Security Perimeters/DMZs & Firewalls

James Farricker (University of Washington)
Rev: January, 2016

As companies have increasing requirements to provide network interconnection with remote vendors, suppliers, customer support centers...., the risk increases that there will be attempts by unauthorized users to access resources in your network. Network Managers and Administrators must provide ease of access to those who need it, while providing the most effective security controls to those who are permitted access while denying unauthorized access. From a legal standpoint, having audit capabilities is critical to the ability to take action against unauthorized access.

Developing strategies for Remote Access & Connectivity one should consider:

- Hardware Selection (Cost, platform, maintenance/sparing, expandability, NICs)

- Software Selection (Cost, In-house/Off Shelf, OSs supported, maintenance, expandability.

- Administrative Support (Setup, Training, Documentation and Installation)

- Firewall Maintenance (Network Management tools, troubleshooting procedures, change management/problem management, capacity planning).

- Risk Analysis (service/application loss, new applications/user requirements, analysis of gateway/firewall failure, proposed network component changes)

- Architecture Development (policies - standardize protocols/applications/components, documented connectivity/access guidelines and procedures.

- International/Government/Military (policies conform to established parameters that differ from commercial/corporate entities). Corporate enterprise international connectivity should be treated separately/differently as the threats and risks differ substantially.

The Rule – You can't do everything for everybody !!!

Policies <u>ARE NOT</u> made to be broken – or a company ends up with a swiss cheese perimeter (full of holes) to accommodate one-off customers, suppliers, Sr. Mgmt, LAN and System administrators who "bypass" the perimeter.

SOx (Sarbanes Oxley) – legal requirements for documented processes for peer review, change management & control. What could this possibly have to do with IT – ***Thank You Enron/Tyco***

Recommendations for Network Security:

Senior Management and Sr. Network Security/Administration set, sign and publish policies guidelines for employee acceptable use, remote access, partner, supplier and customer connectivity. Senior Management must designate a single decision point (focal or team) to arbitrate security, perform risk analysis and risk acceptance.

Would you want the people designing the network to make security policy/decisions ?? Why or Why Not ???.

Responsibility MUST be designated to READ security logs !! Too many times they are underutilized or even ignored. Understand how are internal and external audits are conducted, the available tools (network intrusion devices, port scanners, device (router-switch) configuration (ACLs) analysis/audit, firewalls etc..

Many Companies today follow what is referred to as the AAAA Net. Security policy:

Access - controlling the physical access, encryption, data closet/server room access.

Authentication – knowing you indeed are who I think you are. Multi-factor authent.

Authorization – limiting this access to specific resources.

Audit – maintaining logs of unauthorized access attempts**.**

I. Access

There are multiple strategies of providing and controlling network access.

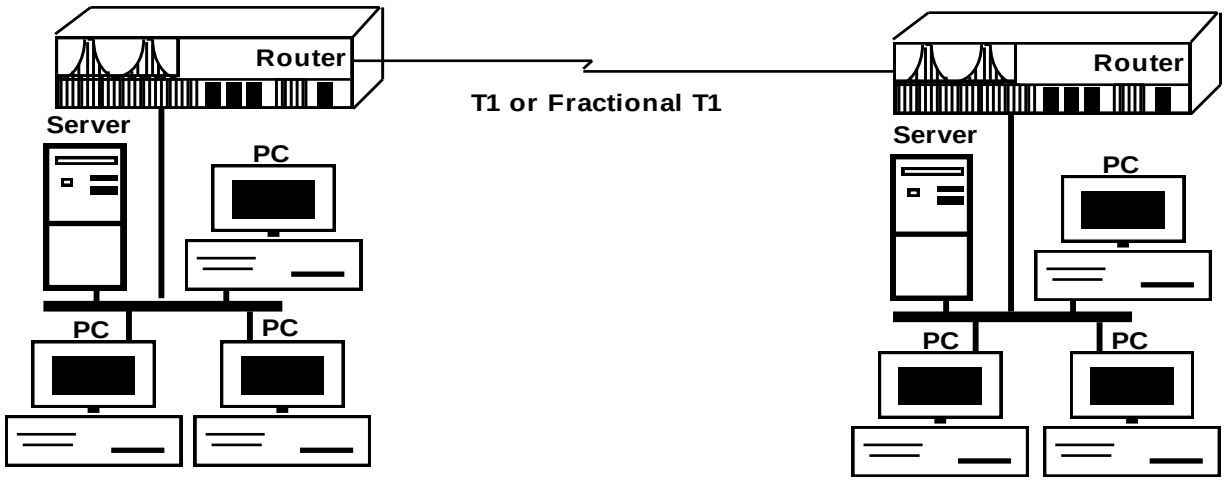
Basic Philosophies include utilization of the following components:

Point to Point - Dedicated Circuits versus shared Frame/SMDS/DSL
Encryption – esp. on RF links
Routers configured to block (THESE ARE NOT Firewalls)
Packet Filters
Application/Gateway Firewalls
VLANs
Tunnels (VPNs – IPSec)
Wireless Access

Point to Point Dedicated Circuits

Point-to-Point:

single communications link not shared with any other stations.

