Session ES132

Implementing Firewalls & Proxy Servers

Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America

+1 718 463 1079
gezelter@rlgsc.com

Tuesday, November 9, 1998
1:30 pm – 2:50 am
Room 11B

Fall 1999 US DECUS Symposium
San Diego Convention Center
San Diego, California

Regardless of whether you are running a single Pentium with Microsoft RRAS and Proxy Server; or a major corporation with hundreds of routers, firewalls and servers, the Goal is the same —

survival.

Robert Gezelter
Software Consultant

Software Installation Notes — General

- ***Keep Notes***
- ***Make Backups***
- ***Use a Test Environment***
- ***Use Blackboards***

Robert Gezelter
Software Consultant

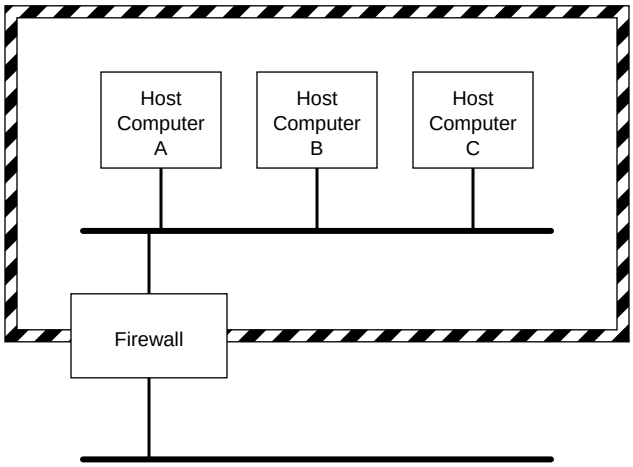
NOTES

Software Installation Notes — WNT Specific

- ***GUI Managed — Keep Notes***
- ***Read ALL WWW pages FIRST***
- ***Make Backups***
- ***Make NEW Recovery Diskette OFTEN!***
- ***Significantly more fragile than OpenVMS***
- ***Registry Hazards***

Robert Gezelter
Software Consultant

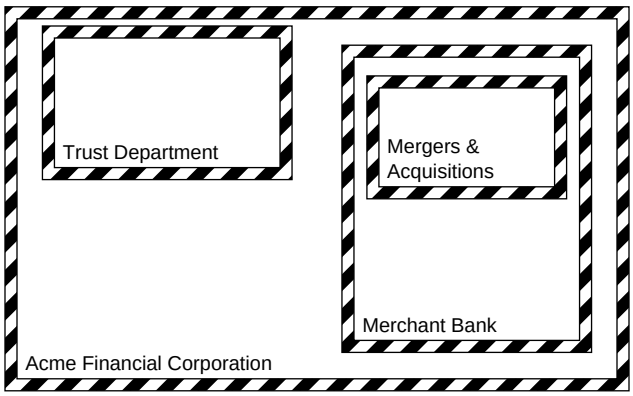
Common Corporate Model



Robert Gezelter
Software Consultant

NOTES

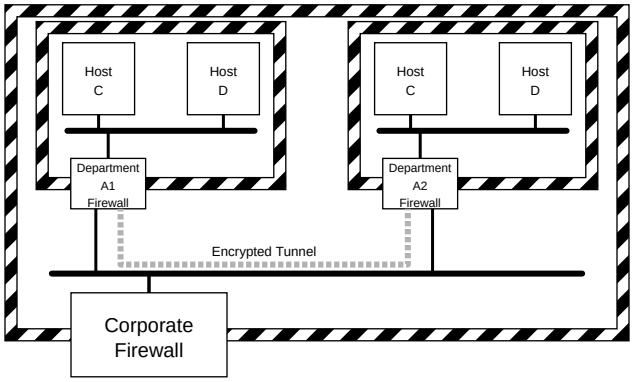
Common Corporate Reality



Implementing Firewalls & Proxy Servers
Slide 6

Robert Gezelter
Software Consultant

Common Corporate Model



Implementing Firewalls & Proxy Servers
Slide 7

Robert Gezelter
Software Consultant

NOTES

Introduction

Issues and Definitions

Terminology

Us/Them

Services

Topologies

Robert Gezelter
Software Consultant

Goals

- ***What are Firewalls and Proxy Servers?***
- ***How to use a single IP address to serve the entire organization***
- ***Why caching is central to performance***
- ***Establish Channels and Controls***

