M.Ahsan Habib

REDESIGN ENTERPRISE NETWORK BY LOCAL INTERNET BREAKOUT: CASE STUDY

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2015

ABSTRACT

Habib, M.ahsan
Redesign Enterprise Network by local Internet Breakout: Case Studies
Jyväskylä: University of Jyväskylä, 2015, 60 p.
Information Systems Science, Master's Thesis
Supervisor: Ristaniemi, Tapani

Nowadays, the popularity of cloud-based services around the web and SaaS applications are empowering customers to improve their business processes and increase user productivity while reducing the company's IT operation costs. The local Internet breakout solution provides improved performance when accessing cloud-based applications along with a greater user experience. The reason behind this is not having data travel through the corporate WAN to access the Internet at a single point. This new network design solution not only improves user experience by lower latency when accessing the Internet, but also offloading the applications traffic from corporate WAN connections.

The main theme of this study was to experiment how local could Internet breakout can help a corporation improve network performance, save bandwidth on corporate WAN link and to improve the end-user experience. Another area of interest is how to implement this Internet breakout on to the current corporate network. After discussing network performance importance for the corporation, this thesis concentrates on improving corporate network performance. Local Internet breakout is presented as a possible solution and how it could be implemented on the current corporate network. The different vendors' solutions are discussed to give the reader a general overview of their solution and how those solutions can be implemented to the current corporate network.

For testing purposes, three vendors' devices are deployed for this case study work. The tests are performed in eight different locations around the globe on the current corporate network. The aim of this experiment is to provide a proof of concept for Internet breakout on the target company's network.

Keywords: Wide Area Network, internet breakout, performance, Local Area Network

TIIVISTELMÄ

Habib, M.ahsan
Redesign Enterprise Network by local Internet Breakout: Case Studies
Jyväskylä: Jyväskylän yliopisto, 2015, 60 p.
Tietojärjestelmätiede, pro gradu-tutkielma
Ohjaaja: Ristaniemi, Tapani

Näinä päivinä on yleistä että yritykset käyttää pilvipalveluita ja SaaS sovelluksia parantamaan liiketoimintaa ja vähentämään yrityksen IT-toiminnan kustannuksia. Paikallinen internet Breakout-ratkaisu tarjoaa parempaa verkon suorituskykyä, jolloin internet-palveluiden käyttökokemus on parempi. Syy tähän on se, ettei verkkoliikenne kulje yrityksen WAN-verkossa käyttäessä internettiä. Tämä uusittu verkkoratkaisu ei pelkästään tarjoa parempia käyttäjäkokemuksia alemmalla latenssilla käyttäessä internettiä, vaan sen lisäksi purkaa sovellusliikennettä yritysten WAN-verkossa.

Tämän tutkimuksen tärkein tavoite oli kokeilla miten paikallinen Breakout-ratkaisu voisi auttaa yrityksiä parantamaan verkon suorituskykyä, säästämään kaistanleveyttä WAN-verkossa ja parantamaan loppukäyttäjän kokemusta. Oli kiinnostavaa nähdä, miten tämä toteutuu yritysten verkossa. Koska tutkimuksessa selvisi verkon suorituskyvyn merkitys yritykselle, opinnäytetyö keskittyy antamaan keinoja yrityksen verkon suorituskyvyn parantamiseen. Paikallinen internet ratkaisu on esitetty mahdollisena ratkaisuna ja kuinka ratkaisu voidaan toteuttaa yrityksen verkossa. Tässä tutkimuksessa käy ilmi minkälaisia erilaisia valmistajien ratkaisuja on olemassa, ja kuinka näitä ratkaisuja voidaan toteuttaa kohde yrityksessä.

Testausta varten on valittu kolmen eri valmistajan tuotteet. Testit tehdään kahdeksassa paikassa eri puolella maailmaa. Tämän tutkimuksen tarkoitus on todistaa että internet Breakout-ratkaisu toimii kohdeyrityksessä.

Hakusanat: Alueverkko, TCP, suotiyuskyky

ACKNOWLEDGEMENTS

I do like to express my sincere thanks to my supervisor Tapani Ristaniemi, for guidance and significant suggestions during the whole process of my thesis work. I also will show my great acknowledment to my family in Finland and dear parents in Bangladesh. During living here in Finland, I can strongly feel their love, support and encouragement every moment, even though I am far away from them. I love and miss them so much !

17th of May 2015

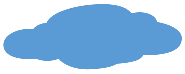
M.Ahsan Habib

FIGURES

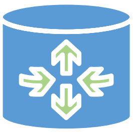
TABLES

TABLE OF CONTENTS

SYMBOLS



Network (wide area network) cloud



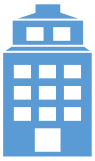
Router

Juniper SRX

FortiGate

Aruba Controller

Aruba remote access point



Satellite office

Hub office

Datacenter

🖥	Computer
- - - - - - -	IPSec connection
————	MPLS connection
————	Internet connection

ABBREVIATIONS

BGP	Border Gateway Protocol
CAD/CAM	Computer-aided Design and Computer-aided Manfacturing
CIFS	Common Internet File System
CoS	Class of Service
CRM	Customer Relationship Management
DSL	Digital Subscriber Line
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IPSec	Internet Protocol Security
LAN	Local Area Network
LTE	Long-Term Evolution
MPLS	Multi-Protocol Label Switching
OSPF	Open Shortest Path Fast
P2P	Peer to Peer
QoS	Quality of Service
RIP	Routing Information Protocol
SaaS	Software as a Service
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
VoIP	Voice over IP
VPN	Virtual Private Network
WAFS	Wide Area File Services
WAN	Wide Area Network
WLAN	Wireless Local Area Network

TERMS

Ethernet – Ethernet is a reliable, efficient and most widely implemented local area network (LAN) technology. It became popular in LAN technology because of its some key characteristics such as easy to manage, deploy, maintain and not difficult to understand (Cisco, 2013).

