IN PARTNERSHIP WITH PLYMOUTH UNIVERSITY

Name: Chirath Deelaka Perera
Student Reference Number: 10569217

Module Code: CNET233SL	Module Name: Network Security
Coursework Title: Security System for ABC Company.	
Deadline Date: 08/05/2017	Member of staff responsible for coursework: Mr. Saliya Patabandi
Programme: Plymouth Computing	

Please note that University Academic Regulations are available under Rules and Regulations on the University website www.plymouth.ac.uk/studenthandbook.

Group work:please list all names of all participants formally associated with this work and state whether the work was undertaken alone or as part of a team. Please note you may be required to identify individual responsibility for component parts.

Vidanagamage Lasitha T B 10569203
Wanniarachchi Hansini Himalshi 10569206
Wijesekara R W K A I Chathurika 10569058
Dharmagunarathna Sharan S 10569137
Chirath Deelaka Perera 10569217

We confirm that we have read and understood the Plymouth University regulations relating to Assessment Offences and that we are aware of the possible penalties for any breach of these regulations. We confirm that this is the independent work of the group.

Signed on behalf of the group:

Individual assignment:***I confirm that I have read and understood the Plymouth University regulations relating to Assessment Offences and that I am aware of the possible penalties for any breach of these regulations. I confirm that this is my own independent work.***

Signed:

Use of translation software: failure to declare that translation software or a similar writing aid has been used will be treated as an assessment offence.

I *have used/not used translation software.

If used, please state name of software……

Overall mark _____% Assessors Initials _____ Date_____

*Please delete as appropriateSci/ps/d:/students/cwkfrontcover/2013/14

NerdLK
WEB SOLUTIONS

PROJECT REPORT
CNET233SL - Network Security

Security System for ABC Company.

NAME	INDEX
Chirath Deelaka Perera	10569217
VidanagamageLasitha T B	10569203
WanniarachchiHansiniHimalshi	10569206
Wijesekara R W K A I Chathurika	10569058
Dharmagunarathna Sharan S	10569137

CONTENTS

NerdLK

NerdLK is a young and dynamic web development group that interested in new web technologies. We are new comers to the web development sector and we anticipate to get an experience from this project. Furthermore, we have active and well-motivated members who willing to contribute.

Acknowledgement

The success of any work depends on the encouragement and the guidance. We take this opportunity to express our gratitude to everyone who have been instrumental in the successful completion of this assignment. This assignment would not have been successful without sincere support. We would like to thanks our sincere gratitude to our Network Security Lecturer Mr. Saliya Patabandi for guiding us to make this assignment a Success. His advice and criticisms helped us to come up with a good system.

Signed:

1).Overview

ABC Company Ltd is a software development company which has many employees using internet and related services daily. As the network security consultants of the company, we have been entrusted with the task of deploying the network foundation protection with ensuring integrity and availability by protecting the management and control planes to avoid disruptions, internet perimeter protection under that focusing connectivity to the internet safely and saving inner users, resources from malicious, data center protection with saving privacy of proprietary data, network access security control with role-based access and authentication, Secure mobility with providing secure protection for mobile devices and smart devices.