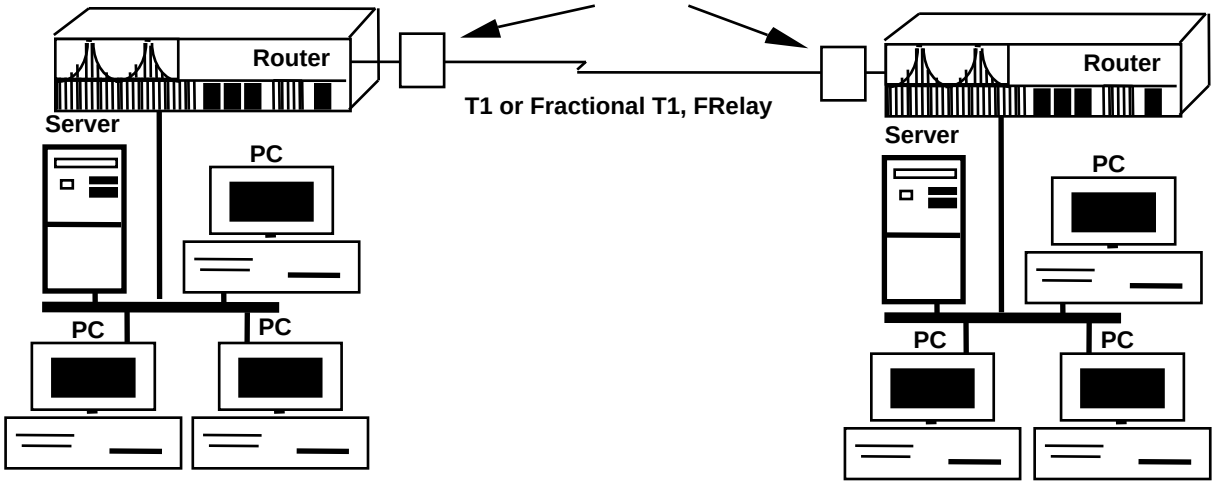


Since the T1 is a dedicated line (nobody else shares the link), there is less concern than technologies using shared bandwidth where multiple users' traffic is on the same network infrastructure simultaneously.

Encryption

If security of the dedicated circuit becomes an issue, the line may be encrypted (using data encryptors - RS232, V.35 interfaces) where the data portion of the frames is scrambled as it is sent over the network. The following illustration shows the use of encryptors in LAN interconnection environment.

