Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Redefining your perimeter with MPLS - an integrated network solution

As networks expand and grow, laws and legal requirements are catching up to address network security. What the current design detailed in this paper helps us to do is really build a flexible model for building networks that are virtually isolated from each other.

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.

watchfire

Redefining your perimeter with MPLS – an integrated network solution.

By
Author : Vijay S Sarvepalli, vijay@ericavijay.net

Adviser: John C.A. Bambenek, bambenek@gmail.com

© SANS Institute 2007, Author retains full rights.

Redefining your perimeter with MPLS – an integrated network solution.

1. INTRODUCTION 3
2. THE DRAWING BOARD 5
   2.1 Collect your requirements and identify basic components of the network..... 6
   2.2 Overlaying design criteria on the network..... 8
   2.3 Introducing MPLS or OTHER ALTERNATIVES..... 9
   2.3 Balancing your design..... 11
3. DEFINE SEGMENTED NETWORKS..... 12
   3.1 Define segmented networks – IP Management and planning..... 12
   3.2 Examples of MPLS configuration and testing..... 14
   3.4 Redraw physical infrastructure and logical infrastructure..... 23
   3.5 Perimeter router and Firewall design..... 24
      3.5.1 Perimeter router ACL example 24
      3.5.1 How to keep your bogon or unassigned IP address updated 28
      3.5.2 Consider some advanced options for access control lists..... 29
      3.5.3 Perimeter Firewall design 30
4. DATA CENTER FIREWALL's and VPN 33
   4.1 Define Data center firewall needs, modes of firewall operation 33
      4.1.a Choice of firewall modes and suitable applications..... 33
      4.1.b Defining simplifying and maintaining the Firewall rule base. 36
   4.3 VPN Placement - think outside the "bun" 39
      4.3.a VPN operation mode encryption and consider SSLVPN user-land / non-administrative operation of VPN 42
5. PUBLIC SERVICES DESIGN – DMZ..... 43
   5.1 Define public facing services : DNS, WEB and MAIL..... 43
      5.1.a Split DNS and firewall protection. DNS protected from local DNS (AD or other database) eDNS implementation. Firewall planning. 43
      5.1.b Public WEB and secure services through reverse proxy and ssl-reverse proxy – apache..... 48
      5.1.c MAIL service defined and protected from local groupware. 49
   5.2 IPS/IDS, Probes and Syslog servers Oh my! 51
      5.2.a Placement considerations of IPS, IDS, Probes..... 51
      5.2.b. Logging servers and tracking 53
6. SECURING YOUR LAYER 2 HOSTS & NETWORKS..... 54
   6.1 Switch and radius configuration and 802.1x design – in Cisco IOS. 54
      6.1.a Providing flexibility to your users using REALMS..... 60
   6.3 Making exception to the rules – printers, Ethernet enabled devices, guest access, non-dot1x aware clients. 62
   6.4 Simplifying your configuration, backing up and auditing of Layer 2 switches..... 65
7. TAKE IT FURTHER..... 69
   7.1 Future networks need segmentation, authentication and authorization – HIPPA, FERPA, CLEA, PCI. 70

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

8. Acknowledgements and References 71
8.1 About the author and acknowledgements: 72
8.2 References 72

1. INTRODUCTION

"What used to be clear lines separating enterprises and consumers have now become blurred, as networks are extended to not only suppliers and partners, but also to customers," Thompson said during a keynote speech at the RSA Conference 2007.

Today's networks are finding their perimeter fudged or fused with many overlaid services being delivered over the same network. These demands placed on the network infrastructure, forces network and security professionals to leave network boundaries undefined or poorly defined. It is no longer possible to draw a *"line in the sand"* and say this is my perimeter. There is not only multiple services, but also multiple access methods to your network. This may sound surprising to you at the first look. Here are a list of multiple entry points to your network

1. VPN (Virtual Private Network) dialed in users
2. Wireless users
3. Business partners B2B, Ecommerce partner
4. Outsourced vendor networks
5. Contract and temporary employees with laptops
6. Redundant ISP links or backbones
7. Out of band network – physical access
8. Temporary networks built for conferences and visitors – guest network.

If you consider these network entry points as possible *"attack vectors"*, it surely changes the picture.

This paper attempts to help network and security professionals to meet these demands to build multiple logical networks on a single physical infrastructure. Telecom providers have traditionally used MPLS (Multiple Protocol Label Switching) to serve multiple customers with the same physical (in many cases even logical/IP) infrastructure. This includes dark fiber, routers, ISP backbone and IP networks.

Today both corporate or campus LAN's are expressing similar needs today. So I will try to define network that will

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

- ➔ Restrict access to multiple networks and define network boundaries – choice of MPLS or other mechanism.
- ➔ Segment networks and built auditable intra-network access schemes.
- ➔ Provide simple well defined role based access – enhance using 802.1x to identify users.

The solution provided will cover

- ⇨ Use of MPLS to build multiple logical networks – configuration examples for Cisco (address questions like is MPLS right for me.)
- ⇨ Criteria and process for determining perimeter / outside firewall placement, VPN placement, extranet links and enhancing MPLS to provide logical segmentation and trust groups.
- ⇨ Data center firewall design and maintenance – firewall mode (transparent / failover) optimization, logging, monitoring with examples.
- ⇨ Design of Public facing network – traditionally called DMZ (De-Militarized Zone) Network.
- ⇨ Design of secure switch infrastructure to provide mobility and flexibility to users – examples of Cisco configuration and macros examples to simplify switch installation.
- ⇨ Implementation of 802.1x under Free-radius and Cisco infrastructure.
- ⇨ Provide exceptions for clients that are unable to authenticate – printers, human safety devices and Ethernet enabled devices. MAC address authenticate. Considerations such as use of Cisco's reflexive ACL's (Access Control List) in smaller network communities such as printers.
- ⇨ Simplified network deployment for installation, replacement, change auditing of switches, routers, backup scripts for configuration – scripts and examples.

The above topics are relevant to the course material which has helped me visualize and design the next generation network. You will see in this paper principles from SANS 504, especially from day 5 called *"Network Design and Assessment."*

As these topics are very wide spread, I will also lay out what will <u>NOT</u> be covered (out of scope) in this paper

1. QOS implementation for security and stability – and its integration with MPLS

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

2. MPLS advanced implementations – encryption and WAN design guidelines. Discussed briefly in disaster recovery.
3. BGP and multi-home or multi-ISP redundant network design.
4. Implementation in non-Cisco environment.
5. Optimization of network for voice over IP.
6. Integration of directory to support multiple client and server environments – Novell E-directory, Microsoft AD, Sun One directory and Oracle directory services.

The above topics are left open to be picked up by other GCFW Gold participants to build on the work. These are also listed at the end in a chapter called "7. TAKE IT FURTHER."

It is important to define the size and scale of network appropriate for this deployment. One of the first principles in network design is defined as "collect your eequirements." I am going specify here a typical scale of the network addressed in this design paper. The paper is targeted for middle to large size corporate or campus networks. An organization with more than 1000 users and a data center of 50 servers is considered mid-size in this assessment. Any corporate or campus environment that serves more than this would be an applicable client. However the design criteria, ideas and planning are valid even for very small networks. An example of a single router networks was defined in the paper *"Securing the Perimeter with Cisco IOS 12 Routers by Scott Winters"* for GCFW.

The target network for this design was planned have 700 Cisco based 24 or 48 port switches (Layer 2 switches) and 8 distribution routers (Layer 2 and Layer 3 networks defined) and two core routers (a layer 3 router). The number of clients in this network is about 4,000 active clients [1] during the day and a maximum of 15,000 possible clients. The network design detailed here can also be applied for networks that are much smaller by adapting the equipment and choosing alternatives for smaller scale network. Some of these options are explored in this paper.

2. THE DRAWING BOARD

"Before everything else, getting ready is the secret of success" – Henry Ford

[1] Includes wired and wireless clients.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

2.1 Collect your requirements and identify basic components of the network

In this chapter I will start laying out some physical structure questions that will collect requirements, plan for growth and provide options for a secure network design. Many of the questions laid out here will help make decisions such as "Does the client really need X technology? – say MPLS" and "What is the cost of ongoing maintenance of another Y technology? – say 802.1x"

Some examples of relevant questions for the customer

1. How many end nodes or users you have on a daily basis? – mix of operating systems, non PC devices, handhelds *(scale)*
2. How big is the customer's data center – servers, mix of operating systems? *(diversity)*
3. What is the current rate of growth of the organization? *(growth)*
4. How many access methods to the network are currently in production – remote access -with or without VPN, wireless access, and teleconference / guest access? *(complexity)*
5. How much reliability you have in your physical infrastructure for data center and network closets – power, cooling and fiber or copper cabling. *(structure)*
6. Regulatory or governmental requirements to be satisfied by the customer – PCARD, HIPPA, FERPA etc. *(basic requirement)*
7. Financial – both onetime and ongoing funding structure *(limitations)*

When collecting requirements it is important that you gather relevant information by asking questions sometimes repeatedly – but not annoying the client. This can be done by asking the questions, which was unanswered or avoided by the client, in a different way. For e.g., if you ask the client about "growth" and the client denies any commitment to scope expansion. You may want to ask the question as to how many new constructions or renovations are going on the customer's location or campus for the next year or even next quarter.

After your analysis if the client details six different access methods to the network combined with a high diversity need, say 3 operating systems and at least one regulatory compliance requirement, it is convincing to say securing and scaling this network is a challenge. The network can be labeled as a mid-size to large-size network, even if technically the number of users is only 600. Take a look at the following equation for example

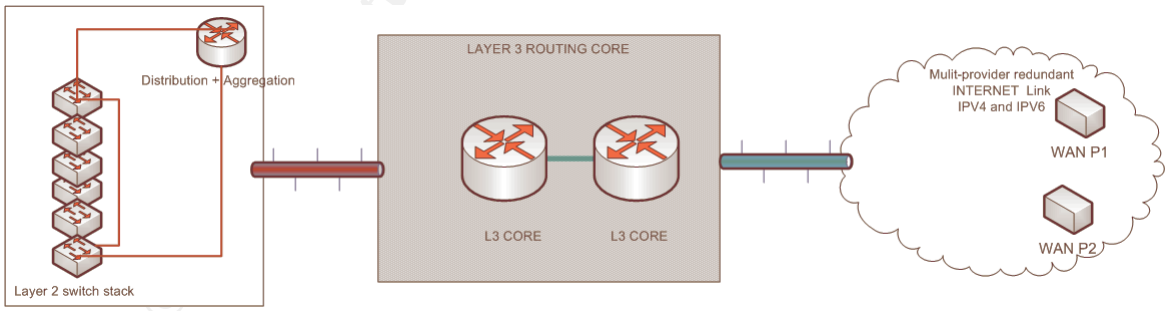
© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

N*L*R = Number of borders to secure and/or audit.

N- Number of access methods to a network
L- Number of buildings / locations
R- Number of regulatory expectations on the network

The requirements process also helps nail down some physical component needed for the client. If the client has a datacenter that was processing credit card that needs to be protected from even internal users and audited independently – you have need for "another new network or a new perimeter" in one sense. An independent firewall and an independent physical switching infrastructure may be needed to meet some of these regulatory requirements. There may be specific client communities that are trusted to access one resource and not another – even that is a "virtual perimeter" that you need to build. After you have learnt the complexity of the client's need, it is important that you don't confuse or scare the client with these challenges.

Once you have learnt of the clients network size, you can start building a diagram with BOM – Bill of Materials to provide network access. Complexity requirement and the need for growth can increase the component count. In some cases additional software / hardware modules will be needed for the network infrastructure that you specified. Take these into consideration, talked to the preferred vendor of the client's needs to verify.



The diagram shown below can satisfy very large client network with expanded number of switches for network expansion. However once you have learned about some physical limitations and the need for redundancy due to power failures you will have to redo the bill of materials.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

This is the first step for identifying number of switches, number of distribution routers and core routers for the network. You can choose to pursue a "collapsed core" model if the network is small enough. In my experience, about 15 "broadcast domains" should be tied to a distribution area. If you see only need for 15 broadcast domains, you can use a collapsed core model as shown above without any "distribution" network. Even if the network is much larger, your initial diagram should be simple. For example if the network needs to 500 switches in 20 buildings, you might choose to show two type of buildings with few switches in them. The idea is to help the client and you visualize the physical infrastructure required for these services.

One important concept in this paper is the fact that switches are considered as part of the "perimeter" or entry point to your network. Example a wireless access point is connected to a switch – which immediately makes the switch another entry point into your network – a virtual perimeter. Part of the reason is we are designing a network where the perimeter is hard to define.

2.2 Overlaying design criteria on the network

On discussing the requirement with the client it will not take long to build a "matrix" of access methods and services offered by these networks *today*. You can see an example below

Services/ Access methods	File-share & document collaboration	Voice & Video conference	Mail & Calendars	Graphics and media publishing
Campus building A	YES	YES	YES	YES
Remote Access – home employees.	NO	NO	YES	YES
Wireless	NO	NO	YES	YES
Business Partner	YES	NO	YES	YES
Campus Cafeteria	NO	NO	YES	YES
Data confidentiality	High – Business	High – Personal + Business	Medium	Low

You can see that the client's need for access from anywhere to any type data in a secure way will become essential. Some additional information such as "Remote Access" or working from home employees don't get "voice or telepresence" today, will tell you that

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

the client does not have VPN in place or has designed VPN to deliver such services.

Wireless clients have been forbidden access to many data due to lack of secure wireless such as WPA-2 or WPA being unavailable on the customer's campus. However the demand for these services through many "network access methods" adds a stretch to your design. You might also consider two various pools of clients as one category for simplifying the design. For e.g., you can recommend your clients to consider "wireless" and "remote access" under one category for confidentiality. Assuming a wireless WPA + 802.1x solution with managed clients is not in place. You might require both wireless and remote access users to terminate at your VPN concentrator before accessing confidential files. This will be to simplify your design. Nevertheless the presence of wireless or VPN termination provides another "attack vector" to be aware of – one you should secure, monitor, and audit.

Once you have determined the network access methods you are ready to draw a virtual perimeter diagram. This is very helpful in determining the scale of network equipment you will use. Number of firewall(s) or border routers you will need. It will also help design the number of locations where you have to "replicate" your configurations such as ACL's, logging, software upgrades etc.

2.3 Introducing MPLS or OTHER ALTERNATIVES.

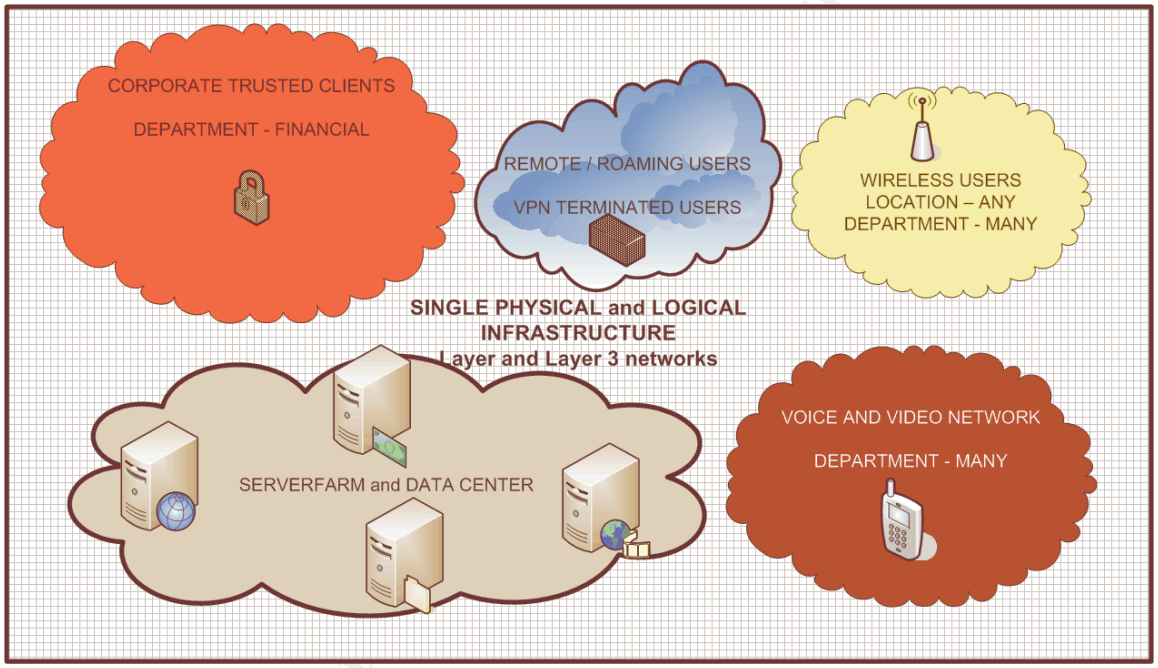
As I mentioned in the abstract before, the need for MPLS in corporate is something new. MPLS was designed to provide a L3 VLAN segmentation. L3 VLAN provides the ability to isolate multiple routed networks from each other. What does MPLS mean to traditional router administrator in simple terms "Multiple layer 3 networks isolated from each other". MPLS extends beyond that by providing the network administrators ability to build trust networks between these multiple Layer 3 networks. In some ways it is consider the next generation of segmentation from the traditional Layer 2 or 802.1Q trunk networks.

The matrix shown earlier as access methods may be defined by a policy, but not understood by the end users. Some of the access methods may have been introduced without even considering their policy implications. Many times the expectation of the end users is

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

that any service is available from any access method. Even if the policy is in place, it may be difficult or impossible to enforce at times. This is where MPLS comes to help. When you build virtual networks, you are require to manage and define each network and its inter-operation with the other networks.

Security provided by logical segmentation via MPLS is considered comparable to Frame-relay or ATM. This is true even without MPLS VPN with encryption[2]. MPLS VPN encryption options are not discussed in here, it is most suited where data is in transit over public WAN (Wide Area Network) to a remote location.



The diagram above shows conceptually what MPLS can do for your network. It can help you build multiple segmented networks on a single physical infrastructure (represented by grid above). These networks co-exist and cannot traverse except by specific "connectors." A connector between MPLS VPN segments or VRF's can be a VPN device, a firewall, an MPLS extranet. MPLS extranets for allowing communications between VRF's are explored in this paper.

[2] This basically means today two MPLS networks cannot VPN hop from one to another.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

2.3 Balancing your design.

"On the road of life, both (Idealism and Realism) are important. Ideals give us direction. Realism gives us traction" from Mart De Hann RBC Ministries. It is important to have "traction" in your design. The If the network design you presented can be built with highly qualified architects and then it is not possible for operations and field staff to understand or troubleshoot this network, there is no "traction" in this design for long term maintenance.

MPLS networks do introduce complexity to your corporate network that requires skilled and/or trained personnel. The MPLS training of your staff (design, operations and field staff) will be an expense for the organization and an ongoing cost that you cannot ignore. You can choose other alternates to MPLS, the most simplistic and popular is using VACL's (VLAN ACL's). This is cumbersome to maintain but traditional routing and switching technicians can understand and maintain.

