Practical Approaches
to
Network Segmentation

BEN CHASE

BEN@CHASENET.NET

HTTPS://GITHUB.COM/L33TMARMOT/

Definitions and Scope

Network Segmentation:

- Movement of endpoints into separate network subnets to limit what those devices can directly communicate with.

Subnet:

- For ease of discussion today, we will equate a 1-to-1 relationship between a subnet and a VLAN, as it is a standard convention (but by no means a requirement).

VLAN: A “channel” for broadcast traffic

- Endpoints tuned into this same “channel” can see each other’s ARP traffic.

Why?

Security

- A compromised host:
  - Has a *much* easier time performing reconnaissance and pivoting on hosts for which it is layer-2 adjacent to, meaning that it can hear the ARP traffic of other hosts.

Resiliency

- Configuration errors and software faults can introduce issues that prevent hosts from communicating within a VLAN
- Broadcast traffic generated by a large number of hosts can overwhelm a network in the right conditions, especially 802.11-based networks.

Part 1

BUILDING THE MODEL BY UNDERSTANDING YOUR BUSINESS

Things to understand first

How many different classes of users do you have?

- Frequently organized by departments or functional areas.
- Temporary or seasonal employees that need access to your network should also be considered.

What regulatory statutes must your business adhere to?

- HIPAA, SOX, GLBA, PCI and others may need to be considered in how you segment your network.

Things to understand first

Does your company store or host data for customers or other 3rd parties?

- Wherever feasible, plan to create network segments that are dedicated for customer resources.

What Internet-facing interfaces does your company have?

- Separate network segments should be created for public API's, websites, and similar things accessible from the Internet.

Secondary considerations

Areas of independent authority

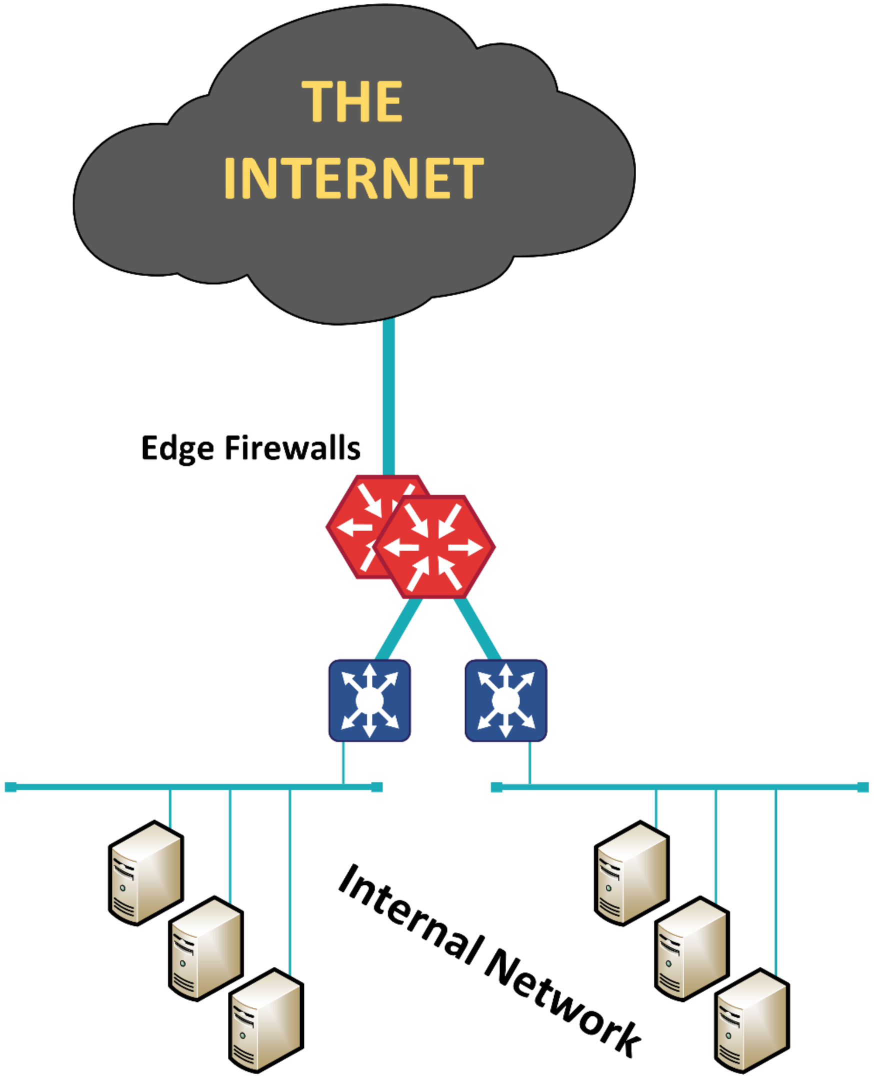
- Is there more than one security or IT organization with the ability to make independent decisions?

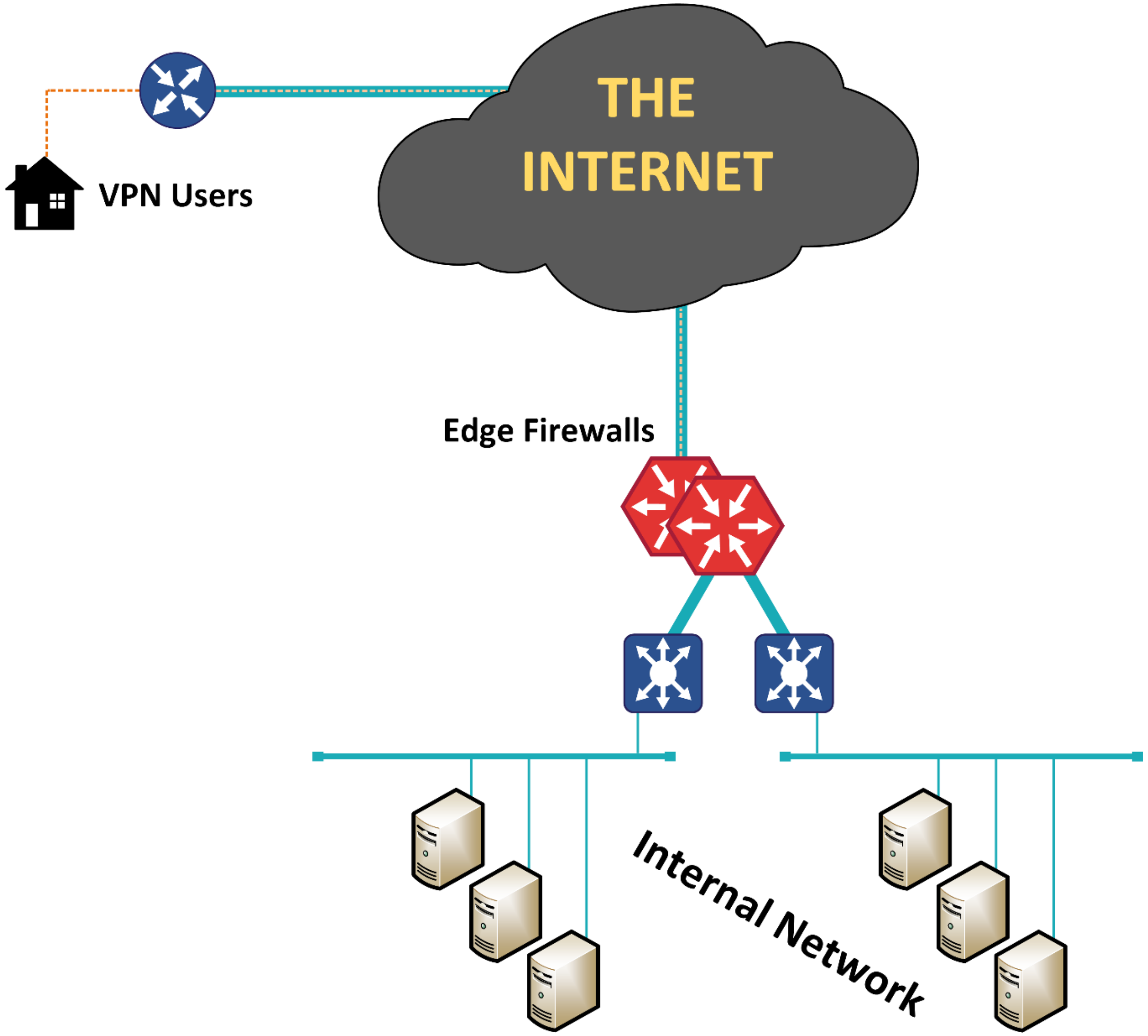
Wherever a separation of authority and accountability exists, segmentation by way of firewall policy should occur.

