Management Through Firewalls

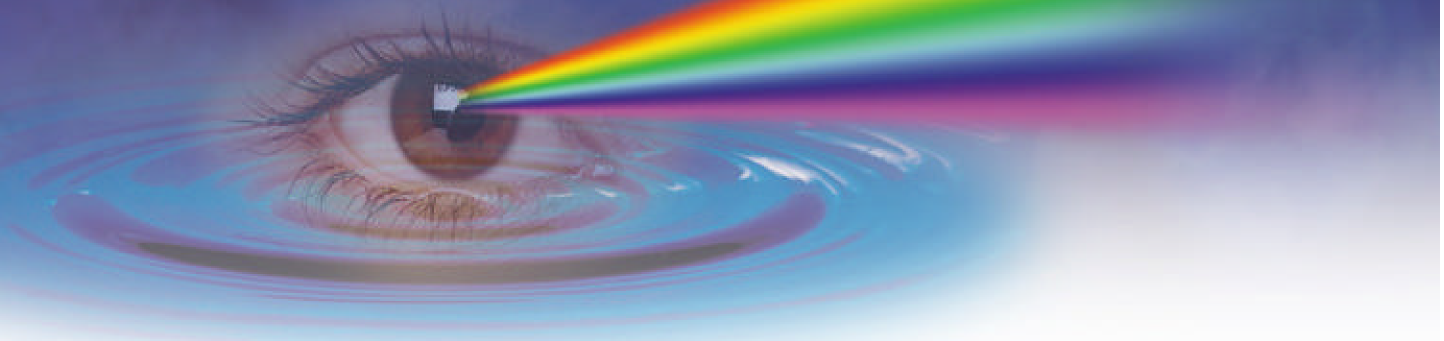
Bob Kelly

NSM Practice Manager

&

Solutions Architect

Melillo Consulting, Inc.



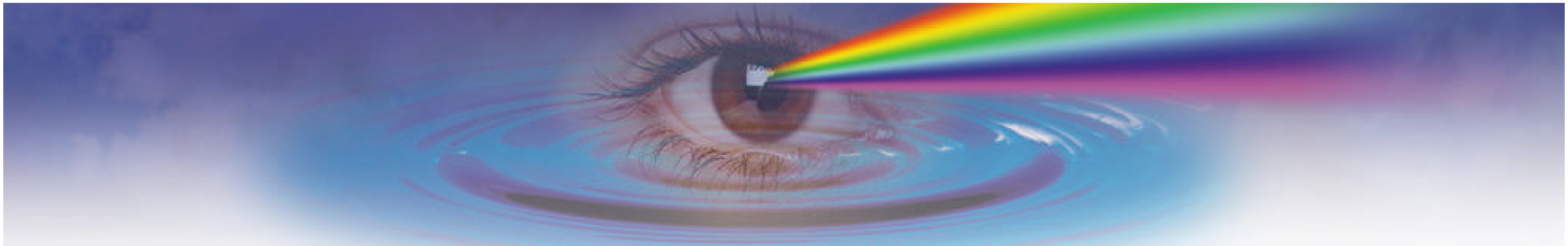
MELILLO CONSULTING, INC.
THE POWER OF SOLUTIONS

What is a Firewall?

- Purpose of a Firewall
- What can Firewalls do for me?
- What can’t Firewalls do for me?
- Why do we need to manage the devices on the other side of a Firewall?