If your network is small, you can also consider using PBR (Policy Based Routing). PBR can be used to direct traffic from various segments to an enforcement point such as firewall with multiple segments for each of these networks. PBR allows for you to define by ACL's a destination for your next hop, routing by decision making ACL's instead of destination IP address. A simple example is shown below, PBR here called WIRELESS will take the users in Vlan102 and route them to a nearest hop router (which can be NAC – Network Admission Control Device or a firewall). The only exception is clients will be able to connect to a "bastion" host 10.30.31.233.

```
interface Vlan102
 description Route-map-testing
 ip address 10.3.177.1 255.255.255.0
! Note IP Helper will forward dhcp request irrespective of route-map
 ip helper-address 10.30.12.1
 ip helper-address 10.30.12.2
!Route map forces a policy check before routing the packet
 ip policy route-map WIRELESS
! The permit 10 statement at the end specifies the order of routing
! lower number being the first ones to be checked
route-map WIRELESS permit 10
 description Route-map-testing
!Match an ACL this is not necessary but gives more flexibility
 match ip address WIRELESS-ROUTER
!Send the IP packets to a nearest router instead of using global route tables.
 set ip next-hop 10.5.37.199
ip access-list standard WIRELESS
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
!This particular host will not be policy routed
 deny 10.30.31.233
! Everybody will else will be routed by policy.
 permit any
!Beware that there is a possibility of asymmetric routing with PBR.
```

There are other options in the horizon for creating multiple segmented routing topologies within one IP based logical network. MTR (Multi-Topology Routing), this is very experimental and still being discussed with IETF as a proposed extension along with the newer link layer protocols such as OSPF-3. Read introduction by Cisco at http://www3.ietf.org/proceedings/06jul/slides/ospf-3/ospf-3.ppt

Given the current options available for segmented networks, MPLS is a very viable choice. MPLS has been in the service and telecom market for a number of years and has shown maturity. As it stands today, it is as secure as ATM or dedicated network and provides many options for segmented multiple networks. Realize this was the case when VLAN's were introduced to segregate layer 2 networks. Later proof of concept and code was provided to "hop" across VLAN's in certain switches and switch setup.

3. DEFINE SEGMENTED NETWORKS

In a world where customers, suppliers and partners all tap into corporate networks, businesses must provide a secure environment for all of them, Symantec's CEO John Thomson – Feb 2007

3.1 Define segmented networks – IP Management and planning.

A proper segmentation of several networks can be achieved by some simple planning of IP addressing schema. For example, choose private class B (CIDR /16) address for each network that you identify uniquely for access. Why? Here are some benefits

1. Firewall rules can be simplified and optimized – as you will see later.
2. ACL's on routers can be simplified as well
3. NAT pools on routers or firewalls can be used to identify each network easily.

Table 3.1 IP Address Management.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Network name	IP Space	Example networks	
NETWORK A – Finance Administrators (RED)	10.239.0.0/16	Small Bldg 703 North –Vlan 910	10.239.10.0/24
		Large Bldg 811 South – Vlan 928	10.239.28.0/22
		Medium Bldg Cafeteria– Vlan 944	10.239.44.0/23
NETWORK B - Switch Management networks (BLUE)	10.9.0.0/16	Small Bldg 703 North – Vlan 31	10.9.0.0/20
		Large Bldg – 811 South – Vlan 32	10.9.16.0/20
		Medium Bldg Cafeteria– Vlan 33	10.9.32.0/20
NETWORK C -	10.240.0.0/16	Small Bldg 703 North – Vlan 803	10.240.10.0/24
		Large Bldg - 811 South – Vlan 831	10.240.28.0/22
		Medium Bldg Cafeteria – Vlan 833	10.240.32.0/20

The above diagram can simplify your firewall rules by allowing servers that manage switches to be able to do ssh/snmp to 10.9.0.0/16 a class B network. A Class B gives you plenty of place to slice your network into (many) smaller "broadcast domains." The IP addresses being private RFC 1918 are not being wasted.

The segmentation as shown above gives several benefits to troubleshooting as well. For example, if you had dedicated clients in network "A" to be able to access a resource – financial database, it will be easy for field staff to determine if a user is in network A using the first prefix bytes of his IP address and is allowed to access a particular network resources – in this example a financial database.

In the design suggested in this paper, it is required that any client entering any network is required to authenticate via 802.1x to verify their identity. A central directory can be used to steer users to various "networks" via "Tunnel-private-group-id" parameter in RADIUS through LDAP or other central directory. The clients can be placed in their network using either as (a) a username / password or

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

(a) mac-address based 802.1x. If you trust mac addresses, it is also possible to run restricted DHCP server that assigns IP addresses only to known mac addresses clients. It is also possible to use newer features such as "DHCP Snooping" and "IP ARP Inspection" to ensure every client on the wire has been identified by mac-address + IP address relationship. Guest and authentication failed VLAN's can also be very useful concepts. It can be used to quarantine users for information, helpdesk and password reset instructions page.

It is very important that you limit the number of segregated L3 networks you can support. In the MPLS context, each segregated network is called a VRF (Virtual/VPN Routing and Forwarding). A number of layer 2 VLAN's can be combined into a single VRF instance. In the above example VLAN 910, VLAN 928 and VLAN 944 are served by a single VRF called network A (or VRF RED as shown later). You should talk to your routing equipment vendor also to learn of the limitations of the number of VRF instances you can run on your equipment / gear.

In MPLS VPN, it is also possible to designate same block of IP addresses across multiple VRF's, I recommend that you limit duplicate IP schemes. This is so that you avoid troubleshooting headaches for field staff. However there are unique cases where duplicate IP schemes may be very handy to explore e.g., disaster recovery is a good example. Planning and choosing VRF's is a very important exercise, one of the clients I had worked with use the homeland security type model of colors to define VRF's. This was very useful in communicating to the clients the various networks and their "security context." For example a public network can be classified as "green VRF", it helps non-technology people to see the need for segregation and levels of security in each context.

3.2 Examples of MPLS configuration and testing

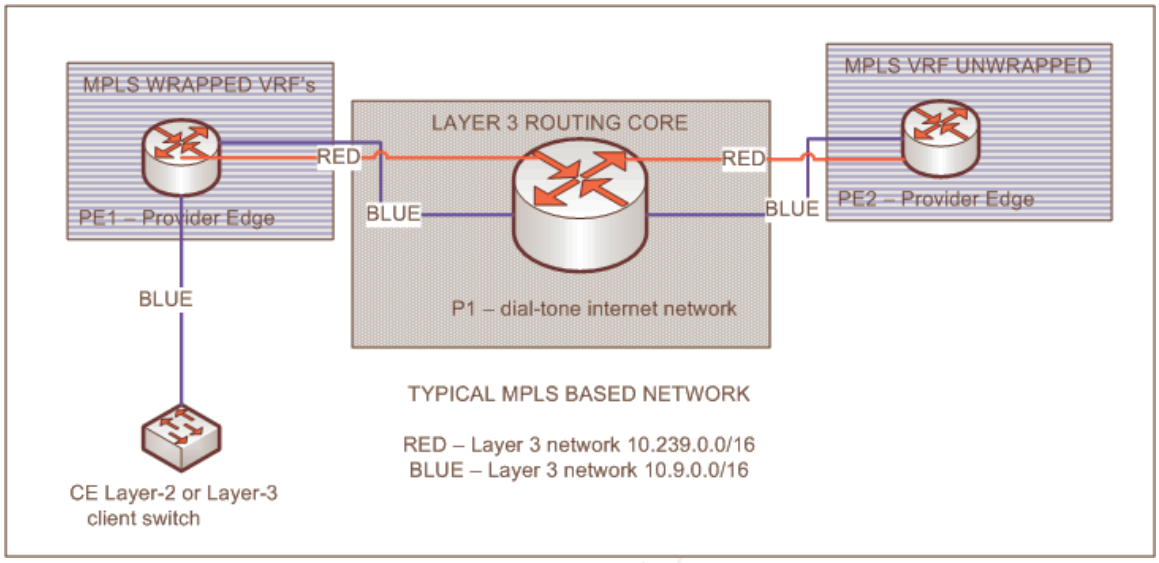
A very basic MPLS configuration example is shown in here. Some of the acronyms, related to MPLS, that you need to be familiar are

CE – Customer Edge device (a Layer 3 or Layer 2 that has no awareness of being in a MPLS network. In my example the device is a simple Layer 2 switch that is not aware of any VRF or MPLS)

PE – Provider Edge device (a layer 3 router that is begin demarcation point for your virtual network or VRF)

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

P – Provider's device / router (a Layer3 carrier provider that is almost like IP dial tone provider)



As shown in the table 3.1 earlier, I will show a very simple example of building an MPLS based network. Most important thing to remember is that we are using a traditional IP transport to carry over multiple routed Layer 3 networks. In this example network RED and network BLUE are two VRF's that are being transported in a single IP based backplane. Let's start with a simple configuration on a Cisco IOS enabled device.

```
hostname PE1
!
ip routing
!
! Start with ip VRF definition this is one network
ip vrf RED
! rd is route distinguisher followed by BGP ASN (private Autonomous System Number)
! ASN:### I have chosen 200 in this example
 rd 64600:200
! This defines where and how we plan to export import routes in this VPNV4 context.
 route-target export 64600:200
 route-target import 64600:200
!
interface Vlan910
! This is our interface or gateway for this network in Small Bldg 703 network A – Finance Dept.
 description Small-Bldg-703-North
! Classify this network as belonging to our RED VRF network
 ip vrf forwarding RED
! Provide the ip address for gateway for clients.
 ip address 10.239.10.1 255.255.255.0
!
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
! Now lets test to make sure this network is isolated.
PE1#sh ip route
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.100/32 is directly connected, Loopback0
C       192.168.1.24/30 is directly connected, GigabitEthernet1/0/12
S    192.168.100.0/24 [1/0] via 192.168.1.26

! We don't see the route in global route table it is hidden under the VRF
PE1#sh ip vrf
  Name                        Default RD        Interfaces
  RED                         64600:200         Vlan910
! Okay you can see the VRF RED is active with ASN 64600 and descriptor 200
PE1#sh ip int br vlan910
Interface            IP-Address      OK? Method Status              Protocol
Vlan910              10.239.10.1     YES manual up                  up
! Okay we can see the interface is up and running, lets try ping - ing
PE1#ping 10.239.101
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.9.234.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
! Hmm.. we cant ping because it is not part of global routes, now lets try VRF ping

PE1#ping vrf RED 10.239.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.239.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

! Okay successful pings.  We can reach it only under the context of VRF RED.
! Here are the codes for interpreting routes, please refer back to here if you need to
! how a route was specified.
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

The above example of configuration is very basic where we have created an isolated layer 3 network called VRF RED consisting of one layer 2 Vlan 910 and a corresponding layer 3 interface (10.239.10.1) and successfully enabled the interface.[3] The network we built called RED exists inside a single switch and is isolated from other layer 3 networks (global route table and other VRF based networks).

Lets move to an advanced example where we have two layer 3 switches and 2 VRF instances (RED-10.239/16 and BLUE-10.9/16) say

[3] Note in your lab exercise, you need to one fake client that is connected to Vlan 910 to bring up the layer 3 interface to active stage.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

in this network. Internal BGP or iBGP is used propagate the routes between the two routers PE1 and PE2. See the configuration examples below of PE1 and PE2

```
! PE1 router basic configuration.
ip routing
! Define VRF BLUE which will carry our network management traffic
ip vrf BLUE
 rd 64600:300
 route-target export 64600:300
 route-target import 64600:300
! Define VRF RED which will carry our financial clients traffic
ip vrf RED
 rd 64600:200
 route-target export 64600:200
 route-target import 64600:200
! This VLAN will serve switch management needs of all North campus.
vlan 31
 name Switch-Management-North-Campus
! This VLAN is part of our Financial network in VRF RED
vlan 910
 name Small-Bldg-703-North
! This VLAN is also part of our Financial network in VRF RED in a different building adjacent
vlan 928
 name Finnace-vlan-at-Large-Bldg-811-South
!
!
interface Loopback0
! Define a loopback interface for doing router management SSH / SNMP etc.
 description Router-Updates-Int
 ip address 192.168.1.100 255.255.255.255
!
interface GigabitEthernet1/0/12
! This the link between PE1 and PE2, the other end is at 192.168.1.26
 description Ip2Ip-Int
 no switchport
 ip address 192.168.1.25 255.255.255.252
 mpls label protocol ldp
 tag-switching ip
! Layer 3 part of the layer 2 VLAN earlier specified are listed here
interface Vlan31
 description Switch-Management-North-Campus
! Assocaite this with the VRF instance BLUE
 ip vrf forwarding BLUE
 ip address 10.9.0.1 255.255.240.0
!
interface Vlan910
 description Small-Bldg-703-North
! Associate this with the VRF instance RED
 ip vrf forwarding RED
 ip address 10.239.10.1 255.255.255.0
!
interface Vlan928
 description Large-Bldg-811-South
! Associate this with the VRF instance RED
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
 ip vrf forwarding RED
 ip address 10.239.28.1 255.255.255.0
! Now comes the fun part of distributing routes to our iBGP neighbor 192.168.1.26
router bgp 64600
! It is very important that you watch any changes to BGP
 bgp log-neighbor-changes
! Declare your neighbor don't trust your feelings ☹
 neighbor 192.168.1.26 remote-as 64600
 ! Declare what routes can propogate both IPV4 and VPNV4 needs to be declared here.
 address-family ipv4
 neighbor 192.168.1.26 activate
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 192.168.1.26 activate
! Community extended ensures the maping of route descriptors happen on both end
! this is more useful later on extranets chapter.
 neighbor 192.168.1.26 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf RED
! This is automatically created to distribute routes to the other router, but do specify
! distribution of static routes. NOTE: iBGP will NOT propogate default route specified
! by "ip route 0.0.0.0 0.0.0.0 XX.YY.253.1" this is by design.
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf BLUE
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
```

The configuration shown above has built a basic MPLS network. Two networks one financial in this example with VRF RED and one switch management network in VRF BLUE. They are on the same routers and switches but they cannot see each other. In layer 2, VLAN segregation keeps them from seeing each other. In layer 3, VRF instances keeps them from seeing each other. In this very basic example, we have built two completely independent layer 3 networks on the same physical and logical (IP) infrastructure. To show some details see blow routes on PE1 and PE2 routers.

```
PE1#sh ip route vrf RED
Routing Table: RED
Gateway of last resort is not set
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
    10.0.0.0/24 is subnetted, 3 subnets
! This route was learned by iBGP from neighbor PE2
B       10.239.44.0 [200/0] via 192.168.1.26, 21:42:54
C       10.239.10.0 is directly connected, Vlan910
C       10.239.28.0 is directly connected, Vlan928
PE1#sh ip route vrf BLUE
Routing Table: BLUE
Gateway of last resort is not set
    10.0.0.0/20 is subnetted, 2 subnets
C       10.9.0.0 is directly connected, Vlan31
! This route was learned by neighbor PE2
B       10.9.32.0 [200/0] via 192.168.1.26, 00:31:57
PE1#sh ip route
Gateway of last resort is not set
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.100/32 is directly connected, Loopback0
C       192.168.1.24/30 is directly connected, GigabitEthernet1/0/12
S    192.168.100.0/24 [1/0] via 192.168.1.26
PE1#
```

Now let's see the routing tables on PE2 to see if routes from PE1 are there and they are isolated from each other.

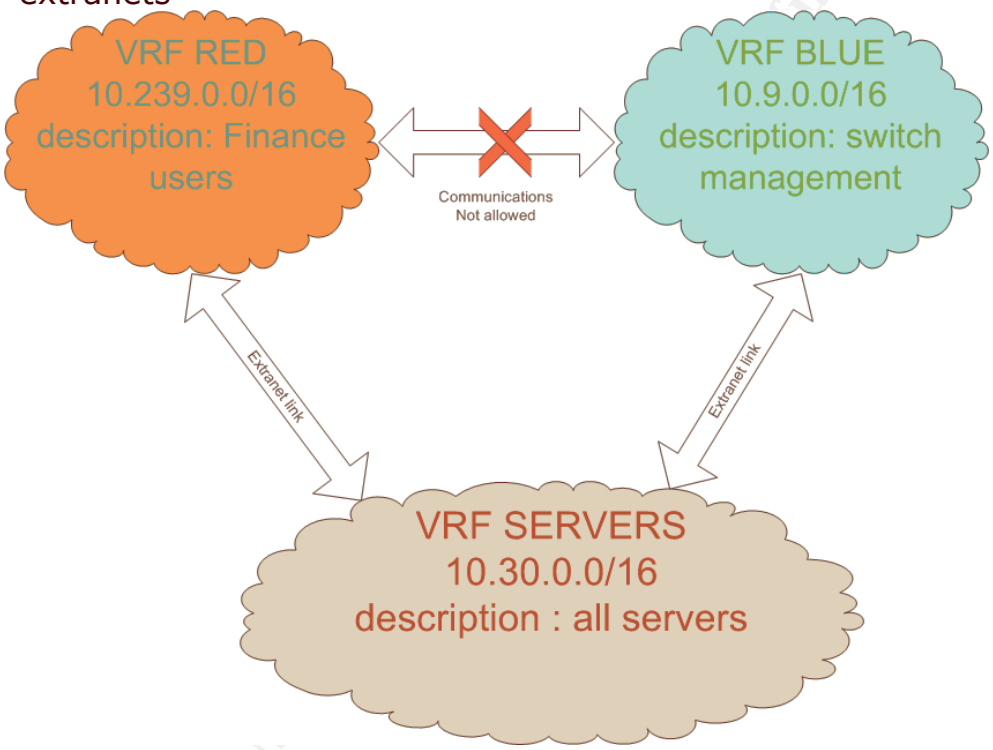
```
PE2#sh ip route vrf RED
Routing Table: RED
Gateway of last resort is not set
    10.0.0.0/24 is subnetted, 3 subnets
C       10.239.44.0 is directly connected, Vlan944
B       10.239.10.0 [200/0] via 192.168.1.25, 21:46:20
B       10.239.28.0 [200/0] via 192.168.1.25, 21:46:20
PE2#sh ip route vrf BLUE
Routing Table: BLUE
Gateway of last resort is not set
    10.0.0.0/20 is subnetted, 2 subnets
B       10.9.0.0 [200/0] via 192.168.1.25, 00:38:36
C       10.9.32.0 is directly connected, Vlan33
PE2#sh ip route
Gateway of last resort is not set
    192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.24 is directly connected, GigabitEthernet1/0/3
    192.168.100.0/30 is subnetted, 1 subnets
C       192.168.100.100 is directly connected, FastEthernet1/0/48
! End of PE2 route tables.
```

Thus you can continue to build multiple networks, once a simple physical and logical (IP in this case) infrastructure has been built. MPLS also has the ability to transport L2 – Ethernet frames, in a mode called Ethernet-over-MPLS or EoMPLS. This is usually not necessary, unless you are doing layer 2 protocols between disperse layer 3 networks.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

3.3 Define overlaying or extranet segments and show examples of configuration.

The network RED and BLUE in the earlier example cannot see each other. Thus financial network A will not be able to attach or get to the switch network. Now the problem arises for when you need two VRF's that need to talk to each other. For example the finance VRF RED (also called network A) needs to be able to access the server-farm network which is called VRF SERVERS. It is possible to build what is called "extranets" with MPLS VPN. In the diagram below VRF RED and VRF BLUE can talk to VRF SERVERS but still they cannot talk to each other. These networks are called overlaying VRF segments or "extranets"



One way to build this extranets is by creating "route imports" and "route exports" across VRF's. This has to be well documented and done, if not you will easily misconfigure and allow communications between VRF's. You will also create unintended route loops, if there is a mistake in your configuration. You can also create links between VRF's using a firewall as a termination point for various VRF's [4]. This is very useful when you are terminating various client network pools

[4] Note: This is not possible if you use transparent firewalls, which are discussed in chapter 4.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

on a firewall to NAT and be allowed to access the internet. A firewall can also be used is to control communications between the VRF's. It is also important that you limit the number of extranets you will build to avoid complexity. Each extranet should be documented and detailed so you know the reason for building extranet and what communications where intended through the extranet links.

Now to the good stuff, configuration on Cisco IOS to achieve is

