIAC Enterprises (i.e. www.giac-enterprises.com) for web server access to external DNS server.

Supplier Interaction

Like customers, suppliers are allowed to send mail to GIAC, as well as query the GIAC DNS server. Suppliers are given web access to GIAC for the purposes of viewing special supplier specific inventory pages, as well as dropping files in a supplier specific folder via a web application form. This is generally all done over port 443/TCP, except where the information is not sensitive, and then port 80/TCP is used. The special inventory pages are built by the web/app server, which in turn queries the Oracle database server. Suppliers are never given direct access to the database.

Source	Destination	Port(s)/Protocol	Description
Supplier	Web/App Server in firewall service network	80/TCP (HTTP) 443/TCP (HTTPS)	Supplier access to web/app sever to view special supplier inventory pages and/or drop files in a supplier-specific folder via a web application form
Supplier	SSL VPN in DMZ Firewall Subnet	SSL over 8080/TCP	Used for special access, such as telnet from a supplier to a test host the supplier is co-hosting (23/TCP), etc. All access is tunneled inside SSL, and access is granted during business hours (5:00am – 7:00pm EST).
Supplier	Mail Server in DMZ Firewall Subnet	25/TCP (SMTP)	E-mail sent from supplier to GIAC Enterprises
Supplier	External DNS Server in DMZ Firewall Subnet	53/UDP (DNS queries)	Name resolution for GIAC Enterprises for web server access to external DNS server.

Partner Interaction

Partners are granted access to GIAC that is similar to that given to suppliers. The one difference is that partners are often given an e-mail account on the GIAC mail server. That mail account is accessed by the partner through the SSL VPN (in the case of GIAC, the partner accesses their mail via a Lotus Notes client through the SSL VPN to the GIAC Mail/Lotus Notes server on port 1352/TCP). Because not all users are encryption savvy or know how to use PGP/GPG, this was provided to ensure that mail was not sent un-encrypted over the Internet that had sensitive financial information in it. All such e-mail is encrypted over the SSL VPN tunnel from partner sites to the GIAC site.

Source	Destination	Port(s)/Protocol	Description
Partner	Web/App Server in firewall service network	80/TCP (HTTP) 443/TCP (HTTPS)	Partner access to web/app sever to view special partner sales/forecast pages and/or drop files in a partner-specific folder via a web application form

Partner	SSL VPN in DMZ Firewall Subnet	SSL over 8080/TCP	Used for special access, such as access to the mail server for GIAC mail accounts supplied to partners (1352/TCP), etc. All access is tunneled inside SSL, and access is only granted all hours of the day.
Partner	Mail Server in DMZ Firewall Subnet	25/TCP (SMTP)	E-mail sent from partner to GIAC Enterprises
Partner	External DNS Server DMZ Firewall Subnet	53/UDP (DNS queries)	Name resolution for GIAC Enterprises (i.e. www.giac-enterprises.com) for web server access to external DNS server.

Internal GIAC Employee Interaction

Internal users are allowed access to the Internet, DMZ and the internal LAN via access controls on the Cyberguard firewall. All internal users are allowed HTTP/HTTPS and SSH access to the Internet. Internal users are also allowed to obtain IP's via DHCP requests to the DHCP server in the DMZ. Internal users are also allowed name resolution via the internal DNS server, as well as HTTP/HTTPS and SSH access to other internal hosts (such as the syslog server by administrators or an intranet web server for HR information running on the proxy server). Finally, internal users (such as a web developer or Oracle DBA) are allowed HTTP/HTTPS and SSH access to the firewall service network hosts such as the VMPS, Oracle and web/app servers.

Note that the proxy server is used to cache commonly accessed pages, as well as to audit where internal employees surf. If in the future the need arises, as Websense content filter may be used in conjunction with the proxy server to block inappropriate sites.

Source	Destination	Port(s)/Protocol	Description
Internal Employee	Internet	80/TCP (HTTP) 443/TCP (HTTPS) 22/TCP (SSH)	Internal employees are allowed to surf the Internet (HTTP and HTTPS), as well as SSH to the Internet.
Internal Employee	DMZ Firewall Subnet	68/UDP (DHCP/bootpc) 22/TCP (SSH) 1352/TCP (Lotus Notes) 80/TCP (HTTP) 443/TCP (HTTPS)	Internal users receive DHCP addresses from the DMZ, and administrators are allowed to SSH to DMZ machines. Internal users query the internal DNS server for name resolution, not the DMZ DNS server (so as not to cache sensitive internal IP/host information). Mail is also sent/received from the Lotus Notes server.

Internal Employee	Internal LAN	53/UDP (DNS) 22/TCP (SSH) 80/TCP (HTTP) 443/TCP (HTTPS)	Name resolution of internal clients and Internet queries use the Internal DNS server. Administrators are allowed SSH access to the syslog server to check IDS alerts, syslog alerts, perform maintenance and SCP logs to an internal host for burning to CD/DVD for archival.
Internal Employee	Web/App Server and Oracle DB in VMPS firewall service network	80/TCP (HTTP) 443/TCP (HTTPS) 22/TCP (SSH)	Internal users are allowed HTTP and HTTPS access to the web/app server and Oracle DB in the firewall service network. Internal users (such as administrators and DBA's) are also allowed SSH access to these servers, as well as the VMPS server.

GIAC Remote User (Sales Force) Interaction

Source	Destination	Port(s)/Protocol	Description
Remote User	Web/App Server in VMPS firewall service network	80/TCP (HTTP) 443/TCP (HTTPS)	Remote users are allowed access to web/app sever to view the online catalog and enter orders in special SSL-enabled web forms. Queries against the Oracle DB for inventory purposes are done via the web/app sever.
Remote User	SSL VPN in DMZ Firewall Subnet	SSL over 8080/TCP	Used for remote e-mail access to the Lotus Notes server (1352/TCP), as well as access to the web/app server (80/TCP and 443/TCP) if using the SSL VPN.

General Public/Internet Interaction

The general public is allowed to connect to the web/app server to browse the product catalog and submit orders. Administrators are also allowed to connect to any of the subnets (DMZ, internal LAN and firewall service network) via the SSL VPN for remote admin purposes. Administrators are also allowed to connect remotely to the router via SSH by first connecting to the SSL VPN. Finally, the SSL VPN may also be used for special access such as troubleshooting by Cisco, subcontractor access, etc.

Source	Destination	Port(s)/Protocol	Description
Internet	Web/App Server in VMPS firewall service network	80/TCP (HTTP) 443/TCP (HTTPS)	Customer access to web/app sever to view online catalog and/or order cookies. Also useful for special access to access-controlled pages for internal users in the field, partners and admins.

Internet (remote admins only)	All GIAC network devices (not including the switches)	SSL over 8080/TCP	Remote SSH access via SSL VPN by administrators to all GIAC network devices (not including switches).
Internet	SSL VPN in DMZ Firewall Subnet	SSL over 8080/TCP	Used for remote e-mail access to selected hosts anywhere in the network (might require a rule on Cyberguard firewall). Useful for when Cisco tech support wants to login and help troubleshoot an issue on the router or firewall (vs. allowing them to SSH directly to those devices). Also used by admins to SSH to any host in the network that has a listening SSH daemon.
Internet	External DNS Server in DMZ Firewall Subnet	53/UDP (DNS queries)	Name resolution for GIAC Enterprises (i.e. www.giac-enterprises.com) for web server access to external DNS server.

