Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW)

Practical Assignment

(version 4.0)

VLANs and their Contribution to Perimeter Defence
&
A Secure Network Architecture for GIAC Enterprises

By: Jon King

Submitted: 24th February 2005

Table of Contents

Abstract

This paper is submitted to satisfy the written assignment required as part of certification for the SANS GCFW. The paper is presented in three sections.

Section one outlines three ways in which VLANs can be used to enhance perimeter defences. Each defence method is explained, example configurations are provided, and the relative merits and drawbacks of each are explored.

Section two proposes a secure network architecture for the imaginary company GIAC Enterprises. Objectives are first outlined followed by a discussion of design considerations. An explanation of the proposed architecture and components is then presented along with supporting tables and diagrams. This is followed by a detailed treatment of the necessary per port/protocol access permissions. The adherence of the design to the principles of defence in depth is appraised as are some shortcomings in the design and the steps taken to alleviate them.

Section three presents a detailed configuration for the primary firewall used in the secure network architecture proposed in section two. The reasoning behind many aspects of the configuration, including the sequencing, is explained. Finally an explanation of some salient items in the configuration is given.

1. VLANs and their Contribution to Perimeter Defence

For many modern networks, securing hosts in a DMZ poses a particular challenge because they are both difficult to protect and at the same time very prone to attack. Since DMZs sit near the perimeter of a network it is often difficult to provide the multiple layers of security called for by the principles of defence in depth. A robust firewall performing stateful inspection is a good start as are ingress and egress access controls on the border router. Hardening of operating systems and application software on DMZ hosts will defeat many attacks, often at zero cost. However, the security-minded administrator will demand one or more additional layers of security. Enter VLANs!

Virtual LANs (VLANs) are a well-established and world-proven fundamental of Ethernet local-area networks (LANs). However, their contribution to layered perimeter security is often overlooked or at least undervalued. This section outlines three ways in which VLANs can be utilised to improve security at the perimeter of a network and to add an extra layer of segregation and classification to traffic crossing inter-network boundaries. This paper will highlight the capabilities of VLANs when deployed on Cisco switches. However, it is possible that switches from other vendors will support some if not all the features discussed.

1.1. Overview of VLANs

It is assumed that the reader is familiar with the basic advantages in segregating switched Ethernet networks using VLANs rather than using physically discrete switches or (worse) employing a single, flat broadcast domain without VLANs. It is also assumed that the reader has a basic understanding of Cisco extended ACLs. All examples are presented using Cisco IOS which seems to be gaining increasing popularity over CatOS with network and security administrators. However, most if not all the examples may also be achieved using CatOS.

Ethernet VLANs are defined by the IEEE 802.1q standard[1]. The standard calls for four additional bytes of data to be added to the standard Ethernet header, including a 12-bit region to be used to designate VLAN membership. In theory therefore, up to 4096 unique VLANs can be created on a switch. In reality however, this number is reduced by hardware capabilities and the use by Cisco of certain VLAN numbers for reserved or otherwise special functions.

Some of the more obvious security applications of VLANs are well documented. Many network architects use VLANs to segregate those users and departments that have no need to converse with one another. For example in a company of several hundred users it is likely that there are specific sales, engineering, finance and marketing departments. Usually the workstations of end-users in one department will have no need to converse with workstations of end-users in other departments; rather they will only need to communicate with workstations in their own department plus shared central hosts such as file, print and email servers as well as network gateways such as routers and firewalls. It therefore makes good sense to separate these departments into separate IP subnets and separate VLANs. An

immediate benefit of this separation is that if a workstation in one department becomes infected with a network-aware worm, users in the other departments are not at direct risk as no inter-departmental communications are permitted.

Basic access control between hosts is usually enforced at a layer 3 network gateway such as a router or firewall using information read from the layer 3 and layer 4 headers of each packet. Since VLANs operate at layer 2, the switches that provide the VLANs cannot perform 'traditional' access control so hosts in a VLAN usually have no access controls between one another and are generally accepted to have similar security exposures and impacts. However, hosts in a VLAN are often not of comparable security exposures and/or impacts. Furthermore even if the hosts are comparable, it is possible that they may not need to communicate using more than a handful of protocols or even at all. Therefore it would clearly be of great value to be able to enforce access controls within a VLAN as well as at the network gateway for that VLAN. This would help to mitigate the problem of undesirable intra-VLAN communications and add a valuable extra layer of security.

This section will outline three applications of VLANs and indicate how they can be employed to improve defence in depth. Particular consideration will be given to how these VLAN applications can benefit security at the network perimeter but in many cases they would also be suitable for implementation closer to the network core.

It is worth noting at this point that VLANs, and in particular Cisco's implementation of VLANs, have a chequered history and have been the subject of several high profile vulnerabilities and weaknesses in default configurations. Two noteworthy examples are the native VLAN (VLAN1) trunking vulnerability[2] and the VLAN hopping attack using a double-encapsulated 802.1q Ethernet header (aka q-in-q)[3]. It is clear that VLAN segregation is not as secure as physical segregation using dedicated switches but in many situations, dedicated switches are not an option. The ability to configure VLANs securely and to employ some of their more advanced capabilities is a valuable tool in any security administrator's repertoire.

1.2. Private VLANs (PVLANs)

Private VLANs allow a network architect to control communication between hosts within the same VLAN on a per-host basis. By designating certain ports within a PVLAN as different types, various degrees of layer 2 segregation of those ports can be achieved. PVLANs can be used to provide simple but effective segregation between hosts that should not need to communicate with one another. This has the benefit of preventing many types of unauthorised intra-DMZ communications meaning that if one host is compromised, any efforts by the intruder to compromise other DMZ hosts now that he or she is 'inside the firewall' will be hampered.

1.2.1. PVLAN basics

There are three types of PVLAN ports and each port in a PVLAN is configured as one (and only one) of the three types:

- **Promiscuous:** A promiscuous port can communicate with all ports in that

PVLAN.

- **Isolated:** An isolated port can only communicate with the promiscuous port(s) in that PVLAN. Note that this is not the same as a PVLAN edge (protected port), which only has local significance (ie on a single switch).
- **Community:** A community port can communicate with other ports in the same community and PVLAN, and the promiscuous ports in that PVLAN. More than one community may be used in a PVLAN but an individual port can only be a member of one community.

The PVLAN ports are then associated with underlying VLANs:

- A **primary VLAN** carries communications from promiscuous ports to isolated ports, community ports and any other promiscuous ports in a given PVLAN.
- An **isolated VLAN** caries communications between isolated port(s) and the promiscuous port(s) in that PVLAN.
- A **community VLAN** carries communications between ports in a given community and their associated promiscuous port(s). As with community ports, there can be more than one community VLAN within a primary VLAN.

Isolated and community VLANs are collectively known as secondary VLANs. PVLANs can traverse VLAN trunks so are also suitable for distributed switched environments. As with regular VLANs, if a host in a PVLAN needs to communicate with another host in a different PVLAN, an intermediate layer 3 device is required.

1.2.2. Example of PVLAN implementation

The best way to illustrate the usefulness of PVLANs is by example. Consider the pre-existing network illustrated in Figure 1.

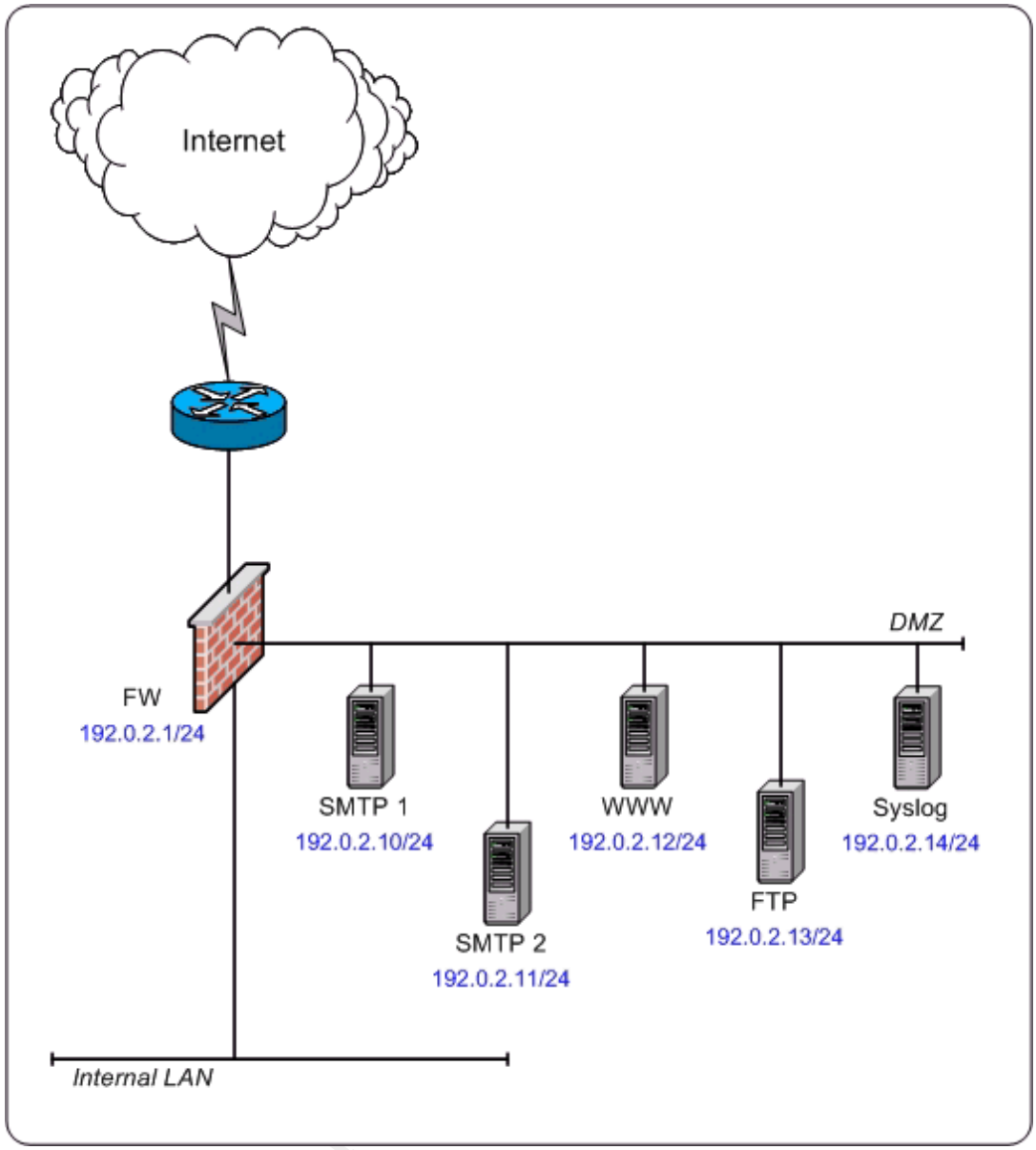

Figure 1: Example network using PVLANs

If a security consultant were brought in and tasked with improving the perimeter security of this imaginary network he or she may first consider splitting the servers onto multiple physical DMZs so that each type of service (SMTP, WWW, FTP, etc) has a dedicated DMZ. However, this might not be an option due to limitations in the firewall hardware, reluctance to re-address servers or any other reason. In such an instance PVLANs could be a useful means of adding an extra layer of security to the existing network architecture, thus helping to provide defence in depth.

Let us assume that only the following DMZ communications are necessary:

- The two SMTP servers need to communicate with one another
- All servers need to send log messages to the syslog server
- All servers need to communicate with hosts outside the DMZ

The above assumptions are quite reasonable. In most DMZ scenarios an FTP

server will not need to send email, a web server will not need to transfer files to/from the FTP server, and so on. In such a case PVLANs may be considered as a way of further segregating the DMZ hosts *in situ*, ie without re-addressing or any physical changes being required. Based on the assumptions above we can segregate this DMZ as follows:

Firewall	Promiscuous *NB: Layer 3 devices will almost always use promiscuous ports*	Primary *NB: Layer 3 devices will almost always use the primary VLAN*	100
SMTP1	Community	Community	101
SMTP2	Community	Community	101
WWW	Isolated	Isolated	102
FTP	Isolated	Isolated	102
Syslog	Promiscuous	Primary	100

Table 1: PVLAN types and numbers for the example network

We can configure PVLAN controls as follows. First the VTP mode must be set to transparent.

```
vtp mode transparent
```

The primary and secondary VLANs are created as per Table 1.

```
vlan 100
 name Primary VLAN
 private-vlan primary
!
vlan 101
 name Community VLAN
 private-vlan community
!
vlan 102
 name Isolated VLAN
 private-vlan isolated
```

The two secondary VLANs are then associated with the primary VLAN.

```
vlan 100
 private-vlan association 101,102
```

Finally the switch port types are set and mapped to the appropriate VLANs.

```
interface FastEthernet0/1
 description Connection to Firewall
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 100 101,102
!
interface FastEthernet0/2
 description Connection to SMTP1
 switchport mode private-vlan host
 switchport private-vlan host-association 100 101
!
interface FastEthernet0/3
```

```
 description Connection to SMTP2
 switchport mode private-vlan host
 switchport private-vlan host-association 100 101
!
interface FastEthernet0/4
 description Connection to WWW
 switchport mode private-vlan host
 switchport private-vlan host-association 100 102
!
interface FastEthernet0/5
 description Connection to FTP
 switchport mode private-vlan host
 switchport private-vlan host-association 100 102
!
interface FastEthernet0/6
 description Connection to Syslog
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 100 101,102
```

Once the above configuration is implemented, the secondary VLAN ports are isolated at layer 2 and can only send frames to specific other ports that the administrator has deemed appropriate. The WWW and FTP servers will each only be able to communicate with the syslog server and hosts beyond the firewall. Similarly, the two SMTP servers will only be able to communicate with one another, the syslog server and hosts beyond the firewall.

1.2.3. Limitations of PVLANs

There is a noteworthy limitation with PVLANs in that a layer 3 device can forward traffic between isolated ports. If a host on an isolated port is compromised, an intruder may be able to send traffic in such a way that it goes from the compromised host to the gateway router or firewall (which will be on a promiscuous port) and is then routed back out the same interface to a host on a different isolated port. This would require the attacker to set a false ARP entry on the compromised host or set a static route to a host in the local subnet (not all operating systems will accept this). However, this limitation would only be present in a poorly implemented solution. The router or firewall should be configured with ingress access controls to block traffic destined for the local subnet.

PVLANs are most appropriate when IP re-numbering is not an option or there is no suitable layer 3 device available to terminate a trunk (see 1.4). PVLANs do not offer very granular access control. For example, in the example used in 1.2.2, should any of the SMTP, WWW or FTP servers become compromised there is no protection at all between the compromised server and both the syslog server and the firewall. Other applications of VLANs offer more granular controls as per protocol ACLs and even application-layer firewalling can be applied between or within VLANs, as will be discussed in 1.3 and 1.4.

When PVLANs are deployed, the VTP mode must be set to transparent so a VTP server cannot be used. This means that in an architecture deploying multiple switches, all VLANs must be manually configured on each switch. Furthermore, if

trunking is used between switches, all secondary VLAN traffic will traverse the trunk, which is likely to be an unwelcome side-effect.

Port security cannot be configured on ports that are members of a PVLAN[4]. This means that the consultant will need to contrast the relative security merits gained by PVLANs versus MAC-based access control. The physical security of the room(s) housing the switch and its connected hosts is likely to be a decisive factor here.

1.3. VLAN Access Control Lists (VACLs)

VLAN access control lists allow a network architect to apply flexible and highly granular controls on network communications traversing a suitable switch. Since VACLs are only available on higher-end Cisco switches, they may not be available at many network perimeters. However, if the architect is fortunate enough to have suitable hardware available, VACLs are a very valuable addition to the security armoury, offering good access control without sacrificing performance.

1.3.1. VACL basics

VACLs are similar in some ways to the extended ACLs frequently employed on Cisco routers but they also have a number of important and interesting differences. Like extended ACLs, VACLs are constructed as a list of permit or deny statements that are processed in sequential order until a match is found or the implicit 'deny' is reached at the end of the ACL sequence. Traffic can be permitted or denied based on any combination of the source and destination IP addresses, transport layer protocol and application layer source and destination ports.

Unlike extended ACLs however, VACLs are applied per VLAN rather than per interface. Also VACLs have no sense of direction (*in* or *out*) since they are applied as the frame crosses the switch bus rather than ingress or egress to a physical or logical interface. As may be expected, VACLs are also stateless so care must be made when architecting VACL-based security to permit any legitimate response or reply traffic.

Until recently VACLs were only available on the Catalyst 6500 series of switches but they are now available on some of Cisco's mid-range switches including the Cat3750 and Cat4500 series. 'Supervisor engine' cards are available for the 4500 and 6500 series switches that use Application-Specific Integrated Circuits (ASICs) to allow VACLs to be processed at wire speed. Therefore, unlike with router ACLs there is no noticeable performance hit from enforcing VACLs. On lower-end switches VACLs are processed in software at an unspecified but most likely significant cost to performance.

Cat3750 series switches do not support logging of VACL operations. The higher-end Cat4500 and Cat6500 series do permit logging but only of dropped packets, not those permitted by a VACL. However logging requests are not processed in ASIC, rather they are passed to software and thus incur a very substantial performance hit. Therefore logging of VACLs is not usually appropriate.

Thanks to their the wire speed operation on the higher-end switches, VACLs can actually improve network performance by blocking unwanted traffic at source and thus removing unnecessary network load, thereby easing processing demands on layers 3 and upwards. VACLs can also be combined with PVLANs to give a two-pronged approach to securing networks at layer 2.

There are three configurational steps required to implement traffic filtering using VACLs:

1. One or more IP or MAC *access-lists* are created to specify which traffic is to be filtered.
2. A *VLAN map* associates the traffic types defined by the access-lists with an action such as forward (the default), drop, or redirect (only available on 6500 series).
3. A *VLAN filter* specifies which VLAN(s) the VLAN map should be applied to. Different VLANs can have different filters but only one filter can be applied to any one VLAN.

Note that the access-lists do not perform the access control themselves; rather they serve as 'match' lists to identify interesting traffic types. A permit line equals a match. A deny line equals no match so the switch moves on to the subsequent line in the access-list and then onto the next access-list as defined by the ordering of the VLAN map, and so on.

1.3.2. Example of VACL implementation

In a web hosting solution we will clearly need to allow HTTP to enter a DMZ from the outside world. It is unlikely however that the servers in the DMZ will need to communicate with one another. VACLs can provide such separation using the configuration excerpts below. In this example we also permit ICMP within the DMZ for ease of troubleshooting but deny all other traffic. Let's assume that the existing setup has a large number of servers connected to a switch and placed in VLAN2. All the servers are addressed within the DMZ subnet 192.0.2.0/24.

Firstly three access-lists are created to identify interesting traffic types. Note that since VACLs do not track connection state it is necessary to include a permit statement for HTTP replies (TCP source port=80).

```
ip access-list extended HTTP_In
#Do not allow intra-DMZ HTTP ...
  deny tcp 192.0.2.0 0.0.0.255 192.0.2.0 0.0.0.255 eq www
#... but permit all other HTTP, including replies
  permit tcp any 192.0.2.0 0.0.0.255 eq www
  permit tcp 192.0.2.0 0.0.0.255 eq www any
  exit
ip access-list extended Intra-DMZ_ICMP
#Match intra-DMZ ICMP ...
  permit icmp 192.0.2.0 0.0.0.255 192.0.2.0 0.0.0.255
#... but don't match any other ICMP, which falls to the 'catch all' All_IP below
  deny icmp any any
  exit
ip access-list extended All_IP
```

```
  permit ip any any
  exit
```

Next the VLAN map *DMZ_VACL* is created to link these ACLs with an appropriate action. Logging of dropped packets is enabled for the purposes of illustration but remember the shortcomings of logging mentioned earlier.

```
vlan access-map DMZ_VACL 10
  match ip address HTTP_In
  action forward
  exit
vlan access-map DMZ_VACL 20
  match ip address Intra-DMZ_ICMP
  action forward
  exit
vlan access-map DMZ_VACL 30
  match ip address extended All_IP
  action drop log
  exit
```

Finally the VLAN map is applied to VLAN2. In our example there is only one VLAN but in a different scenario the VLAN map could be applied to multiple VLANs.

```
vlan filter DMZ_VACL vlan-list 2
```

These controls would ideally be applied in addition to stateful firewalling at the network gateway and perhaps PVLANs, giving us a good example of how VACLs can contribute to defence in depth.

From this basic example it can quickly be seen that VACLs offer much more granular perimeter defence than PVLANs. However it is hopefully also clear that their lack of state will cause problems when filtering 'unusual' protocols such as FTP. A fuller treatment of the configurational steps required to construct and apply a VLAN map to protect the same example DMZ as used in 1.2.2 is given in Appendix A.

1.3.3. Limitations of VACLs

VLAN ACLs are a Cisco proprietary technology and are therefore only available on Cisco's range of Catalyst switches, although other vendors may offer similar features in their switch products. Even within Catalyst switches, VACLs are not available on low-end models and full VACL functionality is only available on high-end (ie expensive!) hardware.

VACLs are not stateful so do not have the connection awareness offered by many modern firewalls. Instead VACLs operate in a similar fashion to packet filters. This is OK for most protocols but in certain cases, such as FTP, it could be necessary to open more ports than an administrator would likely feel comfortable with.