Data Encryption Devices



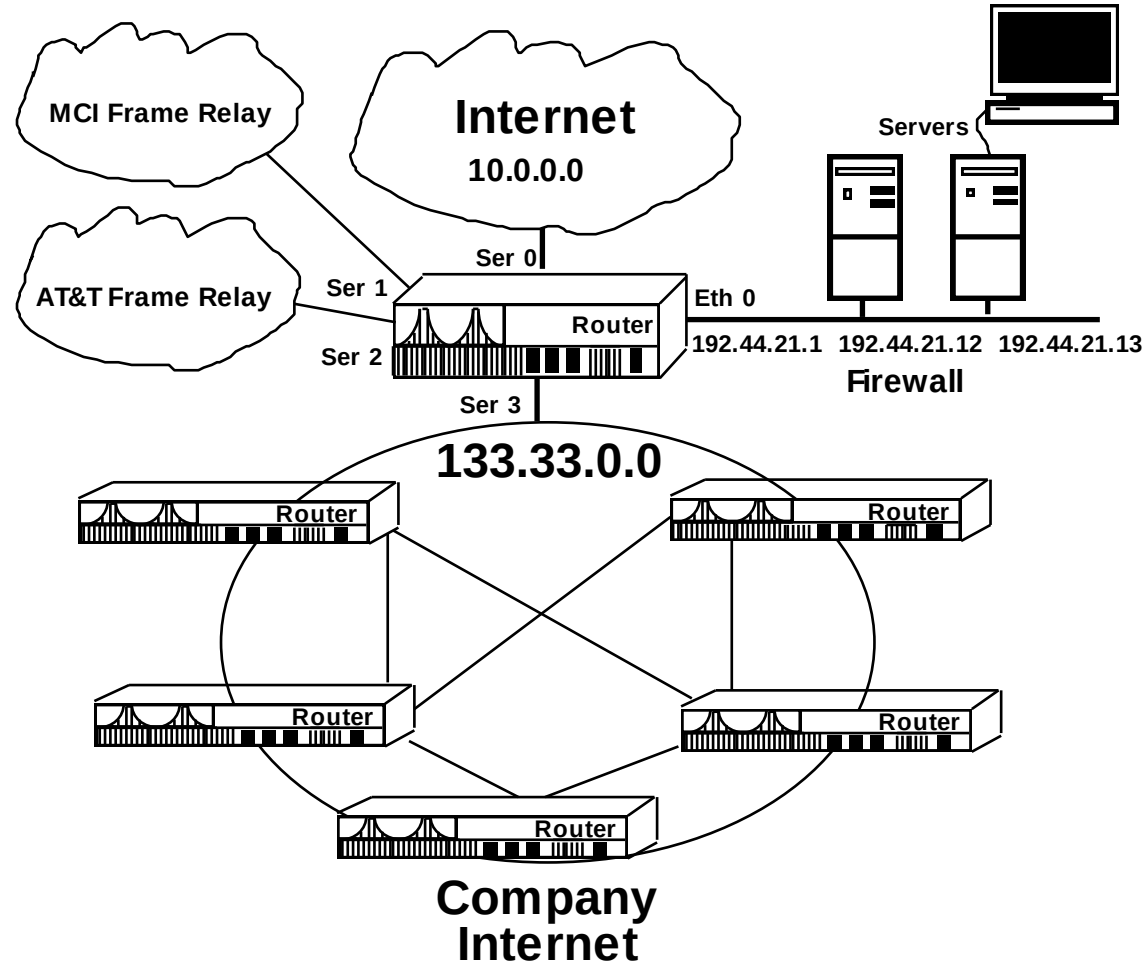
Router Firewalls

Routers have the serial connections that link either LANs at other organizational locations or other company networks. Router firewalls can be used in two ways:

1) filter out networks (by controlling advertisement of networks)

2) apply filters against specific TCP/IP devices - some devices even allow filtering at the device level to include TCP/UDP ports so users whose IP address is allowed may only access/utilize certain TCP/IP applications (Telnet, FTP, SMTP, SNMP)

1a. Filtering out Networks



In the network illustrated above, the firewall is advertised to both the ISP/Internet (Using BGP) and the Company Internet by the routing protocol (for example EIGRP). Specific coding of the routing protocol parameters will advertise the firewall both directions, but not advertise the company Internet to The Internet (and vice versa).

Perimeter Router Sample configuration:

Interface Ethernet 0
ip add 192.44.21.1 255.255.255.0
ip broadcast-address 192.44.21.255

interface serial 0
ip add 10.32.21.2 255.255.255.0

interface serial 1
ip add 133.33.13.1 255.255.255.0

router BGP 100 (To ISP - Internet)
network 10.0.0.0
network 192.44.21.0
Distribute-list 21 in Serial 0 (ISP inbound network route filter)

router EIGRP 200 (internal network)
network 133.33.0.0
network 192.44.21.0

access-list 21 permit (list of addresses from ISP/Internet permitted)
access-list 21 permit 130.44.0.0 0.0.255.255 (allows Customer A 130.44.0.0 net in)
access-list 21 permit 130.49.121.0 0.0.0.255 (allows Customer A 130.49.121.0 net in)
access-list 21 permit 199.12.1.0 0.0.0.255 (allows Customer B 199.12.1.0 net in)

This configuration allows users from behind The Internet to log directly onto devices that reside on the firewall (security island) or users from the internal intranet to access firewall devices directly. Users coming thru The Internet cannot directly log onto devices in the 133.33.0.0 network since they are not in the same autonomous group (they do not share routing information - and would not know how to find each other. The firewall could be configured to contain other autonomous number(s) for routing protocols to allow external users from the frame-relay clouds to have access to firewall devices.

