Energy Connections Network Design Proposal

G3 Consulting Inc.

G3 consulting

Project Overview

Design Team

Aiden Mitchell
Team Leader, Security

Lasse Lammers
Linux & Windows Server

Peter Djordjevic
vSphere/ESXi & Windows Server

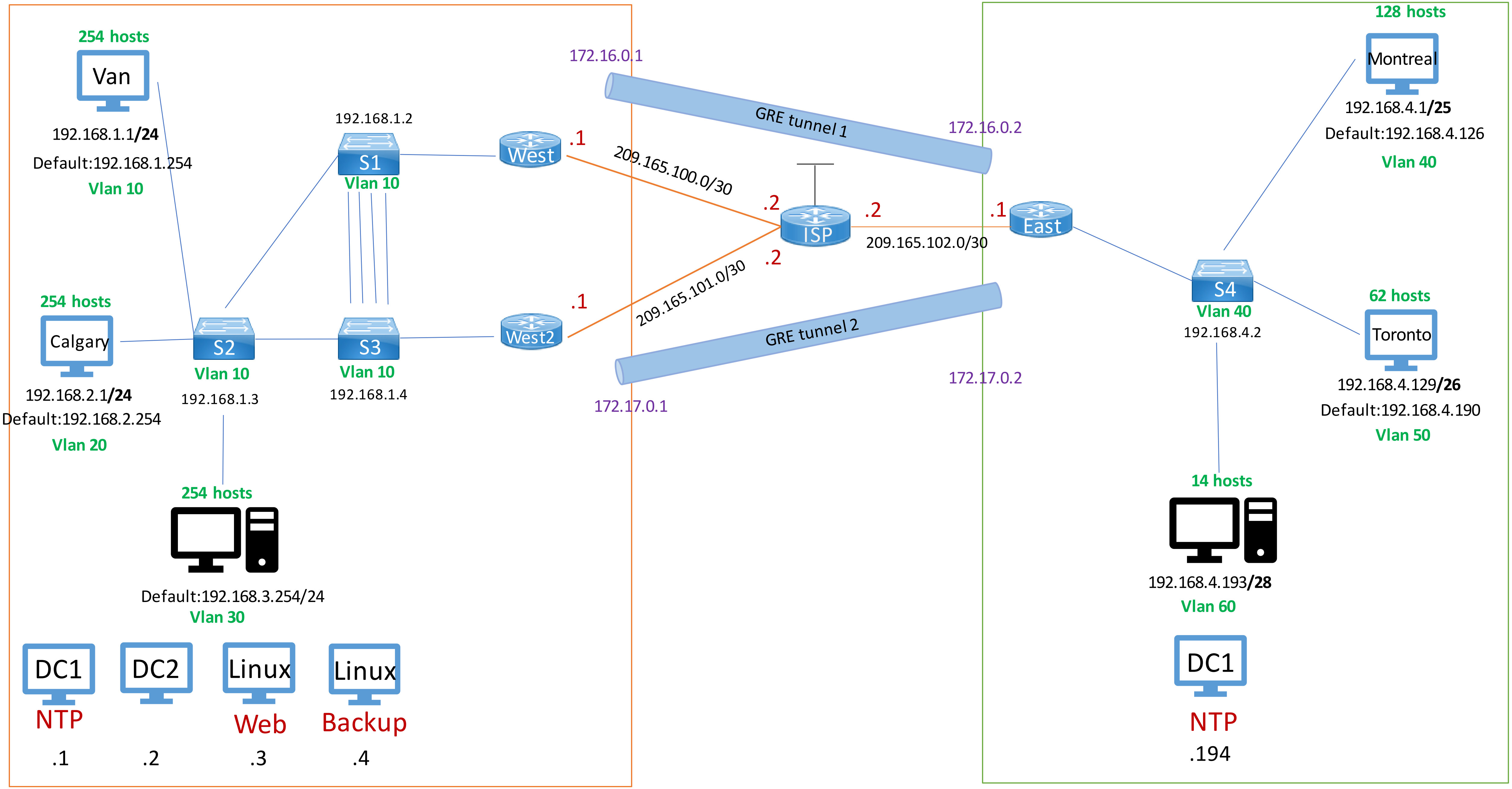
Wilson Liu
Networking Parts 1 & 2, Network Security

Umair Abdullah
Networking Parts 1 & 2, Network Security

Bishmanjot Johal
Networking Parts 1 & 2, Network Security

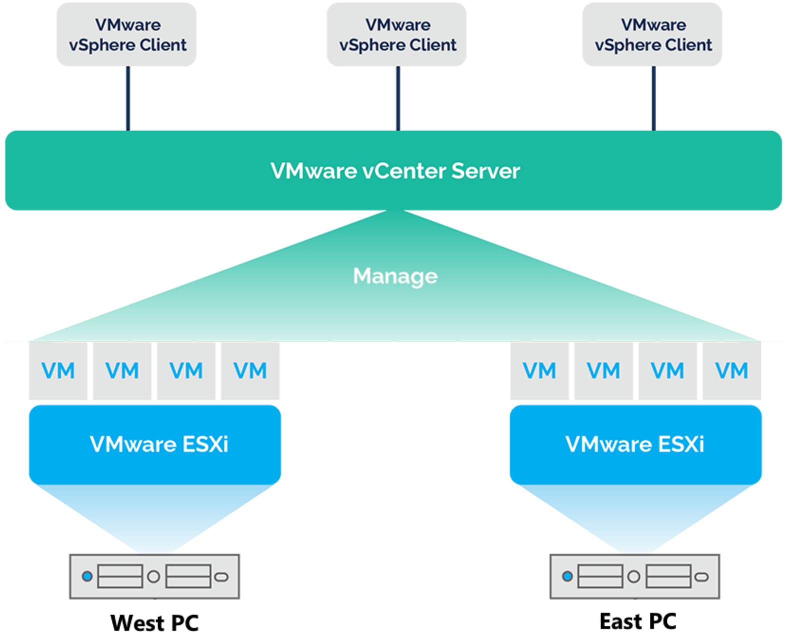
Brandon Huang
Networking Parts 1 & 2, Network Security

