moucha.org - Next Generation Network Upgrade

Abstract: This document describes the current network design of moucha.org and the requirements for the redesign to accommodate Software Defined Networks

1. Introduction

moucha.org is an imaginary enterprise having 5 locations: 2 main locations (Prague and Plzen), further called “main locations” and 3 smaller locations (Podebrady, Ostrava and Cheb), further called “secondary locations”. The differences between the location types (main vs. secondary) are: lack of MPLS cloud connection and lack of datacentres as well as reduced redundancy degree.

All devices are (with the exception of end devices), as expected, Cisco.

2. Main Locations Description

The main locations have a classic 3 tier design. The WAN block is composed by 3 clouds: Internet, MPLS (Multi Protocol Label Switching) and PSTN (Public Service Telephone Network) vor voice services outside the VoIP network. The core routers are each connected to 2 providers in each cloud (marked by the thickened lines in the diagram).

Over the Internet, the chosen routing protocol is eBGP towards the service providers, with transit AS (Autonomous System) option turned off (our locations are not transit autonomous systems).

The core routers are Cisco ISRs (Integrated Services Routers). Their southbound connections are towards 2 Cisco FTDs (Firepower Threat Defense) running as redundant and independent devices (the policy resides on each device). The FTDs are the termination points for the VPN circuits (multipoint, point-2-point and remote access VPNs).

Westbound of the FTDs is the DMZ (Demilitarised Zone). The servers are Cisco UCS VMWare ESXi machines, with VSphere orchestration. The architecture is a thinned leaf-spine as the UCSs ()Unified Computation System) have built-in managed switches. The provided services are: web services, email, database access for external partners.

Eastbound of the FTDs is our datacentre. It is also a thinned spine-leaf design as the UCSs have built-in managed switches and they are orchestrated in VSphere. The services provided by the datacentre are:

- centralised user database - Windows Active Directory - Windows Server 2022
- CUCM (Cisco Unified Call Manager)
- Cisco Unity (multimedia server and voicemail for CUCM)
- Virtual Wireless LAN Controller
- NAS
- local cloud services - NextCloud
- VSphere server to orchestrate the VMWare ESXi UCS servers
- centralised user management - Cisco ISE 3 (Identity Services Engine)
- Certification Authority - Cisco ISE 3
- Cisco WebEx server for teleconferencing
- Cisco Jabber component for WebEx

Southbound of the FTDs are 3 Cisco Catalyst 9800 series distribution switches which terminate the VLANs. The distribution switches have embedded WLAN (Wireless LAN) software controllers.

The Access Layer is formed by Cisco Catalyst 9500 switches with PoE (Power over Ethernet) which powers the LAPs (Lightweight Accesspoints), the VoIP phones and the embedded teleconferencing systems (like cameras). The Access Layer switches are connected via MultiChassis Etherchannel to the Distribution Layer switches (no STP required, no loops). The VSL (Virtual Switch Link) between the distribution switches is required to create a single virtual switch

from the 3 discrete switches. Keep in mind that the actual number of access switches may be higher than 3 (as they are represented in the diagram).

The wireless network insures seamless roaming of devices across the wireless infrastructure.

The two main locations have their services synchronised via MPLS circuit with backup over the Internet between the two datacentres.

3. Secondary Locations Description

The secondary locations follow the exact same design, with the exception of the lacking services.

Wireless LAN Controller at the remote locations is insured by a Cisco SRE (Services Ready Engine) VMWare ESXi installed inside each CR. The same is valid for the voice network (VoIP) - the CUCM Express runs as VM (Virtual Machine) on the Cisco SRE.

The FTDs have localised policies and are managed redundantly and independently.

The remote users accounts are managed at the main sites for remote access and with a VMWare ESXi Windows Server 2022 virtual machine running on the Cisco SRE for local access. Tere is no centralised policy for the users at the remote locations.

4. Your Activity

Analyse the current network design and identify possible problems and/or inefficiencies. For example, managing so many standalone FTD appliances is a nightmare. See what Cisco FMC is.

You were asked by the management of moucha.org to redesign the network, using the latest SD-WAN and SD Access technologies from Cisco. Present the advantages and disadvantages of this redesign. Do not forget that many of the services may be virtualised and devices resold or relocated.