Unite Technology Conference

Basic Network Security For The ClearPath MCP User

Michael S. Recant
MGS, Inc.

Session AS4076
9:15am - 10:15am
Thursday, November 8, 2001

MGS INC
Computer Business Solutions

Introduction

MGS, Inc. is a ClearPath MCP software development and consulting firm

remote computer access is critical to our business

MGS INC
Computer Business Solutions

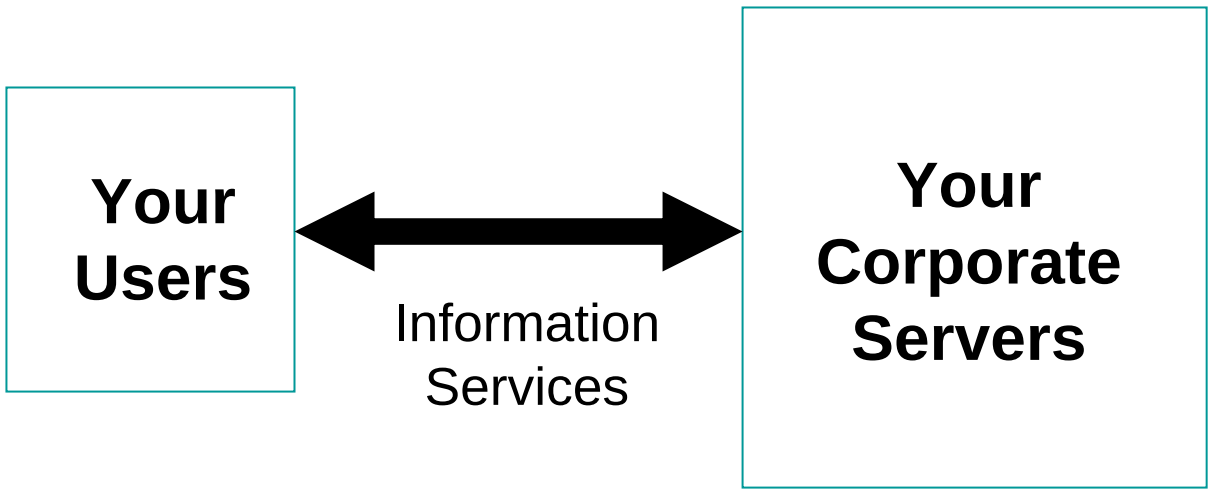
Introduction

- Introduction
- The Business Problem
- Communications Technology
  - Point of Control
  - TCP/IP Basics
- Access Control
  - “Guarded Gate” Strategy
  - “Extended Office” Strategy
- Security Considerations
- References

MGS INC
Computer Business Solutions

The Business Problem

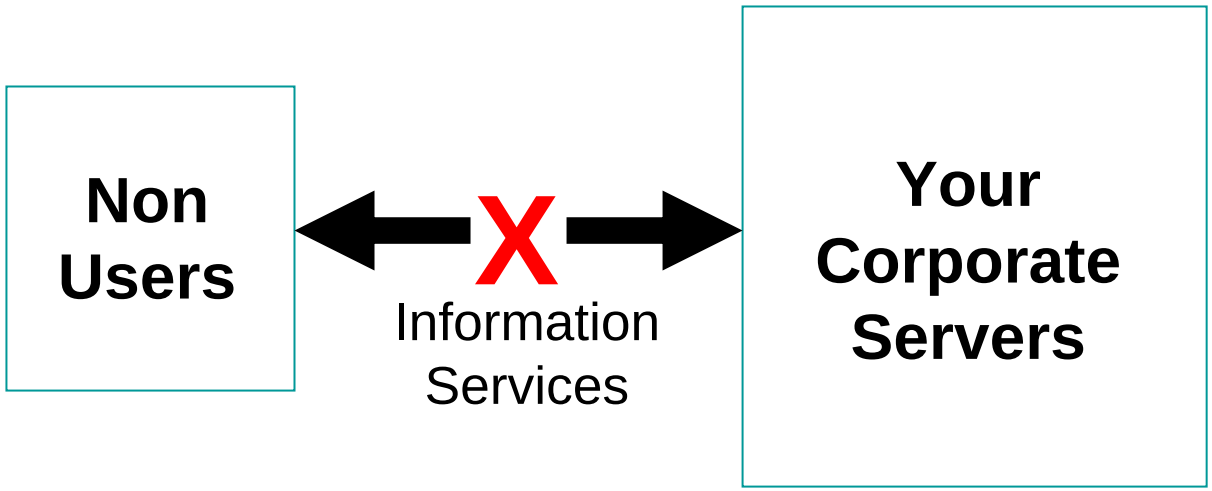
Your job is to provide ....



MGS INC
Computer Business Solutions

The Business Problem

Your job is also to insure ....

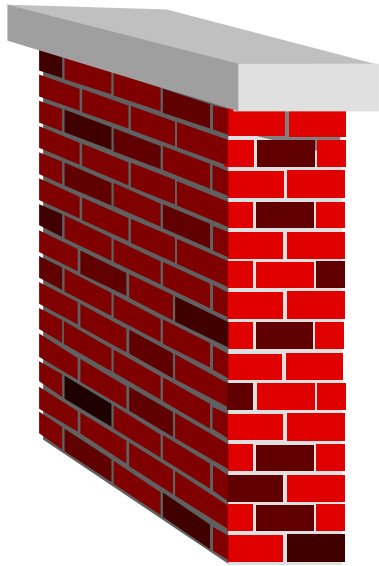


MGS INC
Computer Business Solutions

The Business Problem

The historical approach ....