```
! define the new network VRF SERVERS
ip vrf SERVERS
! put a description, this VRF instance is unique we will see later
 description SERVERFARM-NET-10.30/16
! Define a route distinguisher
rd 64600:900
!Import our own routes this is not important or relevant in this case but for consistency we will do this
! if we need to build serverfarm across multiple L3 routers it is useful
route-target import 64600:900
! This is important so you can import these routes on the other end in VRF BLUE and RED
route-target import 64600:900
! Import routes from  VRF RED
 route-target import 64600:200
! Import routes from VRF BLUE
 route-target import 64600:300
! Add necessary import information on VRF BLUE
ip vrf BLUE
 rd 64600:300
 route-target export 64600:300
 route-target import 64600:300
! Add this line to import the routes from the serverfarm network
 route-target import 64600:900
! Modify the VRF RED as well
ip vrf RED
 rd 64600:200
 route-target export 64600:200
 route-target import 64600:200
! Grab routes to the serverfarm.
 route-target import 64600:900
!
! Lets define one IP interface in this SERVERS VRF network
interface Vlan1020
 description SERVERFARM-OUTSIDE
! Assign appropriate VRF instance
 ip vrf forwarding SERVERS
! Create a single ip termination for class B – we will see later how transparent firewall
! is going to layer 2 bridge this traffic to a outside⇔ inside interface relationship.
 ip address 10.30.254.254 255.255.0.0
!
! Now lets look at the routes. Watch VRF RED and BLUE can see VRF SERVERS but cannot see
! each other.
PE1#sh ip route vrf RED
Routing Table: RED
Gateway of last resort is not set
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
B      10.30.0.0/16 is directly connected, 00:13:03, Vlan1020
B      10.239.44.0/24 [200/0] via 192.168.1.26, 22:51:09
C      10.239.10.0/24 is directly connected, Vlan910
C      10.239.28.0/24 is directly connected, Vlan928
! Note you can see the network VRF SERVERS at 10.30.0.0/16 but cannot see BLUE 10.9.0.0/16
PE1#sh ip route vrf BLUE
Routing Table: BLUE
Gateway of last resort is not set
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C      10.9.0.0/20 is directly connected, Vlan31
B      10.30.0.0/16 is directly connected, 00:13:35, Vlan1020
B      10.9.32.0/20 [200/0] via 192.168.1.26, 01:41:24
! Note you can see the network VRF SERVERS at 10.30.0.0/16 but cannot see RED 10.239.0.0/16

! Now to more diagnostics.  From VRF RED we will ping a local subnet, remote server subnet
! and then the BLUE network to see what is reachable.
PE1#ping vrf RED 10.239.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.239.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
PE1#ping vrf RED 10.30.254.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.254.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
! Lest try and ping an ip address in VRF BLUE from VRF RED  - should be unreachable
PE1#ping vrf RED 10.9.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.9.0.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PE1#
```

The design of server farm is not detailed in this chapter. We will show later the use of transparent firewall and it's design to simplify the design of a serverfarm. This is why the VRF SERVERS is assigned a single class B ip address 10.30.254.254/16. So you can see how these networks (VRF RED and BLUE) as shown in the diagram can both see VRF SERVERS, but cannot have routes or connections to each other. Is this secure? In brief YES! is the answer. MPLS is packet switching according to MPLS tags. MPLS tagged packets cannot cross two VPN VRF segments. They can only be imported and exported as routes, which means the MPLS tagged IP packets will be encapsulated again with new the MPLS tags before reaching their destination network. The takeaway is that the security provided by logical segmentation via MPLS/VPN is considered comparable to Frame-relay, ATM, or VLAN's[5].

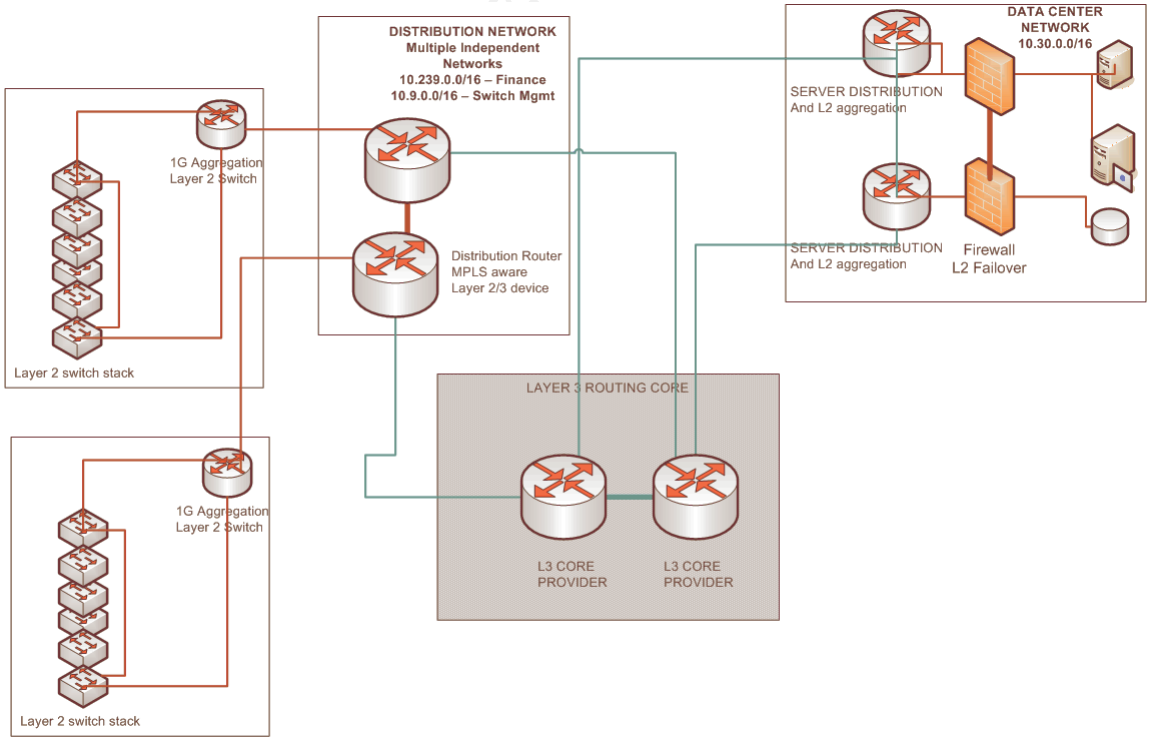
[5] Read more on MPLS Security at Security of the MPLS Architecture
http://www.cisco.com/en/US/products/ps6822/products_white_paper09186a00800a85c5.shtml

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

The question arises can we deploy same type of control using ACL's or VACL (VLAN ACL's) in each of the router. The answer is absolutely yes, but it is surely difficult to manage and not very scalable. Each new IP interface needs the ACL assignments. It is also very easy to do mistakes. VLAN ACL's are powerful. They are used to provide "layered" security such as in the case of perimeter or border router and in some specific applications such as printers, as we will see later. These two security mechanisms (MPLS VPN and VLAN ACL's) should compliment each other. The manipulation of MPLS VPN architecture provides more flexible way to achieve this same purpose and is scalable across even WAN links to remote offices. MPLS switching endpoints are the ones who need to be aware of the MPLS tags. MPLS VPN encryption is also possible which is not covered in this paper.

3.4 Redraw physical infrastructure and logical infrastructure.

It is always good to take a quick look to see where you are in the design of your network components. This is such a review phase. As many components have been added to the mix and now it is time to visualize the design.

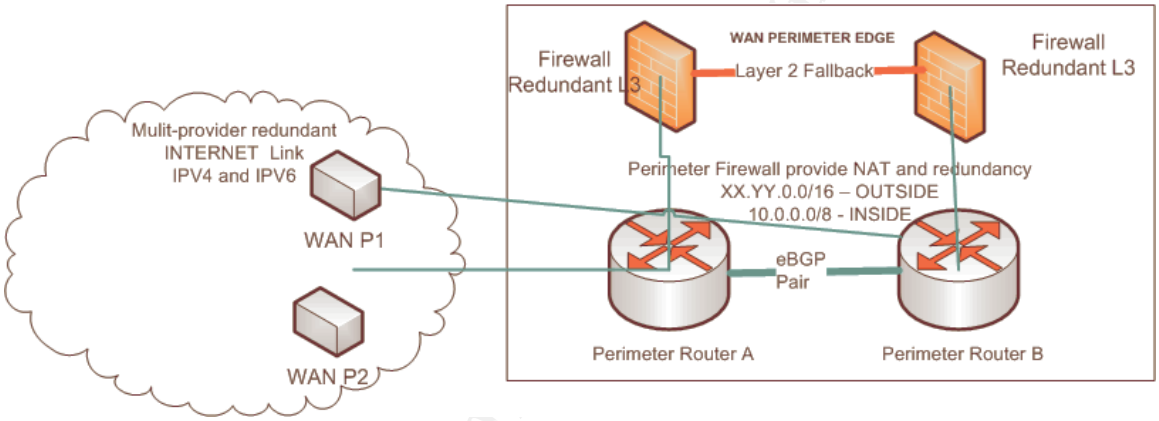


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

The Data center or serverfarm network is actually not as fully defined yet. We will look at this at the very start of the next chapter. Further to this design is the defining our perimeter router and its requirements.

3.5 Perimeter router and Firewall design

The purpose of this chapter is to pursue a router ACL that complies with your policy, optimize this perimeter ACL, test the ACL reliability and see options that you can pursue now or later. The ACL's also consider protecting your global route tables.



3.5.1 Perimeter router ACL example

The below perimeter ACL is designed for a class B IP address of XX.YY.0.0/16. All options in this network are explained with comments. You can see pretty much the purpose of each ACL, and the intended protection provided by the ACL. The architecture shows a small subnet class C of our public IP address XX.YY.33.0/24 is used for providing DNS and SMTP service to the world. These services need ultimate protection from the world, as recommended by SANS. Some of the popular once worth noting

1. Block fragmented ICMP
2. Block fragmented UDP (Should I?)

Answer: This is optional, UDP fragments to higher order port are used for DOS attacks. [6] You can watch perimeter traffic with tcpdump or windump to catch all UDP fragments and verify if there is an application in your environment using this)

```
tcpdump –pnnvvi xl0 'udp and (ip[6:2] & 0xBFFF > 0)'
or windump –pnnvvi 3 "udp and (ip[6:2] & 0xBFFF > 0)"
```

[6] http://www.grc.com/dos/grcdos.htm GRC was attacked by this type of packets. You can search google for "UDP fragment DOS" you will find plenty of reference material.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

3. Block lower order ports UDP/TCP < 20
4. Block RPC (135-139), DCOM(445), RPC over HTTP (593/TCP)
5. Block BGP(TCP 179) from the world protect your global route
6. Allow DNS and SMTP only to designated servers.
7. Block Bogon IP (optional), private IP, 127/8
8. Block SNMP queries from the world

```
ip access-list extended INTERNET-INBOUND
! Deny fragmented ICMP you should never see it in the border
  20 deny icmp any any fragments log-input
! This is surely an option as well, you should not see udp fragments across the perimiter
 ! 30 deny udp any any fragment
! Allow useful ICMP stuff ping, unreachable time-exceeded only for our public IPS
   40 permit icmp any XX.YY.0.0 0.0.255.255 echo-reply
! This is optional to allow unreachables to go through to remote hosts
   50 permit icmp any XX.YY.0.0 0.0.255.255 unreachable
   60 permit icmp any XX.YY.0.0 0.0.255.255 source-quench
   70 permit icmp any XX.YY.0.0 0.0.255.255 echo
   80 permit icmp any XX.YY.0.0 0.0.255.255 time-exceeded
! Deny all other icmp
   90 deny icmp any any
! Permit udp and tcp dns only to our DMZ DNS servers public addresses.
   100 permit udp any XX.YY.33.0 0.0.0.255 eq domain
   110 permit tcp any XX.YY.33.0 0.0.0.255 eq domain
! Drop any other DNS queries
   120 deny udp any any eq domain
   130 deny tcp any any eq domain
! Limit smtp to our designated DMZ SMTP servers
   140 permit tcp any XX.YY.33.0 0.0.0.255 eq smtp
! Deny other SMTP activity . logging was too noisy in this case.
   150 deny tcp any any eq smtp
! Deny non ip and private RFC1918 IP space from entering us
   170 deny ip host 0.0.0.0 any log-input
   180 deny ip 127.0.0.0 0.255.255.255 any log-input
   190 deny ip 169.254.0.0 0.0.255.255 any log-input
   210 deny ip 10.0.0.0 0.255.255.255 any  log-input
   220 deny ip 172.16.0.0 0.15.255.255 any log-input
   230 deny ip 192.168.0.0 0.0.255.255 any log-input
! Log anybody who fakes our source address for 2 reasons
! (1) troubleshoot misconfigured routers at ISP
! (2) Watch for attackers tricking into our network
   240 deny ip XX.YY.0.0 0.0.255.255 any log-input
! IANA Reserved Broadcast space block
   250 deny ip 255.0.0.0 0.255.255.255 any
! Leave enough numbers 260-400 for bogon filters - one example of blackhole
! two class A networks 0.0.0.0/8 and  1.0.0.0/8
   200 deny ip 0.0.0.0 1.255.255.255 any log-input
! Protect your BGP global route tables
   440 deny tcp any any eq 179 log-input
! If you have a tarpit server or tarpit networks - recommend beg and end class C's XX.YY.0/24
! and XX.YY.255/24
   450 permit ip any XX.YY.0.0 0.0.0.255
   460 permit ip any XX.YY.255.0 0.0.0.255
! Deny low order ports
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
   470 deny udp any any range 0 19 log-input
   480 deny tcp any any range 0 19 log-input
! Deny bootps bootpc, NETBIOS, DCOM and tftp  ports both tcp and udp
   490 deny tcp any any range 67 69 log-input
   500 deny tcp any any range 135 139 log-input
   510 deny tcp any any eq 445 log-input
   520 deny udp any any range 67 69 log-input
   530 deny udp any any range 135 139 log-input
   540 deny tcp any any eq 593 log-input
! Allow our partner monitoring servers to get to pub DMZ via sNMP
   620 permit udp host RR.SS.11.12 XX.YY.33.0 0.0.0.255 eq snmp
! Deny all other snmp from world.
   630 deny udp any any range 161 162 log-input
! Deny DCOM in UDP mode
   650 deny udp any any eq 445 log-input
! Permit our class B IP address to get out.
   660 permit ip any XX.YY.0.0 0.0.255.255
! Permit a specific multicast group we use for video.
   670 permit ip any 224.0.0.0 31.255.255.255
! Remember implicit deny will drop packets faking source address or anything else.

ip access-list extended INTERNET-OUTBOUND
! Deny icmp fragment outgoing and log it
   20 deny icmp any any fragments log-input
! This is surely an option as well, you should not see udp fragments across the perimiter
 !  30 deny udp any any fragment
! Map access-list numbers whenever possible with inbound
   40 permit icmp XX.YY.0.0 0.0.255.255 any echo-reply
! This is also optional to send ICMP unreachable
   50 permit icmp XX.YY.0.0 0.0.255.255 any unreachable
   60 permit icmp XX.YY.0.0 0.0.255.255 any source-quench
   70 permit icmp XX.YY.0.0 0.0.255.255 any echo
   80 permit icmp XX.YY.0.0 0.0.255.255 any time-exceeded
! Deny all other ICMP
   90 deny icmp any any log-input
! Permit our DNS servers to server DNS queries in public DMZ XX.YY.33.0/24 Class C for DNS
   100 permit udp XX.YY.33.0 0.0.0.255 any eq domain
   110 permit tcp XX.YY.33.0 0.0.0.255 any eq domain
! Deny all other DNS attempts.
   120 deny udp any any eq domain log-input
   130 deny tcp any any eq domain log-input
!Permit outgoing TCP from our servers in public DMZ XX.YY.33.0/24 Class C for SMTP
   140 permit tcp XX.YY.33.0 0.0.255.255 any eq smtp
! Deny all other SMTP connections . logging is useful in finding bots
   150 deny tcp any any eq smtp log-input
! Deny non ip and private RFC1918 IP space for our hosts as destination
   170 deny ip any host 0.0.0.0 log-input
   180 deny ip any 127.0.0.0 0.255.255.255 log-input
   190 deny ip any 169.254.0.0 0.0.255.255 log-input
   210 deny ip any 10.0.0.0 0.255.255.255 log-input
   220 deny ip any 172.16.0.0 0.15.255.255
   230 deny ip any 192.168.0.0 0.0.255.255
! Useful for learning our unknown routes being sent to the world
   240 deny ip any XX.YY.0.0 0.0.255.255 log-input
! Reserved IANA broadcast space
   250 deny ip any 255.0.0.0 0.255.255.255
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
! Protect other ISP's BGP global route tables
   440 deny tcp any any eq 179 log-input
! If you have a tarpit server or tarpit networks - recommend beg and end class C's XX.YY.0/24
! and XX.YY.255/24
   450 permit ip any XX.YY.0.0 0.0.0.255
   460 permit ip any XX.YY.255.0 0.0.0.255
! Deny low order ports
   470 deny udp any any range 0 19 log-input
   480 deny tcp any any range 0 19 log-input
! Deny bootps bootpc, NETBIOS, DCOM and tftp  ports both tcp and udp
   490 deny tcp any any range 67 69 log-input
   500 deny tcp any any range 135 139 log-input
   510 deny tcp any any eq 445 log-input
   520 deny udp any any range 67 69 log-input
   530 deny udp any any range 135 139 log-input
   540 deny tcp any any eq 593 log-input
! Deny all snmp from going outside our border
   630 deny udp any any range 161 162 log-input
! Deny DCOM in UDP mode
   650 deny udp any any eq 445 log-input
! Permit our class B IP address to get out.
   660 permit ip XX.YY.0.0 0.0.255.255 any
! Permit a specific multicast group we use for video.
   670 permit ip 224.0.0.0 31.255.255.255 any
! Remember implicit deny will drop packets faking source address or anything else.
! This is optional so you can see the noise of other attempts
! 700 deny any any log-input

no ip source-route

interface GigabitEthernet 2/2
  description WAN internet link
  ip address XX.YY.1.1 255.255.255.0
  ip access-group INTERNET-INBOUND in
  ip access-group INTERNET-OUTBOUND out
! This is safe in preventing redirects from our WAN interface
 no ip redirects
! Lets not send ip unreachables except for our networks trying
!the outside world.
  no ip unreachables
! be conservative in your TCAM resource protection.
! high is recommended if you have plenty of horse power like CAT6500 – SUP II or 720
   tcam priority high

! Set the logging level
logging trap debugging
! Logging facility is used in parsing the logs in syslog.conf file
logging facility local2
! Use a source interface that is local only loopbacks are good for this
logging source-interface Loopback0
! Send one copy of logs to our server in DMZ
logging XX.YY.33.22
! Send one copy of logs to our server in INSIDE zone
logging  10.30.11.1
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

!(some of the config related to SNMP and other security acl's are suppressed here)

Now, don't forget to balance your design by considering resource consumption of perimeter routers. The increased level of perimeter ACL's might consume precious TCAM resources on Cisco routers and ASIC based layer 3 switches. Some ideas for optimization are given below

1. Avoid range statements "deny udp any any range 67 69" is more resource consuming than "deny udp any any eq 67" , "deny udp any any eq 68" and "deny udp any any eq 69" – although it is more rules to maintain.
2. Avoid logging for noisy ACL's – e.g., SMTP scanning from outside.
3. Optimize your ACL's – for example two ACL's for bogon routes "deny ip 0.0.0.0 0.255.255.255" and "deny ip 1.0.0.0 0.255.255.255" can be combined to "deny ip 0.0.0.0 1.255.255.255"

Although the rules look fairly good and stable, don't assume anything. Test your rules – use "stream.c" or "trash.c" tools which are DOS tools to verify. Here is the sample of the logs generated by using ping / hping tool to craft icmp and IP packets to test our new ACL's.