Local Area Network – LAN provides data networking capability within limited geographical area such as office building, computer laboratory, home etc. Data-transfer rate is very high in LAN network. In LAN network, connected device can share file, printer, internet connection and other devices (Cisco, 2012).

Packet – Packet is a unit of data that transmitted over a packet switched network. One of major features of packet is that it contains information about sender IP information and destination IP information, and actual message from user. Every user message or file divides into "chunks" of small size of packet and generally, each packet contains around 1000 or 1500 bytes of information for routing. The packet used Transmission Control protocol/ Internet protocol (TCP/IP) when transferring data (HowStuffWorks.com, 2000).

Transmission Control Protocol – TCP is enables between computers to establish a connection and sends unstructured stream of bytes data. TCP use sequence number and received acknowledgement mechanism message. It assurance delivery of data and also guarantees that that all packets will be sent in the similar manner in which order they were delivered. TCP can also identify identical massage and able to drop them correctly. TCP has a feature where it can balance between sender data transfer rate to receiver data transfer rate. If the sender computer sending data in high speed which is fast for the receiver computer, TCP can use it flow control mechanism to slow down data transfer (Cisco, 2005).

Multi Protocol Label Switching – The core concept of MPLS is labeling packets. When packet arrives in a network for the first time, it attached a label to the packet. Each router in the network has own rules of table how to handle of a specific label packet. Once the packet has labeled, routers on the network do not need to examine anymore. This help MPLS network the ability to handle real-time traffic and reduce latency, for example, voice, live streaming video etc (Johnson, 2007).

Wide Area Network – WAN is a collection of computers and network that connected together through network over broad geographic area. For example, network between two or more metropolitan areas, different countries, regions or even the world. It is similar to LAN network, but it is a lot larger. There are several options for WAN connectivity such as leased line, circuit switching, packet switching (Cisco, 2012).

Internet Protocol Security – IPSec is a set of protocols to support securely send and receive data at the internet protocol layer. In today's network, it used to protecting exchange of data between hosts, between networks or between host and network. IPSec has been used widely to implement Virtual private network. To protect data between hosts over IP network, IPSec uses cryptographic security mechanism. IPsec enable features like peer authentication in network level, data origin authentication, data integrity, data encryption and replay protection (Wikipedia.org, 2015).

Virtual Private Network – VPN is a communication network that is built by using public network infrastructure, which is typically the internet to connect branch remote office or isolate employees with secure encrypted connection to corporate network. VPN uses encryption and many other security methods to make sure that only authorized persons can access and information cannot be captured. A VPN can be built with an costly leased lines, which can only used by one company. Here main aim of a virtual private network is to deliver the company with similar capability with less cost (Rouse, 2007).

1 INTRODUCTION

Enterprise network infrastructure has worked as a carrier on which data and information can be transferred between functional units regardless of their global location. Now a days new technologies, new ways of workings and interacting, either via social networking or bring your own device are requesting more and more of the network infrastructure. These new ways of doing business, new possibilities using VoIP, videoconference or simple video 1-on-1 are suggested and demanded by the business. If companies keep the current infrastructure set up, all these lead to a cost increase and to a degradation of performance.

Enterprise network are being called upon to manage risk, improve productivity, enhance the customer's experience, improve network availability and manage growth and change. Further challenged by budget limitations, and demand for security and flawless operation, network professional are being tested like never before.

1.1 Motivation and goal of the research

As the size of enterprise becomes bigger and bigger, the branch offices of the company spread all over the globe and the enterprise also increasingly enhances the request for security transmission of data. With the traditional network mode, that private links based on fixed location are set up to connect to each other, and are already difficult to adapt the demand of enterprise for modern management traffic. So, many enterprises and equipment which make use of the new network technique and equipment set up the network between the headquarters and branch offices to interconnect in order to construct a safe network.

The target company considered in this thesis has different levels of offices which include the datacenter, factory, branch office, country head office, service center, maintenance center and regional office (discussed in chapter 3). Company offices construct enterprise networks across different regions, such as paying for expensive MPLS and IPsec connections. This was fine with all the applications and the data resided in centrally located datacenters owned and run by the enterprise. However, there have been growing complaints for the past ten years on internet performance with the entire external datacenter, especially cloud services, and the problem is becoming unbearable.