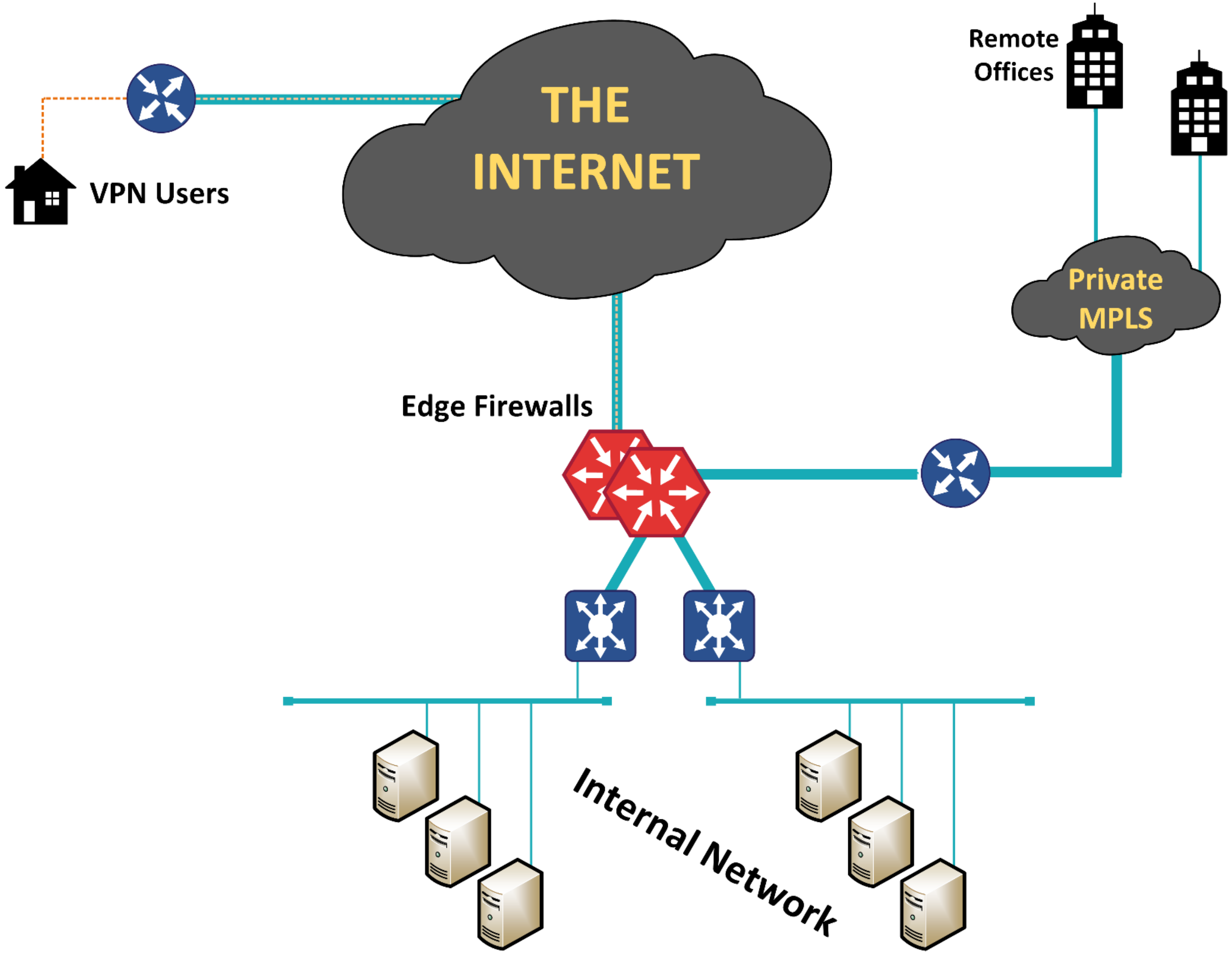
Things to understand about your traffic flows

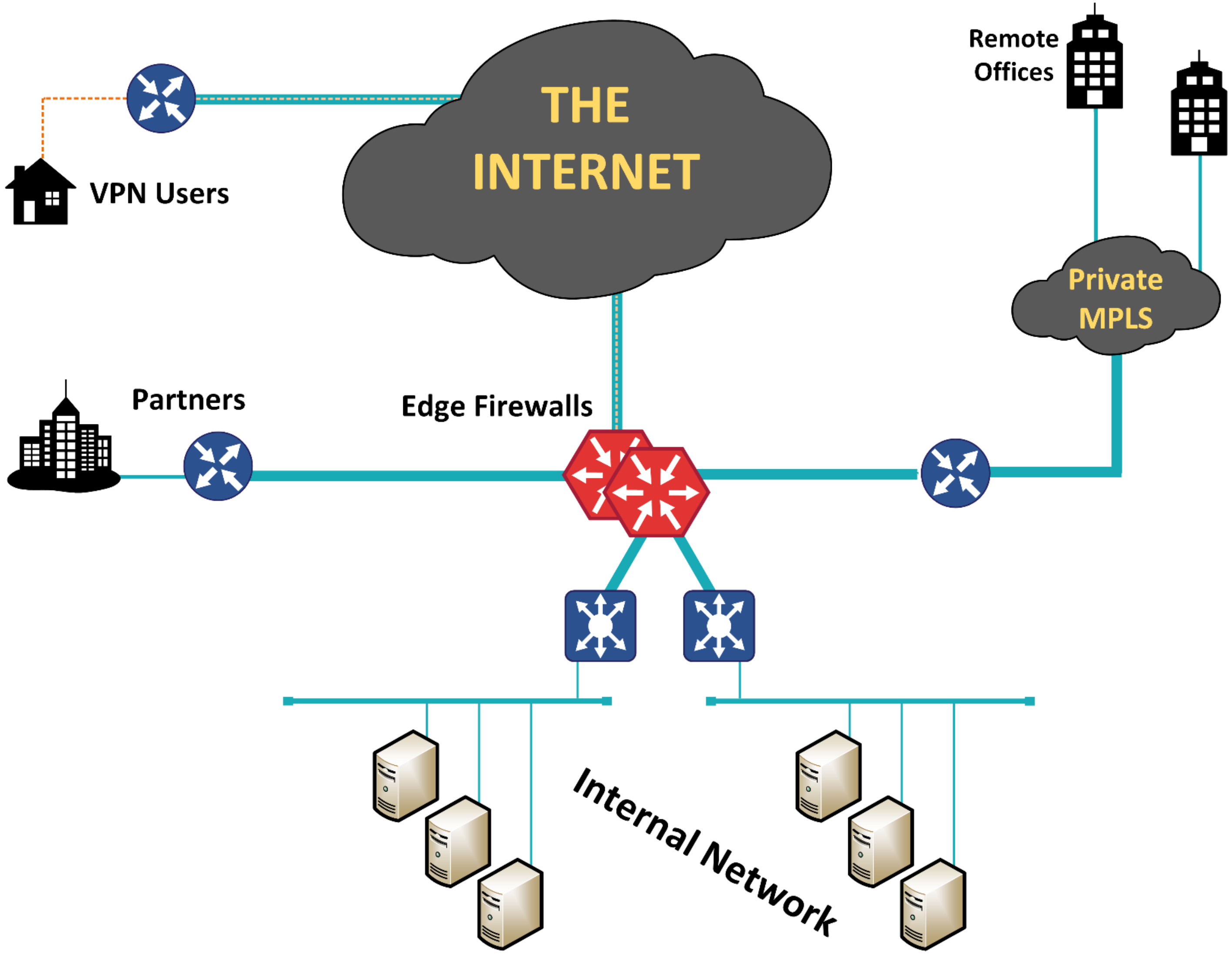
Traffic to/from your network edge– “The place or places where your network connects to places outside of your control.”

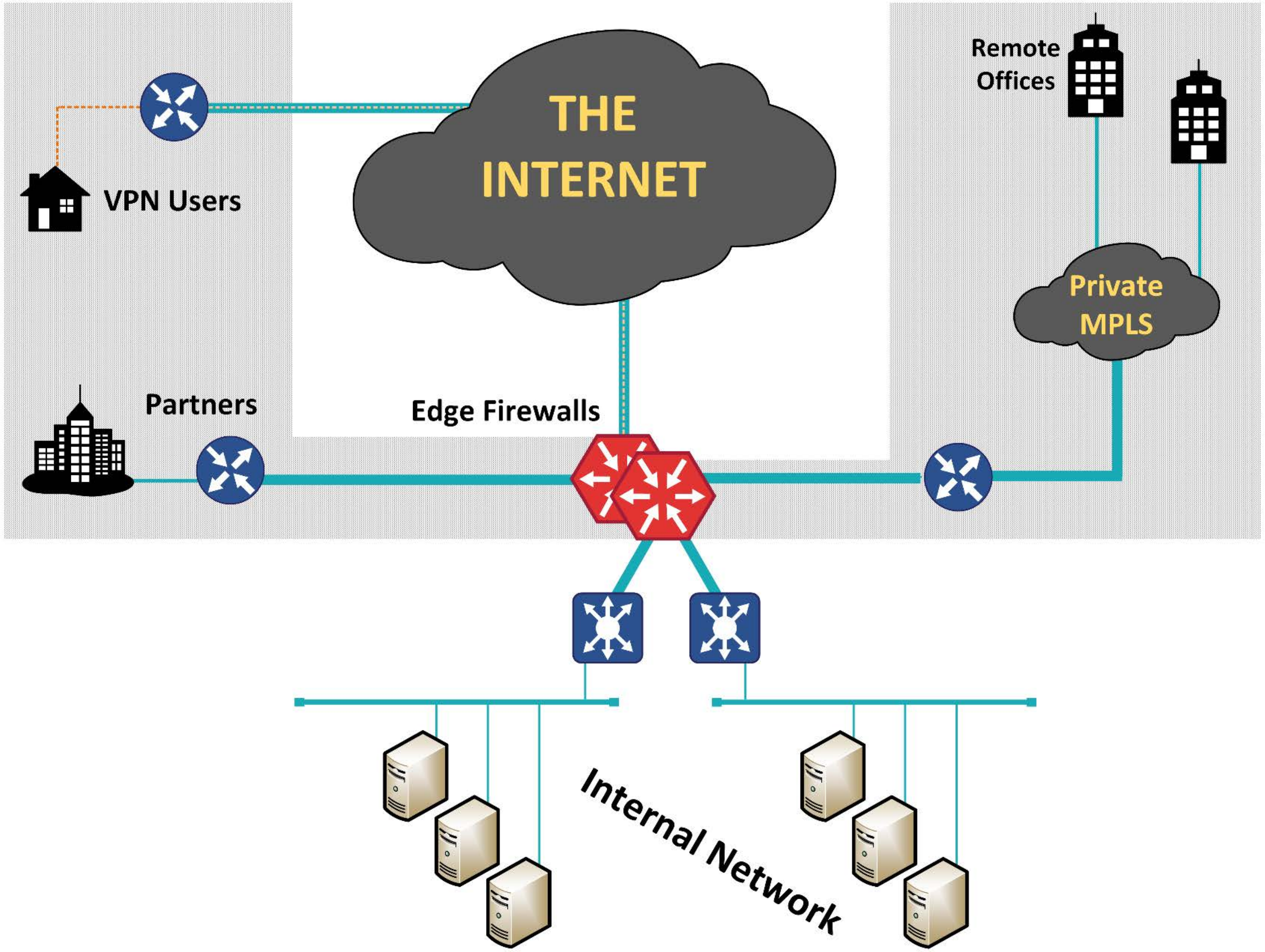
- Employee VPN access, connections to partners or other 3rd parties
- Traffic to/from the public Internet to your network


THE INTERNET
Edge Firewalls
Internal Network


THE INTERNET
VPN Users
Edge Firewalls
Internal Network


THE INTERNET
VPN Users
Remote Offices
Private MPLS
Edge Firewalls
Internal Network


THE INTERNET
Remote Offices
VPN Users
Private MPLS
Partners
Edge Firewalls
Internal Network


THE INTERNET
VPN Users
Partners
Edge Firewalls
Remote Offices
Private MPLS
Internal Network

Things to understand about your traffic flows

How does each class of users that you have access the resources they require today?