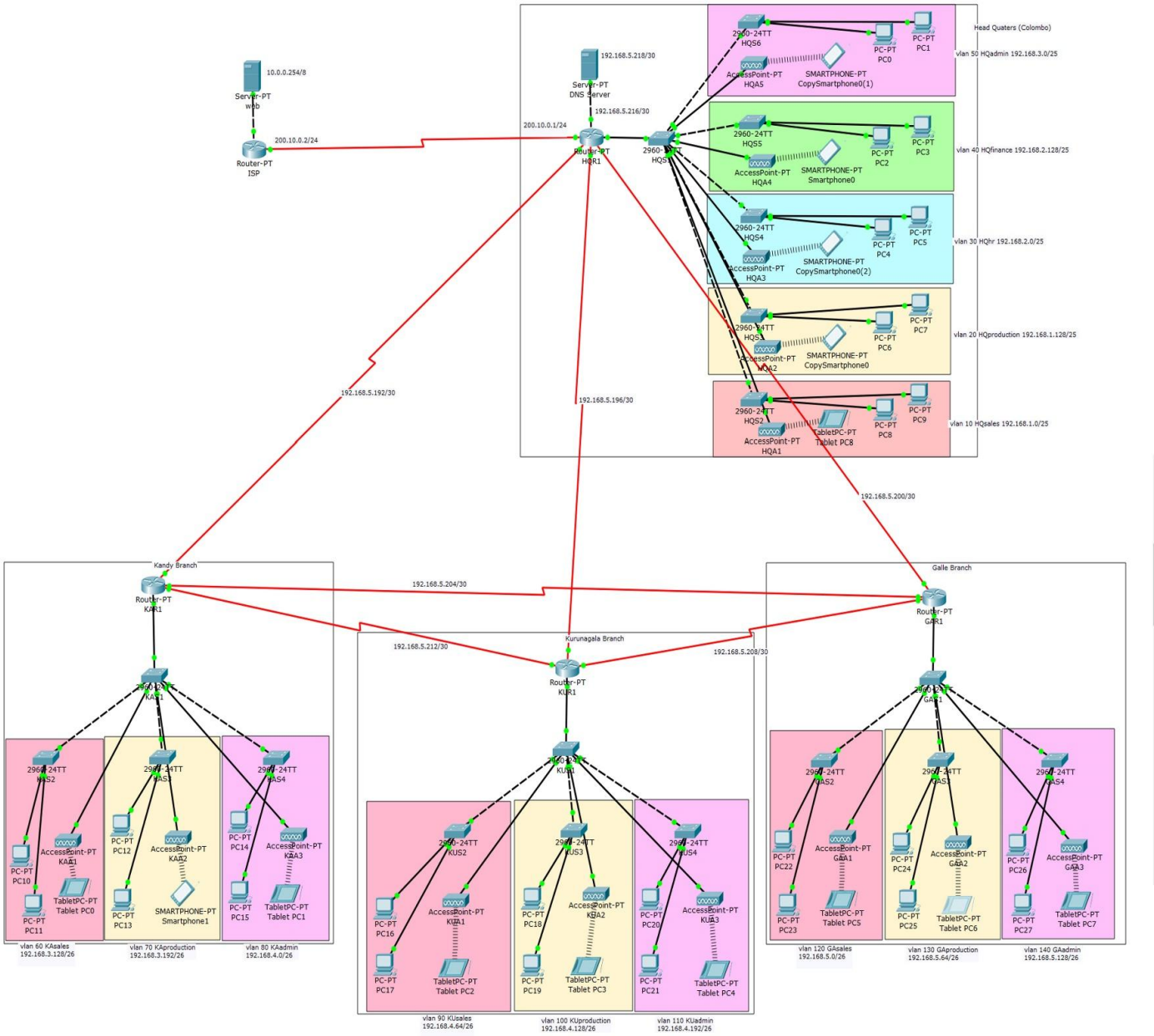
2).Current Situation

Now ABC Company, Ltd using traditional packet filtering firewall which installed at the perimeter of the network and traditional routers, switches. More stages are needed when an IT administrator needs to remove or add devices in the company.

Usually, administrator should manually configure routers, switches, firewalls on a device-by-device. Traditional packet filtering firewall analyze entire outgoing packets and incoming packets and allow them halt based on IP address of the source and destination, protocols.

This company is a software company and there are many users who are accessing internet and networks. So, packet filtering firewall is not the best solution for the company because that firewall can proceed on the layers only. This firewalls not work to the complex rule based models.

3). Network Diagram of ABC Company



The ABC Company was developed a Local Area Network (LAN) and Wide Area Network (WAN) architecture that aligns with its data communication requirements.

The description of the locations to be networked is as follows:

- The company has three branches located at Galle, Kandy and Kurunagala and its headquarters located at Colombo.

- Each branch consists of three departments such as Production, Sales and Admin and head-quarters have HR and Finance departments in addition to Production, Sales and Admin.

- Each department in branches have 20 PCs and each department in headquarters have 60 PCs and senior staff of each branches and headquarters use laptops.

Internal networks of headquarters, branches as well as external network connecting 4 LAN networks together are included in the scope of the design. Management of ABC company have full control over ICT facilities one central connection to internet has been recommended and it should be shared between headquarters and all branches and all ICT services should be hosted in the headquarters and services should be made available for branches as required through the interconnecting WAN net-work.

4). Internet perimeter protection

Perimeter of the network is the outer boundary of the network through which packets flow in and out of the company's network. Perimeter of the network might include;

1. Border Routers
2. Firewalls
3. Intrusion Detection Systems
4. Intrusion Prevention Systems
5. Virtual Private Network (VPN) Devices

This could be a single device providing all the above services or different appliances each providing specific services mentioned above.

Strengthening the perimeter security of a network would mean that putting in place several layers of defense mechanisms or better known as "defense-in-depth" including the ones mentioned above and reducing or at best preventing any security breaches from occurring.

4.1). Proposed Solution

Deploying a Next Generation Firewall (NGFW) system in the perimeter of the company's network which will significantly reduce malware and other malicious security breaches from happening. NGFW is a hardware or software based network security system which able to block or detect sophisticated attacks at the application level or at the port and the protocol levels.

There are some key specifications in NGFWs. They offers

- Application Awareness
- Stateful Inspection
- Integrated Intrusion Protection System (IPS)
- Identity Awareness (User and Group Control)
- Bridge and Routed Modes
- Ability to utilize external intelligence sources.

1. **Application Awareness**

   In traditional firewalls, they are unable to aware the applications because it relies on some common application ports to determine what are the applications running on and to monitor the types of attacks. In NGFW can monitor traffic which is being sent and received without the help of specific applications on those specific ports.

2. **Stateful Inspection**

   In some traditional firewalls, it allows to track traffic based on layer two through layer four. But in NGFWs it allows layer two through layer seven. It provides lot more control to the network administrator or to the company administrator.

3. **Integrated Intrusion Protection System (IPS)**

   IPS is responsible to detect attacks based on different techniques by using their threat signature, traffic behavior analysis etc.
   In traditional firewalls IPS was done with a separate appliance or an appliance that Is logically separate within a single appliance. In NGFWs IPS and IDS (Intrusion Detection System) is fully integrated. In NGFWs IPS performance are higher than traditional firewalls and NGFW provide accessibility to the traffic information of all layers.