With the company current situation, they have MPLS and IPsec connections between different kinds of offices in their organization to data centers and there is no internet breakout in between office and datacenter. All network traffic travels via the central place, which increases the latency to access some services from the internet. And now, more and more offices are added to the network and the numbers of MPLS connections are growing all the time which is very expensive for the company and also for future demand. Company need to increase the bandwidth, which will also be very expensive for them. The Company also examined that their internet traffic is 70% and only 30% traffic is accessing critical applications which are hosted in corporate datacenter. So if they can have local internet breakout, then the company users will have direct access to internet and cloud applications which will decreases the latency and user can experience better performance. In addition, the business can reduce costs by MPLS connections offloading. Furthermore, the company wants to give the user more flexibility in the office by implementing WLAN in all offices. If the company implement Wi-Fi enabled offices, there will be fewer cables which will enable a flexible office moving process and also will bring less troubleshooting problems.

For the above reasons, a Proof of Concept (POC) is being initiated to evaluate specifically how the target company can tackle the new challenges and achieve the goals of cost reduction, improving performance and services.

1.2 Research question

The aim of the following research questions is to help in defining the problem that will be discussed chapter 2 in this thesis. These questions are:

- Why is network performance important for corporations?
- What are the factors affecting network performance?

This thesis has one main research question. The main research question in this thesis is related to the corporate network architecture. Chapter 3 studied first the target company network architecture and then in practice in chapter 6. The main research question is:

- How could local internet breakout help corporations to improve network performance?

An important part of this thesis is to introduce solutions for improving end-user experience, save bandwidth and implement new solutions. As already discussed local internet breakout is the main solution studied in this thesis. This can be done by answering the following subsequent questions:

- How much bandwidth can company save?
- How does it improve the end user experience?
- How easy is it to implement new solutions?
- Does one solutions suit for every location?
- Which locations do we deploy to first?
- How can local internet breakout be implemented to the network?

1.3 Method of the study

The method of the study will be design science methodology. First, starting with identifying the current problem in the target company, and then developing a new solution based on their requirements. After developing the new solution, we need to validate with requirements and implement the solution in real environment to test, and finally evaluate the results. In this case, the researcher has been actively involved in the development of the case project.

1.4 Structure of the thesis

In chapter 2 enterprise wide area network (WAN) in general as well as network technology is discussed. Factors affecting network performance are studied. The chapter concentrates also on future traffic growth. In the following chapter 3, the special focus is target company current network architecture and what kinds of technology solution they use. The expectation of the Proof of Concept (POC) project and business requirement analysis is explained in chapter 4. Chapter 5 introduces the reader to different vendors and their solutions as well as discussed how their technology solutions fit in the target company environment based on their characteristics. Chapter 6 is the empirical part of the work. It is case studies for implementing local internet breakout into corporate networks for testing purpose. First new network design for test locations are described. After that the test plan and the result of the tests are discussed. Finally, in chapter 7, the implication of the study as well as its limitations is discussed.

2 ENTEPRISE-WIDE NETWORK AS TODAY

There is no doubt that in today's globalized modern world, networks form the backbone of an organization. This network consists of important hardware equipment such as router, switches, hubs, gateways, firewalls and servers from different companies. Business continues directly relays on the network availability and its performance. Even few minutes of network breakdown or few seconds of latency issue could have direct impact on the revenue as critical business services and communication get affected. As large organization expends their business in different locations, their network also became larger. Network administrator are continually challenged to make sure the network is always up and running to support business demand (Rao & U.H 2010).

2.1 Characteristic of Enterprise WAN

An enterprise WAN is a corporate network that links multiple locations isolated users areas that could be anywhere in the globe. An enterprise Wide area network connects local area networks in many different locations. Typical enterprise owns the network hardware devices within the LANs. On the other hand, the LANs are usually connected by a service provider (Rouse, 2012).

From a global enterprise network perspective, enterprises mainly have three different types of offices. Those are branch offices, regional head offices and the datacenter. Most of the organizations choose to have their work staff members near to the customer to support better customer service, and for that reason small remote offices increase within one organization. All offices in one organization connect with each other through the corporate WAN. Branch offices that are located different geographical locations are connected through lower bandwidth and high latency to the corporate network. Because of that, those small branch office users experience poor performance when accessing the Internet and corporate applications which are hosted in the datacenter (Taneja, 2005).

Figure 1 illustration shows an example of a typical enterprise network can be constructed from the WAN and LAN. Enterprise WAN includes of service provider backbone and the point-to-point links between the service provider network and different location building LANs. Service provider routes separated all of those locations from each other.