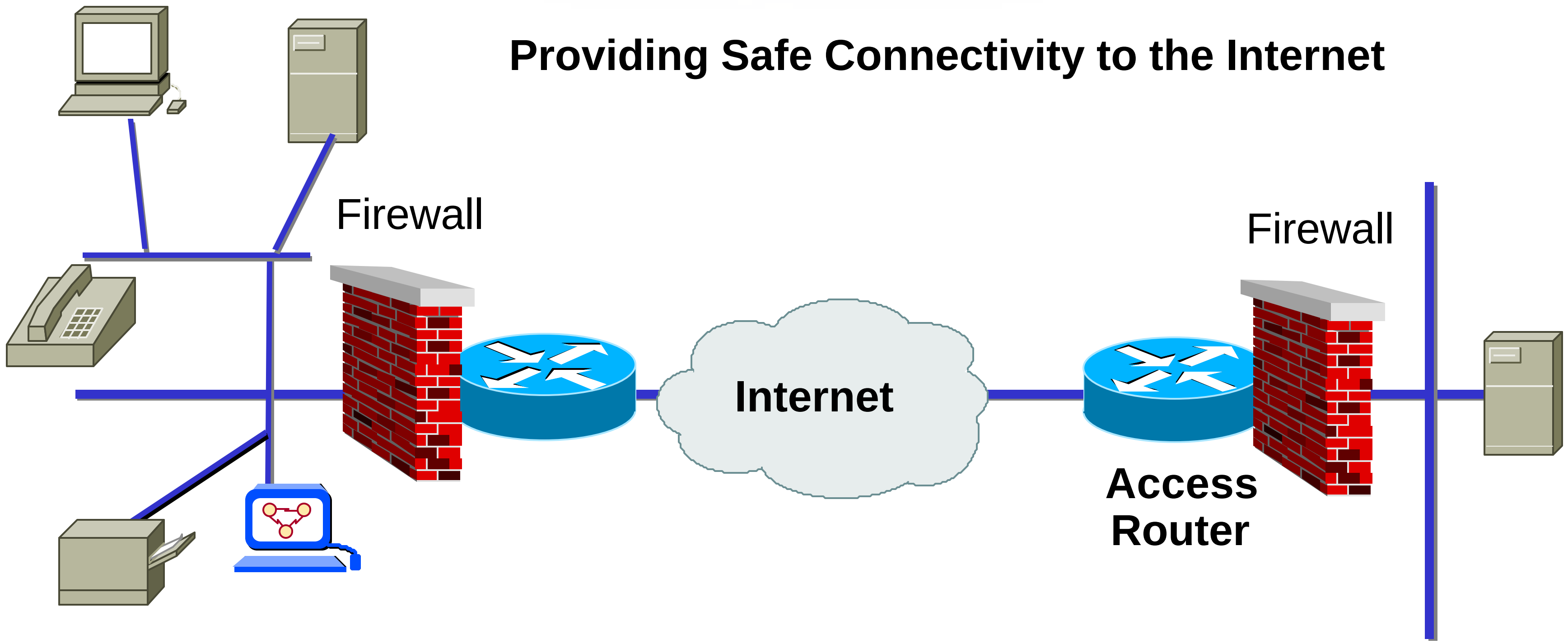
Firewalls, Where and Why are They Used ?

- Internet
- Intranet
- eCommerce solutions
- Extranet
  - B2B
  - B2C
- Outsourcing
- Hosting
  - Web Hosting
  - Application Hosting
  - Management Hosting