Logging of traffic denied by VACLs is not usually practical and logging of permitted traffic is not possible. Since logs are often vital for forensic and legal purposes this will concern some administrators. It is up to the individual administrator to decide whether this is a fatal limitation in VACLs.

1.4. Firewall integration of VLANs

A third strategy for leveraging the capabilities of VLANs is to use an 802.1q-aware firewall to terminate multiple VLANs and perform access-control between them. As with VACLs, this usually has the advantage of not requiring additional hardware or physical changes to an existing architecture. However unlike when using VACLs, enhancements to perimeter defences using VLAN-aware firewalls are available using inexpensive switches and from vendors other than Cisco.

1.4.1. Basics of firewall/VLAN interoperation

By defining sub-interfaces on a firewall an administrator can segment a network logically rather than physically and then apply individual security policies to each sub-interface. The firewall enforces security controls on traffic passing between two sub-interfaces in much the same way that it would on traffic passing between two physical interfaces. This means that the firewall can be used to statefully inspect the traffic and also perform any application-layer security checks that the firewall is capable of.

Logical separation of networks in this way has a number of benefits. Controlling the number of physical Ethernet ports required is of particular advantage when working with 'hardware' (ie appliance-based) firewalls such as those from NetScreen, Nokia and Cisco PIX. Since many of these firewalls are sealed units with limited or no support for modular interfaces, adding additional physical interfaces is often not an option (unlike with 'server-based' firewalls such as FireWall-1, iptables, pf, etc).

Clearly the use of stateful inspection is a considerable security benefit over the stateless inspection performed by VACLs but in addition the use of VLAN-aware firewalls also allows detailed logging of inter-VLAN traffic, a key requirement of any secure perimeter defence.

1.4.2. Example of firewall/VLAN interoperation

Considering the same example as used in 1.2.2 and 1.3.2 we immediately encounter one of the drawbacks of implementing segregation using VLAN-aware firewalls. The existing network illustrated in Figure 1 includes five servers with contiguous IP addresses. Since using VLANs in this way requires the creation of sub-interfaces on the firewall, each server (or server group) must reside on a different IP subnet. Consequently, if VLAN-based firewall protection is to be offered to the five servers then readdressing is a necessity. Of course, this limitation only affects legacy networks – for new installations the IP addressing would be planned in such a way that each class of protected host was in its own subnet from the outset.

Assuming that the opportunity for readdressing exists, the servers could be renumbered as illustrated in Figure 2. Note that a particularly restrictive subnetting strategy has been adopted with regard to the two SMTP servers. Some

administrators might have preferred to have a /29 containing both servers in a single VLAN. We have elected however to enforce firewall controls on communications between the two mail servers. Note also that readdressing has been kept to a minimum. We have been able to retain the IPs of both SMTP1 and Syslog, these two servers require only a change to the subnet mask.

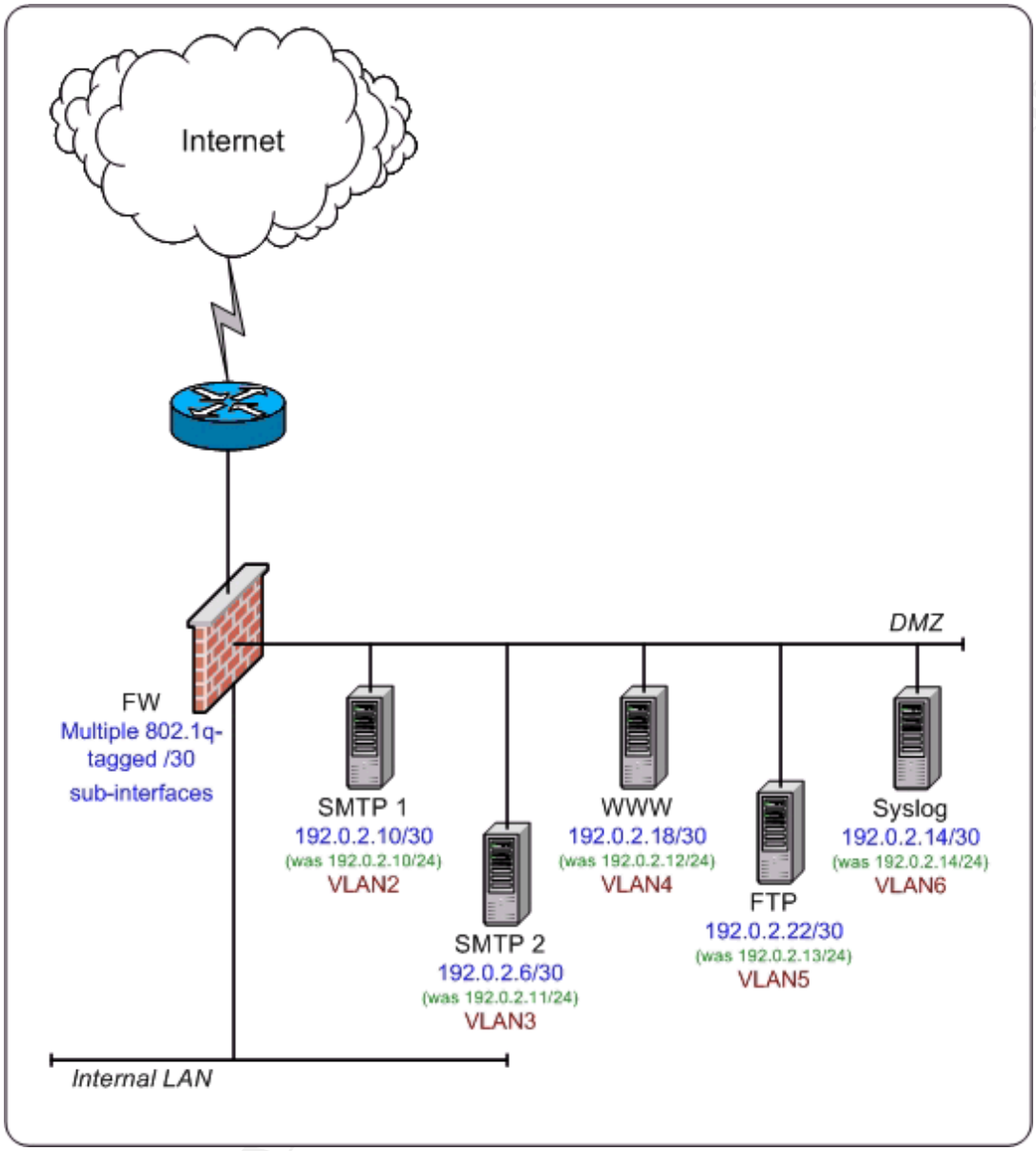

Figure 2: Example network using VLAN-aware firewalls

Once the servers and firewall have been renumbered, the administrator can proceed to apply access controls between the various hosts. A basic firewall security policy based on Figure 2 could be constructed as shown in Table 2.

SMTP1, SMTP2	Internet, Internal mail servers	SMTP
Internet, Internal mail servers	SMTP1, SMTP2	SMTP
SMTP1, SMTP2	Nameservers	DNS
Internet	WWW	HTTP
Internet	FTP	FTP
All DMZ servers	Syslog	syslog

Table 2: Traffic permitted through the firewall in the example

The specific configuration commands to implement this are vendor-specific but an example using NetScreen ScreenOS is given in Appendix B. Regardless of firewall vendor however, the granular controls over traffic entering, leaving or crossing DMZs that VLAN-aware firewalls facilitate offers an excellent way of increasing the segregation of DMZs when additional physical interfaces are not feasible.

1.4.3. Limitations of firewall/VLAN interoperation

VLAN-awareness in firewalls is a fairly recent development and is not yet supported by all firewall products and vendors. Cisco has offered support since PIX OS 6.3 and NetScreen since ScreenOS 4.0.2, although their larger, system models (NS-500 and NS-1000) have supported VLANs for several years as part of their virtual firewalling functionality.

Although the implementations by Cisco and NetScreen have thus far been free of noteworthy vulnerabilities, it is clear that VLAN segregation does not offer the same protection as using dedicated physical interfaces. Furthermore, it could be argued that by applying both VLAN-based and interface-based security checks a security architect is 'placing all his/her eggs in one basket' by trusting the same vendor to offer two adjacent layers of perimeter defence. However, this argument can be countered by noting that multiple logical DMZs offer better granularity than a single, flat DMZ subnet.

For high-performance networks there is a danger of bottlenecking since multiple 100Mbps Ethernet segments are connecting to a single 100Mbps interface. Careful consideration of throughput requirements is vital in such situations and, if network load increases, there may come a time at which additional or gigabit Ethernet interfaces become necessary to provide the throughput required.

1.5. Summary

Each of the three applications of VLANs described above represents a valuable addition to the security consultant's toolkit. Private VLANs, VLAN ACLs and VLAN-aware firewalls can often be useful additions to new security architectures but are also well suited to reinforcing many existing perimeter defences. Each application

of VLANs has strengths and weaknesses and the astute consultant will be able to draw on knowledge of all three to find an appropriate solution for each particular scenario.

PVLANs may be useful in situations where traffic needs to be controlled between hosts that are already deployed and are using the same IP subnet. However, they offer little granularity – hosts can either communicate fully or cannot communicate at all. There is no scope for IP or protocol/port specific access control. Nevertheless, PVLANs represent a useful extra layer of perimeter protection and can also be used in combination with VACLs to offer two layers of defence in depth.

VACLs will only be an option in some solutions as they are only available on specific models of Cisco switch, but where they are available VACLs offer excellent performance and a far more granular level of access control than is offered by PVLANs. They can readily be deployed in new networks but are particularly suitable in legacy networks where changes to physical connectivity and IP addressing are prohibited by commercial, operational or other considerations.

Of the three VLAN-based technologies presented here, VLAN-aware firewalls offer the most comprehensive set of security features. As well as sharing the performance and granularity benefits of VACLs they can track connection state and thus operate with unusual protocols and detect bogus or spoofed responses. In addition they offer the same logging capabilities as their layer 3 counterparts so allow the administrator to see exactly what traffic is being permitted and denied by their VLAN-based access controls.

As with any emerging technology there are early and late adopters of the technologies facilitating VLAN-based access controls. Each of the three described above will have an impact on the Information Security industry as they offer scope for additional controls to be applied to both legacy and greenfield networks, often at no additional cost. The ease of deployment of PVLANs and VACLs into existing networks will mean that they are likely to be added to existing networks, particularly DMZs. Assuming that they become supported on a wider range of switch hardware, and in particular the inexpensive low-end switches, VACLs are the clear leader of the two in functionality and will likely be added to many existing DMZs. As more firewall vendors embrace VLANs, the use of multiple, logical DMZs rather than a single, flat subnet seems likely to become the *de facto* standard for installations where dedicated physical interfaces are not an option.

Security managers, consultants and writers are increasingly beginning to endorse the contribution to layered security offered by VLAN-based access controls. However, it will usually fall to the personnel tasked with the day-to-day operations of perimeter technology to study, test and deploy these new technologies. As with all new technologies the best way for personnel to learn is to experience the technologies first-hand. There will inevitably be a period of inexperience towards the start of the learning curve but since the configurational syntaxes of PVLANs, VACLs and VLAN-aware firewalls are very similar to those already used for other tasks, these new technologies are likely to be easier to adopt that others to which the personnel have had no prior exposure.

2. Security Architecture

GIAC Enterprises (GIACE) are a company that sell fortune cookie sayings to customers around the world. GIACE employ a total of 50 staff with the majority based at their London headquarters. There are also four small satellite offices located across four other continents in New York, Cape Town, Sydney and Beijing. GIACE are a modern, forward looking company and as such much of their business, including all sales, is conducted over the Internet.

Due to the nature of GIACE's business model, ensuring that their electronic data and systems are secured against network-based threats is a key business priority. Following concerns raised by the board of directors, a consultant has been hired by GIACE to design and implement a secure network architecture. The directors of GIACE have given the consultant largely free reign to implement whatever changes he feels necessary. However, a key performance metric of the contract is that the final architecture must offer suitable protection from the myriad threats posed by modern inter-network connectivity while at the same time leaving GIACE free to execute its core revenue generating activities without overbearing constraints.

There is currently a very compelling commercial advantage to GIACE upgrading their network. Most purchases of IT systems and infrastructure are made from US-based companies whose price lists are published in US$. The favourable prevailing £/$ exchange rate means that savings of up to 30% are possible compared to 12 months ago. Since such favourable exchange rates are rarely long-lived, now is an excellent time for UK-based companies to purchase IT systems and infrastructure.

2.1. Objectives

The main objectives of this project can be summarised as follows:

- Design and implement a secure network architecture that offers good protection against network-based threats. This includes both deliberate and accidental attack from both external and internal users.
- Design the solution in such a way that it is logically structured. This allows easy handover of network and security management from the consultant to GIACE's IT department and also helps to simplify writing the necessary documentation to support the design.
- Implement the solution to allow for future growth of GIACE over the coming 2-3 years. The design should not introduce unnecessary bottlenecks or latency and certainly should not limit what changes and/or upgrades can be made to the network architecture in the foreseeable future.

2.2. Types of user

Companies and individuals that GIACE interact with as part of their business operations can be broken down into seven groups. The specific needs of each user group are assessed below.

2.2.1. Customers

GIACE sells fortune cookies to both companies and individuals. To make product information, pricing and ordering facilities available over the Internet, GIACE have implemented an Extranet in the form of a web portal. The portal allows customers to connect using SSL so, unlike an IPSec VPN, the customer requires no special hardware or software – only an SSL-capable web browser. Communications are secured using 128-bit SSL and username/password combinations, with controls to make sure that passwords meet minimum length and complexity requirements.

2.2.2. Suppliers

Suppliers submit new ideas for fortune cookie sayings to GIACE so that GIACE can select the sayings they wish to purchase. Suppliers need to be able to view the status (accepted/pending/rejected) of their submissions, what income their efforts have generated, and details of payments made to them by GIACE for their work. All of these services are available through the SSL portal. The SSL portal exchanges data with a back-end development database to facilitate queries and responses.

2.2.3. Partners

GIACE partner companies require access to a greater range of systems and services than can be served by the SSL portal. After careful vetting and signature of a non-disclosure agreement, trusted partners are permitted read-only access to certain directories on the internal file server. Partners are never allowed access to the master database of fortunes but are allowed access to the development database. GIACE and its partners also routinely exchange highly sensitive business and financial information via email. To ensure the privacy, integrity and authenticity of these communications, IPSec VPNs are built between GIACE and partner companies.

2.2.4. Employees located at GIACE head office

As with most modern companies, both email and web browsing are business critical applications. Email is the primary tool used by GIACE employees to communicate with colleagues, customers, suppliers and partners. Extensive searching of Internet web sites is necessary to obtain market information and ideas for new fortunes in this increasingly competitive industry. As well as these Internet services, all employees use common internal services – file and printer sharing, DNS, DHCP, etc. Access to the master database of fortunes is only granted to appropriate employees. Administrative access to all servers is restricted to members of the IT department.

2.2.5. Employees located at GIACE satellite offices

GIACE has four satellite offices in four different continents. Employees in those offices require largely the same access to network services as employees working at head office. In order to allow a singular security strategy and to remove the need for local IT personnel, all systems at satellite offices are managed from GIACE headquarters. All web browsing and email communication is routed through the headquarters' security infrastructure – there are no proxies or mail servers outside of the headquarters. Unfortunately round trip and latency considerations can result in browsing for satellite users being somewhat slower than desirable but the cost savings far outweigh this minor inconvenience. IPSec VPNs are used to facilitate

secure communications between the satellite offices and the head office.

2.2.6. Mobile and home-based employees

The mobile sales force often needs to connect to GIACE internal systems whilst on the road. Despite the fact they are out of the office, these mobile employees still need to access largely the same resources as they would when in the office. Similarly, members of the IT department need to be able to connect from their homes in order to perform emergency maintenance to servers and other infrastructure. Access for both these types of remote user is provided by an IPSec client installed on the users' laptops. All laptops also run personal firewalls.

2.2.7. The general public

The general public need to be able access the GIACE web site, send and receive email and resolve DNS for the giace.com domain.

2.3. What are we trying to secure?

It is important to assess how precious different assets are to GIACE and how valuable the data contained within each asset is to the company. This will allow focus to be given to data stores that are of particular importance or have a particularly high exposure to risk.

2.3.1. Key data stores

The most significant data store is the master database of fortunes. This is the 'crown jewels' of the GIACE network as it contains the valuable intellectual property upon which GIACE has built the company to the size it is today. Also of utmost importance are the email system and file server as these all include information regarding company strategies, forthcoming campaigns, financial results and so on.

While the public web and DNS servers only hold static content with little intrinsic value, the integrity of the content is still very valuable to GIACE as should it be modified by an unauthorised user, an attacker could disrupt or re-route GIACE's business data flows, intercept web and email traffic, publish spurious information about the company or otherwise undermine the company's commercial image.

2.3.2. Key data flows

The key public data flows are those between GIACE head office and remote users (both satellite offices and mobile sales force), customers, suppliers and partners. These communications can contain sensitive information such as orders, marketing strategies, bank details and credit card information. Within the local networks at GIACE headquarters the key data flows are primarily those to and from the key data stores detailed in 2.3.1. Due to the operational importance of web access the flow of traffic between end users, the proxy server and the Internet is also very important.

2.3.3. Key threats

The world of online fortune cookie sales is surprisingly ruthless. Corporate espionage and sabotage are not unheard of. The secure network architecture must be prepared to repel these threats as well as more commonplace dangers including

automated scans, script-kiddie activity, the general plethora of worm traffic, and advances made by more skilled attackers.

2.3.4. Exposed systems

The most vulnerable systems in GIACE's network are those that accept unrestricted, anonymous connections, namely the public web server, SMTP gateway and DNS server. Extra care must be taken when securing these systems so that should they become compromised, the intruder has the minimum onward access to other, less-accessible GIACE systems.

Also publicly accessible are the SSL portal and the remote access VPN gateway. These systems represent a lower risk as they require authentication before a user-interactive session can be established. Both systems also have a less chequered history with regard to released vulnerabilities. However, this does not mean that they are unsusceptible to unauthenticated attacks, including buffer overflows.

The border router and VPN firewall are also publicly routable but do not accept connections except from a handful of specific source IPs. The router has strict ACLs configured to restrict access to the VTY. The VPN gateway uses only main mode IPSec in order to verify that the peer IP address is permitted before commencing phase 1 negotiations (more on these later).

2.4. Data systems

In order to conduct business and meet the requirements of the individuals and companies detailed in 2.2, GIACE will need to deploy and maintain a number of servers. A list of these servers along with a brief overview of the role played by each is given in Table 3.

Public web server	Serves static web content to the general public	Apache is run in a jail(8) environment[5]
Public e-mail server	Exchanges e-mail with the general public	Sendmail is run in a jail(8) environment SpamAssassin is used to help remove bulk emails Kaspersky is used to virus check mails and remove executable file attachments (.exe, .pif, .bat, .scr, etc)
Public DNS server	Provides DNS resolution to the general public and DNS forwarding for the internal DNS server	BIND is run in a jail(8) environment
SSL portal	Provides secure pricing, ordering and submission services to customers and suppliers	Apache is run in a jail(8) environment
Development database server	Allows suppliers and partners to upload fortunes and query their recent submissions and account status	
Certificate server	Allows the VPN Concentrator to authenticate remote access users	
Proxy server	Provides centralised access controls to enable GIACE employees to browse the Internet	squid-vscan is used to virus check web traffic The *no-adds* PAC file[6] is used to reduce the number of banner ads
SUS/AV server	Provides centralised management and distribution of Windows patches and anti-virus updates	
Internal mail server	Exchanges e-mail between GIACE employees, their colleagues and the public e-mail server	McAfee VirusScan is used to virus check mails
Master database server	Holds the 'crown jewels' of the GIACE network – the master database of fortune cookie sayings	
Domain controller	Required for various Microsoft functions – user logon, AAA services for file and print daemons, etc	
Internal DNS server / DHCP server	a) Provides name resolution services to GIACE employees b) Provides dynamically assigned IP addressing and related information to GIACE employees	
File and print server	Acts as a repository for GIACE user files, company news, employee contact information, HR policies, staff handbook, etc and offers access to shared printers	McAfee VirusScan is used to virus check files
NTP server	Provides time synchronisation for internal users and DMZ servers	
Syslog server	Collates all log files	Syslog-ng is used to separate logs into files based on both the severity and source host of each log entry Swatch is used to alert on specific log entries

Table 3: Servers employed in the GIACE secure network architecture

2.5. Network segregation

The secure architecture is designed to ensure that hosts of differing value, accessibility and importance to business continuity are not connected to the same network segment. By segregating hosts along these lines, with firewalls interconnecting the various segments, tight and granular control over inter-network communications can be achieved.

Table 4 shows how systems in the network are segregated onto separate physical Ethernet segments according to which other networks are allowed to connect to them and which other networks they are allowed to connect to.

