“Stop Me If You’ve Heard This One…” OR ”What a hot mesh”

Background:

We are happy with the first year into our security maturity journey with Fortinet since the business owners started making cybersecurity and IT hygiene a priority. Previously we had out of date ASAs acting as routers and simple ACL lists for IPSEC site-to-site and internet access. Our IT support desk staff at the time did not have the infrastructure knowledge or the cycles to maintain good infrastructure and security hygiene. Before the new mandates, the IT Team (3 desk-side support staff and a team lead as “the server guy”) would be otherwise overwhelmed with the white-glove “extra hand holding” support the users required to otherwise really look into the network and server deployments. To accommodate this it would fall largely on the support of local professional service providers to take care of some of the more specialized tasks in IT while the staff could continue making sure the lights are all on, and focusing on user day-to-day issues. Should any problems arise, these professional services would get engaged to resolve major issues. As the company grew from humble beginnings, and began acquisitions across the province the company has faced many challenges, with a longer list of business uptime needs. To combat the daily outages the company reorganized the small IT team from reporting to the CFO (for rapid access to funding as needed), to a newly hired VP of IT (later to become the CTO) who has managed much larger organizations and teams. With the years of experience brought a new future for the business.

Since then, we have moved from our HQ (6 floors and a server room) being a flat /22 VLAN which suffered outages daily, regular ransomware drive by downloads, and a gambit of power/cooling issues – to a properly designed network with great server/storage health within 6 months. Our business which grew too fast has never seen things run so smoothly…

We now have FortiGates at our HQ site, and our hosted data-center facilities where we moved our critical work loads, as well as about half our branch sites. We have moved forward with acquisitions with a standard model of hooking them to our mothership via IPSEC connections, and slowly moving them over to our posture which would eventually result in our standard branch FortiGates. We have looked at other Fortinet products in the past but have not seen much use-cases beyond FortiClient for VPN. As part of the last year, we have also started moving workloads to SaaS solutions where possible. Our Email, HR systems, Payroll, Intranet, and many other common apps have all been moved to SaaS or PaaS providers.

The business has now started doing acquisitions outside of the province and has on-boarded a business in Victoria, BC and plans in 6 months to onboard another large firm in Markham, ON.

Now that the team has proven a strong service delivery model, their next big endeavour is to provide a bullet proof IT Services Catalogue to our now largest brokerage in Canada maintaining our security milestones and progress. We have been uneasy since renting space in the hosted datacenter as it has passed ownership nearly 3 times since we began working with them and believe now is a good time to start thinking about a “cloud based server room”…

Audience:

The specialist engineers and now CTO have been working with Fortinet and other vendors to accomplish the various cleanup and improvement activities. Now that they are ready to start talking about IaaS to service the interprovincial needs of the business they have invited your team to the table. The CTO has been far removed from the "nuts and bolts" of IT for many years but has maintained the necessary knowledge to lead progress with IT and Security trends. As a courtesy, the CFO has been invited as they have also been receiving positive recognition to the lower overhead costs IT spends have had by way of the CTO. The CFO agreed to join but admits they may get a bit lost on the details. However, the CTO and his engineers are very excited to dive into the details.

<u>In attendance will be:</u>
CTO
CFO
Network Systems Engineer
Server Systems Engineer
Desktop Support Specialist

Additional Information:

- Since the CTO was hired the local LAN and Server infrastructure had been normalized (yay – no more network loops!)
- We forklifted our server room to Z9 (which became) Gell (which became) Equifix's Colo which helped deal with all our environmental issues
- We have deployed Fortigates into our existing acquisitions, HQ, and Colo
- 3 months ago we just moved into new office space and refreshed our switching to FortiSwitch in the process
- We are enjoying the benefits of SD-WAN at sites with Fortigates
- We now maintain HA posture at any Fortinet site we operate.
- Ideally, we want a solution that could be central to our coast-to-coast operation.
- We have not seen a single ransomware instance amongst our users since the modernizations began.
- We have goals to further bolster our endpoint security and visibility into Shadow IT
- Most of our public facing websites are informational only and hosted at various providers (rackspace and digital ocean currently)
    - These websites for the various acquisitions constantly are attacked, with various messages replacing the frontpage.
    - Our IT team has advised this is due to vulnerable code or underlying webservices they claim to not have control of
    - The website designers simply charge us and redeploy the page until it happens again in a few months.
    - We are interested in resolving this but not interested in hosting the webservers ourselves ~~and have started looking at SaaS tools~~