NETWORK AND CLOUD SECURITY

SECURE ARCHITECTURE FOR A MODERN ORGANISATION

STUDENT NAME:	
STUDENT NUMBER:	
COURSE NAME:	Masters in Cybersecurity, Privacy and Trust
CLASS NAME:	Network and Cloud Security
COURSE CODE:	CW_KCCSM_M
SUPERVISOR:	Dr Hisain Elshaafi
DATE OF SUBMISSION:	25th April 2022

CONTENTS

1. Introduction

In this project I will take a fictitious organisation acme.inc who have an infrastructure that is equivalent to many enterprise level organisations. They have a main site with a large campus network where they have many different business functions such as human resources, finance, software developers, information technology operations and engineering departments for network, server and storage design, implementation and support. Along with an information security team and security operations center (SOC). The organisation also has multiple regional sales offices which are staffed by employees in the sales department as well as having some other functions such as local information technology support, human resources and finance.

Acme.inc also has an on-premise data center which hosts all the infrastructure and applications to support the corporate functions as well as the application and database servers to support the organisations public facing website. The organisation also runs some services in the Amazon Web Services (AWS) cloud such as the front-end web servers for their public facing website. The organisation looks to standardise on a number of key infrastructure technologies throughout the organisation for ease of management, interoperability and security. These technologies providers include Cisco, Microsoft, Amazon Web Services (AWS), Pure Storage, RedHat and VMware.

Through the problem analysis I will identify security risks that the organisation could be exposed to both internally and externally. The architecture and orchestration section of this project will then take the different networks flows that make up the network and infrastructure design of acme.inc and explain what technologies and processes I have incorporated into the architecture of this environment to mitigate the security risks identified in the problem analysis. To provide acme.inc with secure on-premise and cloud environments through the use of defense in depth where there are multiple layers of security protecting each network flow.

2. Problem Analysis

In this section, I will take a high-level view of acme.inc network and infrastructure that supports its corporate information technology functions. Having a broad idea of how the company operates as outlined in the introduction will allow me to identify the potential security risks that I need to be aware of when designing a secure architecture for a modern organisation such as acme.inc.

Starting the problem analysis by analysing the information technology requirements of acme.inc. Firstly, the organisation requires a head office campus network which will support the employees of the company in carrying out their day-to-day work. This environment will be made up of the users' corporate laptops which will provide email, collaboration applications such as Microsoft teams, specialist software for software developers, networks engineers, human resources, finance. This network will also have to provide IP phones and wireless network connectivity for both employees who will access the corporate WIFI SSID and guest who will be able to access the GUEST WIFI SSID which will block them from any corporate resources and just give them internet access.

Outside of the head office campus networks the organisation also has multiple remote offices these offices will have the same functionality as the head office campus network. Where there can be employees from multiple business functions connecting to the same local area network and wireless local area network. There can also be visitors to the offices that will need internet access. The remote access will also need to be able to route traffic securely to the head office and to each other.

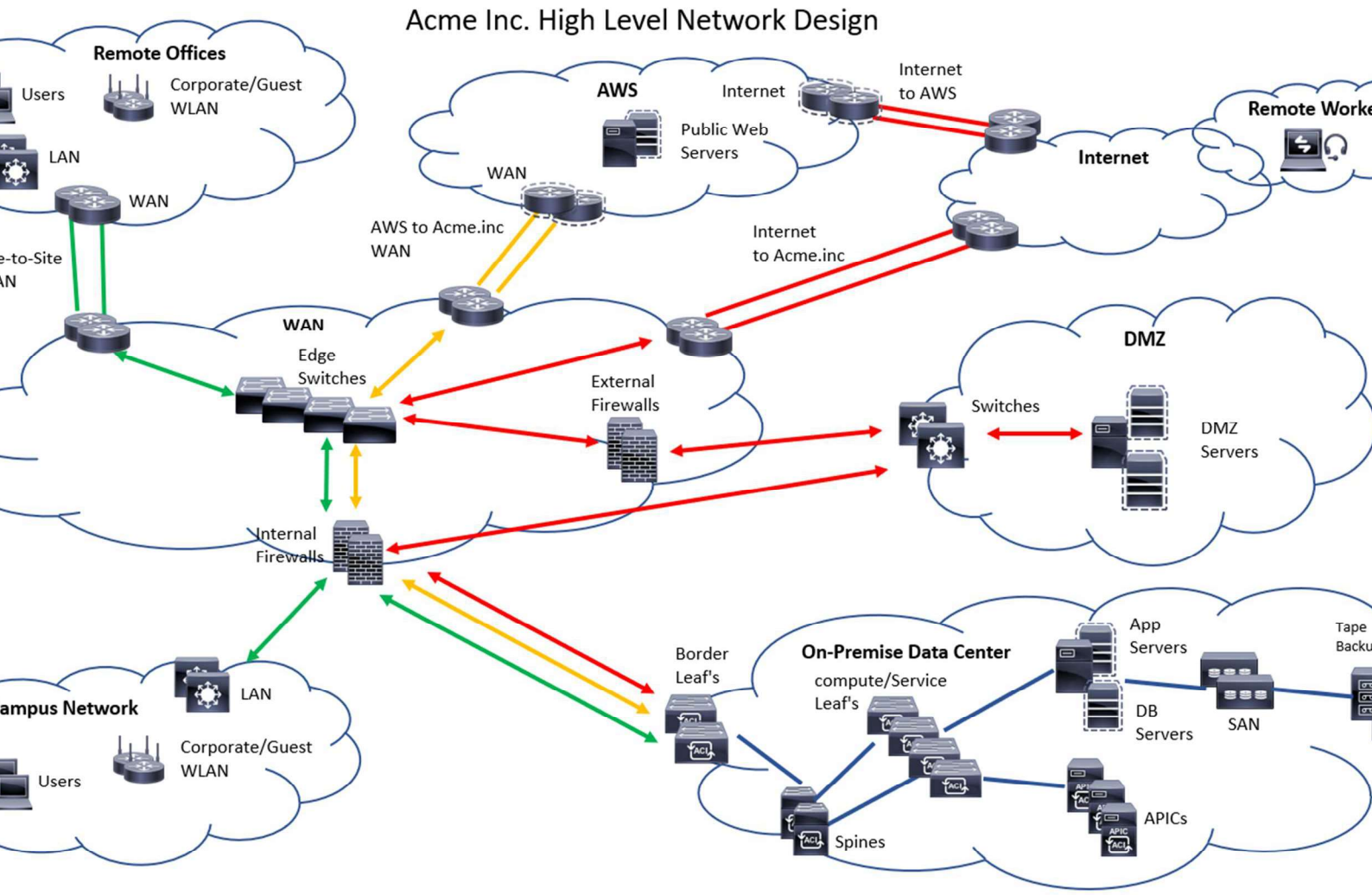
The organisation needs to provide the employees with a way of working remotely when they are not in the office and working from home. Allowing them to access all the same services as they would when connected to the corporate local area network.

Acme.inc also has a large data center footprint both on-premise at the head office and in the cloud using Amazon Web Services (AWS). Both of these data centers have public/internet facing services on AWS they have their public facing web servers that host the organisation public website and in the on-premise data center they host some public facing services to support their corporate functions such as web email that employees can access without being connected to the corporate remote access solution.

Figure 1 illustrates at a high level the areas I need to focus on when assessing the security risks from remote offices to an on-premise data center. By completing this high-level design, I have an idea of the different technology areas and organisational functions that I should be focusing on when trying to identify the security risks I might encounter and need to take into consideration when designing the enterprise architecture. Not yet focusing on the technologies that will make up the design or the solution

to address the security risks here I am just taking the information on how the organisation operates to identify different areas of the network that will be required to fulfil the business requirements of the organisation.

At a high-level I see the traffic that originates from the internet as the riskiest that why I have labelled that as red, then the traffic that traverses the network from my AWS data center less risky as this traffic will already have traversed the security measures I will put in place to secure my AWS environment and finally the internal network flow from the corporate user network to the remote sites and the on-premise data center as the least risky as I will have the most control of those devices.



Acme inc. High Level Network Design

So, what are the security risks I will need to address in my architect of acme.inc network to apply a defence in depth design.

Unauthorised Access to Network and Resources

If malicious users can't access our network, then their ability to compromise the security of our information technology systems will be greatly reduced. However, as well as restricting unauthorised users access to our network, we also need to be able to control the access authorised users have. We don't want to allow employees who work for the finance department to be able to access sensitive data that should only be access by the human resources department and visa vera. This is applicable across all areas of the network from accessing AWS resources which are hosted in our cloud-based data center to accessing file shares on the internal servers which are hosted in our on-premise data center. Designing access control systems into our enterprise architecture will increase our network security by restricting unauthorised user access and allowing authorised users and resources to only access information technology resources that they require to carry out the functions within their specific role.