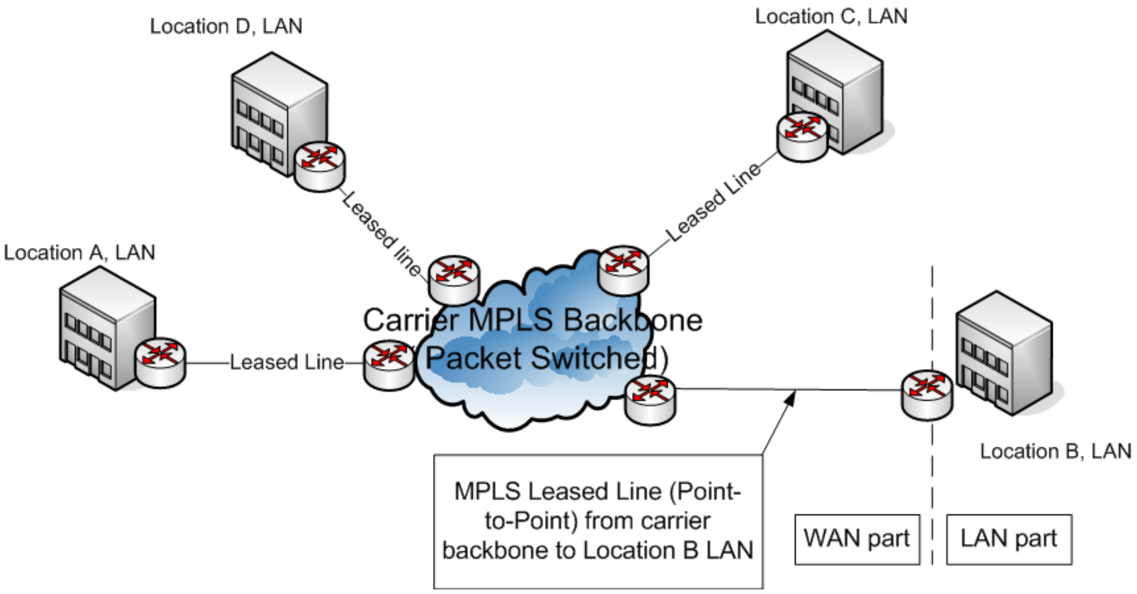


Figure 1. An Illustration of a Corporate Network. The Wide Area Network Include of the Service Provider Network and the Leased Line Connections Between the Different Office Locations (Cisco, 2012)

2.2 Network Performance

Companies have been investing money into cloud-based applications, but they have unable to require changes need to network architecture to delivery better performance and user experience. In (Herndon, VA 2013) Forrester study, which they conducted 154 companies, showed that network upgrades and refreshes were ranked 6th for IT organizations over last three years, in addition only 47 percent of organizations think about investments in their corporate network and 33 percent mentioned that they evaluate their WAN service. The most common investment enterprise made to improve network performance to add more bandwidth to their WAN links. Whether companies depends on point-to-point WAN architecture or a MPLS cloud, most of the organization route all their web based traffic such as browsing internet, cloud based services, email through datacenter. Due to this services the branch offices users have experienced lower application performance. In (Murphy, 2014) Matth Murphy state that faster application performance will distinguish the winners in this competitive enterprise market. There have been studies done by Walmart and Compuware indicate that one second of latency improvement in application delivery can increase revenue by 10%.The large amount of small offices and at the same time, the centralization of servers into datacenter has made the network a critical point for the organizations.

2.3 Network Bandwidth

The amount of data that can be transmitted in a fixed amount time usually second(bps) from one end to another end. Network bandwidth commonly mentioned bits per seconds. Network bandwidth usually measured megabits per second(Mbps) or gigabits per second(Gbps). Network performance can be effect by many other factors bandwidth is one those factor. There is also packet loss, latency and jitter, all of those responsible for downgrade network throughput and make a connection perform like one with lower bandwidth. Not all application requires similar bandwidth. For example, a voice conversation might take one thousand bits per seconds or a messaging exchange needs fifty kilobits (Rouse).

2.4 Delays in Transmission

From source end to destination end how long it take to move a packet usually determine delays in transmission which is performance measures of a data network. It is key performance measurements in data network. In addition to that, delay in communication has great influence on performance of network routing and flow control. There are many reasons that causes to the end to end delay in the transmission of data in the network and those reasons discussed followings sections (Wikipedia.org, 2014).

2.4.1 Processing Delay

Processing delay (Figure 2) is a necessary time needed by a router to access and analyze a packet header and able to make decision how to handle that packet or where to send that packet and it also verification any bits of error in the packets, which can take place during transmission of a packet. Processing delay is one of main component in data network. Processing delay subjects to amount of records in the routing table, data structure implementation and performance of hardware etc. Sometimes processing delay can take lots of time, if the router is processing large or complex encryption and decryption algorithms and analysis or changing packet header information (Bertsekas & Gallager, 1992).