- User-to-server

What is the communication flow required between your back-end systems and applications?

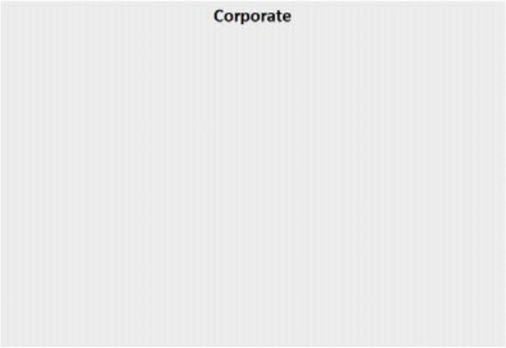
- Server-to-server

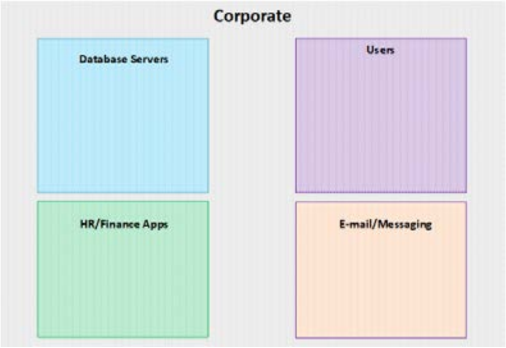
Identify where segmentation should occur

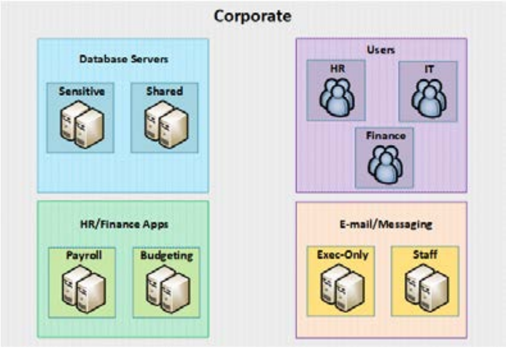
If you have resources that are globally-shared within your company, try to minimize what is in that network segment.

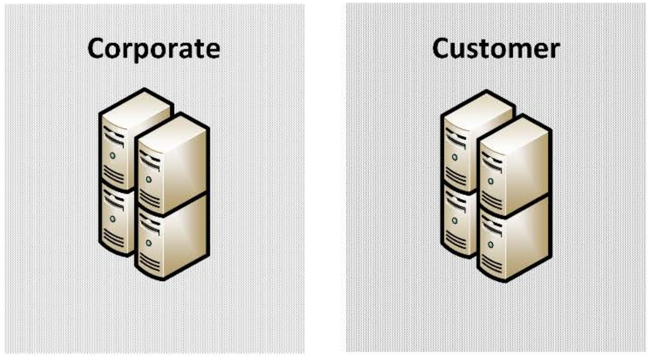
Start with very high-level categories first, work your way down to as much detail as you need.

- The “Russian doll” approach.



