SECURE ARCHITECTURE FOR A MODERN ORGANISATION

Report By 

Carlow Institute of Technology
Network And Cloud Security

Word Count 8925

Introduction

This report outlines a plan to create a secure infrastructure for a fictional business called company.com, which has multiple sites. At each step in the design and implementation process we will have security in mind and apply it in all locations. Resilient infrastructure will be a part of this design and will encompass all data storage and site failover for our users and customers. Securing access to resources while allowing business continuity is the primary concern as the transition from legacy to modern infrastructure is completed.

Problem Analysis

There are multiple sites to take into account and also the cloud infrastructure. The primary location with the most users and office space is Site A and will have the largest amount of data and users to secure. The secondary site, Site B, will be used for hot failover and high availability of services as well as location-based access to resources so that Site B users go to site b for data and services unless they are unavailable so then will go to Site A. The smaller of the three locations, Site C will be used as an offsite backup location for resiliency and backup storage. Similarly, this will be used as a minimum viable services site and will tertiary resource for site resiliency of services. The Cloud infrastructure consists of Azure AD and a public facing static web site.

Overview of Current systems layout

Site A

3 Domain Controllers

2 Exchange 2013 servers

4 File/print Servers

2 Terminal Services Servers

2 SQL Database Servers

2 Sharepoint Servers

2 Salesforce application servers

1 backup server

8 web servers (Partner Portal, Accounting expenses portal, Shipping Portal, Salesforce portal)

1 Fortinet Gateway router

3 of 48 port gigabit cisco catalyst switches

8 of 48 port Dell switches

6 Wireless access points from various manufacturers

Site B

2 Domain controller

2 Exchange 2013 Server

2 file/print server

1 backup server

1 Cisco 800 series router

2 of 48 port dell switches

2 wireless access point

Site C

1 Domain controller

1 Exchange server

1 file/print server

1 NAS (Network attached Storage) unit 4TB

1 Cisco 800 series router

2 of 24 port netgear switch

1 wireless access point

Cloud Resources

Azure AD

Publicly facing static site with contact page

Security Issues found with current design

- Currently an outage of the exchange servers on Site A takes email out for everyone on site A and C and no failover to site B.
- Backups are done to the local backup server. All backups are on their own site. A loss of one site would lose all data for that site.
- All terminal servers are on site A, if the internet link drops here all remote users are affected
- Site A has all the remote users and the web sites connecting through one internet connection
- Virtualisation is not in use for the majority of servers. Physical device still in use
- Publicly facing web servers with sensitive information are just straight Network Address Translation (NAT) from the internet without any Web Application Firewall (WAF) or Intrusion Detection System/Intrusion Prevention System (IDS/IPS) or Single Sign On (SSO) controls
- Flat Network in each location with no isolation and no Virtual Local Area networks (VLANs)
- Lax password policy
- Lax permissions policy
- Multiple HIDS (Host Intrusion Detection System) in use, some out of date, not centrally managed
- Poor logging and visibility of devices and infrastructure
- Front doors are open with no-one on reception duty for site B and C
- Outdated SSLv3 and TLS 1.0, 1.1 still in use for website access
- Weak ciphers used for web site access (3DES, RC4, CAMELLIA)
- No certificate management or responsible person for renewing
- No centralised patch management
- Site C has no power protection for its equipment
- Unlicenced software and non-standard software in use across sites
- Very little spam protection
- No balancing of network resources. Some servers are at max while others are idling
- No centralised Security Information and Event Management (SIEM) or Flow monitoring
- Local admin rights for machines in most departments
- No responsible person in each department for security or Information technology (IT)
- Multiple personal devices used for access externally with little to no security restrictions
- No tracking on data to see if a file is copied out of the network
- Portable storage devices not disallowed
- Multi-Factor Authentication (MFA) authorisation not in use

- No Network monitoring or service monitoring in operation
- Lack of training on security for staff and board members
- No framework compliance in use
- No active General Data Protection Regulation (GDPR) policy
- No security team or Chief Information Security Officer (CISO)
- Wireless Fidelity (WiFi) is Wired Equivalent Privacy (WEP) with no isolation nor dedicated guest network
- No inventory tracking either on prem or with road warriors
- No Change control policy

Architecture and Orchestration

Site A

Site A is the largest site with 355 users. It will have a pair of SonicWall NSa 6700 series firewalls in High Availability mode and will be linked to both site B and C via Site-to-site Virtual Private network (VPN). Locating the Network Operations Centre/Security Operations Centre (NOC/SOC) here makes the most sense as the main services will be hosted on this site as first preference. A Mimecast Spam filtering service off-site will reduce the amount of traffic coming to the internet connection. We will use Dark trace to further filter email in house. We will use Geographic Location (GEO) balancing to have site failover from site A to B and C for web, database, ADFS, and email services. We will use Kemp Load balancers to balance traffic and use the Edge Security Pack (ESP) for Single Sign On (SSO) and Web Application Firewall (WAF) for web apps and exchange access. All web services will be in the De-Militarized Zone (DMZ) for external access and internally will have balanced services on the internal Local Area Network (LAN).

Site B

Site B has almost as many users as site A with 260 users. It will have a single SonicWall NSa 5700 series firewall and will be linked to both site A and C via Site-to-site VPN. This will have an active/active site redundancy where all databases are in Database Availability Group (DAG) and failover is automatic. Similarly, with SharePoint, Active Directory and Web portals. Local users will use local resources as much as possible but will fail over to any available site if the services become unavailable.

Site C

Site C uses Site-to-site VPN to connect to Site A and B. They are a relatively small site with only 35 users. This site can be used as a backup location for site A and B and will take part in the deduplication

of data in the backup software. This site will have a single SonicWall NSa 4700. It will also be the last failover site for geo balancing of services.

Main body

The company has grown fast and acquired other companies in its expansion. As such there is no coherence in the design layout or devices across the networks. To address these multiple areas of deficiency the task will be broken down into the following areas.

- Frameworks, compliance, and governance
- Training and education
- Logical Security
- Resiliency
- Remote Access Security
- Physical Security

These areas will be further broken down in their sections and lists of subheadings will be used for ease of reading.

Frameworks, compliance, and governance

The initial task in understanding any network is to do an inventory of what is currently in place. To gather that information, LanSweeper was used. This installed on a PC and was used to scan the network in all three locations. This allowed a baseline to be created which gave an understanding of the undertaking required to bring the networks and infrastructure into compliance. Feeding this information into the Cobit 2019 design tool allowed the highlighting of areas required to focus on and work towards a more secure, resilient, and compliant system.

A CISO should be appointed, and a dedicated security team and network team should be implemented to manage the systems going forward. Part of this compliance requirement came from a data loss security incident and has presently turned the boards attention to a relatively ignored section of the business. They have set the goal of complying with the National Institute of Standards and technology (NIST) SP800 53 R5 standard and perhaps at a later date of engaging with the International

Organization for Standardization (ISO) 27001 framework for compliance and certification. To ensure that this goal is met in a timely manner the board have allocated a large budget to get the company on track and to refresh the infrastructure to acceptable standards. The regular auditing of the system is the CISOs responsibility and will act as a board liaison to the security team to direct the business needs of the infrastructure and assignation of projects to teams.

The regular testing of the security will be undertaken not only by the SOC teams but also by an external consultancy (AT&T penetration testing services) to ensure all bases are covered and regular examinations are carried out to feedback into security design.

A Change control policy will be implemented company wide for all resources but will vary in detail depending on the type of device being modified.

The CISO will also be advised of the required budget for new implementations of hardware or software and will bring the requests to the board on behalf of the security teams.

A new message of the day will be implemented network wide for all devices and the acceptable usage policy will be displayed before login on systems.

An encryption policy for all business mobile devices will be implemented. The accounts drives will also be encrypted at rest. All databases will be salted and access restricted.

A data encryption policy for sensitive information is to be implemented with AES encryption as standard.

Access control policies based on least privilege is to be implemented across all departments and Multi-Factor Authentication (MFA) to be used wherever appropriate. A zero-trust architecture is to be the default for any resource access.

A theft or loss of device policy was implemented so that any loss of a company device or data would be reported in a timely manner and steps taken to secure that data.

Certificates now to be managed directly by the SOC and wild card certs to be eliminated as much as possible. All certs will be SHA384 and keys to be 2048bit of higher. DigiCert to be used for all public facing certificates.

A proper onboarding and offboarding procedures are to be developed with the assistance of Human Resources (HR) and IT support staff and the SOC/NOC. Timely creation and disabling of privileges is a must and should be communicated directly to the SOC and NOC.

A policy will be implemented so that only senior staff in the NOC will be allowed to manage the external Domain Name System (DNS) and will be responsible for the update, removal and insertion of DNS records.

Device recycling or repurpose policy to be established where termination of devices is set to be one year after retirement data and all data securely erased and then checked before repurposing for schools or recycling.

Training and education

In most cases the Cobit 2019 report indicated that security was not a high priority in the day-to-day business and that the majority of end users considered it to be someone else's job. To combat this a training and education plan was drawn up.

To start with a new Acceptable usage policy" was drawn up and had to be read and digitally signed by every member of staff.

The password reset procedure was introduced which included verification of ID before resetting of a password regardless of the end users position in the company. No staff member, no matter how senior, could bypass the requirements for setting or resetting a password. Once complete the new password policy was implemented with the addition of MFA wherever possible.

Each user had a compulsory video training session on security which included phishing, passwords, bad security practices, social engineering and scamming.

A special email account for suspected spam or phishing messages was activated and the staff were advised if they got any suspicious message not to click on any links but to forward the message to this new email address.

Training for staff will need to be refreshed regularly with a compulsory re-taking of the security awareness training on an annual basis.

To ensure the security, networking and infrastructure teams stay up to date with current trends, a bonus scheme was introduced for every relevant certification acquired by an individual.