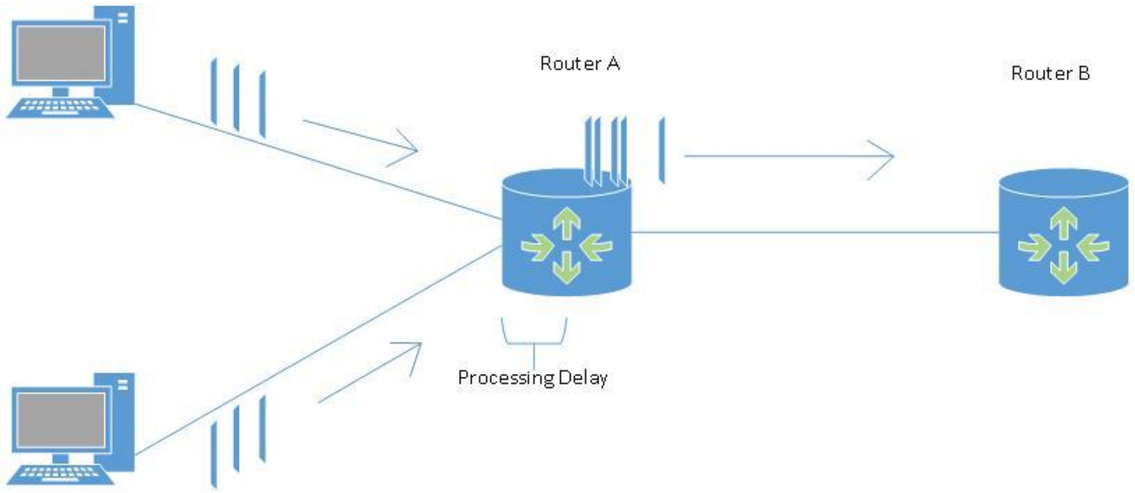


Figure 2. Processing Delay

2.4.2 Queueing Delay

After initial packet processing by router, it sends the packet to the queue that precedes the connection to the following router. Queuing delay (Figure 3) is the time a packet has to wait before transmission starts. Packets are position in the queue when packets come to router quicker than it can analyze them, so it puts them into waiting list until router can starts transmitting those packets. Packet queuing waiting list depends on quantity of packet and packet quality. Queuing delay become high when the queue of packet is longer, however if there is not packet is queue, then queuing delay is zero. Queueing of packet in router also introduce packet drop, because router has limited number of buffer memory, so when router buffer memory became full with queuing packet of data, it has no choice than start to dropping packets (Bertsekas & Gallager, 1992).

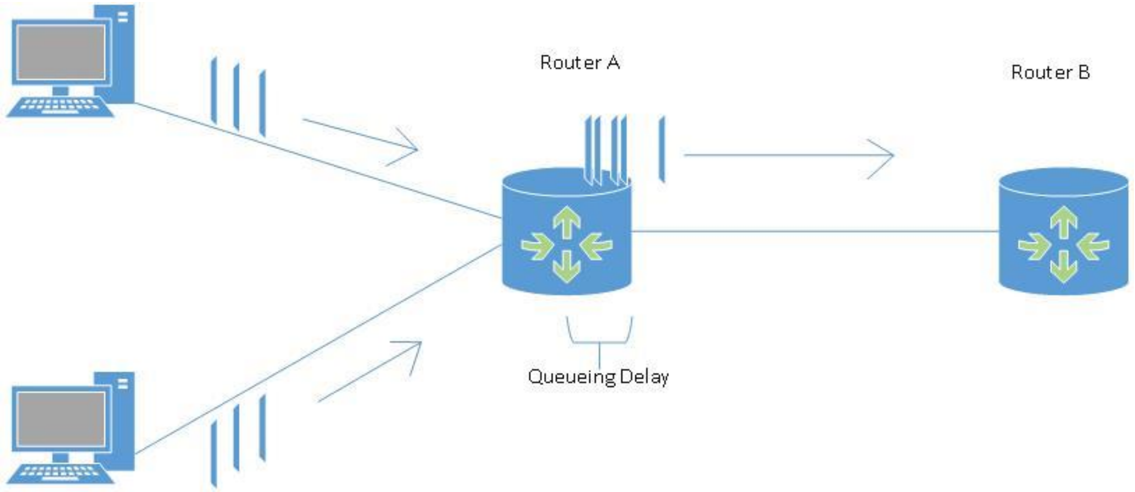


Figure 3. Queueing Delay

2.4.3 Transmission Delay

It is the time required to send out entire packet into a link to data network (Figure 4). The data rate of the connection caused for transmission delay. Transmission delay depends how long the packet is but it does not affect far between sender and receiver machine are. e.g. if a packet size is 10kbps and connection speed is 1Mbps. Then the transmission delay would be 10Kbps/1Mbps and that is .01 second (Bertsekas & Gallager, 1992).