Robert Gezelter
Software Consultant

NOTES

Terminology

- ***IP Address***
- ***Domain Name System DNS***
- ***Bridges***
- ***Routers***
- ***Firewalls***
- ***Proxy***

Robert Gezelter
Software Consultant

ISO Open Systems Interconnect Model

Application
Presentation
Session
Transport
Network
Data Link
Physical

Robert Gezelter
Software Consultant

NOTES

IP Address

- ***32-bits (IPv4)***
- ***Written as ddd.ddd.ddd.ddd***
- ***Assigned by ISP/InterNIC***
- ***Address Classes: A, B, C***
- ***CIDR (Classless Inter Domain Routing)***
- ***Shortened OSI Implementation***

Robert Gezelter
Software Consultant

Domain Name System

- ***Translates Name into IP Addresses***
- ***Distributed, cached database***
- ***Hierarchical Name Space***
- ***Security issues***
- ***Root Level Domains***
- ***Who controls your entries***

Robert Gezelter
Software Consultant

NOTES

Bridges

- ***Data Link level***
- ***LAN/LAN***
- ***Sometimes filtering***

Robert Gezelter
Software Consultant

Routers

- ***Network Level***
- ***Can Screen Packets by address/protocol***
- ***No application knowledge***
- ***Stateless***
- ***Ownership***
- ***Access***

Robert Gezelter
Software Consultant

NOTES

Firewall

- ***Not Generally Defined Term***
- ***Intended as choke point***
- ***Point of control***
- ***Point of access***
- ***Access Control***
- ***Validation/Authentication***

Robert Gezelter
Software Consultant

Proxy

- ***Not well defined***
- ***Can be Routing, or Application***
- ***May or may not include checking***
- ***Acts on behalf of***
- ***Can be simple or complex***

Robert Gezelter
Software Consultant

NOTES

The Gestalt of it All

- ***on the Internet; the nobody has "evolutionary dominance"***
- ***Hubris***
- ***Social Engineering II — Information Warfare***
- ***Like to Know/Need to Know***

Robert Gezelter
Software Consultant

Us vs. Them

- ***Who NEEDS to know?***
- ***Who NEEDS to do what?***
- ***What is permissible?***
- ***What is safe?***
- ***Not black/white***
- ***VERY Gray!***

Robert Gezelter
Software Consultant

NOTES

Services

- ***FTP***
- ***Telnet***
- ***HTTP***
- ***Gopher***
- ***DNS***
- ***PING***
- ***FINGER, ...***

Robert Gezelter
Software Consultant

Facilities

- ***Virtual Private Networks***
- ***Dial-up***
- ***Authentication***
- ***Credentials***

Robert Gezelter
Software Consultant

NOTES

Trust

Trust is the fundamental problem in the online connected world.

Today's environment requires a flexible trust model; including:

- ***colleagues***
- ***collaborators***
- ***competitors***

Robert Gezelter
Software Consultant

Policies and Politics

- ***Company policies***
- ***Disclosure***
- ***Defamation/Harrassment***
- ***Access Control***
- ***Regulations***
- ***Auditing***
- ***Accountability***
- ***Monopoly on Force***

Robert Gezelter
Software Consultant

NOTES

Security Eco-system

A Firewall (or Firewalls) do not exist in a vacuum, they are part and parcel of the entire security plan.