4. **Identity Awareness**

   NGFW can track the identity of the traffic device or the user. For that NGFW use either Active Directory or LDAP (Lightweight Directory Access Protocol). Advantage of this function is network administrator will able to control the types of traffic which are allow to enter and exit from the network and as well as to control the type of traffic which specific user can send and received.

5. **Bridge and Routed Modes**

   This is not a totally new feature but in NGFW it is important to use in either bridge mode or routed mode. Still in most of the networks they are not moved from traditional firewalls to NGFWs. Because of that NGFWs must place on bridge mode. By doing that device itself won't show as part of the routed path. In-order-to use the routed mode all traditional firewalls need to convert in to NGFWs.

4.2). Factors taken into consideration when awarding points

1. **Firewall**

When awarding points to how effective the firewall is, we have taken into consideration the throughput of the device at higher loads, how well the device enforced its firewall policies as well as how effective it was in respect to securing the network.

2. **Antivirus protection**

When awarding points to how effective the antivirus software of the device is, we have taken into consideration the ratio of threats the device was exposed to the ratio of threats the device could block.

3. **Intrusion detection and prevention**

When awarding points to how effective the intrusion detection and prevention system of the device is, we have taken into consideration the number of threats or exploits the device was exposed to and the number of exploits the device could correctly identify, alert and block. Further we have considered the false alarms that the system would fire for non-malicious content.

4. **Application control**

When awarding points to how effective the application controlling mechanism of the device is, we have taken into consideration how effectively and successfully the device could identify or determine the correct application and how effective the device was in taking the appropriate actions based on the policies defined for that application.

5. **Centralized reporting**

When awarding points to how effective the reporting and logging functions of the device is, we have taken into consideration the ability of the device to report any malicious activity and log them for later reference. Also, the ease of use of the reporting application of the device and how correct and efficient it is.

6. Performance

When awarding points to how well the device performed overall, we have taken into consideration the throughput of the device under differing loads and frame sizes and the latency in processing frames through it. Also, we have taken into consideration the response times of the applications when the packets were filtered through the firewall and number of connections it can handle per second as well as the number of connections it can handle.

7. Pricing

when awarding points for how worth the product is for the price it is listed, we have taken into consideration the purchasing price of the device and the total cost of ownership per protected megabit per second

8. Ease of use

When awarding points to how user friendly and easy to use the device, we have taken into consideration how easy it is to use the device's operation system, its user interface, how easy it is to install the device within the network etc.

9. Additional features

When awarding points to this specification we have taken into consideration the additional features the device is included with out of the box which are additional to the requirement specification of the company.

4.3). Product Evolution Criteria

Product Evolution	Fire wall	Antivirus Protection	IDS/IPS	Application Control	Centralized Reporting	Performance	Pricing	Additional Features	Ease of use
Fortinet Fortigate 3200D	5	5	5	5	5	5	5	5	5
Cisco FirePOWER 8350	4	5	5	5	5	4	3	5	5
Check Point 13800 NGFW	3	5	5	5	5	2	4	5	5
Dell SonicWall SuperMassive E10800	3	4	4	5	5	3	4	5	5

Products are evaluated on a 0 to 5 points basis where 5 is awarded to the best product in the category.

Fortinet Fortigate 3200D

The Fortinet Fortigate 3200D next generation firewall delivers amazing performances and also extensive security features.

Fortigate 3200D powered by “FortiASIC” processors that can deliver the power to detect malicious content at multi Gigabit speeds.

- Network Processor

  FortiASIC NP6 network processor works with FortiOS functions and delivers ultra-low latency down to two microseconds as well as provide superior firewall performance for IPv4/IPv6.

- Content Processor

  FortiASIC CP8 content processor provides high speed cryptography and content

- In Fortigate 3200D’s FortiOS provides grater traffic visibility and more consistent control over users.
- In fortigate 3200D there is 960GB internal storage helps companies where there are large number of users.
- When consider system performances Fortigate 3200D has 80Gbps Firewall throughput. And firewall latency of 3 microseconds.

Key Specifications of the Fortigate 3200D

10 GE SFP+ / GE SFP Slots	48
IPS Throughput	14 Gbps
Weight	17.2 kg
Height * Width * Length	3.5 * 17.4 * 21.9 inches
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSl-VPN
Price	US$ 80,000
3 year TCO price	US$ 181,100

Cisco FirePOWER 8350

- Cisco FirePower 8350 has 30Gbps firewall throughput and firewall latency of less than 150 microseconds.
- In Firepower 8350 there is 128GB internal memory which is suitable for medium size of company.

Key Specifications of the Firepower 8350

10 GE SFP+ / GE SFP Slots	8
IPS Throughput	15 Gbps

Price	US$ 264,590
3 year TCO price	US$ 372,348

According to NSS lab reports

Firepower 8350 proved effective against all evasion techniques tested. Also it passed all stability and reliability tests. Also FirePOWER 8350 proved effective in enforcing all firewall policies.

During NSS lab analyze it gives the IPS throughput of 18.771Gbps which exceeds cisco claimed performances of 15Gbps.

Check Point 13800 NGFW

- Next Generation firewall

  Check point is NGFW because, check point identify and control applications by user and scan content to stop threats.

- Next Generation Secure Web Gateway

  Check Point enables secure use of web 2.0 with real time protection.

- Next Generation Threat Prevention

  Check Point prevent sophisticated cyber threats with IPS, Application Control, Antivirus, Anti-Bot, email security and URL Filtering.