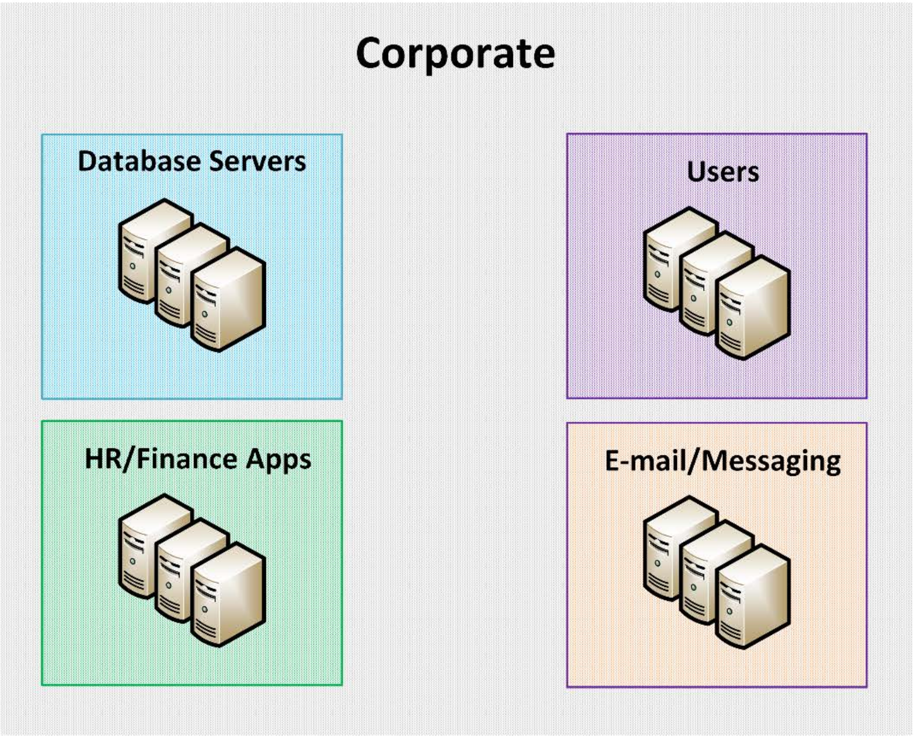


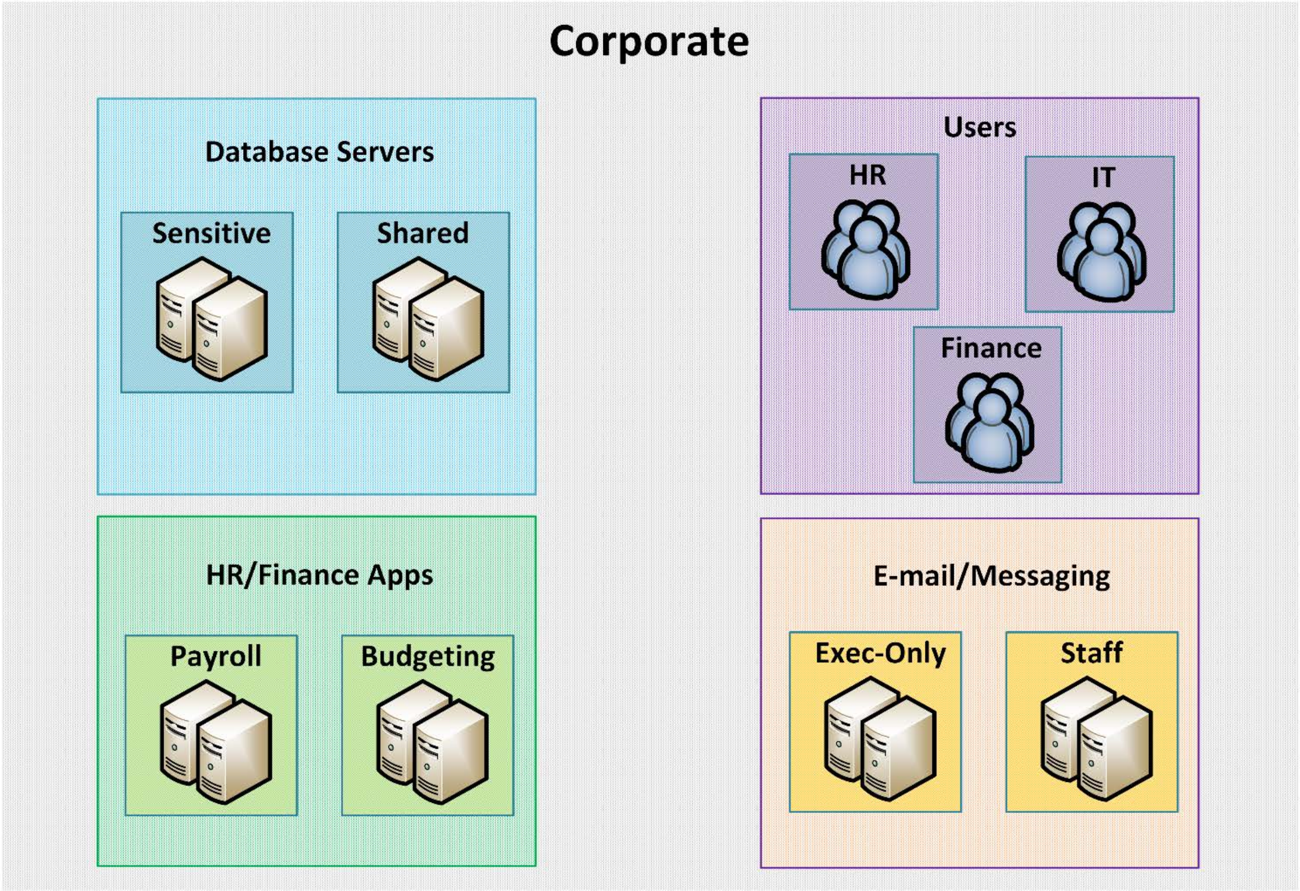




Corporate

Customer


Corporate
Database Servers
Users
HR/Finance Apps
E-mail/Messaging



Corporate

Database Servers

Sensitive

Shared

Users

HR

IT

Finance

HR/Finance Apps

Payroll

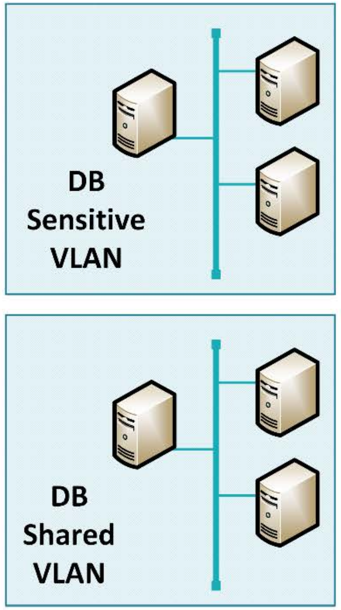
Budgeting

E-mail/Messaging

Exec-Only

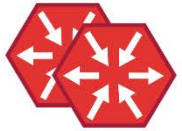
Staff

Firewall Policy

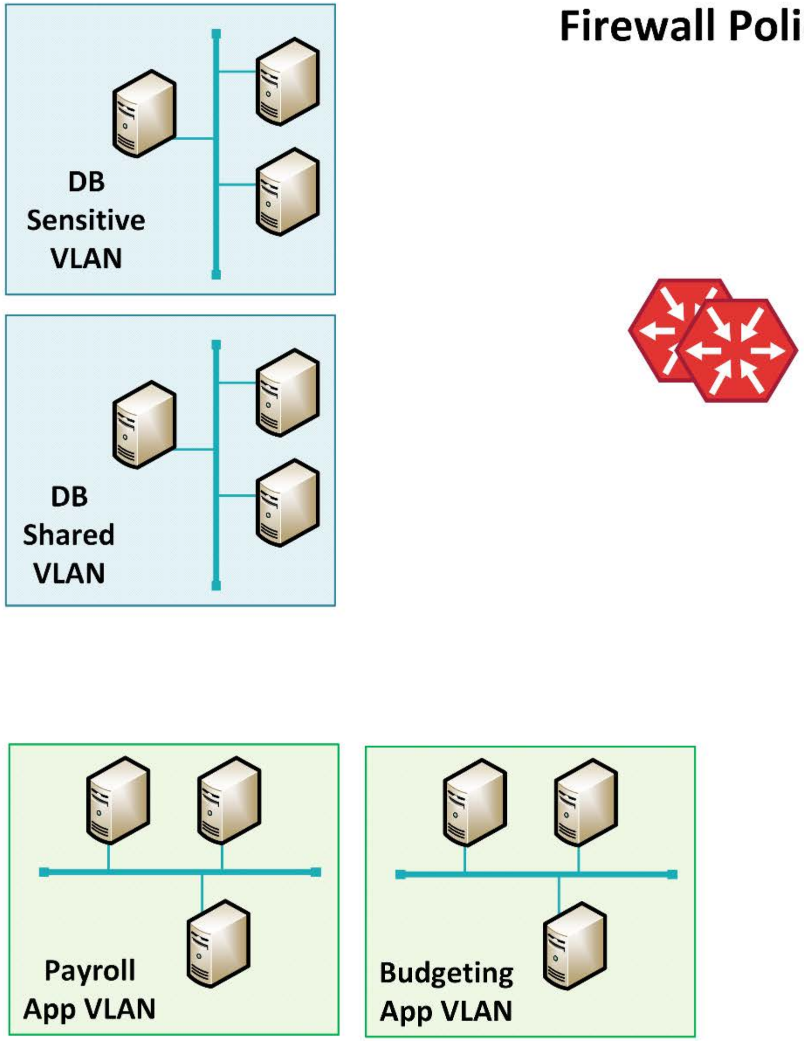


DB Sensitive VLAN

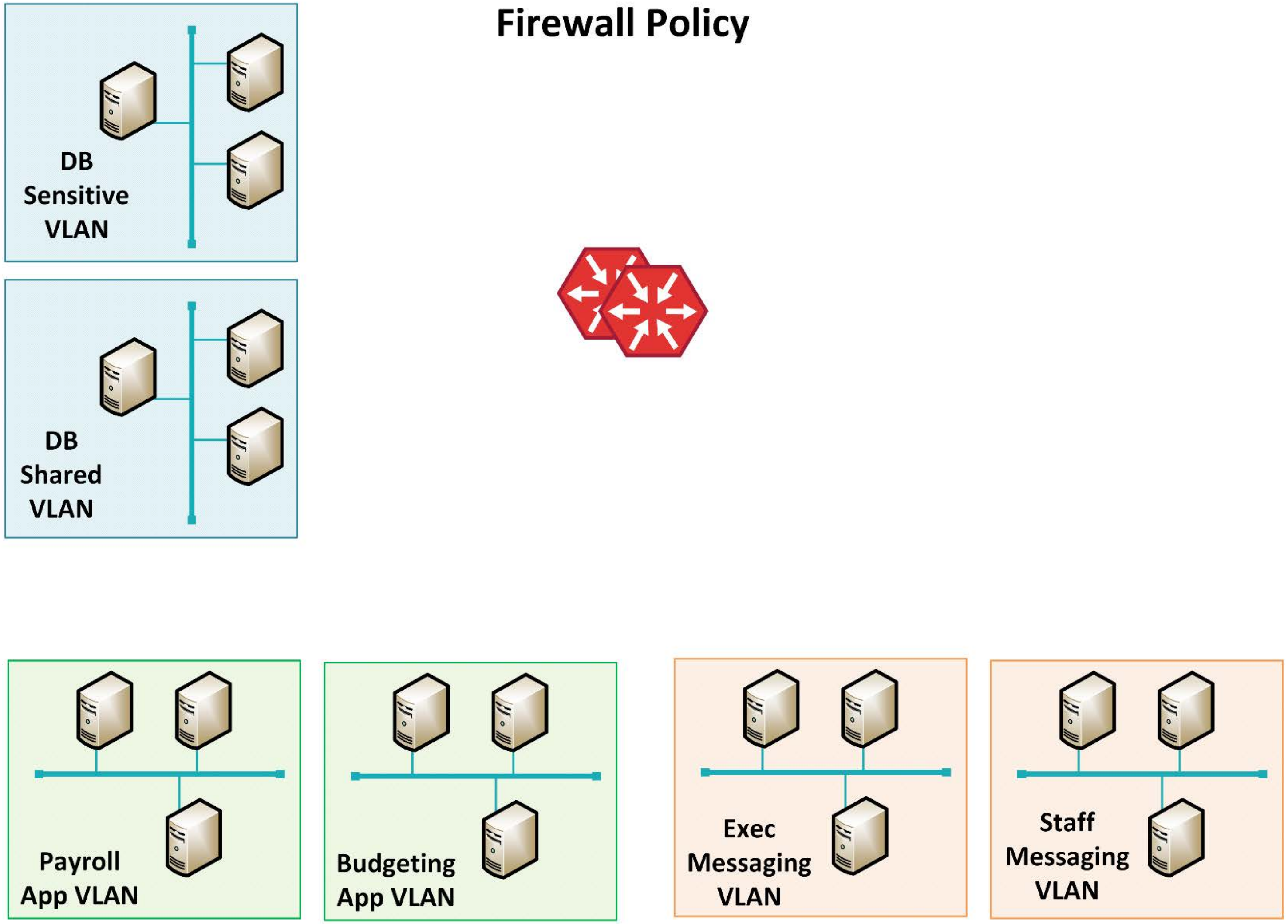
DB Shared VLAN



Firewall Policy



Firewall Policy



DB Sensitive VLAN

DB Shared VLAN

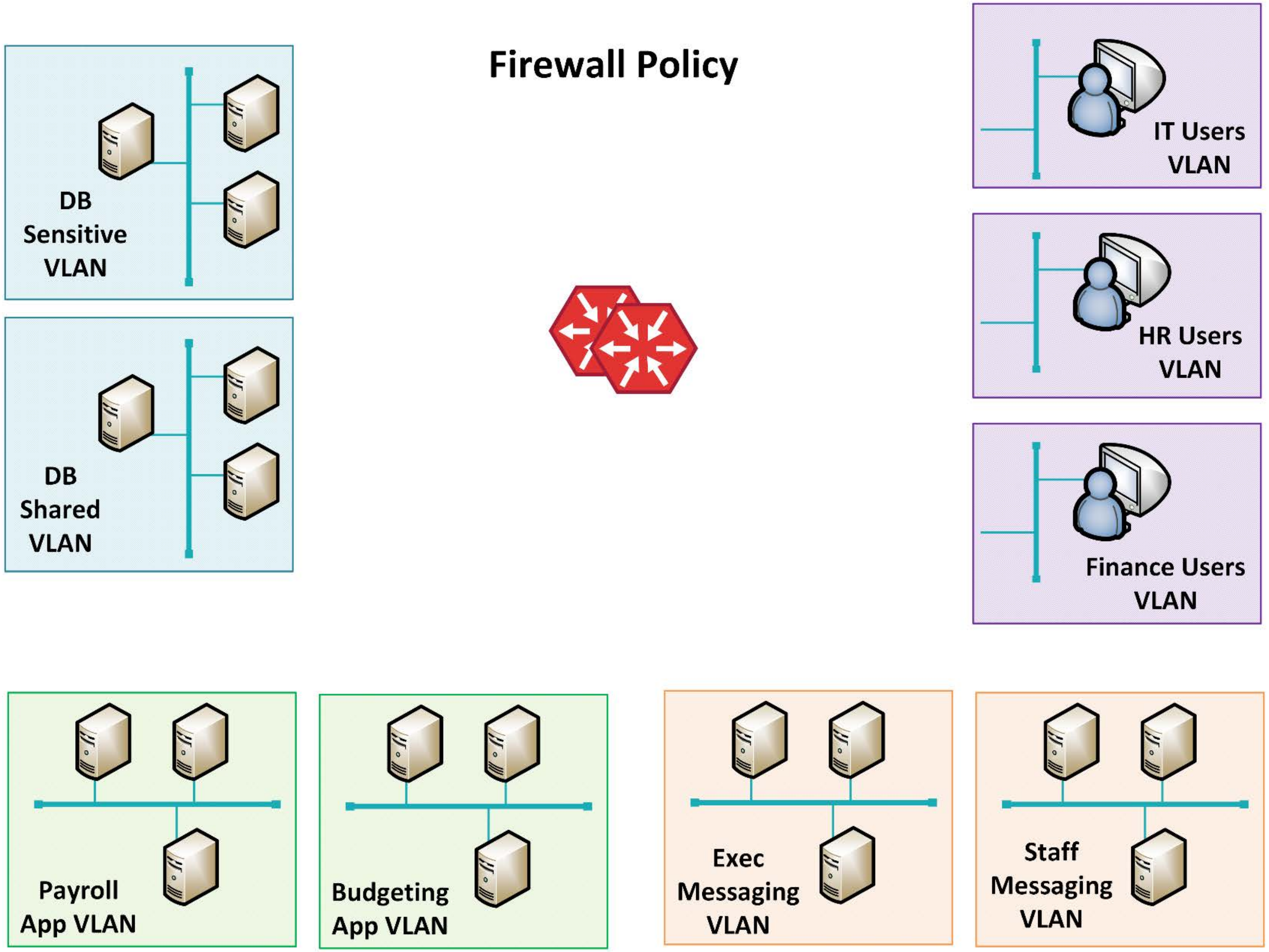
Payroll App VLAN

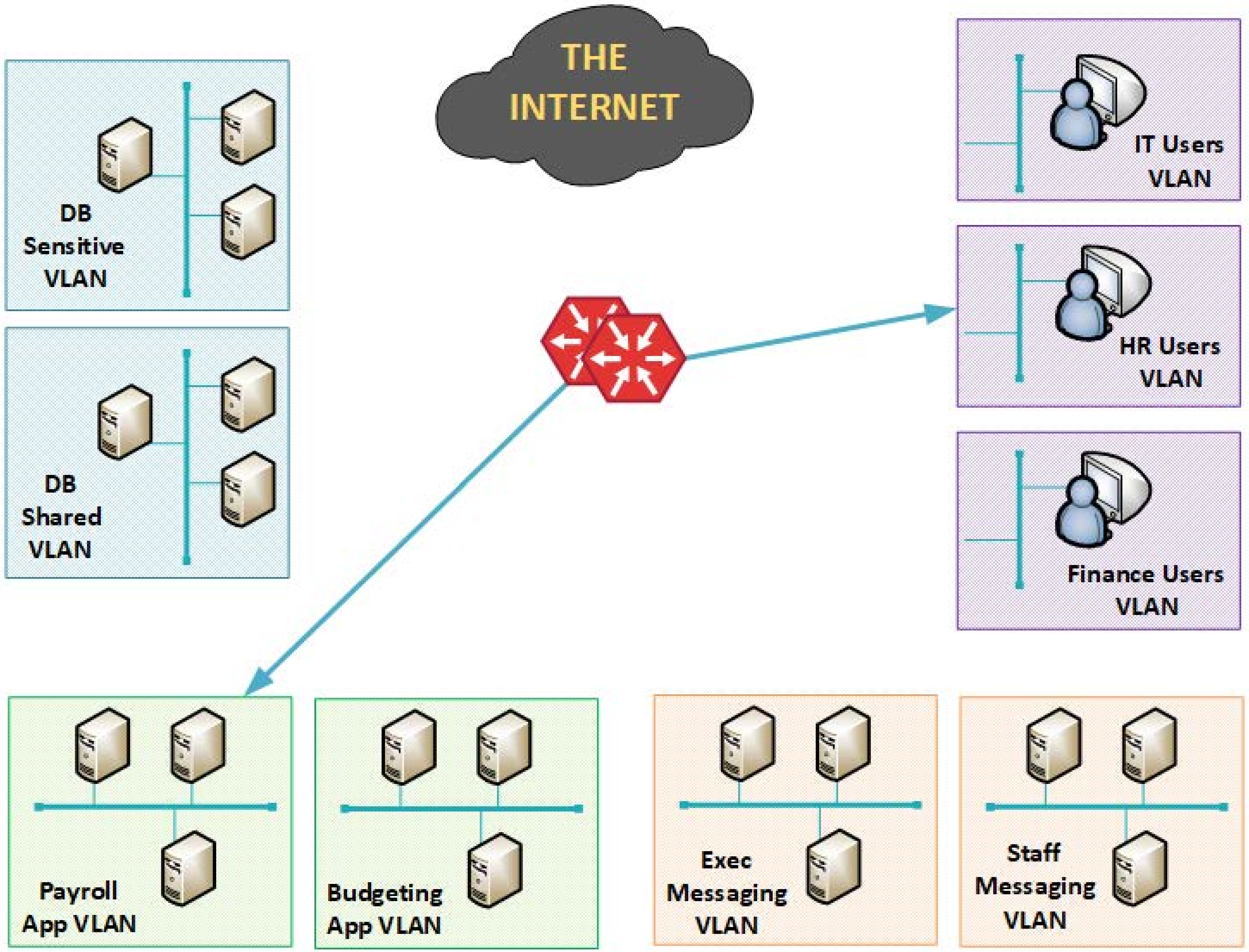
Budgeting App VLAN

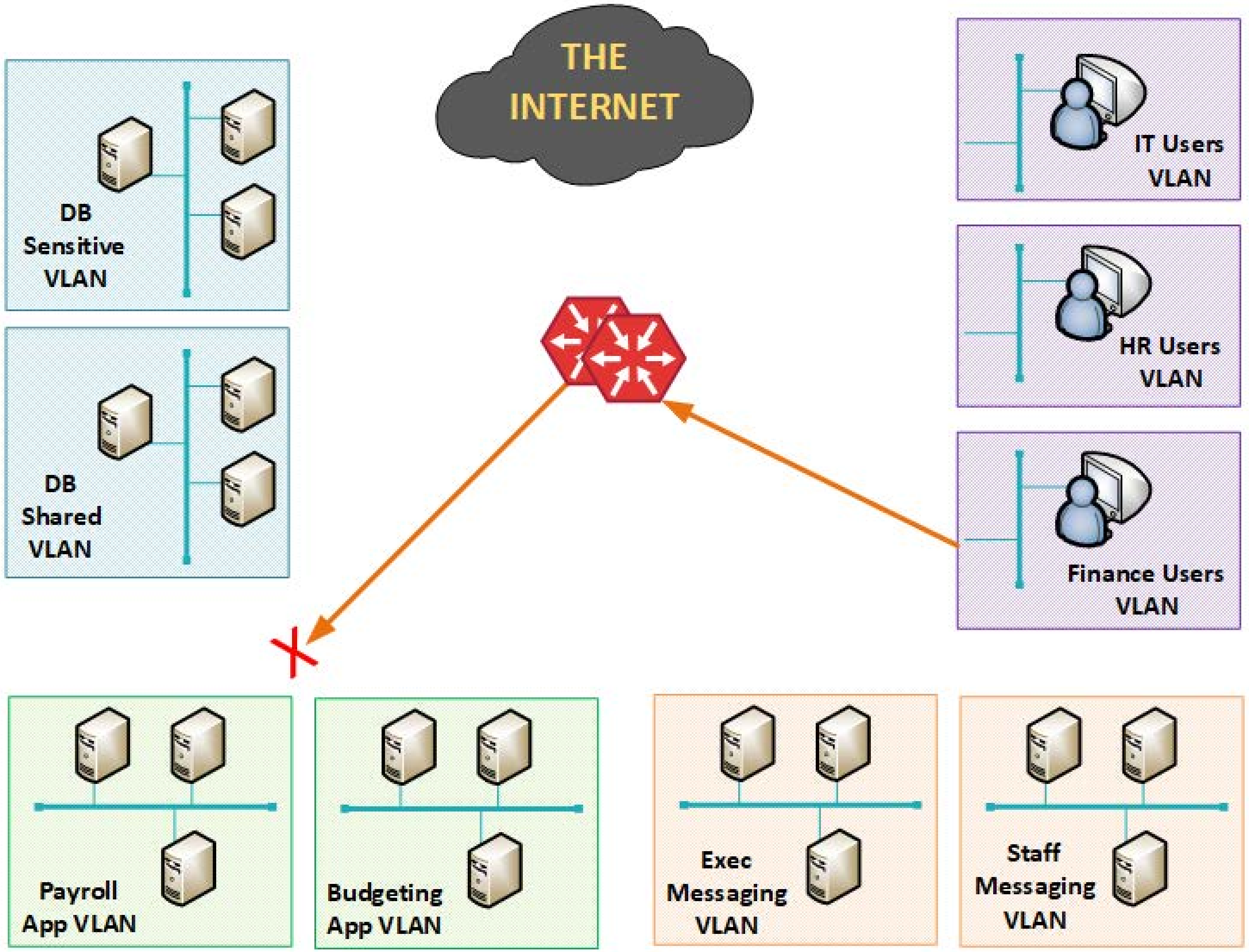
Exec Messaging VLAN

Staff Messaging VLAN

Firewall Policy




THE INTERNET
DB Sensitive VLAN
DB Shared VLAN
IT Users VLAN
HR Users VLAN
Finance Users VLAN
Payroll App VLAN
Budgeting App VLAN
Exec Messaging VLAN
Staff Messaging VLAN


THE INTERNET
DB Sensitive VLAN
DB Shared VLAN
IT Users VLAN
HR Users VLAN
Finance Users VLAN
Payroll App VLAN
Budgeting App VLAN
Exec Messaging VLAN
Staff Messaging VLAN

Identify where segmentation should occur

Decide where you want to apply different types of firewall policy

- Next-gen policy features such as IPS, DLP, Antivirus/Anti-Malware, etc
- Basic L4 policy based on simple port/protocol and source/destination ACLs
- Turning on every feature or inspection type is not always the right answer
  - Some next-gen features are hardware-limited.