Robert Gezelter
Software Consultant

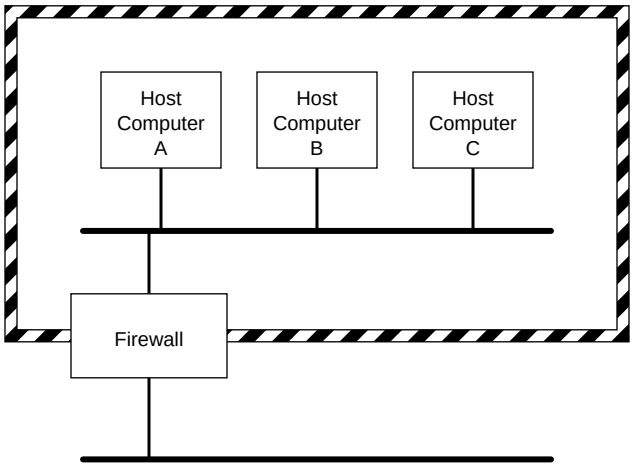
Security Eco-system

Before you can sit down to plan your configuration, you need to well understand your environment.

Robert Gezelter
Software Consultant

NOTES

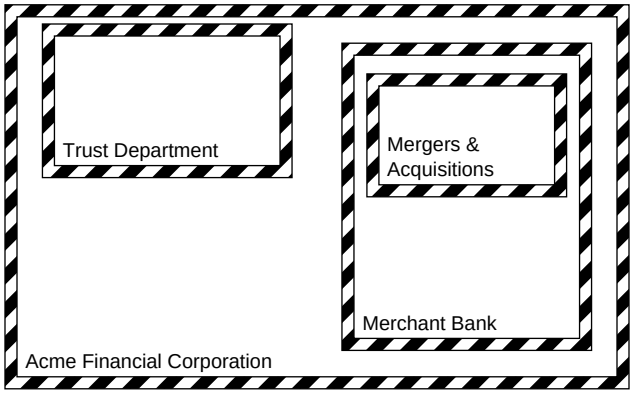
Common Corporate Model



Implementing Firewalls & Proxy Servers
Slide 26

Robert Gezelter
Software Consultant

Common Corporate Reality



Implementing Firewalls & Proxy Servers
Slide 27

Robert Gezelter
Software Consultant

NOTES

Complementary Technologies/Strategies

- ***Hidden Subnets (RFC 1597)***
- ***Virtual Private Networks***
- ***Multi-level DNS***
- ***DHCP restrictions***

Robert Gezelter
Software Consultant

Hidden Subnetworks ÑRFC 159

Robert Gezelter
Software Consultant

NOTES

"Overall, he judged it to be better to be invisible than agile ..."

– Red Storm Rising

Robert Gezelter
Software Consultant

Routers filter packets based upon source and destination addresses and protocol type. Their efficacy is limited.

Robert Gezelter
Software Consultant

NOTES

Firewalls (bastion hosts) should be the exclusive "ports of entry" into your internal network.

Many assets are now addressable via IP, from printers to PBXes. It is highly undesireable that most of these resources be accessable from outside the security perimeter.

Robert Gezelter
Software Consultant

These concerns also apply to nested security environments.

Robert Gezelter
Software Consultant

NOTES

Enter RFC 1597 –
Address Allocation for Private Internets

Robert Gezelter
Software Consultant

RFC 1597 is a scheme which reserves a portion of the IPv4 address space for guaranteed internal use in non-publicly addressible networks.

Robert Gezelter
Software Consultant

NOTES

What is reserved by RFC 1597?

Guaranteed non-public allocation of:

- ***1 Class A Address Block (10.0.0.0 – 10.255.255.255)***
- ***16 Class B Address Blocks (172.16.0.0 – 172.131.255.255)***
- ***255 Class C Address Blocks (192.168.0.0 – 192.168.255.255)***

Robert Gezelter
Software Consultant

RFC 1597 Intent

Permit the connection of large numbers of local devices to LANs via IP without requiring every LAN to hold a Class A address space. It is worth noting that even a private residence could easily overflow a Class C address space.