Exterior firewall	1	Internet	Border router	None	Connects to the public Internet, a totally untrusted network.
	2	Public server DMZ	Catalyst 2950-12	WWW (Apache), SMTP (sendmail), DNS (BIND), nIDS	Systems on this segment allow unauthenticated access to the general public. Although each of the three daemons used (Apache, sendmail, BIND) are the Internet standards in their field, each has a history of serious security problems[7,8,9,10,11] allowing remote compromise, so segregation from other networks is essential.
	3	Encrypted VPN DMZ	Catalyst 2950-12	SSL portal (Apache), VPN Concentrator (external NIC), nIDS	Systems on this segment are accessible by the general public but require prior authorisation. Following online registration, customer-level access to the SSL portal is available immediately. Supplier-level authentication credentials are only made available following proper vetting by GIACE. Authentication credentials for the VPN Concentrator are only provided to GIACE employees following proper internal approval. Although both these applications have somewhat better security records than those in the Public server DMZ, the possibility remains for unauthenticated remote compromise so segregation is crucial.
	4	Unencrypted VPN DMZ	Catalyst 2950-12	VPN Concentrator (internal NIC), nIDS	Allows segregation of remote access communications ensuring that the less trusted encrypted traffic is kept separate from the more trusted cleartext traffic. Other than for management, no connections to this interface should be necessary.
	5	Semi-private server DMZ	Catalyst 2950-12	Development database (MySQL), certificate server (CATool), nIDS	Systems on this segment do not accept connections direct from the Internet or any other totally untrusted sources. They must however accept connections from little-trusted sources in the Encrypted VPN DMZ - the dev DB from the SSL portal and the cert server from the Concentrator. As the hosts in this DMZ accept connections from little-trusted sources they cannot be highly trusted themselves so are segregated from other systems.

	6	Private server DMZ	Catalyst 2950-12	Web proxy (squid), update server (MS SUS & McAfee), nIDS	Systems on this segment only accept connections from internal hosts so are not exposed to the worst threats from Internet attacks. However the web proxy is allowed to initiate direct connections to any public website using the web ports and therefore is at risk from downloaded content. The SUS and AV update server also warrants segregation on this DMZ because in the event of a worm or virus outbreak on the internal network it is likely that the SUS/AV server will be susceptible to the same vulnerability as the infected hosts so needs to be protected to allow vulnerable hosts to reliably obtain patches or DAT updates.
continued	7	Mgmt DMZ	Catalyst 2950-12	NTP server, Syslog server, IDS Sensor, management PC, nIDS	With the exception of the syslog server, systems in this DMZ only offer client services. As the systems in this DMZ are vital for maintaining a secure perimeter, they deserve segregation from other systems.
	8	Internal	Catalyst 2950-12	nIDS	This segment carries traffic from networks of varyingly low trust levels towards a network with a relatively high level of trust.
Interior firewall	1	Internet firewall	Catalyst 2950-12	nIDS	As for Eth8 above
	2	Internal DMZ1	Internal SMTP (MS Exchange)	None	The internal mail server deserves particular protection as it is the only internal host that must accept connections from a little-trusted host - the public mail relay
	3	Internal DMZ2	Master DB (MySQL)	None	The master DB requires particularly tightly controlled access because it contains GIACE's most valuable assets
	4	Internal LANs	Catalyst 4006 (via GigE)	nIDS	The internal VLANs contain only private systems that do not accept connections from anywhere outside their own security domain and do not initiate connections directly to the Internet
	4.1	Server VLAN	Catalyst 4006	Domain Controller, internal DNS, DHCP, file/print server, etc	This VLAN contains the servers necessary to provide common office services
	4.2	Technical VLAN	Catalyst 4006	Technical users workstations & notebooks	These three VLANs contain end user PCs. End users never need to communicate with end users on different VLANs. They only communicate with other end users in the same VLAN, with internal servers in the server VLAN and with servers in the various DMZs
	4.3	Sales VLAN	Catalyst 4006	Sales users workstations & notebooks	
	4.4	Accounts VLAN	Catalyst 4006	Accounts users workstations & notebooks	

Table 4: Logic of segregation of GIACE LANs

2.6. Network architecture

The network topology is shown in Figure 3. Within the physical Ethernet segments detailed in Table 4, further segregation is achieved using VLAN-aware firewalls, (as discussed in 1.4). A discussion of each of the security components used in the architecture follows later in this section.

IP addressing and VLAN membership are shown in Figure 4. Instead of selecting 'obvious' IP schemes using eg 172.16.x.x or 192.168.1.x, IP addresses have been taken from rather less used subnets - 172.22.8.0/22 and 192.168.8.0/22. The reason for this is to help reduce the likelihood of IP address clashes in the future should GIACE take over other companies, or in fact be taken over themselves. VLAN numbers have been selected to correlate with (sub-)interface numbers. The IP addressing scheme has been constructed to allow for future expansion. Each physical and logical DMZ is numbered using a /29 subnet to allow for future clustering of mail, web, etc servers.

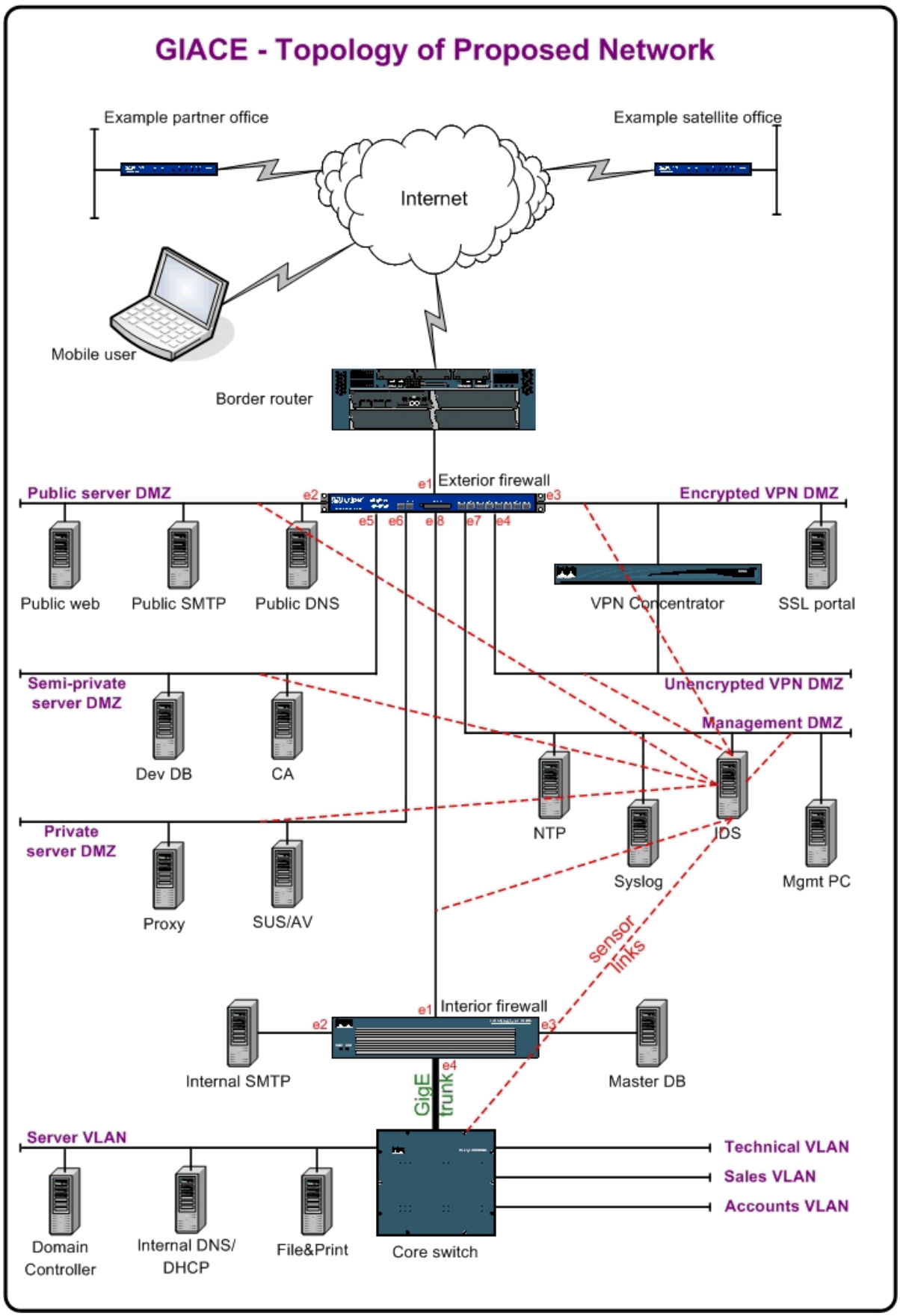

Figure 3: Secure network architecture

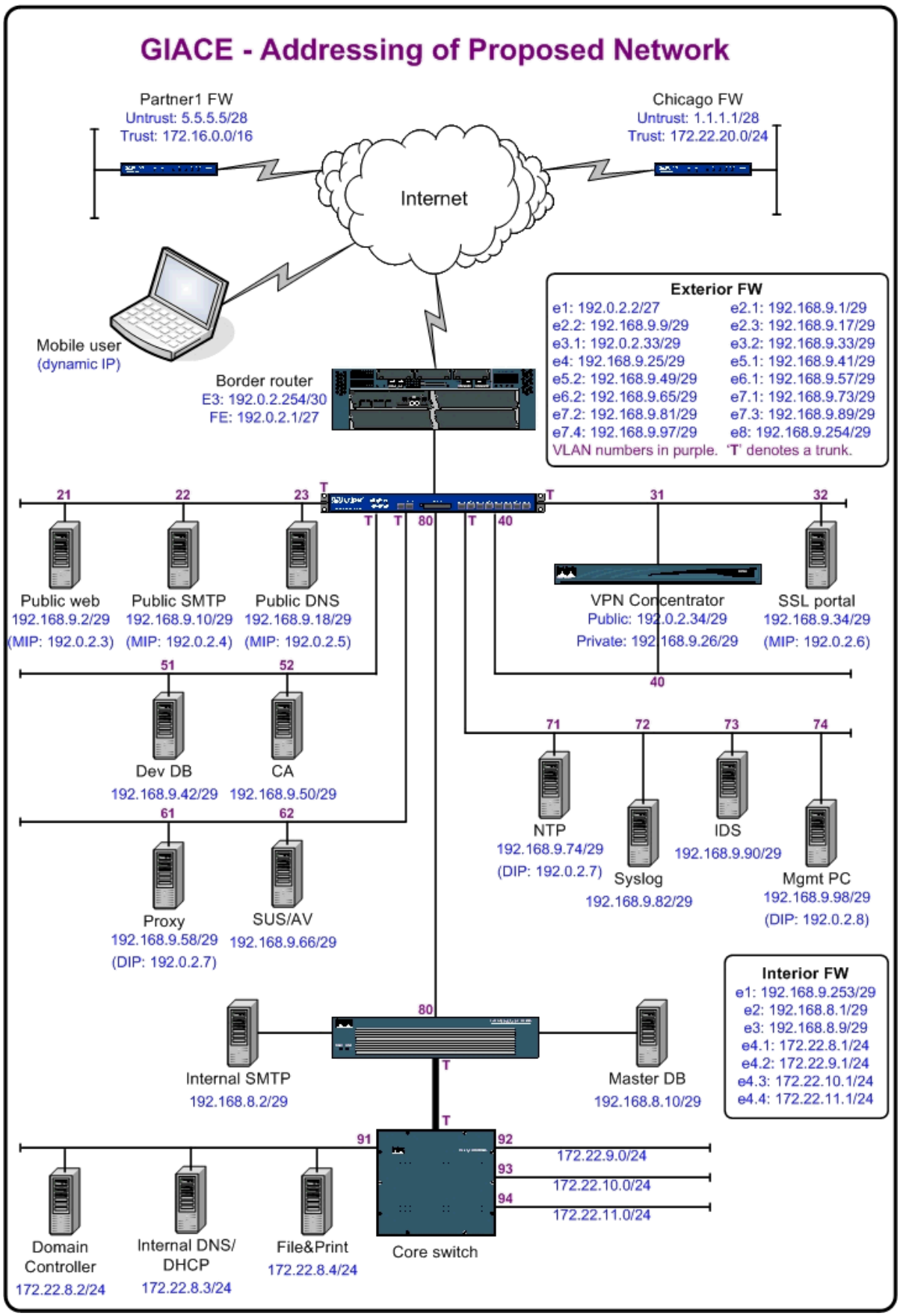

Figure 4: Layer 2 numbering and layer 3 addressing

2.6.1. Internet connection

The Internet connection selected is a tiered E3 service allowing GIACE to increase their Internet bandwidth as they expand. Bandwidth is initially set at 10Mbps but the tiering on the E3 line can easily be increased in 2Mbps increments up to a maximum of 34Mbps. The ISP has supplied the public subnet 192.0.2.0/26 for GIACE's use.

2.6.2. Border router

Cisco are by far the market leader in mid-range routers. Their competitors Juniper offer comparable routers that are considerably more stable, have richer security features and benefit from ASIC-based processing. However, JunOS is very syntactically different to IOS so this would represent an additional operating environment that GIACE's network administrators would need to learn. Considering that IOS-based products are used extensively elsewhere in the GIACE network (see later in this section) it has been deemed that the extra training and man-time necessary to adopt a single JunOS-based product do not warrant the merits of Juniper routers over Cisco. The C3745 model is selected from the extensive Cisco router range as it has sufficient horsepower to enforce lengthy access lists without adversely affecting throughput. The router runs IOS 12.3.12a with the Advanced Security feature set to allow management using SSH.

The C3745 is configured with two access lists to filter both packets entering the GIACE network from the Internet and also leaving the GIACE network destined for the Internet.

The precise details of the router configuration are beyond the scope of this paper but some of the highlights are:

- Wherever possible, the router is configured in line with the *Center for Internet Security benchmarks for IOS and PIX OS*[12].
- The GIACE→Internet ACL only permits packets that have a source IP in the public subnet assigned to GIACE by their ISP (192.0.2.0/26).
- The Internet→GIACE ACL drops all packets with common 'spoofed' source IPs including 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 127.0.0.0/8, 224.0.0.0/3 and (importantly) 192.0.2.0/26, which is GIACE's own netblock and thus should never enter from the Internet.
- The Internet→GIACE ACL has specific 'permit' lines and drops all other traffic. This is preferable to blocking a long list of 'dangerous ports' as any port not explicitly permitted should be considered dangerous. Also a 'deny by default' access list will contain fewer lines so will be more efficient in terms of CPU load. All dropped packets are logged to the syslog server.
- Both these ACLs are applied 'inbound' to the appropriate interface to save the router from processing traffic that would later be dropped by an 'outbound' ACL.
- A third ACL is configured to restrict management access to the router itself. Only connections from the NAT address of the management PC are permitted.

2.6.3. Exterior firewall

Security professionals are increasingly recommending appliance-based firewalls over more traditional server-based firewalls such as FireWall-1 and

ipchains/iptables. This changing allegiance is being very well received amongst network engineers and administrators because not only are appliance-based firewalls less susceptible to hardware failure than server-based firewalls (as they have fewer components and moving parts) they are also quick and easy to deploy because they come pre-installed with hardened, security-specific operating systems. When deploying a server-based firewall an engineer must first install and harden the operating system, which often takes hours; then configure individually such software components as SSH, NTP and syslog; then install any third-party firewall software; all before the actual firewall configuration can begin. With an appliance-based firewall, the engineer can immediately jump straight into configuring the firewall, with additional settings for NTP, syslog and SSH requiring only a few configurational commands on the CLI.

In light of this, a NetScreen-208 is used as the exterior firewall. The NS208 is an ASIC-based security appliance offering stateful inspection and excellent VPN capabilities. The NetScreen was selected over other stateful inspection firewall appliances based on the fact that it is:

- Fast - wire-speed performance of both firewalling and VPN (3DES and AES)
- Easy to manage - having a straightforward webUI and Cisco-esque CLI
- Reasonably priced - in terms of cost/performance
- Richly featured - offering:
    - Some DoS protection capabilities
    - Traffic shaping
    - High availability
    - Deep packet inspection capabilities for 17 protocols (including DNS, FTP, HTTP, SMTP, POP3 and SIP)

The latest stable version of ScreenOS is 5.0.0r9 and this is selected for the NetScreen-208. Although there are some useful additional features in the 5.0.1 branch of ScreenOS, releases from this branch are still too unstable to run on production systems. A virtualisation key is purchased to allow additional security zones, virtual routers and VLANs. The configuration of the NetScreen-208 is discussed at length in section three.

2.6.4. VPN gateways

In secure networks it is common to split VPN and firewall functionality onto physically separate devices. By terminating VPNs on a separate device to the main exterior firewall an extra layer of security is provided because after decryption the traffic still has to cross a DMZ interface on the exterior firewall. This means that should a vulnerability be discovered in either the VPN or firewall products, a 'single step' compromise of the network remains unlikely. However, given the NetScreen's excellent VPN capabilities and performance it has been decided to terminate the VPNs for the satellite offices on the NS208. The abovementioned risks are mitigated in three ways: only allowing main mode IKE (thereby restricting which peers can initiate phase 1 negotiations); filtering at the border router to only permit IPSec from the known IPs of the satellite offices; and forcing the traffic to pass through a second firewall performing stateful inspection (see 2.6.5 below) before reaching the internal networks. These main mode VPNs use preshared keys of at least 32 randomly generated characters. None of the VPN sites are in countries on

the US government's embargo list (Cuba, Iran, Iraq, Libya, North Korea, Sudan & Syria) so exportation of encryption is not a problem.

VPNs for mobile and home workers are provided using a Cisco VPN 3005 Concentrator running code release 4.1.7.D. This provides an inexpensive remote access solution and is used to terminate all aggressive mode VPN access into the GIACE network. The public interface of the Concentrator is connected to the Encrypted VPN DMZ and the private interface is connected to the Unencrypted VPN DMZ. By connecting in this way, IPSec connections from the Internet to the Concentrator are controlled by the exterior firewall and cleartext communications leaving the Concentrator are also firewalled.

Mobile and home users run the Cisco VPN client on their notebooks as well as the bundled Cisco personal firewall, which the user cannot disable. The VPN client is configured to send all connections via the Concentrator – split tunnelling is not permitted. Therefore although out of the office, remote users must still browse via the GIACE proxy server and the SUS/anti-virus server can check patch and DAT file revisions when a user logs on. To further ensure that remote access to the GIACE network is only granted to users with up to date patches and AV the GIACE IT department are keen to evaluate Microsoft Network Access Quarantine Control[13].

All VPNs, whether main mode (site-to-site) or aggressive mode (client-to-site), use the same encryption and authentication standards. In order to offer protection against current and future weaknesses[14,15] in encryption and (in particular) hashing algorithms, different algorithms are used during phase 1 and phase 2. Phase 1 uses 3DES and SHA-1. This combination was selected because SHA-1 uses a longer hash output and thus offers better phase 1 key hashing (and consequently better protection to the phase 2 keys) than MD5. Phase 2 uses AES-256 and MD5. This combination was selected because AES-256 is both stronger yet more computationally efficient than 3DES, which is important for the bulk data encryption performed using the phase 2 keys. Main mode IKE exchanges are protected using Diffie-Helman group 5.

User notebooks hold certificates, which are used for identity verification. When a user attempts to authenticate to the Concentrator, the certificate is checked against the CA server. In addition users must enter a username/password combination before access to the internal network is granted. Notebooks also require the entry of a power-on password before the operating system will load. Two-factor, token-based user authentication was considered but was rejected on the bases that it is expensive to set up for a small user base and that the ongoing administrative burden would be too great.

2.6.5. Interior firewall

As well as proving an extra layer of security for communications with the Internet, the interior firewall also routes between the four VLANs that comprise the internal network. In order to allow wire speed internal communications the interior firewall must therefore come with at least one gigabit Ethernet interface. Furthermore, to achieve defence in depth the interior firewall must be provided by an alternate vendor to the exterior firewall.

A Cisco PIX 525 is selected based on these requirements and also influenced by the benefits of appliance-based firewalls extolled above. Although a Cisco product was also used for the border router, IOS and PIX OS are quite different operating systems, originally developed by different companies (Cisco bought Network Translation, the creators of PIX in 1995[16]) and thus using different kernels. If a vulnerability were discovered in one operating system it does not necessarily mean that the other is likely to suffer the same vulnerability, unless that vulnerability were in an underlying, non-proprietary protocol such as IP, TCP, SSH, etc. The PIX runs version 6.3(4) of Cisco's Firewall OS Software. Where possible, the PIX is configured in line with the *Center for Internet Security benchmarks for IOS and PIX OS* referenced in 2.6.2.

The internal network is split into four VLANs - sales, accounts, technical and servers. A gigabit Ethernet trunk connects the internal interface of the PIX 525 (which is configured with multiple sub-interfaces) to the main internal Catalyst 4006 switch. This allows stateful firewalling to be performed between the internal VLANs without creating too much of a bottleneck. By performing firewalling between the internal VLANs, we significantly improve resistance to internal attack and offer much greater protection to the internal servers than would otherwise be available.

The interior firewall also has two further interfaces connecting to the internal mail server and master database. As discussed in 2.3.1, these two hosts require particular protection. The internal mail server is unique in that it is the only internal host that accepts connections from an untrustworthy source (the DMZ mail relay). Other than for management, the master database does not accept connections from any host. Rather it initiates a connection to the development database on a scheduled basis to 'pull' updates. However, the server does represent the ‘crown jewels’ of the GIACE network as it contains the master database of fortunes - the valuable intellectual property upon which GIACE has built the successful company it is today.

