IT RCSA - Infrastructure

Entity	Apple Bank
Test Name	IT Infrastructure
Test Date	4/9/2021
Process	IT-IFR-P6 Network Architecture
Sub-process	Network Segmentation
Risk # and Description	IT-IFR-R06 - Defense in-depth of the bank's network may not be effective due to poor network segmentation. As a result, the bank's most sensitive data is not appropriately isolated and secured, therefore exposing the bank to malicious attacks.
Control # and Description	**IT-IFR-C11 Network Segmentation** Network is separated into logical segments, based on the relevant trust level and inter-domain workflow, to separate data into domains related to their classification
Level of Risk	High
Control Frequency	As Needed
Process Owner	Debi Gupta
Procedures Performed for Validating Population	Inquiry, Observation, Inspection
SII(s) or Exception(s) Number(s)	Self Reported by Information Security

Test Sample

Control Test Procedures		
Test Step	**Test Procedure**	
A	Determine that the internal network is segregated from the external network	Pg. 2, 3
B	Determine that the internal network is separated into logical segments	Pg. 3
C	Determine that data is separated into domains in the context of classification level.	
D	Determine that data from disparate sources has security handled at classification level (domain) with compatible security attributes	

246 – DMZ Uplift

Schedule	G	Scope	G	Budget	G	OVERALL	G

Project Sponsor	Debi Gupta	Program Manager	Tom Ciccone	Start Date	4/27/2020	Delivery Date	2/5/2021	Report Date	JAN 30, 2021

Objective

Currently, Apple Bank does not have an inbound secured, segmented, scalable or easily manageable networking environment. This could result in compromising of our vital resources' security and network management. Since we do not have any permanent solution in place, it is restricting us to securely segregate external facing services from internal network.
In order to isolate unknown access requests and secure our information, our IT team recommended the implementation of industry standard DMZ environment. This will allow only trusted and secured traffic from internet to internal network and will provide an additional layer between untrusted and trusted network.
As we are introducing various systems, which requires exposing of our internal network, we need to ensure that our network security standards are intact. Implementing DMZ will provide an additional layer of the security for our internal network.

Network Configuration pre DMZ

- Single firewall layer – Cisco FTD
- 3rd Party B2B Vendors connected directly to ABS Network Mainframe & Core Switches
- Web traffic scanned by Cisco Access Lists & Policy Rules