Network Topology & Technologies


254 hosts
Van
192.168.1.1/24
Default:192.168.1.254
Vlan 10
192.168.1.2
S1
Vlan 10
West
.1
172.16.0.1
GRE tunnel 1
172.16.0.2
209.165.100.0/30
.2
ISP
.2
.1
East
209.165.102.0/30
.2
209.165.101.0/30
.1
West2
GRE tunnel 2
172.17.0.1
172.17.0.2
254 hosts
Calgary
192.168.2.1/24
Default:192.168.2.254
Vlan 20
S2
Vlan 10
192.168.1.3
S3
Vlan 10
192.168.1.4
254 hosts
Default:192.168.3.254/24
Vlan 30
DC1
NTP
.1
DC2
.2
Linux
Web
.3
Linux
Backup
.4
128 hosts
Montreal
192.168.4.1/25
Default:192.168.4.126
Vlan 40
S4
Vlan 40
192.168.4.2
62 hosts
Toronto
192.168.4.129/26
Default:192.168.4.190
Vlan 50
14 hosts
192.168.4.193/28
Vlan 60
DC1
NTP
.194

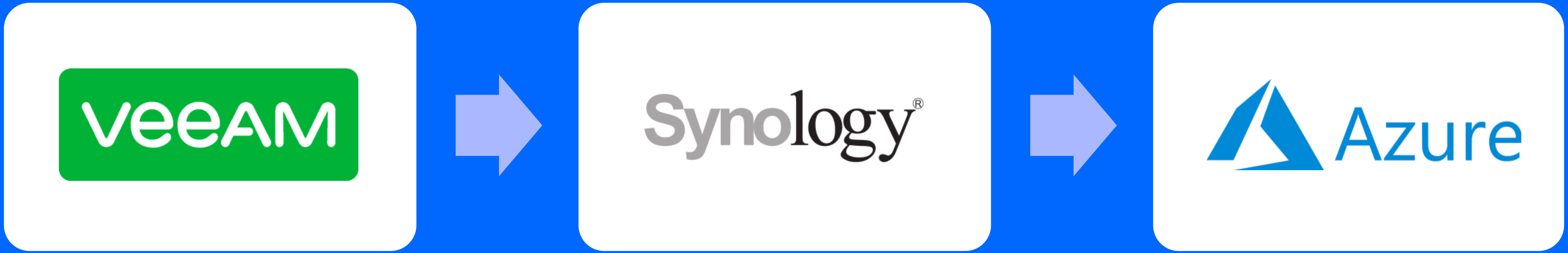
VMware vSphere and ESXi

- Type 1 Hypervisor (Bare-Metal)
- 2 Physical ESXi Hosts
  - West **(142.232.253.217)**
  - East **(142.232.253.227)**
- Linked Through vCenter Server
  - vSphere Client VM **(142.232.253.195)**