2.6.6. Network-based IDS

A *Snort* network-based intrusion detection system (nIDS) sensor is deployed in the management DMZ. Each switch port that the sensor connects to is configured as a SPAN port for all the VLANs that the switch provides. The sensor connects to all DMZ and internal switches but does not connect to the Ethernet segment outside the exterior firewall. Although this loses some visibility of malicious network traffic, it serves to greatly reduce the amount of clutter and irrelevant alarms, which in turn increases the usefulness of the alerts generated by Snort.

Snort is one of the leading nIDSs and benefits from a large, independent group of developers, frequent signature updates and the availability of plenty of online support material. Of course, Snort has another major advantage over its many commercial competitors in that it is free to use. As the sensor will be processing lots of packets, *Barnyard* is used to offload the output processing and send it to a *MySQL* database. This frees Snort of this I/O-hungry task and leaves it free to dedicate all its energies to processing network traffic. *ACID* (run on top of *Apache*) is used to allow simplified viewing, searching, alert grouping and reporting of results. The sensor also runs *Swatch* to send network alerts on certain critical

events.

The Snort sensor runs on a HP DL360 dual-3GHz with 512MB RAM running FreeBSD 5.3 and Snort 2.3.0. The server is quite highly specified to allow it to process traffic from multiple 100Mbps segments. An unwelcome side effect of segmenting the network with many DMZs is that a lot of Ethernet interfaces are required so the server is fitted with two quad port PCI Ethernet cards giving a total of ten 10/100 interfaces.

2.6.7. Server and workstation operating systems

FreeBSD was selected as the operating system for all GIACE DMZ servers as it strikes a good balance between cost of support, stability and security. While Linux seems to be the dominant open source Unix-like operating system, it has quickly become over-engineered for straightforward networking servers and although minimal installations can be performed there is often confusion over which components are required for a certain function. The stability of Linux, while impressive, does not seem to match that of the BSD family of operating systems. At the other end of the spectrum, OpenBSD is arguably the most secure operating system in general production but was not selected as its hardware compatibility and ease of support are often not as good as FreeBSD.

In view of the fact that not everyone in GIACE is a technical user, Microsoft Windows is selected as the main operating system family on the internal network. Windows is used for Active Directory, Exchange, the SUS server, the internal anti-virus update server, DHCP, internal DNS, file and print services as well as for all user workstations. By agreeing to run only two PC operating systems - Windows (XP Pro for users, Win2K Server for servers) and FreeBSD - support and training costs are controlled. All FreeBSD systems are configured in such a way that they only have two listening ports - the port necessary to provide their primary service and also 30947/tcp, to allow management using SSHv2 on a non-standard port.

Wherever possible, both Windows and FreeBSD systems are configured in line with the relevant Center for Internet Security benchmarks[17,18]. All servers log to the central syslog server. Windows servers use *Snare* to convert Windows event logs into syslog.

2.6.8. Layer 2 infrastructure

Each shared Ethernet segment uses a dedicated Cisco Catalyst 2950-12 switch. As with Cisco routers, there are more robust and reliable switches available from other vendors, Foundry and Extreme being two examples. However, these vendors do not offer competing products anywhere near as cheaply as the Cat2950-12. All Cat2950-12 switches run IOS 12.1.22-EA3. For those switches that run multiple logical DMZs (as depicted in Figure 4), multiple VLANs are configured and the switch connects to the firewall using a trunk port. MAC-based port security is also enforced on all access ports to help prevent the introduction of rogue hosts. Switches are hardened in line with the recommendations in Steve Gill's *Catalyst Secure Template*[19].

2.6.9. Satellite offices

The GIACE satellite offices use NetScreen-5GT firewalls running ScreenOS 5.0.0r9 to establish a VPN tunnel to the head office.

2.7. Communications matrix

Table 5 shows the communications matrix for GIACE. In the matrix the terms source and destination are used. These are synonymous with client and server, in other words the host(s) in the source column is/are initiating connections to the host(s) in the destination column. Communications that benefit from some form of encryption are coloured green. This matrix will be integral to the derivation of firewall policies to be performed in section three of this document.

For the sake of brevity the communications matrix only details the access requirements for interactions between the end user groups detailed in 2.2 and GIACE. There are of course a number of other vital communications channels that must also be permitted to allow server to server communications. Some examples are server-to-server SMTP, external DNS resolution, time synchronisation and centralised collation of logs.

General public	Allow general public to access www.giace.com	Any valid public IP[1]	Public web server	80/tcp
	Allow general public to exchange email with GIACE	Any valid public IP, Public email server	Public email server, Any valid public IP	25/tcp
	Allow general public to query GIACE DNS records	Any valid public IP	Public DNS server	53/udp[2]
Customers, Suppliers	Allow customers and suppliers to access SSL portal	Any valid public IP	Extranet server	443/tcp
	Allow SSL portal to query development database	SSL portal	Development database	3306/tcp
Partners	Allow partners to connect via VPN to: i) Exchange email ii) Access development database and internal file server	Fixed IPs of partner VPN gateways	NS208 public interface	500/udp, 50/ip
		SMTP servers of partner companies, Public SMTP server	Public SMTP server, SMTP servers of partner companies	25/tcp
		LAN subnets of partner companies	Development database	3306/tcp
			File server	135/tcp, 135/udp, 137-138/udp, 139/tcp, 445/tcp
Satellite offices	Allow satellite offices to connect via VPN to: i) Send/receive email ii) Access both databases, file server, SUS/AV server and web proxy iii) Access domain controller and internal DNS server	Fixed IPs of satellite office VPN gateways	NS208 public interface	500/udp, 50/ip
		LAN subnets of satellite offices	Internal SMTP server	5000-5001/tcp[3]
			Development database, Master database	3306/tcp
			File server	445/tcp, 445/udp
			SUS/AV server	80/tcp
			Web proxy	8080/tcp

[1] Valid public IPs are taken to include all IPs other that those reserved by RFC1918 or otherwise unroutable, such as 127/8 and 224/3.
[2] Due to the small size of GIACE the DNS server will not need to return responses larger than 512 bytes so TCP is not required.
[3] By default Exchange communicates with Outlook clients using two random TCP ports. However, these ports can be user-defined as explained at http://support.microsoft.com/kb/155831/EN-US.

Continued from above	*Continued from above*	*Continued from above*	Domain Controller	135/tcp, 137-138/udp, 139/tcp, 42/tcp, 389/tcp, 389/udp, 636/tcp, 3268-3269/tcp, 53/tcp, 53/udp, 88/tcp, 88/udp, 445/tcp, 5000-5020/tcp[4]
			Internal DNS server	53/udp, 53/tcp
General mobile users	Allow mobile workforce to remotely connect via VPN to: i) Send/receive email ii) Access both databases, file server SUS/AV server and web proxy iii) Access domain controller and internal DNS server	Any valid public IP	VPNC public interface	500/udp, 50/ip
		General user IP pool from VPN gateway	Internal SMTP server	5000-5001/tcp
			Development database, Master database	3306/tcp
			File server	135/tcp, 135/udp, 137-138/udp, 139/tcp, 445/tcp
			SUS/AV server	80/tcp
			Web proxy	8080/tcp
			Domain Controller	135/tcp, 137-138/udp, 139/tcp, 42/tcp, 389/tcp, 389/udp, 636/tcp, 3268-3269/tcp, 53/tcp, 53/udp, 88/tcp, 88/udp, 445/tcp, 5000-5020/tcp
			Internal DNS server	53/udp, 53/tcp
IT mobile users	Allow IT personnel to remotely connect via VPN to: *(continued below)*	Any valid public IP	VPNC public interface	500/udp, 50/ip

[4] Windows 2000 Server uses a large number of ports for various purposes as detailed in http://support.microsoft.com/kb/179442. RPC ports are usually dynamically assigned but can be user-defined as explained at http://support.microsoft.com/kb/154596.
[5] The management server has onward SSH access to all DMZ and Internet-facing systems.
[6] VNC access to domain controller allows onward VNC and telnet/SSH access to all internal systems.
[7] The SSH port on the border router, firewalls and DMZ hosts is changed from the standard 22/tcp to 30947/tcp.

Continued from above	i) Connect to management server[5] ii) Manage all internal systems[6]	IT department IP pool from VPN gateway	Management server	30947/tcp[7]
			Domain Controller	5900/tcp
General internal users	Allow personnel on the internal network to: i) Send/receive email ii) Access both databases, SUS/AV server and web proxy	Internal VLANs supernet	Internal SMTP server	5000-5001/tcp
			Development database, Master database	3306/tcp
			SUS/AV server	80/tcp
			Web proxy	8080/tcp
IT users	Allow IT personnel to manage all infrastructure and perform general troubleshooting	Management PC	Border router, NS208, All DMZ hosts, Interior firewall, Public interfaces of all satellite office NS5-GTs	30947/tcp
			NS208	22978/tcp[8]
			Satellite office LANs	5900/tcp
			Any IP	ICMP ping, 33434-33523/udp, 21/tcp, 22/tcp, 25/tcp, 53/tcp, 53/udp, 80/tcp, 443/tcp[9]

Table 5: Communications matrix for GIACE

[5] The management server has onward SSH access to all DMZ and Internet-facing systems.
[6] VNC access to domain controller allows onward VNC and telnet/SSH access to all internal systems.
[7] The SSH port on the border router, firewalls and DMZ hosts is changed from the standard 22/tcp to 30947/tcp.
[8] The SSL port on the NetScreen is changed from the standard 443/tcp to 22978/tcp.
[9] The management server has direct Internet access using a number of common service ports to allow troubleshooting in the event of suspected problems with mail delivery, the web proxy, DNS, etc. However, everyday browsing, email, etc are carried out as for general users.

2.8. Defence in depth

"Defense-In-Depth strategy integrates People, Operations, and Technology capabilities to establish information assurance (IA) protection across multiple layers and dimensions. Successive layers of defense will cause an adversary who penetrates or breaks down one barrier to promptly encounter another Defense-In-Depth barrier, and then another, until the attack ends." **National Security Agency website**[20]

Defence in depth is a fundamental of all secure network design. Rather than having a single line of defence against a particular threat it is much more desirable to have multiple, independent, complementary layers of security. By implementing security in such a way, each layer complements the security of its adjoining layers. Should one layer become compromised, one or more additional layers remain between the intruder and their goal. Given time, dedication and skill almost any network can be penetrated regardless of how many layers of defence are implemented. However, by employing defence in depth the security administrator stands a much greater chance of noticing that an attack is underway and implementing controls to mitigate or contain the threat before any valuable data is compromised.

2.8.1. Technical considerations

The network architecture presented above shows excellent adherence to the principles of defence in depth. Each host that accepts connections from the Internet is protected by several layers of defence; each implemented using a complementary but different technology. The stateful inspection firewall is nowadays ubiquitous in secure networks but all too often is relied upon too heavily, leading to other security requirements being neglected. In the network designed for GIACE, the stateful NetScreen-208 is complemented by strict ingress and egress ACLs on the border router, operating system hardening of DMZ hosts, centralised logging and network-based IDS.

Assuming that his or her actions had thus far been stealthy enough not to trigger any network IDS alarms, an attacker who had already successfully compromised these multiple layers of security would also need to penetrate a further stateful firewall before he/she could access the valuable internal network. To complicate matters for the intruder, the internal network is segmented into four VLANs with stateful firewalling between each. This reduces the opening for one compromised host to allow further compromise of other hosts. VLAN-ing the internal network in this way will also help to stop the spread of any network-aware worm.

2.8.2. Human considerations

Of course, one should never forget the fact that the best laid defences can easily be undone by human error, laziness, malice or downright lack of common sense! Although this paper is primarily concerned with perimeter defence it is worth reminding the reader that defence in depth should reach right into the heart of a network. There are many threats that only manifest themselves away from the network perimeter. Mobile users frequently connect their notebooks, firewalled or otherwise, to their home broadband connections and later to the office LAN, potentially bringing with them all manner of malware. Removable media serves not

only as an easy means of information theft but also as a route for malware of all kinds to get straight to the internal LAN, carried (quite literally) past the tens of thousands of pounds of security infrastructure. Users connect wireless access points using default settings because "wireless is easier than running cables all over the place." The list goes on.

Some of the steps taken to mitigate these human threats are given below. The first three steps are components of the network architecture presented above, whereas the remainder are routine tasks that should be performed regularly by GIACE IT personnel.

- Microsoft Software Update Services are used to ensure that all servers, workstations and notebooks running Windows stay up to date with the latest security patches.
- Layered virus checking is performed by DMZ and internal mail servers, the web proxy, the file server and at the user desktop. Clients PCs use a different vendor's AV product to that used on the servers.
- Mobile and home users run firewalls on their notebooks and have VPN tunnels configured such that all communications are routed via GIACE and not direct to the Internet.
- Periodic checks for rogue wireless access points are made using *Kismet*.
- Whenever laptops are brought to the IT department for maintenance, *Spybot* and *A²* are run to check for any malware, spyware, etc.
- Workstation and notebook floppy drives are disabled in the BIOS. A password is set so that only the IT department can change BIOS settings.
- PCs are configured so that administrative privileges are required to install USB drivers meaning that mice and keyboards can be installed by the IT department but users cannot use USB storage devices.

In order to check that the network perimeter is secure, public-facing hosts are periodically scanned via the Internet (ie from a source IP outside 192.0.2.0/26). Unlike an internally-sourced scan, this ensures that the view of the network gained by the IT department is the same as that of a would-be attacker. *Nmap* is used as a general port scanner; *Nessus* is used for general vulnerability analysis and *Nikto* is used for vulnerability analysis of the public web server and SSL portal.

The importance of physical security cannot be over emphasised but is beyond the scope of this paper other than to state that all critical security and infrastructure components are kept in locked rooms with highly restricted access and CCTV. Similarly change control procedures alone could occupy an entire paper. GIACE have implemented a process where each significant network or security change requires a proposer and an approver. The approver also quality checks the change following its execution by the proposer.

There is a written corporate security policy that all new staff members must read and sign. This details what users many and may not do when using GIACE-provided IT equipment and services. The policy also includes a section detailing acceptable usage of web and email.

Finally in this section it is worth remembering that the best way to encourage a

culture of security awareness amongst a workforce is through patient and well considered training. The information security industry and its practitioners seem to be increasingly over reliant on technological solutions to problems. While technology undoubtedly has a pivotal role to play in information security, it is often thought of as the panacea for all threats and risks, which is simply not the case. For some users a 20 minute informal presentation explaining just why running the *sexy.exe* 'game' that their friend emailed them is dangerous may be enough to stop them from running it. Taking five minutes to explain why *they* don't want KaZaA running on their notebook is much more productive and supportive than a dismissive "You can't because our security policy says so." These may be trivial examples and training is, of course, not foolproof but contrast the financial and man-time costs of training (£££s) with those of implementing the latest technological means of *trying* to accomplish the same thing (£££££s).

2.9. Shortcomings in the design

Although adherence to the principles of defence in depth has removed any single points of security failure, the solution does feature a large number of single points of potential network failure. Should the Internet circuit, border router or NS208 fail, all Internet services would be lost. Should the PIX 525 or core LAN switch fail, all internal services would fail. All the DMZ servers represent single points of failure for the services they each provide. While clearly not desirable, this is a limitation in the design brought about by financial constraints. However, the solution has been designed with these limitations in mind and adding redundant firewalls, servers, switches, and so on would be a relatively straightforward task. Hopefully the GIACE success story will continue and the necessary funds will soon become available to transform this secure network into one that is both secure and highly available.

Some commentators may frown on the extensive use of VLANs as a security feature in the design. As was stated in section one, VLANs are not foolproof. However, I feel that their inclusion in the design has lead to a much more segregated solution than would have resulted had the only LAN segregation been provided by layer 3 devices. After all, how many physical interfaces can a firewall realistically have?!

Other than the nIDS there are no warning mechanisms in place to alert the IT department when an intrusion attempt is made. Due to the nature of nIDS technologies they can only advise of *attempted* intrusions and cannot determine whether an intrusion was successful (except by secondary evidence such as detection of unexpected outbound connections from a host). In order to check the integrity of individual hosts and check for compromise a host-based IDS system such as *Tripwire* could be deployed. By periodically taking checksums of key files and then comparing consecutive versions, hIDS systems can detect changes to files typically modified or replaced by attackers, for example $HOME/.rhosts, /etc/passwd, index.html, *ps*, etc.

The security of satellite offices is an area of concern. Due to the size of these offices there is insufficient budget to provide the multi-layered security that is

employed at the headquarters. However, by making all services centric to the head office, this concern can be mitigated. The border routers at each satellite office are configured to filter all traffic except IPSec from the IP of the head office firewall. Furthermore, the border router is configured with only a /32 host route to the headquarters firewall via the ISP upstream router. By not configuring a default route on the border router a great number of security threats are mitigated because any attacker would not receive responses to any stimulus traffic sent. As well as meaning that any attack would be blind, this furthermore makes prediction of TCP sequence numbers very difficult unless the attacker has already compromised a system in the ISP's core network. Of course, designing the solution in this way means that should any of the Internet line, border router NS208, etc at the headquarters fail, the satellite offices would also be without Internet access, email, file sharing, and so on.

3. Firewall Policy

Using the secure network architecture and communications matrix formulated in section two, we now proceed to construct the firewall configuration for the NetScreen-208 primary firewall. Some general considerations for construction of the configuration are outlined before a number of specific items are discussed in more detail, using CLI excerpts to illustrate some important aspects of the configuration. Due to the amount of repetition of similar commands and the length restrictions on this paper, the entire configuration file is not shown in this section but rather is presented in Appendix C.

3.1. General firewall configuration considerations

Policies[10] in a firewall configuration are processed in 'top down' order. As soon as a packet matches one policy, the action (permit, drop, tunnel, etc) is performed on the packet and no processing of later policies is done. Therefore when constructing a firewall configuration it is vital to carefully consider the ordering and placement of the various individual policies so that each type of traffic is processed by the intended policy and not by an alternative policy earlier in the configuration. Usually this means that more specific policies are placed earlier in the configuration, with more general policies placed later on.

A second reason to carefully consider the ordering of policies in a configuration is firewall performance. By placing frequently used policies near the top of a policy list, the number of policies that must be processed before a match is found is reduced and thus the performance impact, particularly when there are a large number of policies, is minimised. However, due to the huge horsepower of the NetScreen-208, this second consideration is largely immaterial. The NS208 has a performance ceiling way beyond that which GIACE are likely to require in the next few years. Therefore the ordering of policies in the configuration can be instead arranged in a logical order that makes it easy for the GIACE IT department to understand, thereby simplifying ongoing firewall management.

3.2. Configuration best practices

The firewall configuration denies all traffic other than that which is explicitly permitted. Denied traffic is silently discarded, that is to say that no TCP RST, ICMP port unreachable or other response is sent. In order to retain a record of permitted and denied connections, logging is enabled on all policies except those permitting syslog (to avoid double logging). Logs are sent to the syslog server and are also held locally in a memory buffer, which is overwritten as required.

[10] Note: Many vendors call individual accept/drop lines "rules" and call the entire set of rules the "policy". Somewhat confusingly, NetScreen does things differently, using "policy" to mean each individual accept/drop line. In this section we adopt NetScreen's approach and take "policy" to mean an individual accept/drop line and "configuration" to mean the complete device settings, including all policies.

It is common when compiling firewall policy lists to implement one or more policies that discard 'noisy' (typically broadcast) services such as NetBIOS and DHCP without logging them. This is not required in the solution proposed for GIACE because the NetScreen-208 has access control devices installed on either side of it, meaning that no noisy or broadcast services should ever reach it.