A Breach procedure to be drawn up which notifies all departments of their responsibilities in case of breach and readiness tests to be implemented on a bi-annual basis. Security is everyone business not just the SOC.

Logical Security

This encompasses the meat and bones of the task to be undertaken. This is going to be broken down into sections to highlight the different steps to be taken, new equipment to be installed, policies to be implemented and separation of networks and services by department and location. There is an overlap with the resiliency in some areas, but this will be indicated.

Firewalls

It was decided that a complete renovation of the firewalls on site was required. SonicWALL with its inbuilt security capabilities were chosen to replace the aging hardware that was in position. Centrally managed from the SOC/NOC using MFA sign on, these SonicWALL devices will all offer the following features, Stateful packet inspection (SPI), Deep Packet Inspection (DPI), Deep packet Inspection for Secure Socket layer (DPI SSL), Advanced Threat Protection (ATP), IPS/IDS, Anti malware, Gateway Anti-Virus (AV), Gateway Anti Spyware, GEO Internet Protocol (IP), Botnet filtering, Content filtering service, VPN endpoint, Internet-connection load balancing. In addition, these SonicWALL devices can use one of their ports to stream the IP Flow Information Export (IPFIX) information to the Flowmon collector and have it analysed further. Any changes on these devices requires a change control request and possible impact analysis report before modification. These devices will backup their configuration on a nightly basis to the centrally managed software in the SOC.

Internet connections

The current model of using one provider for a high bandwidth connection was not fault tolerant and if one set of public IPs were DDoS'ed then it would take a site down. To help alleviate this, two Internet Service Providers (ISP's) are required on each site with load balancing between the interfaces and in the case of Site A, a failover router to ensure uptime. The primary link will be gigabit speed while the secondary line should be 500Mb or better.

DMZ

Setup a DMZ in each site maintaining a separation of internet access from internal resources directly. All externally available resources are to be hosted on the Kemp Load balancer to increase security. The Load balancers will use the best practices cipher set and TLS 1.2/1.3 only when setting up SSL accelerated services. To further enhance security the ESP for SSO will be leveraged together with SAML MFA from the Azure AD instance. On any site that supports it, WAF will be enabled and tuned to the application so that the Open Web Application Security Project (OWASP) ruleset will detect any out of bound request. The Kemp Load balancer will also setup a port 25 and 587 service for SMTP/SMTPS that will only accept connections from the spam filter IP addresses. The Kemp Load balancers will take advantage of their network telemetry feature to send the IPFIX flow information directly to the Flowmon collector on a dedicated 10GB fibre interface. All VLANs will be implemented

on a bonded 40GB (4 x 10GB LACP bond) interface on the Load Balancers for internal connection to the core switches. Port 53 TCP and UDP will be forwarded to the DMZ interface address of the kemp so that the GEO balancing can be utilized. Two of the LM X15s will be used in a High Availability (HA) pair on Site A and another HA pair on site B. A Virtual Load Balancer in HA will be utilised on Site C and will have similar features but lower bandwidth for budgetary reasons. A separate VLAN will be used to manage all network devices and will be accessible from the network and security team alone.

Site to site VPN

SonicWALL built in site-to-site VPN will allow for connectivity between site A, B and C in a secure manner. While not as secure as dark fibre it is significantly cheaper and will suit the current needs of the business. The Access Control List (ACL) on each router will ensure only the IP of the other sites can attempt to connect via the site-to-site VPN. Since all sites will have 2 VPNs connecting them, they will have redundancy and failover built in.

GEO Balancing

GEO proximity-based access and site failover of web resources and email will allow for redundant services on the three locations. There will be an internal and external health checked resource on each site with different weights and locations aware returns for DNS queries to the GEO function on the Load balancers.

Anti-Virus/Anti-Malware

ESET for fully managed Host Intrusion Detection System/Host intrusion Prevention System (HIDS/HIPS) network wide including mobile device's. It will be centrally managed from the SOC. Gateway anti-virus and anti-malware will be enabled on the SonicWALL firewalls and managed from the SOC also. On the Kemp Load Balancer services, the IDS and WAF will be utilised, together with ACLs and IP reputation rules.

Switching

The current Dell switches will be re-utilized depending on performance and capability. The firmware on each switch is to be upgraded and any that support it will have 10Gb fibre modules added for redundant Link Aggregation Control Protocol (LACP) bonds for trunking and stacking. All unused ports are to be disabled. There will also be mirrored 10GB fibre ports for network telemetry taps setup on each switch and fed to Flowmon probes. Any switches that cannot be leveraged will be replaced by Dell EMC Networking N3200-ON_OS6 with 100GB stacking ports. The SAN's and VMware Hosts are to utilize the Dell EMC Power Switch S4148FE-ON and leverage the 100GB stacking backbone between switches so that the hosts and SAN have the highest bandwidth. These will be interconnected to give a mesh topology for SAN and Host access.

VLAN

VLANs to be setup for all departments, on the new VMware Host machines and on the Dell switching network. This will mean sensitive information is never accessible outside of the relevant VLAN. Each internal device that accesses a VLAN will be part of a MAC ACL so that no unknown MACs are allowed to plug into the network. A separate VLAN subnet for all managed network devices will be used to get all the SNMP, Syslog and Alert data from devices. This will also allow a dedicated configuration network used to gain configuration access for things like iLO and iDRAC on physical machines and for configuring the sonic walls, Dell Switches and Kemp load balancers. The SOC/NOC will also have a dedicated VLAN for IPFIX information separate to the normal network so that network taps can be used to collect all information on a network without unduly flooding a production VLAN with packets.

SIEM

Alien Vault Open-Source Security Information and Event Management (OSSIM) will be leveraged for SIEM in the new SOC/NOC on site A. Data will be fed by collectors to site A where the database will be maintained. The Flowmon collector will filter alerts so that the Alien Vault will not be flooded with extraneous alerts. It will collect all Syslog and SNMP data from network devices and will be setup to alert the security team when an Indicator of Compromise (IoC) is determined. Data will be maintained for a period of 6 weeks locally and in the archive for 3 years. There is the option to go for Alien Vault USM at a later date.

IPFIX

Flowmon will be used for service availability monitoring and network monitoring on NOC. Leveraging this data will also be the Flowmon security operations which will feed alerts directly to Alien Vault. This will leverage the Kemp Network telemetry directly and will also have network Taps to collect all information flowing on the network. The NOC team will be in charge of this data collection and will be on a separate VLAN for security and performance. The data will be maintained for 3 months locally and archived for 3 years. A report is to be generated each month on usage and events so that baselines are kept up to date and alert triggering is more accurate for the SOC. Any out of band events are to be highlighted to the SOC team immediately.

Public Web Site

The publicly accessible website hosted in Azure is to be set to port 443 only with TLS 1.2, 1.3 and with secure cipher set used. The contact page will obfuscate the contact email within it to prevent bot harvesting. The page is to be replicated in 3 regions and leverage Microsoft Cloud Defender and Azure DDoS protection. Azure intelligent security graphing will report directly to the SOC for alerting and reporting.

Azure AD

Leveraging the use of Microsoft Azure Active Directory allows the use of Security Assertion Markup Language (SAML) and MFA for authentication of web services across all departments. The inbuilt Deep Learning and analytics allows a secure authentication method to be utilized and to report to the SOC of any anomalies. This will also aid in governance and compliance with reports easily accessible.

Updating Software

There will be a Windows Software Update Service (WSUS) server located in each site which will be maintained by the NOC staff. When updates for Operating Systems (OS's) and MicroSoft (MS) Software are approved, they will be distributed via the WSUS servers on site to reduce overall bandwidth usage.

Sales Force and other third-party updates will be the responsibility of the application owners to test in a sandbox before deployment to production.

Group Policy Object (GPO) will be used to enforce application security levels and updates where appropriate. These will be applied at logon and refresh intervals during the day.

Firmware updates on all networking and server equipment to be undertaken regularly with change control and test in sandbox before rolling out.

Forward Proxy

For user's internet access we will use the Barracuda Web Security Gateway 810 on Site A and B and the Barracuda Web Security Gateway 310 on Site C. This will be centrally managed for web filtering, SSL inspection of outbound traffic, DNS filtering and social media monitoring.

DNS

We will leverage the OpenDNS and Umbrella DNS project by utilizing a PiHole DNS for forward DNS lookups. This will filter out any extraneous and dangerous DNS resolutions on each site and will prevent DNS hijacking. It will also act as a DNS black hole for malware or intrusions present on a network by not resolving to known bad IPs, proxies or The Onion Router (TOR) networks. Using DNS Security Extensions (DNSSEC) on forward lookups will also give greater assurance that the resolution is correct.

WiFi

Current Wi-Fi devices are to be replaced with Cisco MR57 Cloud-managed Wi-Fi 6E access points which will be centrally managed through Meraki. This replaces the multitude of different types of Wi-Fi access points located throughout the sites. For authentication internally a SAML login is required for Wi-Fi use, this will prevent war driving. Bandwidth shaping can be used for application management to give users application priority for business use. Wireless isolation is standard and client location

identification and tracking will be enabled. This will be liked through Meraki to the Closed-Circuit Television (CCTV) system and if an alert is triggered the devices will highlight who is in each location at the time.

A separate WiFi access channel will be used for guest access and only in certain areas. This will have a login page where the guest user can enter their credentials to gain access. They will be isolated via VLAN's and will not have access to any local resource.