Malware and Viruses

Malware refers to malicious software and it refers to software developed by malicious actors such as black hat hackers to damage computer systems, steal data or gain unauthorised access to information technology systems. There are many different types of types of malwares which include computer viruses, worms, keyloggers, trojan horse, spyware and root kits. The most common ways that malware enters our network is through the internet and email. Malware can infect our systems through users connecting to hacked websites, downloading files from the internet which are infected or installing programs or applications from unverified sources that install malware along with the program the user wanted to install.

Looking at a few of the most common forms of malware; Adware is software that is designed to show unwanted advertisements on your device screen. Spyware secretly tracks the activity on your computer and reports back to the command-and-control server with sensitive information such as bank account details. Viruses are infected pieces of software that attaches itself to another program and once executed can propagate throughout the network to infect multiple devices. Rootkit is malware that provides the attacker with Admin privileges or Root access to the systems that the malware has infected. Keylogger records the key stokes on the infected user's computer and send the information back to the command-and-control servers such as passwords, usernames, bank details or credit card information. We need to be able to scan and test for these vulnerabilities within our network.

Email Security

Security vulnerabilities relating to email are an important consideration when designing a secure enterprise network. Since over eighty percent of cyber-attacks are initiated via infected email or links that redirect users to malicious sites it is critical that there is security control put in place around email security. There are multiple security risks that we need to be aware of including; Spoofing and Phishing, email spoofing is when a malicious actor sends an email to a user pretending to be somebody the user knows. Phishing is another method of sending users misleading emails in an attempt to get the user to provide the hacker with sensitive information such as bank account details. Dangerous files, the cybercriminal can also attach infected files to an email that once the user opens can propagate malware throughout the organisation network. Email security software should make up a part of our defense in depth strategy as this type of software can filter out suspicious emails and can also prevent employees from sharing certain forms of data externally.

Unauthorised Network Endpoints

With the increased amount of device that are network enabled and with some organisations introducing policies around bring your own device (BYOD) we need to have security controls around what devices are authorised to be connected to our corporate network and which ones are not. Even devices that are allowed to connect to our network could be still infected with malware so we need to be able to block these devices from connecting to the network or quarantine them until the malware has been removed or the devices anti-virus software has been updated. Having an asset management capability to be able to identify all devices that are connected to the network and alert the security team when attempts are made to connect unauthorised devices need to be a consideration in our architecture.

Intrusion prevention

Intrusion prevention systems are a key consideration that we need to take into account when designing the network and security architecture for acme.inc. The reason being networks have multiple ingress and egress points which handle large amounts of network traffic, this makes manual monitoring of these environments unrealistic. The automated capabilities of an intrusion prevention system allow the security teams to respond to cyber threats quickly and prevent security attacks before they have a chance to infect the inside of our network. There are different types of intrusion prevention systems including; Network Intrusion Prevention Systems (NIPS), Host Intrusion Prevention Systems (HIPS), Network behaviour Analysis (NBA) and Wireless Intrusion Prevention Systems (WIPS). Intrusion Prevention Systems can be signature based, anomaly based or policy based.

Network segmentation

There are different parts of a computer network which host different types of network traffic and have require different security controls to be applied to these areas. Network segmentation allows us to give

the appropriate access to authorised users that require access to the network traffic in a specific segment of the network. By segmenting the network, we can also prevent a cyber-attack or malicious software from propagating throughout the entire network. We can look a segmenting user from different departments in their own subnets and VLANs on our layer 3 switches or by introducing firewalls into our environment to create secure segmentation of our north/south traffic that will ingress and egress from our networks and also to help control the segmentation of the east/west traffic internally within our organisation. The benefits of network segmentation are; slowing down attackers so if an attacker does breach our network and network segmentation has been implement the attacker will also need to break out of different network segments to get to the resources they wanted to exploit. Network segmentation also assists our implement a policy of least privilege so we can restrict users from the systems with the most secure information in our organisation.

Distributed denial of service Attacks

A Distributed denial of service (DDoS) attack occurs when our organisations legitimate users are unable to access the corporate network and resources due to a cyber-attack that over loads our network with connection requests that if untaken on a large enough scale will case the network to become unavailable or even cause our systems to crash. There are different ways of carrying out a denial-of-service attack and a distributed denial of service attack just means that the denial-of-service attack is taking place from multiple location in a co-ordinated manner. There are a few common methods of carrying out a denial-of-service attack, a smurf attack is where the attacker sends ICMP broadcast packets to multiple hosts with spoofed IP addresses that belong to the target host. The hosts that receive the spoofed packets then respond and the target host becomes flooded with these responses. A SYN flood attack occurs when the malicious system sends a SYN request to the target system but then does not complete the rest of the TCP three-way handshake so the connection port is in an occupied state and will eventually saturate the connection limit not allowing genuine connections to be established. (CISA, 2022)

Create and Maintain Access logs

Beings able to view log and event data generated by all the devices on the network is critical when building a comprehensive picture across all the activities occurring on the network. Security Information and Event Management systems will need to be consider when designing the architecture of our organisation. SIEMs have multiple capabilities including; log and context data collection. This includes being able to collect logs and context data using a combination of agentless and agent-based methods. Normalisation and categorisation, being able to convert collected original logs into a universal format. Notification/alerting, trigger notifications or alerts to operators or managers. Reporting, reporting covers all the historical views of data collected by the SIEM. Security role workflow, incident management features such as being able to open cases and perform investigative tasks, as well as automatically or semi-automatically perform typical tasks for security operations.

Ransomware

Ransomware in order to be successful needs to access our information technology systems to be able to encrypt the data on these systems and so the attacker can demand a payment for a decryption key to decrypt our data. We need to be aware of the problem of ransomware in our problem analysis so we can design in protections to stop our systems being infected with ransomware and mitigations if our systems were to be infected with ransomware how could our data be restored without having to pay the attacker of the decryption key.

Data Breaches

A data breach happens when sensitive or confidential information is mistaking shared with or stolen by an unauthorised user. Weak credentials, malware or unauthorised third-party access could all be avenues for a data breach occur. Unencrypted data is going to be the biggest risk when a data breach occurs so we need to build-in data encryption mechanisms into our design to make sure that even if a data breach does occur that the data that has been lost or stolen is not usable to an unauthorised user.

Misconfigurations and Unpatched Systems

Misconfigured and unpatched systems are a major security risk for our organisation. We need to make sure the configuration on our systems complies with industry security standards such as NIST or CIS benchmarks. We would also need to deploy security tools that can interrogate the configuration on our devices to make sure once secure configurations have been applied that configurations changes are not made to the devices that breach these compliance standards.

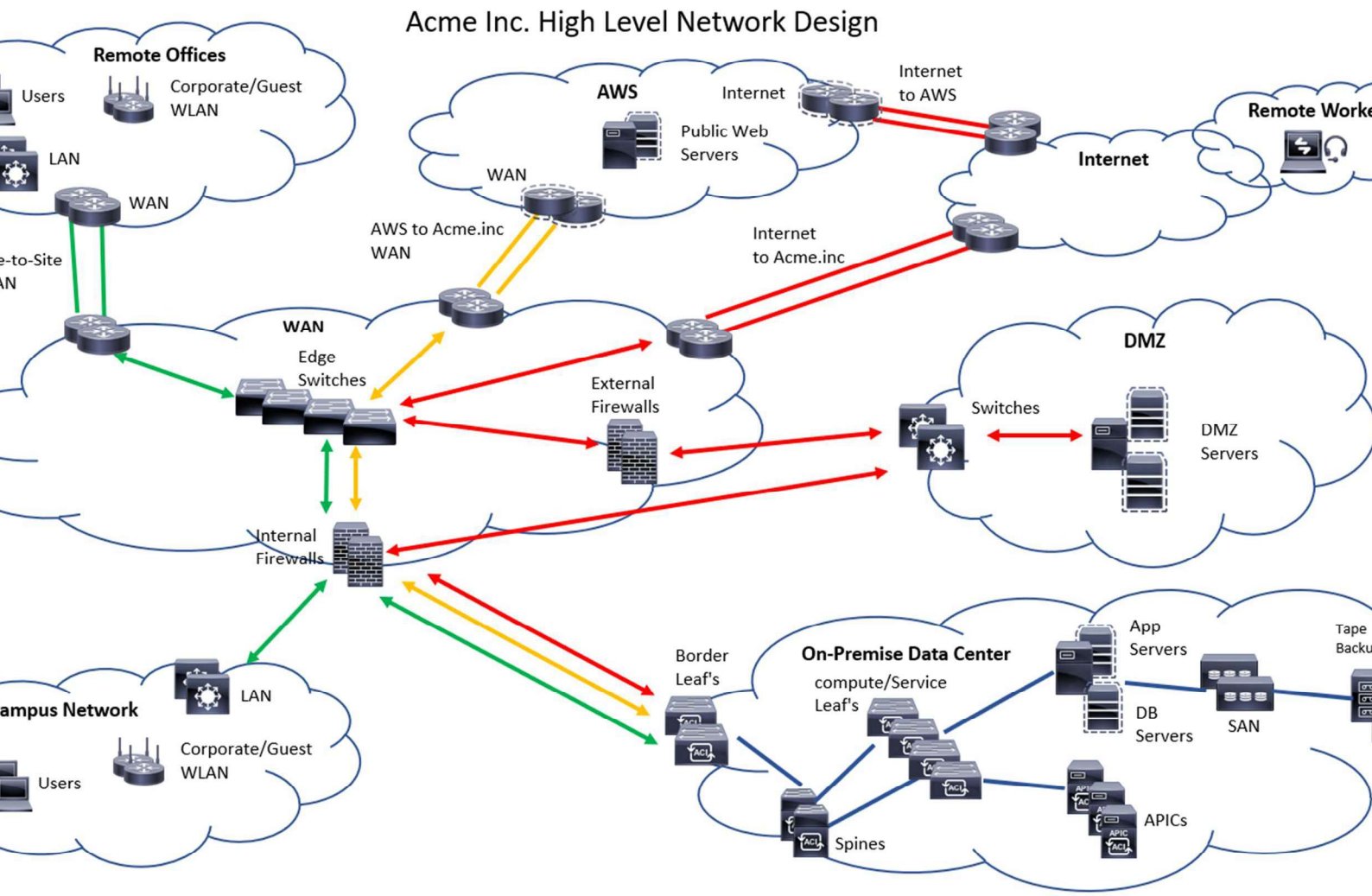
Patching our devices on a regular basis is also crucial to mitigate against bugs and vulnerabilities that are identifies in older software or firmware versions. Implementing a quarterly patching cycle would mitigate these risks and also implementing emergency patches to devices as zero-day or emergency vulnerabilities are discovered. We will also need to design our environment to facilitate this regular patching without impacting the organisations production services, this can be designed into our architecture by making devices highly available so patching one device at a time will not cause a service interruption.