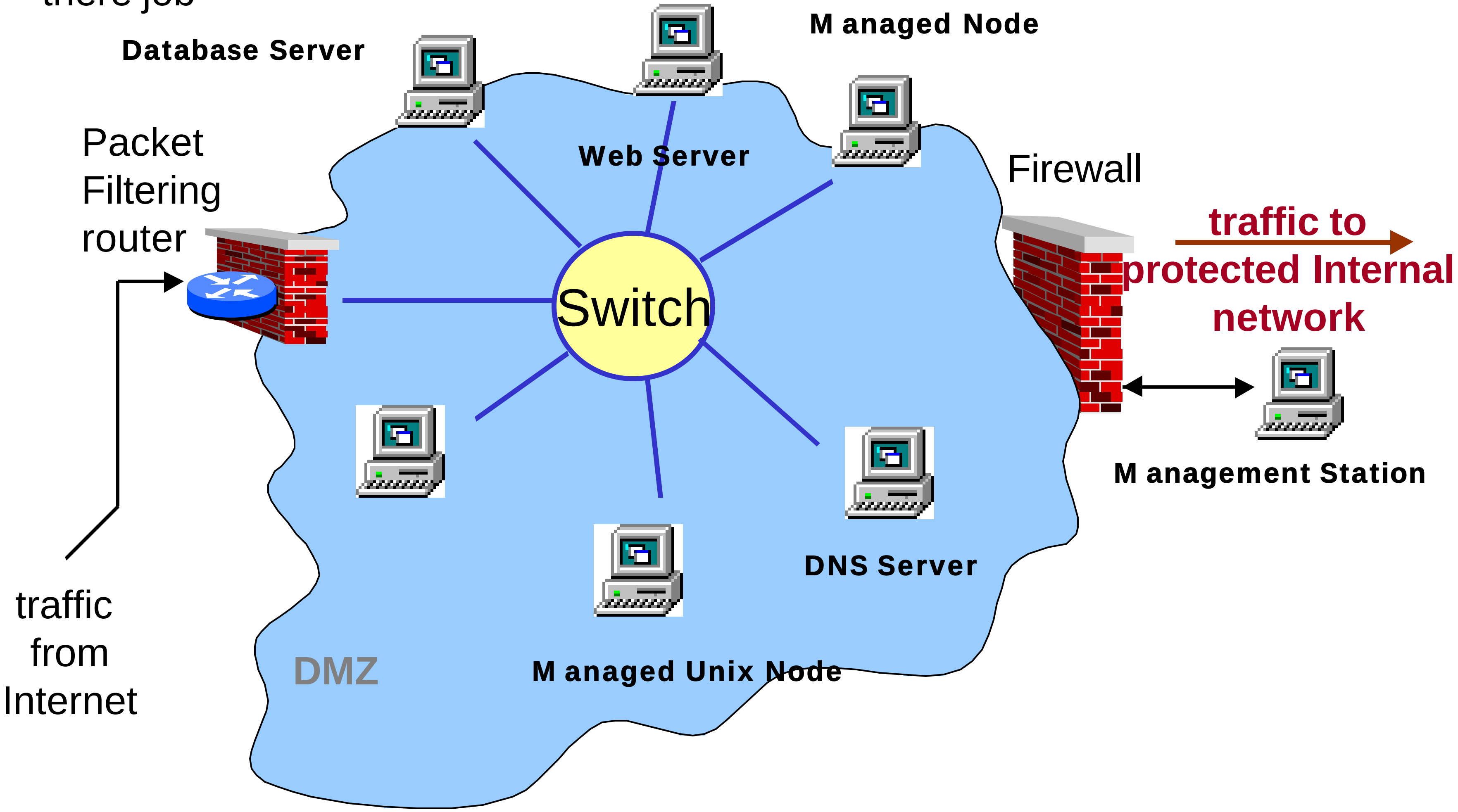
Internet

Providing Safe Connectivity to the Internet



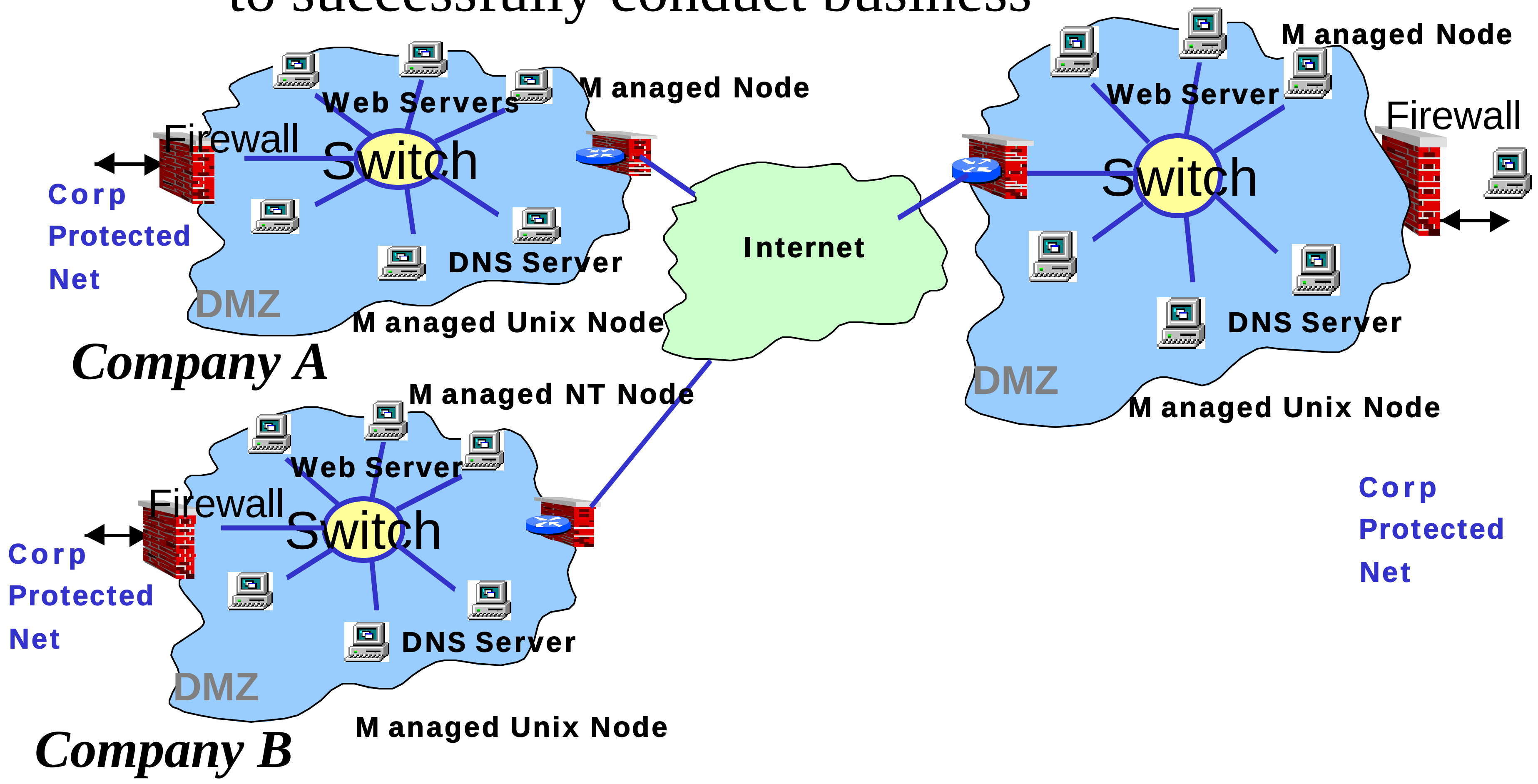
Intranet

Providing your remote users access to the resources they need to perform there job