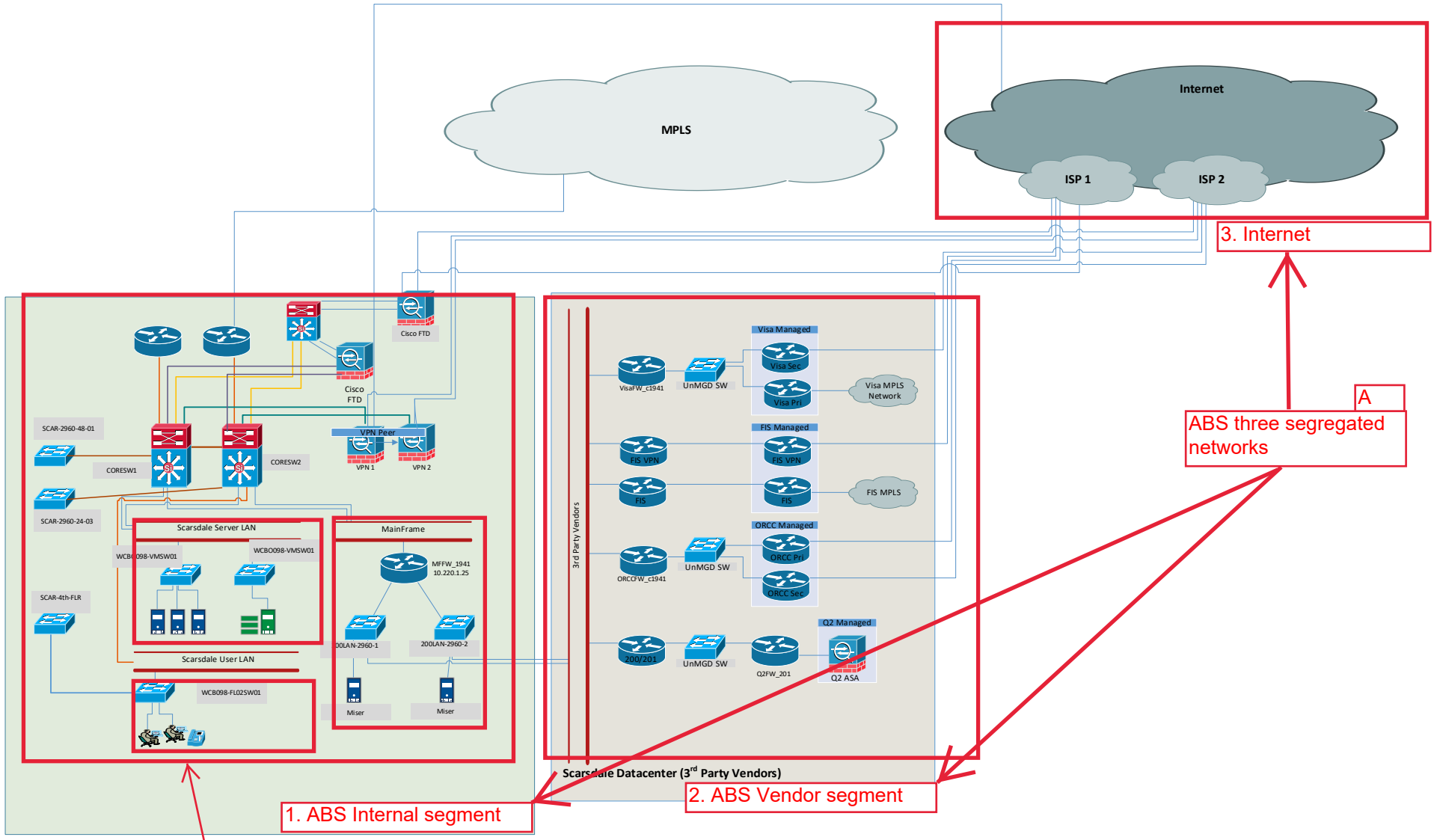
A

ABS DMZ (effective in 2021) segregated the network into three segments: internal, third-party vendors and external