Your Users

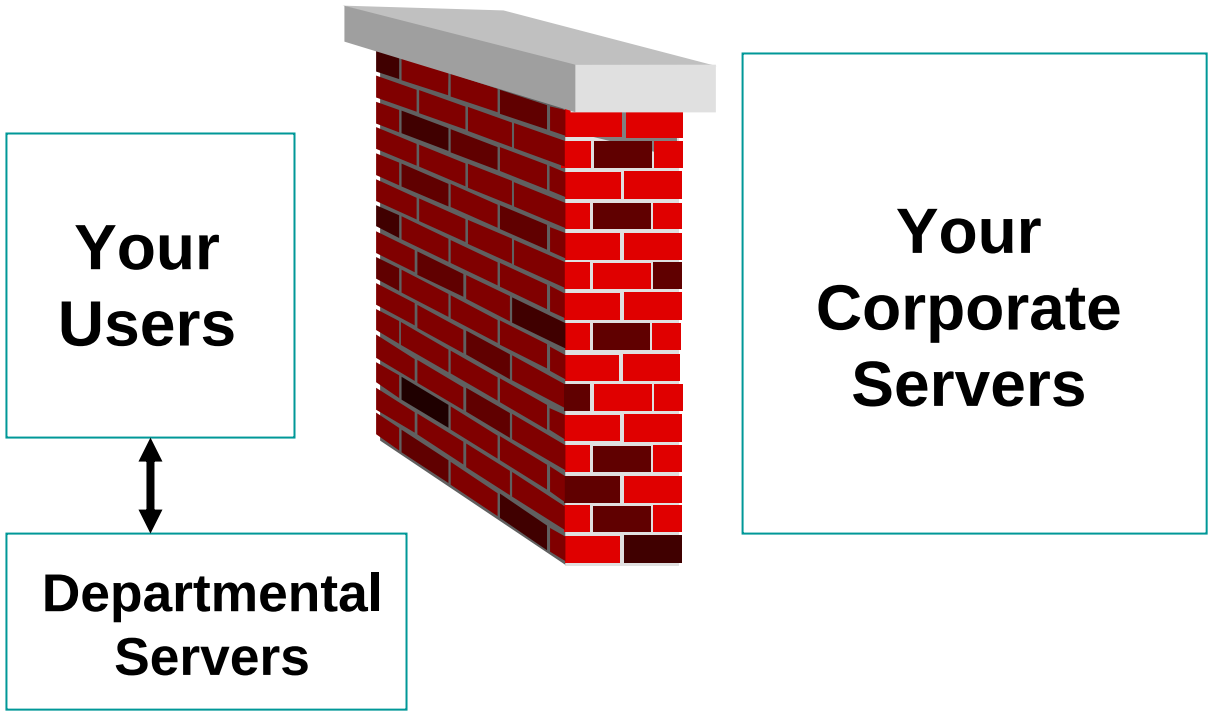


Your Corporate Servers

MGS INC
Computer Business Solutions

The Business Problem

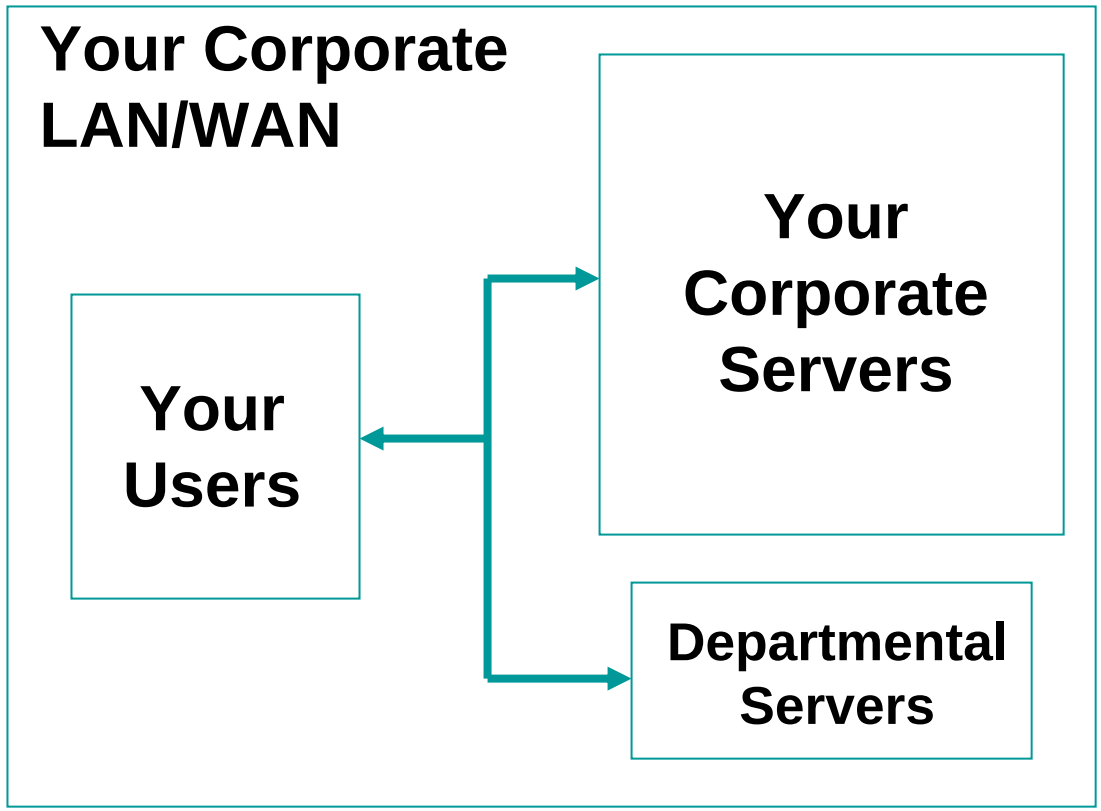
The historical response ....



MGS INC
Computer Business Solutions

The Business Problem

The solution ....