- Check Point 13800 has 3,800 security power and 27.2Gbps firewall throughput.
- It offers Network Connectivity for IPv4/IPv6.
- Check Point 13800 has 16GB memory and its suitable for medium type of network.

Key Specifications of the Check Point 13800

10 GE SFP+ / GE SFP Slots	12
IPS Throughput	6.4Gbps
Weight	17.5kg
Width * Length * Height	17.4 * 23.6 * 3.5 inches

Certifications

Safety:	CB, UL/Cul, CSA, TUV
Emission:	FCC, CE, VCCI, C-Tick
Environment:	RoHS

Price	US$ 99,000
3 Year TCO Price	US$ 166,590

Dell SonicWall SuperMassive E10800

"Sonic Wall SuperMassive E10800" is dell's Next Generation firewall which designed for large type of networks to deliver scalability, reliability and deep security at multi-Gb speeds with Zero latency.
Sonic Wall SuperMassive E10800 powered by SoinOS (Operating System) and it has 64GB memory.
Also it has 80GB SSD storage.

Benefits

- Complete threat protection including high performance IPS and low latency malware protection.
- Full Inspection of SSL encrypted traffic.
- Superior application intelligence, control and visualization.

SuperMassive E10800 has 40Gbps firewall throughput and has 96 processing cores.
And also it has bridge mode to connect to the network perimeter.

Key Specifications of the Sonic Wall SuperMassive E10800

10 GE SFP+ / GE SFP Slots	22
IPS Throughput	28 Gbps
Weight	30.3kg
Width * Length * Height	17 * 18* 7 inches
Certifications	

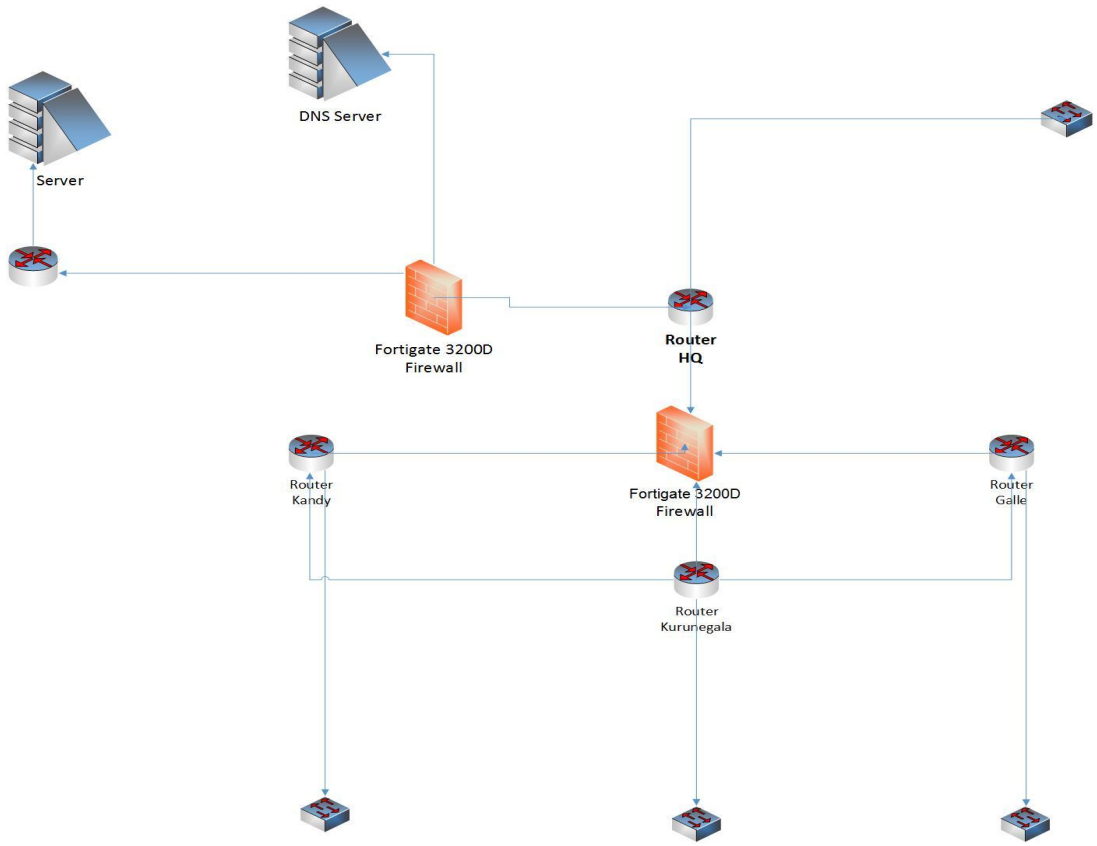
Safety:	CB, UL/cUL, TUV
Emission:	FCC class A, CE, VCCI, C-Tick
Environment:	RoHS,WEEE

Price	US$ 125,000
3 Year TCO Price	US$ 247,700

4.4). Assumptions

- After thorough comparison between three next generation firewalls manufactured by three different highly reputed manufacturers we have decided to go ahead with Foritnet Fortigate 3200D next generation firewall.
- The other devices which were considered are FirePOWER 8350, Check Point 13800 NGFW and Dell SonicWall SuperMassive E10800.
- The main reason for us to pick the Foritnet Fortigate 3200D device was its high throughput, low latency and its price.
- When compared with other two devices Foritnet Fortigate 3200D performed better in all fronts except for application response times which were slightly less compared to others but when compared with the industry standards they were more than acceptable.
- Apart from above factors there were quite a few other factors which were in favour of Foritnet Fortigate 3200D which made it our choice.
- After considering the requirement specification and all factors relating to it we have decided to Foritnet Fortigate 3200D next generation firewall at the perimeter of ABC company's network to enhance and improve the security of the network.