Backups and Redundancy

Virtual Machine Backup Process



On-Site

- Taken hourly
- Stored on a separate machine

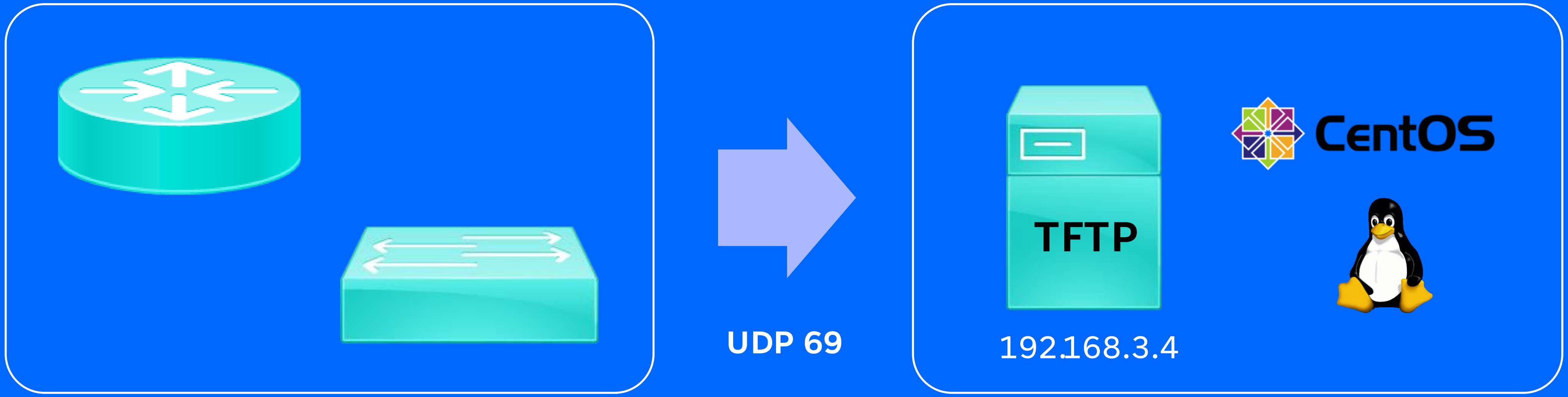
Off-Site

- Connected via Tailscale VPN
- Data is fully encrypted in transit

Cloud

- Located in a different geographical region
- Backed by Azure redundancy

Cisco Config Backup Process

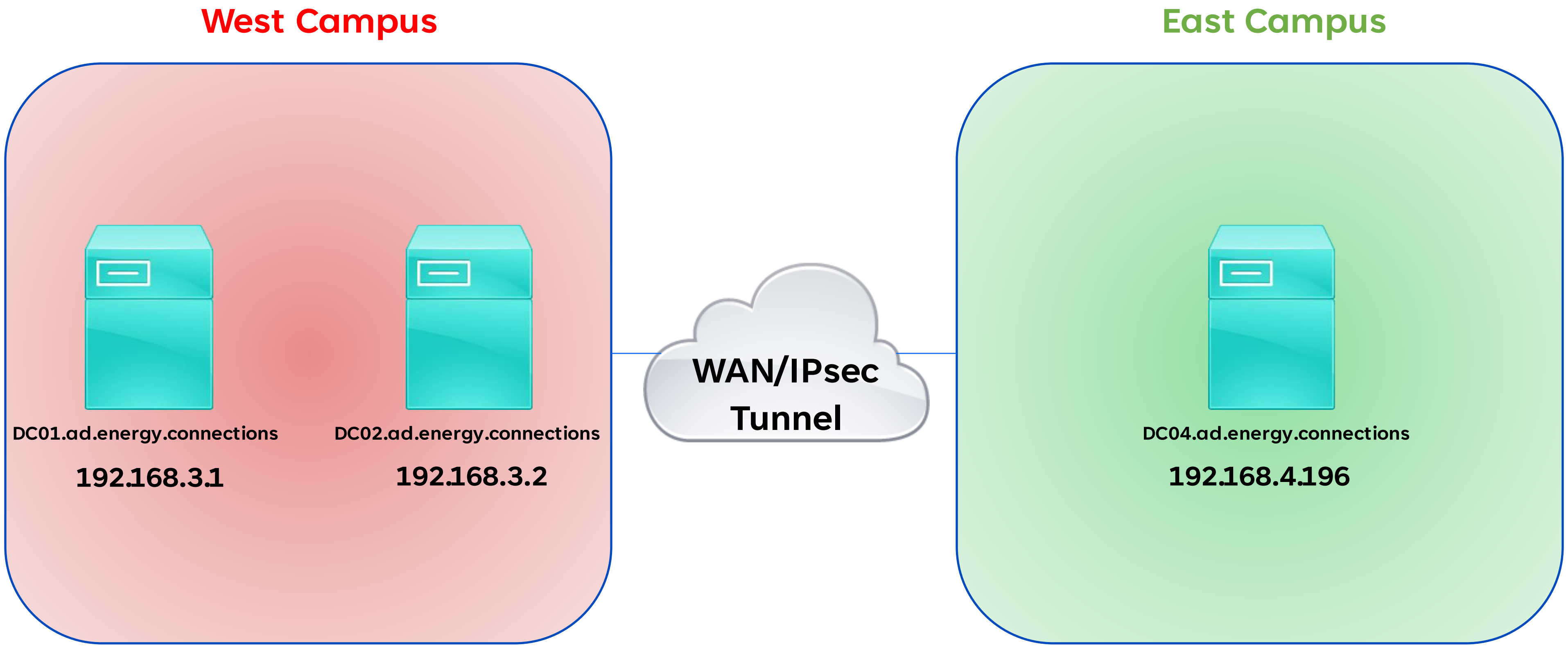


- All start-up configs saved via TFTP
- Executed manually as necessary

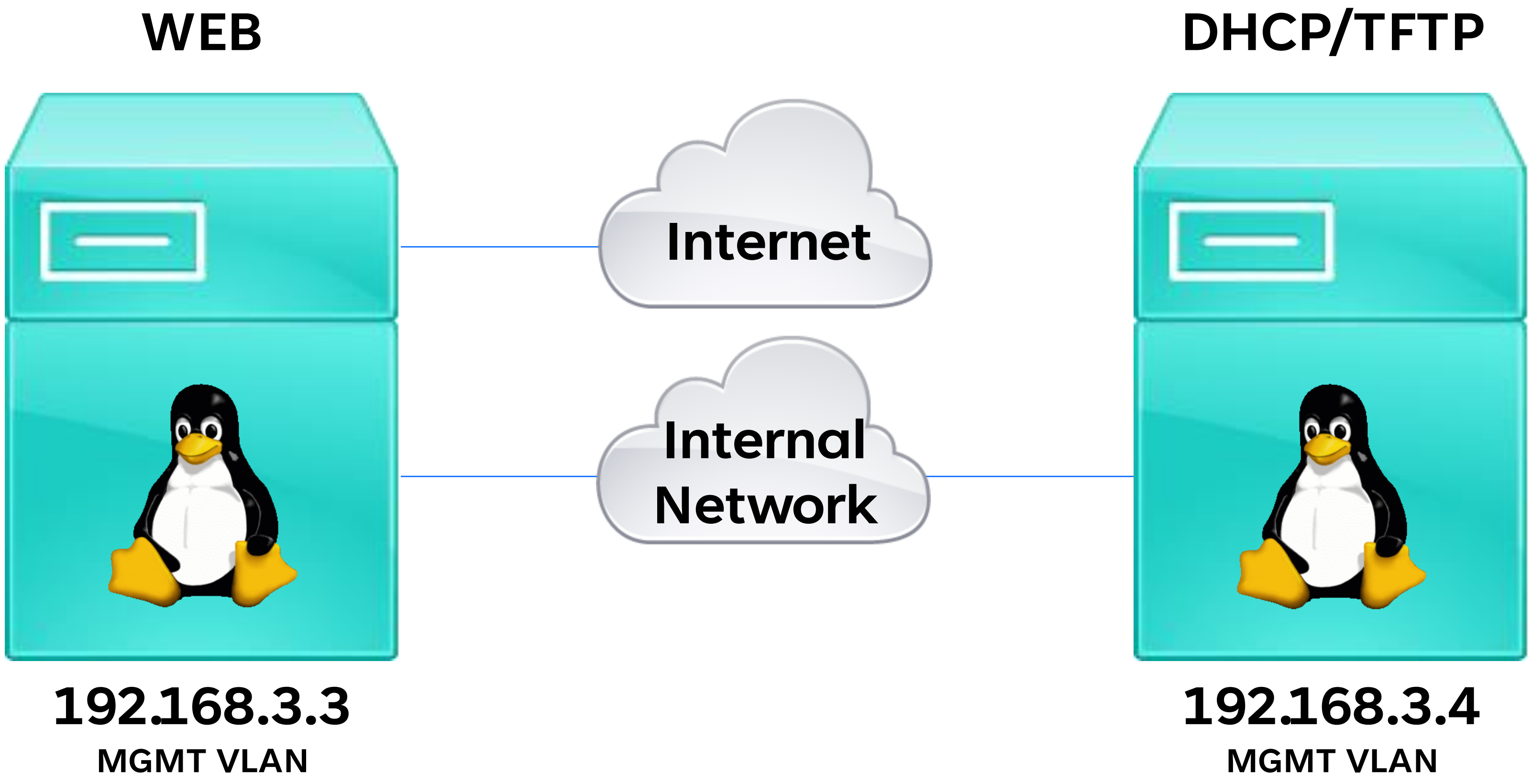
- Replicated to Veeam hourly
- Easily restored by Admins