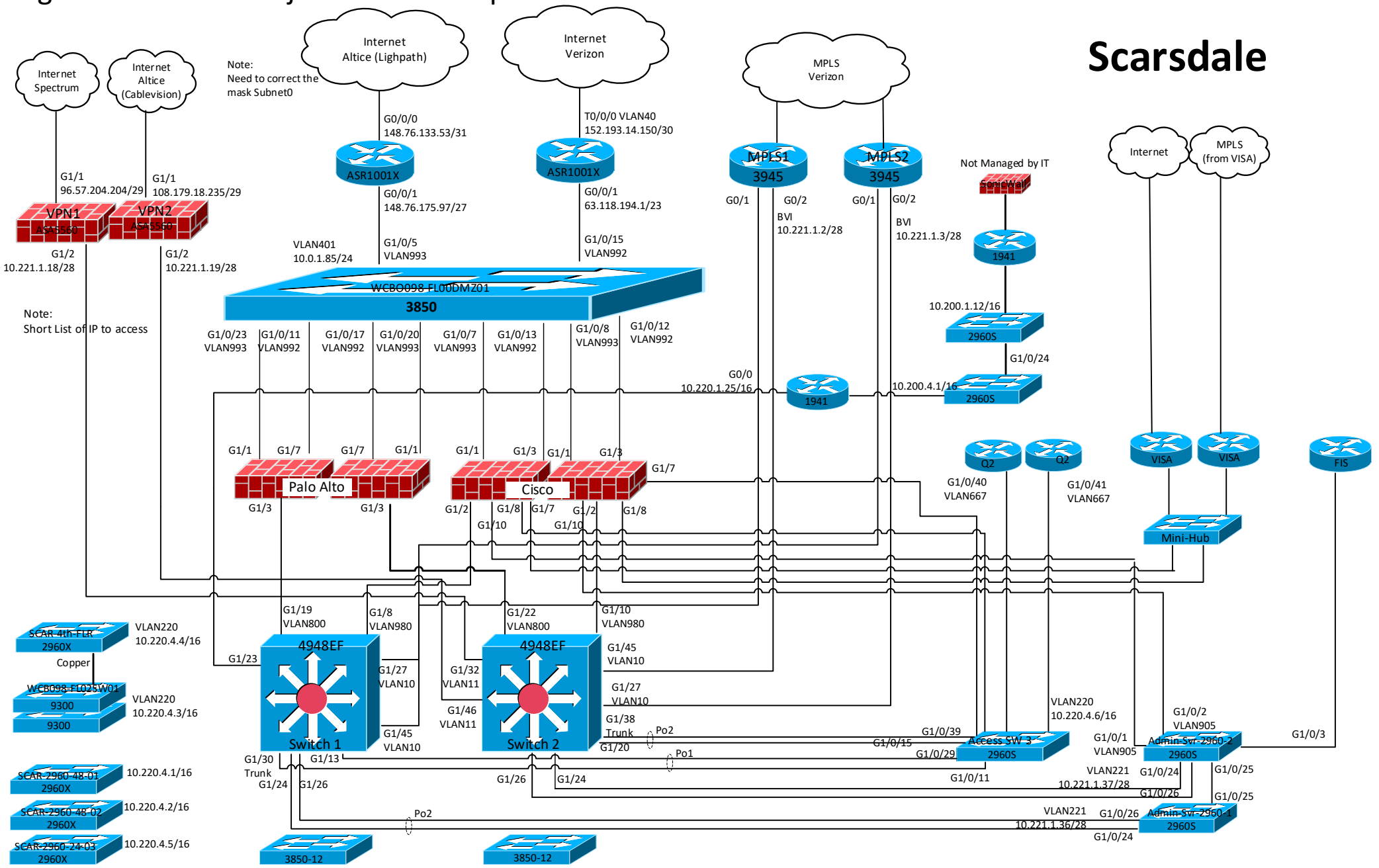
Current Network Configuration with DMZ

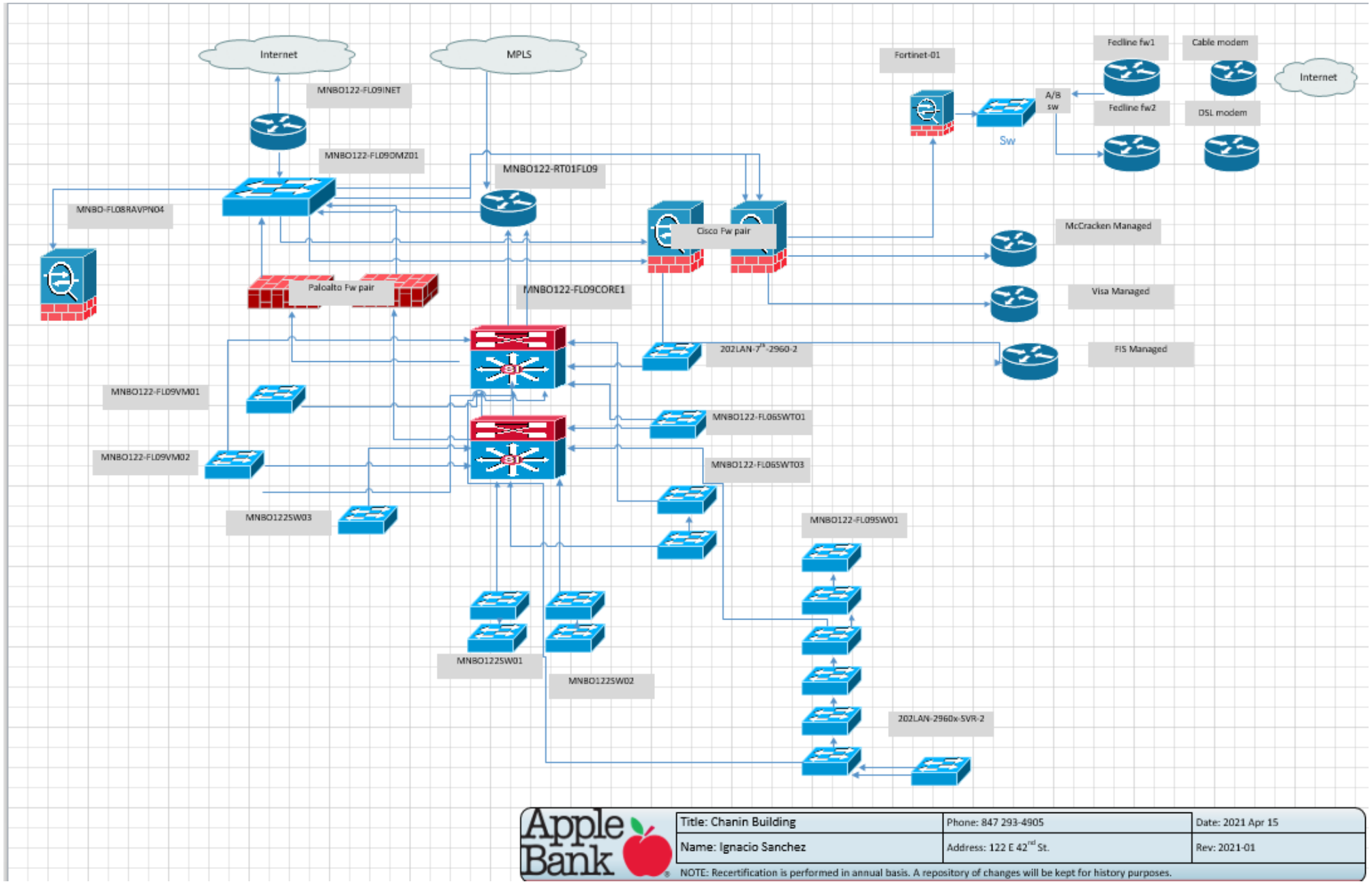
- Dual Firewall layer – External Palo Alto / B2B Concentrator Cisco FTD
- All 3rd Party Vendors assigned to dedicated segments on B2B Firewall – No direct access to ABS Network Core Switches
- URL Filtering / Web Traffic scanned by Netskope and Palo Alto threat detection
- Palo Alto Firewalls Enforce IT & InfoSec policies
- Palo Alto Firewalls generate enhanced logging and diagnosis ex. Able to resolve rule use logs down to single user, IP, or App in the GUI

Configuration at start of Project 246-DMZ Uplift



Configuration end of Project 246-DMZ Uplift




Internet
MPLS
MNBO122-FL09INET
MNBO122-FL09DMZ01
MNBO122-RT01FL09
MNBO-FL08RAVPN04
Cisco Fw pair
Paloalto Fw pair
MNBO122-FL09CORE1
MNBO122-FL09VM01
MNBO122-FL09VM02
MNBO122SW03
MNBO122SW01
MNBO122SW02
MNBO122-FL06SWT01
MNBO122-FL06SWT03
MNBO122-FL09SW01
202LAN-2960x-SVR-2
Fortinet-01
A/B sw
Sw
Fedline fw1
Fedline fw2
Cable modem
DSL modem
Internet
McCracken Managed
Visa Managed
FIS Managed
Apple Bank
Title: Chanin Building
Phone: 847 293-4905
Date: 2021 Apr 15
Name: Ignacio Sanchez
Address: 122 E 42nd St.
Rev: 2021-01
NOTE: Recertification is performed in annual basis. A repository of changes will be kept for history purposes.

Future State 2021 post Network Segmentation Project

Scarsdale