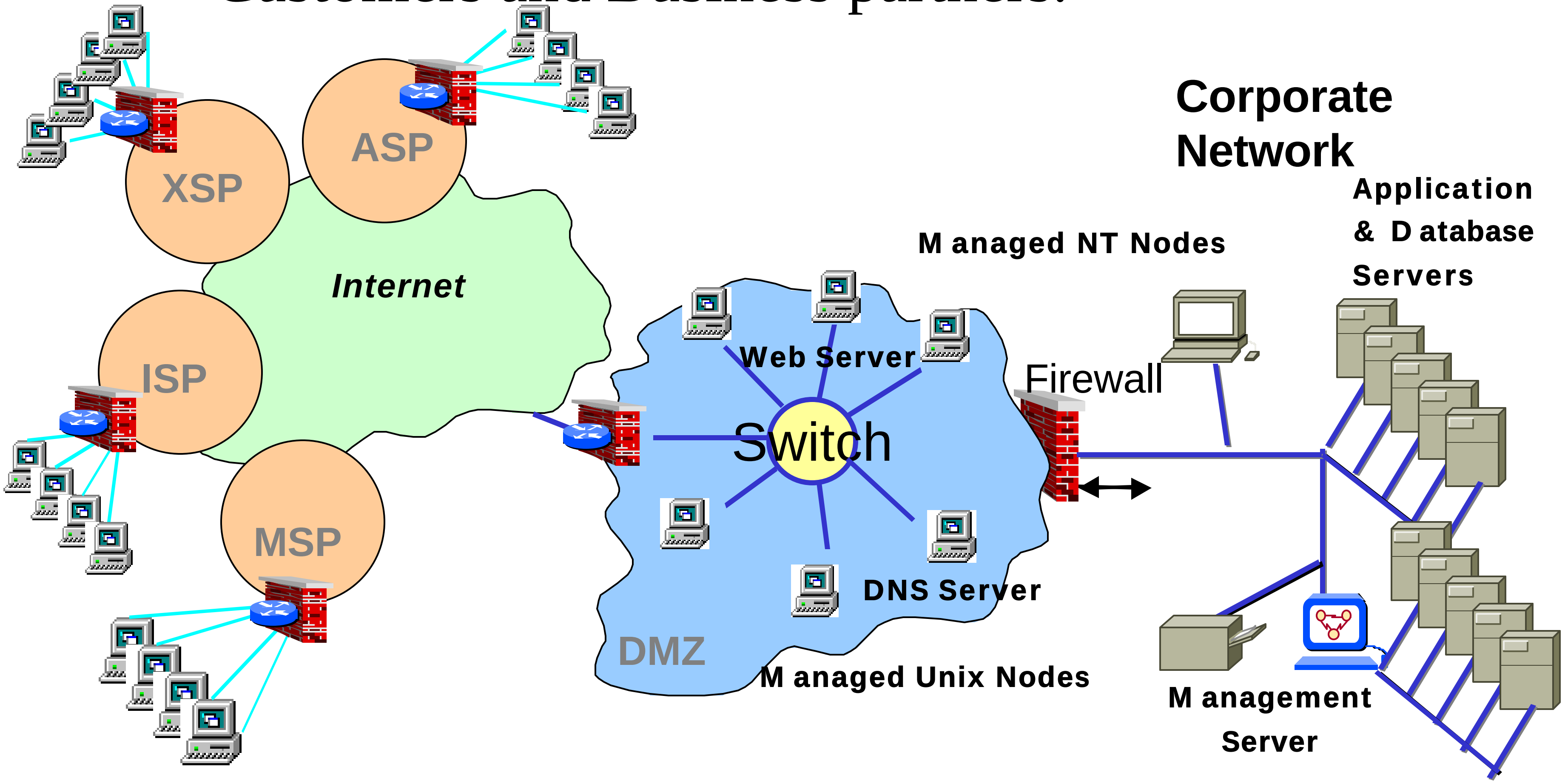
Extranet

Provide your Business partners access to information to successfully conduct business