3. Architecture and Orchestration

In this section, I will breakdown the enterprise architecture of acme.inc and go into the detail of the technologies that I have designed into the network to make the environment secure. This design and the technologies that are deployed in the organisation will protect the organisation from the threats I have outlined in the problem analysis. The architecture is designed with defense in depth so there will be multiple security enforcements for the different traffic flows.

I will start off again with the high-level design that I used to outline the different network segments in the problem analysis in Figure 2, however I will now breakdown that high level diagram into the individual traffic flows that I want to concentrate on to demonstrate how defence in depth has been applied to my design and the different technologies I have designed into the solution to achieve the security requirements.

The first traffic flow I will focus on will be network traffic being sent from the campus network in the head office to the remote office site. The second network flow will be between the AWS cloud data center and the on-premise data center. Then I will look at the network flow from the remote access user back into the on-premise data center and the security solutions that are in place to secure that traffic. To finally moving onto looking at Security Information and Event Management (SIEM) and Vulnerability management solutions which would be used by the security operations center to monitor acme.inc infrastructure and report on any security issues identified.



Acme Inc. High Level Network Design

3.1.Network Flow 1 – Campus Network and Remote Office

This first traffic flow covers communication between one of the organisations remote offices and the head office campus network. Even though I have classified this flow as one of the least risky there are still a lot of security measures built into this communication path. In this network flow a lot of the security concerns are in relation to the devices connecting to the network and making sure they do not introduce a security exploit into our environment such as malware.

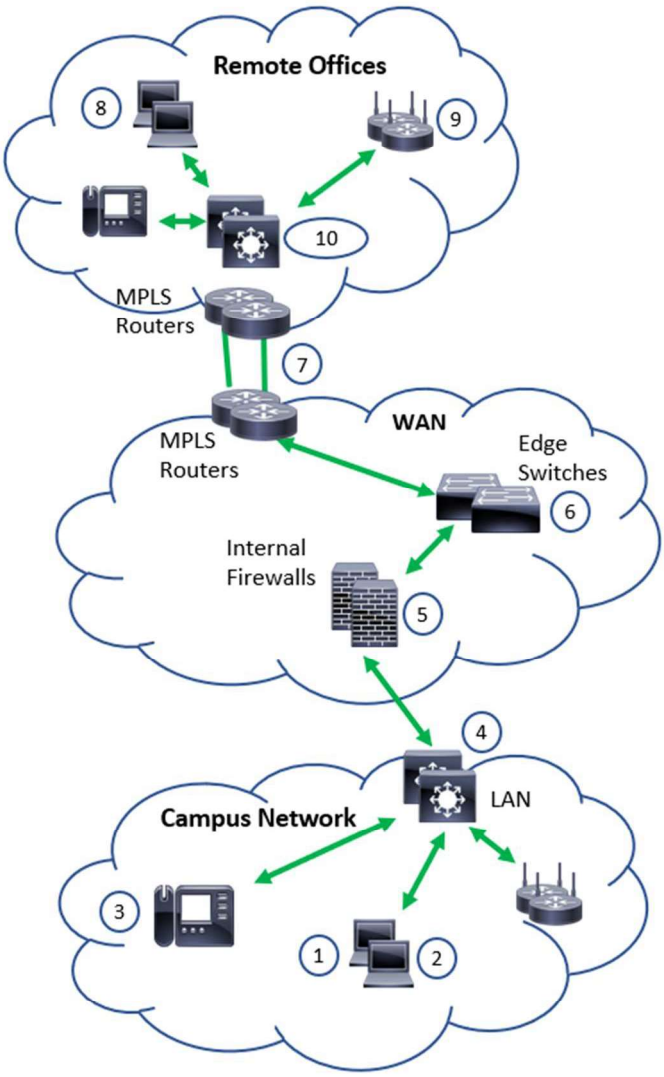


Figure 3: Remote Office and Campus Network Flow

There are ten separate security technologies and techniques I will elaborate on which make up the defense in depth strategy of this particular network flow.

1. Anti-Virus Software

The first step in securing the network is making sure that devices such as laptops connecting to the network are not infected with viruses or malware. This at tits most basis level is having up to date anti-virus software running on the laptops in the organisation. Most anti-virus application these days do a lot more than just scanning the devices for viruses they can also provide protect against malware and ransomware. Vendors such as Sophos also provide advanced Endpoint Detection and Response (EDR) through their Intercept X product which continuously monitors and collects data from the endpoints that could indicate a threat and then automatically respond to these threats to remove or contain then and send notifications to the organisation's security operations center (Sophos, 2022).

2. Network Access Control (NAC) Posture

Network Access Control applications allow us to restrict the devices that are allowed to connect to our network. An important part of what network access control can do for our organisation in term of making sure the endpoint is secure is in relation to posture. Posture means that there is a NAC agent installed on the endpoint which scans the endpoint to make sure certain parameters are met before allowing the endpoint in this case the user laptop to connect to the LAN or WLAN. In this case we could set the posture agent to detect if the anti-virus definitions on the laptop are up-to-date and if not, we could block the laptop from connecting top our network or allow limited connectivity using an access list so the device can only communicate with the anti-virus update server to update its virus definitions. Cisco Identity Services Engine (ISE) is an example of a Network Access Control application which I have researched as part of this project (Cisco ISE, 2022).

3. Network Access Control MAC Authentication

For dumber devices such as IP Phones that we want to connect to the network Cisco ISE allows us to do MAC address authentication. This is where the MAC address of the devices is configured on the network access control system and once the phone is connected to the switchport the phone is authorised to connect to the network using MAC address authentication.

4. Network Access Control Multi-Factor Authentication

Since the switch in the campus network is configured to use the Cisco ISE to authenticate users connecting their laptops to the Local Area Network only authorised users and laptops are able to connect to our network. This happens using 802.1x and can be a combination or certificate and username/password authentication to validate that this is an authorised user and device. Using network

access control to restrict users and devices that can access our LAN adds a comprehensive layer of security to our network perimeter.

5. Internal Firewalls

Firewalls use both static and dynamic packet filtering and VPN support to ensure that all connections between the network, internet, and firewall are valid and secure. They can use whitelists or a signature-based IPS to distinguish between safe applications and unwanted ones, which are then identified using SSL decryption. A firewall solution such as Cisco Firepower would be deployed within acme.inc environment to protect traffic flowing north/south into and out of the network and also east/west traffic which flows internal to the network between such as traffic between the campus and remote office network.

6. High Availability

As with all critical network devices that need to stay in operation to allow the organisation to function, I have installed them in high availability configuration. This is not only to provide high availability in the case that we have a fault in the network, it is also to allow a constant patching and upgrade cycle to take place without disrupting production services. One of the most critical security incident preventions is constant patching of the IT infrastructure to make sure that bugs and exploits that are discovered in the firmware can be patched regularly and critical zero-day vulnerabilities can be patched at very short notice.