Windows Server & Active Directory

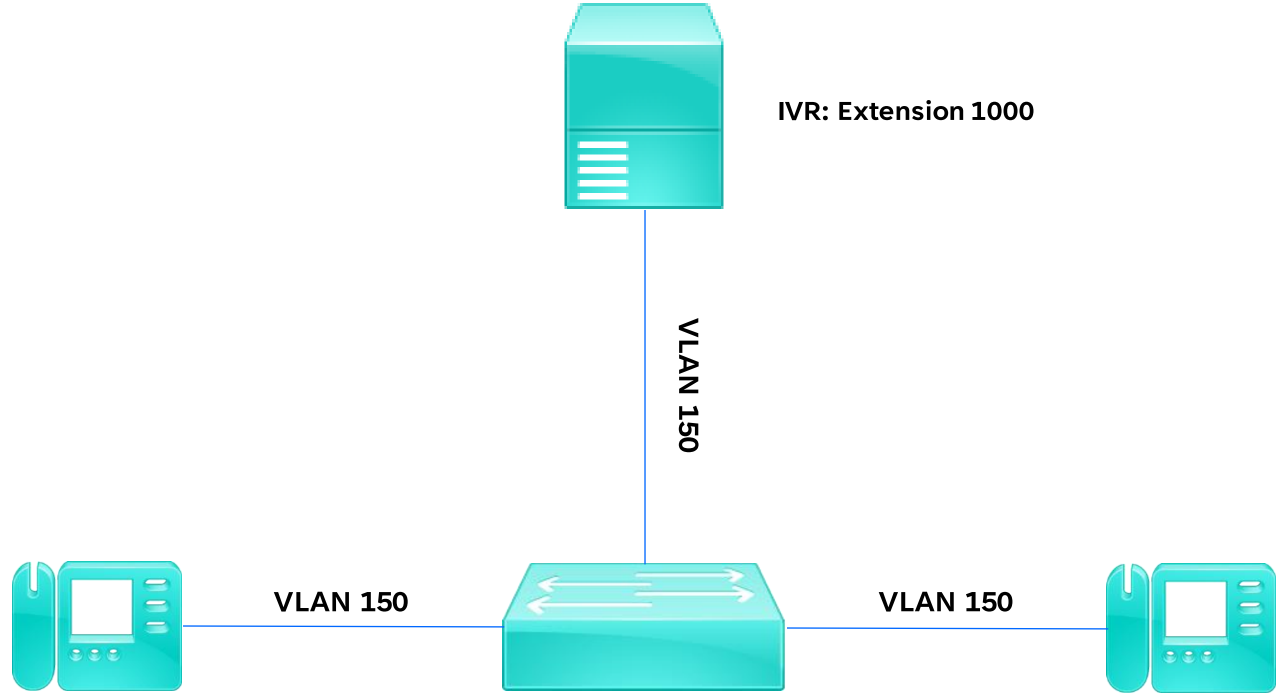
ad.energy.connections


West Campus
East Campus
DC01.ad.energy.connections
192.168.3.1
DC02.ad.energy.connections
192.168.3.2
WAN/IPsec Tunnel
DC04.ad.energy.connections
192.168.4.196

Linux Servers


WEB
DHCP/TFTP
Internet
Internal Network
192.168.3.3
MGMT VLAN
192.168.3.4
MGMT VLAN