TEST #1 : Test Large ICMP which will get fragmented and denied by our ACL

```
Linux_host> ping –s 1900 myrouter
PING myrouter (10.1.1.1): 1900 data bytes
--- 10.1.1.1 ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
[Log file on syslog server]
Feb 17 16:21:56 myrouter 180: Feb 17 16:21:55: %SEC-6-IPACCESSLOGDP: list INTERNET-
INBOUND denied icmp 10.30.12.2 (GigabitEthernet2/2 ****.41b9.80ff) -> 10.1.1.1 (0/0), 3 packets
```

TEST #2 : Test spoofed packet target inside IP, source address fake 0.1.1.1, Location: outside interface

```
Linux_host> hping -a 0.1.1.1 –p 51405 XX.YY.33.11
HPING XX.YY.33.11 (em0 XX.YY.33.11): NO FLAGS are set, 40 headers + 0 data bytes
^C
--- 10.1.1.1 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

Feb 17 16:07:19 myrouter 9204: Feb 17 16:07:18: %SEC-6-IPACCESSLOGP: list INTERNET-
INBOUND denied tcp 0.1.1.1(16429) (GigabitEthernet2/2 ****.41b9.80ff) -> XX.YY.33.11(51405), 1
packet
```

3.5.1 How to keep your bogon or unassigned IP address updated

IANA (www.iana.org) puts out regularly updates at their website for IPV4 space management. The IPV4 addresses unallocated are

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

sometimes used by attackers either for DOS attack or for reconnaissance. If your border router has enough power in it, I highly recommend looking at the script below and modifying it to write ACL's. The output of the below script will be in CIDR format can be used to develop Cisco ACL's or IPTABLES or ACL's relevant to your product. Some example of this reserved IP space are 2.0.0.0/8 has been reserved and not allocated since IPv4 addresses were introduced. The script shown below can be run monthly to ensure that the IPv4 addresses that get allocated by IANA to various providers are updated on your border router.

A simple shell scripts that looks for bogon updates from IANA##

```
#!/bin/sh
#IANA Bogon IP address list from their website.
DATE=`date +%Y%m%d`
wget -q --output-document=/var/inventory/iana.txt.$DATE \
http://www.iana.org/assignments/ipv4-address-space
diff /var/invenotry/iana.txt.$DATE  /var/inventory/iana.txt.current  > /dev/null
if [ $? == 0 ];
# No changes exit quietly
exit
fi
#This is else send an email with changes
diff -c /var/inventory/iana.txt.current /var/invenotry/iana.txt.$DATE \
| mail -s "Updated Changes to IANA bogon list" networks@localhost
#Put the reserved ip's in CIDR format in a file, they are class A
grep 'Reserved\|Multicast' /var/inventory/iana.txt.$DATE  \
| cut -d'/' -f1 | sed -e 's/^0\{1,2\}//' | sed -e 's/^\(.*\)$/.0.0.0\/8/' > reserved
```

3.5.2 Consider some advanced options for access control lists

The newer options in Cisco's ACL in 12.3(4)T and 12.2(25)S train code is the support for advanced inspection of your IP packets using TTL (time to live) and IP options. Read more at http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d4a7d.html

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended INTERNET-INBOUND
! Allow our incoming connections to use record route options with "ping –R"
Router(config-ext-nacl)#  permit ip any any option record-route
! Deny loose source routing packets value = 131
Router(config-ext-nacl)#  deny ip any any option lsr
! Deny strict source routing packcets value = 137
Router(config-ext-nacl)#  permit ip any any option ssr
! Deny packets with TTL less than our 3 router level down where our servers live
! Only for Cisco 12.3 (4T)
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
! Be careful you can drop traceroute
Router(config-ext-nacl)#  deny ip any any ttl lt 3
```

These are very advanced and new options in Cisco's ACL support. As a network consultant, I would recommend some of these options especially source routing. This is true even if you have an IDS (to alert of IP Options packets) or IPS (drop IP Options packet) doing the work. The reason is "Defense in Depth" - which means your protection needs to be reinforced across multiple devices.

3.5.3 Perimeter Firewall design

This is probably the simplified configuration of firewall. The firewall is really designed to provide multiple security layers. The firewall configuration needs to provide

1. NAT services to internal clients for access to WAN.
2. Protection from outside world scanning, probing our network.
3. Permitting specific services in DMZ to be accessible from WAN.
4. Logging specific access attempts – especially denied attempts.

The firewall configuration, in principle is shown below for PIX 7.0 code.

```
interface ethernet0 auto
interface ethernet1 auto
interface ethernet1 vlan538 logical
interface ethernet1 vlan539 logical
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet5 lan-failover security99
nameif vlan538 CLIENT_POOL1 security98
nameif vlan539 CLIENT_POOL2 security99
enable password ********** encrypted
passwd ********** encrypted
hostname defender
domain-name mydomain.com
! Use the available fixup protocols this is a very good timesaver in seeing non-dns traffic in dns port
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol pptp 1723
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
! This is optional, if you use SMTP STARTTLS or SMTP AUTH to remote servers this should be disabled.
!fixup protocol smtp 25
fixup protocol sqlnet 1521
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
fixup protocol tftp 69
! Use object groups to simplify your rules and limit them.
object-group network n_CLIENT_POOL2
  description CLIENT_POOL2-10.4
  network-object 10.239.0.0 255.255.0.0
object-group service s_CLIENT_POOL2 tcp-udp
  description CLIENT_POOL2-allowed-services
  port-object eq www
  port-object eq 443
  port-object eq 22
object-group service s_UNPRIV tcp-udp
  description Unprivileged-ports
  port-object range 1023 65535
! Keep accesslist very simple to interpret here we are saying CLIENT_POOL2 network can access
! service CLEINT_POOL2 to anywhere
access-list CLIENT_POOL2 permit tcp object-group n_CLIENT_POOL2 object-group s_UNPRIV any
object-group s_CLIENT_POOL2
pager lines 20
! our logging design is discussed later.  Surely turn on logging and send it to
! two servers preferably in different subnets.
logging on
logging monitor warnings
logging buffered warnings
logging trap warnings
! Different subnet logging, one going to DMZ and one going to our DATA Center serverfarm.
logging host CLIENT_POOL1 XX.YY.12.1
logging host CLIENT_POOL1 10.30.12.2
ip audit info action alarm
ip audit attack action alarm
! Failover design can be read more at www.cisco.com/go/pix
failover
failover timeout 0:00:00
failover poll 15
failover ip address ssh 192.168.100.171
failover ip address lan-failover 192.168.200.2
failover ip address CLIENT_POOL1 10.5.38.99
failover ip address CLIENT_POOL2 10.5.39.253
failover link lan-failover
failover lan unit primary
failover lan interface lan-failover
failover lan key **********
failover lan enable
! Define access list associations to interfaces.
access-group outside in interface outside
access-group CLIENT_POOL1 in interface CLIENT_POOL1
access-group CLIENT_POOL2 in interface CLIENT_POOL2
! Allow SNMP polling for traffic CPU from HP Openview.
snmp-server host CLIENT_POOL1 10.30.15.129 poll
! HA good one make sure floodguard is enabled.
floodguard enable
!fragmentation – this is upto our design, make sure your IDS / IPS and end host
! are protected and inspected for fragment timing attacks by matching these values
fragment outside size 1500
! Here fragment database is limited to  a maximum size of 1500, a
!maximum chain length of 45, and a wait time of 60 seconds - to match typical IDS's
fragment chain 45 outside
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
fragment outside timeout 60
! Don't telnet, only SSH from a dedicated interface.
ssh 10.30.0.0 255.255.0.0 ssh
ssh timeout 5
! XLATE and CONN timeouts are important to tweak, read and do the tweaking carefully
timeout xlate 0:45:00
! even more for UDP traffic here.
timeout conn 0:45:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
! I would recommend defaults for SIP and H322 traffic.
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
! This is a very useful tool for checking teardown of ftp connections see below
timeout uauth 0:00:00 absolute


! The user goes on with the Telnet or FTP business on the target host, then exits (spends 10 minutes there):
!(pix) 302002: Teardown TCP connection 5 faddr
!    XX.YY.9.25/80 gaddr RR.TT.9.10/128 1
!    laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse)
!   (server stop account) Sun Nov 8 16:41:17 1998
!    megaladon.mydomain.com cse
! PIX 192.168.100.100 stop task_id=0x3 foreign_ip=XX.YY.9.25
!    local_ip=10.39.118.100 cmd=telnet elapsed_time=5
!    bytes_in=98 bytes_out=36
!Whether uauth is 0 (authenticate every time) or more (authenticate once and not again during uauth
! period), an accounting record is cut for every site accessed. Read more at cisco's website
! http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a0080094e7e.shtml
```

Some security and operational options are highlighted for your convenience. Few things to take down on your perimeter firewall design

- ⇨ Enable Logging and log to two servers in different subnets
- ⇨ Enable security fixup and features – ask your vendor. Examples are floodguard, fragguard and http_inspect.
- ⇨ Use fixup to verify what is being passed in layer 4 port numbers. DNS is a good example of this.
- ⇨ Use tcp and udp statefuleness timeouts to be tweaked from default. Default is designed for any network – you need to pick values suitable for yours.
- ⇨ Simplify your access-list for auditing and validating. For generic access lists use object-groups to broadly classify clients and services. For specific services, make a group and check the access list by doing "sh access-lists" regularly and see counters. If counters disappear – rule should be re-visited or *removed*.

As you can see perimeter firewall design can enormously simplified with planning. You should however not simplify required research for many unique conditions such as fragements, translates,

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

icmp statefuleness (not available in PIX) and limits on number of active connections (called embryonic limits in PIX).

4. DATA CENTER FIREWALL's and VPN

"Finally we shall place the Sun himself at the center of the Universe" - Nicolaus Copernicus

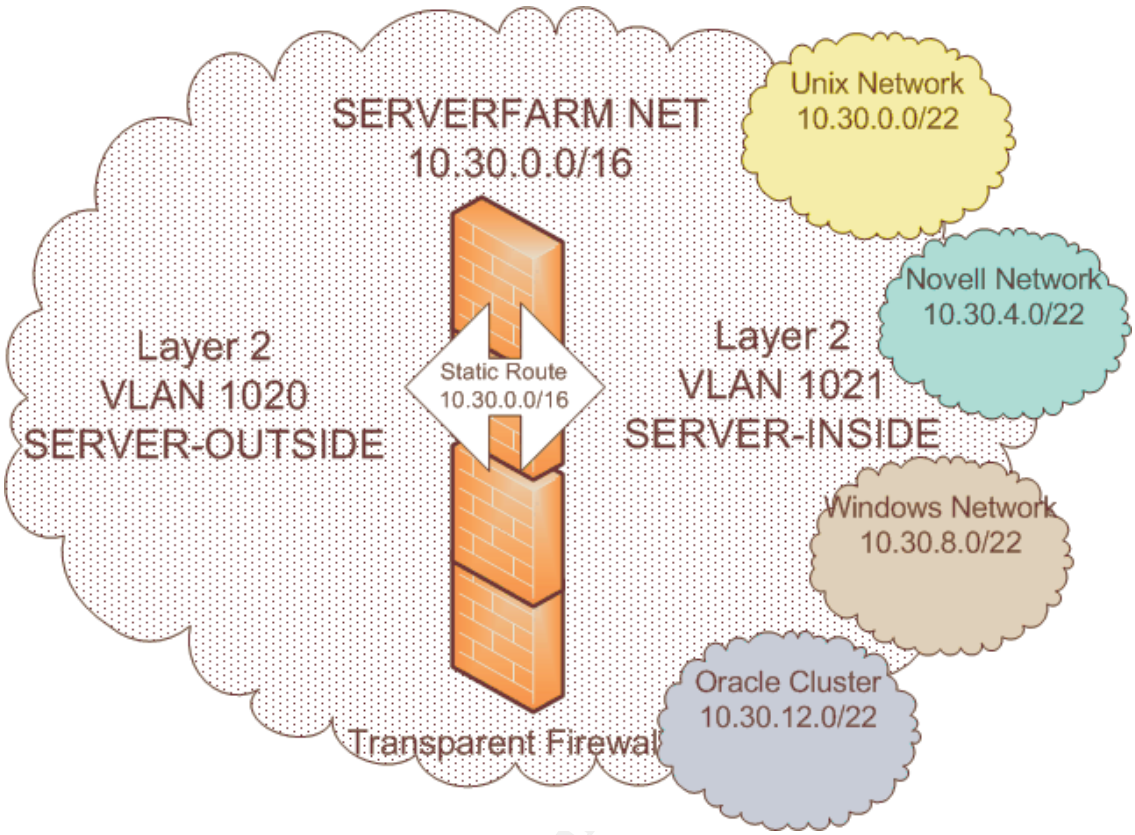
4.1 Define Data center firewall needs, modes of firewall operation

4.1.a Choice of firewall modes and suitable applications.

The PIX Security Appliance can operate in two different modes. Firewall modes of operation are shown below.

1. **Routed mode**—In routed mode, the PIX has IP addresses assigned to its interfaces and acts as a router hop for packets that pass through it. All traffic inspection and forwarding decisions are based on Layer 3 parameters. This is how PIX Firewall versions earlier than 7.0 operate.
2. **Transparent mode**—In transparent mode the PIX does not have IP addresses assigned to its interfaces. Instead it acts as a Layer 2 bridge that maintains a MAC address table and makes forwarding decisions based on that. The use of full extended IP access lists is still available and the firewall can inspect IP activity at any layer. In this mode of operation the PIX is often referred to as a "bump in the wire" or "stealth firewall". There are other significant differences as to how transparent mode operates in comparison to routed mode:
    - Only two interfaces are supported—*inside* and *outside*
    - NAT is not supported or required since the PIX is no longer a hop.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.



The "transparent mode" operation functions in a secure Layer 2 bridging mode, providing Layer 2-7 firewall security services for the protected network while remaining *"invisible"* to devices on each side of it. The biggest benefit is it that this simplifies firewall deployments in existing network environments and creates a quick Layer 2 security perimeters by enforcing rules.

Transparent mode is ideal deployment for situation like a serverfarm or data center firewall. A simple configuration is shown below

```
! Define Firewall mode of operations
firewall transparent
hostname transparent-firewall
enable password ********* encrypted
names
! Interfaces configuration and vlan mapping configuration suppressed for simplicity.
! Choose passive ftp as default. This gives some security from
! being scanned with source port 20
ftp mode passive
pager lines 24
no ip address
no failover
no asdm history enable
! arp timeout is critical to choose on a transparent mode firewall
arp timeout 14400
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
! Be more relaxed in xlate states because it is local clients
! who may do file shares, backups.  Note external clients in
! this model will not see this firewall, except when doing VPN.
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
! Uauth for telnet and ftp still should be kept 0 absolute as shown before.
timeout uauth 0:00:00 absolute
! other configuration options suppressed for this devicce.
! Use the default settings for deep inspection of packet payload and pattern.
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
! Increase this to 768 as recommended in our DMZ DNS server configuration for eDNS
! functionality with a maximum of 768 Bytes
  message-length maximum 768
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
! HA good one make sure floodguard is enabled. Note in 7.0 code floodguard is default enabled.
! If you upgrade from 6.3 to 7.0 code this would not be necessary.
floodguard enable
!fragmentation – this is upto our design, make sure your IDS / IPS and end host
! are protected and inspected for fragment timing attacks by matching these values
fragment outside size 1500
! Here fragment database is limited to  a maximum size of 1500, a
!maximum chain length of 45, and a wait time of 60 seconds - to match typical IDS's
fragment chain 45 outside
fragment outside timeout 60
```

Some of the unique features to data center firewall are relaxed xlate or translate timeouts. They are more relaxed on the inside firewall. This provides more simplified access from internal users to the server resources such as fileshares, applications and backups. DNS inspection needs to be tweaked in our setup; DNS configuration for BIND named is given latter to support this.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

A little bit on eDNS support and the firewall. In this design UNIX servers run DNS for our domain yourdomain.com, the DMZ network is where our public facing DNS servers live. DNS queries by clients go to our internal DNS servers in the datacenter behind the transparent firewall. The DNS exchange between servers in data center and servers in DMZ will cross the transparent firewall. Therefore an optimized 768 byte eDNS queries will be most suitable in reducing the need for TCP DNS for queries larger than 512 bytes. On analyzing DNS queries in a production environment, I had noticed DNS data of 580 bytes are very common today due to many new long domain names (Asian domain names), MX records, TXT records, SPF records, domainkey records. eDNS RFC can be obtained from http://www.faqs.org/rfcs/rfc2671.html , it is support by bind named 9.2 or better. I would recommend that you analyze and review eDNS in your environment. In this example, I have chosen 768 bytes eDNS UDP packets allowing for enough room and thus reducing DNS TCP transactions across this firewall.

4.1.b Defining simplifying and maintaining the Firewall rule base.

As mentioned before, do take advantage of rule-sets that can be bundled together without compromising security or performance. For example, port 443 and port 80 can be defined in one service as an object-group in PIX, if your policy allows port 80 and 443 from say "Wireless clients." In the example shown below, the customer's policy allowed port 80, 443 and SSH from wireless network in the "outside" to any server in the "data center."