Router

The router is a Cisco 1711 Security Access Router. This router is ideal for GIAC Enterprises. According to Cisco:

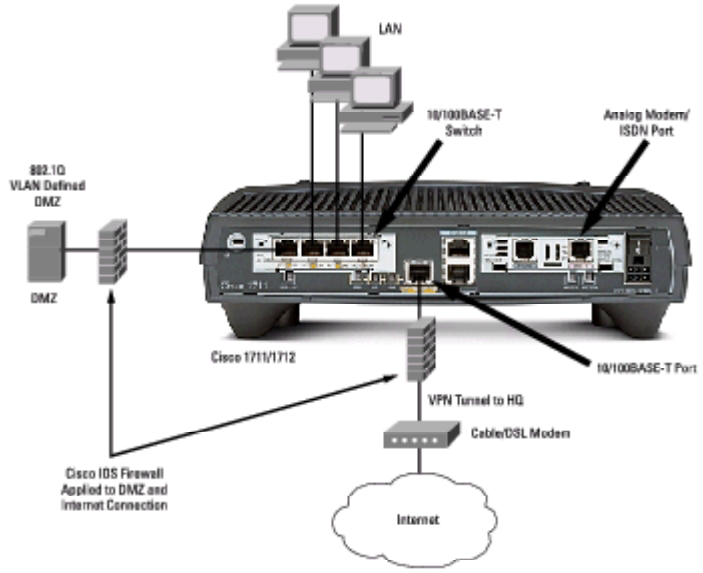
"Cisco 1711 and 1712 routers help businesses reduce costs by allowing deployment of a single device to provide multiple services (router, Fast Ethernet switch, firewall, virtual private network [VPN], Intrusion Detection System [IDS], and redundant WAN interface) typically performed by separate devices. Cisco IOS Software allows this flexibility, providing the industry's most robust, scalable, and feature-rich internetworking software support, using the accepted standard networking software for the Internet and private WANs." [6]

The router is running the following IOS and contains the following amount of memory:

```
dmz_rtr#show hard
Cisco IOS Software, C1700 Software (C1700-K9O3SY7-M), Version 12.3(7)XR3,
RELEASE SOFTWARE (fc2)
Synched to technology version 12.3(7.11)T1
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Sat 25-Sep-04 16:02 by ealyon

ROM: System Bootstrap, Version 12.2(7r)XM4, RELEASE SOFTWARE (fc1)
ROM: Cisco IOS Software, C1700 Software (C1700-K9O3SY7-M), Version
12.3(7)XR3, RELEASE SOFTWARE (fc2)

dmz_rtr uptime is 23 minutes
System returned to ROM by power-on
System image file is "flash:c1700-k9o3sy7-mz.123-7.XR3.bin"

dmz_rtr #show mem
                Head    Total(b)     Used(b)     Free(b)    Lowest(b)
Largest(b)
Processor   824C4C60    50874040     7125144    43748896    42386040
```

```
41249196
      I/O       5457000    12226560     1737164    10489396    10489396
10489344
```

The router has a built-in ISDN and modem port for back-up and out-of-band access, as well as a 4-port 10/100 switch. This makes the 1711 ideal for a small office environment that uses DSL. The image below better depicts the hardware options on the router [6]:



The router has been hardened and uses a hybrid configuration that denies certain traffic, allow all other traffic destined to the firewall's external interface, and then denies all other traffic. This allows the firewall to perform its purpose of firewalling, while at the same time allowing the majority of the traffic to be sniffed by the IDS sensor from the tap between the router and firewall. The router configuration is further discussed in assignment 3.

Firewall

The firewall is a Cyberguard FS600 firewall with one 10/100 and seven 10/100/1000 Ethernet interfaces, 256MB of RAM and a large selection of application proxies such as HTTP, SMTP, Lotus Notes, etc. [7] While the FS600 has VPN support, the Juniper SSL VPN will be used instead due to its freedom from a VPN client and granular access control available to the administrator.

The firewall is configured to proxy all inbound connections to the network using an application proxy (if available). Application proxies on the Cyberguard exist for HTTP, HTTPS (although no payload inspection is possible), SMTP, Lotus Notes, etc. If an application proxy is not available, such as for UDP protocols or custom TCP-based applications, Cyberguard has a stateful UDP proxy and a generic stateful TCP proxy called a "PortGuard proxy". Packet filter rules are also available, and will be utilized for DNS, NTP, VMPS and other UDP protocols that must traverse the GIAC firewall.

Internal traffic is also routed through the firewall between the different internal subnets. This serves to isolate the different internal networks and enforce strict access control policies. All internal addresses are NAT'd to the external IP address of the firewall when traffic is bound for the Internet. Traffic from one internal GIAC subnet to another is not NAT'd, and the firewall has routes to all hosts. Each internal host on the GIAC internal subnets uses the firewall address as its default gateway. Administration of the firewall is accomplished through remote SSH administration from the internal network or over the SSL VPN from remote locations by the security administrator (and the backup firewall admin) only.

Audit logs are sent to the syslog server via syslog, and rotated logs on the firewall are stored to CD/DVD using SCP to transfer them to or from a host with a CD/DVD burner on the internal LAN.

Switches

The switches used in the GIAC Enterprises architecture are Cisco 2950XL 24-port switches (see output from the `show hardware` and `show mem` commands below).

```
dmz_switch #show hard
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(13)EA1c, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Tue 24-Jun-03 17:31 by yenanh
Image text-base: 0x80010000, data-base: 0x805A8000

ROM: Bootstrap program is CALHOUN boot loader

Switch uptime is 4 minutes
System returned to ROM by power-on
System image file is "flash:/c2950-i6q4l2-mz.121-13.EA1c.bin"

cisco WS-C2950-24 (RC32300) processor (revision E0) with 20839K bytes of
memory.
Processor board ID FHK0625X29X
Last reset from system-reset
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:0A:41:10:83:C0
Motherboard assembly number: 73-5781-10
Power supply part number: 34-0965-01
Motherboard serial number: FOC06250AAT
Power supply serial number: DAB062550K6
Model revision number: E0
Motherboard revision number: B0
Model number: WS-C2950-24
System serial number: FHK06200000
Configuration register is 0xF

dmz_switch#show mem
               Head    Total(b)     Used(b)     Free(b)   Lowest(b)
Largest(b)
```

```
Processor   80B9EB20     4834528     1869520     2965008     2712604
2712600
      I/O   A08B4D40     3055040      703864     2351176     2338908
2339208
```

These switches are able to function as VMPS clients, support multiple VLANs and support port spanning/mirroring for the IDS sensors. The switches have been given both a console and enable password and stored encrypted within the config using the `service password-encryption` command. Common services that are not required have been turned off with the following commands, as well as general security precautions (such as no source routing):

```
dmz_switch(config)#no ip finger
dmz_switch(config)#no ip http server
dmz_switch(config)#no udp small-services
dmz_switch(config)#no tcp small-services
dmz_switch(config)#no ip source-route
```

The CDP (Cisco Discovery Protocol) has also been disabled, which prevents the switch from sending out potentially useful information to an attacker on every port (such as router interface information, Cisco platform information and addresses of neighboring Cisco devices) [10].

```
dmz_switch(config)#no cdp run
```

Note that since these switches do not support SSH access, and the GIAC Enterprises office is not very large and only contains a handful of switches, no telnet access is allowed to the routers. Administrators must use a console cable to connect to switches and configure them. This is an inconvenience, however management was advised against using telnet due to sniffing concerns and also for the unwanted precedence that its use creates.

VPN(s)

SSL VPN – The SSL VPN GIAC Enterprises has deployed is a Juniper Networks Netscreen Remote Access SSL VPN 500 RA-525 (which supports 25 simultaneous users). According to Juniper:

"*The Juniper Networks NetScreen-Remote Access 500 series of SSL VPN appliances provide small to medium enterprises a secure, cost-effective way to deploy employee remote access to corporate networks. Because the NetScreen-Remote Access 500 uses Secure Sockets Layer (SSL) to provide encrypted transport, it enables instant access for users with just a Web browser. This eliminates the cost of installing, configuring, and maintaining client software for each user. As a result of this clientless architecture, small to medium enterprises can realize a significantly reduced total cost of ownership versus traditional client-based solutions. Because it uses SSL delivery, the NetScreen-Remote Access 500 also eliminates Network Address Translation (NAT) and firewall traversal issues found with traditional remote access products."* [9]

Especially important to GIAC is the clientless connection method (only a web browser is required, such as Internet Explorer 6.0) and the fact that IPSec NAT issues are eliminated by tunneling connections over port 8080 using SSL (port 443 is reserved for

the web/app server since the Cyberguard uses port forwarding to servers based on the destination port used). By using port 8080, a common proxy port, the changes of remote users being blocked access to the SSL VPN by their corporate or hotel firewalls is greatly reduced (vs. the common occurrence of port UDP/500 and ESP protocol being blocked). The SSL VPN also gives the VPN administrator granular control of user access. For instance, a user can be granted SSH access to a single host with only one change to the SSL VPN, vs. opening up an IPSec tunnel to corporate where the user would have greater access and could not be controlled down to the user level for any protocol.