<u>1b. Filtering out Specific IP addresses</u>
Once the network filters have been configured, another level of filtering can be set on specific interfaces (for example the serial interface that connects the perimeter router to the Internet in the illustration above. In this case, filters will permit/deny specific TCP/IP devices from those networks that are advertised.

interface Ethernet 0
description ; perimeter LAN.
Ip add 192.44.21.1 255.255.255.0
ip broadcast-address 192.44.21.255
ip access-group 110 in

access-list 110 permit tcp host 130.44.12.24 eq SMTP (or SMTP TCP port #) (email)
access-list 110 permit tcp host 130.49.121.24 eq SMTP (or SMTP TCP port #) (email)
access-list 110 permit tcp host 130.44.121.11 eq 21 (FTP TCP port #) Customer B
access-list 110 permit tcp host 130.44.121.11 eq 23 (Telnet TCP port #) Customer B

Medium and larger companies – rather than let the router incur the additional performance overhead of filtering (rather than just routing) – have began using packet filters which have more CPU and can filter on networks, TCP hosts or TCP/UDP ports. SUN and many other vendors make packet filters, which also audit (which routers do not) unauthorized requests.

IPSec (Secure IP) Tunnels and VPNs (Virtual Private Networks)

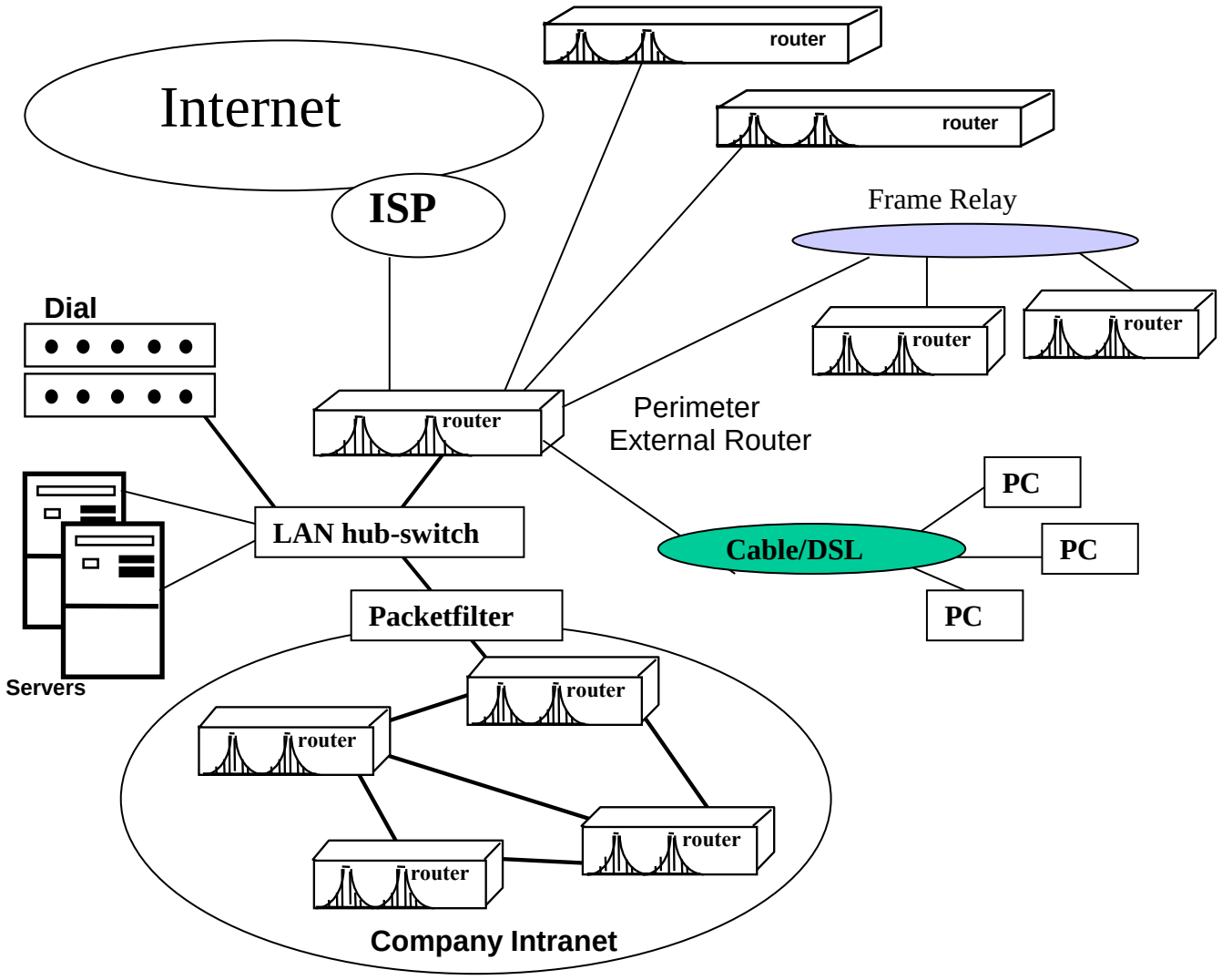
Internet provides WAN communications more cheaply and more globally than a leased line, Frame Relay, or asynchronous transfer mode (ATM) network. While it does provide cost effective connectivity, the Internet does not provide the security, bandwidth, or quality of service (QoS) guarantees typically associated with private networks. Additionally, the Internet supports only TCP/IP, while most networks accommodate a variety of protocols.