EMAIL Security

External Email Spam filtering will be utilized as an easy early win in terms of security but will be greatly enhanced with the use of ACL on the KEMP to prevent email from any outside source other than the spam filtering service from delivering email effectively closing the open relay. On the KEMP itself, ESP logging of connections will be fed to the SIEM and domain filtering will also be used to only accept email destined for the local domain with STARTTLS used for encrypted delivery. The exchange servers are to be updated to Exchange 2019 on prem and DARK TRACE software installed to monitor and report on usage, traffic analysis and phishing protection. Leveraging the Kemp ESP will allow external access to Outlook Web Access (OWA) with SSO MFA using SAML and Azure AD. Site failover and location aware DNS response will limit the overuse of inter-site bandwidth and a customised Login Page presented by the KEMP will ensure that the users easily know that the page they are putting their credentials into is the correct one.

ADFS

Onsite implementation of Active Directory Federation Service (ADFS) to be deployed for access to SharePoint and partner portal for partner access to resources. This will be limited to read only sections and orders are to be placed via email to the sales department.

SOC/NOC passwords

With all this new equipment and logins required a password manager for the team will be required. Dashlane Business is a very secure AES 256bit encrypted password manager that can be used by multiple users to share business passwords for equipment and software in a secure manner. This has the ability to have multiple levels of access so that only a limited few have the access rights to change passwords and enter new or remove old passwords. This will be directly managed by the CISO and will have rights assigned as the Security or Network team member requires.

Subnetting

All departments are to have their own subnet for their VLAN on each site. The Class A private network will be reserved for DMZ and management VLAN's and split accordingly.

Resiliency

Infrastructure

New Virtualisation infrastructure will be utilized in this deployment. Migration form physical to virtual will be done with the vendors on standby for any issues. We will have 3 VMware ESXi hosts on Site A, and 2 VMware ESXi on Site B, with a further 1 on Site C. One VMware ESXi host will be reserved for sandboxing and development on site A. These will be Dell PowerEdge R940xa Rack Servers with 4 processor sockets with 28 cores each and a redundant array of 4TB of RAM. The OS disk will be RAID5 SSD's. They will have redundant Power supplies and have Integrated Dell Remote Access Controller (iDRAC) enabled. Each VM is to be duplicated to a hot standby with a 30 second failover leveraging Vmotion and Fault Tolerance (FT). A cold standby image of each will be located off site. They will have Internet Small Computer Systems Interface (iSCSI) attached drives where all the Virtual machines will be located. The SAN's will be Dell Power Vault ME5 Storage devices with 450TB storage on Site A, 300TB of storage on Site B and a 150TB storage on Site C. They will use Dell ADAPT (Distributed RAID) data protection for the arrays which replaces the older RAID system with network aware RAID across devices for data redundancy. This is quicker and dynamically restores data from lost disks on the fly without having to shut down the systems. They can also be expanded dynamically as the need arises. With 8PB as the maximum storage for one SAN this leaves a lot of headroom for future expansion.

Backup Software and Storage will be via Dell Power Protect DD Virtual Edition software with the Dell Power Protect DP4400 Appliance to provide storage. There will be one located at each site with data deduplication across sites. All data is to be included in these daily backup schedules with network devices also having their configurations backup up daily. The infrastructure team will be responsible for these devices, but the upgrade of the firmware and software falls under the security teams purview. The retention period is a compulsory 5 years for backups.

Power protection on each site will be done by APC UPS systems. An APC Smart-UPS 5000VA 230V Rackmount system will be used for each rack and will allow enough time for failover to another system or site in the case of power outage. These will be monitored by the NOC team and will be part of their daily checks. If an issue is detected it is advanced to either the security or infrastructure team as required.

Kemp Load balancers will all be in High Availability (HA) Pairs which will fail over if one goes offline or if a production interface goes down. They are also responsible for failover between sites and to send data only to online servers. These devices make all services run through them resilient and with the LCAP bonding and the HA pair they will be hardware and network redundant. They are also to be setup securely and can be tested to A+ Qualys standard in testing.

The SonicWALL Routers in Site A are part of a HA pair which has failover redundancy in case of loss of device. All SonicWALL Routers are to have redundant power supplies fed from 2 different UPS systems. Internet connection redundancy is via 2 internet connections per site with the SonicWALL acting as a balancer and failover device.

VPN Links to each site is via Mesh topology with metrics for access to resources. Each site will be connected via Site-to-Site VPN to all other sites.

Each Application server will have multiple servers located in all sites with Site A and B being the main service access and will be geo located for access with multi-site redundancy but site C having a redundant running machine for syncing of applications and databases. All SQL servers to be in Database Availability Groups (DAG) and syncing data over VPN to both other sites.

The Exchange Email servers will be in a DAG (Database Availability Group) and will be geo located for access with multi-site redundancy. The Email Spam filter will have the capacity to hold messages for a week in case of failure of all 3 sites.

Remote Access Security

Remote Desktop Workers

To secure access for remote desktop access, the login will need to originate either onsite through a trusted network or via AOVPN. No external IPs will be allowed access to the remote desktop services directly. In addition, the login with be secured using a combination of ADFS and Azure MFA using SAML.

VPN endpoints

The Microsoft Always On VPN with both Secure Socket Tunnelling Protocol (SSTP) and Internet Key Exchange version 2 (IKEv2) will be used to make sure all laptops that connect to the VPN will be pre-authorised before login. This will be balanced on the Load Balancers and will allow for even distribution on the Routing and Remote Access Servers (RRAS) servers. Device authentication first followed by User Authentication.

Partner Portal

The Partner Portal is to be secured using ADFS and all data accessed by partners is to be read only. Enough so that the partners can quote and download tools and marketing data but not to upload to any site. No access is to be given to any databases or file servers to partners.

External File Sharing

When a large file needs to be shared to a customer or partner, one drive will be leveraged to give access only to that file and a time expiration link sent in a traceable email. File sharing to or from remote workers to internal users is to be done via remote desktop over VPN and file servers directly.

Logging

All external access requests are logged either by ESP on the Kemp Load Balancers for services or VPN logs for external user access. The SSO logs from Azure MFA will be streamed to the SIEM as will the ESP logs. Remote desktop services will log users when logging in and out.

Physical Security

When it comes to physical security it is often overlooked and lack of investment can leave your data vulnerable to shoulder surfing, tailgating, rubber duck attacks and other equally hard to detect attack vectors. To prevent as many avenues of attack as possible, Radio frequency Identification (RFID) badges will be used for all employees and if you have no badge then there is no entry. In addition, the RFID door entry system will be centrally managed and will include an intercom on external access points, on the SOC, NOC and Datacentres for use with the man trap installed at each location. These will be able to log users and report movements to the SIEM. To prevent unauthorised access to the datacentre's, the inner door of the man traps will only be allowed to be opened from the SOC with visual identification made through a CCTV camera.

A proper CCTV system will be installed to record access using the Cisco Meraki Cloud-Managed Smart Cameras. This will allow face recognition through the Virtual Application (V-App) Artificial Intelligence (AI) Customer Analysis and should alert if a non-employee is gaining entry to the buildings.

To protect Site A in case of power loss there will not only be a Uninterruptible power Supply (UPS) but also a backup generator on a 5-minute delay.

Large format printers in each location will be locked down to user ID card and will not print until the user enters their credentials at the printer to make sure the correct person retrieves the print job.

To further protect the datacentres there will be leak sensors located every 2 meters on the floor of each datacentre. Leveraging the Cisco Meraki MT12 Cloud-managed water leak-detection sensor will make sure they are operational and reporting to the centrally managed location in the NOC/SOC.

A GPO will be applied company wide that prevents access to removeable storage media to prevent unauthorised storage devices being attached to company laptops and desktops.

Burglar and Fire alarms to be tested on a quarterly basis and linked to the NOC/SOC for logging and event triggering.

For all company mobile devices, a track and trace program, called Prey Project, with remote wipe capabilities and device encryption will be installed and kept up to date and managed through the SOC. This will allow remote wipe of a device in case of theft and will be managed via the Prey Project site.

Conclusion

As the company grew it expanded its IT resources on a case-by-case basis. With no unified scope or vision behind it, the networks and servers infrastructure was implemented based on what was required in the moment with security being very far down the list of priorities, if present as a thought at all. To bring this sprawling incoherent system together required a large input of resources, time, and effort. The first step as ever is recognising that there was an issue and getting the management and board buy in to the task. Getting a CISO appointed was essential and inventory of assets allowed vision into the systems being used. Once the knowledge of the existing system was established during the discovery, the implementation of changes was then planned and to be phased into the production environment with minimal disruption to business activities. Communication to employees of the changes and the new policies to be implemented was done here with security education being done on a department-by-department basis during the rollout.

Phase 1

Planning the requirements and infrastructure and the implementation timeline. VLAN layout and stacking of switches and data usage throughputs modelled. Research on firewalls and capabilities of each type were discussed and settled upon. Business requirements were laid out and quotation and purchasing of desired equipment and reserving install technicians for implementation was all done during this phase. When all material resources were delivered to site they were unboxed and mounted into the datacentre racks. Power testing to make sure they were accessible, and working was completed, and the nest stage was ready to implement.

Phase 2

Implementing the backbone of the network with the switches and firewalls. This applied segregation to the network and distinct separate VLANs and regions for data access. It also allowed the inspection of internet traffic for the first time and access logs for data. The SOC and NOC were also set up at this stage to start taking in the logging information and to get to grips with what the business use baseline was. This was allowed to bed in over time and access restrictions implemented. Rolled out on a site-by-

site basis starting with Site C and then to Site B and then to Site A allowed the impact of such major changes to be mitigated. Lessons learnt during the install on the smallest site first allowed familiarity with the new equipment to build and staff confidence to increase. As Dell install technicians were utilized at each site for best practices installation methods, the confidence in the deployment would be high, allowing the new network to be working in parallel to the old until the switchover would occur during a maintenance window.