Two-factor authentication was considered but the decision was made not to employ it due to cost and administrative constraints given the size of GIAC. If in the future two-factor authentication is needed, its use will be revisited.

IDS Sensors

The IDS sensors are Sun Ultra5's running Solaris 9.

```
root@quinn:/>uname -a
SunOS quinn 5.9 Generic_112233-04 sun4u sparc SUNW,Ultra-5_10
```

The Ultra5 has a 360MHz UltraSPARC-Iii processor, 256KB of cash, 256MB RAM, and a 9.1GB IDE HD. The sensors are utilizing Snort 2.3.0 RC2 to monitor traffic, and syslog alerts to the syslog server as well as transferring alert files file SCP to the syslog server for inspection in a batched fashion via a cron script and symmetric SSH keys.

Note that the VMPS firewall subnet needs a sensor as Cisco 2950 switches cannot span ports across VLAN's [8], and the IDS sensor interfaces that monitor traffic are plumbed and up'd, but no IP address is assigned (which creates a stealthed interface that promiscuously sniffs traffic but cannot communicate on the local network). The IDS sensor between the router and firewall sniffs traffic using a 10/100 network tap. This provides secure sniffing of traffic, while at the same time not risking the use of a switch to port span traffic and having the switch become overwhelmed by traffic spikes and drop packets.

Management of the IDS sensors is accomplished out-of-band using a switch and the 10.10.0.0/16 network from the syslog server (which has an out-of-band interface, as well as an interface on the 192.168.2.0/24 network). Patches, Snort updates, whois lookups and traceroutes are all done from the Syslog server and then stored to disk (if applicable). IDS sensors then SCP/SFTP to the syslog sever to retrieve them, or conversely the syslog sever can push them out via SCP/SFTP.

Syslog Server

The syslog server, like the IDS sensors, is a Sun Ultra5 running Solaris 9. The /var partition on the syslog server has been sized to be 6GB and made its own partition, with the remainder being allocated to the root directory "/", the user directory "/usr" and

swap "/tmp". The syslog server has also been hardened using the Solaris Security Toolkit (JASS) so that a minimal number of ports are listening, such as 514/UDP (Syslog), 22/TCP (SSH), as well SunRPC ports since X is required for CDE to run. Other hardening steps were taken, such as turning off core dump creation in the /etc/security file. A complete discussion of hardening Solaris 9 is beyond the scope of this document, but general guidelines were followed from Sean Boran's article here. [12]

Syslogs are rotated nightly and compressed for storage for a 7-day period on disk. Weekly, logs are tar'd and transferred to a host with a CD/DVD drive for media creation using SCP. IDS logs are inspected using ACID/MySQL/PHP/Apache/mod-ssl for Snort alert files transferred to the log server using SCP. Alerts are then viewed with ACID on the syslog server that only accepts connections on the NIC addressed with the 10.10.0.3 address. Admins may also SSH to the syslog server from anywhere in the GIAC network. Installation/Configuration of ACID/Snort on a Solaris 9 box was accomplished using this document [13].

Syslogs from other devices (as well as IDS syslogs) are inspected using a custom ASCII based SIM (Security Information Management) script written in Perl for use on a UNIX box. See Appendix 2 for the script.

IP Addressing Scheme

GIAC Enterprises was given a partial class C subnet from their DSL provider when their SDSL line was installed. The subnet given was 66.x.y.1/29. This subnet was variably subneted into the two networks, 66.x.y.1/30 and 66.x.y.4/30. The first subnet is the WAN subnet and is used on the external side of the router (66.x.y.1), and the second subnet is used for the internal side of the router and external side of the firewall (66.x.y.5 for the internal router interface and 66.x.y.6 for the external firewall interface). This was done so that external entities can address the external firewall interface and be proxied by port to a destination server (i.e. traffic that arrives on port 8080/TCP on the external firewall interface is proxied to the SSL VPN 192.168.3.6 listening on port 8080/TCP).

The internal addressing scheme on the GIAC network utilizes RFC 1918 addressing. There are four internal subnets that use private addressing: a DMZ firewall service network subnet, VMPS firewall service network, internal LAN subnet, and an out-of-band IDS sensor management network. The networks are shown below.

VMPS Firewall service subnet: 192.168.8.0/24
DMZ Firewall service subnet: 192.168.3.0/24
LAN subnet: 192.168.2.0/24
Out-of-band IDS sensor management network: 10.10.0.0/16

The IDS sensor network was given a 10.10.0.0/16 address to help distinguish it from the other class C RFC 1918 subnets used on the network in both diagrams and in the syslog server operating system files. The 10.10.0.0.16 traffic is never routed to the

192.168.x./0 networks, nor does it ever get NAT'd to the Internet.

The internal TCP traffic on the 192.168.x./0 networks (if allowed by the firewall access rules) is NAT'd to the external firewall interface address and state is maintained by the firewall for internally initiated connections (and similarly for externally initiated TCP connections). Bi-directional packet filter rules exist for UDP and ICMP traffic. The firewall contains routes to all hosts on the network, and because the SSL VPN is located in the DMZ firewall service network subnet, it is able to reach any 192.168.x. host in the network if the firewall access lists permit this (and also based on the SSL VPN user account permissions). This design enforces the defense-in-depth principle with as much granular access control as is reasonably possible.

Application of Defense-in-Depth Principles

Defense-in-depth principles were applied in the architecting of GIAC Enterprises' network and in the configuration of its network devices. Central to the defensive measures of the network is the application of filtering rules on the router and the use of an application proxy firewall that "denies what is not explicitly allowed". To further enhance the security of the network, numerous other security enhancements were made as follows:

- The elimination of the use of Telnet and FTP into, out of, or within the network. Instead, SSH and SCP/SFTP are used. If Telnet or FTP is absolutely necessary from a business perspective, it is temporarily configured for use and tunneled within the SSL VPN if at all possible.

- Split DNS was designed so that sensitive internal hostnames and IP information is not stored in the external DNS server cache, but rather in the internal DNS server. Zone transfers from the corporate office must occur through the SSL VPN and are initiated by the UNIX administrators with specific SSL VPN accounts that have those privileges. Zone transfers of the external DNS zone to the internal DNS server are allowed through the firewall and further locked down within the named.conf file on the external DNS server. The DNS servers are Sun Ultra5 servers running Solaris 9 and BIND version 9.3.0, are hardened and BIND is chroot'ed.

- NTP is used to keep time within the network using stratum 1 public time servers and an internal time server (192.168.3.4) is used as a stratum 2 server to serve time to all network appliances. Keeping time enforces standardization of timestamps within the audit logs on the GIAC network.

- The internal LAN user workstations are configured to use a proxy server to initiate outbound HTTP and HTTPS connections to the Internet. This allows for audits of web sites visited, blocking of certain sites and performance enhancement of browsing.

- The mail server, along with the proxy/NTP/DHCP and DNS server, is placed in a

firewall service network to isolate them from attack by both internal and external entities. Sophos anti-virus for UNIX is running on the Lotus Notes 6.5 mail server, as well as all Windows user workstations in the LAN. Similarly the other servers in the GIAC network, the mail and proxy/NTP/DHCP servers are running Solaris 9 on Sun Ultra10's.

- The Weblogic web/app and Oracle servers are also Solaris 9 hosts, but run on dual processor Ultra60's. They have been hardened and placed in the same firewall service network as the VMPS server. The VMPS server is running on an Ultra5. Placing these servers together isolates them from the DMZ servers as they contain customer, financial and other important data. The VMPS server is hardened and only listens on a handful of ports, including SSH and 1589/UDP (the VMPS daemon port).

- To keep the network secure, regular vulnerability assessments are performed and patches are applied as necessary.