The firewall configuration applies many best practice standards, most of which have fairly obvious motivations. Setting short timeouts on administrative connections; changing the ports used for administrative protocols; restricting administrative access by both IP and interface; logging attempted connections to the firewall itself; using strong passwords; and displaying legal/warning banner messages all help to make the firewall itself more robust.

```
#Short timeouts are applied to network and console management connections
set admin auth timeout 10
set console timeout 10
#Non-standard ports are used for management services
set admin port 32612
set admin ssh port 30947
set ssl port 22978
#Management connections can only be made from the management PC
set admin manager-ip 192.168.9.98 255.255.255.255
#An otherwise unused IP is configured to accept only management connections
set interface ethernet7.4 manage-ip 192.168.9.99
#Management access is disabled on all interfaces other than the one required
unset interface ethernet1 ip manageable
unset interface ethernet2 ip manageable
unset interface ethernet2.1 ip manageable
unset interface ethernet2.2 ip manageable
<similar lines removed>
set interface ethernet7.4 ip manageable
unset interface ethernet8 ip manageable
#Log packets destined to firewall
set firewall log-self
set firewall log-self ike
set firewall log-self snmp
set firewall log-self icmp
set firewall log-self multicast
#Minimum password length is enforced
set admin password restrict length 15
#Banners for SSH and console are configured (note max length of 220 characters)
set admin auth banner telnet login "WARNING: THIS IS A PRIVATE \
SYSTEM. Unauthorised access to this system is forbidden by company
\ policies, national and international laws. By entry into this \
system you are consenting to the monitoring of your activities."
set admin auth banner console login "WARNING: THIS IS A PRIVATE \
SYSTEM. Unauthorised access to this system is forbidden by company
\ policies, national and international laws. By entry into this \
system you are consenting to the monitoring of your activities."
```

3.3. Screening of undesirable traffic

Many (but not all) of ScreenOS's built in defences against specific undesirable traffic types are enabled. This is done on a per zone basis. Controls are implemented to block, amongst other things, redundant IP options (record route, source route, timestamp); bad combinations of TCP flags (SYN+FIN, FIN without ACK, no flags); common attacks based on malformed packets (teardrop, ping of death, winnuke, etc). Although many of these exploits are several years old they still crop up surprisingly frequently. ScreenOS will remove those packets that are specially crafted to try and defeat the firewall. With regard to those attacks that target end systems, any operating system released in the last several years *should* be immune; however it is prudent to add a further layer of protection.

```
set zone "Trust" screen winnuke
set zone "Trust" screen port-scan
set zone "Trust" screen ip-sweep
set zone "Trust" screen tear-drop
set zone "Trust" screen ip-spoofing
set zone "Trust" screen ping-death
set zone "Trust" screen ip-filter-src
set zone "Trust" screen land
set zone "Trust" screen syn-frag
set zone "Trust" screen tcp-no-flag
set zone "Trust" screen unknown-protocol
set zone "Trust" screen ip-bad-option
set zone "Trust" screen ip-record-route
set zone "Trust" screen ip-timestamp-opt
set zone "Trust" screen ip-security-opt
set zone "Trust" screen ip-loose-src-route
set zone "Trust" screen ip-strict-src-route
set zone "Trust" screen ip-stream-opt
set zone "Trust" screen icmp-fragment
set zone "Trust" screen icmp-large
set zone "Trust" screen syn-fin
set zone "Trust" screen fin-no-ack
set zone "Trust" screen mal-url code-red
set zone "Trust" screen syn-ack-ack-proxy
```

The Untrust zone is configured with some further settings to help protect against certain resource starvation attacks. Thresholds are set high enough to avoid generating excessive numbers of alarms but low enough to offer useful protection against concerted attack.

```
set zone "Untrust" screen icmp-flood threshold 200
set zone "Untrust" screen udp-flood threshold 400
set zone "Untrust" screen limit-session source-ip-based 200
set zone "Untrust" screen syn-flood timeout 10
set zone "Untrust" screen syn-flood alarm-threshold 400
```

```
set zone "Untrust" screen syn-flood attack-threshold 400
```

3.4. Policies

The individual firewall policies are not itemised here as they mirror the requirements already detailed in 2.7. In the configuration presented in Appendix C, the policies are referenced against the communications matrix (Table 5).

3.4.1. 'Lookout' policies

Two policies are used to act as sentinels for problems with the ACLs enforced by other layers in the GIACE defences. A service group called *Filtered_Services* is created containing a number of services that should be filtered inbound from the Internet by the border router. A policy is then created that looks for (and denies) inbound *Filtered_Services* traffic trying to cross the firewall. Because no services are allowed direct from the internal network to the Internet the outbound lookout policy denies all services. Any hits on either of these two policies indicate that either the border router or PIX is not enforcing the correct ACLs or that those ACLs have somehow been defeated. Swatch is used to continuously look for hits on these policies and generate alarms accordingly.

```
set group service "Filtered_Services" comment "Should be \
dropped before FW"
set group service "Filtered_Services" add FTP
set group service "Filtered_Services" add SSH
set group service "Filtered_Services" add TELNET
set group service "Filtered_Services" add TFTP
set group service "Filtered_Services" add FINGER
set group service "Filtered_Services" add POP3
<some lines removed>
set policy id 1 from "Untrust" to "Global" "Any" "Any" \
"Filtered_Services" deny log
set policy id 2 from "Trust" to "Untrust" "Any" "Any" ANY deny log
```

3.4.2. ALG policies

ScreenOS's application-layer gateways (ALGs) are used to add some layer 7 syntactical checking to inbound connections to the three public servers (DNS, HTTP and SMTP).

```
set zone "Untrust" reassembly-for-alg
set policy id 3 from "Untrust" to "Global" "Any" \
"MIP(192.0.2.3)" "HTTP" permit log
set policy id 3 application HTTP
set policy id 4 from "Untrust" to "Global" "Any" \
"MIP(192.0.2.4)" "MAIL" permit log
set policy id 4 application SMTP
set policy id 5 from "Untrust" to "Global" "Any" \
"MIP(192.0.2.5)" "DNS-UDP" permit log
set policy id 5 application DNS
```

3.4.3. Intra-zone policies

The default behaviour of NetScreens is to implicitly permit all traffic between hosts in the same zone. This is contrary to our stance of denying all traffic except that which is explicitly permitted. Therefore, intra-zone blocking is enabled for all zones to ensure that traffic between hosts in the same zone is dropped by default.

```
set zone "Trust" block
set zone "Untrust" block
set zone "Public_DMZ" block
set zone "Encrypted_DMZ" block
set zone "Unencrypted_DMZ" block
set zone "SemiPrivate_DMZ" block
set zone "Private_DMZ" block
set zone "Mgmt_DMZ" block
```

3.5. NAT

MIPs are configured to statically (1-to-1) NAT traffic to the publicly available servers. DIPs are configured to dynamically (many-to-1) NAT hosts that only make outgoing connections behind a 'phantom' IP that is not used elsewhere and does not appear in DNS. This helps (although only a little!) to mask the source of communications from other Internet users. The management PC has a dedicated phantom IP of 192.0.2.8 while all other servers (such as the NTP server and proxy server) share the phantom IP of 192.0.2.7.

```
set interface "ethernet1" mip 192.0.2.3 host 192.168.9.2 \
netmask 255.255.255.255 vrouter "trust-vr"
set interface "ethernet1" mip 192.0.2.4 host 192.168.9.10 \
netmask 255.255.255.255 vrouter "trust-vr"
set interface "ethernet1" mip 192.0.2.5 host 192.168.9.18 \
netmask 255.255.255.255 vrouter "trust-vr"
set interface "ethernet1" mip 192.0.2.6 host 192.168.9.34 \
netmask 255.255.255.255 vrouter "trust-vr"
set interface "ethernet1" dip 4 192.0.2.7 192.0.2.7
set interface "ethernet1" dip 5 192.0.2.8 192.0.2.8
```

3.6. VPNs

Route-based VPNs are selected over policy-based VPNs as they offer more flexibility in creating policies; easier setup and modification; and allow for future implementation of dynamic tunnel failover. The VPNs are configured using the encryption and authentication methods discussed in 2.6.4. The maximum segment size for tunnelled TCP traffic is reduced to avoid fragmentation issues due to the overhead IPSec places on packet size.

```
set ike p1-proposal "pre-g5-3des-sha" preshare group5 esp \
3des sha-1
set ike p2-proposal "g5-esp-aes256-md5" group5 esp aes256 \
md5 second 3600
set interface "tunnel.1" zone "Unencrypted_DMZ"
set interface "tunnel.2" zone "Unencrypted_DMZ"
<similar lines removed>
set ike gateway "NewYork-ns5gt_ph1" address 1.1.1.1 Main \
outgoing-interface "ethernet1" preshare <removed> proposal \
"pre-g5-3des-sha"
set ike gateway "CapeTown-ns5gt_ph1" address 2.2.2.2 Main \
outgoing-interface "ethernet1" preshare <removed> proposal \
"pre-g5-3des-sha"
<similar lines removed>
set vpn "NewYork-ns5gt_ph2" gateway "NewYork-ns5gt_ph1" \
replay tunnel idletime 0 proposal "g5-esp-aes256-md5"
set vpn "NewYork-ns5gt_ph2" monitor rekey
set vpn "NewYork-ns5gt_ph2" bind interface tunnel.1
set vpn "NewYork-ns5gt_ph2" proxy-id local-ip 172.22.8.0/22 \
remote-ip 172.22.20.0/24 "ANY"
set vpn "CapeTown-ns5gt_ph2" gateway "CapeTown-ns5gt_ph1" \
replay tunnel idletime 0 proposal "g5-esp-aes256-md5"
set vpn "CapeTown-ns5gt_ph2" monitor rekey
set vpn "CapeTown-ns5gt_ph2" bind interface tunnel.2
set vpn "CapeTown-ns5gt_ph2" proxy-id local-ip 172.22.8.0/22 \
remote-ip 172.22.21.0/24 "ANY"
<similar lines removed>
set flow tcp-mss 1400
```

3.7. Routing

The Untrust virtual router (VR), which contains only the Untrust zone, has no routes to the Trust VR, which contains all other zones. This helps to isolate the Untrust zone from the other zones. The Trust VR has a default route to the Untrust VR; a static route to the pool of IPs assigned to RAS VPN users via the private interface of the VPN Concentrator; and static routes to the internal networks via the PIX.

```
set vrouter "untrust-vr"
set route  0.0.0.0/0 interface ethernet1 gateway 192.0.2.1
exit
set vrouter "trust-vr"
set route  192.168.10.0/24 interface ethernet4 gateway \
192.168.9.26
set route  192.168.8.0/28 interface ethernet8 gateway \
192.168.9.253
set route  172.22.8.0/22 interface ethernet8 gateway \
192.168.9.253
```

```
set route 0.0.0.0/0 vrouter "untrust-vr"
exit
```

3.7.1. Routing to VPN sites

The Trust VR also has static routes to the remote VPN sites via the appropriate tunnel interfaces. If a VPN fails the tunnel interface goes down and its routes are removed. In this situation private traffic would route to the Internet via the combined default routes of he two VRs, resulting in an unwanted leakage. (NB: in reality our defence in depth approach would mean that the border router would discard this private traffic but nevertheless it is prudent to stop it leaving the exterior firewall). To prevent this potential leakage, corresponding higher metric routes are configured to point to the syslog server. The syslog server is acting as a pseudo bit bucket (in ScreenOS v5 the NetScreen has no *null* interface), and has IP forwarding disabled to avoid looping the traffic.

```
set vrouter "trust-vr"
set route  172.22.20.0/24 interface tunnel.1
set route  172.22.20.0/24 interface e7.2 gateway \
192.168.9.82 metric 99
set route  172.22.21.0/24 interface tunnel.2
set route  172.22.21.0/24 interface e7.2 gateway \
192.168.9.82 metric 99
set route  172.22.22.0/24 interface tunnel.3
set route  172.22.22.0/24 interface e7.2 gateway \
192.168.9.82 metric 99
set route  172.22.23.0/24 interface tunnel.4
set route  172.22.23.0/24 interface e7.2 gateway \
192.168.9.82 metric 99
set route  172.16.0.0/16 interface tunnel.5
set route  172.16.0.0/16 interface e7.2 gateway \
192.168.9.82 metric 99
exit
```

4. Appendices

4.1. Appendix A: Example VACL configuration

This is an IOS configuration based on the example used in 1.3.2. Only the salient parts of the configuration are shown.

```
#Create extended access-lists
ip access-list extended DMZ_Syslog
 remark Match syslog from DMZ to syslog server
 permit udp 192.0.2.0 0.0.0.255 host 192.0.2.14 eq syslog
 exit
!
ip access-list extended SMTP_Out
 remark Match SMTP from both mail servers
 #Permit both mail servers to send mail anywhere
 permit tcp 192.0.2.10 0.0.0.1 any eq smtp
 permit tcp any eq smtp 192.0.2.10 0.0.0.1          #Matches reply packets
 exit
!
ip access-list extended SMTP_In
 remark Match SMTP to both mail servers
 #Do not permit other DMZ hosts to talk to mail servers (no reverse rule required as no
initial SYN means no later SYN/ACK, etc)
 deny tcp 192.0.2.0 0.0.0.255 192.0.2.10 0.0.0.1 eq smtp
 #Permit both mail servers to receive mail from anywhere outside DMZ
 permit tcp any 192.0.2.10 0.0.0.1 eq smtp
 permit tcp 192.0.2.10 0.0.0.1 eq smtp any
 exit
!
ip access-list extended HTTP_In
 remark Match HTTP to web server
 #Do not permit other DMZ hosts to talk to web server
 deny tcp 192.0.2.0 0.0.0.255 host 192.0.2.12 eq www
 #Permit web requests from anywhere outside DMZ
 permit tcp any host 192.0.2.12 eq www
 permit tcp host 192.0.2.12 eq www any
 exit
!
ip access-list extended FTP_In
 remark Match FTP to FTP server
 #Do not permit other DMZ hosts to talk to FTP server
 deny tcp 192.0.2.0 0.0.0.255 host 192.0.2.13 eq ftp
 #Permit FTP control connections from anywhere outside DMZ
 permit tcp any host 192.0.2.13 eq ftp
 permit tcp host 192.0.2.13 eq ftp any
 #Permit active FTP data connection
 permit tcp host 192.0.2.13 eq ftp-data any
 permit tcp any host 192.0.2.13 eq ftp-data
 #Permit passive FTP data connection
```

```
 permit tcp any host 192.0.2.13 gt 1023
 permit tcp host 192.0.2.13 gt 1023 any
 exit
!
ip access-list extended Catch_All
 remark Match all traffic
 permit ip any any
 exit
!
!
#Access-map is created to link together access-lists in correct order
vlan access-map DMZ_VACL 10
 match ip address DMZ_Syslog
 action forward
 exit
!
vlan access-map DMZ_VACL 20
 match ip address SMTP_Out
 action forward
 exit
!
vlan access-map DMZ_VACL 30
 match ip address SMTP_In
 action forward
 exit
!
vlan access-map DMZ_VACL 40
 match ip address HTTP_In
 action forward
 exit
!
vlan access-map DMZ_VACL 50
 match ip address FTP_In
 action forward
 exit
!
vlan access-map DMZ_VACL 90
 match ip address extended Catch_All
 action drop log
 exit
!
!
#VLAN filter is applied to VLAN2
vlan filter DMZ_VACL vlan-list 2
!
!
#All interfaces are placed into VLAN2
interface FastEthernet0/1
 description Connection to Firewall
 switchport access vlan 2
 switchport mode access
```

```
!
interface FastEthernet0/2
 description Connection to SMTP1
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/3
 description Connection to SMTP2
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/4
 description Connection to WWW
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/5
 description Connection to FTP
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/6
 description Connection to Syslog
 switchport access vlan 2
 switchport mode access
!
end
```

4.2. Appendix B: Example VLAN-aware firewall configuration

These are ScreenOS and IOS configurations based on the example used in 1.4.2. Only the salient parts of the configurations are shown.

#Configure IP addressing and VLAN membership for sub-interfaces

```
set interface eth2.1 tag 2 zone dmz
set interface eth2.1 ip 192.0.2.9/30
set interface eth2.1 route
set interface eth2.2 tag 3 zone dmz
set interface eth2.2 ip 192.0.2.5/30
set interface eth2.2 route
set interface eth2.3 tag 4 zone dmz
set interface eth2.3 ip 192.0.2.17/30
set interface eth2.3 route
set interface eth2.4 tag 5 zone dmz
set interface eth2.4 ip 192.0.2.21/30
set interface eth2.4 route
set interface eth2.5 tag 6 zone dmz
set interface eth2.5 ip 192.0.2.13/30
set interface eth2.5 route
```

#This is a critical line. Without it intra-zone traffic is not subject to policy table look-up!

```
set zone dmz block
```

#Reassemble fragments that may otherwise be missed by deep packet inspection

```
set zone dmz reassembly-for-alg
```

#These lines are configured to apply additional protection against common malicious packet types. They are a good illustration of how VLAN-aware firewalls can offer more than 'just' the addition of stateful-ness and logging to VLAN-based defence, when compared with VACLs

```
set zone dmz screen icmp-flood
set zone dmz screen udp-flood
set zone dmz screen winnuke
set zone dmz screen port-scan
set zone dmz screen ip-sweep
set zone dmz screen tear-drop
set zone dmz screen syn-flood
set zone dmz screen ping-death
set zone dmz screen ip-filter-src
set zone dmz screen land
set zone dmz screen syn-frag
set zone dmz screen tcp-no-flag
set zone dmz screen unknown-protocol
set zone dmz screen ip-bad-option
set zone dmz screen ip-record-route
set zone dmz screen ip-timestamp-opt
set zone dmz screen ip-security-opt
set zone dmz screen ip-loose-src-route
set zone dmz screen ip-strict-src-route
set zone dmz screen ip-stream-opt
```

```
set zone dmz screen icmp-fragment
set zone dmz screen syn-fin
set zone dmz screen mal-url code-red
set zone dmz screen syn-ack-ack-proxy

#Define address book entries and groups
set address trust Internal_Mail1 172.16.1.1/32
set address trust Internal_Mail2 172.17.1.1/32
set group address trust Internal_Mail add Internal_Mail1
set group address trust Internal_Mail add Internal_Mail2
set address dmz SMTP1 192.0.2.10/32
set address dmz SMTP2 192.0.2.6/32
set address dmz WWW_Server 192.0.2.18/32
set address dmz FTP_Server 192.0.2.22/32
set address dmz Syslog 192.0.2.14/32
set group address dmz SMTP_Servers add SMTP1
set group address dmz SMTP_Servers add SMTP2
set group address dmz Syslog_Clients add SMTP1
set group address dmz Syslog_Clients add SMTP2
set group address dmz Syslog_Clients add WWW_Server
set group address dmz Syslog_Clients add FTP_Server
set address untrust External_Nameserver1 158.43.128.72/32
set address untrust External_Nameserver2 217.35.209.188/32
set group address untrust External_Nameservers add
External_Nameserver1
set group address untrust External_Nameservers add
External_Nameserver2

#Define policies
#Intra-zone blocking is enabled so we need to explicitly define the necessary DMZ-->DMZ
policies for mail and syslog
#Policies 1-3 check that traffic is actually SMTP/HTTP/FTP by checking layer 7 information,
not just by checking the destination port number
set policy id 1 from untrust to dmz Any SMTP_Servers MAIL permit
log
set policy id 1 application smtp
set policy id 2 from untrust to dmz Any WWW_Server HTTP permit log
set policy id 2 application http
set policy id 3 from untrust to dmz Any FTP_Server FTP permit log
set policy id 3 application ftp
set policy id 4 from untrust to dmz Any Any ANY deny log
set policy id 5 from dmz to untrust SMTP_Servers
External_Nameservers dns permit log
set policy id 6 from dmz to untrust SMTP_Servers any MAIL permit
log
set policy id 7 from dmz to untrust Any Any ANY deny log
#Probably don't want to log syslog!
set policy id 8 from dmz to dmz Syslog_Clients Syslog syslog permit
set policy id 9 from dmz to dmz SMTP_Servers SMTP_Servers MAIL
permit log
set policy id 10 from dmz to dmz Any Any ANY deny log
set policy id 11 from dmz to trust SMTP_Servers Internal_Mail MAIL
permit log
```

```
set policy id 12 from dmz to trust Any Any ANY deny log
set policy id 13 from trust to dmz Internal_Mail SMTP_Servers MAIL
permit log
set policy id 14 from trust to dmz Any Any ANY deny log

---

#Create necessary VLANs.  Don't use VLAN1!
vlan 2
!
vlan 3
!
vlan 4
!
vlan 5
!
vlan 6
!
!
#Port 1 is a trunk connection to Eth2 on the NetScreen
#NB: port-security cannot be configured on trunk ports
interface FastEthernet0/1
 description Trunk to NetScreen eth2
 switchport mode trunk
!
#Ports 2-6 are access ports for DMZ servers.  Each is in a different VLAN to match up with
the tagging applied by the NetScreen.
interface FastEthernet0/2
 description Connection to SMTP1
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security mac-address 0000.2222.3333
!
interface FastEthernet0/3
 description Connection to SMTP2
 switchport access vlan 3
 switchport mode access
 switchport port-security
 switchport port-security mac-address 0000.3333.4444
!
interface FastEthernet0/4
 description Connection to WWW_Server
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security mac-address 0000.4444.5555
!
interface FastEthernet0/5
 description Connection to FTP_Server
 switchport access vlan 5
 switchport mode access
 switchport port-security
```

```
 switchport port-security mac-address 0000.5555.6666
!
interface FastEthernet0/6
 description Connection to Syslog
 switchport access vlan 6
 switchport mode access
 switchport port-security
 switchport port-security mac-address 0000.6666.7777
!
end
```