```
FIREWALL# sh object-group
object-group network n_Wireless-Public
  description: Wireless-Public-10.4
  network-object 10.4.0.0 255.255.0.0
object-group network n_PROXY
  description: Proxy servers
  network-object XX.YY.8.0 255.255.255.128
object-group service s_Wireless-Public tcp-udp
  description: Wireless-Public-allowed-services
  port-object eq www
  port-object eq 443
  port-object eq 22
object-group service s_UNPRIV tcp-udp
  description: Unprivileged-ports
  port-object range 1023 65535
object-group service s_PROXY tcp
  description: Proxy server
  port-object eq 3128
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
FIREWALL# sh access-list Wireless-Public
access-list Wireless-Public; 8 elements
access-list Wireless-Public line 1 permit tcp object-group n_Wireless-Public object-group s_UNPRIV any
object-group n_PROXY object-group s_PROXY
access-list Wireless-Public line 1 permit tcp 10.4.0.0 255.255.0.0 range 1023 65535 XX.YY.8.0
255.255.255.128 eq www (hitcnt=93002)
access-list Wireless-Public line 1 permit tcp object-group n_Wireless-Public object-group s_UNPRIV any
object-group n_SERVERS object-group s_Wireless-Public
access-list Wireless-Public line 1 permit tcp 10.4.0.0 255.255.0.0 range 1023 65535 10.30.0 255.255.0.0
eq www (hitcnt=30377006)
access-list Wireless-Public line 1 permit tcp 10.4.0.0 255.255.0.0 range 1023 65535 10.30.0.0 255.255.0.0
eq https (hitcnt=2057091)
access-list Wireless-Public line 1 permit tcp 10.4.0.0 255.255.0.0 range 1023 65535 10.30.0.0 255.255.0.0
eq ssh (hitcnt=0)
FIREWALL# show cpu usage
CPU utilization for 5 seconds = 23%; 1 minute: 25%; 5 minutes: 19%
FIREWALL  # show fragment outside
Interface:outside
Size:1500, Chain:45, Timeout:60
Queue:1060, Assemble:809, Fail:0, Overflow:0
FIREWALL# sh xlate count
1141 in use, 4259 most used
FIREWALL# sh conn count
800 in use, 3642 most used
```

When you review the ACL hit-counts, there is a little bit of a problem, which you will see. The port 22 traffic has never been used (hitcnt=0) by "Wireless clients", is this rule necessary? Is it time to review the policy. How about Windows servers we saw in the mix 10.30.8.0/22 do they run this service? The Cisco PIX command "show access-list" is very useful in verifying the rules. Review your access lists hit counts regularly. Every 6 months, you can do *"clear access-list counters"* command to reset the counters so you can start viewing the counters that were sometimes entered as temporary rules and were never taken out.

In PIX firewall rule base are inspected and enforced in a sequential data structure. It is very important that you inspect your rules carefully to improve performance and to remove the rules that are not being used anymore. You see in the above example, the rules for proxy are declared before the rules for port 80 and 443 on the serverfarm. However on reviewing the hit counts, it looks like the prosy servers were used 93002 times whereas port 80 traffic hit 30377006, do we need to move this rule up? Does some port numbers in some object-groups needs to be eliminated or reviewed?

These are some process questions, you need to leave with the client so the client can successfully maintain operation of the firewall.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Firewall CPU usage is another one you need to watch. Current CPU on this firewall is reasonable and under control.

High throughput firewalls can run in CPU usage of 30 to 40% without affecting traffic. You need to ensure your HP Openview or other network monitoring tools have threshold set to view the CPU usage on the firewall.

Another important monitoring task is fragmentation. Fragmentation monitoring is a dreaded firewall administrator's job. In the shown example the "outside" interfaces fragment database has the following

- ⇨ A database size limit of 1500 packets. (configured[7])
- ⇨ The chain length limit of 45 fragments. (configured)
- ⇨ A timeout of 60 seconds. (configured)
- ⇨ 1060 packets is currently awaiting re-assembly. (run-time value)
- ⇨ 809 packets has been fully reassembled. (run-time value)
- ⇨ No failure. (not bad ;) day for firwall admin)
- ⇨ No overflow. (very happy ☺ firewall admin)

The current xlate and conn count also are very helpful numbers to see. Xlate shows the number of translations 1141 current of which maximum value of 4259 seen. The "show conn count" shows all active connections, even those that were not translated, or NATed. This is also a useful number. The commands such as "show xlate detail" provide you with more thorough information about the NAT and translation states. Some more advanced options such as xlate detail are show below:

```
FIREWALL# show xlate detail
3 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
     o - outside, r - portmap, s - static
TCP PAT from inside:10.30.1.25/1039 to outside:XX.YY.239.1/1024 flags ri
UDP PAT from inside:10.20.1.15/1028 to outside:XX.YY.239.3/1024 flags ri
ICMP PAT from inside:10.30.1.25/305 to outside:XX.YY.239.1/0 flags ri
```

The first entry is a TCP NAT for host 10.30.1.25, port 1039 on the inside network to host XX.YY.239.1, 1024 on the outside network. The flag "r" denotes the translation is a NAT port. The flag "i" denotes that the translation applies to the inside address-port.
The second entry is a UDP NAT for host 10.20.1.15, port 1028 on the inside network to host XX.YY.239.3, port 1024 on the outside network. The flags "ri" as indicated before show NAT and translation is from inside address-port.

[7] These are also called design-time variables as they are done at configuration. The run-time variables are more "read-only" for output.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

The third entry is an ICMP Port Address Translation for host 10.30.1.25, ICMP id 305 on the inside network to host 192.150.49.1, ICMP id 0 on the outside network. The flags "ri" as indicated before show NAT and translation is from inside address-port.

Many of these monitoring can be done by HP Openview or simple opensource tools using SNMP. In MRTG, you can watch CPU usage and connection count using the variable

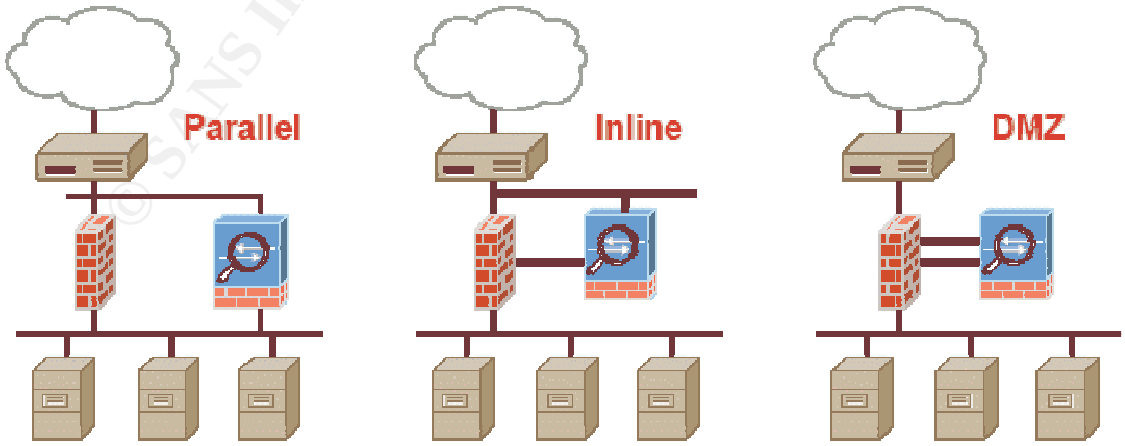
Target[firewall.cpu]: 1.3.6.1.4.1.9.9.109.1.1.1.1.3.1&1.3.6.1.4.1.9.9.109.1.1.1.1.5.1:mysecretsnmp@firewall

Target[firewall.conn]: enterprises.9.9.147.1.2.2.2.1.5.40.6&enterprises.9.9.147.1.2.2.2.1.5.40.7:mysecrectsnmp@firewall

The most important takeaway is that firewall, once configures cannot be left unattended. It is an integral part of network security to monitor the firewall. Sudden increase in "connection count" for example can show possibility of inside compromise or outside DOS attack. Watch these settings over a reasonable cycle of business operations and then you should set thresholds in HP Openview or other network monitoring products to be alerted for out of the window changes.

4.3 VPN Placement - think outside the "bun"

Cisco has VPN placement considerations divided into three categories, introduced by Pete Davis, VPN prodcut manager at Cisco. Most vendors recommend a deployment called "Parallel" so a user can bypass the Perimeter firewall and end up in a segment like any user on the LAN. Compare the pictures shown below from Cisco's documentation:



© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Parallel design comes with significant risks, some of them detailed below

1. Unmanaged home machine being used as a VPN client with possible virus / malware
2. VPN concentrator itself is unprotected from being attacked (e.g., group password guessing or shared key guessing attacks, Fingerprinting, DOS attacks)
3. Possible split tunneling by the remote user who may be used as a bounce node for attacking the local LAN or serverfarm.

The "Inline" option has its benefits as well. However we still leave the VPN server or VPN concentrator itself exposed to the internet. One of my favorite options is the DMZ options, although I have introduced some tweaks to it.

DMZ option provides a very good compromise. In Pete's example, VPN concentrator can be in a "one-legged" deployment where the incoming users are seen as DMZ users, a separate category from internal users. Why? It is because VPN is another perimeter or entry point to the network; we need to protect this entry point without hampering the need for mobility for the user.[8]

The recommended design in this paper is actually a modified version of the DMZ design. A single legged VPN deployment has some limitations, some of them are (a) routing trouble with single leg deployment (b) IDS seeing two types of traffic making tuning very difficult, (c) throughput of one legged deployment is less (usually less of a concern) . In brief, a single legged deployment is less flexible. The design shown below however provides more flexibility. DMZ interface on the firewall can be controlled for traffic. Users can be dropped in the "Inside" zone, giving them like LAN experience. We can still have "layer 7" inspection on the VPN outgoing interface with IDS and/or IPS. Auditing and maintaining the VPN server is also flexible.

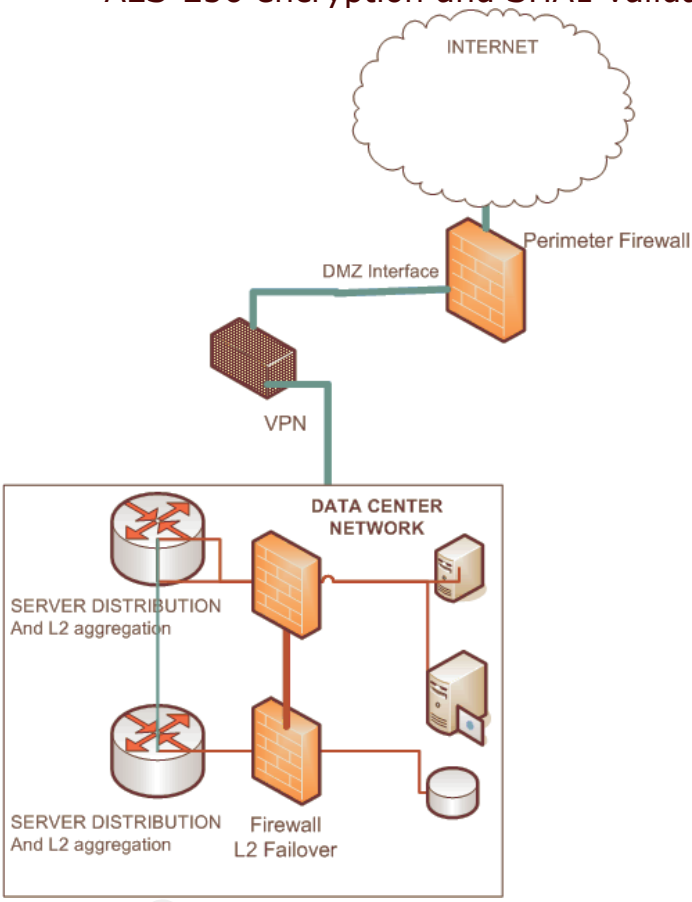
Use your vendor's VPN deployment guide, but don't assume anything. Ask some relevant questions. Here is a good collections of them

1. Does your VPN support flexible authentication and authorization (LDAP/ RADIUS / AD Policy)?
2. What routing protocols are supported by VPN or is static routing required / recommended?
3. Does your VPN support clientless or equivalent SSL VPN?

[8] When blaster worm attacked large networks in the US, many of the corporate networks had blocked Microsoft SMB based protocols, however roaming VPN users came in to cause blaster havoc to the LAN

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

4. Is it possible to restrict / disable split tunneling? (even for local LAN access at the remote user end and DNS queries)
5. What type of failover or redundancy setup is supported (Active / Active or Active/Standby). Is layer 2 adjacency required?
6. Does your VPN have NAC (Network Admission Control) policy by client workstation posture assessment (A/V up-to-date, AD policy, services running, KSL Keystroke Logger detection)
7. Does your VPN support behind NAT users – IPSEC NAT-T or UDP NAT IPSEC payload?
8. Does your VPN client support encryption enforcement (SSL VPN example – Cipher requirements: require RSA key exchange, AES-256 encryption and SHA1 validation under TLSv1 ?)



VPN recommended setup.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

4.3.a VPN operation mode encryption and consider SSLVPN user-land / non-administrative operation of VPN

A brief look at your tunneling and operational options with VPNs.

Tunneling Protocol	**Encryption algorithm**	**Authentication**	**Verification or Integrity**
1. IPSEC [9] 2. L2TP + IPSEC 3. SSL based	• DES • 3-DES • AES • RC4	Digital Certificate (RSA) Pre-shared key	HMAC-MD5 HMAC-SHA1

Most VPN vendors support many of these options. Most VPN vendors are leaning towards SSL VPN where they can provide same amount of encryption (AES-256) with Digital Certificate (Root CA verification instead of client certificates or shared key / pass phrase) and still provide equivalent message integrity checking with SSL. The biggest attraction for SSL based VPN is the ability for a "clientless" VPN solution. It also can virtually work much like https allowing the user to connect from highly restricted access locations even through a proxy.

While the solution is convenient for the clients to come to your network from anywhere with any PC, it poses a bigger risk mitigation at your end[10]. Consider unmanaged PCs that can now access your network – even PCs from any internet café. Before you deploy a clientless or SSL VPN solution consider the following

1. Does your roaming user need virtual access to office from anywhere and any PC?
2. Is it possible to develop a Citrix type access to a managed machine once the client has terminated?
3. Is it possible for the SSL VPN client to require certain type of encryption and verification – For e.g., if you use default Internet Explorer as your SSL termination point or use windows API to run SSL (or https) you are limited to RC4 (stream cipher) for encryption and MD5 for MAC (Message Authentication Code) with 128-bit encryption. However stronger block ciphers AES with SHA-1 for MAC and 256 bit encryption is possible with SSL.

One of the best business questionnaire for SSL VPN is at Aventail's website:

[9] IPSEC Transport mode is considered here for terminating roaming clients here.
[10] Remember every solution or service needs to be brought into security context as we discussed earlier.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

http://www.aventail.com/why_aventail/why_ssl_vpn/ssl_vpn_buyers_guide.asp

5. PUBLIC SERVICES DESIGN – DMZ

"You can't consider the problem of defense without first understanding the problem of attack." - Doug Tygar, a professor of computer science and information management at UC Berkeley

5.1 Define public facing services : DNS, WEB and MAIL.

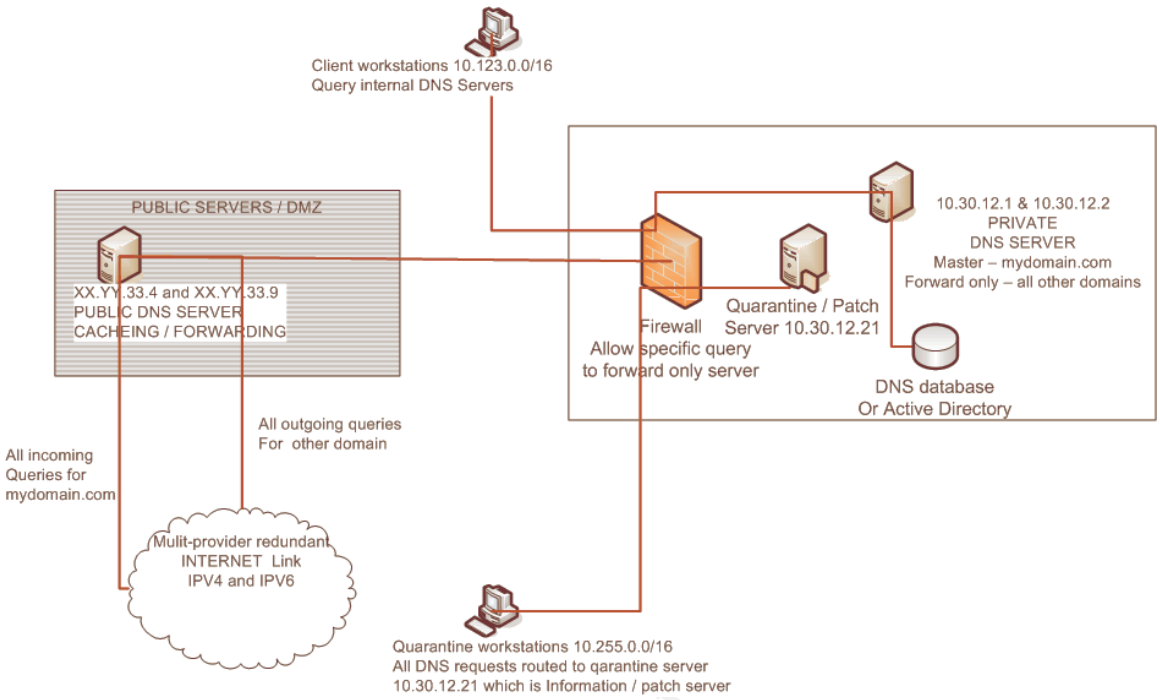
5.1.a Split DNS and firewall protection. DNS protected from local DNS (AD or other database) eDNS implementation. Firewall planning.

DNS is a very important resource in your network. Two important communication principles to keep in mind when you design your internal network and public facing network (traditional term DMZ).

1. All servers in internal network will be proxied for any communications to the external network (e.g., patching of servers, vendor upgrades, collaboration with outside companies)
2. All communications incoming from external network (unstrusted) will terminate at the DMZ before being "reverse" proxied to be served from the internal or serverfarm network.

You will see this message (2) prevalent in this design later as well. However in some cases it is not possible to enforce these two requirements, for e.g., business partners exchange calendaring system or Lotus server to server trust. Every exception needs to be documented and audited. Here we pursue a "split" DNS solution that will show some robust design in security, while still providing flexibility to clients and system administrators internally. Walk through the DNS configuration notes to see how this is accomplished.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.