Phase 3

Installing the new Virtualisation Hosts and setting up the Vmotion for live migration and hot standby was setup for all sites. Once the hosts were connected and setup the migrating from physical to virtual could be completed and was done department by department so that staff disruption was minimised. As each physical server was migrated to virtual the old servers were removed but kept onsite in case any data was required after implementation of the virtual machines. At this time the VLANs were utilised, and the departments separated into their own areas. Drive encryption for the accounts was also carried out at this time. Backups to the Vaults were done after each successful migration to have a start point. After this a data deduplication method would be used for changes to data to keep the backup image up to date.

Phase 4

Now that the data was on the virtual hosts it was time to start securing access. Leveraging the capabilities of the Kemp Load Balancers the SSO SAML implementation was done. WAF was then enabled and tuned with the help of the developers to ensure it was working as desired. IPS/IDS was also implemented to ensure full protection of intrusion from outside. Once verified for each application and functionality tested, the users were swapped to the new MFA system.

Phase 5

The WiFi was replaced on a site-by-site basis. Starting with the largest site and working down to Site C, these were fast to implement due to the configuration being applied before mounting so that no onsite config of the devices was required. Each was tested to make sure it operated with the Meraki console and that remote configuration was enabled.

Phase 6

The securing of mobile devices and encryption of handsets and track and trace programs was achieved here. This then allowed the total visibility of the device infrastructure and the testing of the log reporting mechanisms. The system was allowed to stabilize and to gather the business use baseline for alerting by Flowmon and the AlienVault.

Phase 7

Continuous improvement of security will be done through running tests against the systems and updating as necessary. Some pro-active measures are to be taken by the security team such as firmware updates, certificate renewal, Azure AD management, SSO management and IoC detection and remediation. Regular exercises are to be performed for breach procedures and escalation methods to become streamlined and quick to resolve. The Goal of reaching ISO27001 and NIST SP800 53 R5 compliance remains a priority and procedures and policies will need to be updated and refined continuously in a never-ending cyclic method.

The major infrastructure elements on each site will be installed as follows. See Appendix 3 for diagrams

Site A

3 Dell PowerEdge R940xa VMware Hosts

1 Dell Power Vault ME5 450TB

5 Virtualised Domain Controllers

2 Virtualised WAP servers

2 Virtualised ADFS servers

2 Virtualised Exchange 2019 servers

1 Virtualised File/print Servers

2 Virtualised Remote Desktop Services Servers

2 Virtualised SQL Database Servers

2 Virtualised Sharepoint Servers

2 Virtualised Salesforce application servers

1 Dell Power Protect DP4400 Appliance as backup server

8 Virtualised web servers (Partner Portal, Accounting expenses portal, Shipping Portal, Salesforce portal)

8 of 48 port Dell switches

6 Wireless Cisco Meraki access points

2 of SonicWALL NSa 6700 Router Firewalls in HA pair

2 Kemp LM X-15s in HA pair

Site B

2 Dell PowerEdge R940xa VMware Hosts

1 Dell Power Vault ME5 300TB

3 Virtualised Domain controllers

1 Virtualised ADFS server

1 Virtualised WAP server

2 Virtualised Exchange 2019 Servers

1 Virtualised file/print server

6 Virtualised Web servers

2 Virtualised Salesforce application server

1 Virtualised Sharepoint server

1 Virtualised SQL server

1 Dell Power Protect DP4400 Appliance as backup server

1 SonicWALL NSa 5700 Router Firewall

6 of 48 port dell switches

4 Wireless Cisco Meraki access point

2 Kemp LM X-15s in HA pair

Site C

1 Dell PowerEdge R940xa VMware Host

1 Dell Power Vault ME5 150TB

2 Virtualised Domain controllers

2 Virtualised Exchange 2019 servers

1 Virtualised ADFS server

1 Virtualised WAP server

1 Virtualised file/print server

6 Virtualised Web servers

1 Virtualised Sharepoint Server

1 Virtualised Salesforce application servers

1 Virtualised SQL server

1 Dell Power Protect DP4400 Appliance as backup server

1 SonicWALL NSa 4700

2 48 port Dell switch

2 Wireless Cisco Meraki access points

2 Virtualised Kemp LM 3000 in HA pair

With all this work caried out it is important to remember to remove the old devices from the network for later sanitisation, one year after completion date, to make sure nothing that is required is lost in the transition. As a security precaution all devices will be staged for data deletion and recycling once they reach end of life.

Appendices

Appendix 1.

The project would need a timeline of approx. 6 months to install and get to the point of having a security focused architecture. From there it would be an ongoing process to further refine and tune the alerts and issues. While this would be a great start point for secure infrastructure, as the security goal posts are in constant motion it would need to develop as time went by. As each device becomes obsolete it must be replaced or upgraded. As each vulnerability is defined the security must shift to counter it.

At each phase some reluctance by the departments and end users could derail any particular point and continuing to use the legacy services would need to be discouraged. A firm hand from the CISO would smooth some feathers but ruffle others. It would be best to get not only the board buy in but also the management team buy in and eventually then the staff before starting any work beyond planning and discovery of the project. The roll out of each phase would need to be completed with as little disruption

as possible for everyone involved. A lot of IT work affects end users directly and getting ahead of this before rolling out the changes would help alleviate any disruption to the end users and so resentment for the changes would be reduced. Many times, projects are delayed or stopped by protestations of the end users.

The budget was not overly sensitive in this project but as I have rolled out similar projects before I know every penny counts. In the end if you cut costs on projects like this it will bite you in the backside later. It is best to spend what you can on quality equipment to get the best bang for your buck. A combination of Dell networking and infrastructure equipment (including the SonicWALL) means that you will only have to worry about one vendor, and they provide setup assistance on large spends like this. You can set the goal of the setup at the beginning and the Dell technicians must deliver this before they sign off. This can be very helpful when deploying such a large and complex network and they will have all the best practices ready before you begin. This leads to a high confidence that the project can not only be completed as desired but also in the time scale provided.

When setting up the Kemp Equipment a professional service can be purchased which will see their senior engineer's setup delivery of your services, geo balancing, ESP and WAF. They will make custom WAF rule and ACLs and even a customised login page for your services. As a lot of security depends on these devices the service will pay for itself in eliminating the headache of learning yet another technology for your security and network teams. The Flowmon collector and probes can also be setup at this time as Flowmon is owned by Kemp.

The Alien Vault OISSM is a complex and comprehensive SIEM. Some consultancy when setting this up would be beneficial. As we are purchasing the AlienVault penetration testing on a Bi-Annual basis, I would leverage the first session to get the Alien Vault configured correctly for all devices and ensure that all relevant information is being gathered.

The newest security technology is the Single Sign On leveraging the Azure AD, MFA and SAML. This takes time to get to grips with and would need focus by the nominated team member who needs to set that up. I have done this for a few clients, and it can prove to be frustrating if approached without all the information. As this is integrating with the Kemp ESP this is very important to get right. Allow time for this to be completed correctly and it will not have a knock-on effect as later phases are deployed. Deploying this MFA is key as it is central to user access for most services and is used to protect the infrastructure as a whole.

This report was done from a network security perspective and covered a lot of areas. There are some future considerations to work towards and allowing for a high bandwidth backbone on each site was part of that consideration. Currently the phone system is a traditional landline and mobile handset solution. I would see VOIP either being implemented on site in the form of Skype for business or in a hybrid situation with Office 365 and Teams. I would see as business needs expand more hypervisors

being implemented and added to the current system for V-motion and resources. The Wireless deployment is expandable and with remote configure this can be grown to encompass new areas without detriment to the exiting infrastructure. It may be required to go completely dark fibre between sites and the firewalls have been chosen to take this in their stride. The Switching network has a 100gb backbone for stacking and can bond up to 8 40GB fibre ports each for trunking if required and should see the bandwidth limitation increase with requirements. The BYOD conversation would need to be debated but with all resources locked down with MFA it reduces the impact of these insecure devices accessing the network. With MAC address filtering then this also becomes an issue as we would have no record of end user's devices until brought on site. Possibly setting all these devices to only work on the guest wireless is a solution. Expanding the capability of the SIEM to the AlienVault USM would possibly happen as the network expands. This is a paid option but would be the next logical step for the SIEM. As threats evolve the network must too. Most devices and software selected are chosen so that they can be expanded upon at a later date and integrate with a larger system if required.

Appendix 2.

The locking down of remote machines by using IKEv2 Always On VPN is a new security feature for me. Leveraging the device authentication to be completed before the user can login means that there is already secure communication to the workplace before the user can do anything detrimental. Further locking mobile devices down with full disk encryption and track and trace programs mean that even the loss of a device if reported quickly will have a high probability of a breach being prevented.

The Flowmon products are new to me too, but they are comprehensive and take a bit of setting up. They will give you deep insight to what is happening on the network though and can be leveraged to be as complex or a simple as needed. The modularity of the design allows for further expansion as the capabilities of a team increase.

The new Meraki AI programs that can run on their camera systems was very interesting which allows for identification of an individual's location in cloud data without having to personally identify the person, only that they are not in a location that is open to the public as previously defined. This requires further thought and to delve deeper into this aspect of security

I like that the IOT (Internet Of Things) is now coming into mainstream with the leak detectors being managed by the Meraki software. Usually these would either be custom built or bought as individual devices off the shelf with no central management or detection. This allows for the people who need to know being notified in a timely manner of a leak in sensitive areas.