Robert Gezelter
Software Consultant

NOTES

Implications of RFC 1597

- ***Repeatedly sub-divideable***
- ***internal nodes (workstations, servers, PCs) cannot connect to outside servers EXCEPT through an approved application proxy on an outside addressable host.***
- ***inbound connections must go through approved proxies on the (externally visible) gateways***
- ***internal nodes need not be renumbered due to changes in externally visible address ranges caused by CIDR adjustments and/or access provider changes.***

Robert Gezelter
Software Consultant

Router Configuration

- ***Access Providers should filter the RFC 1597 Address Blocks***
- ***Nested internal routers should filter addresses***
- ***Your router outside your firewall should filter RFC 1597 addresses***

Robert Gezelter
Software Consultant

NOTES

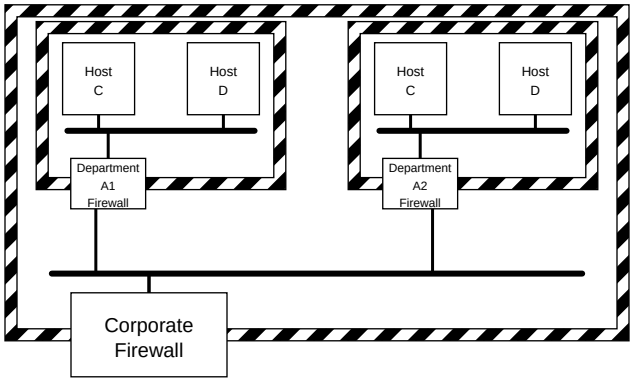
Router Implications

- ***Internal hosts (possibly nested) are invisible to systems outside the firewall***
- ***Even if your router fails, the from address is ambiguous***
- ***The previous note is not as safe as might be perceived, an attack on your link might be feasible.***

Robert Gezelter
Software Consultant

RFC 1597 and Domain Name Services

- ***Internal DNS serving***
- ***External DNS serving***
- ***Implications***

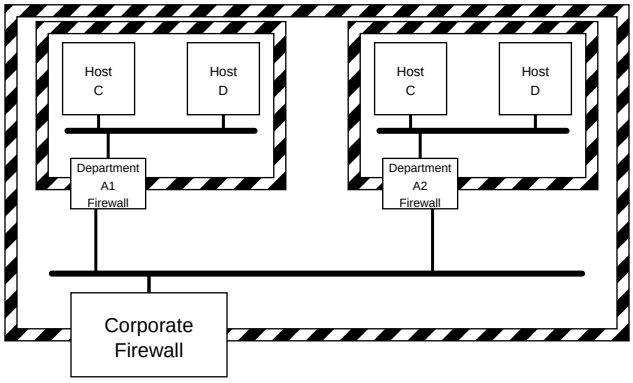


Robert Gezelter
Software Consultant

NOTES

Internal DNS

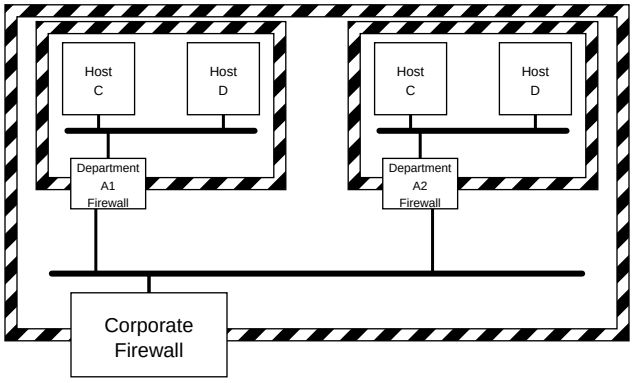
- ***Final authority on nodes inside the firewall***
- ***Uses firewall to resolve external DNS***



Robert Gezelter
Software Consultant

External DNS

- ***all internal mail targets are represented by MX records***
- ***Internal nodes which are not to be addressed may be totally absent from the External DNS***