4.3. Appendix C: NetScreen-208 configuration

```
#Clock is set by NTP with zero offset from GMT
set clock ntp
set clock timezone 0
#Routes from trust-vr do not automatically populate untrust-vr
unset vrouter "trust-vr" auto-route-export
#Define non-default ports/protocols.  NB: Default DNS service includes both TCP and UDP so define a new
service for inbound nameserver requests using only 53/udp
set service "Alternate_SSH" protocol tcp src-port 1024-65535 dst-port 30947-30947
set service "DNS-UDP" protocol udp src-port 1024-65535 dst-port 53-53
set service "Fixed_RPC_Range" protocol tcp src-port 1024-65535 dst-port 5000-5020
set service "IPSec" protocol udp src-port 500-500 dst-port 500-500
set service "IPSec" + 50 src-port 0-65535 dst-port 0-65535
set service "Kerberos" protocol tcp src-port 1024-65535 dst-port 88-88
set service "Kerberos" + udp src-port 1024-65535 dst-port 88-88
set service "LDAP_UDP" protocol udp src-port 1024-65535 dst-port 389-389
set service "LDAP_SSL" protocol tcp src-port 1024-65535 dst-port 636-636
set service "LDAP_GlobalCatalogue" protocol tcp src-port 1024-65535 dst-port 3268-3269
set service "MS_Exchange" protocol tcp src-port 1024-65535 dst-port 135-135
set service "MS_Exchange" + tcp src-port 1024-65535 dst-port 5000-5001
set service "MS_Filesharing" protocol tcp src-port 1024-65535 dst-port 135-135
set service "MS_Filesharing" + udp src-port 1024-65535 dst-port 135-135
set service "MS_Filesharing" + udp src-port 1024-65535 dst-port 137-138
set service "MS_Filesharing" + tcp src-port 1024-65535 dst-port 139-139
set service "MS_Filesharing" + tcp src-port 1024-65535 dst-port 445-445
set service "MS_Terminal_Services" protocol tcp src-port 0-65535 dst-port 3389-3389
set service "MySQL" protocol tcp src-port 1024-65535 dst-port 3306-3306
set service "Proxy_HTTP" protocol tcp src-port 1024-65535 dst-port 8080-8080
set service "SNMP-TRAP" protocol udp src-port 0-65535 dst-port 162-162
set service "UDP_1434" protocol udp src-port 0-65535 dst-port 1434-1434
set service "VNC" protocol tcp src-port 1024-65535 dst-port 5900-5900
set service "WINS" protocol tcp src-port 1024-65535 dst-port 42-42
#User authentication is done by onboard database
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
#Add separate read-write and read-only users; passwords must be • 15 characters
set admin name rw-admin
set admin password restrict length 15
set admin password gk1EZi2hUuYcbLGb
set admin user "ro-admin" password EhlAyd5Twa5b378l privilege "read-only"
#Management connections can only be made from the management PC
set admin manager-ip 192.168.9.98 255.255.255.255
#Change default management ports (NB: We are disabling HTTP management but change port from default 80
anyway)
set admin port 32612
set admin ssh port 30947
#Set number of failed logins before closing administrative connections and session timeout
set admin access attempts 3
set admin auth timeout 10
#Administrator authentication is done by onboard database
set admin auth server "Local"
#Set appropriate logon banner messages
set admin auth banner telnet login "WARNING: THIS IS A PRIVATE SYSTEM. Unauthorised access to this
system is forbidden by company policies, national and international laws. By entry into this system you are
consenting to the monitoring of your activities."
set admin auth banner console login "WARNING: THIS IS A PRIVATE SYSTEM. Unauthorised access to this
system is forbidden by company policies, national and international laws. By entry into this system you are
consenting to the monitoring of your activities."
#when config file is dumped (eg using TFTP) UNIX-style LF line breaks are used, as opposed to DOS-style
CRLF
```

```
set admin format unix
#Create security zones in addition to the default 'Untrust', 'DMZ' and 'Trust' zones ('DMZ' is not used to avoid
confusion)
set zone name "Public_DMZ"
set zone name "Encrypted_DMZ"
set zone name "Unencrypted_DMZ"
set zone name "SemiPrivate_DMZ"
set zone name "Private_DMZ"
set zone name "Mgmt_DMZ"
#All zones are placed in the trusted virtual router except 'Untrust', which is placed in the untrusted VR
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "untrust-vr"
set zone "Public_DMZ" vrouter "trust-vr"
set zone "Encrypted_DMZ" vrouter "trust-vr"
set zone "Unencrypted_DMZ" vrouter "trust-vr"
set zone "SemiPrivate_DMZ" vrouter "trust-vr"
set zone "Private_DMZ" vrouter "trust-vr"
set zone "Mgmt_DMZ" vrouter "trust-vr"
#No intra-zone communications are implicitly allowed - specific policies are required
#Packets out of state are responded to with a TCP reset except for those entering from the Internet
set zone "Trust" block
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "Public_DMZ" block
set zone "Public_DMZ" tcp-rst
set zone "Encrypted_DMZ" block
set zone "Encrypted_DMZ" tcp-rst
set zone "Unencrypted_DMZ" block
set zone "Unencrypted_DMZ" tcp-rst
set zone "SemiPrivate_DMZ" block
set zone "SemiPrivate_DMZ" tcp-rst
set zone "Private_DMZ" block
set zone "Private_DMZ" tcp-rst
set zone "Mgmt_DMZ" block
set zone "Mgmt_DMZ" tcp-rst
#Most of ScreenOS's protections against undesirable packet types, lengths, options, etc are enabled for every
security zone
set zone "Trust" screen winnuke
set zone "Trust" screen port-scan
set zone "Trust" screen ip-sweep
set zone "Trust" screen tear-drop
set zone "Trust" screen ip-spoofing
set zone "Trust" screen ping-death
set zone "Trust" screen ip-filter-src
set zone "Trust" screen land
set zone "Trust" screen syn-frag
set zone "Trust" screen tcp-no-flag
set zone "Trust" screen unknown-protocol
set zone "Trust" screen ip-bad-option
set zone "Trust" screen ip-record-route
set zone "Trust" screen ip-timestamp-opt
set zone "Trust" screen ip-security-opt
set zone "Trust" screen ip-loose-src-route
set zone "Trust" screen ip-strict-src-route
set zone "Trust" screen ip-stream-opt
set zone "Trust" screen icmp-fragment
set zone "Trust" screen icmp-large
set zone "Trust" screen syn-fin
set zone "Trust" screen fin-no-ack
set zone "Trust" screen mal-url code-red
set zone "Trust" screen syn-ack-ack-proxy
set zone "Untrust" screen icmp-flood
```

```
set zone "Untrust" screen udp-flood
set zone "Untrust" screen winnuke
set zone "Untrust" screen port-scan
set zone "Untrust" screen ip-sweep
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ip-spoofing
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "Untrust" screen syn-frag
set zone "Untrust" screen tcp-no-flag
set zone "Untrust" screen unknown-protocol
set zone "Untrust" screen ip-bad-option
set zone "Untrust" screen ip-record-route
set zone "Untrust" screen ip-timestamp-opt
set zone "Untrust" screen ip-security-opt
set zone "Untrust" screen ip-loose-src-route
set zone "Untrust" screen ip-strict-src-route
set zone "Untrust" screen ip-stream-opt
set zone "Untrust" screen icmp-fragment
set zone "Untrust" screen icmp-large
set zone "Untrust" screen syn-fin
set zone "Untrust" screen fin-no-ack
set zone "Untrust" screen mal-url code-red
set zone "Untrust" screen syn-ack-ack-proxy
#Reassemble inbound fragments before deep packet inspection to help prevent fragmentation-based
avoidance tactics
set zone "Untrust" reassembly-for-alg
set zone "Public_DMZ" screen winnuke
set zone "Public_DMZ" screen port-scan
set zone "Public_DMZ" screen ip-sweep
set zone "Public_DMZ" screen tear-drop
set zone "Public_DMZ" screen ip-spoofing
set zone "Public_DMZ" screen ping-death
set zone "Public_DMZ" screen ip-filter-src
set zone "Public_DMZ" screen land
set zone "Public_DMZ" screen syn-frag
set zone "Public_DMZ" screen tcp-no-flag
set zone "Public_DMZ" screen unknown-protocol
set zone "Public_DMZ" screen ip-bad-option
set zone "Public_DMZ" screen ip-record-route
set zone "Public_DMZ" screen ip-timestamp-opt
set zone "Public_DMZ" screen ip-security-opt
set zone "Public_DMZ" screen ip-loose-src-route
set zone "Public_DMZ" screen ip-strict-src-route
set zone "Public_DMZ" screen ip-stream-opt
set zone "Public_DMZ" screen icmp-fragment
set zone "Public_DMZ" screen icmp-large
set zone "Public_DMZ" screen syn-fin
set zone "Public_DMZ" screen fin-no-ack
set zone "Public_DMZ" screen mal-url code-red
set zone "Public_DMZ" screen syn-ack-ack-proxy
set zone "Encrypted_DMZ" screen winnuke
set zone "Encrypted_DMZ" screen port-scan
set zone "Encrypted_DMZ" screen ip-sweep
set zone "Encrypted_DMZ" screen tear-drop
set zone "Encrypted_DMZ" screen ip-spoofing
set zone "Encrypted_DMZ" screen ping-death
set zone "Encrypted_DMZ" screen ip-filter-src
set zone "Encrypted_DMZ" screen land
set zone "Encrypted_DMZ" screen syn-frag
set zone "Encrypted_DMZ" screen tcp-no-flag
```

```
set zone "Encrypted_DMZ" screen unknown-protocol
set zone "Encrypted_DMZ" screen ip-bad-option
set zone "Encrypted_DMZ" screen ip-record-route
set zone "Encrypted_DMZ" screen ip-timestamp-opt
set zone "Encrypted_DMZ" screen ip-security-opt
set zone "Encrypted_DMZ" screen ip-loose-src-route
set zone "Encrypted_DMZ" screen ip-strict-src-route
set zone "Encrypted_DMZ" screen ip-stream-opt
set zone "Encrypted_DMZ" screen icmp-fragment
set zone "Encrypted_DMZ" screen icmp-large
set zone "Encrypted_DMZ" screen syn-fin
set zone "Encrypted_DMZ" screen fin-no-ack
set zone "Encrypted_DMZ" screen mal-url code-red
set zone "Encrypted_DMZ" screen syn-ack-ack-proxy
set zone "Unencrypted_DMZ" screen winnuke
set zone "Unencrypted_DMZ" screen port-scan
set zone "Unencrypted_DMZ" screen ip-sweep
set zone "Unencrypted_DMZ" screen tear-drop
set zone "Unencrypted_DMZ" screen ip-spoofing
set zone "Unencrypted_DMZ" screen ping-death
set zone "Unencrypted_DMZ" screen ip-filter-src
set zone "Unencrypted_DMZ" screen land
set zone "Unencrypted_DMZ" screen syn-frag
set zone "Unencrypted_DMZ" screen tcp-no-flag
set zone "Unencrypted_DMZ" screen unknown-protocol
set zone "Unencrypted_DMZ" screen ip-bad-option
set zone "Unencrypted_DMZ" screen ip-record-route
set zone "Unencrypted_DMZ" screen ip-timestamp-opt
set zone "Unencrypted_DMZ" screen ip-security-opt
set zone "Unencrypted_DMZ" screen ip-loose-src-route
set zone "Unencrypted_DMZ" screen ip-strict-src-route
set zone "Unencrypted_DMZ" screen ip-stream-opt
set zone "Unencrypted_DMZ" screen icmp-fragment
set zone "Unencrypted_DMZ" screen icmp-large
set zone "Unencrypted_DMZ" screen syn-fin
set zone "Unencrypted_DMZ" screen fin-no-ack
set zone "Unencrypted_DMZ" screen mal-url code-red
set zone "Unencrypted_DMZ" screen syn-ack-ack-proxy
set zone "SemiPrivate_DMZ" screen winnuke
set zone "SemiPrivate_DMZ" screen port-scan
set zone "SemiPrivate_DMZ" screen ip-sweep
set zone "SemiPrivate_DMZ" screen tear-drop
set zone "SemiPrivate_DMZ" screen ip-spoofing
set zone "SemiPrivate_DMZ" screen ping-death
set zone "SemiPrivate_DMZ" screen ip-filter-src
set zone "SemiPrivate_DMZ" screen land
set zone "SemiPrivate_DMZ" screen syn-frag
set zone "SemiPrivate_DMZ" screen tcp-no-flag
set zone "SemiPrivate_DMZ" screen unknown-protocol
set zone "SemiPrivate_DMZ" screen ip-bad-option
set zone "SemiPrivate_DMZ" screen ip-record-route
set zone "SemiPrivate_DMZ" screen ip-timestamp-opt
set zone "SemiPrivate_DMZ" screen ip-security-opt
set zone "SemiPrivate_DMZ" screen ip-loose-src-route
set zone "SemiPrivate_DMZ" screen ip-strict-src-route
set zone "SemiPrivate_DMZ" screen ip-stream-opt
set zone "SemiPrivate_DMZ" screen icmp-fragment
set zone "SemiPrivate_DMZ" screen icmp-large
set zone "SemiPrivate_DMZ" screen syn-fin
set zone "SemiPrivate_DMZ" screen fin-no-ack
set zone "SemiPrivate_DMZ" screen mal-url code-red
set zone "SemiPrivate_DMZ" screen syn-ack-ack-proxy
set zone "Private_DMZ" screen winnuke
```

```
set zone "Private_DMZ" screen port-scan
set zone "Private_DMZ" screen ip-sweep
set zone "Private_DMZ" screen tear-drop
set zone "Private_DMZ" screen ip-spoofing
set zone "Private_DMZ" screen ping-death
set zone "Private_DMZ" screen ip-filter-src
set zone "Private_DMZ" screen land
set zone "Private_DMZ" screen syn-frag
set zone "Private_DMZ" screen tcp-no-flag
set zone "Private_DMZ" screen unknown-protocol
set zone "Private_DMZ" screen ip-bad-option
set zone "Private_DMZ" screen ip-record-route
set zone "Private_DMZ" screen ip-timestamp-opt
set zone "Private_DMZ" screen ip-security-opt
set zone "Private_DMZ" screen ip-loose-src-route
set zone "Private_DMZ" screen ip-strict-src-route
set zone "Private_DMZ" screen ip-stream-opt
set zone "Private_DMZ" screen icmp-fragment
set zone "Private_DMZ" screen icmp-large
set zone "Private_DMZ" screen syn-fin
set zone "Private_DMZ" screen fin-no-ack
set zone "Private_DMZ" screen mal-url code-red
set zone "Private_DMZ" screen syn-ack-ack-proxy
set zone "Mgmt_DMZ" screen winnuke
set zone "Mgmt_DMZ" screen port-scan
set zone "Mgmt_DMZ" screen ip-sweep
set zone "Mgmt_DMZ" screen tear-drop
set zone "Mgmt_DMZ" screen ip-spoofing
set zone "Mgmt_DMZ" screen ping-death
set zone "Mgmt_DMZ" screen ip-filter-src
set zone "Mgmt_DMZ" screen land
set zone "Mgmt_DMZ" screen syn-frag
set zone "Mgmt_DMZ" screen tcp-no-flag
set zone "Mgmt_DMZ" screen unknown-protocol
set zone "Mgmt_DMZ" screen ip-bad-option
set zone "Mgmt_DMZ" screen ip-record-route
set zone "Mgmt_DMZ" screen ip-timestamp-opt
set zone "Mgmt_DMZ" screen ip-security-opt
set zone "Mgmt_DMZ" screen ip-loose-src-route
set zone "Mgmt_DMZ" screen ip-strict-src-route
set zone "Mgmt_DMZ" screen ip-stream-opt
set zone "Mgmt_DMZ" screen icmp-fragment
set zone "Mgmt_DMZ" screen icmp-large
set zone "Mgmt_DMZ" screen syn-fin
set zone "Mgmt_DMZ" screen fin-no-ack
set zone "Mgmt_DMZ" screen mal-url code-red
set zone "Mgmt_DMZ" screen syn-ack-ack-proxy
#Apply rate limiting on certain inbound traffic to help mitigate resource starvation attacks
set zone "Untrust" screen icmp-flood threshold 200
set zone "Untrust" screen udp-flood threshold 400
set zone "Untrust" screen limit-session source-ip-based 200
set zone "Untrust" screen syn-flood timeout 10
set zone "Untrust" screen syn-flood alarm-threshold 400
set zone "Untrust" screen syn-flood attack-threshold 400
#Speed and duplex are specified on all interfaces and likewise on the connecting switches/hosts!!
set interface ethernet1 phy full 100mb
set interface ethernet2 phy full 100mb
set interface ethernet3 phy full 100mb
set interface ethernet4 phy full 100mb
set interface ethernet5 phy full 100mb
set interface ethernet6 phy full 100mb
set interface ethernet7 phy full 100mb
set interface ethernet8 phy full 100mb
```

```
#Define zone and VLAN membership of interfaces and sub-interfaces
set interface "ethernet1" zone "Untrust"
set interface "ethernet2.1" tag 21 zone "Public_DMZ"
set interface "ethernet2.2" tag 22 zone "Public_DMZ"
set interface "ethernet2.3" tag 23 zone "Public_DMZ"
set interface "ethernet3.1" tag 31 zone "Encrypted_DMZ"
set interface "ethernet3.2" tag 32 zone "Encrypted_DMZ"
set interface "ethernet4" zone "Unencrypted_DMZ"
set interface "ethernet5.1" tag 51 zone "SemiPrivate_DMZ"
set interface "ethernet5.2" tag 52 zone "SemiPrivate_DMZ"
set interface "ethernet6.1" tag 61 zone "Private_DMZ"
set interface "ethernet6.2" tag 62 zone "Private_DMZ"
set interface "ethernet7.1" tag 71 zone "Mgmt_DMZ"
set interface "ethernet7.2" tag 72 zone "Mgmt_DMZ"
set interface "ethernet7.3" tag 73 zone "Mgmt_DMZ"
set interface "ethernet7.4" tag 74 zone "Mgmt_DMZ"
set interface "ethernet8" zone "Trust"
#Route-based VPNs are terminated in the 'Unencrypted_DMZ' zone so that VPN traffic is subject to a firewall
lookup following decryption
set interface "tunnel.1" zone "Unencrypted_DMZ"
set interface "tunnel.2" zone "Unencrypted_DMZ"
set interface "tunnel.3" zone "Unencrypted_DMZ"
set interface "tunnel.4" zone "Unencrypted_DMZ"
set interface "tunnel.5" zone "Unencrypted_DMZ"
#Define IP addressing of interfaces & sub-interfaces and disable interface-based NAT
#Tunnel interfaces are unnumbered to the interface in the Unencrypted_DMZ zone
unset interface vlan1 ip
set interface ethernet1 ip 192.0.2.2/27
set interface ethernet1 route
set interface ethernet2.1 ip 192.168.9.1/29
set interface ethernet2.1 route
set interface ethernet2.2 ip 192.168.9.9/29
set interface ethernet2.2 route
set interface ethernet2.2 ip 192.168.9.17/29
set interface ethernet2.2 route
set interface ethernet3.1 ip 192.0.2.33/29
set interface ethernet3.1 route
set interface ethernet3.2 ip 192.168.9.33/29
set interface ethernet3.2 route
set interface ethernet4 ip 192.168.9.25/29
set interface ethernet4 route
set interface ethernet5.1 ip192.168.9.41/29
set interface ethernet5.1 route
set interface ethernet5.2 ip 192.168.9.49/29
set interface ethernet5.2 route
set interface ethernet6.1 ip 192.168.9.57/29
set interface ethernet6.1 route
set interface ethernet6.2 ip 192.168.9.65/29
set interface ethernet6.2 route
set interface ethernet7.1 ip 192.168.9.73/29
set interface ethernet7.1 route
set interface ethernet7.2 ip 192.168.9.81/29
set interface ethernet7.2 route
set interface ethernet7.3 ip 192.168.9.89/29
set interface ethernet7.3 route
set interface ethernet7.4 ip 192.168.9.97/29
set interface ethernet7.4 route
set interface ethernet8 ip 192.168.9.254/29
set interface ethernet8 route
set interface tunnel.1 ip unnumbered interface ethernet4
set interface tunnel.2 ip unnumbered interface ethernet4
set interface tunnel.3 ip unnumbered interface ethernet4
set interface tunnel.4 ip unnumbered interface ethernet4
```

```
set interface tunnel.5 ip unnumbered interface ethernet4
#Restrict access so that management connections can only be made via eth7.4 and to a dedicated
management IP.  Disable cleartext management protocols (telnet, SNMP & HTTP)
set interface ethernet7.4 manage-ip 192.168.9.99
unset interface vlan1 ip manageable
unset interface ethernet1 ip manageable
unset interface ethernet2 ip manageable
unset interface ethernet2.1 ip manageable
unset interface ethernet2.2 ip manageable
unset interface ethernet2.3 ip manageable
unset interface ethernet3 ip manageable
unset interface ethernet3.1 ip manageable
unset interface ethernet3.2 ip manageable
unset interface ethernet4 ip manageable
unset interface ethernet5 ip manageable
unset interface ethernet5.1 ip manageable
unset interface ethernet5.2 ip manageable
unset interface ethernet6 ip manageable
unset interface ethernet6.1 ip manageable
unset interface ethernet6.2 ip manageable
unset interface ethernet7.1 ip manageable
unset interface ethernet7.2 ip manageable
unset interface ethernet7.3 ip manageable
set interface ethernet7.4 ip manageable
unset interface ethernet8 ip manageable
unset interface ethernet7.4 manage telnet
set interface ethernet7.4 manage ssh
unset interface ethernet7.4 manage snmp
unset interface ethernet7.4 manage web
set interface ethernet7.4 manage ssl
#Define NAT: MIPs (static/1-to-1 NAT) and DIPs (dynamic/1-to-many/masquerading)
set interface "ethernet1" mip 192.0.2.3 host 192.168.9.2 netmask 255.255.255.255 vrouter "trust-vr"
set interface "ethernet1" mip 192.0.2.4 host 192.168.9.10 netmask 255.255.255.255 vrouter "trust-vr"
set interface "ethernet1" mip 192.0.2.5 host 192.168.9.18 netmask 255.255.255.255 vrouter "trust-vr"
set interface "ethernet1" mip 192.0.2.6 host 192.168.9.34 netmask 255.255.255.255 vrouter "trust-vr"
set interface "ethernet1" dip 4 192.0.2.7 192.0.2.7
set interface "ethernet1" dip 5 192.0.2.8 192.0.2.8
#Control the maximum segment size for tunnelled TCP connections (helps avoid fragmentation problems with
IPSec)
set flow tcp-mss 1400
#Remove session from state table when a TCP RST is encountered
set flow tcp-rst-invalid-session
#Allow the NetScreen to discover the maximum transmission unit and send ICMP requests to reduce MTU if
necessary
set flow path-mtu
#Check TCP sequence numbers are consistent.  Amongst other things, this helps to defend against some
sequence number brute-forcing attacks
unset flow no-tcp-seq-check
#Check that a TCP packet has the SYN flag set before making a state table entry
set flow tcp-syn-check
#Verify that packets with a destination port of 53/udp have the query bit set
unset flow allow-dns-reply
#Enable aggressive aging out of sessions - helps protect against DoS attacks that attempt to saturate the state
table.  When the state table exceeds 80% capacity, sessions older than 40 (4*10) seconds are agressively
aged out until the state table falls below 70% capacity
set flow aging low-watermark 70
set flow aging high-watermark 80
set flow aging early-ageout 4
#Set timeout for console connections
set console timeout 10
#Set hostname
set hostname giace-ext-fw-ns208-a
#Allow multiple DNS replies using the same source port. This is required for some servers that send multiple
```

```
UDP replies to a single request (as per RFC2671)
set dns udp-session-normal
#Define address book entries and groups
set address "Trust" "Internal_SMTP" 192.168.8.2 255.255.255.255
set address "Trust" "Master_DB" 192.168.8.10 255.255.255.255
set address "Trust" "Domain_Controller" 172.22.8.2 255.255.255.255
set address "Trust" "Internal_DNS_DHCP" 172.22.8.3 255.255.255.255
set address "Trust" "File_Print" 172.22.8.4 255.255.255.255
set address "Trust" "Internal_Net" 172.22.8.0 255.255.252.0 "Supernet of all internal VLANs"
set address "Trust" "Interior_FW_eth1" 192.168.9.253 255.255.255.255
set group address "Trust" "Trust_Clients" add "Internal_SMTP"
set group address "Trust" "Trust_Clients" add "Master_DB"
set group address "Trust" "Trust_Clients" add "Internal_Net"
set group address "Trust" "Trust_Clients" add "Interior_FW_eth1"
set address "Untrust" "Border_Router" 192.0.2.1 255.255.255.255
set address "Untrust" "NewYork_FW" 1.1.1.1 255.255.255.255
set address "Untrust" "CapeTown_FW" 2.2.2.2 255.255.255.255
set address "Untrust" "Sydney_FW" 3.3.3.3 255.255.255.255
set address "Untrust" "Beijing_FW" 4.4.4.4 255.255.255.255
#Three nameservers from respected ISPs are used for external DNS resolution
set address "Untrust" "cache0000.ns.eu.uu.net" 158.43.128.72 255.255.255.255 "Public DNS server"
set address "Untrust" "ns0.bt.net" 217.32.105.90 255.255.255.255 "Public DNS server"
set address "Untrust" "resolver1.eu.level3.net" 212.113.0.3 255.255.255.255 "Public DNS server"
#Three timeservers from respected ISPs/universities are used as time sources
set address "Untrust" "ntp1.pipex.net" 158.43.128.66 255.255.255.255 "Public access stratum 2 server"
set address "Untrust" "ntp0.cis.strath.ac.uk" 130.159.196.118 255.255.255.255 "Public access stratum 2
server"
set address "Untrust" "utserv.mcc.ac.uk" 130.88.200.6 255.255.255.255 "Public access stratum 2 server"
set group address "Untrust" "Satellite_Office_FWs" add "NewYork_FW"
set group address "Untrust" "Satellite_Office_FWs" add "CapeTown_FW"
set group address "Untrust" "Satellite_Office_FWs" add "Sydney_FW"
set group address "Untrust" "Satellite_Office_FWs" add "Beijing_FW"
set group address "Untrust" "Internet_DNS_Servers" add "cache0000.ns.eu.uu.net"
set group address "Untrust" "Internet_DNS_Servers" add "ns0.bt.net"
set group address "Untrust" "Internet_DNS_Servers" add "resolver1.eu.level3.net"
set group address "Untrust" "Internet_NTP_Servers" add "ntp1.pipex.net"
set group address "Untrust" "Internet_NTP_Servers" add "ntp0.cis.strath.ac.uk"
set group address "Untrust" "Internet_NTP_Servers" add "utserv.mcc.ac.uk"
set address "Public_DMZ" "Public_Web" 192.168.9.2 255.255.255.255
set address "Public_DMZ" "Public_SMTP" 192.168.9.10 255.255.255.255
set address "Public_DMZ" "Public_DNS" 192.168.9.18 255.255.255.255
set group address "Public_DMZ" "Public_DMZ_Hosts" add "Public_Web"
set group address "Public_DMZ" "Public_DMZ_Hosts" add "Public_SMTP"
set group address "Public_DMZ" "Public_DMZ_Hosts" add "Public_DNS"
set address "Encrypted_DMZ" "VPN_Concentrator_Public" 192.0.2.34 255.255.255.255
set address "Encrypted_DMZ" "SSL_Portal" 192.168.9.34 255.255.255.255
set address "Unencrypted_DMZ" "VPN_Concentrator_Private" 192.168.9.26 255.255.255.255
#Mobile/home users are assigned an IP from this pool when connecting via the VPN Concentrator
set address "Unencrypted_DMZ" "VPNC_IP-Pool" 192.168.10.0 255.255.255.128 "VPNC-assigned client IP
pool"
#IT department users are assigned an IP from this different pool when connecting via the VPN Concentrator
set address "Unencrypted_DMZ" "VPNC_ITUsers_IP-Pool" 192.168.10.128 255.255.255.240 "VPNC client IP
pool for IT dept"
set address "Unencrypted_DMZ" "NewYork_LAN" 172.22.20.0 255.255.255.0
set address "Unencrypted_DMZ" "CapeTown_LAN" 172.22.21.0 255.255.255.0
set address "Unencrypted_DMZ" "Sydney_LAN" 172.22.22.0 255.255.255.0
set address "Unencrypted_DMZ" "Beijing_LAN" 172.22.23.0 255.255.255.0
set address "Unencrypted_DMZ" "Partner1_LAN" 172.16.0.0 255.255.0.0
set address "Unencrypted_DMZ" "Partner1_Mail_Server" 172.16.1.100 255.255.255.255
set group address "Unencrypted_DMZ" "Satellite_Office_LANs" add "NewYork_LAN"
set group address "Unencrypted_DMZ" "Satellite_Office_LANs" add "CapeTown_LAN"