The Open path RFID door locks and intercom systems are leading edge. Personally, I would love to get my hands on a unit to play around with, but they seem to have the potential to be an integral part of any

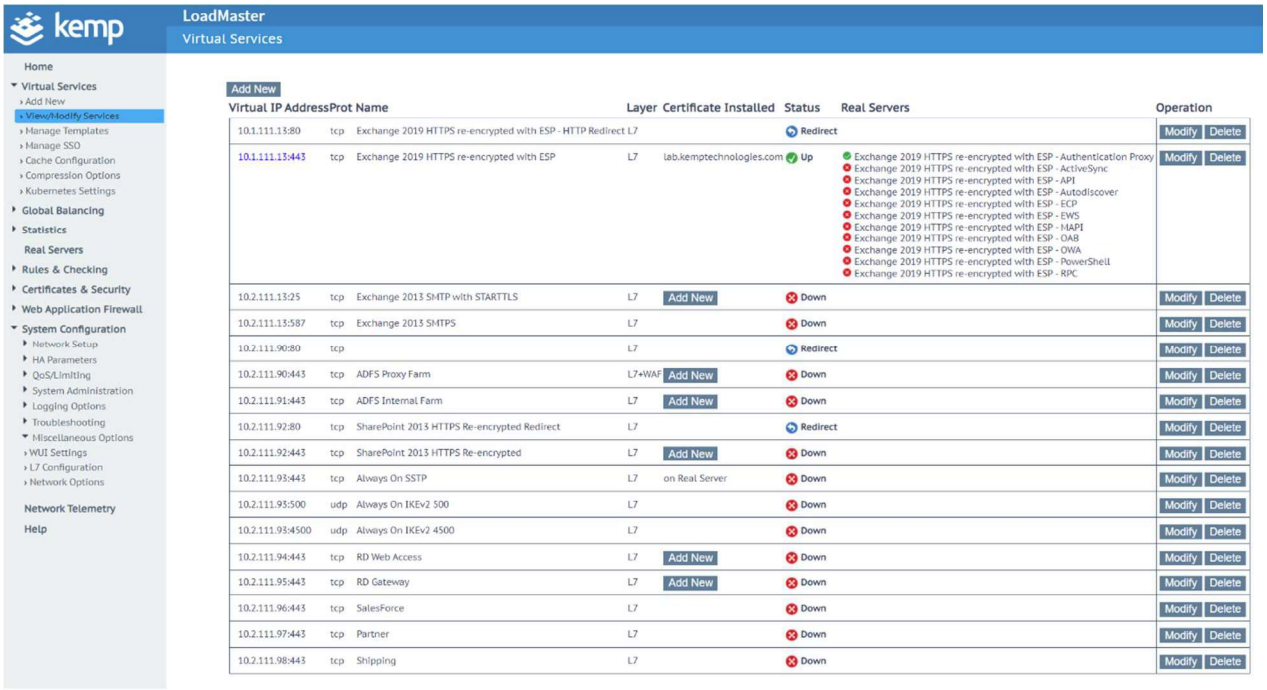
security conscious deployment. They have the ability to centrally manage door access over a site and to report to a logging facility. Highly recommended.

As I am the Security SME for Kemp in EMEA I have used the features within it for 7 years and am familiar with the IDS/IPS SNORT rules, ACL, PCRE rules and the WAF rules. I know that the device is a hardened network device and operates on default deny operation. It is capable of much more than just load balancing and leveraging all the capabilities will help secure services and maintain service capability. The Cipher sets and OpenSSL versions are upgraded on a regular basis and lead to a very secure and fast connection over SSL. You can install multiple certs for a service and even do CSR directly form the device. They also have the capability to communicate with Azure AD MFA and do SSO using multiple methods. Login screens can be customised to the client and display company logo etc. The health checking facility built in allows for fail over of servers, fail over of network interfaces, failover of devices, and failover of sites. As a redundant scheme this checks all the boxes.

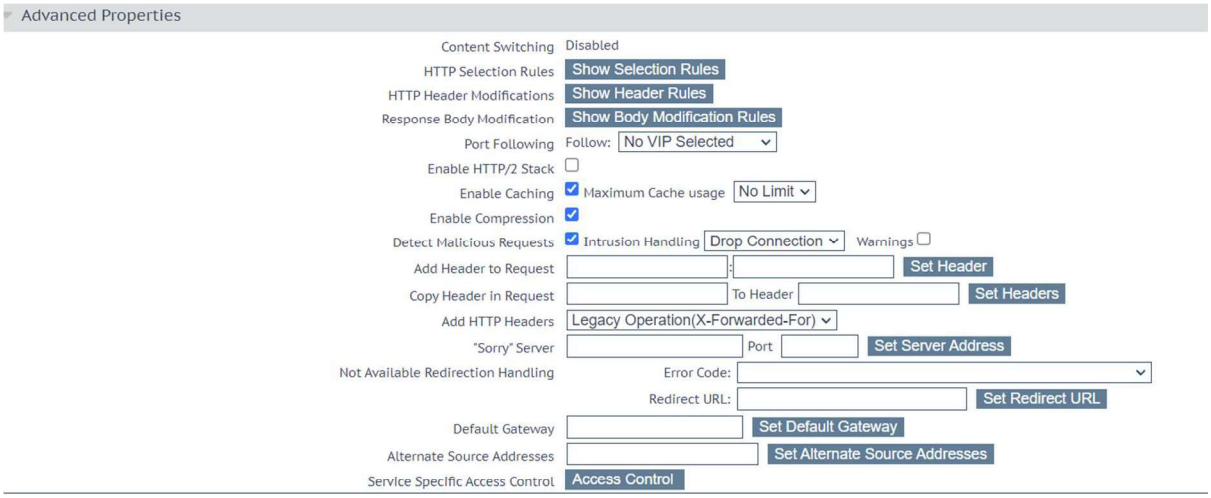
Appendix 3.

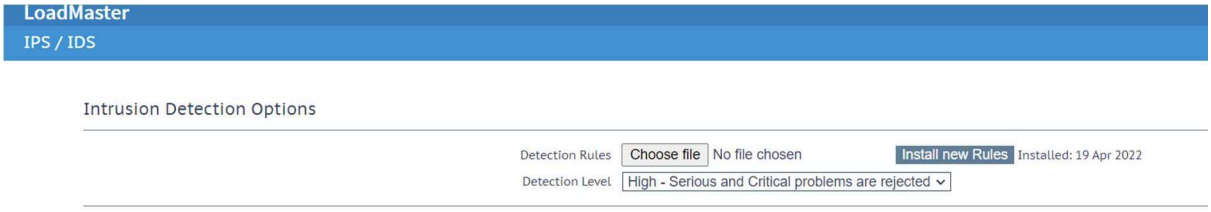
Some screen shots of the configuration pages on the Kemp will show some of the capabilities

This is a sample layout from a HA pair on Site A. All the services are terminated on the LM in the DMZ before ever getting to the internal servers. Each service will utilise ESP SSO, WAF, IDS/IPS, Content rules and ACLs to prohibit unauthorised access.

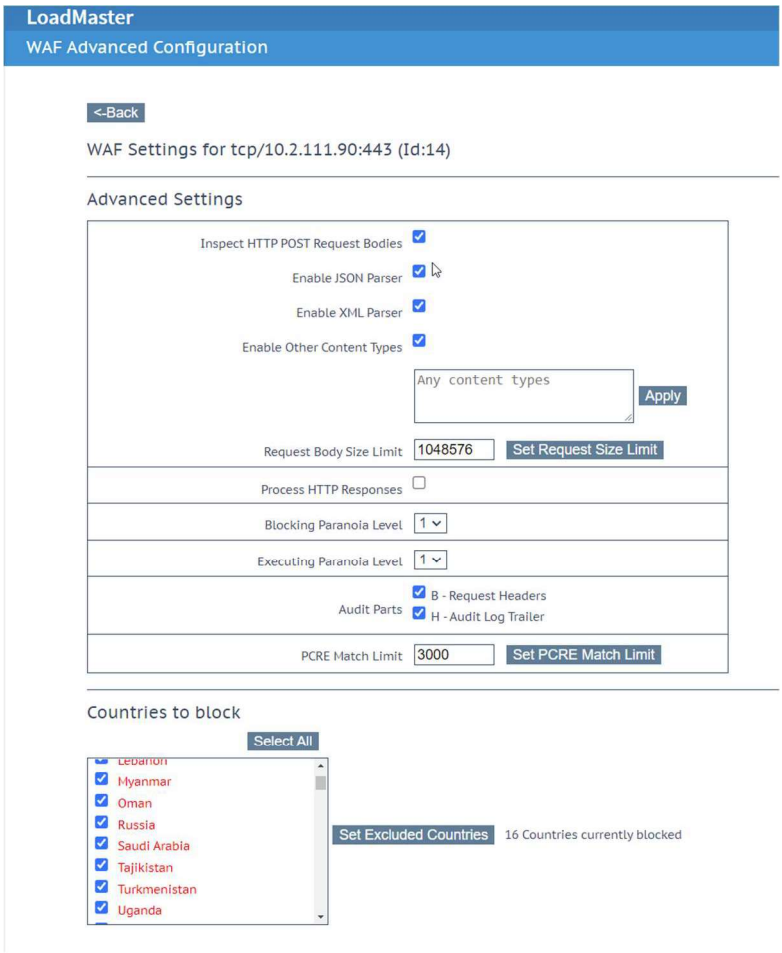


IDS/IPS Snort community TALOS rules are installed and then the paranoia level is set.