MGS INC
Computer Business Solutions

The Business Problem

User

User

User

User

User

User

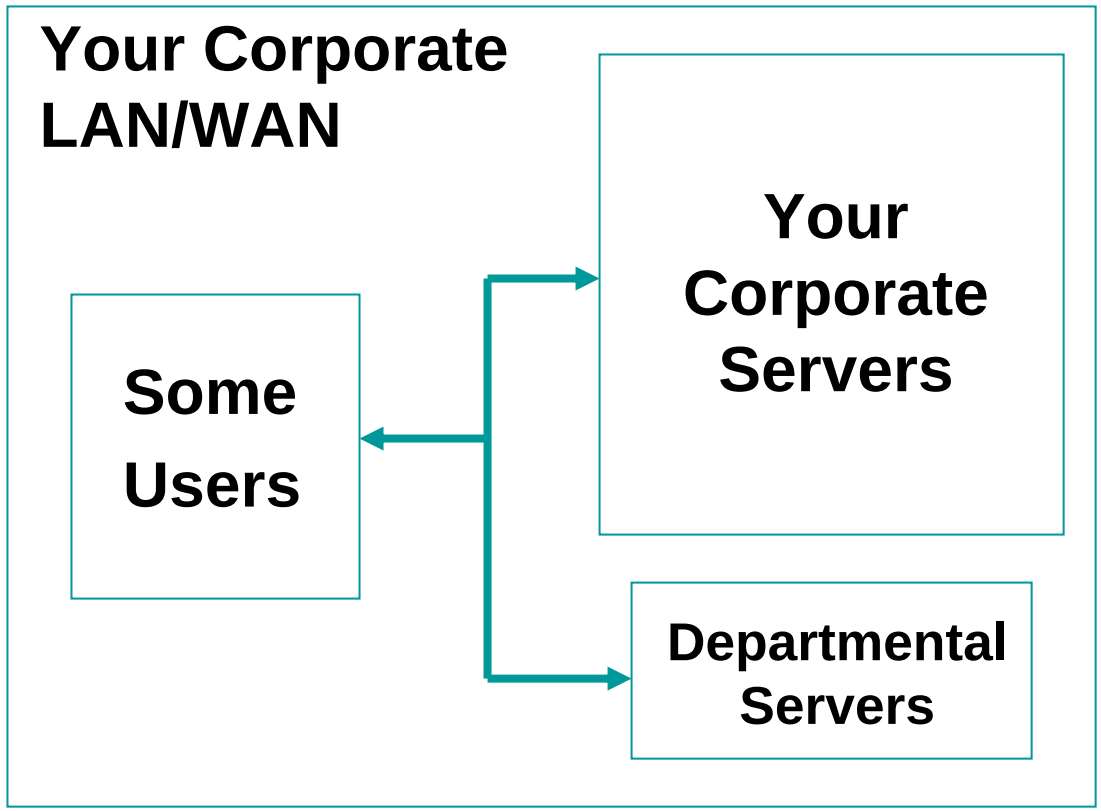
User

User

User

User

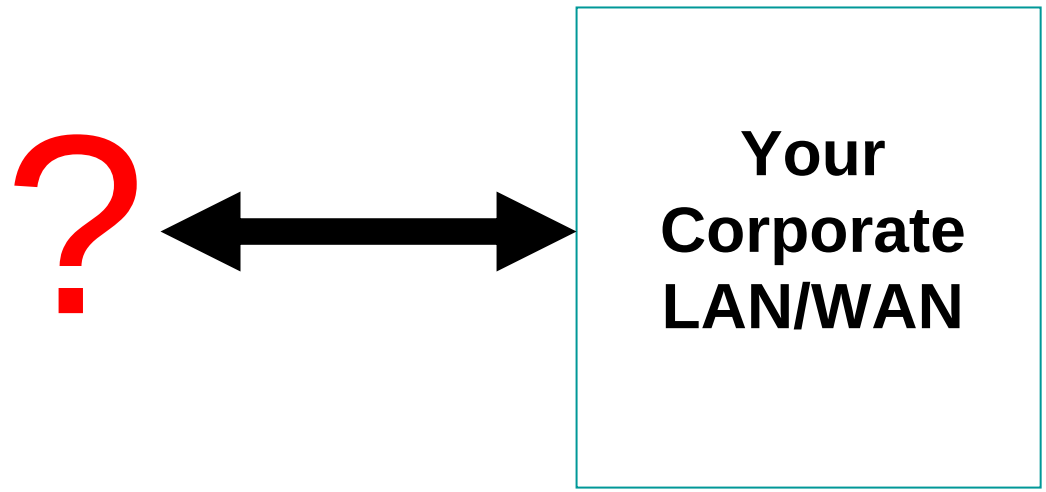
But now there is a new problem ...



MGS INC
Computer Business Solutions

The Business Problem

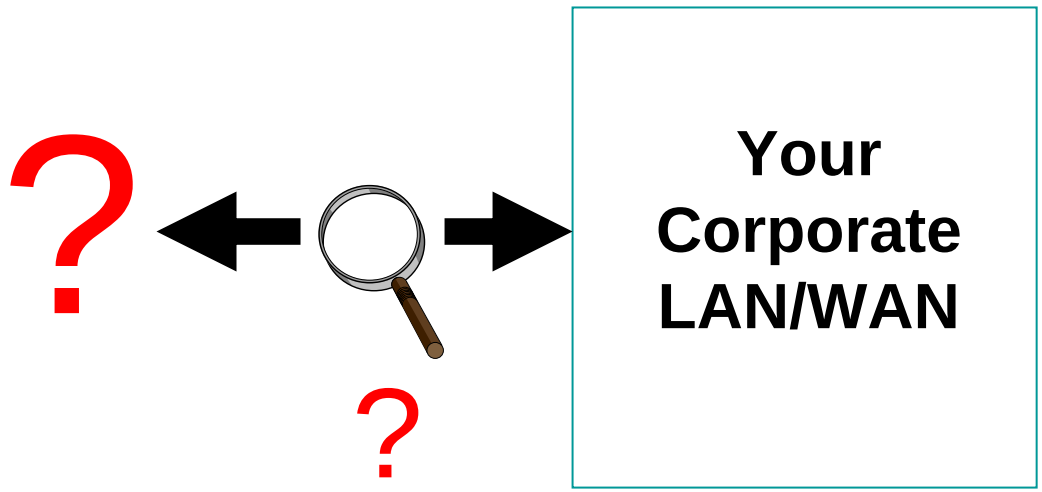
The problem has a name, it is called the Internet ....



MGS INC
Computer Business Solutions

The Business Problem

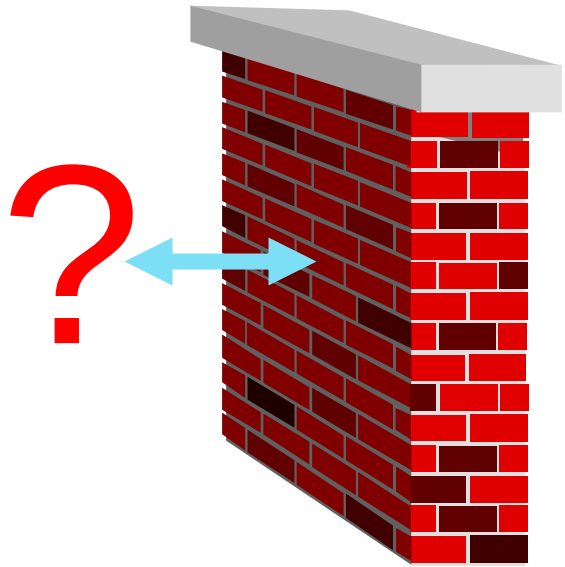
And the problem is worse than you think ....



MGS INC
Computer Business Solutions

The Business Problem

The perfect IS solution ....

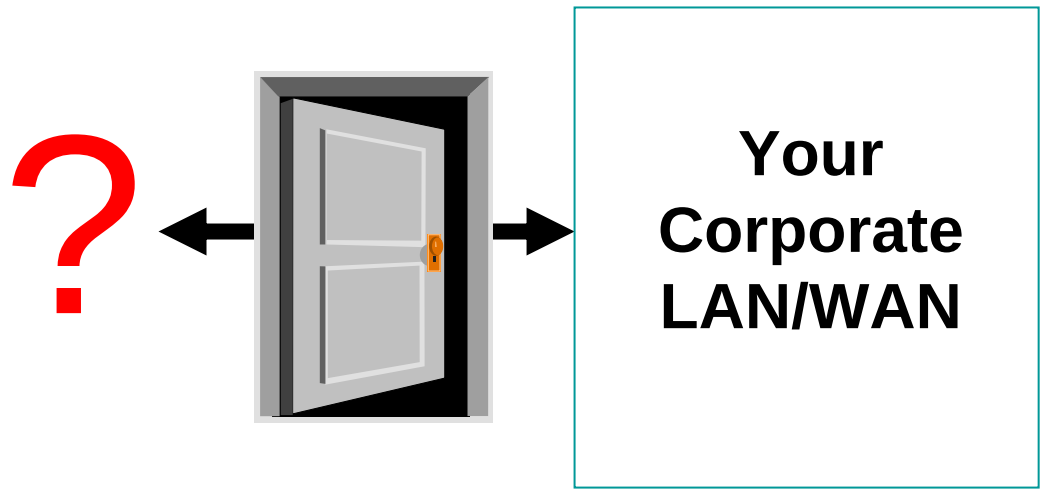


Your Corporate LAN/WAN

MGS INC
Computer Business Solutions

The Business Problem

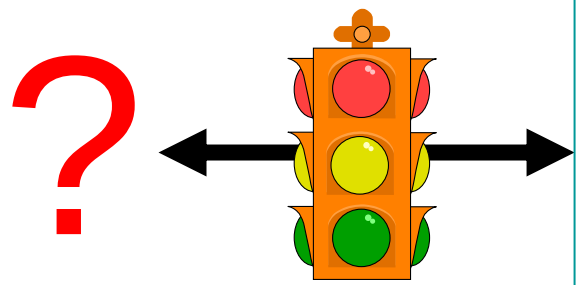
The perfect user solution ....