It is better to fix this firewall in between HQ router and other router which is connected the web server in the Head Quarter. Because the data packets are coming from that way.



5). Network foundation protection (NFP)

Network Foundation Protectionis a framework. It provides the technologies and tools to shield different types of network traffic.NFP has three planes. They are control plan, data plan and management plan.

5.1). Proposed Solution

We should reduce network traffic of this ABC company while transforming data to one peer to another together with ensuring availability and integrity of the network by protecting management planes and control plan to avoid disruptions of the network.

- Excessive access control for handling devices than granting management protocols on entire interfaces.
- Cultivating performance for datagrams on no management interfaces.
- Contributing for scalability of the network.
- Management packets are transferred on routing and switches interfaces are prevented from reaching the CPU.
- Offering rate reducing of control plane traffic.
- Allowing a quality of service filter. It manages the traffic of control plane packet.
- Protect edge routers from malicious traffic.
- Ability to forward data, route data and manage data.

5.2). Management Plane Protection Techniques

- Password policy
- Role Based Access Control (RBAC)
- AAA services (Authentication, Authorization and Account)
- Network Time Protocol (NTP)
- Access Control Lists (ACLs)
- Encrypted Remote Sessions
- VLANs
-

5.3). Control Plane Protection Techniques

- Control Plane Policing
- Cisco Control Plane Protection
- Routing Protection Authentication