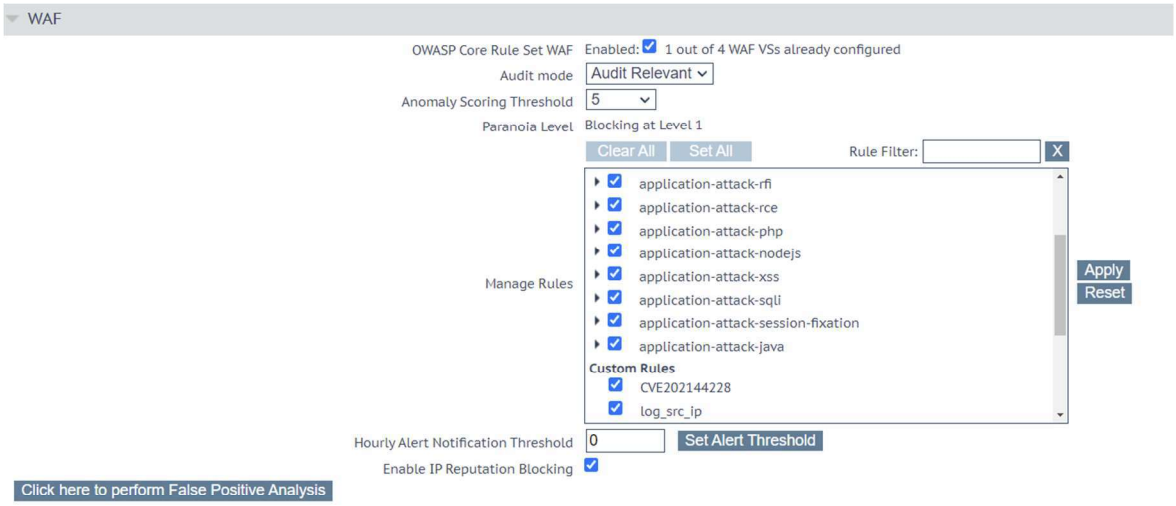




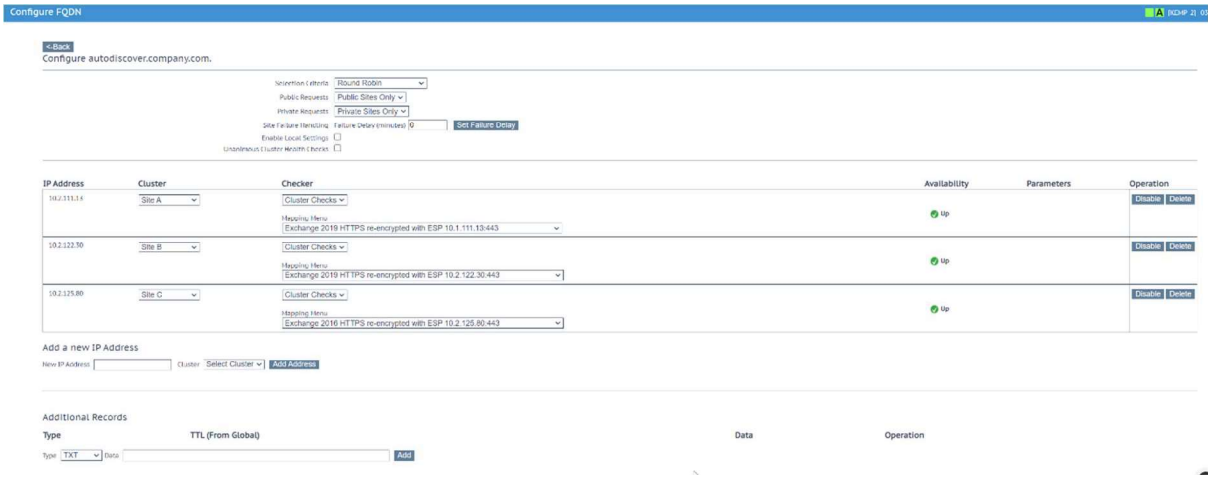
Web Application firewall is enabled on all the SSL offloaded services to protect the web servers from exploits. As we use the OWASP rules this works on anomaly scoring rather than having to match a rule and will pick up and block even unknown intrusion attempts. Geo Blocking is also used to prevent access from selected countries. IP reputation rules and core rule sets are downloaded automatically each day. Processing responses on things like sharepoint can be used to prevent data leakage.

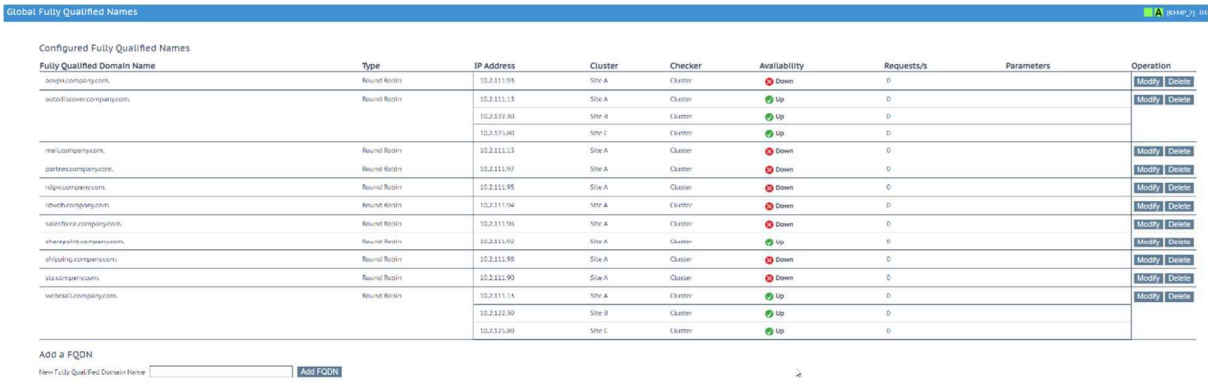


Custom rules can be added manually and enabled or disabled on a service-by-service basis.

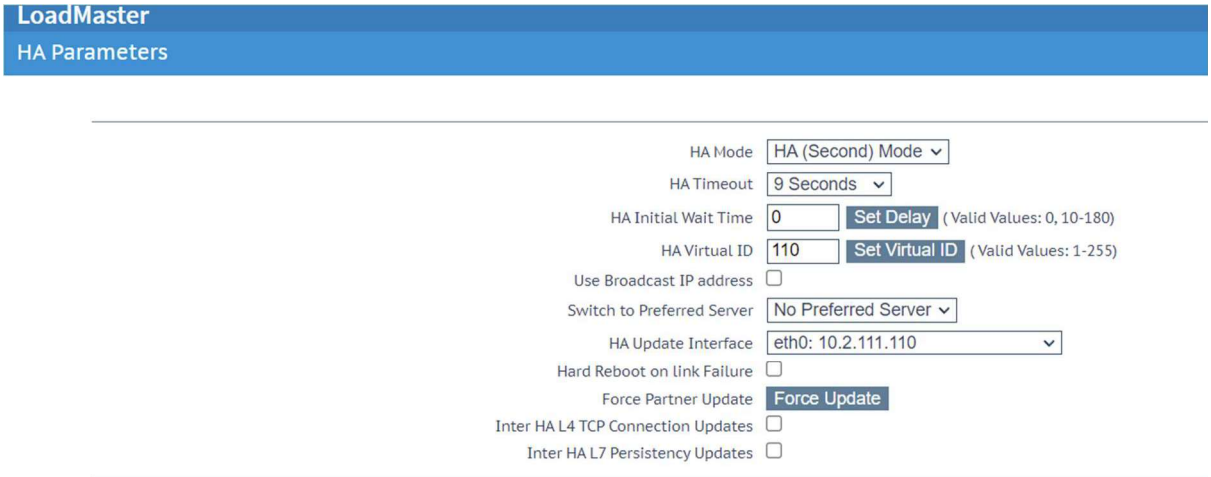


GEO functionality allows for health checks to remote and local sites and allows for site failover and recovery dynamically.