7. MPLS Remote Site Connectivity

How I chose to connect my remote sites together as well as the connectivity from the remote sites back to the head office network also adds an extra layer of security to this network flow. Unlike using the Internet for the WAN connectivity between my remote sites and head office MPLS provides more secure connectivity. Using MPLS as well as giving me a bandwidth and latency guarantee for connecting the sites also gives me a private network with my services providers network which is more secure than a shared public connect and I can also use encryption over the MPLS connection for further security.

8. Email Security

One of the most prevalent ways attackers can introduce malware or a virus into our organisations network is via email. To combat this risk, we can use a hosted email security service such as Cisco IronPort, which cleans up all inbound email by using industry leading anti-spam and anti-virus to make sure the email that reach the users are free from malware.

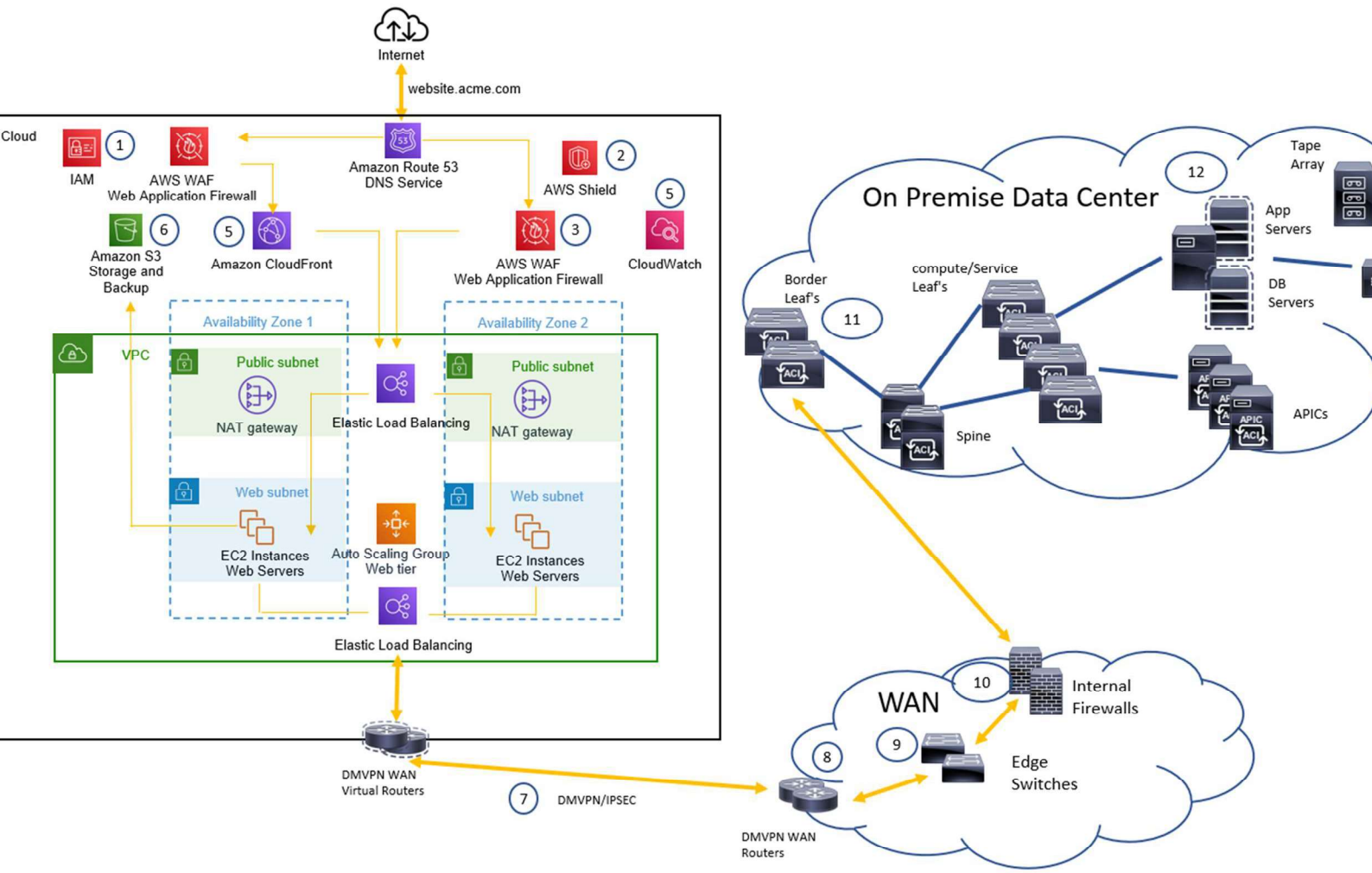
9. Wireless LAN authentication

As well as securing access to the LAN Network Access Control applications such as Cisco ISE can also control access to the Wireless LAN in the same manner. In the case of the wireless LAN, we may also want to provide access to a guest LAN for visitors to our offices or to support users' non-corporate BYOD devices. Cisco ISE also allows us to create a guest wireless access landing page where they can request sponsor approved access to the guest wireless network. The guest wireless access can then be segregated from the corporate network using access lists to allow the guest user access just to the public internet. We can also complete some agentless posturing to make sure that the guest devices connecting to our wireless guest network are running up-to-date virus definitions for added security.

10. Network Segregation

As outlined in the introduction this organisation has multiple departments working in the same building and connecting to the same LAN switches. Network segregation adds an extra layer of security to the network by keeping these departments in separate VLAN's. By doing this we can also deploy Dynamic Access Lists (DACs) to the switches or wireless controllers to make sure depending on which Organisation Unit (OU) you are port of you only have access to the specific IT resources that you need access to. An example of this would be for the network operations teams where as well as restricting access to connect to the network routers and switches via TACACS, this access would also be controlled via a Dynamic Access List. So only devices connected to the network and authenticated to be laptops used by the network operations teams would even be able to connect to the routers and switches. So, users in the human resources VLAN wouldn't even be able to ping the routers and switches and would only have access to the resources they require for doing their job.

etwork Flow 2 – AWS and On-Premise Data Center



WS and On-Premise Data Center Network Flow

1. Amazon Web Services Identity and Access Management (IAM)

AWS IAM is used to securely control access to our AWS resources. A principal is an entity that can perform actions on an AWS resource. A user, a role or an application can be a principal. To confirm the identity of the principal and allow them to access our AWS resources we authenticate using identity and access management using credentials or private keys. AWS IAM allows us to provision individual usernames and passwords for each user or resource looking to access acme.inc resources in AWS. We can also configure granular permissions and apply access policies to individual requests for example we can allow a user to download files from AWS but block certain users from editing the information in those files through the IAM access policies (AWS IAM, 2022).

AWS IAM also allows us to implement Multifactor authentication (MFA) this gives an extra layer of security to our user accounts as we can request the user provide multiple forms of identification before giving them access to our AWS resources. This could be requesting the user to provide a username and password along with a one-time password generated by an RSA token or an authentication app on the user's phone. IAM also allows us to provision identify federation, this is where IAM is configured to trust another authentication source. In this case our users could have already authenticated via a google account and using identity federation we can allow access to our AWS resources via this authentication. This gives us the capability to use Single Sign On (SSO) functionality to allow users use the same account details, username and password to log onto both the AWS cloud platform as well as our organisations on-premise resources.

IAM can also help us achieve our compliance standards we have implemented in our environment as IAM is compliant with some of these standards including the Payment Card Industry Security Standard (PCI DSS). PCI DSS would be applicable if our organisation amce.inc was processing credit card payments for services they are selling through our website hosted in our AWS data center. PCI DSS is made up of twelve controls in order to be complaint with the PCI DSS standard and one of these is to maintain proper password protections which is where AWS IAM fulfils this requirement.

In terms of cost AWS IAM is free of charge as there are no additional costs associated with IAM security and we can create as many users, groups and policies as we need to control the access to our environment for free.

2. AWS Shield

AWS Shield is another security web service provided by AWS which is designed to protect our AWS data center and public facing web services against a Distributed Denial of Service (DDOS) attack. Since we are hosting our public website (website.acme.com) in the AWS cloud it is important to enable AWS Shield to mitigate against a DDoS attack being executed against our website.

AWS Shield offers multiple services including traffic monitoring which enables AWS Shield to inspect traffic entering our network and apply a combination of traffic signatures and algorithms to detect suspicious traffic patterns. The core service AWS Shield provides is the Distributed Denial of Service mitigation where ninety nine percent of attacks are automatically mitigated within less than one second of the attack occurring. AWS Shield also provides a global threat dashboard which can be used by our organisation security operations center (SOC) as it provides DDoS information on attacks that are ongoing across the AWS network and this combined with the advanced real-time metrics and reports from AWS Shield provides valuable insights for our SOC. In the event of a DDoS attack taking place against our AWS public facing website AWS Shiels also provides 24 x 7 access to the AWS DDoS Response Team (DRT). The DRT can provide assistance during a DDoS attack and help to customise mitigation techniques (AWS Shield, 2022).