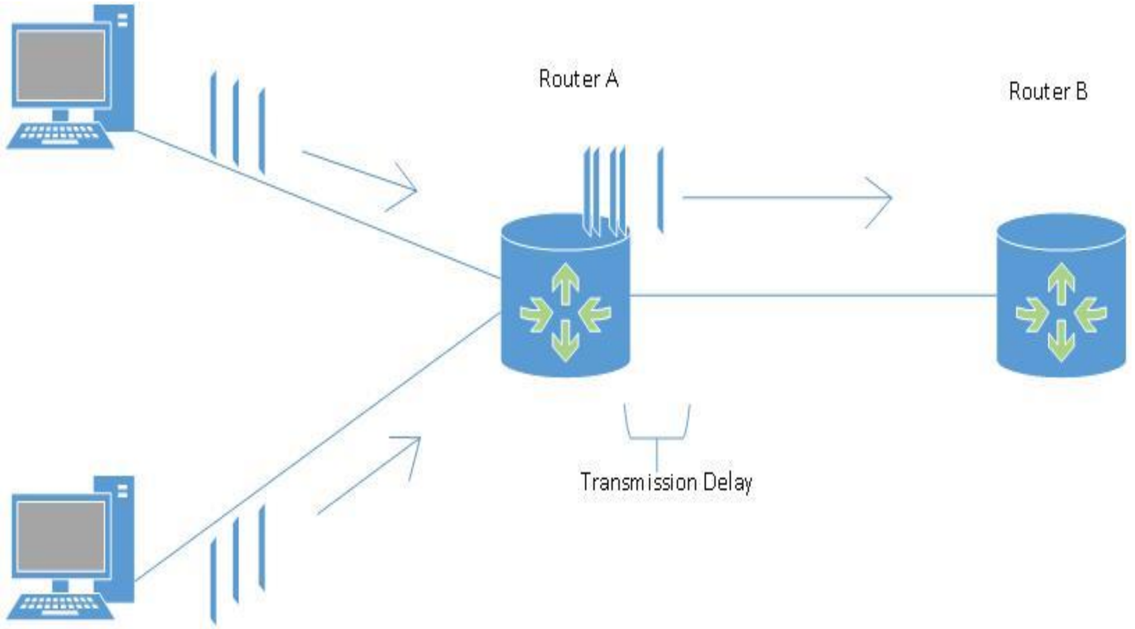


Figure 4. Transmission Delay

2.4.4 Propagation Delay

Propagation delay (Figure 5) is, how long time it takes to transmit first bit of the packet from its source router to destination router. It can be measured by calculation distance between source and destination routers and the speed of propagation of the line (Bertsekas & Gallager, 1992). e.g. if distance between source and destination router is D and speed of propagation is S. so the propagation delay P is defined as

$$P = D/S$$

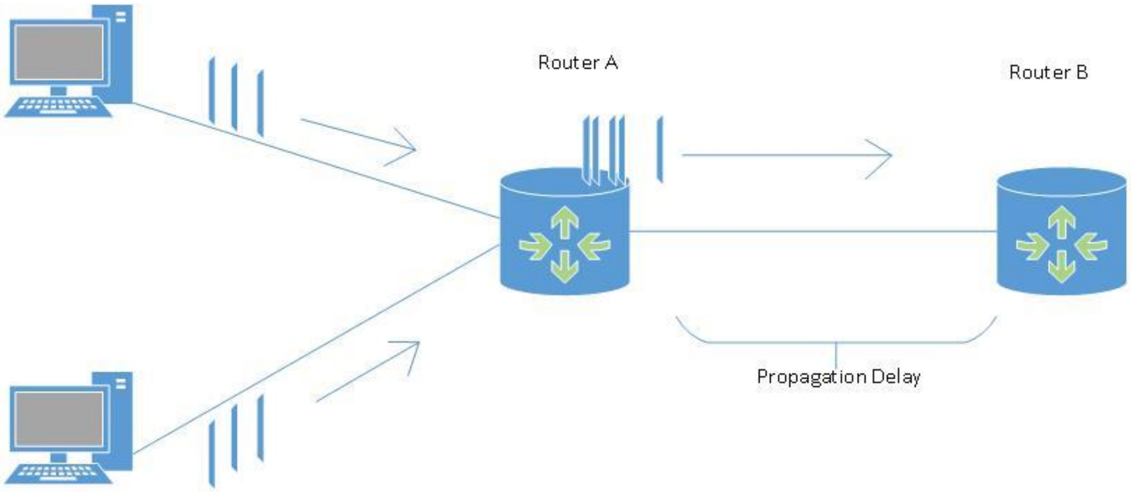


Figure 5. Propagation Delay

2.5 Traffic Growth

The increase popularity of cloud based applications, social media, real-time application and multimedia applications services on the internet have driven a high traffic growth. In large enterprise, users are increasingly located in branch offices. From 2005 to 2009, the amount of branch offices increased an average of 9.2 percent every year. As branch offices and remote workers get services from centralized datacenter that means about 90 percent users get their applications delivery through corporate WAN (Johnson, 2010). In (Cisco, 2014) cisco predicts that business IP traffic will increase at a CAGR of 18 percent between 2013 and 2018. The rise of real-time application such as video communication adoption could double that number. In addition, organization IP WAN will grow at a CAGR of 10 percent. However, total business internet traffic will grow faster pace than IP WAN compare with a CAGR of 18% for fixed business internet and 55 % for mobile internet.

2.6 Use of external expertise

Many organizations are reducing the workload of managing and troubleshooting their network through co-operation with 3rd party managed services provider (MSPs). MSPs consist of service providers, outsource companies, resellers, system integrators and some case it could be vendors. There has been incredible demand in the number of companies outsource their IT infrastructure to MSPs. In 2005, 27 percent of companies mentioned that they are using MSPs to help them to manage their branch offices and remote location offices. In 2006, that number had increased to 46 percent (Gareiss, 2009).

Some organizations entirely outsource the IT management of remote offices and branch offices, on the other hand some organization partner with the MSP. For instance, they may have the MSP take care of all implementation, level 1 support issue, and internal organization taking care of training, level 2 and level 3 supports.

Still, many other organizations have the internal expertise team to manage and troubleshooting their corporate network using only internal resources. Usually organizations invest money to buy and implement several management and monitoring tools for operate and support different applications, hardware devices, and Corporate WAN infrastructure (Gareiss, 2009).