Internet service providers (ISPs), equipment vendors, and software developers say they can give you the best of both worlds: the security, performance, availability, and multi-protocol support of a private network over the inexpensive and pervasive Internet. It's called a virtual private network (VPN), and the technology is currently being considered primarily as a means of extending the reach of private networks. The following illustration depicts a non-VPN environment, where dedicated links or Frame circuits/PVCs are used for inter-company communications. Additionally a dedicated link is maintained for Internet connectivity for access to Internet resources, Web, e-mail etc.

Tunneling Defined

A key component of the virtual service is tunneling, a vehicle for encapsulating packets inside a protocol that is understood at the entry and exit points of a given network. These entry and exit points are defined as tunnel interfaces. The tunnel interface itself is similar to a hardware interface, but is configured in software.

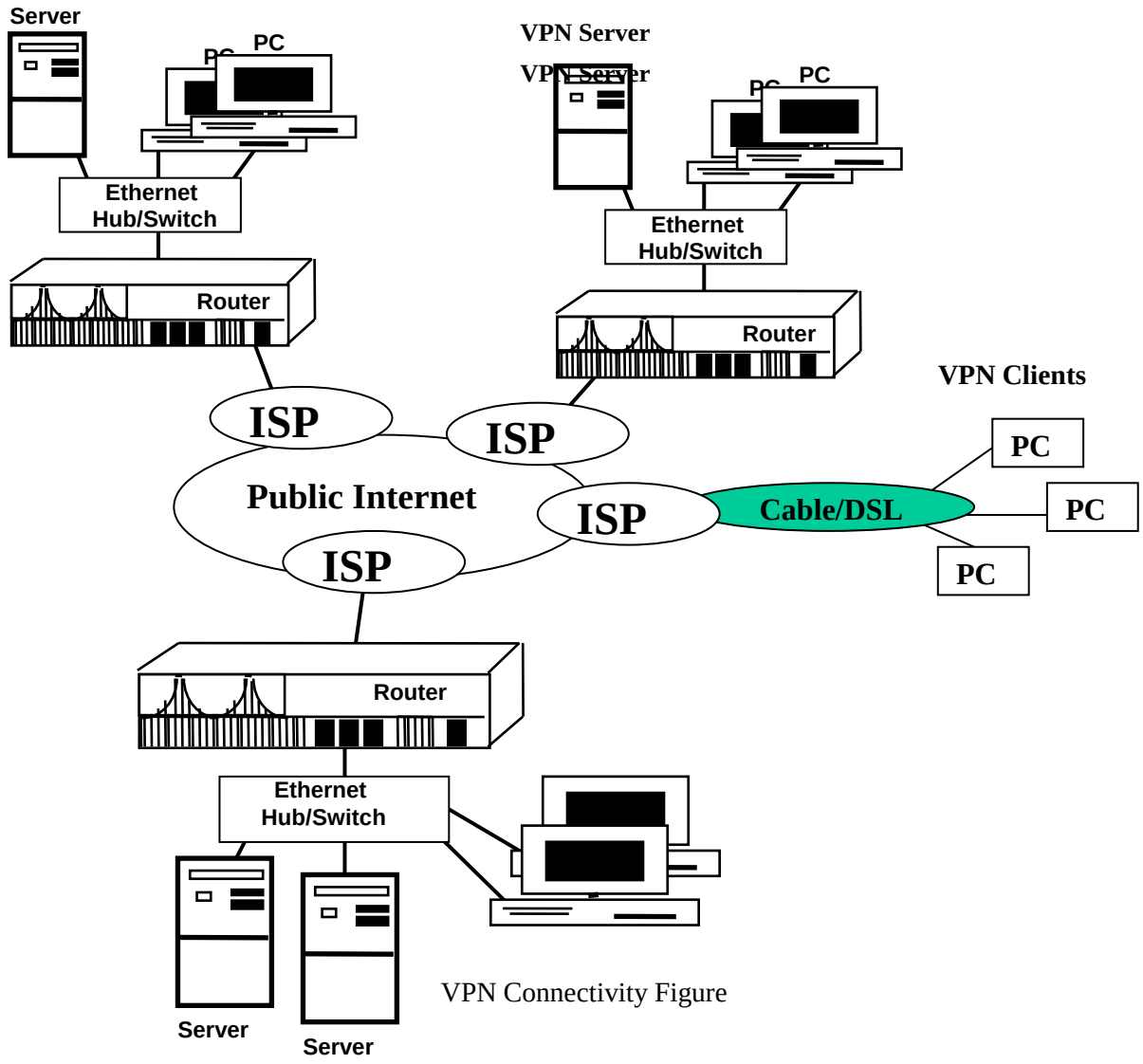
VPNs and secure IP tunneling, one of the underlying technologies) raise several challenges, including; dealing with the issues of QoS, non-IP traffic, authentication and assignment of IP addresses.