Common DDoS attacks that AWS Shield protects us against would be a SYN Flood Attack, this is where an attacker initiates a connect to our web server and send the SYN packet to start the TCP three-way handshake. However, instead of completing the TCP three-way handshake the attacker just keeps send SYN packets which consume the connection state table to where our server can no longer accept genuine connections. AWS Shield also offers protection against volumetric attacks, this is where the attacker sends a large amount of malicious traffic to our network which overwhelms our network and causes our applications and services to become unavailable to legitimate users or employees.

There are two different tiers available when using AWS Shield, AWS Shiels Standard and AWS Shield Advanced. AWS Shield Standard is the free tier of AWS Shield and it does offer DDoS protection against some of the most common layer 3 and layer 4 DDoS attacks. AWS Shield Advanced is a paid service which provides additional DDoS protection at the application and network layers.

3. AWS Web Application Firewall

AWS Web Application Firewall (WAF) is a security web service that control the network traffic entering and existing the AWS public cloud for applications and websites. By provisioning AWS WAF's in the flow of the network traffic before it hits our web servers, we can configure security rules that allow us to deny or monitor the requests before they hit our web servers. There are a few key features of AWS WAF's including protecting our web servers from web attacks by filtering the web requests according to the rules we create on the web application firewall. These rules can filter by IP address, HTTP headers, URI strings from a website and HTTP body. AWS WAF's also provides for integrations into other AWS services including Amazon EC2, CloudFront, Load balancer.

4. AWS CloudWatch

Amazon CloudWatch is an infrastructure monitoring and management platform. The features of Amazon CloudWatch offer two major services, namely logging and metrics. This is achieved through

CloudWatch logs insights, CloudWatch logs, CloudWatch alarms and CloudWatch events. These are all very useful tools for our organisations SOC to give insights into what is happening in our AWS data center. CloudWatch Logs insights assists us in visualising and analysing log data. We can do this by creating graphs to visual the data and publish that data to our CloudWatch dashboard where our security operations team can also filter and aggregate the log data. CloudWatch logs can be used to collect and store the logs from multiple AWS services, on-premise resources or applications. Using CloudWatch Alarms an alert can be triggered to the metrics we have configured exceed a specific threshold we have setup. These alerts can also be displayed on the CloudWatch dashboard which can be monitored by our security operations center. CloudWatch Events, monitors state changes on our AWS resources.

5. Amazon CloudFront

AWS CloudFront is a content delivery network (CDN) that allows us to transfer static web content such as files, media, images and videos to users across the globe securely and at high speeds. Amazon CloudFront is extremely secure in that it provides both network and application-level protection. CloudFront uses AWS Shield to protect our website and application from Distributed Denial of Service attacks and also uses the HTTPS protocol for secure encrypted transfers. AWS CloudFront offers pay as you go pricing and there are no transfer fees for origin fetches from any AWS origin and ASWS Certificate Manager (ACM) offers TLS certificates at no charge.

6. Amazon S3 bucket for backup and recovery

We use an Amazon S3 bucket to back up a copy of the data on our web servers, this is so our data can be recovered quickly in the event of a failure of the primary data on these web servers. This could be caused by a cyber-attack on our web servers where the data could be destroyed or encrypted in the event of a ransomware attack. There are also other unplanned events which might require us to us our data backups to restore our web servers which as data corruption or the accidental deletion of our data by an administrator of the system.

7. DMVPN/IPSEC WAN connectivity

We need a secure connection method to allow network connectivity between our AWS data center and our on-premise network. There are multiple ways we could design the network to achieve this aim, however in this case since I am running Cisco routers at my WAN edge, I have chosen to create a Dynamic Multipoint VPN (DMVPN) between my cisco routers. In AWS I can provision the Cisco 1000v router and connect this to my on-premise physical routers building a scalable IPsec Virtual Private Network (VPN) over the Internet. This creates and encrypted tunnel over which my sites can communicate securely and I can then route my traffic between the AWS cloud and my on-premise data center using private addressing.

8. Network Device Hardening

There are multiple standards we can use for hardening the configurations of our network devices some of the bodies that release these standards are the National Institute of Standards and Technology (NIST) and the Computer Information Security (CIS) Center for Internet Security. By joining one of these institutes, we can download configuration files that document the configurations we need to add and remove from our network devices to meet the standard. There will be separate configurations for different equipment manufactures and different network devices including routers, switches and firewalls. Some of these configurations may include configuring network access privileges, shutting down inactive network ports, disabling certain network protocols or encrypting network traffic. Since we are using mostly Cisco networking equipment Cisco also maintain equipment hardening guidelines, however using an industry standard such as NIST or CIS can make it easier to be audited against if we are aiming to achieve a compliance standard such as PCI DSS or ISO 27001.

9. Access Lists on the switch VTY lines configuration

By adding access control lists to the VTY lines of the routers and switches we can make sure that only static IP address or subnets assigned to the network engineers can access these devices. This will provide an extra layer of security as well as being protected by TACACS where the engineers also need to provide username/password to connect to the network devices. We could also use Cisco AnyConnect in combination with Cisco ISE to have the network engineers authenticate using multifactor authentication to Cisco AnyConnect before being assigned an IP address in the subnet that is allowed to connect to the network devices.

10. Internal Firewalls

We add internal as firewalls as well as external firewalls to protect the internal or east to west network flows within our organisation. The internal firewalls can be used to provide network segmentation as well as inspect traffic flowing through our network. These firewalls need to be application aware and provide functions such as deep packet inspection to be able to identify protocols and applications by payload and not just via the IP header. This should also include SSL inspection. Our internal firewalls should also perform intrusion prevention so the firewall can identify malicious traffic, unusual traffic patterns or data breach attempts. Cisco Firepower firewalls provide our organisation these features and we can size the firewalls accordingly to the network traffic throughput we expect to flow through these firewalls.

11. Cisco ACI zero trust software defined on-premise data center network

I have chosen to design the on-premise data center to use Cisco Application Centric Infrastructure (ACI) as the core network technology for the data and also to provide zero trust connectivity between the resources connected to the data center network. Cisco ACI uses a spine and leaf connectivity model

which is very efficient method of network connectivity as all resources on the network are no more than two hops away from each other. Cisco ACI is a software-define networking solution and is configured using the APICs that are connected to the network. Cisco ACI uses the Cisco Nexus 9000 series of switches for both the spines and the leaf's which are connected using 100Gbps cables for maximum throughput.

Cisco ACI uses bridge aggregation groups along with endpoint groups to control the connectivity of devices to the network and communication between these endpoint group are tightly controlled using contracts. The contracts are similar to access lists in traditional networking however unlike traditional networking where traffic is implicitly allowed until the access list is applied to block network traffic. In Cisco ACI the network traffic between EPG's is implicitly denied until contracts are put in place to allow communication between devices on the network. This is where the zero-trust network security architect comes from, unless we specially trust a connection between two endpoints on the network then no traffic can pass between them.

12. Access Control using Red Hat Identity Management (IDM)

Since a lot of our servers are running on Red Hat Enterprise Linux (RHEL) we can use the built-in access management to secure the access management to these servers. Red Hat IDM provides a way for us to securely manage the identities for users, machines and servers with our RHEL environment. Red Hat IDM allows us to define access control policies and delegate specific administrative tasks to other power users to create a clear separation of responsibilities. Red Hat IDM also provides a Public Key Infrastructure (PKI) service to allow us to sign and publish certificates for both hosts and services along with allowing us to create Certificate Revocation Lists (CRL) to revoke invalid certificates that we have generated. All this functionality provided by Red Hat IDM is free of charge and included with our RHEL licenses.