Summary Tables of GIAC Enterprises Security Components

Device, Brand and Version	**Router**, Cisco 1711 (C1700-K9O3SY7-M) running IOS 12.3(7)XR3
Purpose of component	Route traffic to GIAC LAN and perform ingress/egress filtering and limited access control.
Security function performed	Blocks RFC1918 and GIAC internal IP addresses from ingressing network, spoofed addresses from leaving network, and certain traffic from entering/leaving network. Logs audit data to syslog server.
Placement affects function how?	The router should be placed in front of the firewall and connected to the firewall's external interface with a network tap to facilitate the in-lining of an IDS sensor. Doing so allows the router to ingress and egress filter all traffic inbound and outbound to/from the GIAC network.
What are security weaknesses or strengths of the component?	The weaknesses of the router include susceptibility to Cisco vulnerabilities that have not had a patch released. The other weakness of the router is that it allows all but a few protocols to the firewall's external interface. This was done to allow the firewall to firewall, as well as the IDS sensor hanging off the tap to capture traffic for inspection (which is a strength of the architecture). The other strength of the router is its ingress/egress filtering of RFC 1918, spoofed and other traffic that should be not allowed in or out of the GIAC network.
How are weaknesses mitigated using defense-in-depth?	The router weaknesses are mitigated by the firewall defenses and the fact that the firewall "denies all traffic that is not explicitly allowed".
Are there technical, budget or political reasons to use it?	GIAC has standardized on Cisco routers and switches due to Cisco's lion share of the market and financial stability of the company.

Device, Brand and Version	**Firewall**, Cyberguard FS600 Appliance Firewall, OS Version 5.1
Purpose of component	Allows traffic that has been permitted in access lists and denies all other traffic. Stateful application proxies are used when they exist, otherwise packet filters rules used.
Security function performed	Permits and denies traffic at each firewall interface according to access rules. Also inspects payloads of traffic that application proxies exist for against the applicable RFC. Logs audit data to syslog server.

Placement affects function how?	The firewall needs to be placed directly behind the router and at the ingress point into all subnets so that it may inspect and either proxy, pass or deny traffic both inbound and outbound (as well as allow stateful replies). By placing the firewall "before" the firewall service network servers, they are provided additional defense-in-depth with only a negligible impact on firewall performance from to the additional traffic load placed upon it.
What are security weaknesses or strengths of the component?	The weaknesses of the firewall include its use of a multi-level OS which does not lend itself to custom hardening of the box. The appliance comes pre-hardened from the vendor, and custom changes are difficult to introduce. The strengths include application proxies for many protocols, a GUI-driven system that allows for quick, easy configuration changes and the ability to remotely admin the firewall using SSH.
How are weaknesses mitigated using defense-in-depth?	The firewall weaknesses are not easy to mitigate due to the appliance nature of the box. Shell scripts may be written, and have been, to accomplish certain tasks (such as rotating logs on a more frequent basis when auditing is turned to the verbose setting).
Are there technical, budget or political reasons to use it?	Cyberguard provides many application level proxies that enhance security (over the few that a Cisco PIX provides), as well as being a hardened security appliance that can be fully installed and configured within a few hours. The security administrator's prior use and knowledge of Cyberguard firewalls was also a decision driver.

Device, Brand and Version	**SSL VPN**, Juniper Networks Netscreen Remote Access SSL VPN 500 RA-525, ScreenOS 5.0.0
Purpose of component	Allows all external entities, such as partners, remote employees (including admins), corporate, and satellite offices to remotely connect to GIAC in a secure fashion via an SSL tunnel.
Security function performed	Allows secure remote access to GIAC enterprises from external entities and remote employees. Also allows granular access control on an IP and port/application basis without the need for a VPN client and without the issues of NAT. Logs audit data to syslog server.
Placement affects function how?	The SSL VPN should be placed behind the router, and by placing it behind the firewall, additional defense-in-depth is achieved by it not being directly addressed by traffic allowed through the router. Again, some load is placed on the firewall due to this architectural decision, however the firewall is plenty robust enough in terms of connection capacity and processor/memory to handle the additional load.
What are security weaknesses or strengths of the component?	The weaknesses of the SSL VPN include the requirement to login from satellite sites and corporate, vs. a point-to-point IPSec tunnel that is "always" up. The strengths, however, greatly outweigh the weaknesses. SSL VPNs are not only secure, but much easier to manage, have very granular controls that can be imposed upon groups of users or individual users, and are clientless (only requiring a web browser).
How are weaknesses mitigated using defense-in-depth?	There is no mitigating defense other than going to a point-to-point IPSec tunnel for "always on" connectivity that will eliminate the need to always login to the SSL VPN. However, the default timeout on the SSL VPN session may be increased, or users can keep an application alive (like Lotus Notes) that will check for mail every x number of minutes and therefore keep the tunnel up (or a simple script can be written to ping a host that will accomplish this same task).
Are there technical, budget or political reasons to use it?	Juniper is one of the market leaders in the SSL VPN market. The security administrator's experience with the Cisco 3000 Concentrator's SSL VPN features was a driver not to use the Cisco. The Juniper was chosen due to its recommendation by the Meta Group and also in evaluating their product on-site.

Device, Brand and Version	**Switch**, Cisco 2950XL running IOS 12.1
Purpose of component	Allow hosts within a subnet to communicate with each other while utilizing ARP cache tables to minimize broadcast traffic. Also used to place consultants in a private VLAN using VMPS client capabilities.
Security function performed	Diminishes the risk of sniffing due to switching technology used. Also allows GIAC to employ VMPS to quarantine consultants into a private VLAN.
Placement affects function how?	Switches are generally placed in a subnet where multiple hosts need to communicate with each other on the same broadcast domain (VLAN). In the case of the VMPS client switch, the placement and VLAN'ing across the firewall is crucial to the implementation of VMPS and the isolation of consultants into the private VLAN 8. The switches also port mirror traffic to the IDS sensors.
What are security weaknesses or strengths of the component?	Weaknesses associated with switches include susceptibility to attack tools such as Dsniff, to attacks like VLAN jumping, and can be turned into a "hub" by ARP cache flooding. The strengths obviously include the use of VLANs to reduce broadcast traffic and make sniffing attacks more difficult than if a hub was used. Also inherent in switches are applications such as port access controls, VMPS, and ACLs.
How are weaknesses mitigated using defense-in-depth?	Hardening switches can mitigate switch weaknesses and implementing port security, as well relying on the IDS sensors to monitor for attacks. Also, do not use the native VLAN 1 on the switch.
Are there technical, budget or political reasons to use it?	GIAC has standardized on Cisco routers and switches due to Cisco's lion share of the market and financial stability of the company.

Device, Brand and Version	**IDS Sensor**, Sun Ultra5 running Solaris 9
Purpose of component	To promiscuously sniff LAN and WAN traffic and compare traffic against signatures for known attacks and other custom rules.
Security function performed	Monitors network for network-based attacks and logs data to a central syslog server. Also has the capability to notify administrators of an important attack. Can be used inline to kill TCP and UDP based attacks if so desired (using active-response or Hogwash).
Placement affects function how?	IDS sensors must be placed where they can sniff traffic based upon the ingress/egress point and/or particularly important hosts. In GIAC's case, the IDS sensor monitors all traffic that traverses the router and is bound for the external firewall interface via a network tap, as well as the other three subnets attached to the other three firewall interfaces via port spanning on the switches.
What are security weaknesses or strengths of the component?	IDS sensors suffer from having to compare attacks against known signatures. If a signature is not contained in the rule set for an attack, the attack may be missed. Sensors are also subject to dropping packets if not properly sized. The benefits include great insight into the traffic on the network with only a modest investment for GIAC, and technologies like active-response and intrusion prevention in general allow for more reactive measures as their technology matures.
How are weaknesses mitigated using defense-in-depth?	IDS sensors can be regularly updated with new signatures to mitigate the risk from not identifying an attack due to lack of a signature. Using properly sized hardware for the segment will also mitigate the risk of packet loss. Tuning of the IDS rule set, and custom IDS signatures, will greatly enhance the effectiveness of the IDS as well.
Are there technical, budget or political reasons to use it?	Due to the availability of spare Ultra5 servers sent from the corporate office, and the fact that Snort and ACID are open source software, cost was the primary driver in choice of the IDS sensor platforms and software. The security administrator's recommendation to use Snort was also taken into consideration.