Secure Perimeter Connectivity Figure

There are two main architectures for setting up a tunnel: client-initiated or client-transparent. Client-initiated tunneling requires tunneling software both for clients and for tunnel servers (or gateways). The latter typically reside at the corporate central site, though it may reside at the ISP point of presence (POP) that serves the central site. With client software for tunneling, the client and the tunnel server simply establish the tunnel, using authentication based on a user ID and password. The client and the tunnel server may also negotiate encryption. Once the tunnel is established, communications proceed as if the ISP were not mediating the connection.

For tunneling to be transparent to the client, the ISP's or network administrator can configure a set of routers to do a LAN to LAN Tunnel where the two networks interact as if the two were directly attached. The following illustration demonstrates how using VPNs for external connectivity reduces requirements for dedicated links, and router ports.



VPN Connectivity Figure

Since 1996, two tunneling protocols have competed for users' attention: Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer Two Forwarding (L2F). The essential technical difference between the two is that PPTP tunnels by wrapping PPP packets in IP, a Layer Three protocol, while L2F uses Layer Two protocols, such as Frame Relay and ATM, for tunneling.

PPTP can be client-initiated (and transparent to the ISP) or client-transparent. It requires both a Windows client and server. In contrast, L2F requires support in access servers and routers; thus the ISP has to support L2F. In its defense, L2F provides functionality that PPTP doesn't, such as authentication for tunnel endpoints (i.e., between the access server and the tunnel server). A major advantage of PPTP is Microsoft's support for it. Both a client and a tunnel server for PPTP were shipped in NT 4.0. Another advantage is PPTP's support for flow control, keeping clients and servers from getting overwhelmed by traffic and enhancing performance by minimizing dropped packets and thus retransmissions. However, PPTP requires IP (though it can tunnel IPX and NetBEUI, as well as PPP), and it doesn't include authentication for tunnel endpoints. PPTP, leveraging PPP, relies on user authentication. In addition, some analysts think PPTP may not scale as well as hardware-based solutions such as L2F.

Recognizing the merits of each others' protocols, Microsoft and Cisco agreed to merge their competing protocols into Layer Two Tunneling Protocol (L2TP), which is supposed to offer the best of PPTP and L2F. Secure IP, or IPSEC, is expected to be commonly used to coordinate encryption between L2TP endpoints. (Standardized encryption has not been a feature of PPTP or L2F.)