3 TARGET COMPANY CURRENT NETWORK SOLUTION

Target company, as many as other international companies are facing the similar challenges, growing exotic markets, more demanding utilization and availability of information. Among other reasons, push us to re-think the company network infrastructure. The traditional approach to network is questioned on a daily basis. The competitiveness in all market segments is a reality driving them to provide added-value solutions and support to their business. The next couple of sections will provide a high-level overview information about the company network architecture.

3.1 High –level architecture

The existing architecture was founded in the business need for service and availability of the network. Different office locations have different needs regarding information access and service. As example a call center have different needs then a branch office. More information can be found in Appendix 1.

The target company has subcontract its network operations and move to more centralized network architecture. Decision being centralization has come from business need and it discussed below in section 3.2.1. It is important for the company to be near to the customers to support their needs and that is leads to increase number small remote offices. The service provider provided WAN, LAN and Voice services to the company users. WAN services are enhanced VPN Services and IPsec. A global enhanced virtual private WAN network, connecting the company offices in EMEA, the Americas and Asia pacific. They also provided internet service in different region datacenters. LAN Services are WAN accelerator services, DHCP appliance, ACS radius server for WiFi access and LAN switches on all the company offices. Voice over IP (VoIP) and teleconference service (Audio conference) are the Voice services provided by the service provider.

Figure 2 below gives an overview of all WAN services and office connections types in the company.

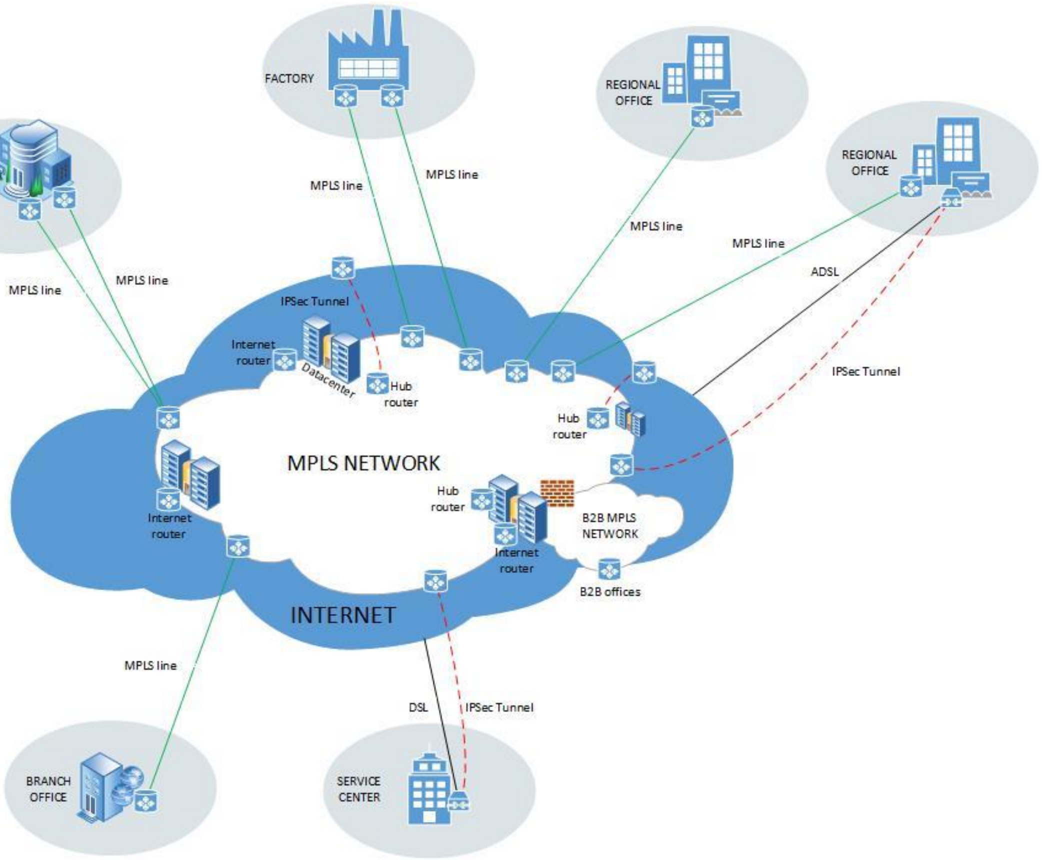


Figure 6. Target Company WAN Network Overview and Different WAN Services

Currently, office criticality levels are based on business criticality and have specific aspects of WAN network connectivity. More information on the office Level description in Appendix 1.

3.2 Datacenter and internet connectivity

Following couple of sections, we will discuss about target company different datacenters location and internet connectivity. In addition to that how they are connected to corporate network.

3.2.1 Datacenters

The company has started a program to centralize application landscape a couple of years ago. This program is not yet over but most of their applications are hosted in datacenters. Company has corporate and regional datacenters. Corporate datacenter are located different locations in Europe and Asia. Each of these datacenters is composed of two separated locations (half-DC) interconnected via fiber and sharing VLANs across both half-DCs. Each half-DC has its own network connectivity to the corporate WAN and internet. The Company has different regional datacenters as well.