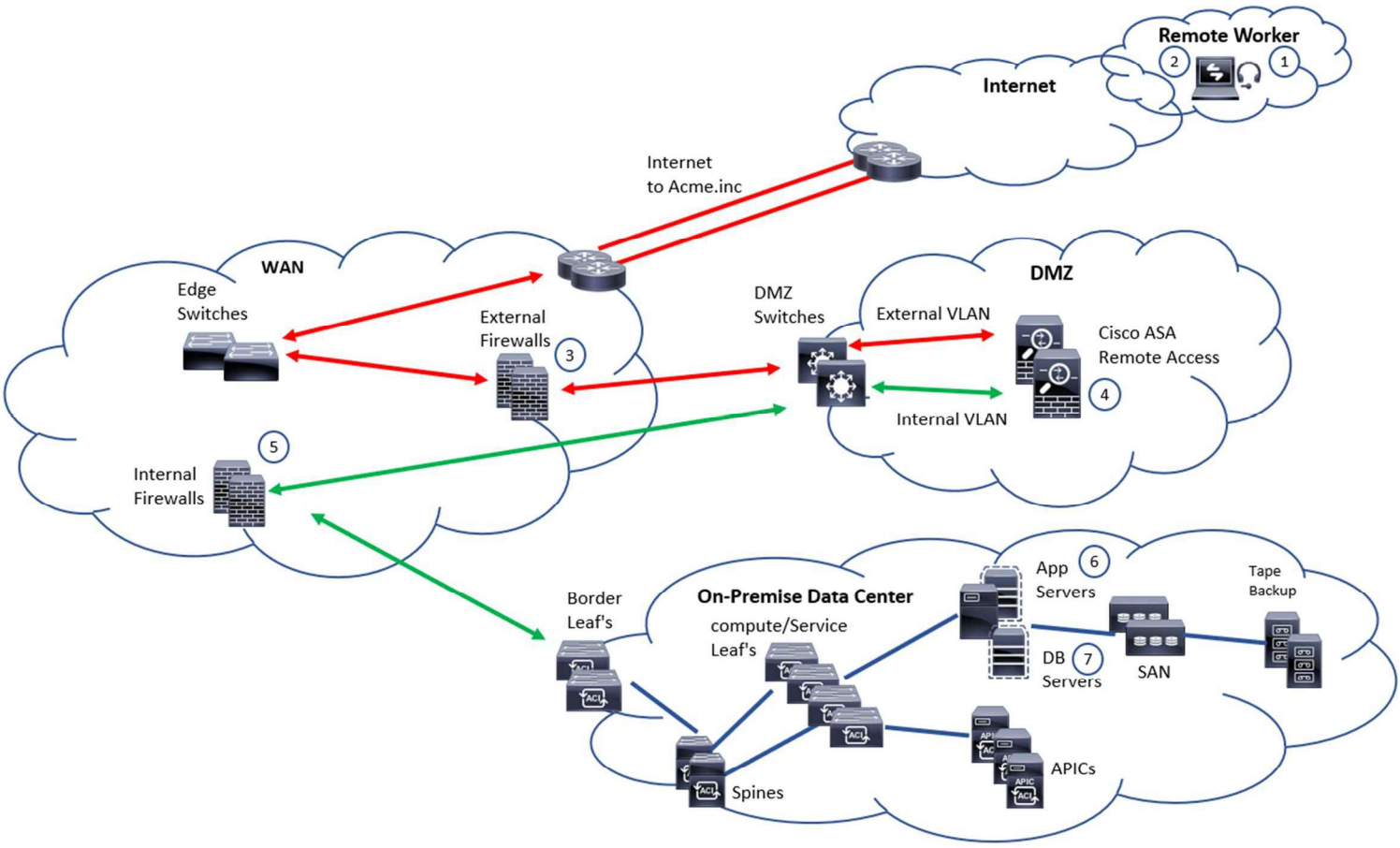
13. Storage Area Network (SAN) security

There are many different storage area network providers in the market for this design I have chosen to use Pure Storage as they specialise in all flash arrays and offer some interesting security features that I can integrate into my overall network design. Two of the main security features that I am trying to implement when designing the storage area network is making sure that my data is encrypted at rest and that I can recover data quickly and securely if my organisation is exposed to a ransomware attack. Pure SafeMode snapshots protect our organisations backup data and metadata by creating a secure copy. If acme.inc is infected with ransomware the ransomware attack can't modify, delete or encrypt SafeMode snapshots even with administrator credentials. By following a straightforward process, we can restore business critical data and be back operating quickly. Pure storage also provides data encryption at rest using AES-256-bit encryption.

14. Offsite tape backup and recovery

Providing offsite backups of our data can be critical to making sure we can restore data in the event of a security breach, malware attack or another disaster recovery situation that might occur at our on-premise data center. We could use a cloud backup service for this or in this case we will use a tape backup service such as Veritas NetBackup with the tapes being collected and stored in a secure location on a weekly basis. If there is a successful ransomware attack against our organisation as well as having the multiple defense in depth layers that we have built into our enterprise architecture we will also add offsite tape backups as an extra layer of defense. That way if our production data or on-site backups were compromised, we could still recover our data from our offsite tape backups.

etwork Flow 3 – Remote Worker and On-Premise Data Center



emote Worker and On-Premise Data Center Network Flow

1. Cisco AnyConnect remote access client

We will use the Cisco AnyConnect client on our employees' corporate laptops to provide full remote access connectivity to our on-premise resources. The Cisco AnyConnect client creates a remote access VPN connection to the Cisco ASA's that are located in our DMZ which are used to authenticate the user and assign the laptop a private IP address that can be used to access resources in our on-premise data center. For remote access authentication we will use multifactor authentication which will include three forms of authentication to authenticate the remote access users. These three forms of authentication will be a username/password, a certificate installed on the clients' laptops and finally a one-time password provided via an RSA token. This means that as well as authenticating the user we are also authenticating the laptop to provide a layered approach to securing our remote access connections. Cisco AnyConnect also integrates with the Cisco Identity Services Engine (ISE) to provide a capability to posture the user's laptop before allowing the laptop to connect to our network, we can setup a posture rule to check if the laptop is running up-to-date anti-virus definitions. If the anti-virus definitions are not up to date the laptop will not be allow to connect until they have been updated.

2. Operating System Hardening

The laptops that our remote users are using are Windows 10 laptops. As well as installing the latest anti-virus software to protect the security of these laptops we can also harden the Windows 10 operating system build. We can use the Center for Internet Security (CIS) hardening standards to harden the Windows 10 operating system which will also map to other security standards such as NIST SP 800-53 and ISO 27001. By hardening the Windows operating system, we will be encrypting the hard disk, enabling and configuring Secure Boot, and limiting and authenticating system access permissions along with other configurations that will make the operating more secure. In this case we will harden the operating system to align with CIS Level 2 hardening which is the most secure configuration we can apply.

3. External Firewalls

The external firewalls protect the flow of traffic in and out of our network, also referred to as North/South traffic. They are configured with policies to block traffic based on IP address and Port number. In this case we will use Palo Alto firewalls for our external firewalls since we are using Cisco Firepower firewalls for our internal firewalls. This is to give extra defense in depth to our solution just in case a vulnerability was discovered with the Palo Alto firewall software that allows a cyber-attack to breach our external firewalls out internal firewalls would not be using the same software as they are a different vendor so the same exploit would not be on our internal firewall software. These firewalls with also run advanced threat protection features and URL filtering.

4. Cisco ASA Remote access appliances

The remote access Cisco ASA appliances are located in the DMZ and will have an external interface for the remote access users on the internet to connect to and an internal interface to allow the remote access users to connect to our internal network resources once they have been fully authenticated. The connection between the Cisco AnyConnect client creates an IPsec encrypted tunnel for the network traffic to secure traverse the internet.

5. Internal Firewalls

We add internal as firewalls as well as external firewalls to protect the internal or east to west network flows within our organisation. The internal firewalls can be used to provide network segmentation as well as inspect traffic flowing through our network. These firewalls need to be application aware and provide functions such as deep packet inspection to be able to identify protocols and applications by payload and not just via the IP header. This should also include SSL inspection. Our internal firewalls should also perform intrusion prevention so the firewall can identify malicious traffic, unusual traffic patterns or data breach attempts. Cisco Firepower firewalls provide our organisation these features and we can size the firewalls accordingly to the network traffic throughput we expect to flow through these firewalls.