MGS INC
Computer Business Solutions

The Business Problem

Your job is to meet both goals ....



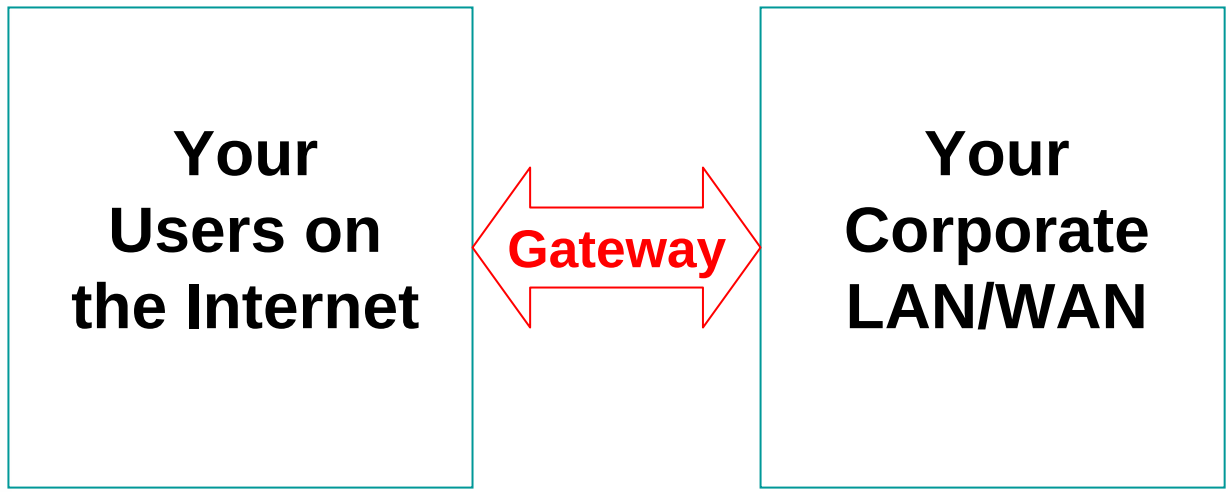
Your Corporate LAN/WAN

.... but how can you do that?

MGS INC
Computer Business Solutions

Communications Technology - Point of Control

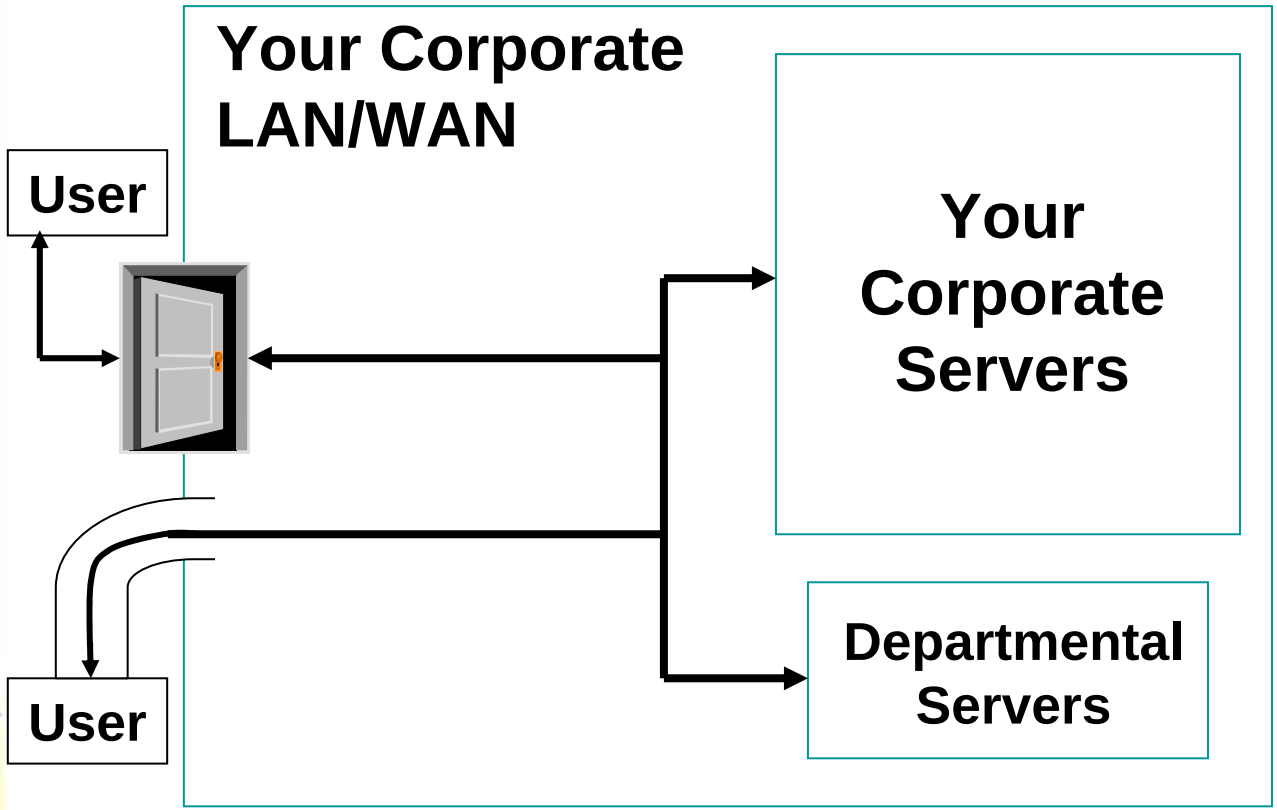
Somewhere there is a boundary ....