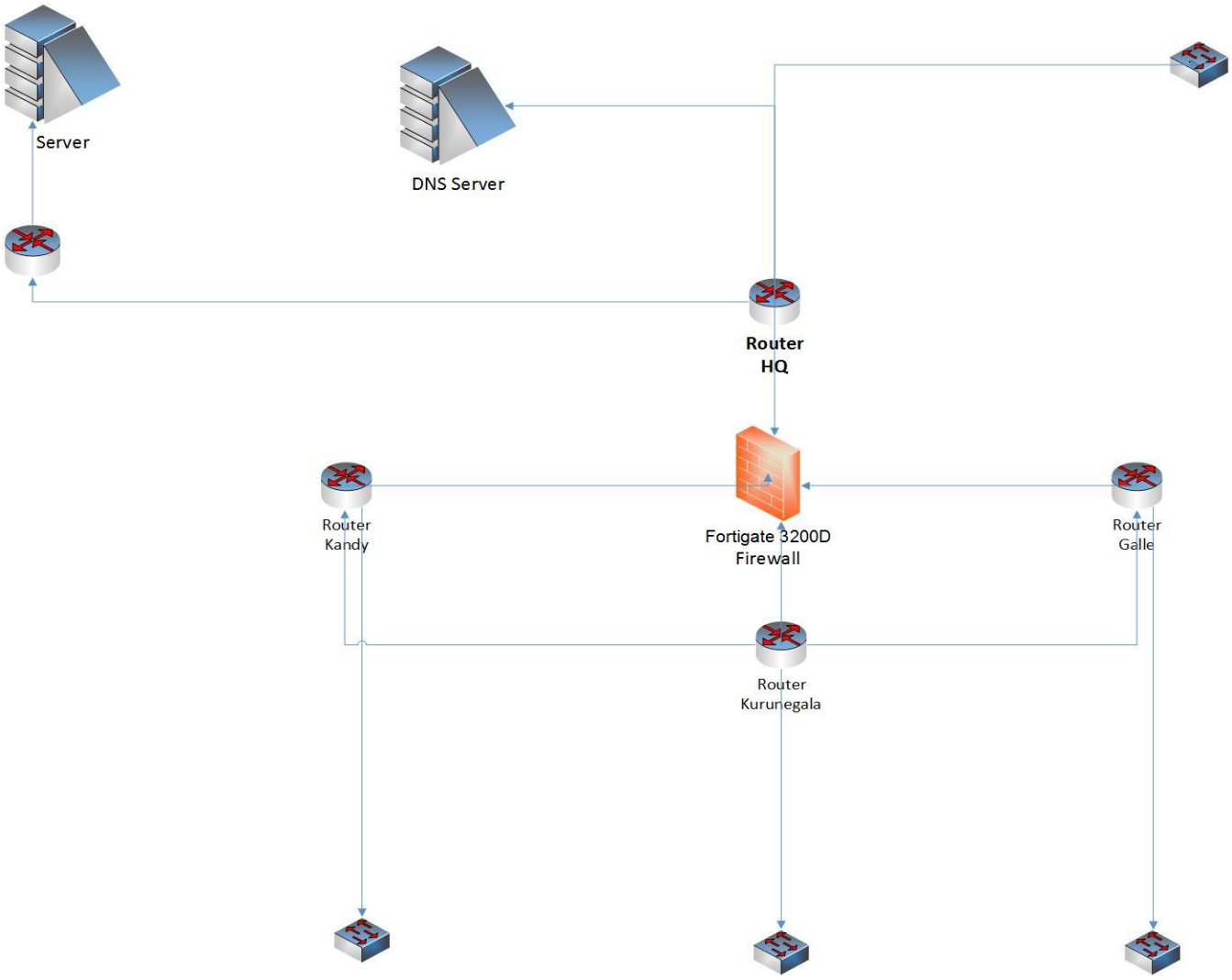
5.4). Data Plane Protection Techniques

- Block Unwanted Traffic using Access Control Lists
- Prevent Denial of Service
- Prevent Spoofing Attacks
- Implement Bandwidth Management
- Use Intrusion Detection Systems and Intrusion Prevention Systems
- Implement Port Security

We have to select a next generation firewall to manage data plane, control plane and management plane. It better to place between routers of branches and HQ.

There few characteristics of Next Generation Firewall,

- Application Awareness
- Stateful Inspection
- Integrated Intrusion Protection System (IPS)
- Identity Awareness (User and Group Control)
- Bridge and Routed Modes
- Ability to utilize external intelligence sources.



5.5). Assumptions

The firewall is an obstruction devices between a trusted and untrusted network. The firewall is placed in the forwarding way Therefore entire packets should be checked by that firewall. Above ABC company has LAN that has host computers and a switch on each branch. The routes are connected all together and HQ Router is connected to the servers. The firewall is always ready to protect the LANs of ABC company. The data are incoming to the LAN and outgoing from the LAN because of that we set the firewall in between router and switch.

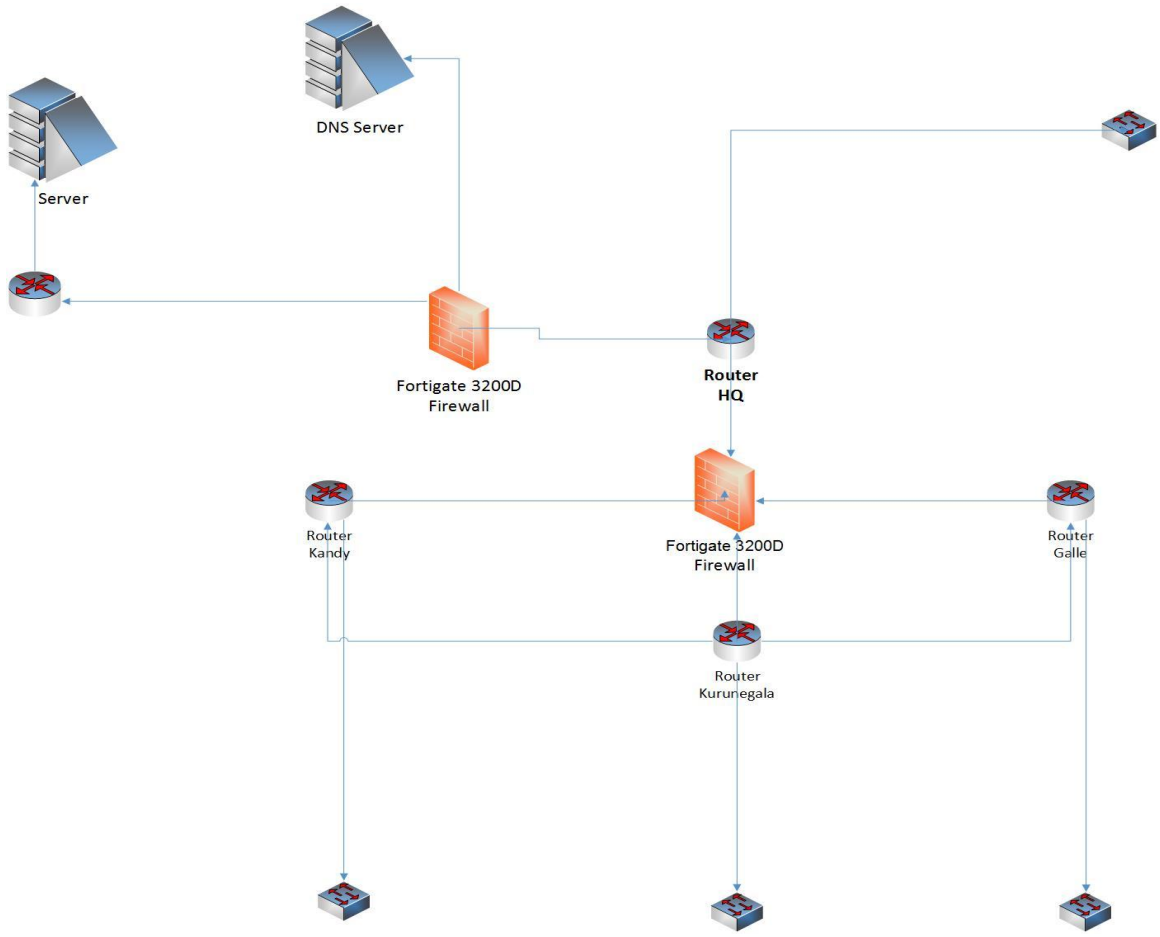
6). Data center protection

Date Center can run any organization while the data center roles are executing takings, saving sensitive data and producing critical services of business. Applications of Business, storage, databases, sensitive data, network devices have internal attacks and external attacks**.** Data centers have inflexible needs for scalability and performances. Also, the latest attacks to protect the security layers against both the known and the unknown threats has become necessary for the business. In addition to their great performance and security requirements of the data center environment require high reliability rigid requirements.