IP Telephony



FreePBX Server

192.168.8.101

IVR: Extension 1000

VLAN 150

VLAN 150

VLAN 150

IP Phone #1 (Management)
Extension 1001

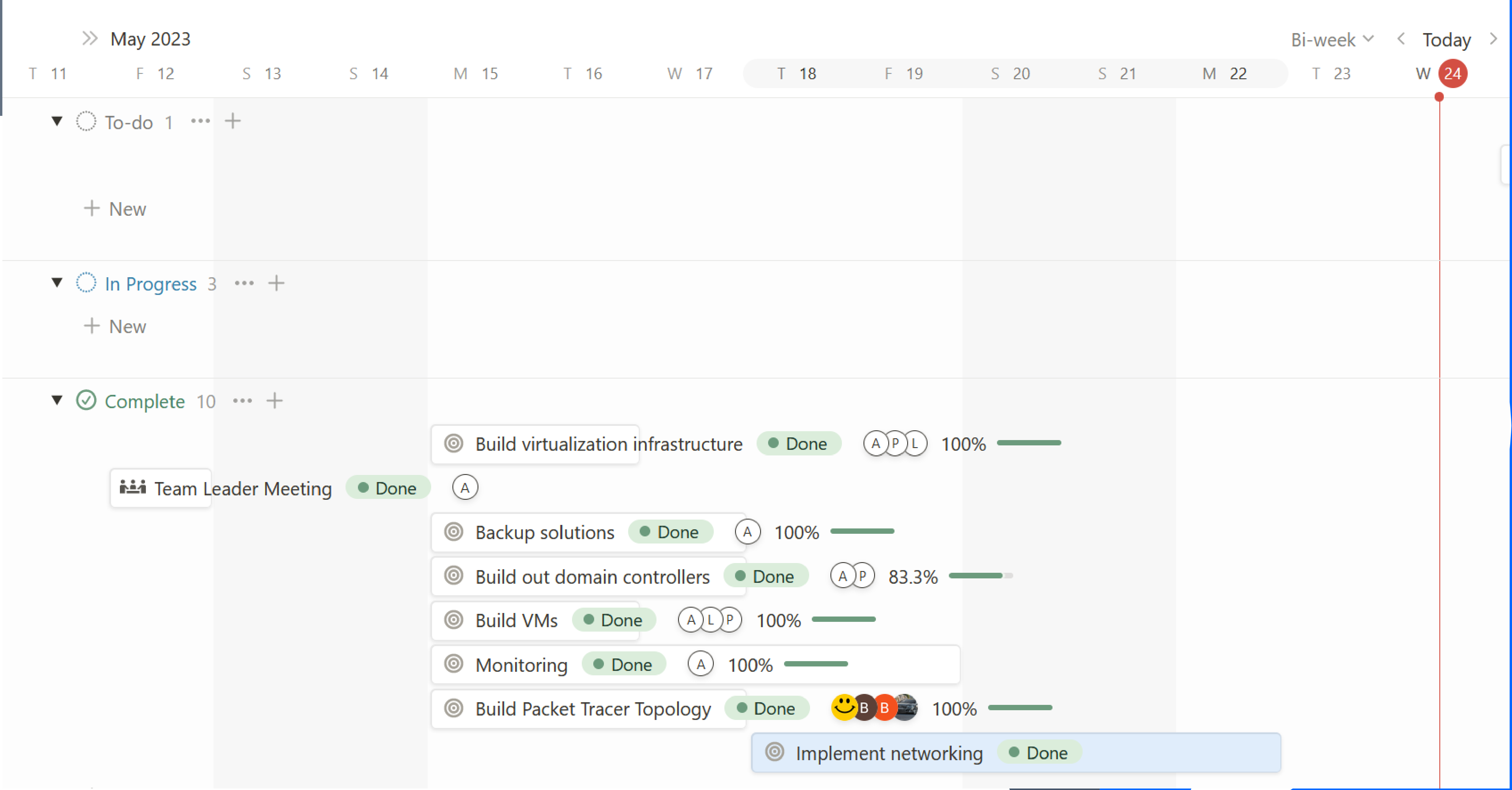
S1

IP Phone #2 (Datacentre)
Extension 1002

Project Management

Work Progress

- Arranging devices
- Designing VLAN
- Assigning IP addresses
- DHCP scope
- Routing between sites
- Secure communication between sites
- VMs
- Mission critical devices
- Network security