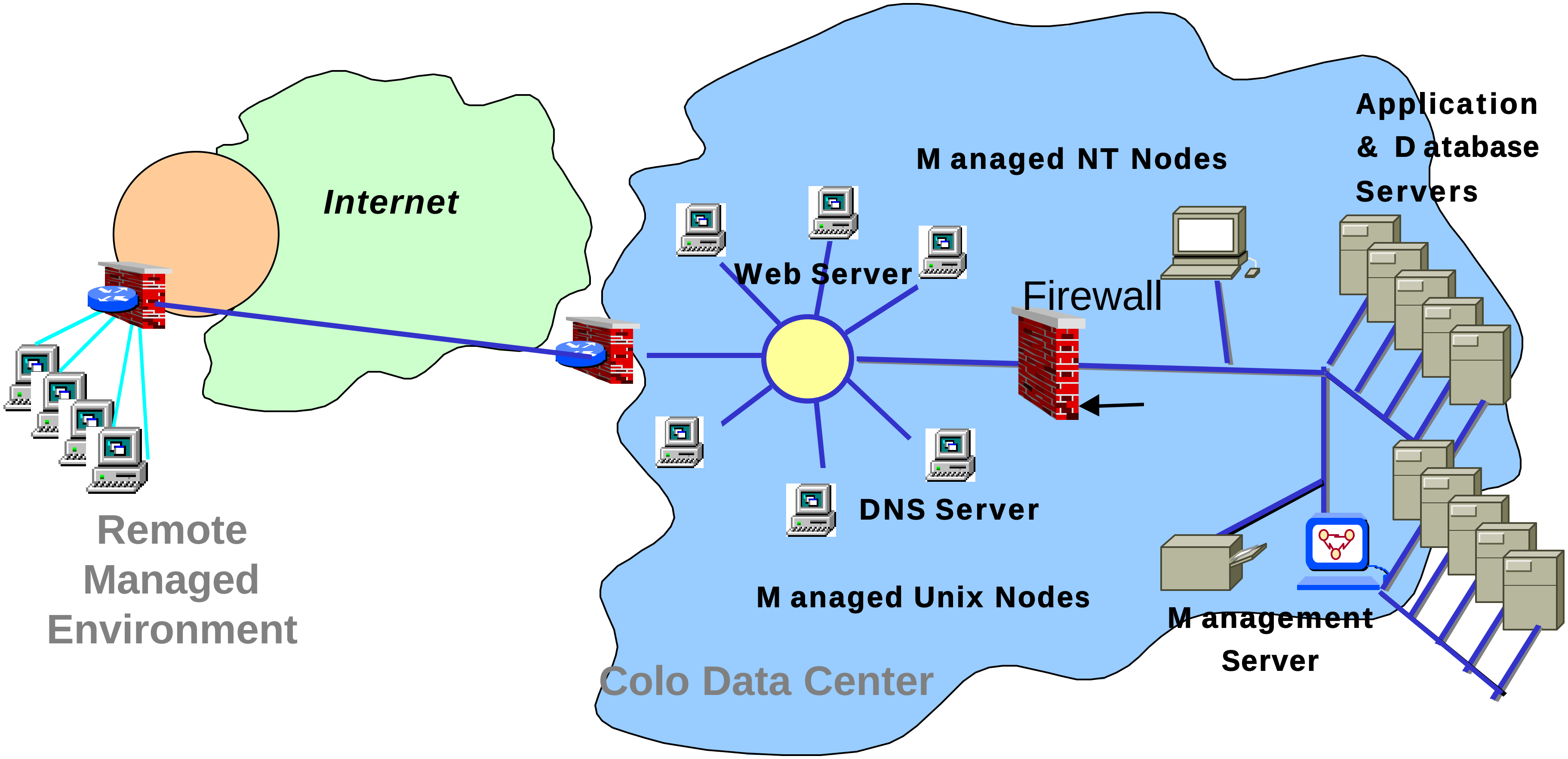
eCommerce

Conduct Business over the Internet, with your Customers and Business partners.



Hosting

Provide Application and System hosting at both a Remote Data Center and at a Companies’ own site



About my Firewall

- Identify the Firewalls in my environment
- What Firewall product am I using?
  - Hardware
  - Software
- What are the capabilities of each product?
- What are the specifics for each device used?
- Is my Firewall using NAT?

Areas Of Management

- Network Management
- Network Performance Management
- Network Device Management
- System Management
- System Performance Management
- Database Management
- Application Management
- Backup & Recovery Management

Management Components

- Components of the Management environment
  - Management Server
  - Managed agent/element
  - User interface
- Understand your Firewall’s configuration
- Be aware of what you are opening up
- Determine if a Management function is critical
- For each Management solution maintain a Firewall configuration requirement list

Network Node Manager and Firewalls

- Communication to Managed Elements
  - ICMP
  - SNMP
  - SNMP Traps
- Management Server to Collection Stations
  - SNMP
  - OV_events
  - Telnet
  - Topology
- User interface to Management Server
  - HTTP, Java, X-Windows

Network Node Manager Firewall Port Requirements

Network Node Manager Firewall ports

Source IP	Destination IP	Protocol	SRC Ports	DST Ports	Description/Service
Mangement Station	Manged element	UDP	1024-65535	161	SNMP
Managed elements	Mangement Station	UDP	1024-65535	162	SNMP Trap
Collection Station	Mangement Station	TCP	1024-65535	162	OV events
Management Station	Manged element	IP	N/A	N/A	ICMP
Management Station	Manged element	TCP	1024-65535	80	HTTP Java GUI
Management Station	Collection Station/ Managed Element	TCP	1024-65535	23	Telnet
Collection Station	Mangement Station	TCP	1024-65535	6000	X-Windows ovw

VPO and Firewalls

Communication from the manager to the agent

- – Heartbeat

(RPC Only when ICMP blocking on Firewall)