```
##############EXAMPLE OF PUBLIC DNS SERVER CONFIGRUATION#####
################ FOR BIND 9.* FROM OPENSOURCE ISC.ORG #############
#### Run NAMED unprivileged and chroot with
#### /usr/sbin/named –t /var/nameroot –u named
### create device nodes for doing null, random and zero functions for named
#### mkdir /var/nameroot/dev
#### mknod /var/nameroot/dev/null c 1 3
#### mknod /var/nameroot/dev/random c 1 8
#### mknod /var/nameroot/dev/zero c 1 5
#### remember to modify syslogd to Unix type logging can be local at /dev/log
#### syslogd –a /var/nameroot/dev/log

acl "mynet" {
   XX.YY.0.0/16;
   10.0.0.0/8;
};
acl “ispparter” {
// This is our ISP’s nameservers acting as slaves.  Make sure he
// does not allow zone transfer from outside – verify regularly.
   RR.SS.TT.0/24;
}
options {
// We have already been chrooted to /var/security/named
   directory "/namedb";
   pid-file "/namedb/named.pid";
   check-names master ignore;
   check-names slave ignore;
   check-names response ignore;
   allow-query { any; };
//
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
   allow-recursion {
//This is to avoid any unknown ip trying to use recursion. more useful on the DMZ server than here.
     127.0.0.1/32;
     "mynet";
   };
// Who wil get our transfered data
   allow-transfer { "isppartner"; };
// Ha dont forget to hide our version info
   version "*";
};
// Dont forget what to do with logging.
logging {
   category default { default_syslog; default_debug; };
   category lame-servers { null; };
   category notify { default_syslog; };
   category queries { null; };
   category update { null; };
   category xfer-out { null; };
   category security { null; };
};

// RNDC Stuff for local access only default port is 953
include "/etc/rndc.key";
controls {
   inet 127.0.0.1 port 953 allow { localhost; } keys { rndc-key; };
};
// Standard zones
//
zone "." {
      type hint;
// You can do “dig @a.root-servers.net . NS > root.hint”
      file "standard/root.hint";
};
// Declare delegation-only zones
// a zone which has been declared delegation-only will be effectively
//limited to containing NS RRs for subdomains
zone "com" {
      type delegation-only;
};
zone "net" {
      type delegation-only;
};
//Master domain
zone "mydomain.com" {
      type slave;
      file "slave/mydomain.com";
      check-names ignore;
      masters { 10.30.12.1; 10..30.12.2; };
};
zone "mydomain2.com" {
      type slave;
      file "slave/mydomain2.com";
      check-names ignore;
      masters { 10.30.12.1; 10..30.12.2; };
};
zone "YY.XX.in-addr.arpa" {
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
        type slave;
        file "slave/YY.XX.in-addr.arpa";
// This is to avoid complains about _ underscore zones from new environments
// and Active Directory environments.
        check-names ignore;
        masters { 10.30.12.1; 10..30.12.2; };
};
```

############# END OF FILE #######################

```
################EXAMPLE PRIVATE DNS SERVER CONFIGURATION ######
################ FOR BIND 9.* FROM OPENSOURCE ISC.ORG #############
# use the same principles shown above for chroot environment ####
acl "mynet" {
    XX.YY.0.0/16;
    10.0.0.0/8;
};
acl "quarantine" {
    10.255.0.0/16;
};
options {
// We have already been chrooted to /var/security/named
    directory "/namedb";
    pid-file "/namedb/named.pid";
    check-names master ignore;
    check-names slave ignore;
    check-names response ignore;
    forward only;
// Forward information to our DMZ servers dont resolve
    forwarders  { XX.YY.33.4; XX.YY.33.18; };
// This is very nice for firewall configuration, you will always see source queries coming from this port
    query-source address * port 36000;
    allow-query { any; };
//
    allow-recursion {
//This is to avoid any unknown ip trying to use recursion. more useful on the DMZ server than here.
      127.0.0.1/32;
      "mynet";
    };
// Who wil get our transfered data
    allow-transfer { "nameslaves"; };
// Ha dont forget to hide our version info
    version "*";
//Who to notify in change of zones.
    also-notify {
            XX.YY.33.4;
            XX.YY.33.18;
    };
// notify uses a different source port ?  - this is optional
    notify-source * port 36001;
// Notofy only explicit servers
    notify explicit;
// This is very cool in noting EDNS behavior.
//You can limit EDNS size on PIX firewall - this is handy to verify who is using DNS service
// command line syntax on pix 6.3 or better firewall
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
// fixup protocol dns maximum-length 768
   edns-udp-size 768;
};
// Dont forget what to do with logging.
logging {
   category default { default_syslog; default_debug; };
   category lame-servers { null; };
   category notify { default_syslog; };
   category queries { null; };
   category update { null; };
   category xfer-out { null; };
   category security { null; };
};

// RNDC Stuff for local access only default port is 953
include "/etc/rndc.key";
controls {
   inet 127.0.0.1 port 953 allow { localhost; } keys { rndc-key; };
};
// Quarnatine users limit what they can access
view "quarantine" {
  match-clients { "quarantine"; };
  recursion yes;
zone "." {
            type "master";
            file "fake/sinkeme.zone";
/*
; A simple zone file below will catch all DNS requests from this host and forward it
; to our quarantine server;sample zone file sinkme.zone
$TTL 600
@       IN      SOA     reserved. postmaster.mydomain.com.  (
                        2007021507  ; Serial
                        3600        ; Refresh
                        900         ; Retry
                        3600000     ; Expire
                        3600 )      ; Minimum
                NS      reserved.
$ORIGIN .
; currently guestaccess server does proxying when necessary
guestaccess             A       10.30.233.4
; Widlcard everything to go to net registration or quarantine information server
*                       A       10.30.12.21
$ORIGIN reserved.
; currently guestaccess server does proxying when necessary
guestaccess             A       10.30.233.4
; Widlcard everything to go to net registration or quarantine information server
*                       A       10.30.12.21
$ORIGIN mydomain.com.
; currently guestaccess server does proxying when necessary
guestaccess             A       10.30.233.4
; Widlcard everything to go to net registration or quarantine information server
*                       A       10.30.12.21
; END OF FILE.
*/
};
};
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
//Everybody else
view "global" {

   match-clients { "any"; };
   zone "localhost" IN {
      type master;
      file "localhost.zone";
      allow-update { none; };
   };

   zone "0.0.127.in-addr.arpa" IN {
      type master;
      file "named.local";
      allow-update { none; };
   };

   zone "mydomain.com" IN {
      type master;
      file "master/mydomain.com";

   };

   zone "mydomain2.com" in {
      type master;
      file "slave/mydomain2.com";
      masters { 10.30.4.27; 10.30.4.9; };
   };
// End of global view.
};
```

5.1.b Public WEB and secure services through reverse proxy and ssl-reverse proxy – apache

When I address the issues of restricting incoming communications to internal servers, some of my clients have a simple question "How do I run any webserver that provides public content? e.g., www.mydomain.com ? Reverse proxy is the short answer. I see so few clients taking advantage of reverse proxying all their servers. This is a grand benefit for audited and defining your "public" data services.

It is also possible to run SSL offloading with reverse proxies. This is also a major benefit. A sample configuration of an SSL reverse proxy, using apache is shown below. It is very simple and provides an SSL / https front end to client and a non encrypted service on the back end. Running reverse proxy without SSL configuration can also be easily derived from this example.

```
#### /etc/httpd/conf.d/ssl.conf EXAMPLE with comments #########
<VirtualHost _default_:443>
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
ServerName mysecure.thisdomain.com
# A fake directory for
DocumentRoot /var/www/empty
# Location /e/ we don't want to proxy – this can be used for server-status
ProxyPass /server-status/  !
#Another Direcotry we don't want to proxy
ProxyPass /locals/  !
# We will proxy / or root request or our main server
ProxyPass / http://server-real.thisdomain.com/
# Reverse proxy ensures reverse path is maintained on HTTP replies
ProxyPassReverse /  http://server-real.thisdomain.com/
# We will proxy Application under directory /appx to APP server in inside zone
ProxyPass /appx http://appx-real.thisdomain.com/
# Reverse proxy ensures reverse path is maintained on HTTP replies
ProxyPassReverse /appx  http://appx-real.thisdomain.com/
#Cache images if we can
CacheRoot /var/www/cache
CacheSize 1000000
# Simpify proxy operation to avoid dead connections of HTTP 1.1
SetEnv force-proxy-request-1.0 1
SetEnv proxy-nokeepalive 1
#Gather logs to our server loggerhead
ErrorLog syslog:local5
LogLevel warn
#SSL for the outside and non-SSL on the inside
SSLEngine on
#Dont accept  0 encryption of < 128 bit encryption equivalent of MEDIUM
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
SSLCertificateFile /etc/httpd/conf/ mysecure.thisdomain.com.crt
SSLCertificateKeyFile /etc/httpd/conf/ mysecure.thisdomain.com.key
# Good old MSIE dead or unclean shutdowns
SetEnvIf User-Agent ".*MSIE.*" \
        nokeepalive ssl-unclean-shutdown \
        downgrade-1.0 force-response-1.0
CustomLog logs/ssl_request_log \
         "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
```

5.1.c MAIL service defined and protected from local groupware.

Many times email system on a LAN is really a "groupware" solution providing collaboration in calendaring, tasks, resources planning (conference room etc.) and workflow. It happens to be more than just email, supported by large groupware products such as Microsoft Exchange, IBM Lotus Notes or Novell Groupwise.

However this collaboration requires software that has very complex functions and thus has potential vulnerabilities that can be exploited remotely. In most cases, these special functions are only needed by the client's own employees – may even be useful only when the employees are in the local LAN. There is plenty of argument to

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

protect your valuable asset such as groupware system from the internet.

The mailservers in DMZ in my design actually are really MTA (Mail Transfer Agents), there are many benefits to using this model, instead of throwing your Lotus Notes or Exchange server in DMZ network. The biggest reason would be isolate your groupware application from the internet. There are very few cases where you might need collaboration with business partners in groupware. This has to be considered carefully, as it becomes another "weak point" in your perimeter for an attacker to enter in from your business partner.

The following crucial work can be done using DMZ MTA scanner

1. Run a mail spooling system in unprivileged spool only mode (both Sendmail and Postfix can be configured to run as an MTA with low or no system level privileges even within a chroot environment)
2. Add multiple filters to verify incoming email. Milters from www.milter.org and multiple filters in Postfix can be used to scan for viruses, spam and phishing / scams. Robust commercial products such as Sophos www.sophos.com (software) and Ironport www.ironport.com (hardware / blackbox) can be used to scan and enforce your policies for incoming / outgoing email. Design a scanner that uses multiple Anti-Virus software vendor products that is kept up to date.
3. Don't forget to scan your outgoing email. Scanning your outgoing email is also crucial. Have high alert for local users who might be sending out virus. It is recommended that you log and quarantine viruses that have originated from local machine so you can thoroughly investigate and lock down compromised machines in your LAN.
4. Enforce your email policy. Your policy for email needs be enforced for your employees. If a disclaimer is required, many software such as milters – provide tools to add disclaimers to email originating from your domain. If your email policy denies exe files from being exchanged via email – it is good to enhance your filtering products to do this in practice.
5. Always verify sender and recipient with whatever methods are possible. Your end users will trust email from ceo@mycompany.com actually came from the CEO. It is your duty to verify senders from outside cannot fake your internal domains. LDAP database to virtual user database can be synched with some simple scripts. Sendmail and Postfix have plugins to do so, take advantage of these features.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Remember this design is to provide convenience for local user for groupware application and collaboration, but still protect the resources (servers) from the external attacker or intruder. Simplified calendar collaboration and workflow collaboration is a necessity in today's internet based economy. It is important that you keep your perimeter email entry point another "checkpoint." Data that enters as an email is also another source of attack. Securing email is critical for your perimeter security.

5.2 IPS/IDS, Probes and Syslog servers Oh my!

5.2.a Placement considerations of IPS, IDS, Probes.

Today the number of inline devices to your WAN link is growing in number and complexity. This continues to make network and security administrator job more difficult in troubleshooting and management. A number of inline devices today include

1. IPS as inline packet inspection – e.g., Tippingpoint Unity one, Greenborder and Sourcefire.
2. Light probes to mirror traffic for IDS, Sniffer – Fluke Probe, Snort sensors.
3. Inline traffic shaper – e.g., Packeteer and NetEqualizer

If you require many of these devices inline, then it is time to review their role in your network carefully. Some principles that will help narrow down locations for these devices.

- ⇨ Choose a device that has multiple interface pairs that can be controlled by different profiles or rules
- ⇨ Choose a device or options that can "fail closed" so you are not dependant on it
- ⇨ Design your IP traffic so it does not cross multiple sections of the same IPS/Probe
- ⇨ Use passive light splitters for IDS, Sniffers and traffic analyzer.
- ⇨ Enhance the use of Cisco's Netflow type analysis tools that don't need to be inline.
- ⇨ Ensure remote logging of the device is possible.

Snort is very reliable IDS software that can be easily installed on a UNIX box and placed in your DMZ. Consider sending the log data via syslog to two locations that are in two different subnets and possibly

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

two different security zones (one in DMZ itself and the other in SERVERFARM security zone).

If you choose a packaged IPS and traffic shaping inline device, ensure logging is possible and monitoring of this device via remote syslog. This is very helpful, as you can send the logging data to server(s) which can be used to analyze data and troubleshoot problems. Every inline device comes with additional hours of maintenance and monitoring. Offline devices, like IDS, also need to be managed and monitored to get value out of their presence.

Many times it is useful to use tarpit such as Labrea tarpit from labrea.sourceforge.net can be very powerful ways to get alerts about systems in your network that are accessing a dedicated "dark space" network. Here is a brief example, suppose your LAN network is 10.0.0.0/8 as in our design and your public IP is XX.YY.0.0/16 ; you can pick one (or two) subnet(s) such as XX.YY.255.0/24 (and XX.YY.0.0/24) [11]and create a "dark space" IP. The ideal location for the tarpit is outside the firewall in its own zone. Labrea tarpit is not designed to operate with any layer 3 functionality, so static routes to the tarpit server will not work. However Labrea will automatically arp for the full subnet in this case XX.YY.255.0/24.

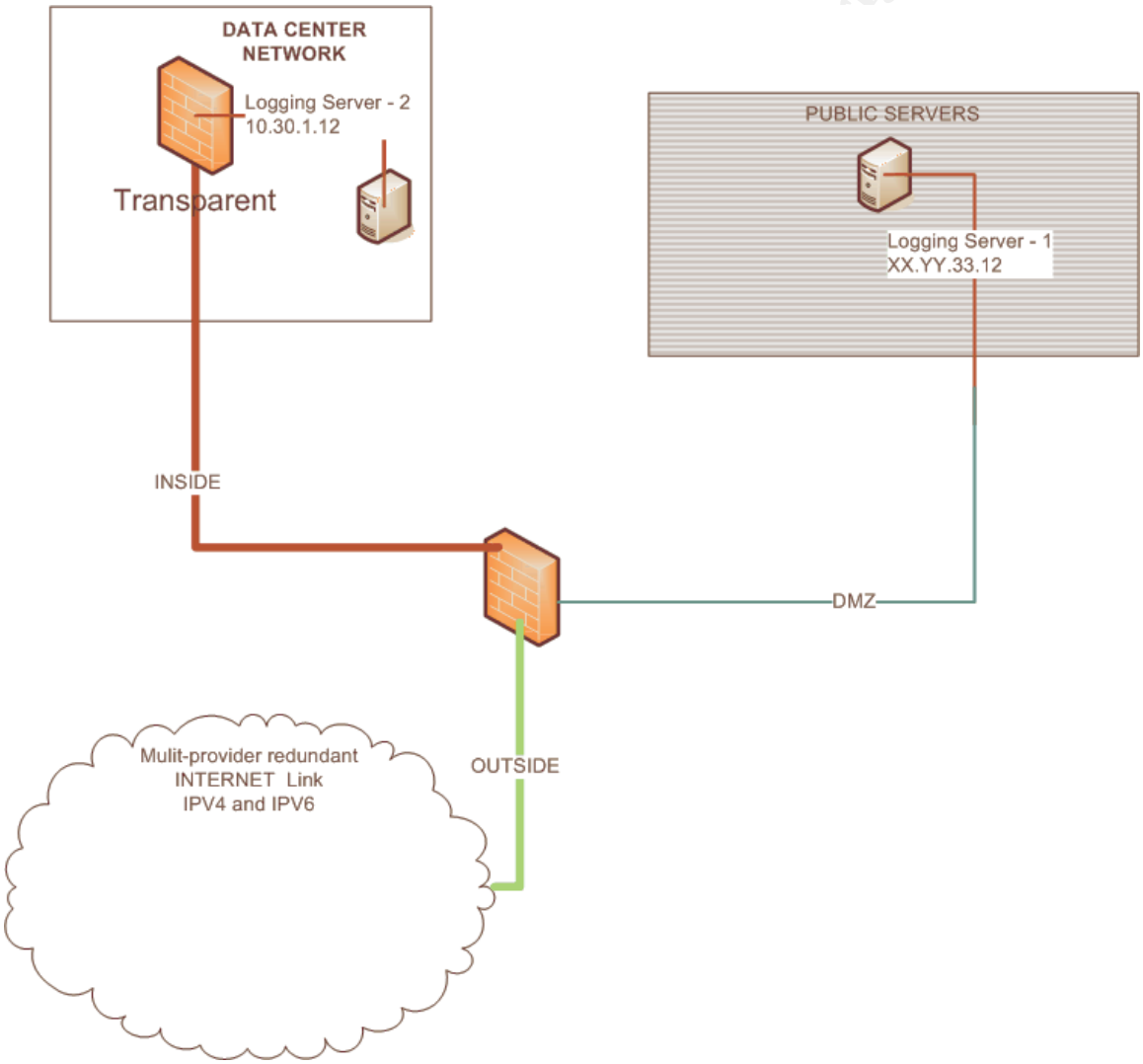
```
#!/bin/bash
! Here is start LaBrea script that will run it in foreground mode
/usr/local/sbin/labrea --switch-safe --verbose -v  --no-resp-excluded-ports --log-bandwidth \
--foreground --log-to-stdout --device eth1 -n XX.YY.255.0/24  --max-rate 2000000 \
--init-file /etc/labrea.conf -z –q

# snort.conf to watch for LAN people contacting your dark space.
output alert_syslog: LOG_AUTH LOG_ALERT
# Ignore our own IP
pass ip XX.YY.255.31 any -> any any
pass ip any any -> XX.YY.255.31 any
# Ignore our scanners
pass ip XX.YY.107.1 any -> any
# Alert anybody from our public IP reaching this dark space
alert ip XX.YY.0.0/16 any -> XX.YY.0.0/16 any \
(msg: Local Public Networks trying to reach darkspace contacting tarpit; sid: 23213;)
# Alert anybody using our private IP reaching this dark space.
alert ip 10.0.0.0/8 any -> XX.YY.0.0/16 any \
(msg: Local Private Networks trying to reach darkspace contacting tarpit; sid: 19213;)

# Run snort with syslog
/usr/loca/bin/snort -l /var/snort/log/ -D -c /etc/snort/snort.conf
```

[11] Typical remote scanners either start at your lowest IP or highest IP address to start the scan, you can possibly keep them busy in the "tarpit"

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

5.2.b. Logging servers and tracking

It is critical to decide the location of your logging servers. The typical debate has been before the DMZ or inside zone of the firewall. In this design, I recommend two syslog servers one in DMZ and one in INSIDE zone of the firewall. Your logging server is a critical audit trail, it is important that you gather and preserve this data. In this design I have recommended install of two UNIX servers, one in the UNIX SERVERFARM (10.30.1.12) and one in DMZ ZONE (XX.YY.33.12).



The server design itself is also critical. It is good to design a special partition of the hard drive for output files. In this example, I have created a very large partition called "/sensitive" that is created locally. You can choose an iSCSI / NFS or external drives for this partition as well. A sample syslog.conf for syslogd in UNIX is shown

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

below. It is designed according the requirements and the planning done in the earlier chapters.