Device, Brand and Version	**Syslog Server**, Sun Ultra5 running Solaris 9
Purpose of component	To serve as a central collection point for all audit logs from network devices. Also used to view IDS alerts and serve as a central master console for the IDS sensors which reside on a private, out-of-band network.
Security function performed	Serves as a central collection point for audit logs, which may be a requirement for any number of reasons (corporate policy, SOX compliance, government or financial regulations, etc.). GIAC also uses their syslog server as a console and administration host for their IDS sensors on an out-of-band network.
Placement affects function how?	The syslog server is less dependent upon placement in the network. However, by placing it on the internal LAN, it is protected from DMZ-type hosts in the firewall service subnets should they be compromised, and is reachable by all hosts in the network via port 514/UDP either directly or through the firewall. To further protect the syslog server from internal host attacks, it has been hardened as described previously in the syslog server discussion.
What are security weaknesses or strengths of the component?	Syslog servers must carefully be built with enough size in the /var partition so that they do not run out of disk space. Syslog is also subject to packet loss if using the default UDP method of delivery (vs. the use of syslog-ng that uses TCP). The strengths include the centralized collection of audit logs with little impact on the network. Syslog servers may also be hardened to the point that they only listen on port 514/UDP and a few other ports (like 22/TCP) to enhance their security defenses.
How are weaknesses mitigated using defense-in-depth?	Proper sizing of the /var partition, as well as ensuring it is its own partition (and not located under the root partition) will keep the /var partition from filling up too quickly and crashing. This also is greatly dependent upon the careful rotating of logs and the archival of rotated logs to keep the /var partition under a certain threshold in terms of size. GIAC also made the decision to live with the risk of dropped packets due to the use of UDP for syslog packet delivery.
Are there technical, budget or political reasons to use it?	The decision to use an Ultra5 and the resident syslog daemon in Solaris was also driven by cost savings and standardization upon a well supported operating system. The security administrator's knowledge of Solaris system administration was also taken in consideration.

Assignment 3: Router and Firewall Policies

Router

The following table shows the rules applied to **inbound** traffic on the external interface of the router. The security design and ordering of ACLs is to ingress filter RFC 1918 addresses, block traffic that should not be ingressing the GIAC router and network from the Internet (such as SNMP and TFTP), allow all traffic that was not blocked by the previous rules to the external interface of the firewall (which will proxy the traffic to the internal LAN and firewall service networks), and then deny all other traffic if it did not match a previous rule. [11] This ordering of the ACLs is critical to the router's application of its security policy.

The reason for the design of this access list is that traffic that is clearly not allowed on the GIAC network (RFC 1918 and SNMP/TFTP) from the Internet should be blocked at the router to provide defense-in-depth and take load off of the firewall. Traffic that is

bound for the firewall's external IP should be allowed, as a firewall should be allowed to firewall (and to log the denies to the syslog server with more detail than a router's syslog would provide). Any resulting traffic that has not matched a previous ACL is denied. Note that ICMP requests to the external interface of the router are allowed, whereas ICMP redirects are not.

Traffic violations are logged to the syslog server where applicable (based upon the severity of the violation subjectively determined by the router administrator).

ACL 101 Applied to Inbound Traffic on External Interface of Router

Interface	Source IP	Dest. IP	Service / Protocol	Action	Comments
External	10.0.0.0 0.255.255.255	any	ip	deny	Deny RFC1918 addresses. Log violations to syslog server when they occur.
External	172.16.0.0 0.15.255.255	any	ip	deny	Deny RFC1918 addresses. . Log violations to syslog server when they occur.
External	192.168.0.0 0.0.255.255	any	ip	deny	Deny RFC1918 addresses. . Log violations to syslog server when they occur.
External	66.x.y.4 0.0.0.3	any	ip	deny	Deny firewall subnet addresses from Internet. . Log violations to syslog server when they occur.
External	224.0.0.0 31.255.255.255	any	ip	deny	Deny multicast from Internet. . Log violations to syslog server when they occur.
External	169.254.0.0 .0.0.255.255	any	ip	deny	Deny traffic from DHCP clients that were not allocated an address
External	any	any	69/udp (TFTP)	deny	Deny TFTP from Internet. . Log violations to syslog server when they occur.

External	any	any	161/udp (SNMP)	deny	Deny SNMP from Internet. . Log violations to syslog server when they occur.
External	any	any	ICMP redirect	deny	Deny ICMP redirects from Internet. . Log violations to syslog server when they occur.
External	any	66.x.y.1	ICMP echo request	permit	Allow ICMP echo requests to the router from the Internet
External	any	66.x.y.6	ip	permit	Allow traffic to external interface of firewall not previously denied
External	any	any	ip	deny	Deny all other traffic from Internet. . Log violations to syslog server when they occur.

The following table shows the rules applied to **inbound** traffic on the internal interface of the router (vs. applying the ACL to outbound traffic). ICMP traffic that could be used to map the GIAC network is denied. Traffic to the internal interface of the firewall is allowed, with all other traffic being denied. The deny rule ensures egress filtering of spoofed addresses on the internal network takes place as a defense-in-depth measure, as the GIAC firewall would be the first line of defense in blocking spoofed addresses from internal hosts and servers. [11]

ACL 102 Applied to Inbound Traffic on Internal Interface of Router

Interface	Source IP	Dest. IP	Service/Protocol	Action	Comments
Internal	any	any	icmp time exceeded	deny	Deny ICMP time exceeded messages
Internal	any	any	icmp host unreachable	deny	Deny ICMP host unreachable messages
Internal	any	any	icmp echo reply	deny	Deny ICMP Echo Reply messages

Internal	66.x.y.6	any	ip	permit	Permit traffic from firewall (allows admins to SSH into SSL VPN from remote locations and then access router back through the firewall using SSH). **Note that all internal traffic is NAT'd to the external firewall address 66.x.y.6.**
Internal	any	any	ip	deny	Deny all other traffic Internet. . Log violations to syslog server when they occur.

Firewall

The following rules apply to the four different interfaces on the Cyberguard firewall. Each set of rules applies to traffic that ingresses the particular firewall interface. Note that the firewall itself must be given permission to perform an action (such as SSH to the syslog server), and that for TCP rules, stateful replies are inherent in the rule creation. For UDP and ICMP, two uni-directional rules must be created as statefulness is not inherent in these protocols. Also, except where noted that the UDP proxy was used, all UDP (and ICMP) rules are packet filter rules (and therefore do not have a proxy destination). For this reason, the "permit with stateful replies" option is not applicable to UDP packet filter rules.

All TCP based rules use either an existing pre-defined TCP proxy (such as those that exist for HTTP and SMTP) or a port-guard proxy (generic proxy used for non-standard and custom protocols).

The firewall rule set has a default deny rule at the end so that all traffic that is not explicitly allowed is denied. The ordering of the firewall rules is not significant to the enforcement of the access policies.