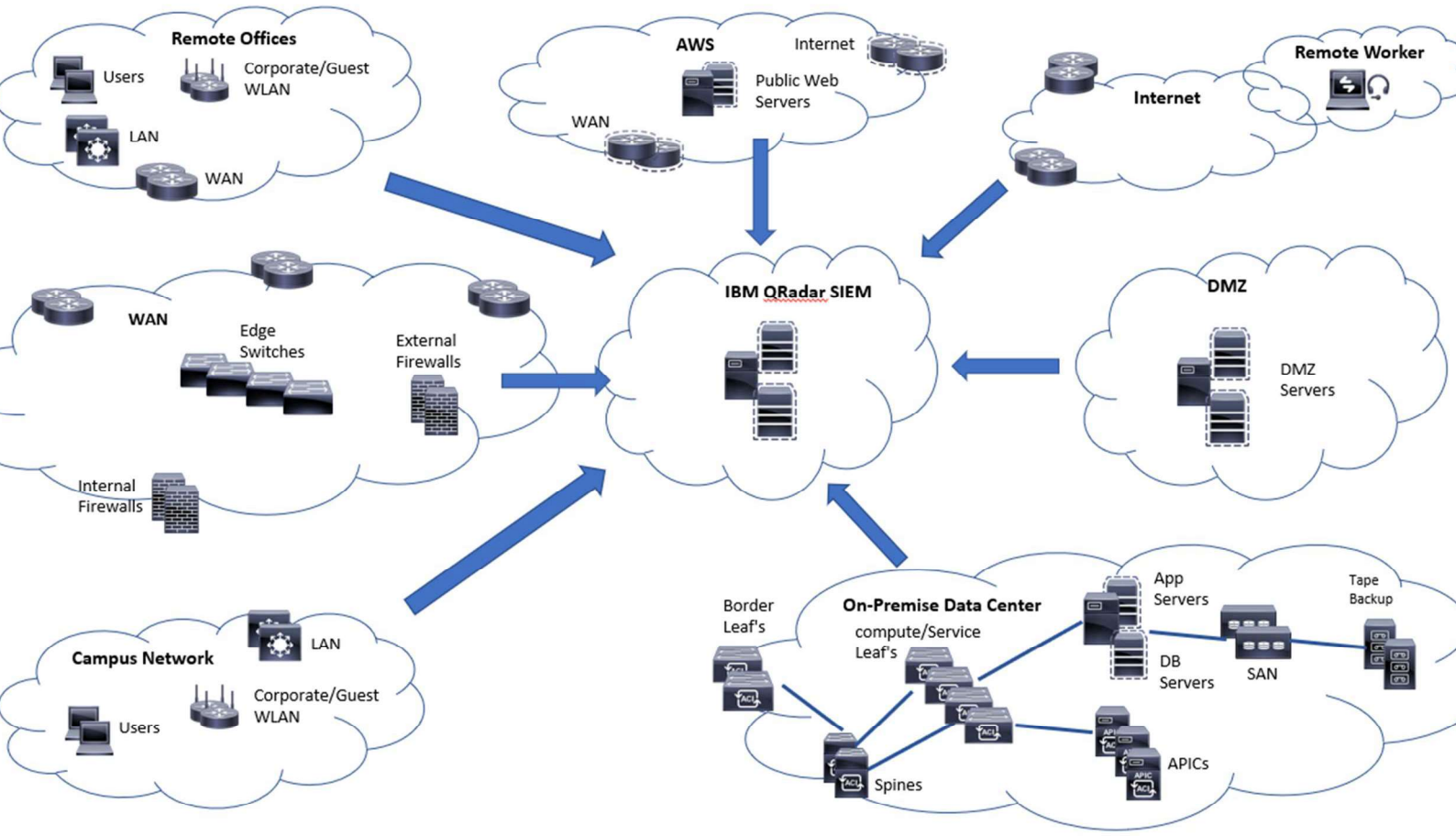
6. Server Hardening

Using the Center for Internet Security (CIS) we can also harden the configuration of our server infrastructure. This involves securing the components, functions, data, ports and permissions of the servers by hardening the security configurations at the software, firmware and hardware layers. These security measures can include making sure that the servers are regularly patched, that access controls are in place to make sure that unauthorised users cannot access our servers and locking our user accounts that have made multiple unsuccessful attempts to connect to our servers. We can also disable the USB ports on the servers to stop somebody intentionally or unintentionally connecting a USB device infected with malware to our servers.

7. Database Hardening

We can also harden our databases by securing the database management system (DBMS) and the data stored within the database itself. This can be achieved by encrypting the information stored in the database, while also making sure that the data in encrypted both at rest and in-transit. We also need to make sure there are appropriate access controls in place such as adding role-based access control (RBAC) polices so that the users accessing the database can only access the tables they are required to access to complete they jobs and limiting the user access on a need-to-know basis. Audit logging is also an important component of making sure the databases are secure as we can see what users accessed when they were logged into the database and if they made any changes to the information stored in the databases.

etwork Flow 4 –Security Information and Event Management (SIEM)



IBM QRadar Security Information and Even Management (SIEM)

Security information and event management (SIEM) is software that enhances security visibility and awareness of our security operations center (SOC) by automatically aggregating and analysing the log and event data generated by all the network devices, network endpoints and applications running across our entire IT environment. There are multiple SIEM offerings in the market including Splunk, SolarWinds and AlienVault. However, in this case we will design IBM Security QRadar SIEM into our environment as our security information and event management system. QRadar will monitor our entire enterprise network using machine learning and artificial intelligence algorithms to provide our security operations center with insights into any anomalies in the log or event data that may suggest that there is a security incident taking place in our network.

IBM QRadar correlates and analyses multiple data types across a wide variety of endpoints that are locate on our network as well as all the network devices including routers, switch and firewalls. QRadar also collects data from our Amazon Web Services (AWS) resources and from our identity management solutions such as Red Hat IDM. It can be deployed as a hardware, software or virtual appliance in our environment and can integrate with a security orchestration automation response (SOAR) platform for incident response and remediation. It can also be deployed on-premise on in cloud environments. By providing this advanced monitoring solution to our security operations personnel it will enable them to make better and faster decisions to protect our organisation against critical cyber security threats. (IBM, 2022)

Figure 7 illustrates and example of the QRadar dashboard that our security operations center would be monitoring. There are many different views that our security teams can use to identify issues with the below view showing information on our corporate users.

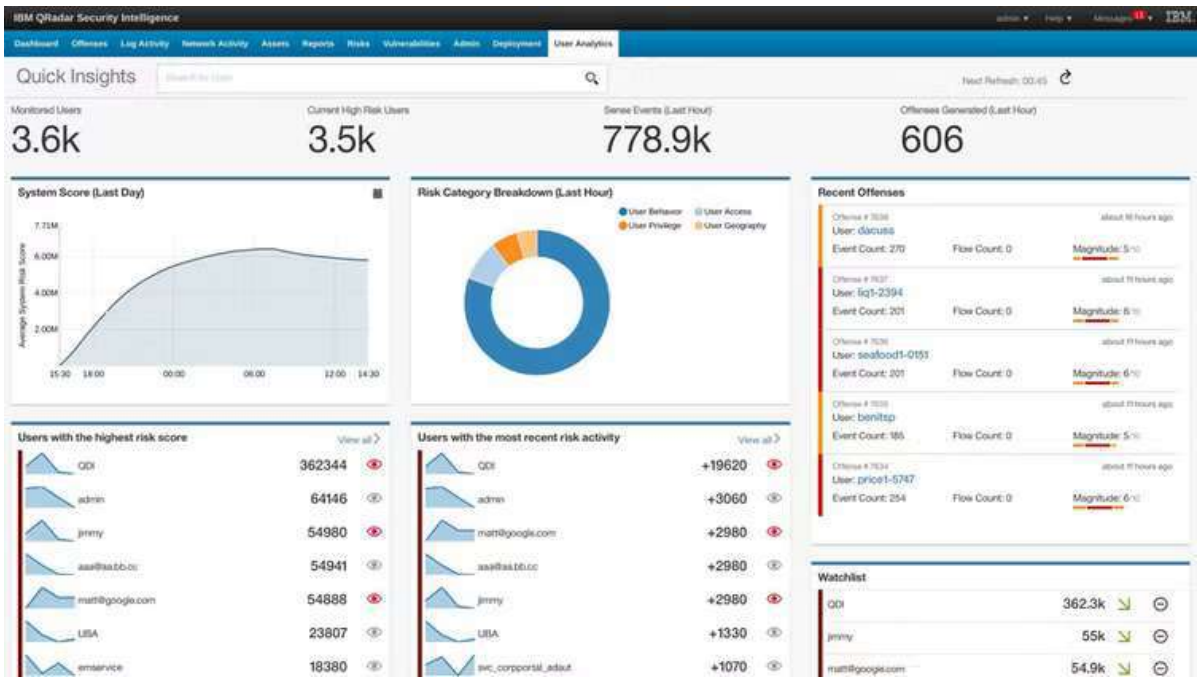
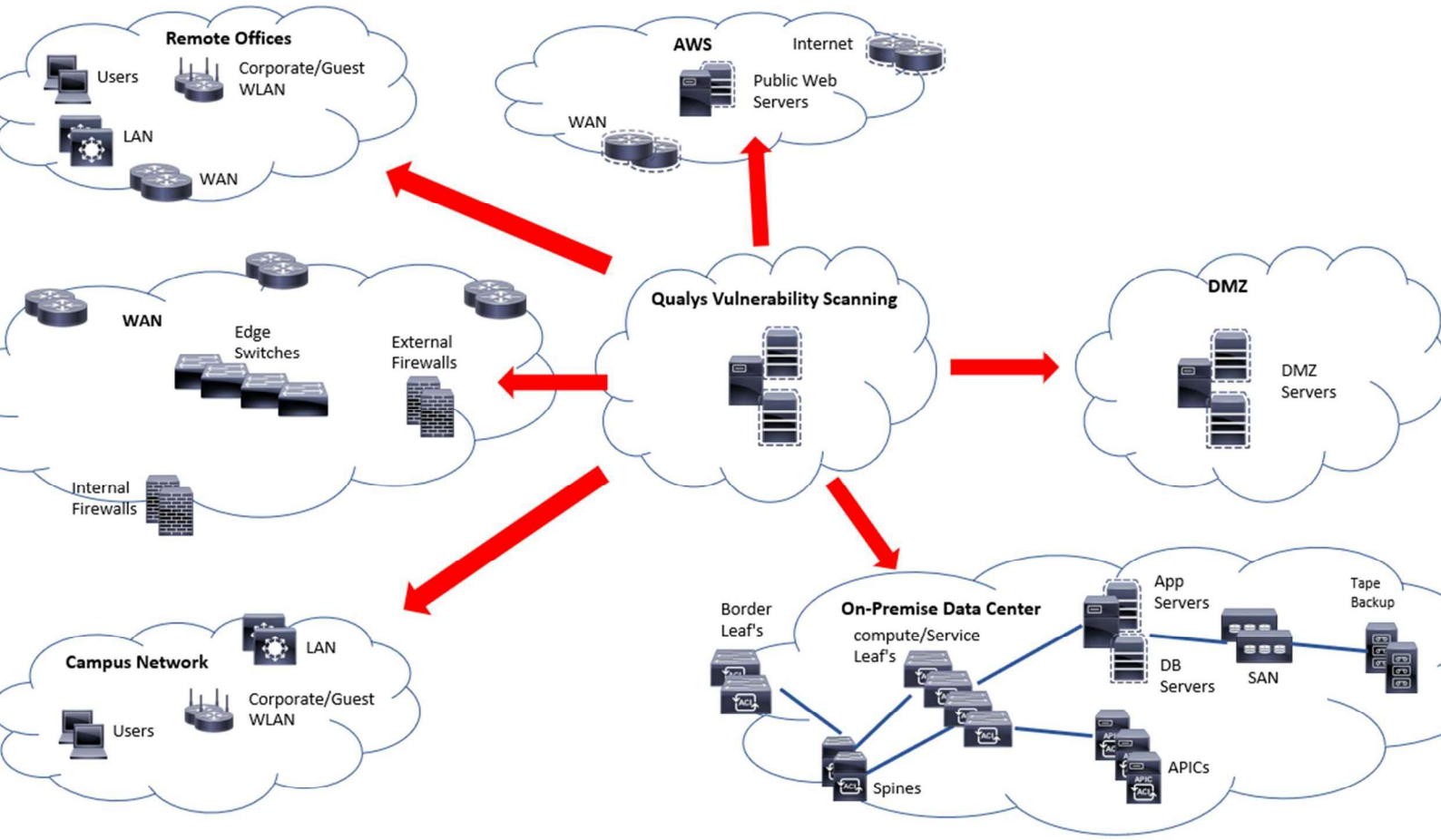