```
#reduce console noise
*.err;ftp,local0,local1,local2,local3,local4,local5,local6,local7.none          /dev/console
kern.debug;auth.notice;authpriv.none;mail.crit        /dev/console

# Get some of these to root if logged in
*.emerg                                  root

# /sensitive is a safe asset consider mount a seperate device drive
# partition with "append only" file system
auth,authpriv,cron,kern,lpr,mail,ftp,local0,local1.none,user.none      /sensitive/messages
daemon,local2,local3,local4,local5,local6,local7.none        /sensitive/message
s
kern.debug,syslog.info                          /sensitive/messages
auth,syslog.notice                        /sensitive/messages
auth.info                              /senstive/authlog

#These are logs we are collecting remotely
authpriv.*                          /senstive/secure
cron.*                             /sensitive/cronlog
daemon.*                                /senstive/daemon
lpr.*                             /senstive/lpd.log
mail.*                              /senstive/maillog
ftp.*                               /senstive/ips.log
local0.*                              /senstive/vpn.log
local1.*                              /senstive/dhcpd.log
local2.*                              /senstive/core-network.log
local3.*                              /senstive/access-network.log
local4.*                              /senstive/pix.log
local5.*                              /senstive/ssl-offloader.log
local7.*                              /senstive/wireless.log
local6.*                              /senstive/server_status.log
user.*                                /senstive/nac.log
```

6. SECURING YOUR LAYER 2 HOSTS & NETWORKS

"More people are killed every year by pigs than by sharks, which shows you how good we are at evaluating risk." -Bruce Schneier

6.1 Switch and radius configuration and 802.1x design – in Cisco IOS.

IEEE 802.1x is fairly new Ethernet standard which allows for a user to be identified before allowed to pass any traffic. The identification can be by MAC Address or by EAPOL (Extended

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Authentication Protocol Over LAN). I will demonstrate the use of Cisco IOS based switches to authenticate a user using a backend directory (such as LDAP). One can also assign a VLAN segment for a particular user depending on his/her department as derived from the backend directory.

There is also a lot special options for mac address based authentication in Cisco IOS switches, which we will explore later. The requirements for this is a basic RADIUS server and an LDAP server. RADIUS server does the authentication and assignment of VLAN to Ciscco IOS switch. I have used freeradius from www.freeradius.org as the RADIUS server. LDAP server is just a backend database that is very extensible, we can use LDAP object-group options to assign VLAN's. In this example Novell LDAP on Suse Linux is used as the LDAP server.

Freeradius setup:
Download freeradius www.freeradius.org

```
#These options are relevant if you want to support MS-CHAPv2 authentication – native windows
# for a backend Novell LDAP directory. "edir" option sets up support for MSCHAP on radius server.
prompt>tar zxvf freeradius.X.Y.Y.tar.gz && cd freeradius.X.Y.Z
#disable shared keeps dependencies out of the picture, edir option is to support novell directory
# prefix is where you want to install the program
prompt>./configure –disable-shared –with-edir –enable-ldtl-install –prefix=/usr/local/eap-novell/  \
&& make && make install
# If all goes well, do a basic, run a debug mode to see if install went well.
prompt>/usr/local/eap-novell/sbin/radiusd –X
#configuration options for /usr/local/eap-novell/etc/raddb/radiusd.conf : LDAP section.
      ldap_finance {
            server = "novellauth.mydomain.com"
            identity = "cn=bigadmin,o=MYCOMPANY"
            password=given0tmepaffwo7d
            basedn = "ou=finance,o=mycompany"
            filter = "(cn=%{User-Name})"
            tls_mode = yes
            port = 636
            dictionary_mapping = ${raddbdir}/ldap.attrmap
            ldap_connections_number = 5
            password_attribute = nspmPassword
            timeout = 4
            timelimit = 3
            net_timeout = 1
      }
#Now authorize section modifications
     authorize {
        preprocess
        chap
        mschap
        suffix
        ldap_finance
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
        eap
    }
    authenticate {
        Auth-Type PAP {
                pap
        }
       Auth-Type LDAP_FIN {
          ldap_finanace
        }
        Auth-Type MS-CHAP {
                mschap
        }
        eap
}
#EOF
#/usr/local/eap-novell/etc/raddb/users
DEFAULT         Auth-Type == LDAP_FIN
                Tunnel-Type = 13,
                Tunnel-Medium-Type = 6,
                Tunnel-Private-Group-Id = 928
# You can add here other LDAP directories or OU or object filters.

#/usr/local/eap-novell/etc/raddb/eap.conf
        eap {
                default_eap_type = peap
                ignore_unknown_eap_types = yes
                md5 {
                }
# Disable leap if you don't need it.
                gtc {
                        auth_type = ldap
                }
                tls {
                        private_key_file = ${raddbdir}/certs/mycompany.com.key
                        certificate_file = ${raddbdir}/certs/mycompany.com.crt
                        CA_file = ${raddbdir}/certs/thawte-server-ca.crt
                        dh_file = ${raddbdir}/certs/dh
                        random_file = ${raddbdir}/certs/random
                }
                ttls {
                        default_eap_type = md5
                }
                peap {
                        default_eap_type = gtc
                }
                mschapv2 {
                }
#EOF eap.conf
```

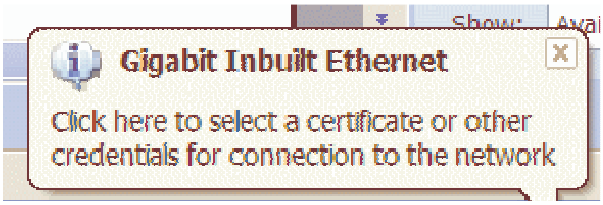
Above radius configuration assign Vlan 928 to clients in ou=finance in directory novellauth.mydomain.com. You can also use ISA radius server and Microsoft A/D backend to achieve the same. This was also tested in the LAB, not detailed in here.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Now going to setting up the switch to authenticate via 802.1x

```
#Switch named CE2 – Customer Edge Layer 2 switch is shown here in configuration.
! Start AAA model  Authorization Authentication Accounting
aaa new-model
! use radius for backend of AAA
aaa authentication dot1x default group radius
aaa authorization network default group radius
!Specify where the radius server will live and the secret key
radius-server host 10.30.1.12 auth-port 1812 acct-port 1813 key sys_control
!This is a very useful feature for your firewall rules, if you have firewall between
! switches and radius server like in our model, you can simplify the firewall rule.
! instead of saying "allow udp from switch-network port range 1023-65535 to radius_server
! port range 1812-1813" , the rule can be "llow udp from switch-network port range 1812-1813 to
! radius-server port range 1812-1813"
radius-server source-ports 1812-1813
! Define a guest access / quarantine vlan for clients who fail authentication or don't have 802.1x supplicant
vlan 2041
 name Guest-Access
! Define finance vlan and other vlans that are designated from above configruation
vlan 928
 name Finance-vlan-at-Large-Bldg-811-South
!Enable 802.1x system auth control so the service is running
dot1x system-auth-control
interface FastEthernet0/48
! The port is 8021x required port
 description DOT1x ports
! This is an access port
 switchport mode access
! 802.1x can be bypassed by mac-address detailed later in exceptions
 dot1x mac-auth-bypass eap
!Allow control of VLAN assignment via 802.1x
 dot1x port-control auto
! If not 802.1x supplicant is available drop them into our Guest Access Vlan 2041
 dot1x guest-vlan 2041
!If 802.1x authentication fails / expires, drop them into our Guest Access Vlan 2041

!where they can be directed to reset password, call helpdesk etc.
 dot1x auth-fail vlan 2041
exit
end
```

When connecting a windows host which has 802.1x native supplicant running, you will see a popup window on the status bar like shown below:



© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

When you click on the bubble, you should see a login window as shown below:

When you pass authentication, you should get the assigned VLAN and status. To verify at the CE2 switch the status of authentication.

```
CE2>sh dot1x int f0/48
Dot1x Info for FastEthernet0/48
-----------------------------------
PAE                    = AUTHENTICATOR
PortControl            = AUTO
ControlDirection       = Both
HostMode               = SINGLE_HOST
ReAuthentication       = Disabled
QuietPeriod            = 60
ServerTimeout          = 30
SuppTimeout            = 30
ReAuthPeriod           = 3600 (Locally configured)
ReAuthMax              = 2
MaxReq                 = 2
TxPeriod               = 30
RateLimitPeriod        = 0
Mac-Auth-Bypass        = Enabled (EAP)
   Inactivity Timeout  = None
Auth-Fail-Vlan         = 2041
Auth-Fail-Max-attempts = 3
Guest-Vlan             = 2041
CE2>sh int f0/48 status
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
Port      Name            Status      Vlan      Duplex  Speed Type
Fa0/48    DOT1x ports     connected   928       a-full  a-100 10/100BaseTX
CE2>
```

So we were able to map user novell-username in directory. Lets take a brief look at the LDAP directory backend

```
-bash-2.05b# ldapsearch -h novellauth –x -bo=mycompany cn=novell-username
# extended LDIF
#
# LDAPv3
# base <o=MYCOMPANY> with scope sub
# filter: cn=novell-username
# requesting: ALL
#
# novell-username, FINANCE, DEPT, MYCOMPANY
dn: cn=novell-username,ou=FINANCE,ou=DEPT,o=MYCOMPANY
preferredSurname: Test Account
preferredInitials: S
preferredGivenName: Vijay
mail: novell-username@MYCOMPANY.COM
uid: novell-username
initials: S
givenName: Vijay
sn: Sarvepalli
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: Person
objectClass: ndsLoginProperties
objectClass: Top
cn: novell-username

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

If you look at the DN (Distinguished Name) of this user, you can see the OU assignment for finance. He is now able to drop into a VLan 928 which is mapped into a VRF RED and has been limited to access to resources and isolated from other VRF networks. In a small table, this is shown below

Username	Department	Vlan	VRF
Novell-username	Finance : source LDAP dn: cn=novell-username,ou=FINANCE,ou=DEPT,o=MYCOMPANY	928: Finance-vlan Source RADIUS	RED: Assignment by VRF definition

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

You can also define other LDAP directories and other mechanisms for authentication through radius. People who fail authentication after default number of trails (3 in Cisco's dot1x configuration) will be dropped into guest vlan 2041. In this vlan, you can provide a guest access / quarantine server which runs basic proxy service and web service for providing information about resetting password or calling the helpdesk. Earlier shown DNS named.conf configuration shows ways to use views to redirect quarantine / guest access users to a "bastion host" server which can provide information and access via proxy for patches, updates etc.

This service can further be extended to campus wireless users. WPA2 and 801.1x coupled together with TLS/EAP or PEAP, is very reliable and secure method to permit a user into your network. Radius EAP configuration laid out here. The configuration of radius server in this example was tested by WPA2 enabled clients also successfully. The configuration of Cisco autonomous AP's are not enclosed here.

6.1.a Providing flexibility to your users using REALMS.

We have designed a network that can authenticate and authorize the user to his end point – that is our perimeter. The design does provide greater mobility and flexibility to user, but it limits the user into one department. One of RADIUS server's extensions is the use of REALMS. I will show a little bit on how REALMS can be used to enhance and provide the end user with options of changing his VLAN, if he is authorized.

The users can choose the right VLANS by using a login such as username@DEPARTMENT or username/DEPARTMENT

```
#Define realms recognition //usr/local/eap-novell/etc/raddb/radiusd.conf
        #  Two config options:
        #       format     -  must be 'prefix' or 'suffix'
        #       delimiter  -  must be a single character
        realm suffix {
                format = suffix
                delimiter = "@"
        }
        realm realmslash {
                format = prefix
                delimiter = "/"
        }
        realm realmpercent {
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
                format = suffix
                delimiter = "%"
        }

    realm ntdomain {
        format = prefix
        delimiter = "\\"
        ignore_default = no
        ignore_null = no
    }
#EOF of /usr/local/eap-novell/etc/raddb/radiusd.conf

#/usr/local/eap-novell/etc/raddb/proxy.conf very simple declaration of relams

realm FINANCE {

}
realm NETWORKS {
}
#EOF / usr/local/eap-novell/etc/raddb/proxy.conf

#Configuration in the /usr/local/eap-novell/etc/raddb/users
DEFAULT             Auth-Type == “LDAP_FIN”, Realm == "FINANCE"
                Tunnel-Type = 13,
                Tunnel-Medium-Type = 6,
                Tunnel-Private-Group-Id = 928
DEFAULT             Auth-Type == “LDAP_NET”, Realm == “NETWORKS”
                Tunnel-Type = 13,
                Tunnel-Medium-Type = 6,
                Tunnel-Private-Group-Id = 210
#EOF of  / usr/local/eap-novell/etc/raddb/users
```

The users who has privileges and permissions setup in the LDAP tree to be in both OU=FINANCE and OU=NETWORKS, can now authenticate either as “username/FINANCE” and be dropped into vlan 928 or as “username/NETWORKS” and dropped into vlan 210. This provides greater flexibility for users who are like security analyst or network analyst who needs to be simulate conditions as different users. If you use the native window 802.1x client, the client caches your authentication in a “crypted” form in registry. You have to either manually or with a script remove registry entries that are cached in [HKEY_CURRENT_USER\Software\Microsoft\EAPOL\UserEapInfo]

In the current example user can move between networks, thus move between VRF’s using a REALM. If you are using active directory from Microsoft, you can achieve the same by radius attributes tied to “roles” of user. The radius design is very flexible and extensible, however your management or policy might want to limit use of REALMS.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

6.3 Making exception to the rules – printers, Ethernet enabled devices, guest access, non-dot1x aware clients.

There is increasing use of IP based networks for various purposes. Printing via HP's jetdirect is by far the most popular network based device used. Devices like printers are not 802.1x aware or able to have a supplicant to authenticate and be assigned an appropriate VLAN or network segment. It is always a challenge to address needs of various devices sharing this network. Cisco and other vendors also support MAC address based authentication for these clients. MAC Address of the clients can be dropped into a database and checked for right vlan assignment. Here we have setup a VLAN 1023 as a printer VLAN. The printer VLAN is assigned only for trusted MAC addresses, through a database configuration, a sample text database is shown here. The switch configuration adapted earlier supports MAB (MAC authentication bypass) [12]

```
#/usr/local/eap-novell/etc/raddb.users default auth for the VLAN accept with vlan # 1023
0011434f7580        Auth-Type := Accept
                Tunnel-Type = 13,
                Tunnel-Medium-Type = 6,
                Tunnel-Private-Group-Id = 1023
#EOF Configuration sample
```

.

The process is as follows, a printer/device is plugged in to the network, the device sends ethernet frames. The switch sends EAPOL (EAP Over LAN) messages to the client 3 times. The switch then understands that client cannot understand EAP, so he goes to MAC address based authentication. If you turn on debug on Cisco IOS switch with command "debug dot1x events" you will see messages like

```
02:40:26: dot1x-ev:dot1x_switch_is_dot1x_forwarding_enabled: Forwarding is disabled on Fa0/47
02:40:26: dot1x-ev:Host access is 1 on port FastEthernet0/47
02:40:26: dot1x-ev:Succeeded in setting host access to deny on FastEthernet0/47
02:40:26: dot1x-ev:dot1x_switch_mac_address_notify: MAC 0011.434f.7580 discovered
onFastEthernet0/47(1) consumed by MAB
```

[12] Dot1x mac-auth-bypass (MAB) from Cisco's website => If a port is in unauthenticated state, it remains unauthenticated, and if MAB is active, the authentication will revert back to the 802.1X Authenticator. If the port is authorized with a MAC address, and the MAB configuration is removed the port remains authorized until re-authentication takes place.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

The message basically means MAB session is going to start and the switch will try authenticating the user via MAC address as the username. Below you will see the radius packet sent by the switch

```
rad_recv: Access-Request packet from host 10.9.254.11:1645, id=57, length=146
    User-Name = "0011434f7580"
    Service-Type = Call-Check
    Framed-MTU = 1500
    Called-Station-Id = "00-13-7F-C6-34-33"
    Calling-Station-Id = "00-11-43-4F-75-80"
    EAP-Message = 0x020300060304
    Message-Authenticator = 0x4e13b9c3594c04853411b6ab84e8f879
    NAS-Port-Type = Ethernet
    NAS-Port = 50047
    State = 0x5b0dc4b104215826b1ea12fbca989da6
    NAS-IP-Address = 10.9.254.11
```

Now the radius server can verify the mac address and not require password this mac address. You will see this debug message on the freeradius server as shown below, allowing the printer to authenticate and join in the vlan 1023 as a printer device.

```
 rad_check_password:  Found Auth-Type Accept
 rad_check_password: Auth-Type = Accept, accepting the user
Login OK: [0011434f7580/<no User-Password attribute>] (from client Switches port 50047 cli 00-11-43-
4F-75-80)
 Processing the post-auth section of radiusd.conf
modcall: entering group post-auth for request 0
 modcall[post-auth]: module "ldap" returns noop for request 0
modcall: leaving group post-auth (returns noop) for request 0
Sending Access-Accept of id 80 to 10.30.254.11 port 1645
    Tunnel-Type:0 = VLAN
    Tunnel-Medium-Type:0 = IEEE-802
    Tunnel-Private-Group-Id:0 = "1023"
```

However there is an issue, any person can plug into the same port and fake the mac address of the device. Many of the printers or other Ethernet devices have their mac address visible as part of the serial number token or label in the rear. If we don't restrict what this device is allowed to do, someone can plugin and bypass the security mechanism laid in place.

Here is where some new techniques learnt from SANS 502 class about reflexive ACL's on Cisco routers come handy. As the printer traffic is fairly minimal, there is no need to build a whole firewall ruleset and interface for this device. You can use Cisco's reflexive ACL's to restrict only incoming communication to the printer from serverfarm / data center and keep state in outgoing TCP packets. If you use Cisco's standard ACL's, some user can use his source port as

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

9100 (hp jetdirect printing port) and be able to scan or bypass authentication.

In our example configuration, I have set aside 10.143.0.0/16 class B network for printers under a VRF called DEVICES. This network is also tightly restricted for access for only incoming communications from serverfarm where the print spools are managed. If you allow users to directly print, you can modify to allow the various print groups. The ACL is designed so that you can implement in multiple distribution locations as a template. You will not need to tweak it for each distribution location or building.

```
! Define a new network and MPLS cloud
ip vrf DEVICES
! all routing fun that we had done before for each network
 rd 64600:93
 route-target export 64600:93
 route-target import 64600:93
! Get serverfarm to talk this network
 route-target import 64600:900
! Define a new access lit
ip access-list extended DEVICES_out
! Permit all servers to access 9100 jetdirect port – mark for reflection as "print"
 permit tcp 10.30.0.0 0.0.255.255 10.143.0.0 0.0.255.255 eq 9100 reflect print
! Allow www and https based printing support in newer printers – mark as reflection as "www-print"
 permit tcp 10.30.0.0 0.0.255.255 10.143.0.0 0.0.255.255 eq www reflect www-print
 permit tcp 10.30.0.0 0.0.255.255 10.143.0.0 0.0.255.255 eq 443 reflect www-print
!Allow any other communications.
ip access-list extended DEVICES_in
!Allow return communications for "print" and "www-print"
 evaluate print
 evaluate www-print
!
interface Vlan1023
 description Printer-VLAN
! Assign VRF
 ip vrf forwarding DEVICES
!This is one of the distribution locations
 ip address 10.143.29.1 255.255.128.0
!Apply the acess lists in
 ip access-group DEVICES_in in
! apply the access list out
 ip access-group DEVICES_out out
!
```

In the current model, you cannot allow DNS queries from printers or outgoing SMTP email from jobs done by printers. These may be necessary, after checking your policy and procedure, you can opt in allowing other communications. Any communications that originates from the printer can be faked by a non printer device on the same port or switch. If the end user changes his mac address to

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

mimick a printer, this cannot be stopped by newer security features such as "ip arp inspection" or "ip dhcp snooping."