There are some characteristics in data center protection,

- Flexible, unmatched performances.
- Obligate security policies
- Recognize and prevent threats
- Simplify save time and administration
- Up-to-date protection deliver.

Deploying a Next Generation Firewall (NGFW) system, It is better to use to protect the data center of our ABC company. It will ensure the availability and confidentiality because we have placed this firewall in the center of routers connecting to that firewall together and between two routers of Head Quarter. Because data center of the network reduces adherence on a secondary firewall layer and remove it all together while providing protection. Therefore, we decided to place Foritnet Fortigate 3200D as data center protection devices.



6.1). Assumptions

We take this firewall as Network Foundation Protection device and Internet Parameter Protection Device. We have already fix the firewall to our network.

7). Network access security and control

Worms, Viruses and botnets are usually increase by unknowing victims which are connected to the ABC company network. Network access control is to computer security which tries to consolidate end points in ABC company example: - end points of ABC company, are all computers and mobile devices in branches and head quarter.

Network Access Security and Controls Achievements

- Encryption of wireless and wired data.
- Accounting, Authentication and Authorization of network connections.
- Role based controls of user, application and security authentication.
- Automation with tools.
- Enforcement of policy.
- Access and Identity controls.

7.1) Problems in Current Network

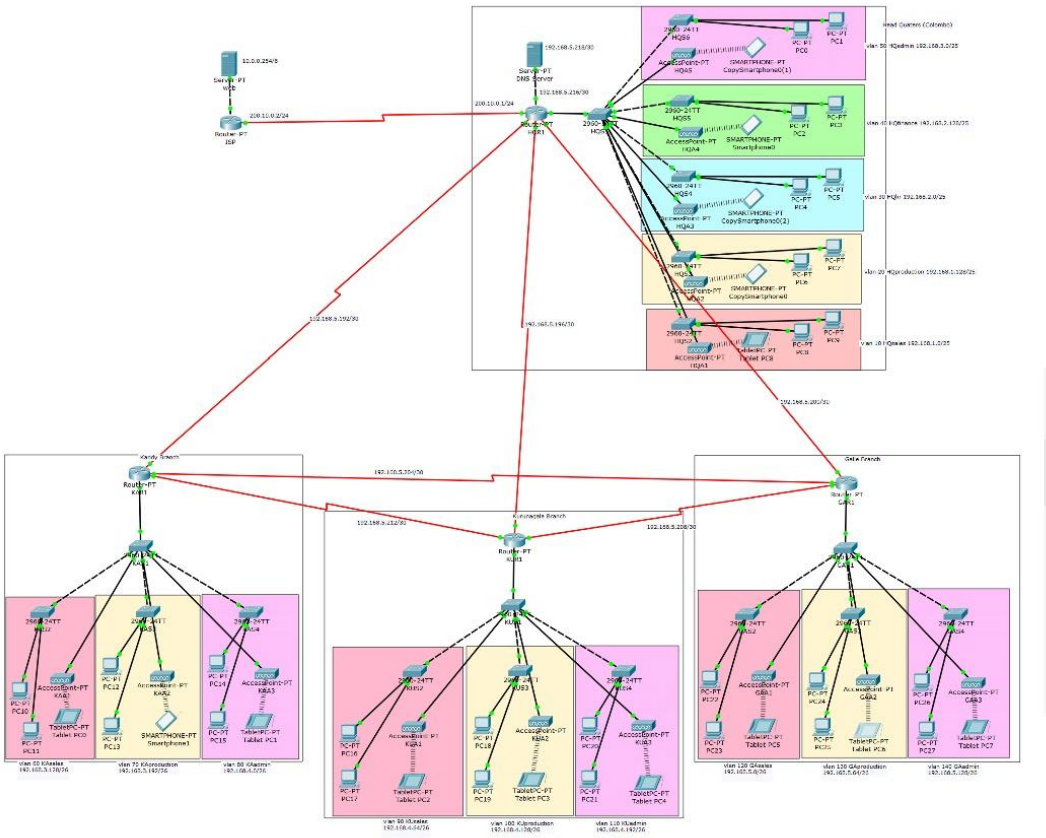
End points machines are slowed by Anti-virus where users of ABC company can disable automatic updates and stop antivirus software scanning. There is no opportunity to prevent users who come from outside to the anti-virus software. VPN access users have the protection where provided by local firewall enforcement. There is no anti-spyware and host intrusion prevention solution deployed.

7.2) Solutions

- Deploy inclusive endpoint solutions which consists anti-spyware, anti-virus and host intrusions prevention capabilities.
- Don’t give permissions to allow disable protections for end users.
- Install personal firewall software to all end users’ computers not only VPN enabled machines.