MGS INC
Computer Business Solutions

Communications Technology - Point of Control

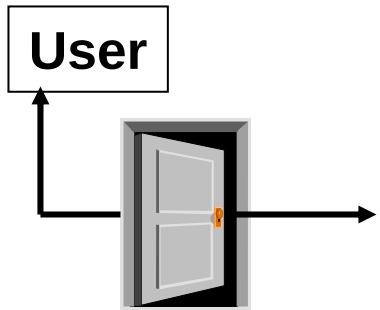
Control access through the boundary



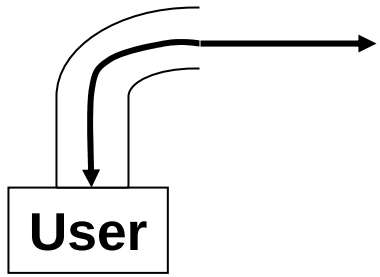
MGS INC
Computer Business Solutions

Communications Technology - Point of Control

The two standard techniques are ....



Guarded Gate



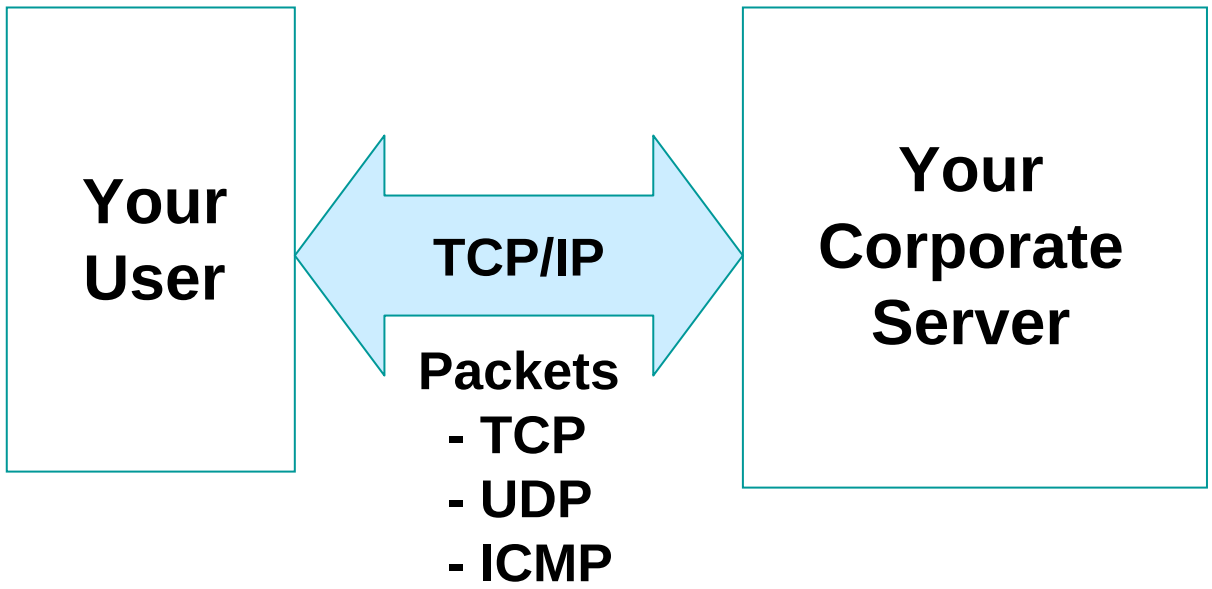
Extended Office

but first, what actually goes through the boundary?

MGS INC
Computer Business Solutions

Communications Technology - TCP/IP Basics

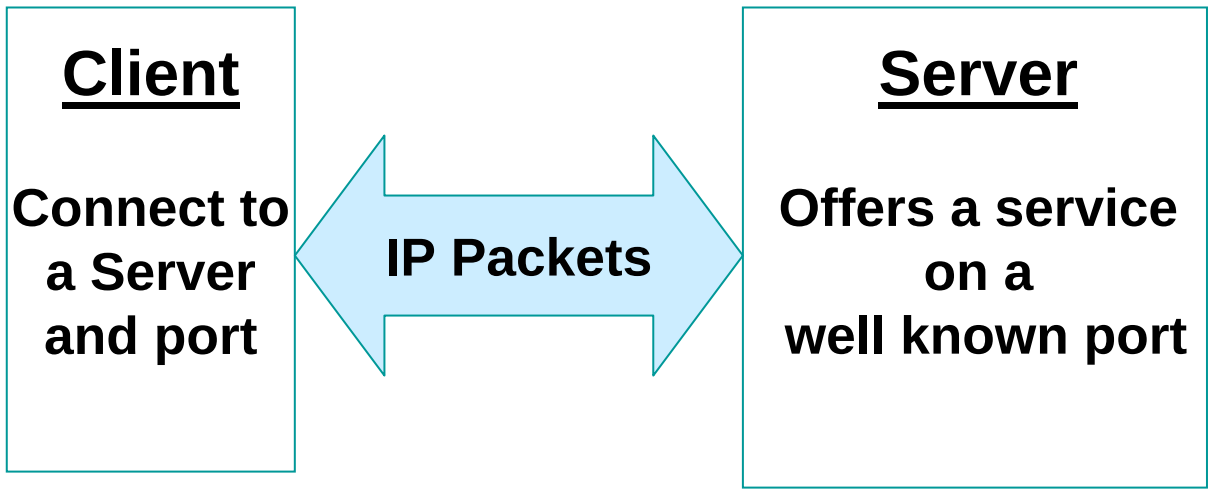
Current communications technology is based on TCP/IP



MGS INC
Computer Business Solutions

Communications Technology - TCP/IP Basics

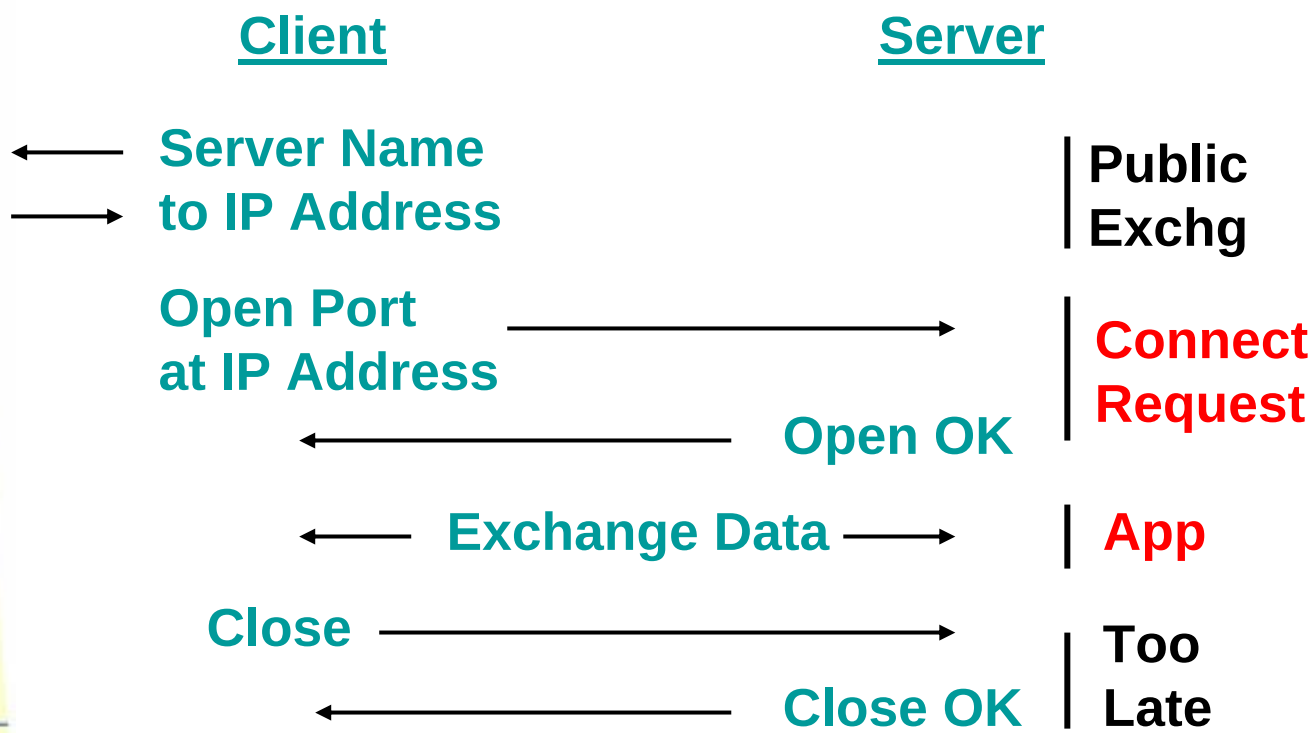
TCP Client software connects to services offered by TCP Server software