Traffic that ingresses external firewall interface (66.x.y.6)

Interface	Source IP	Dest. IP	Destination Port / Protocol	Proxy Dest.	Action	Comments
External Interface 66.x.y.6	any	66.x.y.6	80/TCP (HTTP)	Web/App Server (192.168.8.4)	permit with stateful replies	Firewall proxies connection to port 80 to web server

External Interface 66.x.y.6	any	66.x.y.6	443/TCP (HTTPS)	Web/App Server (192.168.8.4)	permit with stateful replies	Firewall proxies connection to port 443 to web server
External Interface 66.x.y.6	any	66.x.y.6	8080/TCP (HTTPS)	SSL VPN (192.168.3.6)	permit with stateful replies	Firewall proxies connection to port 8080 to SSL VPN
External Interface 66.x.y.6	any	66.x.y.6	53/UDP (DNS Queries)	External DNS Server (192.168.3.5)	permit	Firewall proxies connection to port 53 to external DNS server
External Interface 66.x.y.6	External DNS Server 192.168.3.5	any	UDP Ephemeral ports	Return destination is firewall where state has been established	permit	Return DNS traffic for DNS query replies
External Interface 66.x.y.6	Router 66.x.y.5	66.x.y.6	123/UDP (NTP)	Time Server (192.168.3.4)	permit	Permit router to get time from internal time server. Firewall proxies connection to NTP server
External Interface 66.x.y.6	NTP server 192.168.3.4	Router 66.x.y.5	123/UDP (NTP)	Return destination is firewall where state has been established	permit	Return NTP traffic (uses reflexive port 123/UDP)
External Interface 66.x.y.6	any	66.x.y.6	25/TCP (SMTP)	Mail Server (192.168.3.3)	permit with stateful replies	Firewall proxies connection to port 25 on mail server
External Interface 66.x.y.6	Router 66.x.y.5	66.x.y.6	514/UDP (Syslog)	Syslog Server (192.168.2.4)	permit	Firewall proxies syslog messages to syslog server (uni-directional rule)
External Interface 66.x.y.6	Router 66.x.y.5	66.x.y.6	ICMP Echo Request	N/A as traffic is between internal subnets	permit	Permit router to ping firewall

External Interface 66.x.y.6	Firewall 66.x.y.6	Router 66.x.y.5	ICMP Echo Reply	N/A as traffic is between internal subnets	permit	Permit ICMP echo replies to router

Traffic that ingresses DMZ firewall service network interface (192.168.3.1)

Interface	Source IP	Dest. IP	Destination Port / Protocol	Proxy Dest.	Action	Comments
DMZ Firewall Service Network Interface 192.168.3.1	any	Internet	80/TCP (HTTP)	N/A as firewall proxies connections to Internet	permit with stateful replies	Firewall proxies connection to port 80 to Internet. Used for obtaining patches.
DMZ Firewall Service Network Interface 192.168.3.1	any	Internet	443/TCP (HTTPS)	N/A as firewall proxies connections to Internet	permit with stateful replies	Firewall proxies connection to port 443 to Internet. Used for obtaining patches.
DMZ Firewall Service Network Interface 192.168.3.1	NTP Server 192.168.3.4	timegps.net 69.228.59.2 otc1.psu.edu 128.118.46.3	123/UDP (NTP)	69.228.59.2 or 128.118.46.3 using UDP Proxy available in Cyberguard	permit	Firewall and internal hosts allowed to get time from public time servers. Firewall proxies outbound connections.
DMZ Firewall Service Network Interface 192.168.3.1	timegps.net 69.228.59.2 otc1.psu.edu 128.118.46.3	NTP Server 192.168.3.4	123/UDP (NTP)	Time Server (192.168.3.4) using UDP Proxy available in Cyberguard	permit	Return NTP traffic (uses reflexive port 123/UDP). Firewall proxies return traffic.
DMZ Firewall Service Network Interface 192.168.3.1	Hosts on 192.168.3.0 network	Syslog server 192.168.2.4	514/UDP (Syslog)	N/A as traffic is between internal subnets	permit	Uni-directional syslog traffic to syslog server

DMZ Firewall Service Network Interface 192.168.3.1	Mail server 192.168.3.3	Internet	25/TCP (SMTP)	N/A	permit with stateful replies	Firewall proxies connection to port 25/TCP to Internet
DMZ Firewall Service Network Interface 192.168.3.1	SSL VPN 192.168.3.6	Firewall and all other hosts in 192.168.x.0 networks	22/TCP 80/TCP 443/TCP	Determined during SSL VPN by session by user and permitted or denied based upon VPN rules	permit with stateful replies	Firewall proxies connections to ports from remote SSL VPN sessions
DMZ Firewall Service Network Interface 192.168.3.1	SSL VPN 192.168.3.6	Firewall and all other hosts in 192.168.x.0 networks	53/UDP	N/A as traffic is between internal subnets	permit	DNS queries to internal DNS server. SSL VPN allows connections to internal hosts for SSH access, and name information is only stored on internal DNS server (since split-DNS has been utilized).
DMZ Firewall Service Network Interface 192.168.3.1	Firewall and all other hosts in 192.168.x.0 networks	SSL VPN 192.168.3.6	UDP Ephemeral ports	N/A as traffic is between internal subnets	permit	Return DNS traffic
DMZ Firewall Service Network Interface 192.168.3.1	Hosts in 192.168.3.0 network	Firewall 192.168.3.1	ICMP Echo Request	N/A as traffic is between internal subnets	permit	Permit hosts to ping firewall
DMZ Firewall Service Network Interface 192.168.3.1	Firewall 192.168.3.1	Hosts in 192.168.3.0 network	ICMP Echo Reply	N/A as traffic is between internal subnets	permit	Permit ICMP echo replies to hosts

Traffic that ingresses VMPS firewall service network interface (192.168.8.1)

Interface	Source IP	Dest. IP	Destination Port / Protocol	Proxy Dest.	Action	Comments
VMPS Firewall Service Network Interface 192.168.8.1	any	Internet	80/TCP (HTTP)	N/A	permit with stateful replies	Firewall proxies connection to port 80 to Internet. Used for obtaining patches.
VMPS Firewall Service Network Interface 192.168.8.1	any	Internet	443/TCP (HTTPS)	N/A	permit with stateful replies	Firewall proxies connection to port 443 to Internet. Used for obtaining patches.
VMPS Firewall Service Network Interface 192.168.8.1	All hosts in 192.168.8.0 network	Syslog server 192.168.2.4	514/UDP (Syslog)	N/A as traffic is between internal subnets	permit	Hosts in 192.168.8.0 network allowed to syslog to syslog server
VMPS Firewall Service Network Interface 192.168.8.1	All hosts in 192.168.8.0 network	NTP Server 192.168.3.4	123/UDP (NTP)	N/A as traffic is between internal subnets	permit	Hosts in 192.168.8.0 network allowed to get time from NTP server
VMPS Firewall Service Network Interface 192.168.8.1	NTP Server 192.168.3.4	Hosts in 192.168.8.0 network	123/UDP (NTP)	N/A as traffic is between internal subnets	permit	Return NTP traffic (uses reflexive port 123/UDP)
VMPS Firewall Service Network Interface 192.168.8.1	Hosts in 192.168.8.0 network	DHCP server 192.168.3.4	68/UDP (BOOTPC)	N/A as traffic is between internal subnets	permit	Permit DHCP traffic
VMPS Firewall Service Network Interface 192.168.8.1	DHCP server 192.168.3.4	Hosts in 192.168.8.0 network	UDP Ephemeral hosts	N/A as traffic is between internal subnets	Permit	Permit return DHCP traffic

VMPS Firewall Service Network Interface 192.168.8.1	Hosts in 192.168.8.0 network	Firewall 192.168.8.1	ICMP Echo Request	N/A as traffic is between internal subnets	permit	Permit hosts to ping firewall
VMPS Firewall Service Network Interface 192.168.8.1	Firewall 192.168.8.1	Hosts in 192.168.8.0 network	ICMP Echo Reply	N/A as traffic is between internal subnets	permit	Permit ICMP echo replies to hosts

Traffic that ingresses internal LAN firewall interface (192.168.2.1)

Interface	Source IP	Dest. IP	Destination Port / Protocol	Proxy Dest.	Action	Comments
Internal LAN Firewall Interface 192.168.2.1	Hosts in 192.168.2.0 network	Internet and VMPS firewall service network and DMZ firewall service network	80/TCP (HTTP)	Proxy server (192.168.3.4)	permit with stateful replies	Firewall proxies connection to port 80 to Internet. Must use proxy server (192.168.3.4)
Internal LAN Firewall Interface 192.168.2.1	Hosts in 192.168.2.0 network	Internet and VMPS firewall service network and DMZ firewall service network	443/TCP (HTTPS)	Proxy server (192.168.3.4)	permit with stateful replies	Firewall proxies connection to port 443 to Internet. Must use proxy server (192.168.3.4)