- – Installation

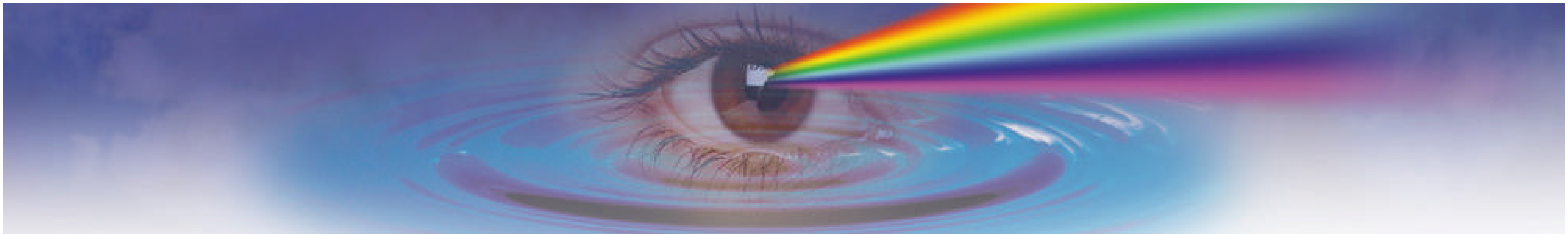
(Not recommended through Firewall)

- – Distribution
- – Action
- – Messaging

VPO UNIX Firewall Ports

VPO Firewall ports

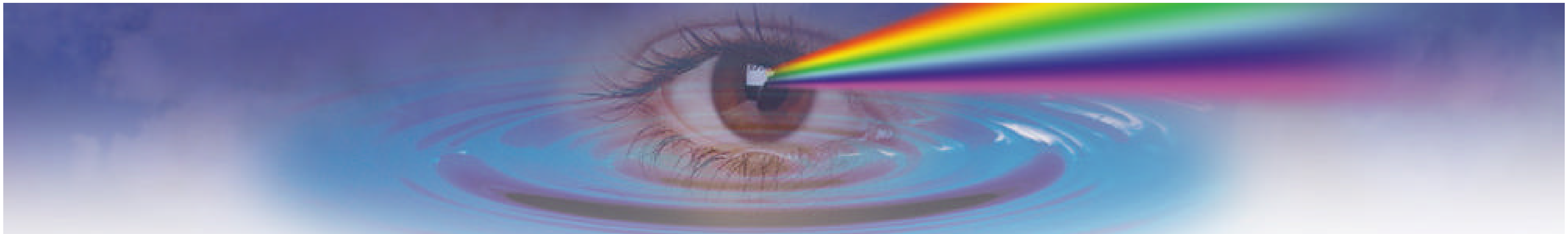
Source IP	Destination IP	Protocol	SRC Ports	DST Ports	Description/Service
Mangement Station	Managed Node	UDP	1024-65535	161	SNMP
Managed Node	Mangement Station	UDP	1024-65535	162	SNMP Trap
DCE Managed Nodes	Management Station	TCP	1024-65535	12001-12030	Distribution
Management Station	Manged element	IP	N/A	N/A	ICMP
GUI Station	Management Station	TCP	ANY	2531	HTTP Java GUI
Mangement Station	Managed Node	TCP	1024-65535	20,21	ftp
Mangement Station	Managed Node	TCP	1024-65535	512	rexec
Mangement Station	Managed Node	TCP	1024-65535	513	rlogin
Mangement Station	Managed Node	TCP	1024-65535	23	telnet
Mangement Station	Managed Node	TCP	1024-65535	514	remsh
DCE Managed Nodes	Management Station	TCP	13001-13010	135	RPC/DCE
Management Station	DCE Managed Nodes	TCP	12001-12030	135	RPC/DCE
DCE Managed Nodes	Management Station	TCP	13001-13010	12001-12030	RPC restricted port range
Management Station	DCE Managed Nodes	TCP	12001-12030	13001-13010	RPC restricted port range



VPO NT Firewall Ports

NT Agents

Source IP	Destination IP	Protocol	SRC Ports	DST Ports	Description/Service
NT Managed Nodes	Management Station	TCP	Any	135	RPC/DCE
Management Station	NT Managed Nodes	TCP	12001-12030	135	RPC/DCE
NT Managed Nodes	Management Station	TCP	Any	12001-12030	RPC restricted port range
Management Station	NT Managed Nodes	TCP	12001-12030	13001-13010	RPC restricted port range
NT Managed Nodes	Management Station	ICMP echo request	N/A	N/A	ICMP
Management Station	NT Managed Nodes	ICMP echo reply	N/A	N/A	ICMP