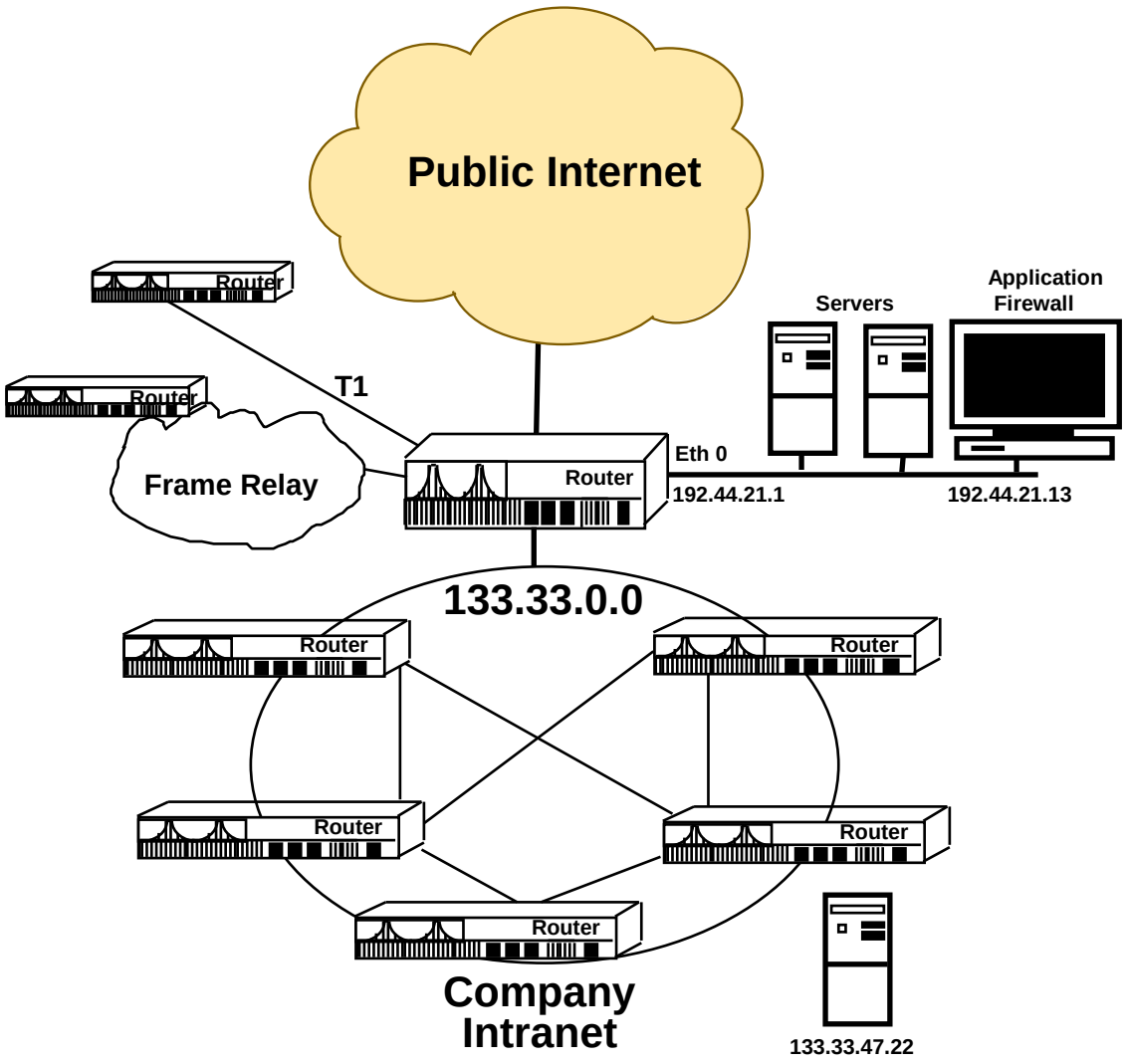
Application/Gateway Firewalls

Application/Gateway firewalls will lock down a particular session to a specific device. It also takes advantage of the router filtering by permitting only certain IP addresses. In the network illustrated below, the application gateway (192.44.21.13) would be defined as the only IP address on the firewall that outside/external TCP/IP addresses could access. Users log on (userID and password authentication), then control is passed for whatever session that particular user is entitled to - in this case it will pass the connection to server (133.33.47.22). The user can only access that particular device and is locked down from Telnet/FTP/SMTP applications from the same server. When the session is complete, it passes control back to the end station and clears the paths utilized.

Application Firewalls provide second and third elements of security – Authentication and Authorization