Figure 7: IBM QRadar User Analytics

etwork Flow 5 – Qualys Vulnerability Scanning



ualys Vulnerability Scanning

Vulnerability scanning is a critical component of our vulnerability management program, it is the process of identifying security vulnerabilities such as open ports, configuration mistakes and security flaws in the software running in our environment. In this case I will chose to add the Qualys vulnerability management system to Acme Inc. environment to provide a vulnerability scanning capability. Qualys generates detailed reports on the security risks identified in our environment ranking the identified risks from urgent to minimal. Figure 9 display the five severity levels for vulnerabilities or possible vulnerabilities identified by Qualys.

Severity	Description
Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Figure 9 - Definition of Vulnerability Severity Levels

There are multiple types of reports that can be generated by Qualys, these include; Map reports which provide a network topology to where we can compare the network map with a previous network map to see if there have been any network endpoints added or removed from the network. Scan reports are the detailed vulnerability assessment reports which we are most focused on as they provide detailed reports on the vulnerabilities that Qualys has identified on our systems. We can view these vulnerabilities or potential vulnerabilities live on the Qualys dashboard however the reports are going to be very useful for distribution to the individual IT teams that will be required to remediate any of the issues identified.

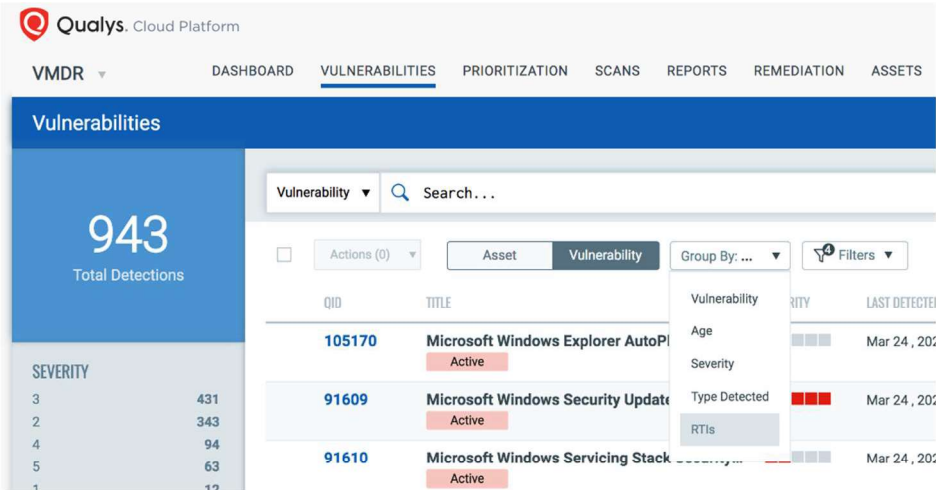


Figure 10 – Qualys Vulnerability Dashboard

4. Conclusion

This project was a comprehensive exercise in designing an enterprise architecture for an organisation to take into consideration all the security tools, software and processes required to build a defense in depth architecture and a layered security approach. Security by design is the major theme throughout this project and it illustrates how security is not just deploying one tool or adding firewalls to the network it is a comprehensive approach that has to be designed into every element of the information technology environment. The approach I took of breaking down the network communication flows internally within the organisation and externally to the remote sites and internet was the best way for me to illustrate all the security controls I had built into my design.

A lot of the time I spent on the project was researching all the possible ways security vulnerabilities could be introduced into the network and investigating what tools and applications are used in industry to mitigate these vulnerabilities. Starting from the user devices such as laptop security and moving throughout the different segments of the network to encompass a zero-trust on-premise data center network to the many security web services amazon web services offers to protect our public websites and data in their cloud data center. The challenge here was to plan the design so each of the security mitigations I designed into the solution would work together to provide layers of security so if one layer was breached out most sensitive and critical data in our on-premise data centre would still be protected. There are also a vast number of tools to choose from when selecting the correct technologies to deploy within our organisation to provide all the security needs. Also, the focus of the project has to be very broad as just looking at the network security would not give us that defense in depth security architecture we require where we also need to evaluate server, client, storage, cloud and database security risks and security tools to protect our resources at every step of the network flow.

I learned a lot through the completion of this project there a number of technologies and tools I have added to my design that I have not deployed before. Cisco Application Centric Infrastructure (ACI) is one of those technologies that is completely redefining the way traditional networking was thought of. Being able to programme the network and moving away from traditional VLAN and Subnets to segment the network to using Bridge Domains, End Point Groups and Tenants with zero-trust being the default option makes the network security design critical as we need to know in advance of implementation which network endpoints need to communicate and on which ports to have the contracts in place for these devices to communicate. Also, security information and event management tools such as IBM QRadar are fundamental to knowing what happening on our network so make it more efficient to identify and mitigate against vulnerabilities and cyber-attacks. While all of these tools and practices in isolation make up a piece of our security defence the real challenge is designing a truly secure architecture is combining all these tools and processes into a cohesive design.

5. References

AWS IAM (2022). What is IAM? Retrieved from https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

AWS Shield (2022). AWS Shield managed DDoS protection. retrieved from https://aws.amazon.com/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc

Cisco ISE (2022). Cisco Identity Services Engine Data Sheet. Retrieved from https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.html?ccid=cc001033&dtid=odicdc000016&oid=dstsc025999

CISA (2022). Understanding Denial-of-Service Attacks. Retrieved from https://www.cisa.gov/uscert/ncas/tips/ST04-015#:~:text=A%20distributed%20denial%2Dof%2Dservice%20(DDoS)%20attack%20occurs,carry%20out%20large%20scale%20attacks.

IBM (2022). IBM QRadar solution brief. Retrieved from https://www.ibm.com/qradar/security-qradar-siem

Sophos (2022). Sophos endpoint protection features. Retrieved from https://www.sophos.com/en-us/products/endpoint-antivirus

Qualys (2022). Qualys Vulnerability Management Sheet. Retrieved from https://www.qualys.com/docs/vulnerability-management-datasheet.pdf