set group address "Unencrypted_DMZ" "Satellite_Office_LANs" add "Sydney_LAN"
set group address "Unencrypted_DMZ" "Satellite_Office_LANs" add "Beijing_LAN"
```

```
set address "SemiPrivate_DMZ" "Dev_DB" 192.168.9.42 255.255.255.255
set address "SemiPrivate_DMZ" "CA_Server" 192.168.9.50 255.255.255.255
set group address "SemiPrivate_DMZ" "SemiPrivate_DMZ_Hosts" add "Dev_DB"
set group address "SemiPrivate_DMZ" "SemiPrivate_DMZ_Hosts" add "CA_Server"
set address "Private_DMZ" "Proxy_Server" 192.168.9.58 255.255.255.255
set address "Private_DMZ" "SUS-AV_Server" 192.168.9.66 255.255.255.255
set group address "Private_DMZ" "Private_DMZ_Hosts" add "Proxy_Server"
set group address "Private_DMZ" "Private_DMZ_Hosts" add "SUS-AV_Server"
set address "Mgmt_DMZ" "NTP_Server" 192.168.9.74 255.255.255.255
set address "Mgmt_DMZ" "Syslog_Server" 192.168.9.82 255.255.255.255
set address "Mgmt_DMZ" "IDS_Sensor" 192.168.9.90 255.255.255.255
set address "Mgmt_DMZ" "Mgmt_PC" 192.168.9.98 255.255.255.255
set group address "Mgmt_DMZ" "Mgmt_DMZ_NTP_Clients" add "Syslog_Server"
set group address "Mgmt_DMZ" "Mgmt_DMZ_NTP_Clients" add "IDS_Sensor"
set group address "Mgmt_DMZ" "Mgmt_DMZ_NTP_Clients" add "Mgmt_PC"
set group address "Mgmt_DMZ" "Mgmt_DMZ_Syslog_Clients" add "NTP_Server"
set group address "Mgmt_DMZ" "Mgmt_DMZ_Syslog_Clients" add "IDS_Sensor"
set group address "Mgmt_DMZ" "Mgmt_DMZ_Syslog_Clients" add "Mgmt_PC"
set group address "Mgmt_DMZ" "Mgmt_DMZ_SSH" add "NTP_Server"
set group address "Mgmt_DMZ" "Mgmt_DMZ_SSH" add "Syslog_Server"
set group address "Mgmt_DMZ" "Mgmt_DMZ_SSH" add "IDS_Sensor"
set group address "Mgmt_DMZ" "Mgmt_DMZ_Hosts" add "NTP_Server"
set group address "Mgmt_DMZ" "Mgmt_DMZ_Hosts" add "Syslog_Server"
set group address "Mgmt_DMZ" "Mgmt_DMZ_Hosts" add "IDS_Sensor"
set group address "Mgmt_DMZ" "Mgmt_DMZ_Hosts" add "Mgmt_PC"
set group service "Browsing_Services" add FTP
set group service "Browsing_Services" add HTTP
set group service "Browsing_Services" add HTTPS
set group service "Certificate_Verification" comment "LDAP and OCSP supported"
set group service "Certificate_Verification" add HTTP
set group service "Certificate_Verification" add LDAP
set group service "Filtered_Services" comment "Should be dropped before FW"
set group service "Filtered_Services" add FTP
set group service "Filtered_Services" add SSH
set group service "Filtered_Services" add TELNET
set group service "Filtered_Services" add TFTP
set group service "Filtered_Services" add FINGER
set group service "Filtered_Services" add POP3
set group service "Filtered_Services" add NFS
set group service "Filtered_Services" add NNTP
set group service "Filtered_Services" add NTP
set group service "Filtered_Services" add IMAP
set group service "Filtered_Services" add SNMP
set group service "Filtered_Services" add SNMP-TRAP
set group service "Filtered_Services" add LDAP
set group service "Filtered_Services" add MS_Filesharing
set group service "Filtered_Services" add RLOGIN
set group service "Filtered_Services" add RSH
set group service "Filtered_Services" add SYSLOG
set group service "Filtered_Services" add RIP
set group service "Filtered_Services" add UDP_1434
set group service "Filtered_Services" add WINFRAME
set group service "Filtered_Services" add L2TP
set group service "Filtered_Services" add NetMeeting
set group service "Filtered_Services" add PPTP
set group service "Filtered_Services" add MS_Terminal_Services
set group service "Filtered_Services" add PC-Anywhere
set group service "Filtered_Services" add VNC
set group service "Filtered_Services" add X-WINDOWS
set group service "Filtered_Services" add IRC
set group service "Filtered_Services" add Proxy_HTTP
set group service "Mgmt_Services" add Alternate_SSH
set group service "Mgmt_Services" add PING
```

```
set group service "MS_Domain_Services" add ICMP-ANY
set group service "MS_Domain_Services" add WINS
set group service "MS_Domain_Services" add DNS
set group service "MS_Domain_Services" add Kerberos
set group service "MS_Domain_Services" add LDAP
set group service "MS_Domain_Services" add LDAP_UDP
set group service "MS_Domain_Services" add MS_Filesharing
set group service "MS_Domain_Services" add LDAP_SSL
set group service "MS_Domain_Services" add LDAP_GlobalCatalogue
set group service "MS_Domain_Services" add Fixed_RPC_Range
set group service "Troubleshooting_Services" add PING
set group service "Troubleshooting_Services" add TRACEROUTE
set group service "Troubleshooting_Services" add FTP
set group service "Troubleshooting_Services" add SSH
set group service "Troubleshooting_Services" add MAIL
set group service "Troubleshooting_Services" add DNS
set group service "Troubleshooting_Services" add HTTP
set group service "Troubleshooting_Services" add HTTPS
#Define policies - referenced against column 1 of Table 5
#Lookout policies
set policy id 1 from "Untrust" to "Global" "Any" "Any" "Filtered_Services" deny log
set policy id 2 from "Trust" to "Untrust" "Any" "Any" ANY deny log
#General public
set policy id 3 from "Untrust" to "Global" "Any" "MIP(192.0.2.3)" "HTTP" permit log
set policy id 3 application HTTP
set policy id 4 from "Untrust" to "Global" "Any" "MIP(192.0.2.4)" "MAIL" permit log
set policy id 4 application SMTP
set policy id 5 from "Untrust" to "Global" "Any" "MIP(192.0.2.5)" "DNS-UDP" permit log
set policy id 5 application DNS
#Customers and suppliers
set policy id 6 from "Untrust" to "Global" "Any" "MIP(192.0.2.6)" "HTTPS" permit log
set policy id 7 from "Encrypted_DMZ" to "SemiPrivate_DMZ" "SSL_Portal" "Dev_DB" MySQL permit log
#Partners
set policy id 8 from "Unencrypted_DMZ" to "Public_DMZ" "Partner1_Mail_Server" "Public_SMTP" MAIL permit
log
set policy id 9 from "Public_DMZ" to "Unencrypted_DMZ" "Public_SMTP" "Partner1_Mail_Server" MAIL permit
log
set policy id 10 from "Unencrypted_DMZ" to "SemiPrivate_DMZ" "Partner1_LAN" "Dev_DB" MySQL permit log
set policy id 11 from "Unencrypted_DMZ" to "Trust" "Partner1_LAN" "File_Print" MS_Filesharing permit log
#Satellite offices
set policy id 12 from "Unencrypted_DMZ" to "Trust" "Satellite_Office_LANs" "Internal_SMTP" MS_Exchange
permit log
set policy id 13 from "Unencrypted_DMZ" to "SemiPrivate_DMZ" "Satellite_Office_LANs" "Dev_DB" MySQL
permit log
set policy id 14 from "Unencrypted_DMZ" to "Trust" "Satellite_Office_LANs" "Master_DB" MySQL permit log
set policy id 15 from "Unencrypted_DMZ" to "Trust" "Satellite_Office_LANs" "File_Print" MS_Filesharing permit
log
set policy id 16 from "Unencrypted_DMZ" to "Private_DMZ" "Satellite_Office_LANs" "SUS-AV_Server" HTTP
permit log
set policy id 17 from "Unencrypted_DMZ" to "Private_DMZ" "Satellite_Office_LANs" "Proxy_Server"
Proxy_HTTP permit log
set policy id 18 from "Unencrypted_DMZ" to "Trust" "Satellite_Office_LANs" "Domain_Controller"
MS_Domain_Services permit log
set policy id 19 from "Unencrypted_DMZ" to "Trust" "Satellite_Office_LANs" "Internal_DNS_DHCP" DNS permit
log
#General mobile users
set policy id 20 from "Untrust" to "Encrypted_DMZ" "Any" "VPN_Concentrator_Public" IPSec permit log
set policy id 21 from "Unencrypted_DMZ" to "Trust" "VPNC_IP-Pool" "Internal_SMTP" MS_Exchange permit
log
set policy id 22 from "Unencrypted_DMZ" to "SemiPrivate_DMZ" "VPN_Concentrator_Private" "CA_Server"
Certificate_Verification permit log
set policy id 23 from "Unencrypted_DMZ" to "SemiPrivate_DMZ" "VPNC_IP-Pool" "Dev_DB" MySQL permit log
set policy id 24 from "Unencrypted_DMZ" to "Trust" "VPNC_IP-Pool" "Master_DB" MySQL permit log
```

```
set policy id 25 from "Unencrypted_DMZ" to "Trust" "VPNC_IP-Pool" "File_Print" MS_Filesharing permit log
set policy id 26 from "Unencrypted_DMZ" to "Private_DMZ" "VPNC_IP-Pool" "SUS-AV_Server" HTTP permit
log
set policy id 27 from "Unencrypted_DMZ" to "Private_DMZ" "VPNC_IP-Pool" "Proxy_Server" Proxy_HTTP
permit log
set policy id 28 from "Unencrypted_DMZ" to "Trust" "VPNC_IP-Pool" "Domain_Controller"
MS_Domain_Services permit log
set policy id 29 from "Unencrypted_DMZ" to "Trust" "VPNC_IP-Pool" "Internal_DNS_DHCP" DNS permit log
#IT mobile users
set policy id 30 from "Untrust" to "Encrypted_DMZ" "Any" "VPN_Concentrator_Public" IPSec permit log
set policy id 31 from "Unencrypted_DMZ" to "Mgmt_DMZ" "VPNC_ITUsers_IP-Pool" "Mgmt_PC"
Alternate_SSH permit log
set policy id 32 from "Unencrypted_DMZ" to "Trust" "VPNC_ITUsers_IP-Pool" "Domain_Controller" VNC permit
log
#General internal  users
set policy id 33 from "Trust" to "SemiPrivate_DMZ" "Internal_Net" "Dev_DB" MySQL permit log
set policy id 34 from "Trust" to ""Private_DMZ" "Internal_Net" "Proxy_Server" Proxy_HTTP permit log
set policy id 35 from "Trust" to ""Private_DMZ" "Internal_Net" "SUS-AV_Server" HTTP permit log
#IT users
set policy id 36 from "Mgmt_DMZ" to "Untrust" "Mgmt_PC" "Border_Router" Mgmt_Services permit log
set policy id 37 from "Mgmt_DMZ" to "Public_DMZ" "Mgmt_PC" "Public_DMZ_Hosts" Mgmt_Services permit
log
set policy id 38 from "Mgmt_DMZ" to "Encrypted_DMZ" "Mgmt_PC" "SSL_Portal" Mgmt_Services permit log
set policy id 39 from "Mgmt_DMZ" to "Unencrypted_DMZ" "Mgmt_PC" "VPN_Concentrator_Private"
Mgmt_Services permit log
set policy id 40 from "Mgmt_DMZ" to "SemiPrivate_DMZ" "Mgmt_PC" "SemiPrivate_DMZ_Hosts"
Mgmt_Services permit log
set policy id 41 from "Mgmt_DMZ" to "Private_DMZ" "Mgmt_PC" "Private_DMZ_Hosts" Mgmt_Services permit
log
set policy id 42 from "Mgmt_DMZ" to "Mgmt_DMZ" "Mgmt_PC" "Mgmt_DMZ_SSH" Mgmt_Services permit log
set policy id 43 from "Mgmt_DMZ" to "Trust" "Mgmt_PC" "Internal_FW_eth1" Mgmt_Services permit log
set policy id 44 from "Mgmt_DMZ" to "Untrust" "Mgmt_PC" “Satellite_Office_FWs” Alternate_SSH permit log
set policy id 45 from "Mgmt_DMZ" to "Unencrypted_DMZ" "Mgmt_PC" "Satellite_Office_LANs" VNC permit log
set policy id 46 from "Mgmt_DMZ" to "Untrust" "Mgmt_PC" "Any" Troubleshooting_Services nat src dip-id 5
permit log
#Define additional policies further to those detailed in Table 5
#Name resolution
set policy id 47 from "Public_DMZ" to "Untrust" "Public_DNS" "Internet_DNS_Servers" DNS permit log
set policy id 48 from "Public_DMZ" to "Public_DMZ" "Public_SMTP" "Public_DNS" DNS permit log
set policy id 49 from "Private_DMZ" to "Public_DMZ" "Private_DMZ_Hosts" "Public_DNS" DNS permit log
set policy id 50 from "Mgmt_DMZ" to "Public_DMZ" "Mgmt_PC" "Public_DNS" DNS permit log
set policy id 51 from "Trust" to "Public_DMZ" "Internal_DNS_DHCP" "Public_DNS" DNS permit log
#Mail delivery
set policy id 52 from "Public_DMZ" to "Trust" "Public_SMTP" "Internal_SMTP" MAIL permit log
set policy id 53 from "Trust" to "Public_DMZ" "Internal_SMTP" "Public_SMTP" MAIL permit log
#Web browsing and security updates
set policy id 54 from "Private_DMZ" to "Untrust" "Proxy_Server" "Any" Browsing_Services nat src dip-id 4 permit
log
set policy id 55 from "Private_DMZ" to "Private_DMZ" "SUS-AV_Server" "Proxy_Server" Proxy_HTTP permit
log
#These rules will only be used during scheduled maintenance and are left disabled at other times.  Swatch
watches these policies as they should not be hit during normal operations (any hit suggests a potential
compromise).
set policy id 56 from "Public_DMZ" to "Private_DMZ" "Public_DMZ_Hosts" "Proxy_Server" Proxy_HTTP permit
log
set policy 56 disable
set policy id 57 from "Encrypted_DMZ" to "Private_DMZ" "SSL_Portal" "Proxy_Server" Proxy_HTTP permit log
set policy 57 disable
set policy id 58 from "SemiPrivate_DMZ" to "Private_DMZ" "SemiPrivate_DMZ_Hosts" "Proxy_Server"
Proxy_HTTP permit log
set policy 58 disable
set policy id 59 from "Mgmt_DMZ" to "Private_DMZ" "Mgmt_DMZ_Hosts" "Proxy_Server" Proxy_HTTP permit
log
```

```
set policy 59 disable
set policy id 60 from "Trust" to "Private_DMZ" "Internal_SMTP" "Proxy_Server" Proxy_HTTP permit log
set policy 60 disable
set policy id 61 from "Trust" to "Private_DMZ" "Master_DB" "Proxy_Server" Proxy_HTTP permit log
set policy 61 disable
#Database synchronisation (NB: Master_DB connects to Dev_DB, not vice versa)
set policy id 62 from "Trust" to "SemiPrivate_DMZ" "Master_DB" "Dev_DB" MySQL permit log
#Time synchronisation
set policy id 63 from "Mgmt_DMZ" to "Untrust" "NTP_Server" "Internet_NTP_Servers" NTP nat src dip-id 4
permit log
set policy id 64 from "Trust" to "Mgmt_DMZ" "Trust_Clients" "NTP_Server" NTP permit log
set policy id 65 from "Public_DMZ" to "Mgmt_DMZ" "Public_DMZ_Hosts" "NTP_Server" NTP permit log
set policy id 66 from "Encrypted_DMZ" to "Mgmt_DMZ" "SSL_Portal" "NTP_Server" NTP permit log
set policy id 67 from "Unencrypted_DMZ" to "Mgmt_DMZ" "VPN_Concentrator_Private" "NTP_Server" NTP
permit log
set policy id 68 from "SemiPrivate_DMZ" to "Mgmt_DMZ" "SemiPrivate_DMZ_Hosts" "NTP_Server" NTP
permit log
set policy id 69 from "Private_DMZ" to "Mgmt_DMZ" "Private_DMZ_Hosts" "NTP_Server" NTP permit log
set policy id 70 from "Mgmt_DMZ" to "Mgmt_DMZ" "Mgmt_DMZ_NTP_Clients" "NTP_Server" NTP permit log
#Syslog (don't log these policies!)
set policy id 71 from "Trust" to "Mgmt_DMZ" "Trust_Clients" "Syslog_Server" syslog permit
set policy id 72 from "Public_DMZ" to "Mgmt_DMZ" "Public_DMZ_Hosts" "Syslog_Server" syslog permit
set policy id 73 from "Encrypted_DMZ" to "Mgmt_DMZ" "SSL_Portal" "Syslog_Server" syslog permit
set policy id 74 from "Unencrypted_DMZ" to "Mgmt_DMZ" "VPN_Concentrator_Private" "Syslog_Server" syslog
permit
set policy id 75 from "SemiPrivate_DMZ" to "Mgmt_DMZ" "SemiPrivate_DMZ_Hosts" "Syslog_Server" syslog
permit
set policy id 76 from "Private_DMZ" to "Mgmt_DMZ" "Private_DMZ_Hosts" "Syslog_Server" syslog permit
set policy id 77 from "Mgmt_DMZ" to "Mgmt_DMZ" "Mgmt_DMZ_Syslog_Clients" "Syslog_Server" syslog
permit
#Default deny rules are implicit but without logging so explicit rules are added
set policy id 78 from "Trust" to "Trust" "Any" "Any" ANY deny log
set policy id 79 from "Untrust" to "Trust" "Any" "Any" ANY deny log
set policy id 80 from "Public_DMZ" to "Trust" "Any" "Any" ANY deny log
set policy id 81 from "Encrypted_DMZ" to "Trust" "Any" "Any" ANY deny log
set policy id 82 from "Unencrypted_DMZ" to "Trust" "Any" "Any" ANY deny log
set policy id 83 from "SemiPrivate_DMZ" to "Trust" "Any" "Any" ANY deny log
set policy id 84 from "Private_DMZ" to "Trust" "Any" "Any" ANY deny log
set policy id 85 from "Mgmt_DMZ" to "Trust" "Any" "Any" ANY deny log
set policy id 86 from "Untrust" to "Untrust" "Any" "Any" ANY deny log
set policy id 87 from "Public_DMZ" to "Untrust" "Any" "Any" ANY deny log
set policy id 88 from "Encrypted_DMZ" to "Untrust" "Any" "Any" ANY deny log
set policy id 89 from "Unencrypted_DMZ" to "Untrust" "Any" "Any" ANY deny log
set policy id 90 from "SemiPrivate_DMZ" to "Untrust" "Any" "Any" ANY deny log
set policy id 91 from "Private_DMZ" to "Untrust" "Any" "Any" ANY deny log
set policy id 92 from "Mgmt_DMZ" to "Untrust" "Any" "Any" ANY deny log
set policy id 93 from "Trust" to "Public_DMZ" "Any" "Any" ANY deny log
set policy id 94 from "Untrust" to "Public_DMZ" "Any" "Any" ANY deny log
set policy id 95 from "Public_DMZ" to "Public_DMZ" "Any" "Any" ANY deny log
set policy id 96 from "Encrypted_DMZ" to "Public_DMZ" "Any" "Any" ANY deny log
set policy id 97 from "Unencrypted_DMZ" to "Public_DMZ" "Any" "Any" ANY deny log
set policy id 98 from "SemiPrivate_DMZ" to "Public_DMZ" "Any" "Any" ANY deny log
set policy id 99 from "Private_DMZ" to "Public_DMZ" "Any" "Any" ANY deny log
set policy id 100 from "Mgmt_DMZ" to "Public_DMZ" "Any" "Any" ANY deny log
set policy id 101 from "Trust" to "Encrypted_DMZ" "Any" "Any" ANY deny log
set policy id 102 from "Untrust" to "Encrypted_DMZ" "Any" "Any" ANY deny log
set policy id 103 from "Public_DMZ" to "Encrypted_DMZ" "Any" "Any" ANY deny log
set policy id 104 from "Encrypted_DMZ" to "Encrypted_DMZ" "Any" "Any" ANY deny log
set policy id 105 from "Unencrypted_DMZ" to "Encrypted_DMZ" "Any" "Any" ANY deny log
set policy id 106 from "SemiPrivate_DMZ" to "Encrypted_DMZ" "Any" "Any" ANY deny log
set policy id 107 from "Private_DMZ" to "Encrypted_DMZ" "Any" "Any" ANY deny log
set policy id 108 from "Mgmt_DMZ" to "Encrypted_DMZ" "Any" "Any" ANY deny log
set policy id 109 from "Trust" to "Unencrypted_DMZ" "Any" "Any" ANY deny log
```

```
set policy id 110 from "Untrust" to "Unencrypted_DMZ" "Any" "Any" ANY deny log
set policy id 111 from "Public_DMZ" to "Unencrypted_DMZ" "Any" "Any" ANY deny log
set policy id 112 from "Encrypted_DMZ" to "Unencrypted_DMZ" "Any" "Any" ANY deny log
set policy id 113 from "Unencrypted_DMZ" to "Unencrypted_DMZ" "Any" "Any" ANY deny log
set policy id 114 from "SemiPrivate_DMZ" to "Unencrypted_DMZ" "Any" "Any" ANY deny log
set policy id 115 from "Private_DMZ" to "Unencrypted_DMZ" "Any" "Any" ANY deny log
set policy id 116 from "Mgmt_DMZ" to "Unencrypted_DMZ" "Any" "Any" ANY deny log
set policy id 117 from "Trust" to "SemiPrivate_DMZ" "Any" "Any" ANY deny log
set policy id 118 from "Untrust" to "SemiPrivate_DMZ" "Any" "Any" ANY deny log
set policy id 119 from "Public_DMZ" to "SemiPrivate_DMZ" "Any" "Any" ANY deny log
set policy id 120 from "Encrypted_DMZ" to "SemiPrivate_DMZ" "Any" "Any" ANY deny log
set policy id 121 from "Unencrypted_DMZ" to "SemiPrivate_DMZ" "Any" "Any" ANY deny log
set policy id 122 from "SemiPrivate_DMZ" to "SemiPrivate_DMZ" "Any" "Any" ANY deny log
set policy id 123 from "Private_DMZ" to "SemiPrivate_DMZ" "Any" "Any" ANY deny log
set policy id 124 from "Mgmt_DMZ" to "SemiPrivate_DMZ" "Any" "Any" ANY deny log
set policy id 125 from "Trust" to "Private_DMZ" "Any" "Any" ANY deny log
set policy id 126 from "Untrust" to "Private_DMZ" "Any" "Any" ANY deny log
set policy id 127 from "Public_DMZ" to "Private_DMZ" "Any" "Any" ANY deny log
set policy id 128 from "Encrypted_DMZ" to "Private_DMZ" "Any" "Any" ANY deny log
set policy id 129 from "Unencrypted_DMZ" to "Private_DMZ" "Any" "Any" ANY deny log
set policy id 130 from "SemiPrivate_DMZ" to "Private_DMZ" "Any" "Any" ANY deny log
set policy id 131 from "Private_DMZ" to "Private_DMZ" "Any" "Any" ANY deny log
set policy id 132 from "Mgmt_DMZ" to "Private_DMZ" "Any" "Any" ANY deny log
set policy id 133 from "Trust" to "Mgmt_DMZ" "Any" "Any" ANY deny log
set policy id 134 from "Untrust" to "Mgmt_DMZ" "Any" "Any" ANY deny log
set policy id 135 from "Public_DMZ" to "Mgmt_DMZ" "Any" "Any" ANY deny log
set policy id 136 from "Encrypted_DMZ" to "Mgmt_DMZ" "Any" "Any" ANY deny log
set policy id 137 from "Unencrypted_DMZ" to "Mgmt_DMZ" "Any" "Any" ANY deny log
set policy id 138 from "SemiPrivate_DMZ" to "Mgmt_DMZ" "Any" "Any" ANY deny log
set policy id 139 from "Private_DMZ" to "Mgmt_DMZ" "Any" "Any" ANY deny log
set policy id 140 from "Mgmt_DMZ" to "Mgmt_DMZ" "Any" "Any" ANY deny log
set policy id 141 from "Trust" to "Global" "Any" "Any" ANY deny log
set policy id 142 from "Untrust" to "Global" "Any" "Any" ANY deny log
set policy id 143 from "Public_DMZ" to "Global" "Any" "Any" ANY deny log
set policy id 144 from "Encrypted_DMZ" to "Global" "Any" "Any" ANY deny log
set policy id 145 from "Unencrypted_DMZ" to "Global" "Any" "Any" ANY deny log
set policy id 146 from "SemiPrivate_DMZ" to "Global" "Any" "Any" ANY deny log
set policy id 147 from "Private_DMZ" to "Global" "Any" "Any" ANY deny log
set policy id 148 from "Mgmt_DMZ" to "Global" "Any" "Any" ANY deny log

#Define strong phase 1 and phase 2 proposals as discussed in 2.6.4
set ike p1-proposal "pre-g5-3des-sha" preshare group5 esp 3des sha-1
set ike p2-proposal "g5-esp-aes256-md5" group5 esp aes256 md5 second 3600
#Configure peer IKE gateways using main mode and preshared keys
set ike gateway "NewYork-ns5gt_ph1" address 1.1.1.1 Main outgoing-interface "ethernet1" preshare
"V3InFPteTRsfYhJ6tekBLWGGJRiyV7Oi86ESwxA8SzcDVdTdkZVBHVk=" proposal "pre-g5-3des-sha"
set ike gateway "CapeTown-ns5gt_ph1" address 2.2.2.2 Main outgoing-interface "ethernet1" preshare
"6Dkqg0pJCrp8E2VA7JKTtZWHR3i2rIVxaPMqdTIpAcnQOj1VZchFREb=" proposal "pre-g5-3des-sha"
set ike gateway "Sydney-ns5gt_ph1" address 3.3.3.3 Main outgoing-interface "ethernet1" preshare
"lHp8rpS7oXzKCEj2z75ljtVbe7tH6pL2AKhoCOCyMSsdNBl0Rslc0AP=" proposal "pre-g5-3des-sha"
set ike gateway "Beijing-ns5gt_ph1" address 4.4.4.4 Main outgoing-interface "ethernet1" preshare
"3SDi3g2i1BPBUFJRp567LhCm1zfLW4mDEdFpYcKlCXuzuVadICO51O0=" proposal "pre-g5-3des-sha"
set ike gateway "Partner1-ns5gt_ph1" address 5.5.5.5 Main outgoing-interface "ethernet1" preshare
"uuYlzEmHkqpIqd2AOVj7vM5HQ9VVFzVEOjqUHNrTvAFBuhVPKEUud0T=" proposal "pre-g5-3des-sha"
#Respond to IKE packets with bad security parameter index values, but only do so once per peer gateway
(allows quick recovery from genuine IKE errors without offering much reconnaisance potential)
set ike respond-bad-spi 1
#Configure route-based VPNs. Proxy IDs are manually specified to reduce likelihood of mismatch. Status of
tunnels is monitored and they automatically renegotiate in event of failure.
set vpn "NewYork-ns5gt_ph2" gateway "NewYork-ns5gt_ph1" replay tunnel idletime 0 proposal "g5-esp-aes256-
md5"
set vpn "NewYork-ns5gt_ph2" monitor rekey
set vpn "NewYork-ns5gt_ph2" bind interface tunnel.1
```

```
set vpn "NewYork-ns5gt_ph2" proxy-id local-ip 172.22.8.0/22 remote-ip 172.22.20.0/24 "ANY"
set vpn "CapeTown-ns5gt_ph2" gateway "CapeTown-ns5gt_ph1" replay tunnel idletime 0 proposal "g5-esp-
aes256-md5"
set vpn "CapeTown-ns5gt_ph2" monitor rekey
set vpn "CapeTown-ns5gt_ph2" bind interface tunnel.2
set vpn "CapeTown-ns5gt_ph2" proxy-id local-ip 172.22.8.0/22 remote-ip 172.22.21.0/24 "ANY"
set vpn "Sydney-ns5gt_ph2" gateway "Sydney-ns5gt_ph1" replay tunnel idletime 0 proposal "g5-esp-aes256-
md5"
set vpn "Sydney-ns5gt_ph2" monitor rekey
set vpn "Sydney-ns5gt_ph2" bind interface tunnel.3
set vpn "Sydney-ns5gt_ph2" proxy-id local-ip 172.22.8.0/22 remote-ip 172.22.22.0/24 "ANY"
set vpn "Beijing-ns5gt_ph2" gateway "Beijing-ns5gt_ph1" replay tunnel idletime 0 proposal "g5-esp-aes256-
md5"
set vpn "Beijing-ns5gt_ph2" monitor rekey
set vpn "Beijing-ns5gt_ph2" bind interface tunnel.4
set vpn "Beijing-ns5gt_ph2" proxy-id local-ip 172.22.8.0/22 remote-ip 172.22.23.0/24 "ANY"
set vpn "Partner1-ns5gt_ph2" gateway "Partner1-ns5gt_ph1" replay tunnel idletime 0 proposal "g5-esp-aes256-
md5"
set vpn "Partner1-ns5gt_ph2" monitor rekey
set vpn "Partner1-ns5gt_ph2" bind interface tunnel.5
set vpn "Partner1-ns5gt_ph2" proxy-id local-ip 172.22.8.0/22 remote-ip 172.16.0.0/16 "ANY"
#Always send an ARP broadcast to obtain IP - don't simply trust incoming frames
set arp always-on-dest
#Set default X509 settings and DN settings for SSL cert
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set pki x509 dn country-name "UK"
set pki x509 dn local-name "London"
set pki x509 dn org-name "GIACE"
set pki x509 dn org-unit-name "IT"
set pki x509 dn name "Bruce Lee"
set pki x509 dn phone "12345678"
set pki x509 dn ip "192.168.9.49"
set pki x509 dn email "bruce.lee@giace.co.uk"
set pki x509 default send-to "bruce.lee@giace.co.uk"
set pki x509 cert-fqdn giace-ext-fw-ns208-a.giace.co.uk
#Log system events to local0 and and policy hits to local1
set syslog config "192.168.9.82"
set syslog config "192.168.9.82" facilities local0 local1
set syslog config "192.168.9.82" log traffic
set syslog src-interface ethernet7.2
set syslog enable
#Log packets destined to firewall
set firewall log-self
set firewall log-self ike
set firewall log-self snmp
set firewall log-self icmp
set firewall log-self multicast
#Enable SSH (version 2)
set ssh version v2
set ssh enable
#Set timer for config locking (useful if config needs to be rolled back)
set config lock timeout 5
#Specify SSL cert, set strongest SSL encryption settings and non-standard port
set ssl encrypt 3des sha-1
set ssl port 22978
set ssl cert-hash "79F57B7045AB925D5A2AD8970B37CB90A1F561C8"
#Configure hourly time sync
set ntp server "192.168.9.74"
set ntp interval 60
#Configure routing as described in section 3.7
set vrouter "untrust-vr"
set route  0.0.0.0/0 interface ethernet1 gateway 192.0.2.1
```

```
exit
set vrouter "trust-vr"
unset add-default-route
set route  172.22.20.0/24 interface tunnel.1
set route  172.22.20.0/24 interface e7.2 gateway 192.168.9.82 metric 99
set route  172.22.21.0/24 interface tunnel.2
set route  172.22.21.0/24 interface e7.2 gateway 192.168.9.82 metric 99
set route  172.22.22.0/24 interface tunnel.3
set route  172.22.22.0/24 interface e7.2 gateway 192.168.9.82 metric 99
set route  172.22.23.0/24 interface tunnel.4
set route  172.22.23.0/24 interface e7.2 gateway 192.168.9.82 metric 99
set route  172.16.0.0/16 interface tunnel.5
set route  172.16.0.0/16 interface e7.2 gateway 192.168.9.82 metric 99
set route  192.168.10.0/24 interface ethernet4 gateway 192.168.9.26
set route  192.168.8.0/28 interface ethernet8 gateway 192.168.9.253
set route  172.22.8.0/22 interface ethernet8 gateway 192.168.9.253
set route 0.0.0.0/0 vrouter "untrust-vr"
exit
```