MGS INC
Computer Business Solutions

Communications Technology - TCP/IP Basics

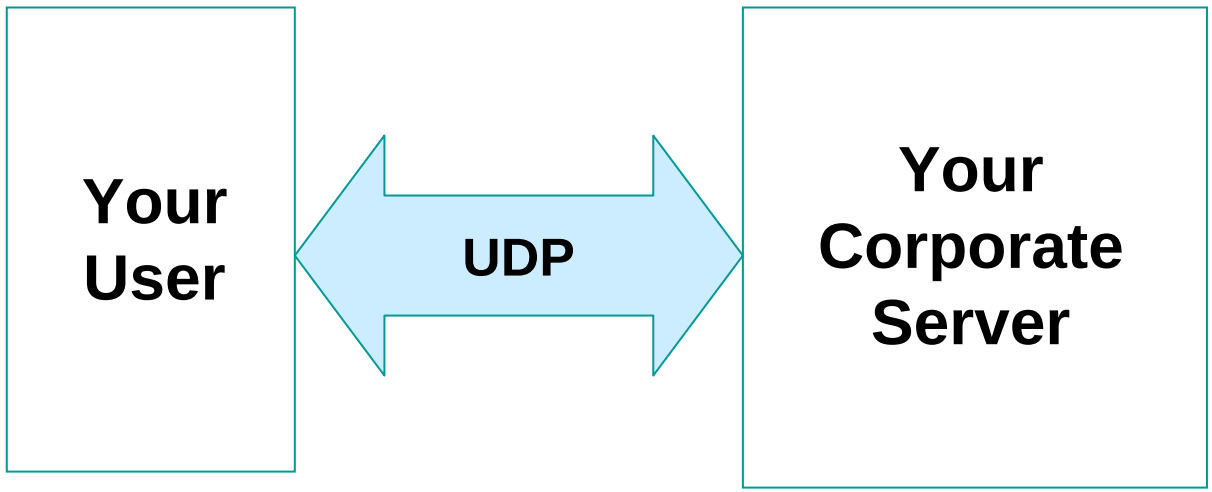
TCP communications process



MGS INC
Computer Business Solutions

Communications Technology - TCP/IP Basics

UDP client/server software interacts using “connectionless” communications



MGS INC
Computer Business Solutions

Communications Technology - TCP/IP Basics

UDP communications process

MGS INC
Computer Business Solutions

Communications Technology - TCP/IP Basics

ICMP exchanges are similar to UDP

MGS INC
Computer Business Solutions

Access Control - Overview

Two basic access control strategies

- "Guarded Gate" Strategy
  - Firewall
  - Application Level Security
- "Extended Office" Strategy
  - Virtual Private Network
  - Internet Protocol Security

Access Control - Guarded Gate Strategy

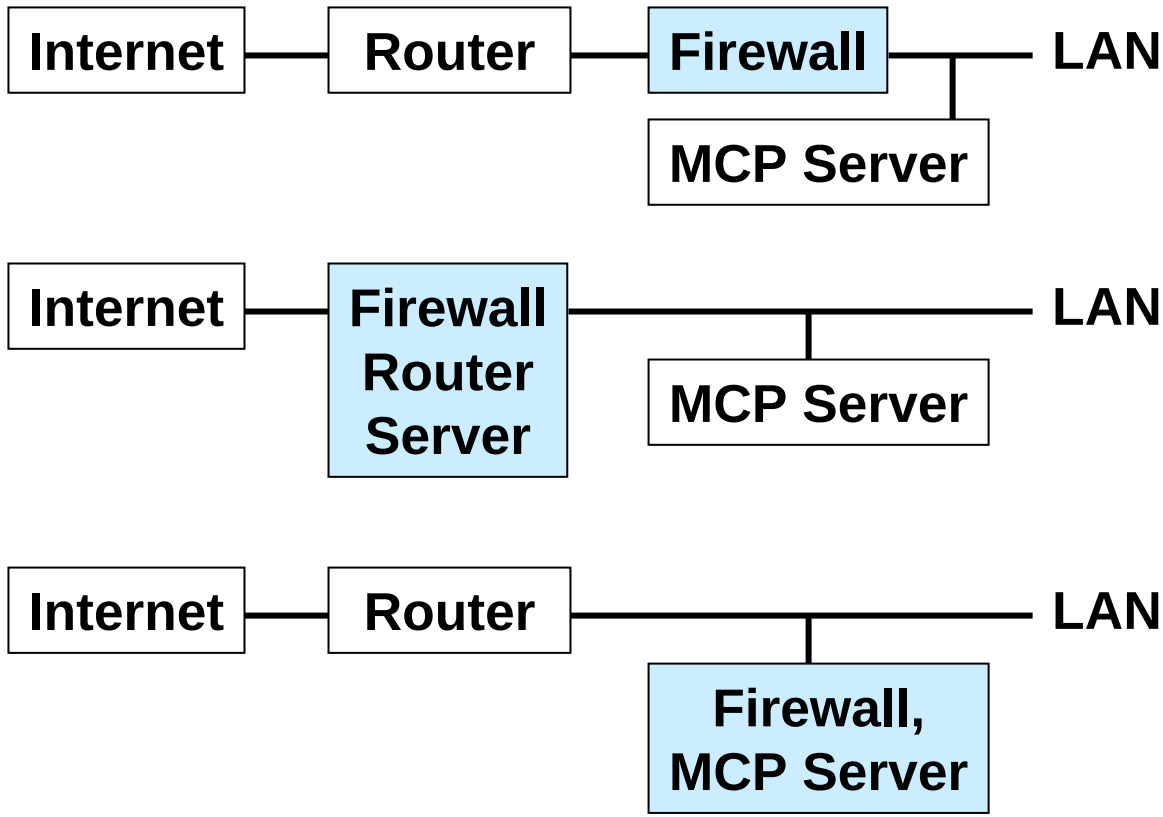
A Firewall is used to control server access