▼ ○ To-do 1 ••• +

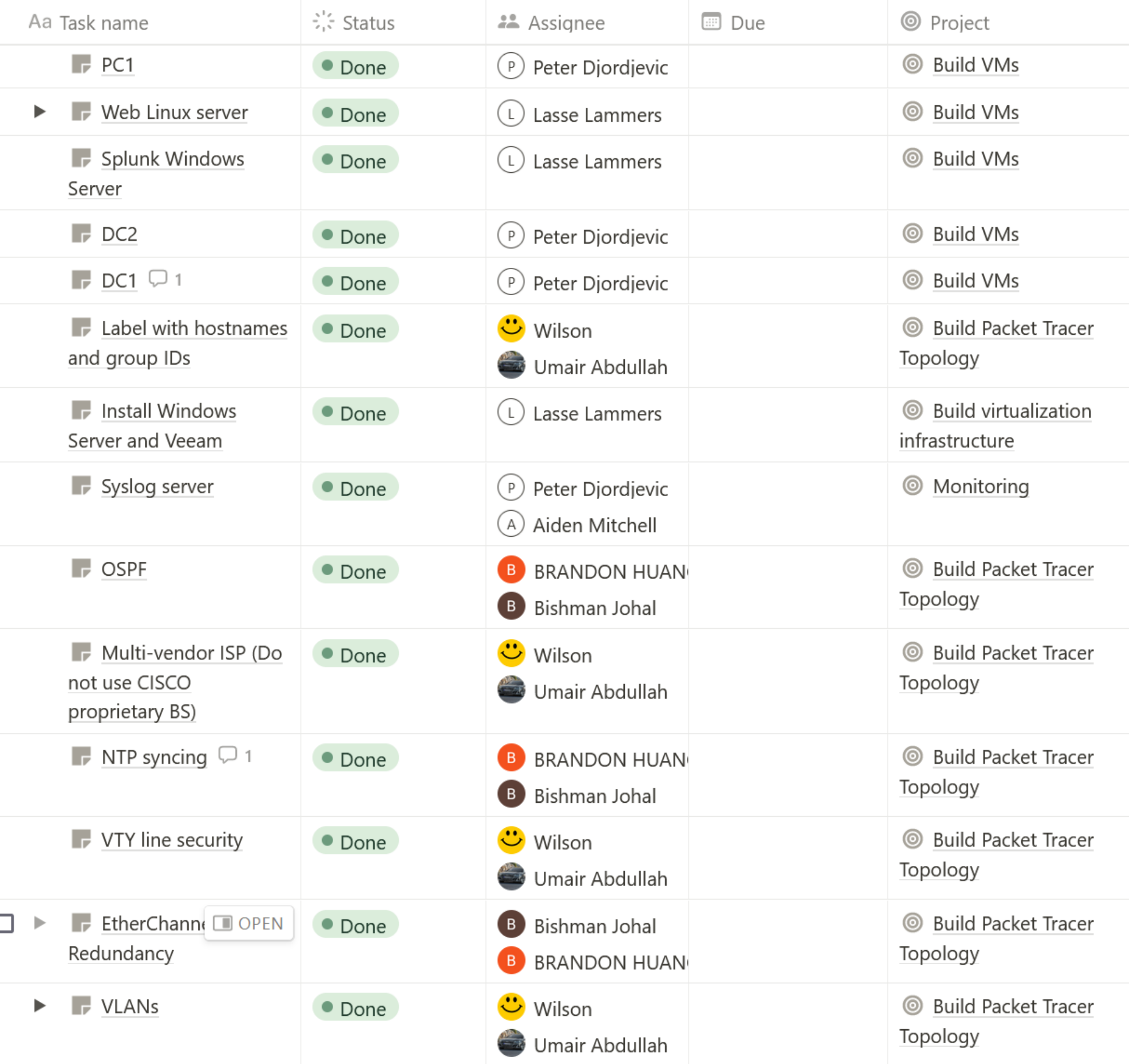
+ New

▼ ○ In Progress 3 ••• +

+ New

▼ ✓ Complete 10 ••• +

Task	Status	Assignees	Progress
Build virtualization infrastructure	● Done	A P L	100%
Team Leader Meeting	● Done	A	
Backup solutions	● Done	A	100%
Build out domain controllers	● Done	A P	83.3%
Build VMs	● Done	A L P	100%
Monitoring	● Done	A	100%
Build Packet Tracer Topology	● Done	B B	100%
Implement networking	● Done		

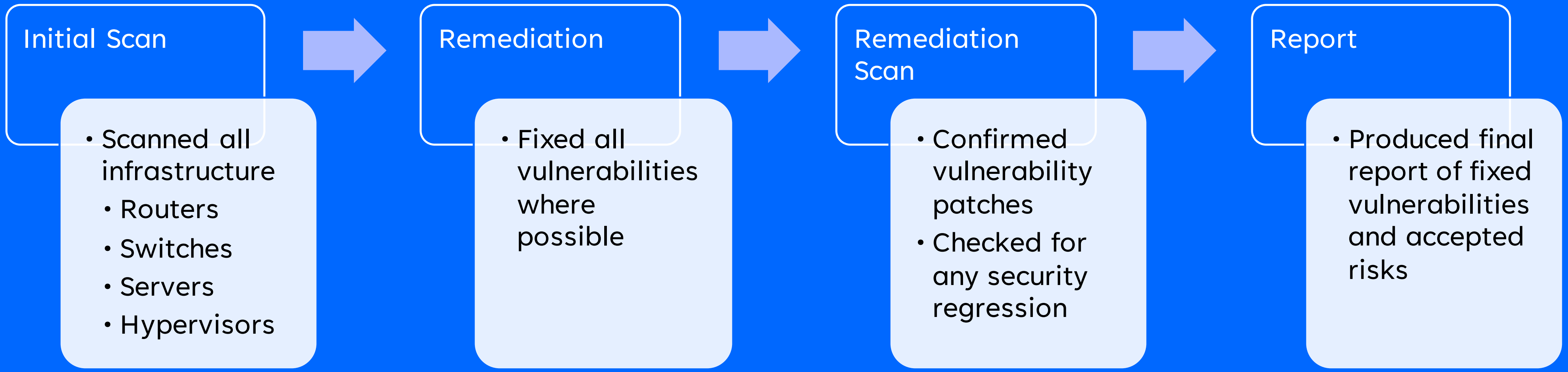


Task name	Status	Assignee	Due	Project
PC1	Done	Peter Djordjevic		Build VMs
Web Linux server	Done	Lasse Lammers		Build VMs
Splunk Windows Server	Done	Lasse Lammers		Build VMs
DC2	Done	Peter Djordjevic		Build VMs
DC1 🗨 1	Done	Peter Djordjevic		Build VMs
Label with hostnames and group IDs	Done	Wilson Umair Abdullah		Build Packet Tracer Topology
Install Windows Server and Veeam	Done	Lasse Lammers		Build virtualization infrastructure
Syslog server	Done	Peter Djordjevic Aiden Mitchell		Monitoring
OSPF	Done	BRANDON HUAN Bishman Johal		Build Packet Tracer Topology
Multi-vendor ISP (Do not use CISCO proprietary BS)	Done	Wilson Umair Abdullah		Build Packet Tracer Topology
NTP syncing 🗨 1	Done	BRANDON HUAN Bishman Johal		Build Packet Tracer Topology
VTY line security	Done	Wilson Umair Abdullah		Build Packet Tracer Topology
EtherChann OPEN Redundancy	Done	Bishman Johal BRANDON HUAN		Build Packet Tracer Topology
VLANs	Done	Wilson Umair Abdullah		Build Packet Tracer Topology