References

[1] IEEE Computer Society. IEEE Std 802.1Q™, 2003 Edition. The Institute of Electrical and Electronics Engineers, Inc., 2003.
[2] Taylor, Dave, and Steve Schupp. "VLAN Security." Bugtraq. 1 Sep 1999. 17 Feb. 2005 < http://www.securityfocus.com/archive/1/26008>.
[3] Convery, Sean. "Hacking Layer 2: Fun with Ethernet Switches". Blackhat Briefings. 2002. 17 Feb. 2005 <http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf>.
[4] "Configuring Private VLANs." Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide, Release 12.2SX. 17 Feb. 2005 <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/pvlans.pdf>.
[5] Sarmiento, Evan. "Chapter 4 The Jail Subsystem." FreeBSD Architecture Handbook. 2001. 17 Feb. 2005 <http://www.freebsd.org/doc/en_US.ISO8859-1/books/arch-handbook/jail.html>.
[6] Lo Verso, John R. "Bust Banner Ads with Proxy Auto Configuration" 2005. 17 Feb. 2005 <http://www.schooner.com/~loverso/no-ads>.
[7] "CERT® Advisory CA-2003-07 Remote Buffer Overflow in Sendmail." CERT Coordination Center. 3 March 2003. 17 Feb. 2005 <http://www.cert.org/advisories/CA-2003-07.html>.
[8] "CERT® Advisory CA-2003-25 Buffer Overflow in Sendmail." CERT Coordination Center. 18 September 2003. 17 Feb. 2005 <http://www.cert.org/advisories/CA-2003-25.html>.
[9] "CAN-2003-0245." Common Vulnerabilities and Exposures. 2003. 17 Feb. 2005 <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0245>.
[10] "CVE-2002-0392." Common Vulnerabilities and Exposures. 2002. 17 Feb. 2005 <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0392>.
[11] "Security Matrix." Internet Systems Consortium. 17 Feb. 2005 <http://www.isc.org/sw/bind/bind-security.php>.
[12] "Level-1 / Level-2 Benchmarks and Audit Tool for Cisco IOS Routers and PIX firewalls." Center for Internet Security. 2004. 17 Feb. 2005 <http://www.cisecurity.org/bench_cisco.html>.
[13] Hassell, Jonathan. "Deploying Network Access Quarantine Control, Part 1." SecurityFocus. 4 August 2004. 17 Feb. 2005 <http://www.securityfocus.com/infocus/1794>.
[14] Wang, Xiaoyun. et al. "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD." The School of Mathematics and System Science, Shandong University, China. et al. 2004. 17 Feb. 2005 <http://csrc.nist.gov/hash_standards_comments.pdf>.
[15] "NIST Brief Comments on Recent Cryptanalytic Attacks on Secure Hashing Functions and the Continued Security Provided by SHA-1." National Institute of Standards and Technology. 2004. 17 Feb. 2005 <http://csrc.nist.gov/hash_standards_comments.pdf>.
[16] "Cisco Systems Acquires Network Translation, Inc." Cisco Newsroom. 27 October 1995. 17 Feb. 2005 <http://newsroom.cisco.com/dlls/1995/corp_102795.html>.
[17] "Benchmarks and Scoring Tool for Windows XP Professional, Windows Server 2003, Windows 2000 and Windows NT." Center for Internet Security. 2004. 17 Feb. 2005 <http://www.cisecurity.com/bench_win2000.html>.
[18] "Level-1 Benchmark and Scoring Tool for FreeBSD." Center for Internet Security. 2004. 17 Feb. 2005 <http://www.cisecurity.com/bench_freebsd.html>.
[19] Gill, Stephen. "Catalyst Secure Template." qorbit. 2002. 17 Feb. 2005 <http://www.qorbit.net/documents/catalyst-secure-template.htm>.
[20] "FAQ - Information Assurance." National Security Agency. 17 Feb. 2005 <http://www.nsa.gov/about/about00019.cfm#6>.