Part 2

IMPLEMENTING YOUR NETWORK SEGMENTATION MODEL

The IP Addressing Plan

The networking and security teams ***must*** work together to develop a well-designed IP addressing plan.

The design of the addressing plan determines:

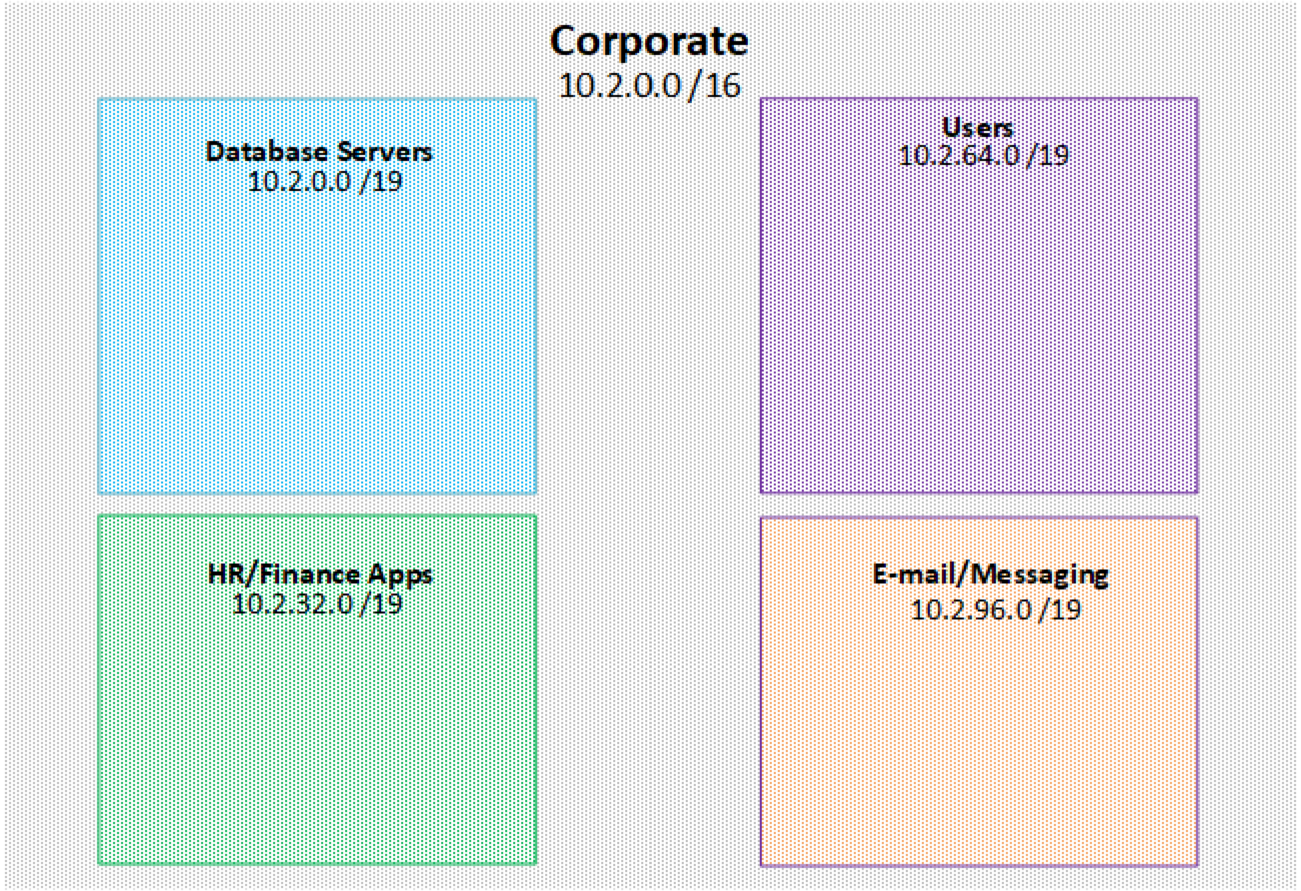
- Limiting factors where segmentation can easily be applied, both now & in the future.
- The effectiveness and performance of dynamic routing protocols in use.
  - Larger routing tables can make understanding the network topology unnecessarily difficult and may lengthen the troubleshooting time when issues do arise.

The IP Addressing Plan

Use contiguous space wherever possible.

- Give yourself enough room for growth & unexpected requirements.
- Stick to /24 masks for user segments to minimize configuration errors.
- Consider using the “Russian doll” approach to simplify firewall policy configuration.

Corporate
10.2.0.0/16



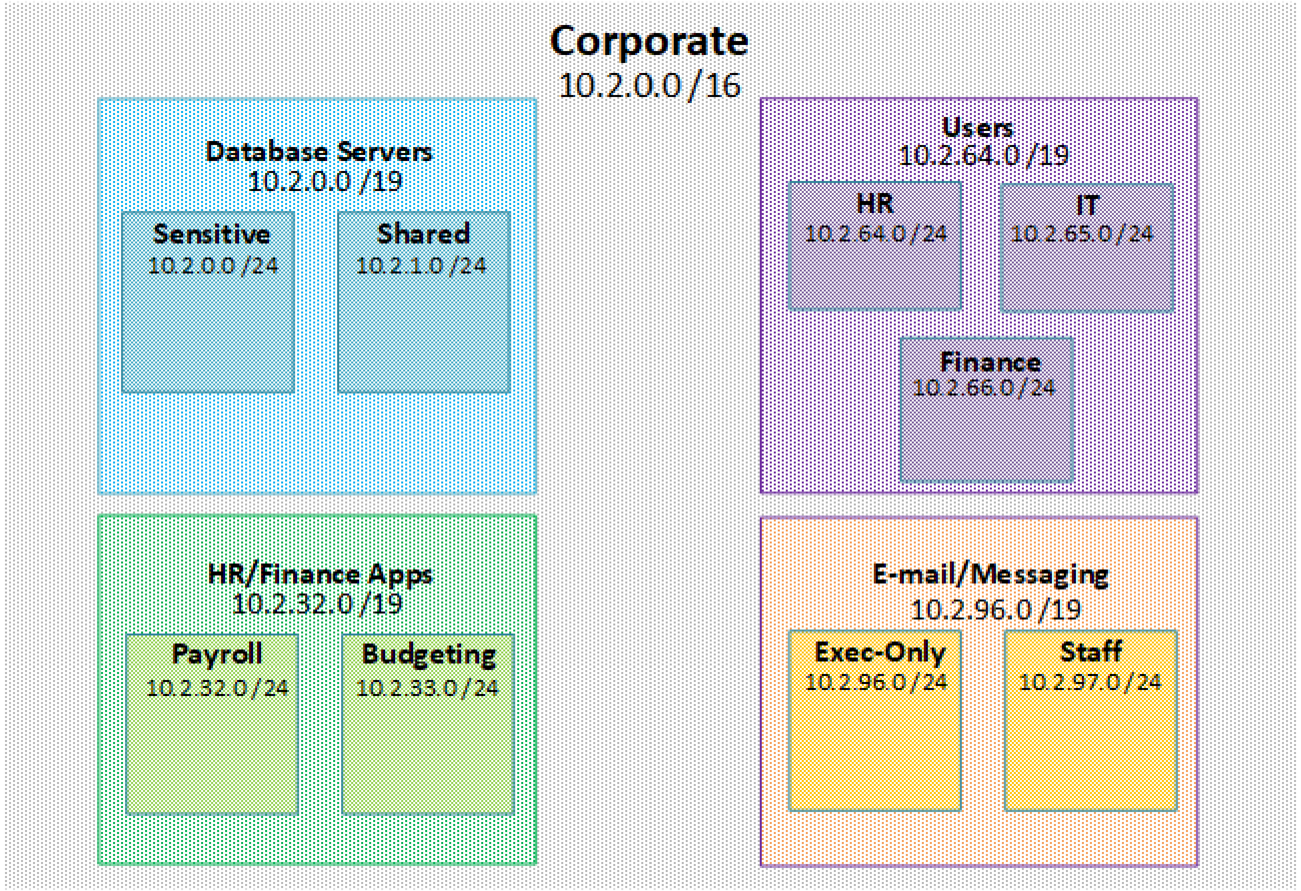
Corporate
10.2.0.0 /16

Database Servers
10.2.0.0 /19

Users
10.2.64.0 /19

HR/Finance Apps
10.2.32.0 /19

E-mail/Messaging
10.2.96.0 /19



Corporate
10.2.0.0 /16

Database Servers
10.2.0.0 /19

Sensitive
10.2.0.0 /24

Shared
10.2.1.0 /24

Users
10.2.64.0 /19

HR
10.2.64.0 /24

IT
10.2.65.0 /24

Finance
10.2.66.0 /24

HR/Finance Apps
10.2.32.0 /19

Payroll
10.2.32.0 /24

Budgeting
10.2.33.0 /24

E-mail/Messaging
10.2.96.0 /19

Exec-Only
10.2.96.0 /24

Staff
10.2.97.0 /24

The IP Addressing Plan

Remediating an existing production network

- First assess the scale of what you are trying to accomplish

Common Examples:

“Many of our servers are in the same VLAN with most sharing several business functions”

“Many of our servers are in the same VLAN but are mostly dedicated to one function/role”

The IP Addressing Plan

“Many of our servers are in the same VLAN with most sharing several business functions”

- This is one of the most challenging issues to solve.
- Likely to be both labor and cost-intensive depending on the scale.