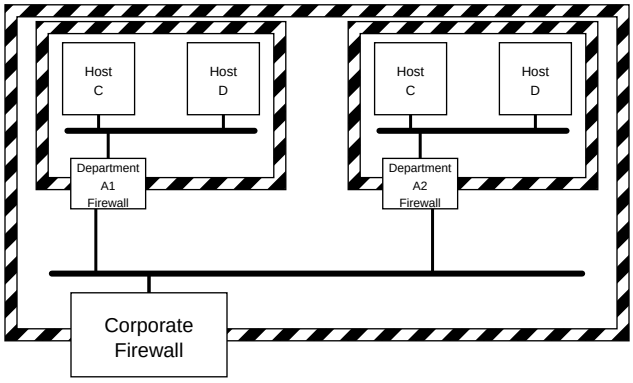


Robert Gezelter
Software Consultant

NOTES

DNS Implications

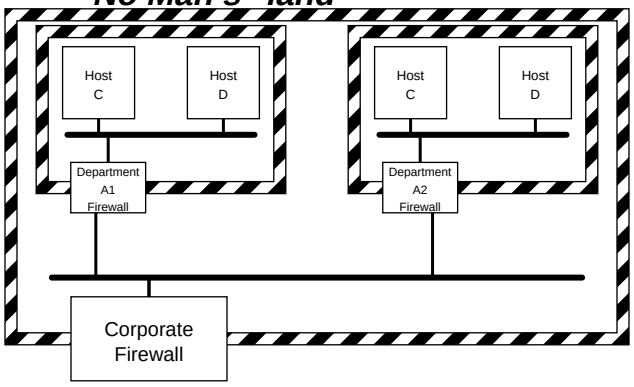
- ***SMTP mail is forced to the route through the gateway***
- ***FTP, TELNET, HTTP cannot even resolve the address of interior systems.***



Robert Gezelter
Software Consultant

Relationship Connectivity

- ***RFC 1597 address can be used together with careful management to protect IP links with business and strategic partners***
- ***Mutual distrust***
- ***"No Man's" land***



Robert Gezelter
Software Consultant

NOTES

Summary

RFC 1597 provides and excellent framework for implementing an environment which enhances the safety support provided by your firewall(s)

Robert Gezelter
Software Consultant

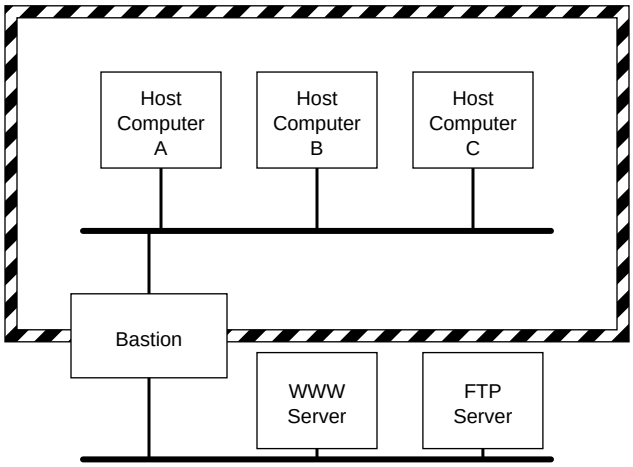
Corporate Strategy

- ***Keep things outside***
- ***Minimize Trust***
- ***Minimize Exposure***
- ***Minimize Firewall use***
- ***Public/Semipublic Outside***
- ***Nest Security/Access Domains***
- ***Parents AND Sibling Domains***

Robert Gezelter
Software Consultant

NOTES

General Corporate Implementation



Robert Gezelter
Software Consultant

Virtual Private Networks

- ***Use Encryption***
- ***Caution: Derived Trust***
- ***Efficient Solution***
- ***Ease of Use***
- ***Make it easy to be good***

Robert Gezelter
Software Consultant

NOTES

Multi-level DNS

- ***Keep inside invisible***
- ***Mail headers***
- ***Fake Authorities***
- ***Ambiguities***

Robert Gezelter
Software Consultant

DHCP restrictions

- ***Within domain***
- ***Within physical department***
- ***DO NOT Proxy***
- ***Point of attack***
- ***Availability issues***

Robert Gezelter
Software Consultant

NOTES

Bibliography

Hutt, Bosworth, Hoytt
"The Computer Security Handbook, 3rd Edition/Updated", John Wiley & So

Internet RFCs

Littman "The Fugitive Game"
Little Brown

Stoll, Clifford "The Cuckoo's Egg"

Robert Gezelter
Software Consultant

NOTES