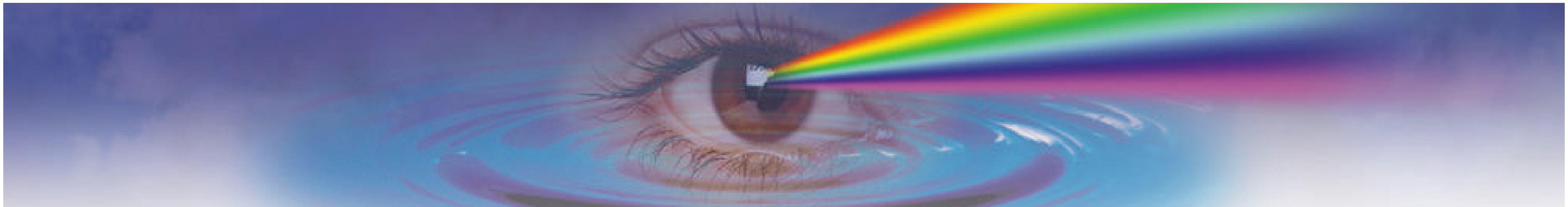
ManageX and Firewalls

- Communication from Server to Agent
  - DCE/RPC for communications
  - Name Services
- Communication from Agent to Server
  - DCE/RCP for responses
  - Message Broadcasts
  - Directed messages
- Integration to VPO
  - DCE/RPC from ManageX agent to VPO server
  - SNMP traps from ManageX agent to NNM or VPO

ManageX Firewall Ports

ManageX Firewall ports

Source IP	Destination IP	Protocol	SRC Port	DST Port	Description/Service
Console	Agent	TCP	1024	135	RPC location
Agent	Console	TCP	135	1024	RPC response
Console	Agent	TCP	1024	RANGE	RPC-session
Agent	Console	RPC	RANGE	1024	RPC response
Console	Master browser/PDC for ext. domain	UDP	1024	138	Netbios datagram, browse-request
Master browser/PDC for ext. domain	Console	UDP	138	1024	Netbios datagram response
Console	Agent	TCP	1024	139	Netbios session (smartbroker install)
Agent	Console	TCP	139	1024	Netbios session response
Agent	Broadcast	UDP	138	138	Mailslot message broadcast
Agent	Console	UDP	1024	138	Mailslot message directly
Console	Agent	UDP	138	1024	Mailslot message response if ack required



PerfView and MeasureWare

- Communication
  - DCE Server Daemon on PerfView Server
  - DCE Server Daemon on MeasureWare agent node
  - PerfView Agent on Management Server
  - MeasureWare Agent on Managed Nodes

PerfView and MeasureWare

PerfView MeasureWare Firewall ports

Source IP	Destination IP	Protocol	SRC Ports	DST Ports	Description/Service
MeasureWare agent	PerfView Server	UDP	135	Perfview ports	MeasureWare DCE UDP
MeasureWare agent	PerfView Server	UDP	Measure Ware Ports	135	PerfView DCE UDP
MeasureWare agent	PerfView Server	TCP	1024-65535	382 383	Perflbd
MeasureWare agent	PerfView Server	UDP	Measure Ware Ports	Perfview ports	MeasureWare agent

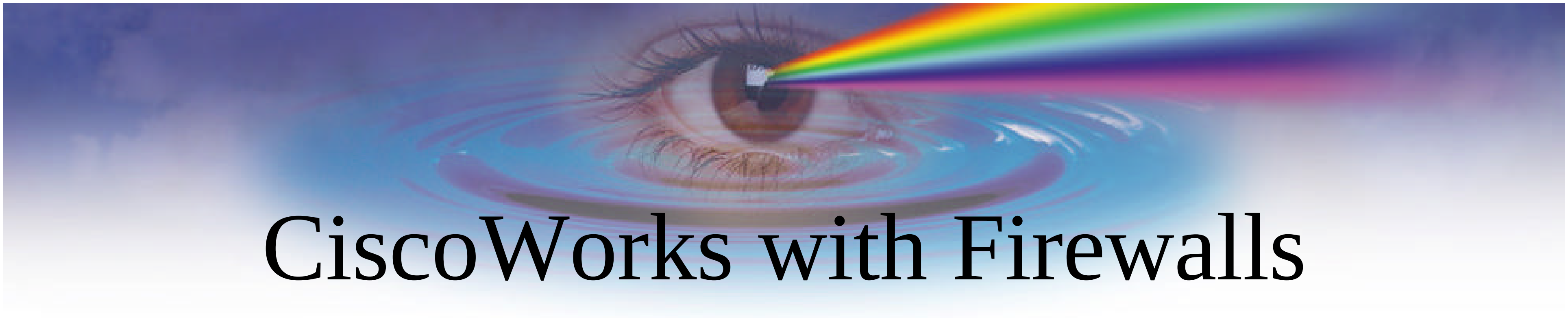
BMC Patrol with Firewalls

- Communication
  - Console to Agent
  - Agent Configuration
  - PatrolView to ITO agent
- Notes
  - Can use TCP for communication from console to agent