Possible Approaches

- Carve out specific business functions or processes in order of sensitivity/risk by building new VM’s and migrating those applications and data into the new environment.

The IP Addressing Plan

“Many of our servers are in the same VLAN but are mostly dedicated to one function/role”

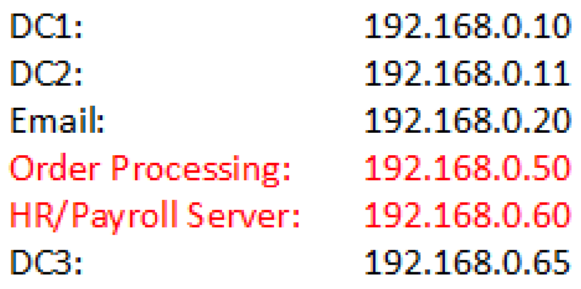
Possible Approaches

- Create new segments
  - Re-address servers in those new segments, based on their role or function.
- Change subnet masks
  - You might consider this approach if IP addresses are hard coded in applications or referenced directly in ways that are difficult or impossible for you to control.
  - Can be tricky depending on where the IP’s fall in relation to each other.

The IP Addressing Plan

Exercise: Changing subnet masks

- Your company has two servers which are referenced by specific IP address by other compiled code which are either poorly documented or fragile.
- You need to segment the network, but you aren’t allowed to change the IP addresses of the HR/Payroll server, nor the Order Processing server.
- **Requirements**: Segment the network such that the Order Processing and HR/Payroll servers are not in the same subnet.



DC1:	192.168.0.10
DC2:	192.168.0.11
Email:	192.168.0.20
Order Processing:	192.168.0.50
HR/Payroll Server:	192.168.0.60
DC3:	192.168.0.65

The IP Addressing Plan

Exercise: Changing subnet masks

Approach:

- Break up the /24 into smaller segments in such a way that minimizes the number of changes needed, but provides growth for the future.

126 hosts per subnet	/25	/25

Subnets

192.168.0.0/25

192.168.0.128/25

DC1:	192.168.0.10
DC2:	192.168.0.11
Email:	192.168.0.20
Order Processing:	192.168.0.50
HR/Payroll Server:	192.168.0.60
DC3:	192.168.0.65

62 hosts per subnet	/26	/26	/26	/26
126 hosts per subnet	/25		/25	

Subnets

192.168.0.0/26
192.168.0.64/26
192.168.0.128/26
192.168.0.192/26

DC1:	192.168.0.10
DC2:	192.168.0.11
Email:	192.168.0.20
Order Processing:	192.168.0.50
HR/Payroll Server:	192.168.0.60
DC3:	192.168.0.65

<table>
<tr><td>30 hosts per subnet</td><td>/27</td><td>/27</td><td>/27</td><td>/27</td><td>/27</td><td>/27</td><td>/27</td><td>/27</td></tr>
<tr><td>62 hosts per subnet</td><td colspan="2">/26</td><td colspan="2">/26</td><td colspan="2">/26</td><td colspan="2">/26</td></tr>
<tr><td>126 hosts per subnet</td><td colspan="4">/25</td><td colspan="4">/25</td></tr>
</table>

Subnets
192.168.0.0/27
192.168.0.32/27
192.168.0.64/27
192.168.0.96/27
192.168.0.128/27
192.168.0.160/27
192.168.0.192/27
192.168.0.224/27

DC1:	192.168.0.10
DC2:	192.168.0.11
Email:	192.168.0.20
Order Processing:	192.168.0.50
HR/Payroll Server:	192.168.0.60
DC3:	192.168.0.65

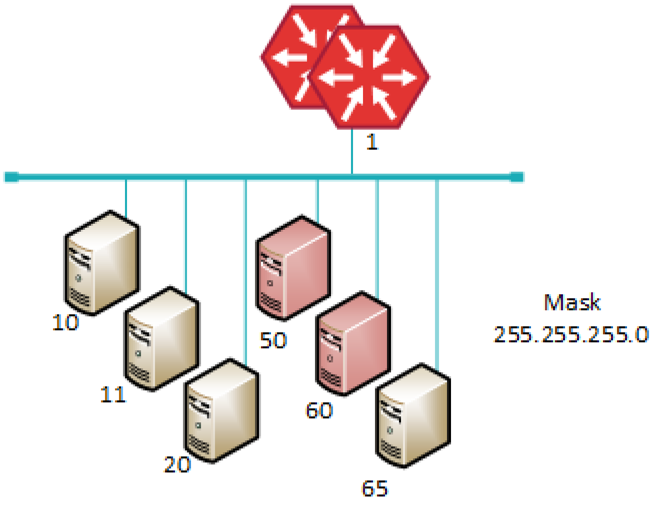
Solution:
192.168.0.0/27 = Network Services VLAN
192.168.0.32/28 = Available for use
192.168.0.48/29 = Order Processing VLAN
192.168.0.56/29 = HR/Payroll Systems VLAN
192.168.0.64/26 = Available for use
192.168.0.128/25 = Available for use

<table>
<tr><td>30 hosts per subnet</td><td>/27</td><td>/27</td><td>/27</td><td>/27</td><td>/27</td><td>/27</td><td>/27</td><td>/27</td></tr>
<tr><td>62 hosts per subnet</td><td colspan="2">/26</td><td colspan="2">/26</td><td colspan="2">/26</td><td colspan="2">/26</td></tr>
<tr><td>126 hosts per subnet</td><td colspan="4">/25</td><td colspan="4">/25</td></tr>
</table>

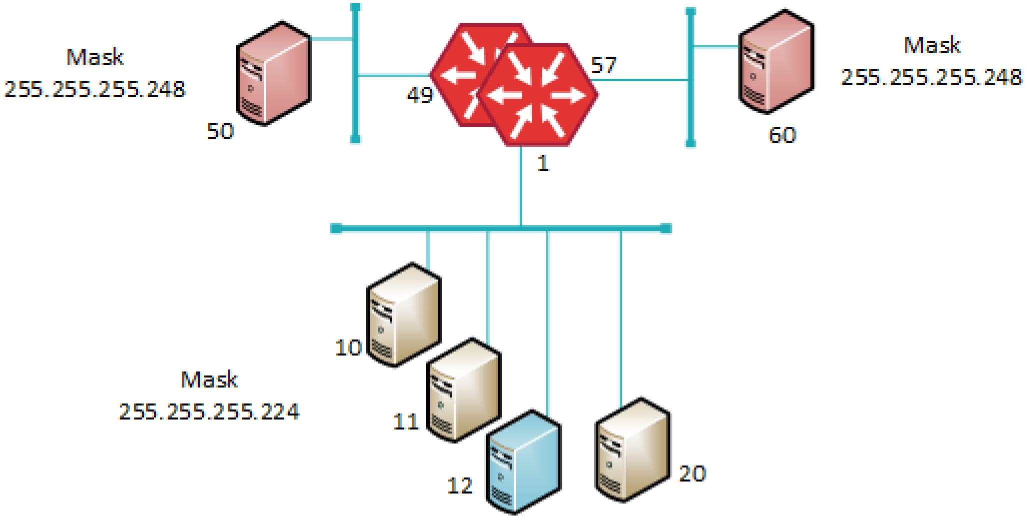
Subnets
192.168.0.0/27 → Done
192.168.0.32/27 → 192.168.0.32/28
192.168.0.48/28 → 192.168.0.48/29
192.168.0.56/29
192.168.0.64/27
192.168.0.96/27
192.168.0.128/27
192.168.0.160/27
192.168.0.192/27
192.168.0.224/27

DC1:	192.168.0.10
DC2:	192.168.0.11
Email:	192.168.0.20
Order Processing:	192.168.0.50
HR/Payroll Server:	192.168.0.60
DC3:	192.168.0.65

Original



Modified



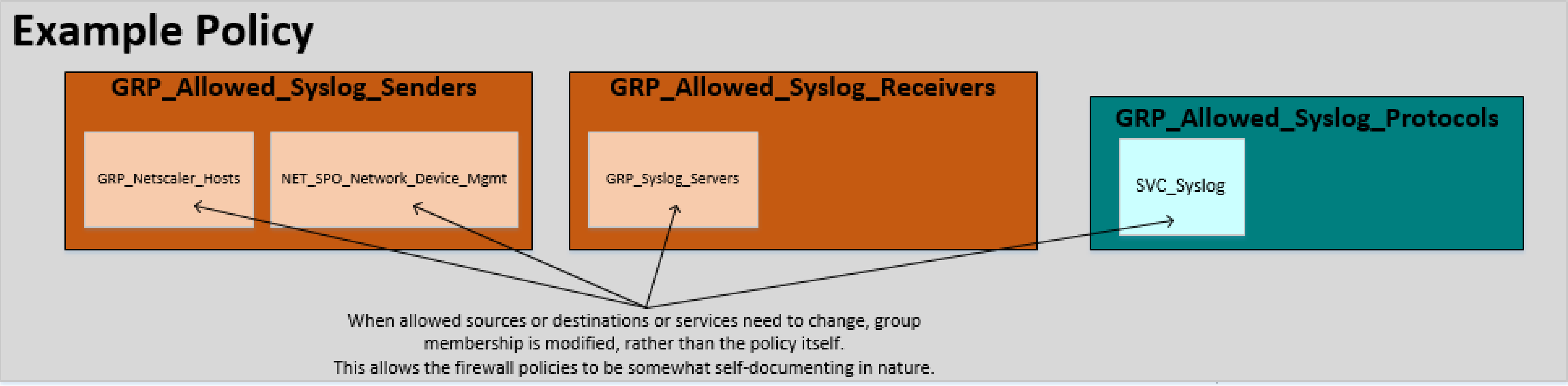
Thinking Ahead

Consider both future events and ongoing support in your plan

- Mergers and acquisitions
- New categories of customers, resources, users, or services
- Consider future self-auditing activities and new employees
  - For every firewall policy, try to assign a named person or role who can speak to it’s need to be there, and the date last reviewed.