- Firewall is placed between the Internet and your Corporate data processing
- Looks at each individual TCP connection to decide if it is OK
- Looks at an individual UDP or ICMP packet to decide if it is OK

MGS INC
Computer Business Solutions

Access Control - Guarded Gate Strategy

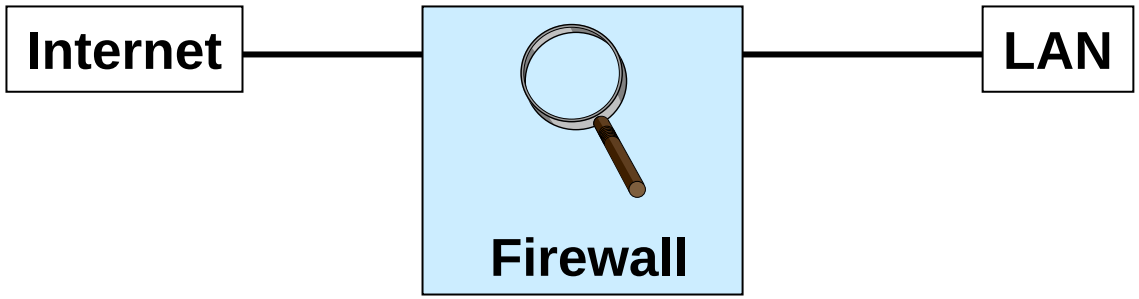
Where can you put the Firewall?



MGS INC
Computer Business Solutions

Access Control - Guarded Gate Strategy

The Firewall inspects all TCP/IP packets



- Server IP Address
- Server Port number
- Client IP Address
- Client Port number
- TCP, UDP or ICMP

MGS INC
Computer Business Solutions

Access Control - Guarded Gate Strategy

Firewall Considerations

- What decisions can be made?
  - The default should be to always deny access
  - Allow unrestricted access to “public” services
  - Allow limited access to “private” services by “known” IP Addr
- Remember that data is visible unless the application uses encryption

Access Control - Guarded Gate Strategy

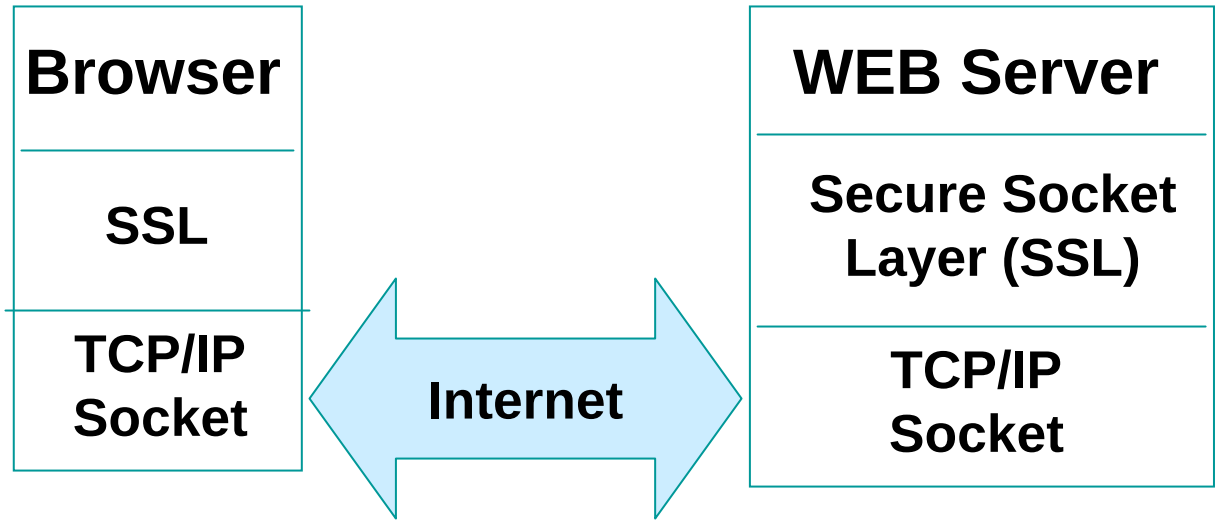
Application level security limits are imposed by the individual server/app

- Requires application modifications
- Does not secure other servers and other applications
- Client and server must be security aware
- SSL provides security for WEB Browser/Server exchanges

MGS INC
Computer Business Solutions

Access Control - Guarded Gate Strategy

Application-to-Application is secure ....



.... but nothing else is

MGS INC
Computer Business Solutions

Access Control - Extended Office Strategy

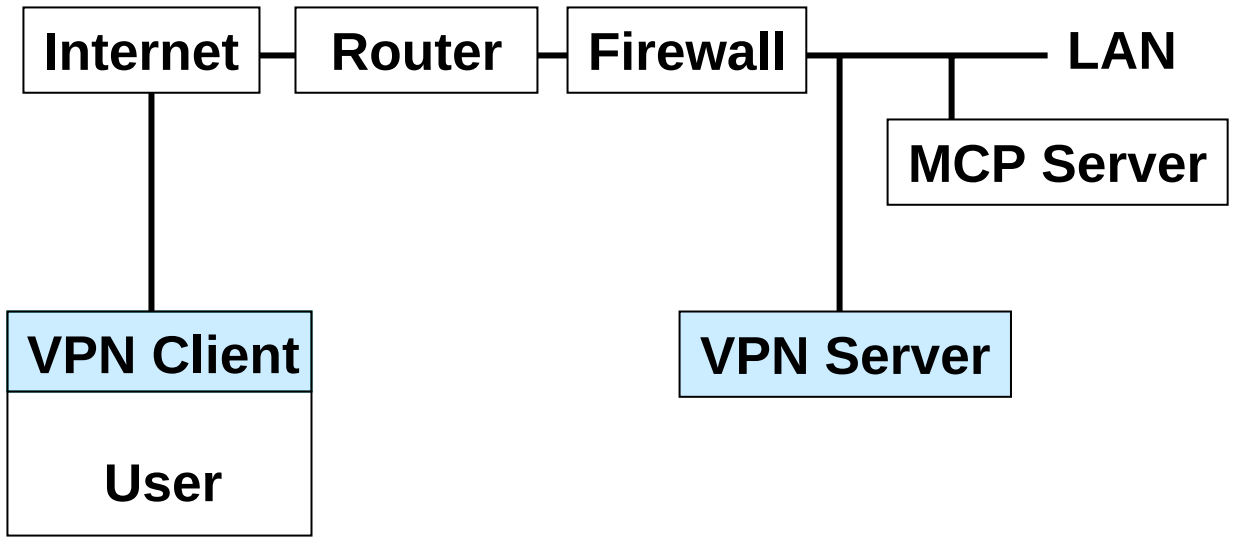
Virtual Private Network (VPN)

- Provides a secure “tunnel” through the Internet
- TCP/IP is unaware of the “tunnel”
- TCP/IP communication is not restricted

MGS INC
Computer Business Solutions

Access Control - Extended Office Strategy

Where do you put the VPN “tunnel”?