BMC Patrol with Firewalls

BMC Patrol Firewall ports

Source IP	**Destination IP**	**Protocol**	**SRC Ports**	**DST Ports**	**Description/Service**
Patrol Agent Node	Patrol Console Node	UDP	1988	1987	Agent to console
Patrol Console Node	Patrol Agent Node	UDP	1989	1987	Agent for Config
Patrol Agent Node	Patrol Console Node	UDP	1987	1988	Agent to Console
Patrol Console Node	Patrol Agent Node	UDP	1987	1989	Agent for Config
Patrol Console Node	Patrol Agent Node	UDP	1024-65535	161	SNMP
Patrol Agent Node	Patrol Console Node	UDP	1024-65535	162	SNMP Trap



CiscoWorks with Firewalls

- Communication
  - – Management Server to Managed Elements
  - – Requires SNMP Capabilities to Retrieve Data
  - – Console GUI to Management Server
  - – TCP Communications to Perform Administration

CiscoWorks with Firewalls

CiscoWorks Firewall ports

Source IP	Destination IP	Protocol	SRC Ports	DST Ports	Description/Service
Mangement Station	Managed Element	UDP	1024-65535	161	SNMP
Managed Elements	Mangement Station	UDP	1024-65535	162	SNMP Trap
Management Station	Managed Element	IP	N/A	N/A	ICMP
Console Station	Mangement Station	TCP	1024-65535	80 or 1741	HTTP Java GUI
Management Station	Managed Element	TCP	1024-65535	23	Telnet
Console Station	Mangement Station	TCP	1024-65535	6000	X-Windows
Mangement Station	Managed Element	TCP	1024-65535	23	telnet
Mangement Station	Managed Node	TCP	1024-65535	20,21	ftp
Console Station	Mangement Station	TCP	1024-65535	42340	Essentials Daemon Manager, Manages server processes
Console Station	Mangement Station	TCP	1024-65535	42341	Open Server Gateway
Console Station	Mangement Station	TCP	1024-65535	42342	Osagent
Console Station	Mangement Station	TCP	1024-65535	42343	Jrun
Console Station	Mangement Station	TCP	1024-65535	8000	CWSI database port

OmniBackII with Firewalls

- Communication
  - Cell server to Client
  - Omniback Service Daemon
  - Session Manager
  - User Interface
- Notes
  - Usually 200 TCP ports which will be dynamically allocated for session processes
  - Larger environments may require more

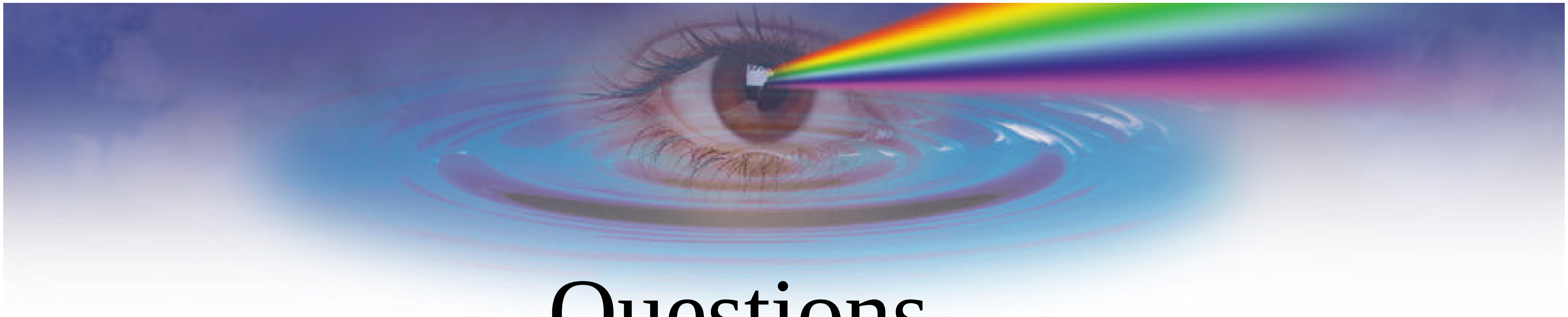
OmniBack II Firewall Ports

OmnibackII Firewall ports

Source IP	Destination IP	Protocol	SRC Ports	DST Ports	Description/Service
Cell Server	Client Node	TCP	5555	5555	OmniInet service
Cell Server	Client Node	TCP	5000-5199	5000-5199	Session Manager Processes
Client Node	Cell Server	TCP	5000-5199	5000-5199	Session Manager Processes

Summary

- Understand the Managed Environment
- Understand the Management Solution
- Determine the Communication From the Management Server to the Managed Object
- Determine What Protocols the Communication is Using
- Determine What Ports the Services Will be Using
- Understand How to Configure the Firewall to Enable This Communication
- Make Sure You Realize Any Vulnerabilities Associated With These Configurations
- Determine if the Management Function is worth the Vulnerability



Questions

Thanks!

MJM

MELILLO CONSULTING, INC.
THE POWER OF SOLUTIONS

Bob Kelly

kelly@mjm.com

Practice Manager,

Network & System Management

Melillo Consulting, Inc.