Thinking Ahead

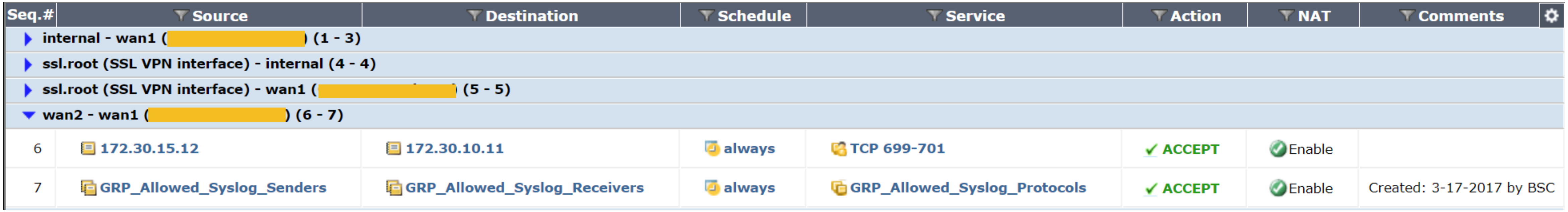
- Try to use self-documenting naming conventions and language between the security and networking teams
  - Having firewall policies that use descriptive group objects
  - Readability matters!


Example Policy
GRP_Allowed_Syslog_Senders
GRP_Netscaler_Hosts
NET_SPO_Network_Device_Mgmt
GRP_Allowed_Syslog_Receivers
GRP_Syslog_Servers
GRP_Allowed_Syslog_Protocols
SVC_Syslog

When allowed sources or destinations or services need to change, group membership is modified, rather than the policy itself.
This allows the firewall policies to be somewhat self-documenting in nature.

Thinking Ahead

Compare rule #6 versus rule #7, which is more intuitive?



Seq.#	Source	Destination	Schedule	Service	Action	NAT	Comments
internal - wan1 ([redacted]) (1 - 3)							
ssl.root (SSL VPN interface) - internal (4 - 4)							
ssl.root (SSL VPN interface) - wan1 ([redacted]) (5 - 5)							
wan2 - wan1 ([redacted]) (6 - 7)							
6	172.30.15.12	172.30.10.11	always	TCP 699-701	✓ ACCEPT	Enable	
7	GRP_Allowed_Syslog_Senders	GRP_Allowed_Syslog_Receivers	always	GRP_Allowed_Syslog_Protocols	✓ ACCEPT	Enable	Created: 3-17-2017 by BSC

Segmentation in context with firewall policy conventions

A well-designed IP schema can help to minimize the number of firewall policies required.

- Allows a “simple where possible, complex where necessary” approach.

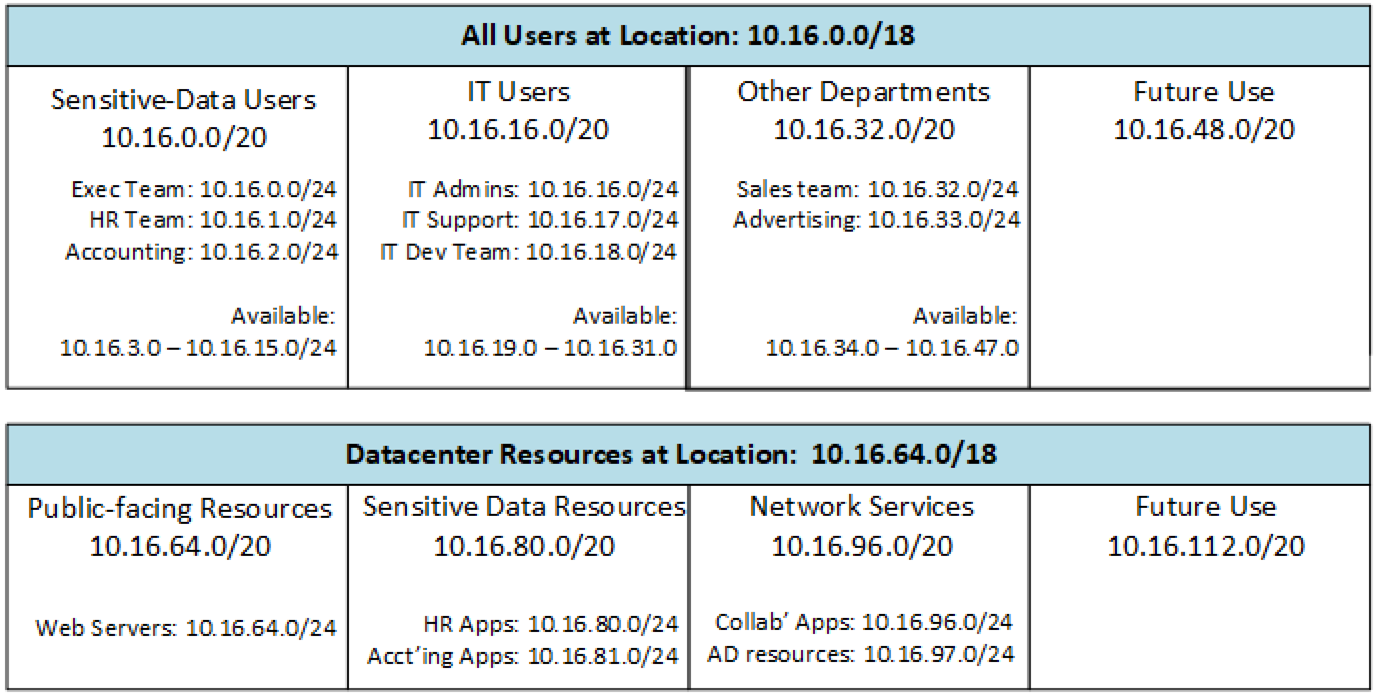
Scenario – discontiguous networks :

Your company has established the following networks:

Internet-Facing Servers:	192.168.0.0/24
HR Users:	192.168.1.0/24
HR Application Servers:	192.168.2.0/24
IT Users:	192.168.3.0/24
Meeting/Collaboration App Servers:	192.168.4.0/24
Dev team users:	192.168.5.0/24
Dev server environment:	192.168.6.0/24

Pseudo-firewall rules required to permit all user networks access to the collaboration server network on TCP port 443:

Source	Destination	SP	DP	Action
192.168.1.0/24	192.168.4.0/24	*	443	Permit
192.168.3.0/24	192.168.4.0/24	*	443	Permit
192.168.5.0/24	192.168.4.0/24	*	443	Permit



All Users at Location: 10.16.0.0/18			
Sensitive-Data Users 10.16.0.0/20	IT Users 10.16.16.0/20	Other Departments 10.16.32.0/20	Future Use 10.16.48.0/20
Exec Team: 10.16.0.0/24 HR Team: 10.16.1.0/24 Accounting: 10.16.2.0/24	IT Admins: 10.16.16.0/24 IT Support: 10.16.17.0/24 IT Dev Team: 10.16.18.0/24	Sales team: 10.16.32.0/24 Advertising: 10.16.33.0/24	
Available: 10.16.3.0 – 10.16.15.0/24	Available: 10.16.19.0 – 10.16.31.0	Available: 10.16.34.0 – 10.16.47.0	

Datacenter Resources at Location: 10.16.64.0/18			
Public-facing Resources 10.16.64.0/20	Sensitive Data Resources 10.16.80.0/20	Network Services 10.16.96.0/20	Future Use 10.16.112.0/20
Web Servers: 10.16.64.0/24	HR Apps: 10.16.80.0/24 Acct'ing Apps: 10.16.81.0/24	Collab' Apps: 10.16.96.0/24 AD resources: 10.16.97.0/24	

Pseudo-firewall rules required to permit all user networks access to the collaboration server network on TCP port 443:

Source	Destination	SP	DP	Action
10.16.0.0/18	10.16.96.0/24	*	443	Permit

Other Segmentation Strategies

Transparent firewalling

- Involves placing a firewall in between switched interfaces.
- Often referred to as “Bump in the wire”
- Useful in cases where:
  - There is a desire to avoid changing the routing infrastructure
  - The firewall does not have good routing protocol support.
  - There is any need to firewall at a more “covert” level.

Other Segmentation Strategies

Host-Level Firewalling

- Windows firewall managed via Group Policy
  - Allows a very fine level of control, however, it requires a mature organization with mature staff to implement properly at a large scale.
  - Firewall changes made at the GPO level aren’t normally implemented instantly
    - Normally updated every 90 minutes + randomized offset up to 30 minutes

Corner cases in Network Segmentation

Multiple subnets in a single VLAN – Use cases

- Occasionally used for legacy or “Sketchy” devices that support a fixed IP space that can’t be changed.

- Avoids having to initially reconfigure switchports during a transition from one IP space to another.
    - Opinions differ on this, but I recommend not doing this if at all possible.
    - Increases the amount of broadcast traffic within the VLAN which all hosts must process at some level.

The importance of peer review and collaboration

- Try to use self-documenting naming conventions and language between the security and networking teams

- Consider future self-auditing activities and new employees
  - How intuitive are the rules?

Q & A