- Work went smoothly, and consistently on time
- Milestones were reached as planned
- Work output was consistent, and no significant management was necessary
- Team worked independently of the team leader where required

Security

Report Methodology



Initial Scan

- Scanned all infrastructure
  - Routers
  - Switches
  - Servers
  - Hypervisors

Remediation

- Fixed all vulnerabilities where possible

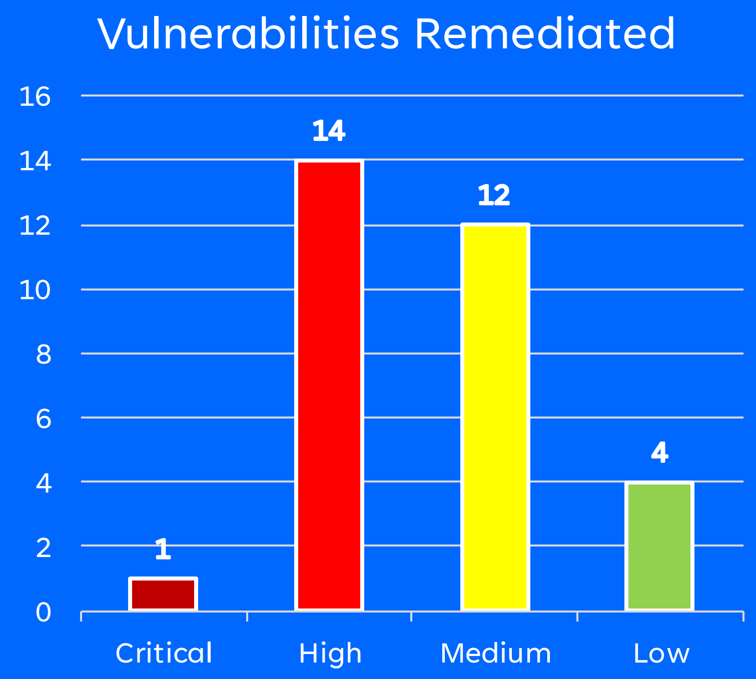
Remediation Scan

- Confirmed vulnerability patches
- Checked for any security regression

Report

- Produced final report of fixed vulnerabilities and accepted risks

Report Overview



24% decrease in vulnerabilities after remediation.

0 critical vulnerabilities after remediation.

0 Windows vulnerabilities after remediation.

- After conducting the initial scan, we fixed the vulnerabilities that were found.
- Results from the remediation scan showed a 24% decrease in the vulnerabilities.

Security Difficulties

- Cisco hardware too old for most security patches
  - Most vulnerabilities identified were from Cisco systems and routers were identified as most vulnerable.
  - All vulnerabilities that rated High and above were from Cisco systems
  - Most vulnerabilities were ranked from medium to high for the risk exposure level, and the common reason for all of them was that hardware was too old to be fixed by a software patch.

Identifier	Source of Discovery	Current Risk Exposure	Operational Requirements Rationale
10882 – Network devices	Nessus	High	SSH version cannot be updated on Cisco IOS.
97861 – Network devices	Nessus	Medium	NTP mode 6 cannot be configured on Cisco IOS.
153953 – Network devices	Nessus	Low	SSH cannot be updated on Cisco IOS.
70658 – Network devices	Nessus	Low	SSH cannot be updated on Cisco IOS.
71049 – Network devices	Nessus	Low	SSH cannot be updated on Cisco IOS.
128051 – Routers	Nessus	High	Unable to fix, hardware is too old for software patch.
148107 – Routers	Nessus	High	Unable to fix, hardware is too old for software patch.
165675 – Routers	Nessus	High	Unable to fix, hardware is too old for software patch.
129695 – Routers	Nessus	High	Unable to fix, hardware is too old for software patch.
129943 – Routers	Nessus	High	Unable to fix, hardware is too old for software patch.
148095 – Routers	Nessus	High	Unable to fix, hardware is too old for software patch.
129537 – Routers	Nessus	Medium	Unable to fix, hardware is too old for software patch.
141119 – Routers	Nessus	Medium	Unable to fix, hardware is too old for software patch.
129827 – Routers	Nessus	Medium	Unable to fix, hardware is too old for software patch.
129531 – Routers	Nessus	Medium	Unable to fix, hardware is too old for software patch.
137332 – Routers	Nessus	Medium	Unable to fix, hardware is too old for software patch.
137631 – Routers	Nessus	Medium	Unable to fix, hardware is too old for software patch.
137408 – Routers	Nessus	Medium	Unable to fix, hardware is too old for software patch.
123793 – Routers	Nessus	Medium	Unable to fix, hardware is too old for software patch.
76474 – Routers	Nessus	Medium	Unable to fix, hardware is too old for software patch.
153953 – Routers	Nessus	Low	Unable to fix, hardware is too old for software patch.

Challenges

Challenges

Redundancy was an issue due to the limitation of devices

- Implementing redundancy with few network devices was a tough decision to make as only a part of the network could be redundant with the design we came up with.

Developing the most feasible topology

- Arranging the network layout so everything is compatible while meeting all requirements and expectations.