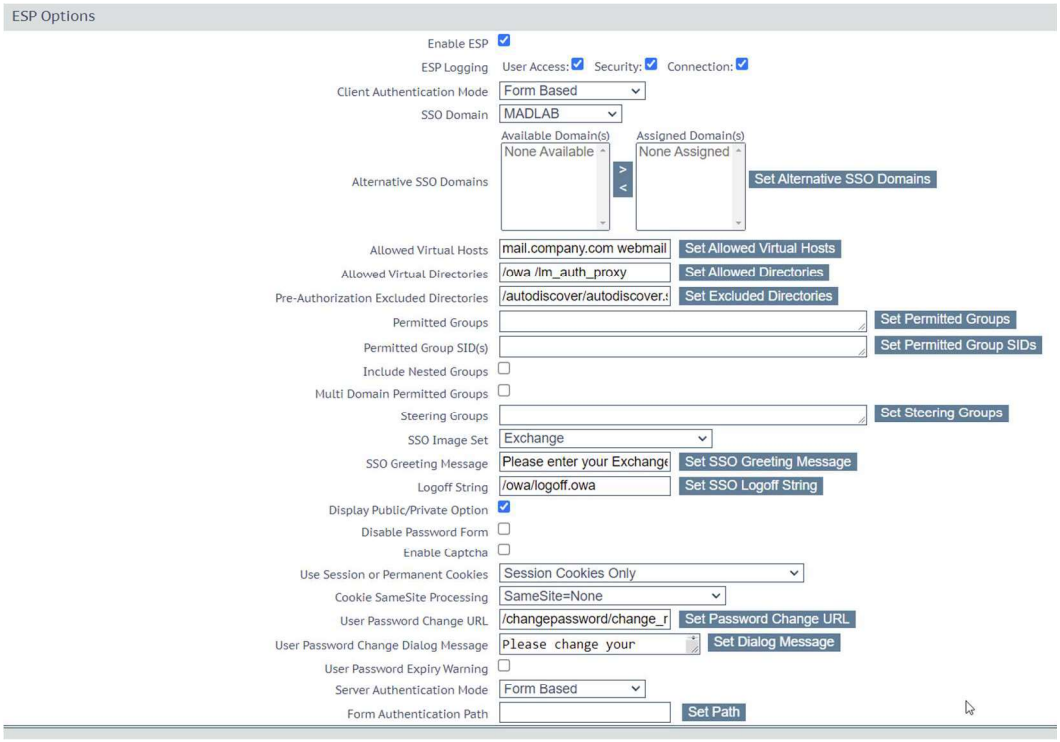




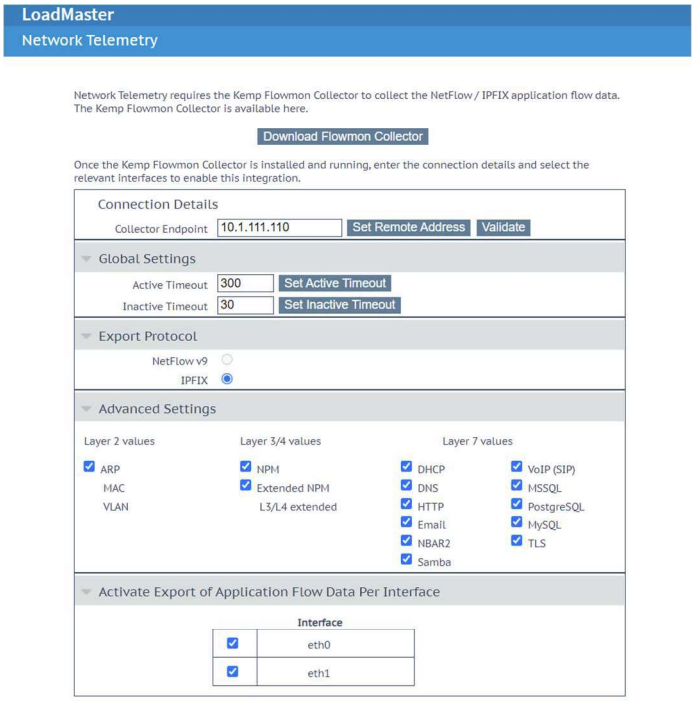
HA configuration allows for failing over if a production interface goes down or if a device fails.



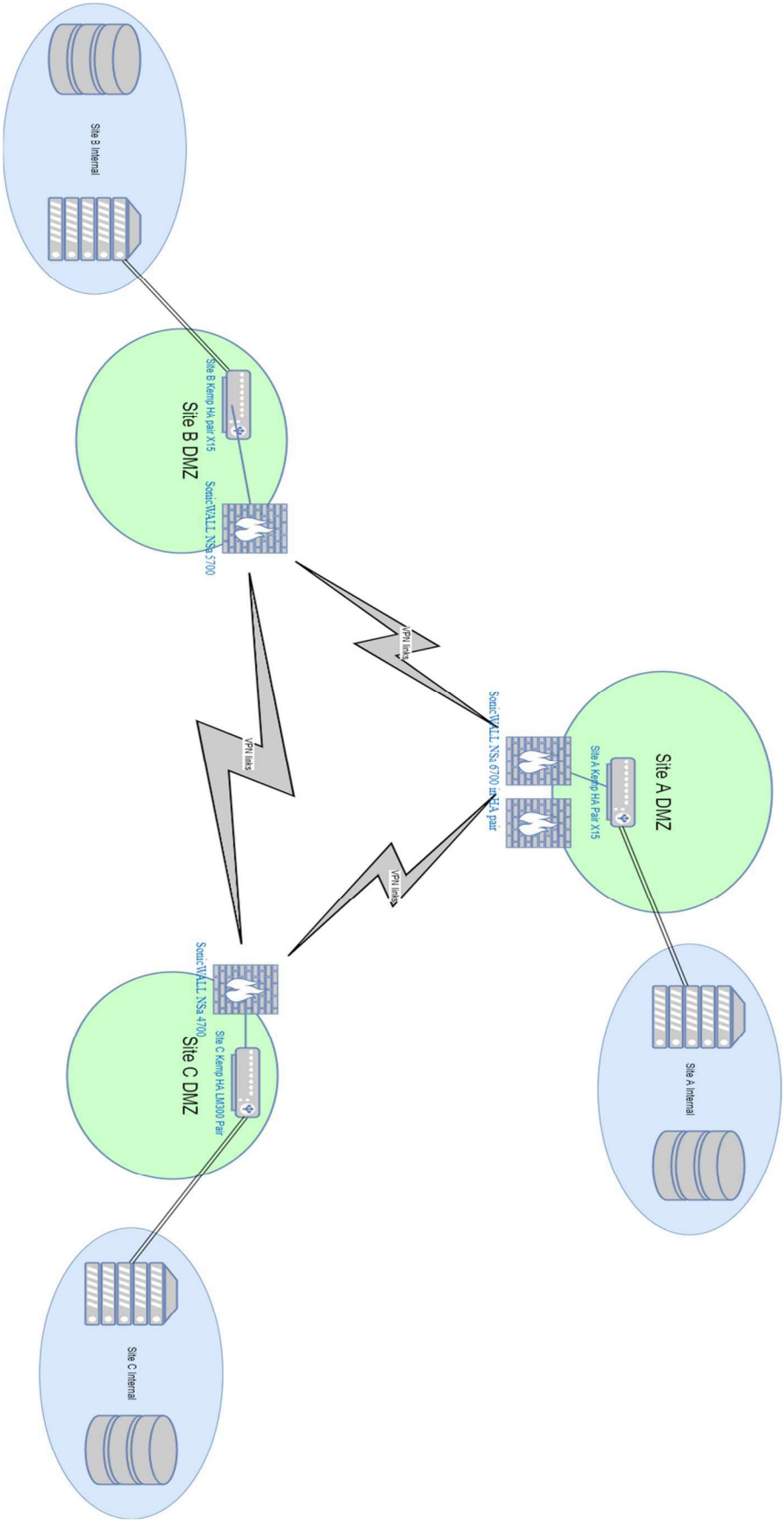
ESP SSO can be leveraged on a service-by-service basis for HTTP/HTTPS traffic. You can also enable ESP logging for SMTP traffic. This allows integration with multiple types of login including Azure AD and SAML or KCD.



IPFIX can be used to stream connection information to the flowmon collector direct form the kemp using the network telemetry feature.