There may be other devices such as vending machines, access locks and card processor which may need to be in this network. It is very important that you take into account the risk of mixing and matching multiple types of devices to the same network. Some special services such as credit card processing device may require an independent network and be compliant with PCI or other regulations.

However with an MPLS enabled network, you have the ability to virtualize a new network on the top of the same infrastructure. This has great benefits, but is also brings in a large amount of responsibility. It surely cuts down the greater need for building new physical infrastructure for every new isolated network. It still requires clear procedures and definitions of each VRF network, not to exclude a policy framework tied to each one.

6.4 Simplifying your configuration, backing up and auditing of Layer 2 switches.

Cisco provide a simple macros that can be re-used and applied to multiple switchports on a single switch. An example template configuration is shown in here.

```
service password-encryption
banner login [
This computer system is the property of ***.
****LEGAL STUFF****
[
macro name host-access
description Host Access Port
switchport
switchport mode access
switchport nonegotiate
switchport port-security
switchport protected
switchport port-security maximum 1
switchport port-security violation restrict
storm-control broadcast level 5
dot1x port-control auto
dot1x guest-vlan $AVLAN
dot1x mac-auth-bypass eap
dot1x pae authenticator
dot1x port-control auto
dot1x guest-vlan $AVLAN
dot1x auth-fail vlan $AVLAN
@
macro name wireless
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
description Wireless Access Point Port
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan $WVLAN,$MVLAN,$WPAVLAN
switchport trunk native vlan $MVLAN
@
macro name uplink-core
description Core/Distribution Uplink Port
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
ip dhcp snooping trust
ip arp inspection trust
@
vtp mode transparent
spanning-tree uplinkfast
ip dhcp snooping
no ip dhcp snooping information option
aaa new-model
aaa authentication login default radius local
aaa authentication enable default radius enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
enable secret ************
username backdoor privilege 15 password 0 *********
radius-server host 10.30.12.1 auth-port 1812 acct-port 1813
radius-server host 10.30.12.2 auth-port 1812 acct-port 1813
radius-server retransmit 1
radius-server timeout 2
radius-server key ***************
interface vlan 1
shutdown
exit
vlan 31
name Network-Management
exit
logging 10.30.12.1
logging 10.30.12.2
logging facility local3
logging trap warnings
service timestamps log datetime local
service timestamps debug datetime local
logging buffered 4096
snmp-server community ****** ro
snmp-server community ******** rw
snmp-server enable traps
snmp-server enable traps snmp auth linkup linkdown coldstart warmstart
snmp-server system-shutdown
snmp-server host 10.30.12.1 trap ************
snmp-server host 10.30.12.2 trap ************
no ip http server
ip domain-name mydomain.net
ip name-server 10.30.12.1
ip name-server 10.30.12.2
no ip domain lookup
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
ntp server 10.30.12.1
ntp server 10.30.12.2
clock timezone EST -5
clock summer-time EDT recurring
int Vlan31
ip address dhcp
description Network-Management
exit
!can be done later by network admin or be part of bootfile loaded to the switch.
interface range  Fa 1/0/1 - 47
macro apply host-access 932
exit
interface Fa 1/0/48
!Last port is dedicated for uplinking UPS with management as guest VLAN.
!UPS mac address should be registered still to gain access in dhcp TABLE.
description UPS-Ethernet-port
macro apply host-access 31
exit
!
interface range Gi 1/0/1
macro apply uplink-core
exit
end
```

You can use "macro-apply" command and simplify your configuration. The template shown above can be deployed one every switch as a startup configuration. The switches are designed to trunked to central location and then terminated on a distribution router. Cisco and many other manufacturers support first time configuration through dhcp bootfile options which makes it easy to deploy large number of switches and bring them up with this template. A network admin can apply the macro to change particular ports for say "UPS network monitoring" or new trunk ports for expanding switches in the LAN. The current network where this deployment is in its second refresh cycle has 700 switches (approx) and 6 distribution routers and 2 core routers.

A complex network is hard to manage and maintain. It is important that you standardize all your networking equipment installation and configuration procedure as shown above. It is also important that you design a simple backup and restore procedure for all your active devices. Here is a very simple SNMP based script can save you a lot of trouble by backing up weekly your switches and routers configurations. It is also designed to do a "diff" audit of all changes to switching infrastructure done in a week.

```
#!/bin/bash
#This I sour backup directory under /tftpboot
BACKUPDIR=/Network-Backups
#This is our backup server
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
TFTPHOST=10.33.12.1
#RW community string on switches routers
COMMRW=X*X*X*X*X*X
# A random variable for snmp uses UNIX Shell's RANDOM env variable
RAND=$RANDOM
#Save switches and routers in their own directory
for TYPE in SWITCH ROUTER; do
#Remove old files
rm -rf /tftpboot/$BACKUPDIR/$TYPE.OLD
#Backup the last week config
mv /tftpboot/$BACKUPDIR/$TYPE /tftpboot/$BACKUPDIR/$TYPE.OLD
#Create directory for the current config
mkdir /tftpboot/$BACKUPDIR/$TYPE
# Grab the list of switches and routers from an inventory file if you use mysql you can do this with
# /usr/local/bin/mysql –u$dbuser –p$dbpass inventory -e "SELECT hostname FROM $TYPE "
for SW in `cat /var/inventory/$TYPE.txt`; do
# ping and make sure the switch is up
ping -w1 -c1 $SW > /dev/null
if [ ! $? == 0 ]; then
# if switch is not up spit out inventory error.
echo "Error Switch $SW is unreachable"
#loop to the next one
continue
fi
#ConfigCopyProtocol from Cisco read process
#http://www.cisco.com/warp/public/477/SNMP/copy_configs_snmp.shtml
snmpset -v 1 -c $COMMRW $SW  .1.3.6.1.4.1.9.9.96.1.1.1.1.2.$RAND i 1
#( echo "Switch is not configured for SNMP"; continue; )
if [ ! $? == 0 ]; then
echo "$SW Switch is not snmp enabled please fix configuration "
continue
fi
#Create the file and make it world writeable for tftp process.
touch /tftpboot/$BACKUPDIR/$TYPE/$SW && chmod 0666 /tftpboot/$BACKUPDIR/$TYPE/$SW
# Walk through config snmp copy commands
snmpset -v 1 -c $COMMRW $SW .1.3.6.1.4.1.9.9.96.1.1.1.1.3.$RAND i 4
snmpset -v 1 -c $COMMRW $SW .1.3.6.1.4.1.9.9.96.1.1.1.1.4.$RAND i 1
snmpset -v 1 -c $COMMRW $SW .1.3.6.1.4.1.9.9.96.1.1.1.1.5.$RAND a "$TFTPHOST"
snmpset -v 1 -c $COMMRW $SW .1.3.6.1.4.1.9.9.96.1.1.1.1.6.$RAND s  $BACKUPDIR/$TYPE/$SW"
# wait for a second for tftp udp packets to finish gathering – make this longer if needed.
sleep 1
snmpset -v 1 -c $COMMRW $SW .1.3.6.1.4.1.9.9.96.1.1.1.1.14.$RAND i 1
fi
#wait after each switch/router cycle is complete to give I/O enough time to flush
sleep 2
done
#Finished backups now change it backup to world readable or stricter if needed.
chmod 444 /tftpboot/AccessNetwork-Backups/$TYPE/*
# Send audit changes on all switches as email to networkers@localhost
diff -c -I'^ntp' -I'^!' /tftpboot/$BACKUPDIR/$TYPE.OLD /tftpboot/$BACKUPDIR/$TYPE \
| mail -s "Switching/routing/AP Config changes last week $TYPE" \
networkers
# This is the loop for switches and routers, the networks will get two emails one
done
```


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

A sample email from this script is shown below. You can see that there was a new snmp community added to the switch called public and private, which are default values. This could be due to upgrade of IOS or due to some strange configuration management tool. The auditing has saved us trouble many times than I can admit in this paper.

```
From: mcmaster@xxsi
Message-Id: <200702180832.l1I8WZ4b029646@xxsi>
To: alladmins@xxsi
Date: Sun, 18 Feb 2007 03:32:35 -0500 (EST)
Subject: Switching/AP Config changes last week CSO

diff -c -I^ntp -I^! /tftpboot//AccessNetwork-Backups/CSO.OLD/CSO-002-031-20
/tftpboot//AccessNetwork-Backups/CSO/CSO-002-031-20
*** /tftpboot//AccessNetwork-Backups/CSO.OLD/CSO-002-031-20          Sun Feb 11 03:00:12
2007
--- /tftpboot//AccessNetwork-Backups/CSO/CSO-002-031-20          Sun Feb 18 03:00:13 2007
***************
*** 257,262 ****
--- 257,263 ----
  logging facility local3
  logging 152.13.12.1
  logging 152.13.12.2
+ logging 152.13.12.25
+ snmp-server community public RO
+ snmp-server community private RW
  snmp-server system-shutdown
#EOM EndofMail
```

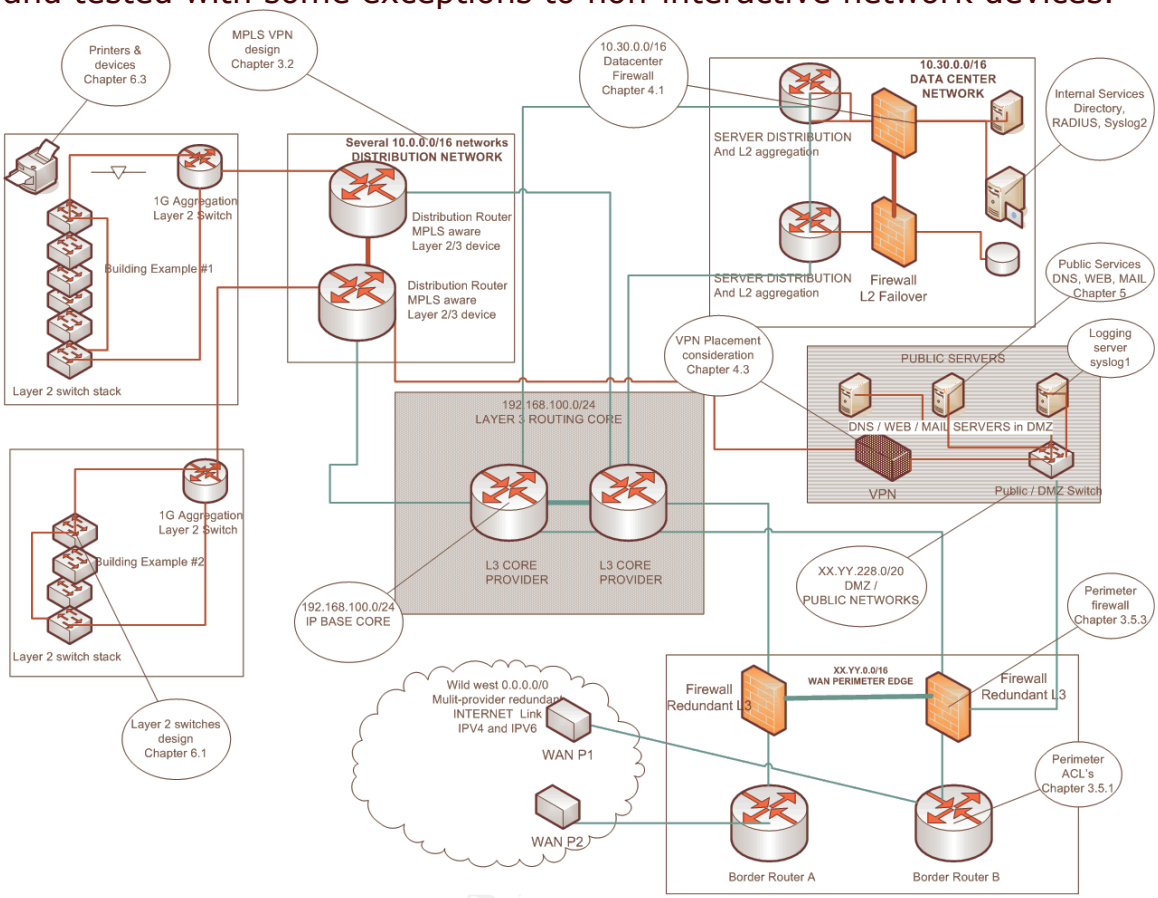
7. TAKE IT FURTHER.

"The superior man, when resting in safety, does not forget that danger may come. When in state of security he does not forget the possibility of ruin. When all is orderly, he does not forget disorder may come. Thus his person is not endangered and his states and all their clans are preserved." -Confucius (551 BC - 479 BC)

Let's take a quick look at what has been achieved and what the network looks like now. The picture shown below now represents the network. The biggest network needs for isolation and segmentation between networks has been possible. Definition and limitations of public web services was achieved. The traditional perimeter /border router with the well defined ACL's was put in place. VPN was plaed with reasonable compromise and protection. 802.1x was implemented

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

and tested with some exceptions to non-interactive network devices.



Finally the network looks fairly secure and segmented, but is it good enough? Not really. There is multiple network security issues that still need to be dealt with. We will cover more topics that can be spearheaded to solutions such as QoS, Voice, IPV6 have not been considered in this design. Network security for global route tables have been loosely defined, however this has to be taken further for BGP, EIGRP, OSPF security definitions.

7.1 Future networks need segmentation, authentication and authorization – HIPPA, FERPA, CLEA, PCI.

As networks expand and grow, laws and legal requirements are catching up to address network security. What the current design detailed in this paper helps us do is really build a flexible model for building networks that are virtually isolated from each other. Each of these networks can be highlighted as "RED" or "MAROON" network with very high security concern.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

New business processes and business solutions come around the corner and technology needs to be designed to accommodate these needs. This paper only scratches the surface in starting to build a multi-layered defense-in-depth modeled network. There is still much to be done to develop and address other issues and precursor to this framework that I have laid out. Some of them can be complete paper in themselves. Here is my list of great technology toolbox that needs to be addressed for security

1. Qos as a security strategy: Quality of Service is being implemented in most voice centered networks today. However QoS can be great benefit for protecting against DOS attacks, spreading of worms from internal compromised hosts. This is full topic itself. QoS in an MPLS Context is challenging and needs to be addressed. Some great books are being written in this field by Cisco Press and O'Reilly.
2. Voice over IP security: Voice over IP deployments is more popular nowadays with multiple vendors and newer standards. There is a need for security and privacy needed for voice specific deployment. MPLS in voice environment is a great match of interests and capabilities.
3. Wireless Security: Wireless technologies today pose great potential in providing seamless networking to clients. Bluetooth, 802.11, cellular and Wimax are some of the technologies that provide unwired connectivity to desktops, phones, PDA's and devices. It is important to provide a security model even for 802.11i implementation that includes Wireless IDS and client anomaly detection.
4. BGP/OSPF WAN Security: Your wan routing protocols have been largely ignored by ISP's and large organizations for security.
5. IPv6 Security: IPv6 is growing largely in Asia. While it has many benefits of learning from IPv4 mistakes, such as avoiding fragmentation, it still poses greater challenges for security. Encryption and native VPN in IPv6 poses greater challenges to IDS and IPS.
6. Enhanced directory: Single Sign On SSO is a very popular topic of interest. Identity management across multiple platforms of servers and services is a great challenge. A paper can be dedicated for secure design of SSO for clients.

8. Acknowledgements and References

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

8.1 About the author and acknowledgements:

Vijay Sarvepalli is a senior network architect at UNCG (University of North Carolina at Greensboro). He has a Bachelor of Engineering degree in Electronics & Telecommunications from University of Madras, India and a Master of Science degree in Electrical & Computer Engineering from University of Utah. He has worked at various levels from microprocessor pre-sales engineer, to RF design engineer, instrumentation engineer, UNIX systems engineer, network engineer, to his current position as network architect at UNCG. His earlier publications have been in "Fifteenth annual meeting of IEEE bio-electromagnetics society", "Applied physics letters", "Journal of vacuum science and technology" and "Journal of electronic materials." He lives now in North Carolina with his wife Erica Sarvepalli and three kids (Rajiv (7) – boy, Kiran (5) –boy and Pori (3) – girl).

The work accomplished in this paper was done with input from many other people. Here is a short list of engineers and network specialists who have helped me sharpen my ideas. Joff Thyer is a senior network architect at UNCG, who has networking and UNIX systems experience and has provided many analytic and conceptual insights into this design. Chuck Curry is information security officer at UNCG has provided many of the technology needs and data compliance "matrix" to help define isolated networks for a campus. Gary Cox is Senior IT administrator, MPW (Muscatine Power and Water, Iowa) who has provided many insightful design tips for email and web gateway design. John Gale is security analyst at UNCG, who has also been pivotal in providing the design criteria for diverse clients such as at a university campus. John L Williams Jr. is a senior network architect at UNCG, whose expertise is in Cisco 6500 and Cisco QoS design at enterprises has provided some valuable methodology for implementing edge QoS as a security and performance solution.

8.2 References

Online Resources

Cisco (2006). The University of Minnesota Upgrades Network Security with a Cisco MPLS Network – a case study
Retrieved on Jan 22, 2007 from

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

http://www.cisco.com/en/US/products/hw/switches/ps708/products_case_study0900aecd802b1d7f.shtml

RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs)
http://www.ietf.org/rfc/rfc4364.txt

RFC 4381: Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs)
http://www.ietf.org/rfc/rfc4381.txt

Cisco (2006). Security of the MPLS Architecture
Retrieved Jan 24, 2007 from
http://www.cisco.com/en/US/products/ps6822/products_white_paper09186a00800a85c5.shtml

Schneider, M. (2004). Ten risks of PKI
Retrieved Jan 22, 2007 from
http://www.schneier.com/paper-pki.html

Netcraftsman.com (2006). MPLS for WAN.
Retrieved Feb 2, 2007 from
http://www.netcraftsmen.net/welcher/papers/mplsvpn.html

Juniper Networks (2007). Multiple Instances for Label Distribution Protocol
Retrieved Jan 23, 2007 from
https://www.junipernetworks.com/techpubs/software/junos/junos63/feature-guide-63/html/fg-mi-ldp.html

Book References

Monique J. Morrow, Azhar Sayeed (2006). "MPLS and Next-Generation Networks," Cisco Press ISBN: 1-58720-120-8

Lancy Lobo, Umesh Lakshman (2006). "MPLS Configuration on Cisco IOS Software," Cisco Press ISBN: 1-58705-199-0

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Last Updated: June 18th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**