7.3). Product Evolution Criteria

	Cisco NAC	Microsoft NAC	Juniper NAP
User Authentication	Integrates current infrastructure	Requires MS RADIUS	Requires group Mapping support
Device Posture Assessment	Full Support	Full Support	Full Support
Remediation	Full Support	Very Limited	Full Support
Full OS Support	MS,Mac OSX	Only MS	MS,Mac OSX
Guest Access Portal	Full support	Requires 3rd party	Not temporary logins
Asset Management	Automated	None	Manual



7.4). Assumptions

We selected Cisco Network Access Control Software to install to the all end user's computers, because it has best characteristics other than the Microsoft NAC and Juniper NAC.

8). Secure Mobility

Mobile technology has changed the IT world on how people work, live, play and learn. As the results of that, companies identify that the impact of mobility could be great as which of the website, more website are in trouble with what to do about it. IT managers must guide the transformation on what have to do with mobility. The mobile consumers who works at ABC company, can connected with using APN to ABC company anytime.

8.1). Mobile Device Challenges

- Access policy enforcement on all devices.
- Reduce the resources needed to bring mobile devices on board.
- Delivering a great mobile business experience, even with network-heavy applications, large business customers, Mobile Phones.
- Mitigating security and privacy risks such as the loss of intellectual property, malware and reduce the security and privacy risks.
- Enforcing the right level of data and application security across the spectrum of risk scenarios.
- Simplifying mobility for users and IT.
- Building a flexible mobility infrastructure to meet different work styles and application needs.

8.2). Solutions

- Gives tricks and plans to improve mobile infrastructure of the network, devices which connected to the ABC network, security and mobile application platform.

- Produce services access and manage mobile devices and apps stores. They are reducing risk and complexity of mobile devices using flexible delivery, manage and cloud.

- Intrust set of secure services and softwires when using emails and others through internet.

ARUBA 7000 SERIES MOBILITY CONTROLLER

The Aruba 7200 series Mobility Controller is the next-generation networking platform, optimized for mobile application delivery to ensure the best mobility experience over Wi-Fi. With a new central processor that employs up to eight cores with four threads each, it's like having a total of 32 virtual CPUs. Thus, the 7200 series supports up to 32,000 mobile devices and performs stately firewall policy enforcement at 40 Gbps – plenty of capacity and speed for BYOD and 802.11ac devices.

PERFORMANCE AND CAPACITY				
Features	**7205**	**7210**	**7220**	**7240/7240XM**
Maximum APs (licenses)	256	512	1,024	2,048
Maximum RAPs	256	512	1,024	2,048
Maximum concurrent devices	8,192	16,384	24,576	32,768
VLANs	2,048	4,094	4,094	4,094
Concurrent GRE Tunnels (System BSSIDs)	8,192	8,192	16,384	32,768
Concurrent Tunneled Ports	4,096	8,192	12,288	16,384
Concurrent IPsec sessions	4,096	16,384	24,576	32,768
Concurrent SSL fallback sessions	4,096	8,192	8,192	8,192
Active Firewall Sessions (Concurrent sessions)	1,000,000	2,015,291	2,015,291	2,015,291
Wired Throughput (large packets)	12 Gbps	20 Gbps	40 Gbps	40 Gbps

SonicWALL Mobile ConnectApplication

SonicWALL™ Mobile Connect for OS X is an app for Apple Mac notebooks and desktops running OS X Mavericks (10.9) or newer versions, including macOS Sierra (10.12), that enables secure, mobile connections to private networks protected by SonicWALL security appliances. The SonicWALL Mobile Connect for OS X app provides secure, mobile access to sensitive network resources. Mobile Connect establishes a Secure Socket Layer Virtual Private Network (SSL VPN) connection to private networks that are protected by SonicWALL security appliances. All traffic to and from the private network is securely transmitted over the SSL VPN tunnel.

8.3). Assumption

We have decided to state this mobility controller to branches and Head Quarter. We decide to fix this Aruba 7000 series Mobile controller instead of access points of branches and HQ because the mobiles are connected to the ABC company network through access points. Also, we decided to install the SonicWALL mobile connect application for mobile devices which are going to connect with ABC company network.

9). References

Aruba, a Hewlett Packard Enterprise company. N.p., 2017. Web. 8 May 2017.

"Cisco - Global Home Page". *Cisco*. N.p., 2017. Web. 8 May 2017.

"Documents". *Sonicwall.com*. N.p., 2017. Web. 8 May 2017.

"Fortinet". *Fortinet*. N.p., 2017. Web. 8 May 2017.

"Industry-Leading Cyber Security Solutions For Networks, Data Centers, Mobile Devices & Endpoints | Check Point Software". *Check Point Software*. N.p., 2017. Web. 8 May 2017.

"Mcafee - Antivirus, Endpoint Security, Encryption, Firewall, Email Security, Web Security, Network Security". *Mcafee.com*. N.p., 2017. Web. 8 May 2017.

"Separation Of Control Plane And Data Plane In Performance Networks". *Daniel Kleviansky | Part of the Human Network*. N.p., 2017. Web. 8 May 2017.

Services, Products et al. "Cisco Firepower 8000 Series Appliances Data Sheet". *Cisco*. N.p., 2017. Web. 8 May 2017.

Support, Product, Cisco Appliances, and Configuration TechNotes. "Configuration Of Stack On The Cisco Firepower 8000 Series Devices". *Cisco*. N.p., 2017. Web. 8 May 2017.

Zeltser, Lenny et al. "Perimeter Security Fundamentals | Terms Of The Trade | Informit". *Informit.com*. N.p., 2017. Web. 8 May 2017.