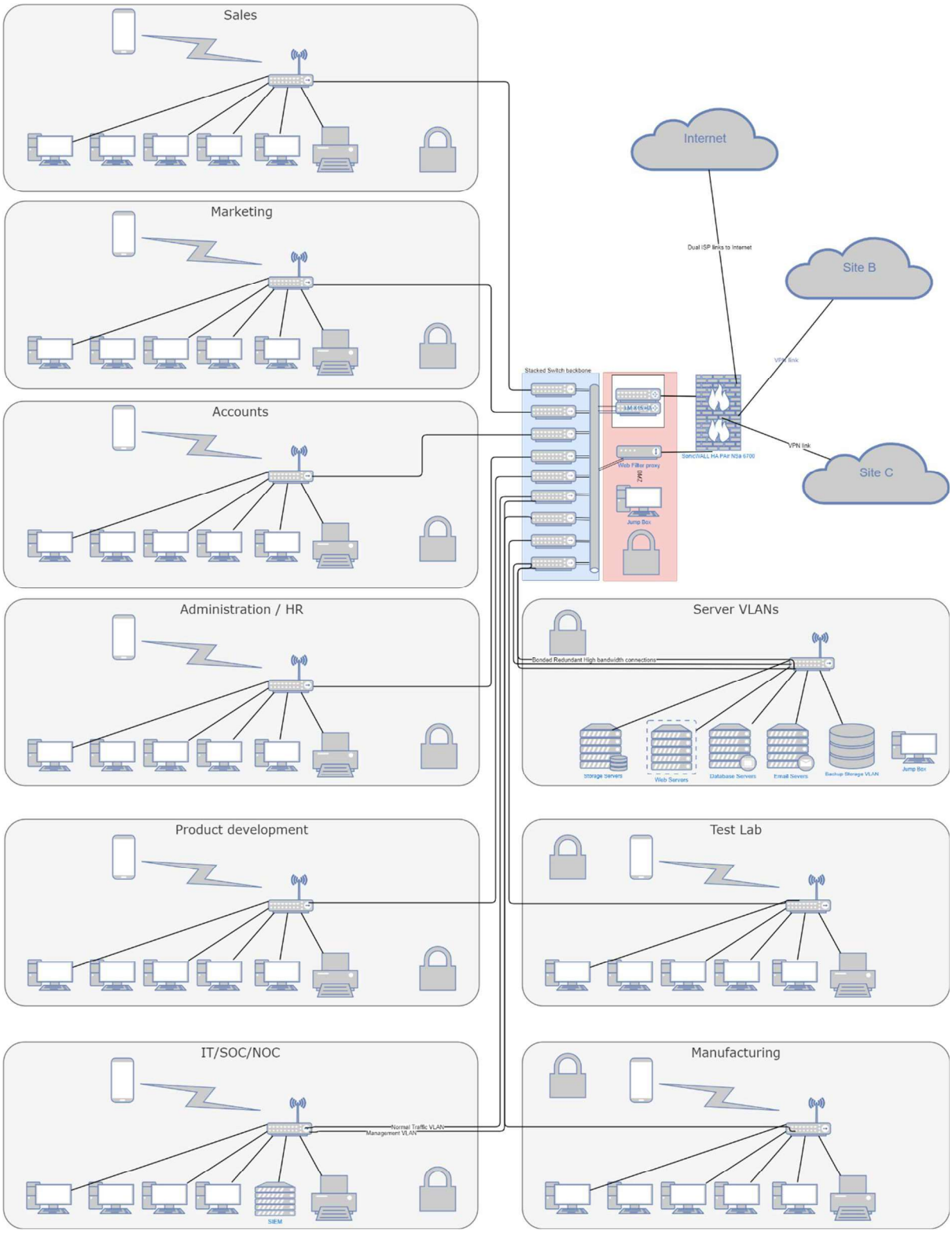


The overall layout of the multi-site network is below

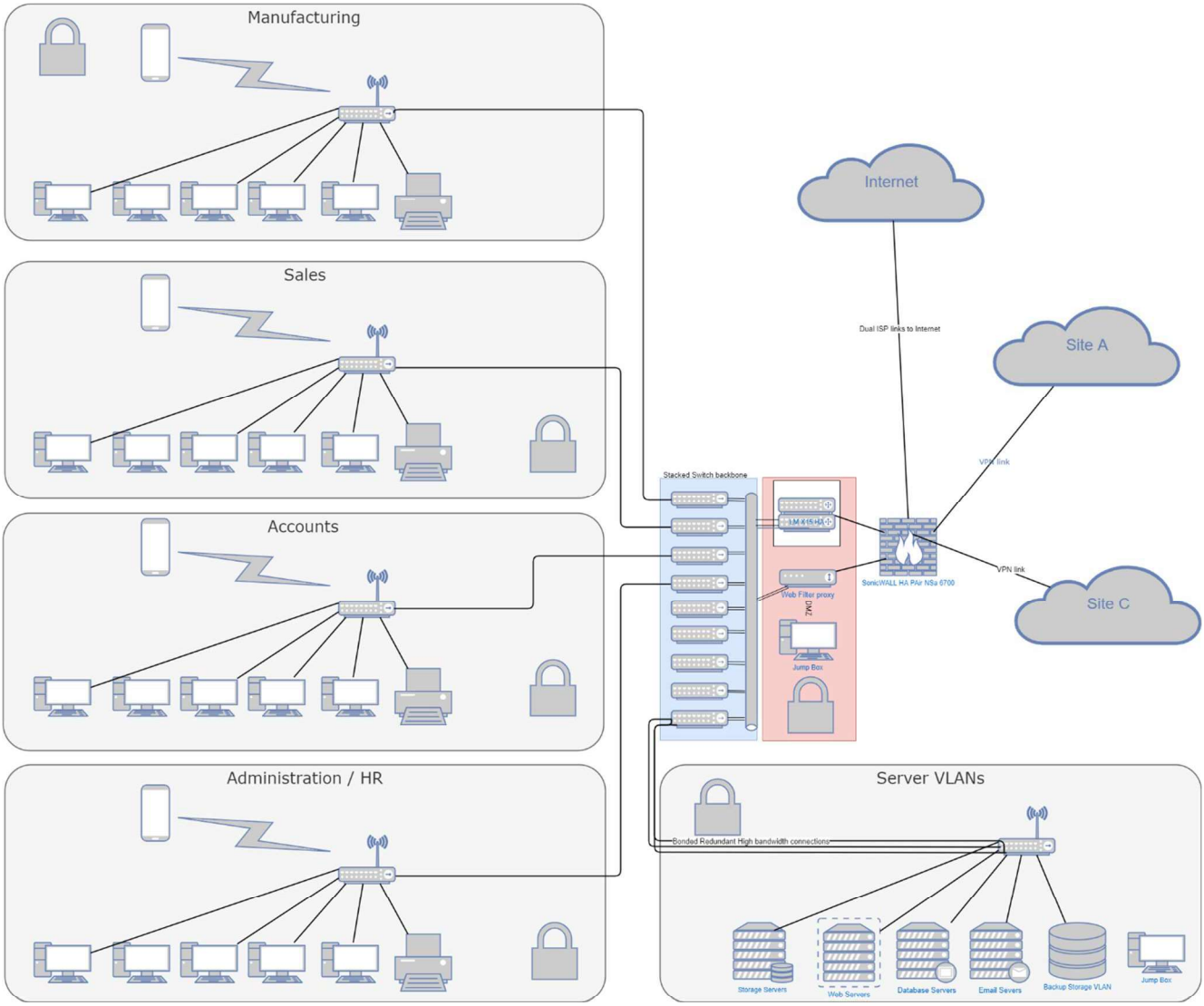


Each site then is logically laid out as follows.

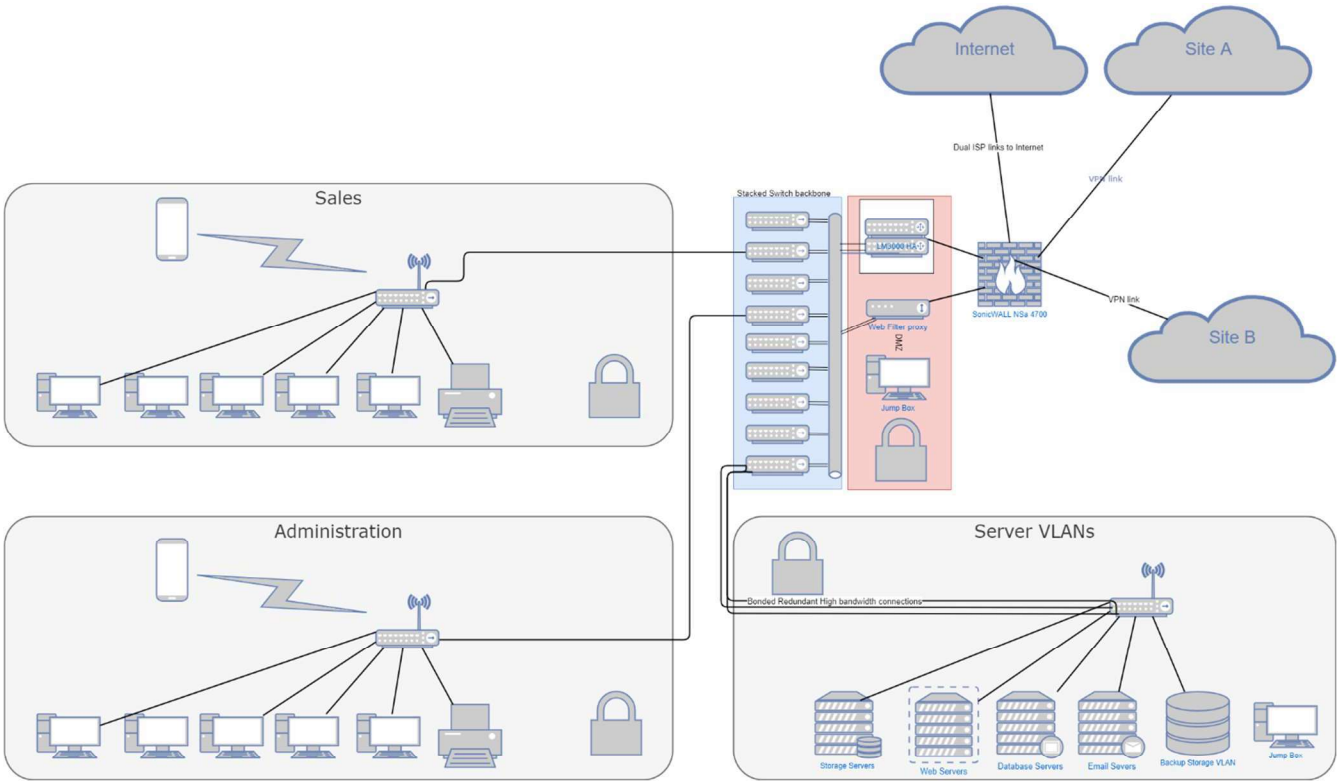
Site A



Site B


Manufacturing
Sales
Accounts
Administration / HR
Internet
Dual ISP links to Internet
Site A
VPN link
VPN link
Site C
Stacked Switch backbone
SonicWALL HA PAir NSa 6700
Web Filter proxy
DMZ
Jump Box
Server VLANs
Bonded Redundant High bandwidth connections
Storage Servers
Web Servers
Database Servers
Email Severs
Backup Storage VLAN
Jump Box

Site C


Internet
Site A
Dual ISP links to Internet
VPN link
Sales
Stacked Switch backbone
LM9000 HA
Web Filter proxy
DMZ
Jump Box
SonicWALL NSa 4700
VPN link
Site B
Administration
Server VLANs
Bonded Redundant High bandwidth connections
Storage Servers
Web Servers
Database Servers
Email Severs
Backup Storage VLAN
Jump Box

References

Sonicwall data sheet -> https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-gen-7-nsa-series.pdf

Mimecast Email filtering service -> https://www.mimecast.com/content/email-spam-filter/

ESET HIPS -> https://www.eset.com/us/business/enterprise-protection-bundle/

Dark Trace -> https://www.darktrace.com/en/products/antigena-email/exchange/

Kemp Load balancer -> https://kemptechnologies.com/virtual-load-balancer/#per

Flowmon IPFix/netFlow monitoring ->https://www.flowmon.com/en/solutions/network-and-cloud-operations/netflow-ipfix

RFC for IPFIX -> https://datatracker.ietf.org/doc/html/rfc5101

Flowmon Security operations -> https://www.flowmon.com/en/solutions/security-operations

Network inventory Tool – Lan Sweeper -> https://www.lansweeper.com/

WSUS -> https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus

Cobit 2019 -> https://www.isaca.org/resources/cobit

NIST -> https://www.nist.gov/cybersecurity

Barracuda Web Security appliances -> https://www.barracuda.com/products/websecuritygateway/models#paranav-navbar

APC UPS -> https://www.apc.com/shop/uk/en/products/APC-Smart-UPS-5000VA-230V-Rackmount-Tower/P-SUA5000RMI5U

Pi-Hole -> https://pi-hole.net/

Alien Vault OSSIM -> https://cybersecurity.att.com/products/ossim

AT&T penetration testing services -> https://cybersecurity.att.com/products/penetration-testing-services

Cisco Meraki Cloud-Managed Smart Cameras -> https://meraki.cisco.com/product/security-cameras/outdoor-security-cameras/mv72/

MT12 Cloud-managed water leak-detection sensor -> https://meraki.cisco.com/product/sensors/indoor-sensors/mt12/

Cisco MR57 Wifi -> https://meraki.cisco.com/product/wi-fi/indoor-access-points/mr57/

OpenPath RFID Door locks -> https://www.openpath.com/hardware

Prey anti-theft -> https://preyproject.com/solutions/business/?s=menu

Azure AD MFA -> https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa

Dashlane Password manager for business -> https://www.dashlane.com/business/pricing