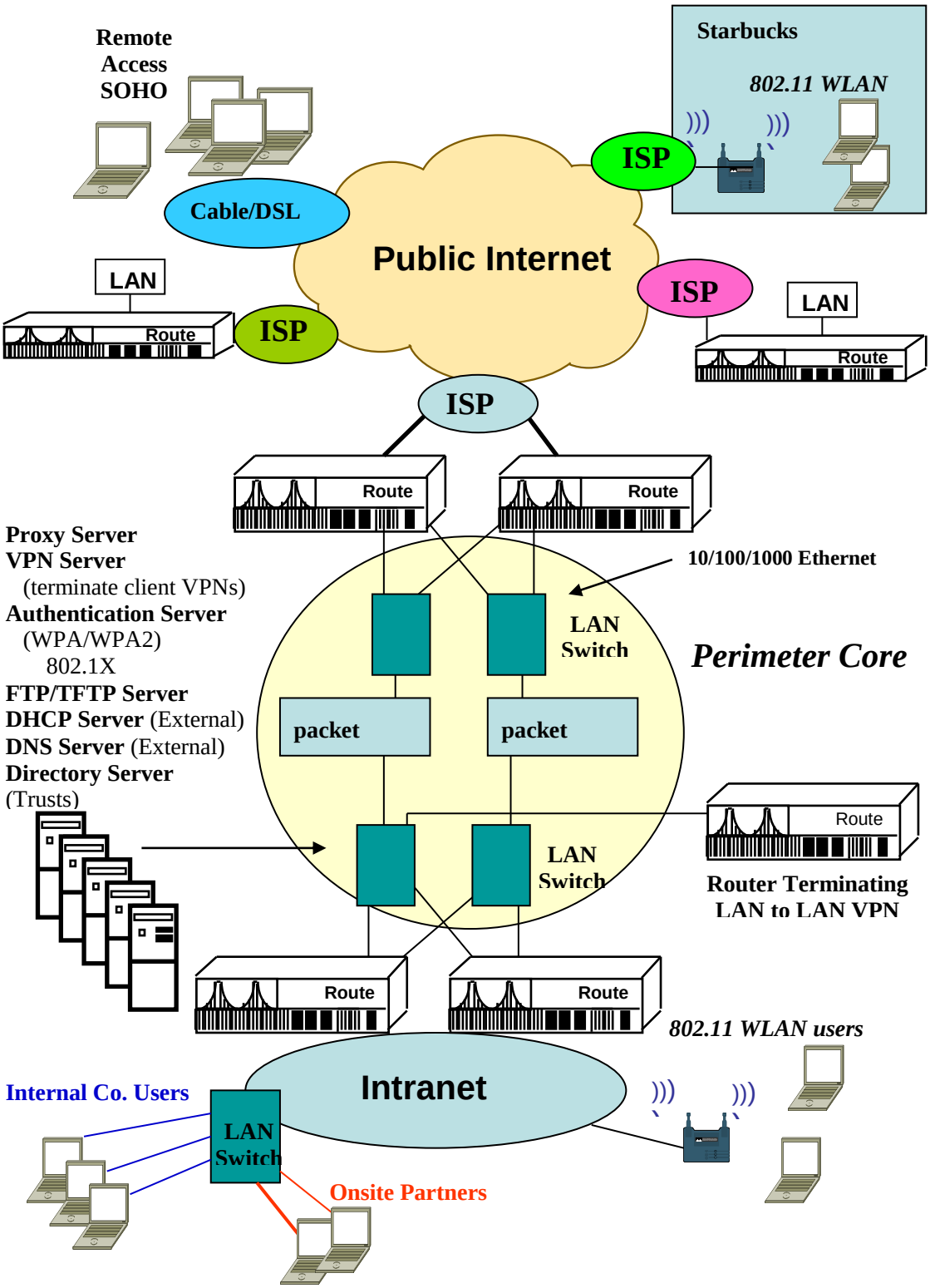
Putting the Pieces Together - Security Perimeters/DMZ's

Security Perimeters/DMZ's – circa late 1990's



The point – Security perimeters/DMZs/firewalls are extremely complicated systems. Effective access control and prevention (from unauthorized access) is achieved by using a combination of hardware (routers, firewall systems) for access control and software for authentication, authorization and audit.

Security Perimeters/DMZ's – circa 2010



Proxy Server:

A proxy server is a program that serves as an intermediary between a client and a server. The proxy is a server from the user's point of view, but is a client as far as the target server is concerned. Proxy servers are used in situations where filtering or shielding is desirable—for exam-ple, if a client computer is inside a firewall (protective program) and wants to communicate with a server outside the firewall. In such a situation, the client's request is passed to the proxy server, which communicates with the other side of the firewall. By forcing traffic to go through the proxy server, the firewall software has an easier time filtering.

Once the target server has responded, the proxy server checks the reply and does any required filtering. Then the proxy server passes the reply to the client. As far as the client is concerned, the interaction took place directly between the client and target server.

A Proxy Server is a World Wide Web server that acts as the sole web server for your entire domain or whatever clients you place behind the firewall, a logical block between your clients and the rest of the Internet. The proxy server usually sits on your firewall and intercepts all web requests coming from clients within the firewall. If the web page request is not on the proxy server's access control list, the request is processed normally and the retrieved web page is sent back to the requesting client. If, however, the requested web page or web site is on the control list, the client instead receives a message indicating that the URL is not accessible or not valid.

Your network must be set up such that clients needing access control must use the proxy server as their Internet gateway. This can be accomplished through proper router setup, placing all clients needing access control "behind" the firewall.

Setting up a proxy server is relatively simple if your server supports proxy operation. Maintaining the proxy access control list can be a daunting task. Most proxy web servers can accept domain names, individual page names, or wildcard URL specifications, actual identification of inappropriate web sites and pages is like shooting at a moving target. As old, already-documented sites disappear, new ones appear. Some vendors market client-based products that will block access to objectionable sites, the updated lists they provide through subscription designated to work with their product only.

Material/References Cited:

Firewalls and Internet Security, Cheswick and Bellovin,
Addison-Wesley, Reading, MA, 2003

The DataBus - Vol. 36, No. 1; Internet Access Control Using Proxy Servers
December, 1995-January, 1996