Upgrading the old hardware

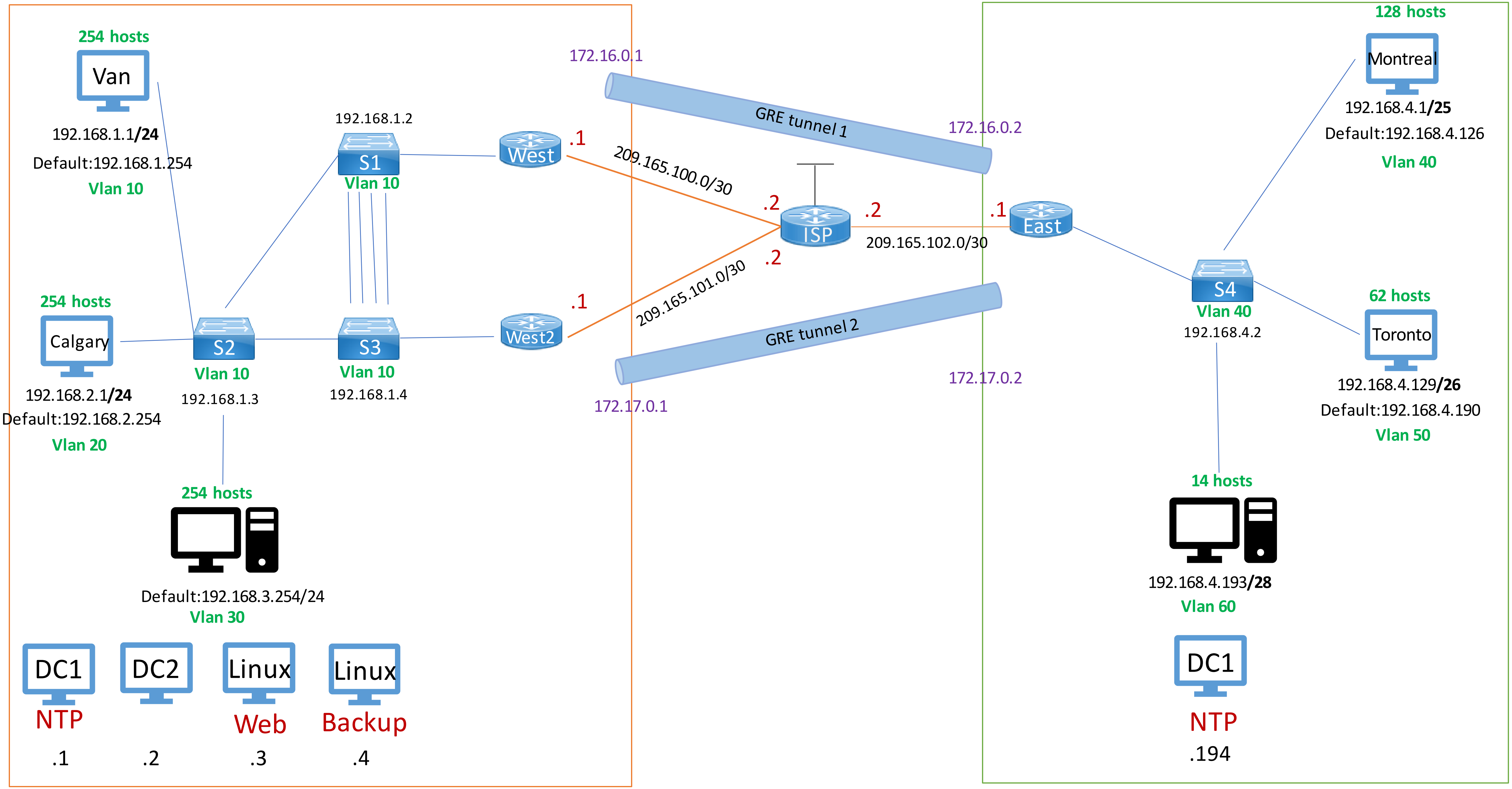
- Some devices were previously configured with older firmware, which didn't support newer security protocols, hence we had to upgrade the firmware to meet our requirements.

Troubleshooting was a lengthy process at times until the network build was nearly complete

- Router-on-a-Stick topology was difficult as it requires configuration on each sub-interface.
- A frequent issue we faced was site-to-site connectivity.

Implementing security measures was a significant challenge

- Having to ensure secure access to the network and protecting against potential threats was stressful.


254 hosts
Van
192.168.1.1/24
Default:192.168.1.254
Vlan 10
192.168.1.2
S1
Vlan 10
West
.1
172.16.0.1
GRE tunnel 1
172.16.0.2
209.165.100.0/30
.2
ISP
.2
209.165.102.0/30
.1
East
.2
209.165.101.0/30
.1
West2
GRE tunnel 2
172.17.0.1
172.17.0.2
254 hosts
Calgary
192.168.2.1/24
Default:192.168.2.254
Vlan 20
S2
Vlan 10
192.168.1.3
S3
Vlan 10
192.168.1.4
254 hosts
Default:192.168.3.254/24
Vlan 30
DC1
NTP
.1
DC2
.2
Linux
Web
.3
Linux
Backup
.4
128 hosts
Montreal
192.168.4.1/25
Default:192.168.4.126
Vlan 40
S4
Vlan 40
192.168.4.2
62 hosts
Toronto
192.168.4.129/26
Default:192.168.4.190
Vlan 50
14 hosts
192.168.4.193/28
Vlan 60
DC1
NTP
.194

Achievements

Achievements

Hypervisor & network integration

- Configuring the hypervisors to connect to our Cisco equipment for VLAN management took less time than anticipated.

Upgrading the old hardware

- Enabled SecurityK9 to be able to implement IPsec.

Vulnerability scan & remediation

- We were able to close all critical vulnerabilities and significantly decrease the number of vulnerabilities.

Teamwork

- The team worked efficiently and communicated clearly throughout the entire project.

Troubleshooting

- When issues arose, the team stepped up to the challenge and was able to fix any issues as we progressed.