VPN - Virtual Private Network

MGS INC
Computer Business Solutions

Access Control - Extended Office Strategy

VPN Considerations

- User appears to be on the Corporate LAN/WAN
- VPN client/server can provide authentication and encryption
- User's PC must be considered a physical extension of the "office"
- VPN client environment
  - must not be replicable
  - requires external password

MGS INC
Computer Business Solutions

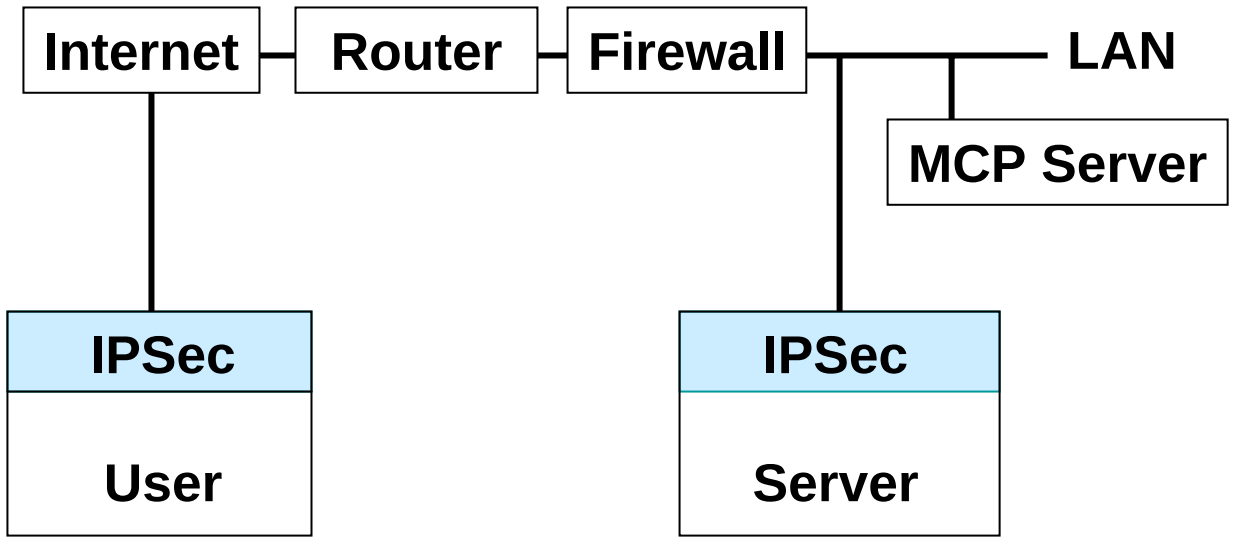
Access Control - Extended Office Strategy

Internet Protocol Security (IPSec)

- Provides security encapsulation for TCP/IP communication
- TCP/IP is unaware of the encapsulation
- TCP/IP communication is not restricted

Access Control - Extended Office Strategy

Secure computer-to-computer communications



MGS INC
Computer Business Solutions

Access Control - Extended Office Strategy

IPSec Considerations

- Secure computer-to-computer link that provides authentication and encryption
- Applications are unaware of IPSec
- Runs below the TCP/IP protocol stack (OS Support required)
- May require participation in a security domain
- Firewall/NAT issues

MGS INC
Computer Business Solutions

Security Considerations

Overall Security Goals

- Authentication - is the user who he claims to be and what access is he allowed
- Encryption - provides data integrity, replay prevention and eliminates the possibility of eavesdropping
- Non-Repudiation - provides verification so the sender cannot deny sending the message

Security Considerations

Guarded Gate Strategy

- Only exposes specific services
- Identify “public” services like Mail, Web, FTP as they require monitoring
- Do not “publicly” expose services that provide general access
  - weak usercode/password
  - hard to audit
  - Example: TELNET

Security Considerations

- Guarded Gate Strategy
  - Attach a revocable limit to “private” services
    - Usercode/password is not enough
    - plan for terminated employee
  - Understand your application’s security
    - TELNET
    - FTP
    - WEB

Security Considerations

Guarded Gate Strategy

- Don’t expose Microsoft’s networking services or WinRPC
  - Limited by many ISPs
  - Many security bugs
  - Near impossible to audit
- Enable PING/TRACEROUTE for all exposed servers

Security Considerations

Extended Office Strategy

- The user PC is now an extension of the office
- When terminating an employee get his PC when you get his office key
- Use encryption
- If possible, limit user access through VPN
- If possible attach an IP Address or hostname to each VPN user

MGS INC
Computer Business Solutions

Security Considerations

ClearPath MCP Considerations

- Supported ClearPath MCP services/port
  - FTP 21
  - TELNET 23
  - SMTP 25
  - WEB 80
  - HOSTS2 81
  - ONC+RPC 111
  - NXEDIT 129
  - NETBIOS 139
  - SNMP 161
  - ??? 279
  - LPD 515
  - WINRPC ???

Security Considerations

ClearPath MCP Considerations

- In general, do not open a ClearPath MCP server to the Internet
- WEB can be safely exposed
- SSL supported
- Only expose required services
- Limit access to exposed services
- IPSec not supported

Reference Material

- TCP/IP Illustrated, Vol 1 by W. Richard Stevens, Addison-Wesley
- TCP/IP Illustrated, Vol 2 by W. Richard Stevens, Addison-Wesley
- Business Data Communications and Networking by Fitzgerald & Dennis, John Wiley & Sons, Inc
- TCP/IP Network Administration by Craig Hunt, O'Reilly & Associates, Inc.
- Microsoft Windows 2000 Server TCP/IP Core Networking Guide (Windows 2000 Resource Kit), Microsoft Press
- Unisys e-@action ClearPath Enterprise Servers Security Administration Guide for MCP 6.0 (860 0973-407)

Additional Questions?

Michael S. Recant
VP Software Development

MGS, Inc.
10901 Trade Road, Suite B
Richmond, VA 23236

Voice: (804)379-0230
Fax: (804)379-1299
Email: Mike.Recant@mgsinc.com
Web: www.mgsinc.com

This presentation is available on our WEB site

MGS INC
Computer Business Solutions

Unite Technology Conference

Basic Network Security For The ClearPath MCP User

MGS INC
Computer Business Solutions