Internal LAN Firewall Interface 192.168.2.1	Hosts in 192.168.2.0 network	Firewall and all other hosts in 192.168.x.0 networks	22/TCP (SSH)	N/A	permit with stateful replies	Firewall proxies connections to port 22/TCP on internal hosts. Used for administratio n purposes between all subnets, if necessary (vs. allowing DMZ subnet to initiate SSH connections to VMPS network).
Internal LAN Firewall Interface 192.168.2.1	Hosts in 192.168.2.0 network	Mail server 192.168.3.3	1352/TCP (Lotus Notes)	Mail server (192.168.3.3)	permit with stateful replies	Firewall proxies connection to port 1352 to mail server
Internal LAN Firewall Interface 192.168.2.1	Internal LAN hosts	DHCP server 192.168.3.4	68/UDP (BOOTPC)	N/A as traffic is between internal subnets	permit	Permit DHCP traffic
Internal LAN Firewall Interface 192.168.2.1	DHCP server 192.168.3.4	Internal LAN hosts	UDP Ephemeral hosts	N/A as traffic is between internal subnets	Permit	Permit return DHCP traffic
Internal LAN Firewall Interface 192.168.2.1	Hosts in 192.168.2.0 network	Firewall 192.168.2.1	ICMP Echo Request	N/A as traffic is between internal subnets	permit	Permit hosts to ping firewall
Internal LAN Firewall Interface 192.168.2.1	Firewall 192.168.2.1	Hosts in 192.168.2.0 network	ICMP Echo Reply	N/A as traffic is between internal subnets	permit	Permit ICMP echo replies to hosts
Internal LAN Firewall Interface 192.168.2.1	Internal DNS server 192.168.2.3	External DNS server 192.168.3.5	53/TCP DNS Zone Transfer	External DNS server (192.168.3.5)	permit with stateful replies	Permit zone transfer of external zone map on external DNS server to internal DNS server

Traffic that originates from firewall

Interface	Source IP	Dest. IP	Destination Port / Protocol	Proxy Dest.	Action	Comments
DMZ Firewall Interface 192.168.2.1	Firewall 192.168.3.1	NTP Server 192.168.3.4	123/UDP (NTP)	N/A	permit	Firewall retrieves time from NTP server
DMZ Firewall Interface 192.168.2.1	NTP Server 192.168.3.4	Firewall 192.168.3.1	123/UDP (NTP)	N/A	permit	Return NTP traffic (uses reflexive port 123/UDP
DMZ Firewall Interface 192.168.2.1	All Firewall Interfaces	All 192.168.x.0 hosts and 66.x.y.5 router interface	ICMP Echo Request	N/A	permit	Permit hosts to ping firewall
DMZ Firewall Interface 192.168.2.1	All 192.168.x.0 hosts and 66.x.y.5 router interface	All Firewall Interfaces	ICMP Echo Reply	N/A	permit	Permit ICMP echo replies to hosts
DMZ Firewall Interface 192.168.2.1	Firewall 192.168.2.1	Syslog server 192.168.2.4	514/UDP (Syslog)	N/A	permit	Firewall syslogs messages to syslog server (uni-directional only)
External Firewall Interface 66.x.y.6	Firewall 66.x.y.6	Internet	80/TCP (HTTP)	N/A	permit with stateful replies	Firewall connections to Internet. Used for obtaining patches.
External Firewall Interface 66.x.y.6	Firewall 66.x.y.6	Internet	443/TCP (HTTPS)	N/A	permit with stateful replies	Firewall connections to Internet. Used for obtaining patches.

Appendix 1 – OpenVMPS Default VLAN Configuration File

root@grace:/export/home/downloads/software/vmpsd>cat vlan.db

```
!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode { open | secure }
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req { allow | deny }
!
! The default value is allow.

vmps domain mydomain
vmps mode open
vmps fallback --NONE--
vmps no-domain-req deny

!MAC Addresses

vmps-mac-addrs
!
! address <addr> vlan-name <vlan_name>

! netreg extension - default vlan
address 0010.a49f.30e1 vlan-name --DEFAULT--
! disabled - no access
address 0010.a49f.30e2 vlan-name --NONE--
! vlan TEST restricted
address 0010.a49f.30e3 vlan-name TEST
! vlan TEST1 unrestricted
address 0010.a49f.30e4 vlan-name TEST1

!Port Groups
!
!vmps-port-group <group-name>
! default-vlan <vlan-name>
! fallback-vlan <vlan-name>
! device <device-id> { port <port-name> | all-ports }

vmps-port-group myswitch
  default-vlan  VLAN1
  fallback-vlan VLAN2
  device 10.0.0.1 port 2/4
  device 10.0.0.2 all-ports

!VLAN groups
!
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>

vmps-vlan-group myvlans
  vlan-name TEST

!VLAN port Policies
!
!vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
! { port-group <group-name> | device <device-id> port <port-name> }
```

```
vmps-port-policies vlan-group myvlans
  port-group myswitch
```

Appendix 2 – SIM Syslog Parsing Script (log_parse.pl)

```
#!/bin/perl -w
use strict;

######################################################################
# Program: log_parse.pl
# Purpose: Parse through consolidated syslog file and create specific files to further investigate
#          based upon device and/or criticality of the alert.
#
#       The script also supports entering regex arguments and operators and builds the regex search string for you
#        and outputs a file as well as STDOUT.
#       There are formatting rules to follow. See the syntax and examples below.
#
# Author: Jeff Holland
# Date of Creation: 11/13/04
#
# Usage:  (note that log_parse.pl and Syslog file must be in same directory. You may run the
#       script on any syslog file, but it is primarily built for the GIAC SyslogCatchAll file.)
#
#     log_parse.pl SyslogCatchAll
# **OR**
#     log_parse.pl SyslogCatchAll regex <operator in double quotes | string>
#     <operator in double quotes | string> <operator in double quotes | string> ...
#
#     Operators: ! == "NOT", && == "AND", || = "OR"
#
#     Examples:
#           (1) log_parse.pl SyslogCatchAll regex IDS "||" DMZ
#              NOTE: This searches the syslog file for the strings IDS or DMZ and returns any line
#                  that contains either (or both) of these strings
#
#           (2) log_parse.pl SyslogCatchAll regex "!" IDS "&&" 10.1.1.198
#              NOTE: This searches the syslog file for the strings that do not contain "IDS" and does
#                  contain "10.1.1.198" and returns the line that match that string. Note that you
#                  don't need the quote around the IP address, unless you wanted to add a single space
#                  or something, like "10.1.1.198 ".
#
#           (3) log_parse.pl SyslogCatchAll regex "!" IDS "&&" 10.1.1.198 "&&" " 16:00"
#              NOTE: This searches the syslog file for the strings that do not contain "IDS" and does
#                  contain "10.1.1.198" and a time that starts 16:00 (the and returns the line that
#                  space between the double quote and 16 is necessary so you don't pick up times like
#                  12:16:00).
#
#           (4) log_parse.pl SyslogCatchAll regex "!" IDS "&&" 10.1.1.198 "&&" "L2L:\s+XtericVPN"
#              NOTE: This searches the syslog file for the strings that do not contain "IDS" and does
#                  contain "10.1.1.198" and the string "L2L:  XtericVPN". Note that for multiple spaces
#                  in your search string, you MUST use the regular expression "\s+", which means to search
#                  for 1 or more space characters.
#
#           (5) log_parse.pl SyslogCatchAll regex "11-15-2004.*tcp"
#              NOTE: This uses a pure regex expression to search for any string that starts with 11-15-2004,
#              has any amount of characters in between and ends with tcp. Note that any regex can be used as a
#              search parameter if the syntax is correct. Be sure to put regex's in double quotes, though.
#
#  REMEMBER: You MUST put binary operators in double quotes!!!!!!!!!!!!!!!!!!!
#
######################################################################
```

```
open (LOG, "$ARGV[0]") || die "Can't open Syslog file. Pass the file as an argument to the log_parse.pl script.";
system `touch ids_alerts tcp_udp_denies vpn_alerts misc_alerts vpn_users_report regex_alerts`;
if (-s "ids_alerts" || -s "tcp_udp_denies" || -s "vpn_alerts" || -s "misc_alerts || -s vpn_users_report" || -s
"regex_alerts")
      { system `rm ids_alerts tcp_udp_denies vpn_alerts misc_alerts vpn_users_report regex_alerts`; }
my $counter = 2; #counter starts at 2 for the case where a regex is entered.
my $regex = &arg_builder ($counter); #call regex argument builder subroutine

while (<LOG>)
 {
  chomp $_;

 if ($ARGV[0] && !$ARGV[1]) #only one argument, the syslog file
  {

  if (/IDS/)
   {
    open (IDS_ALERTS, ">>ids_alerts");
    s/\s+/ /g; #clean up the white space
    print IDS_ALERTS "$_\n";
   }

  elsif (/Deny/)
   {
    s/\s+/ /g; #clean up the white space
    open (TCP_UDP_DENIES, ">>tcp_udp_denies");
    print TCP_UDP_DENIES "$_\n";
   }

   elsif ((/IPSEC/i) || (/IKE/i) || (/ISAKMP/i))
   {
    s/\s+/ /g; #clean up the white space
    open (VPN_ALERTS, ">>vpn_alerts");
    print VPN_ALERTS "$_\n";
    open (VPN_USERS_REPORT, ">>vpn_users_report");
     if (/Group\s\[(\w+)\]\sUser\s\[(\w+)\]\sConnection\sterminated/)  #Show terminated connections
      {
       my $group = $1;
       my $user = $2;
       my @temp_array = split /\s/, $_;
       print VPN_USERS_REPORT "$temp_array[0] $temp_array[1] Terminated Group is: $group, Terminated
User is: $user\n";
      }

     elsif (/IPSEC\[(\w+)\]:(\w+)\sIncoming\sclient/)  #Show initial logins
      {
       my $user = $1;
       my @temp_array = split /\s/, $_;
       print VPN_USERS_REPORT "$temp_array[0] $temp_array[1] IPSEC User is: $user\n";
      }
   }

  else
   {
    s/\s+/ /g; #clean up the white space
    open (MISC_ALERTS, ">>misc_alerts");
    print MISC_ALERTS "$_\n";
   }

 } #end of if loop for only one argument
```

Now handle the case where we have at least two arguments, syslogcatchall and at least one search string, and 2nd argument must be a series of strings starting with "regex" and can contain with binary operators for a regex search if enclosed in double quotes. This is the more powerful search option for the script, and can be run on the syslog files created from running the script without the "regex" option.

```
 elsif ($ARGV[0] && $ARGV[1] eq "regex")
  {
    if (eval($regex))
     {
      #print "regex is: $regex\n"; #for debugging only
      s/\s+/  /g; #clean up the white space
      print "$_\n\n";
      open (REGEX_ALERTS, ">>regex_alerts");
      print REGEX_ALERTS "$_\n\n";
     }
  } #end of elsif for multiple arguments
}  #end of while loop

### Build regex search string using subroutine. This is done only once (when the script is run), vs. for every line in the file if done inside the while loop.

sub arg_builder
 {
   if (!$ARGV[1]) {$ARGV[1]="";} #hack to handle only one arg so error does not print out from this function
   if ($ARGV[0] && $ARGV[1] eq "regex")
    {
     my @temp_array;
     my $temp_val;
     my $index = 0;
     while ($counter < 14 && $ARGV[$counter]) #handle up to 12 search strings/binary operators (counter starts at 2)
      {
       if ($counter == 2) #Special case for first time through loop
        {
          if ($ARGV[$counter] eq "!") {$temp_val = "$ARGV[$counter]";}

          elsif (($ARGV[$counter] eq "||") || ($ARGV[$counter] eq "&&")) {print "First arg can't be || or &&\n"; exit;}

          else {$temp_val = "/$ARGV[$counter]/";}

          $temp_array[$index] = $temp_val;
          $index++;
        }

       else
        {
          if ($ARGV[$counter] eq "!") {$temp_val = "$ARGV[$counter]";}

                elsif (($ARGV[$counter] eq "||") || ($ARGV[$counter] eq "&&")) {$temp_val = "$ARGV[$counter]";}

                else {$temp_val = "/$ARGV[$counter]/";}

          push (@temp_array, $temp_val);
        }
       $counter++;
      } #end of while loop

       ####Now assign regex from argument array
       my $array_vals = "@temp_array";
       $_ = $array_vals;
```

```
        $array_vals =~ s/! \//!\//g; #clean up the white space in the entire regex
        $array_vals = $array_vals; #clobber variable on purpose to force return value to be $array_vals string

    } #end of if loop on ARGs

  elsif ($ARGV[0] && $ARGV[1] && $ARGV[1] ne "regex")
    {
      print "\n   The 2nd argument was not \"regex\". Did you forget to type \"regex\"?\n\n";
      exit;
    }

  } #end of arg_builder function. Return value is regex expression string stored in $array_vals.
```

References

[1] Cisco, “Troubleshooting the Catalyst VMPS Switch”, URL: http://www.cisco.com/warp/public/473/157.html, (January 15, 2005)

[2] Cisco, “VLAN Membership Policy Server (VMPS) / Dynamic VLANs”, URL: http://www.cisco.com/en/US/tech/tk389/tk814/tk839/tech_protocol_home.html, (January 15, 2005)

[3] SourceForge.net, OpenVMPS vmpsd vlan config file, vlan.db file, URL: http://sourceforge.net/projects/vmps (January 15, 2005)

[4] Cisco, “Configuring Dynamic VLAN Membership” URL: http://www.cisco.com/en/US/products/hw/switches/ps637/products_configuration_guide_chapter09186a008007f03c.html#xtocid255797 (January 16, 2005)

[5] Fischback, Nicolas and Lacoste-Seris, Sabastien, “Protecting your IP Network Infrastructure”, URL: http://www.securite.org/presentations/secip/BHAMS2001-SecIP-v105.ppt, Pages 3 – 6, (January 17, 2005)

[6] Cisco, “Cisco 1700 Series Modular Access Routers”, URL: http://www.cisco.com/en/US/products/hw/routers/ps221/products_data_sheet09186a00801a030a.html, (January 17, 2005)

[7] Cyberguard.com, “Cyberguard FS600 Firewall/VPN Datasheet”, URL: http://www.cyberguard.com/include/pdf/fs300_600.pdf, (January 20, 2005)

[8] Cisco, “Configuring SPAN”, URL: http://www.cisco.com/en/US/products/hw/switches/ps637/products_configuration_guide_chapter09186a008007e838.html#xtocid22, (January 19, 2005)

[9] Juniper Networks, “Juniper Networks NetScreen-Remote Access 500 Series”, URL: http://www.juniper.net/products/ssl/dsheet/110029.pdf, (January 19, 2005)

[10] Javvin.com, “CDP: Cisco Discovery Protocol”, URL: http://www.javvin.com/protocolCDP.html, (January 20, 2005)

[11] GIAC, Stout, Kent, “GIAC Certified Firewall Analyst (GCFW) Practical Assignment Version 1.7”, URL: http://www.giac.org/practical/Kent_Stout_GCFW.doc, (January 20, 2005)

[12] boran.com, Boran, Sean, “Hardening Solaris with Jass”, URL: http://www.boran.com/security/sp/Solaris_hardening4.html, (January 21, 2005)

[13] Snort.org, “SNORT• ACID install on Solaris9“, URL: http://www.snort.org/docs/snort-acid_solaris9.pdf, (January 22, 2005)

[14] Cisco.com, “Securing Networks with Private VLANs and VLAN Access Control Lists” URL: http://www.cisco.com/warp/public/473/90.shtml, (February 27, 2005)

[15] Cisco.com, “Configuring VLAN ACLs”, URL: http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080160a7e.html (March 4th, 2005)

[16] Cisco “Configuring VLAN ACLs”, URL: http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00801679f8.html#wp1359352 (March 4th, 2005)

[17] NSA, “Cisco IOS Security Configuration Guide”, URL: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/switch-guide-version1_01.pdf (March 4th, 2005)