3.2.2 Internet Connectivity

Company's current model is only considering a few internet breakouts. This is mainly inherited from the perimeter security model the company use. Each internet breakout is protected by a firewall and all outgoing connections are proxied (Proxy + proxy AV). One European country DC provide internet breakout for EMEA area, USA DC provide three countries internet breakout northern and Central America. China and Australia used Singapore DC and Egypt DC to access internet, another European country DC provide act as Nordics countries internet breakout.

3.3 Hardware assets overview

The company network hardware divided in three main categories and those are WAN router, WAN accelerators and LAN switches.

WAN routers are owned by the WAN service provider and are directly linked to the WAN circuit. The company doesn't have to take care of the lifecycle of this equipment. These WAN devices are mainly of three types:

a. Router that can be connected to a MPLS type circuit.
b. Router used as IPSec termination point (used to build a tunnel with a central IPSec termination point hosted in the datacenter)
c. Proprietary LAN switch/router/IPSec platform from the WAN service provider. This platform provides IPSec connectivity to an entry point in to the MPLS backbone and can act as local.

The company has just started together with current WAN service provider a program to deploy WAN accelerators. They have so far installed appliances in their major DC locations and some key branch office locations.

3.4 Business critical applications

The company network traffic use of the WAN backbone can be divided into following two categories, first is those traffic which remains inside corporate network that is 30% of traffic and second is those traffic which ends on the internet that is 70% of traffic.

The corporate applications are hosted in the datacenter and they are the following:

a. SAP
b. Video conference
c. CAD document management platform
d. VoIP
e. Field mobility systems
f. Planning tool
g. Exchange
h. SharePoint
i. Fileshares

The traffic ending on the internet can be divided into:

a. Browsing
b. External email
c. SaaS (Mainly Salesforce.com)

3.5 Quality of service (QoS)

The company applications network performance requirements are not homogeneous, thus corresponding traffic flows has to be classified and prioritized accordingly. Currently such mechanisms are in place on all WAN links.

WAN QoS control is performed on CE-routers, where traffic priority requirements are discovered with a globally harmonized IP policy-map. WAN policy-map assigns applicable QoS class by analyzing forwarded packet's destination and source IP addresses. Once the analyzed packet is assigned to the correct priority queue, related quality control characteristics are used to achieve needed per hop behaviors and subsequent application performance levels.

Above mentioned in section 3.1 network quality analysis and enforcement actions are implemented and performed by the company WAN service provider.

3.6 Site classification and capacity management guidelines

The company office levels are based on business criticality and have specific aspects of WAN network connectivity. Appendix 1 provides more information about office classification and capacity management guideline.

3.7 Network monitoring platforms

The company network operations are outsourced to multiple managed services partners. Each partner has their own technology domain related fault management and performance monitoring solution for their reactive and capacity management purposes.

Current mainstream the company in-house network monitoring tools are Cacti and NetFlow Tracker. Cacti are monitoring WAN-link utilizations and possible interface errors. Information is collected from CE-routers. NetFlow Tracker illustrates detailed NetFlow information and is typically used to identify reasons behind WAN-link congestion on an individual user and/or application basis.

4 GLOBAL SOLUTION STRATEGIES

4.1 Expectation from this POC

As discussed in section 3.3, the company offices are connected through MPLS and IPsec connection. Currently, the company has few entry points to the Internet. Since more and more branch offices, remote locations are connected to corporate network, the company costs keep growing at a high pace. This cost growth added to their applications performance challenges force them to rethink the way they do networking today. Approximately 70% of company's traffic can be considered non-critical, leaving the remaining 30% in need for closer attention.

The company expectation from this Proof of Concept is to have tested successfully the new network architecture solution. They believes a mashed network will suite their current needs and put them in an edge position for the next 5 to 10 years for increase performance, increase service and keep costs down.

4.2 Network architecture consideration

Future network design is expected to loosen the current data center centric star-topology architecture. Reference architecture is seen to be driven by following areas:

a. Performance: Internet break-outs moving from data centers towards remote sites.
b. Security: Data center level security mechanisms have to be maintained on the distributed architecture.
c. Financials: Affordable and easily deployable small site connectivity and security appliances.

d. Management: Efficient centralized solution management and monitoring capability.

Above-mentioned four key drivers have all their respective influence to the optimum architectural design fundamentals.

4.3 Business requirements

The company has different functionality in different offices (more information Appendix 1). But from a network point of view there are some common requirements which can be found all types of office levels. Those requirements are as follows:

4.3.1 Security

a. Corporate network must be protected against internet treat and certain level of control what user can access in internet and those different functionality can be integrating in same device or separately.
b. All firewall must manageable from a central management system.
c. Proxy policies must be centrally managed but should accommodate local regulation. For example, china has different types of policies to access internet.

4.3.2 Application performance

a. User must experience same or better latency as it is now, when they will access corporate applications, which are in corporate datacenter. Thanks for offloading (internet, email etc.) traffic from corporate MPLS network.
b. Latency reduces and user will have better experience when they access to internet and any other cloud based applications, thanks to the local internet breakout.

4.3.3 Application management and monitoring

a. The future solution should include a management platform or integrate with current management system.
b. The future solution should provide at least same level of visibility (monitoring) as it is now and more.

4.3.4 End-user experience

a. Simplify data path to improve end user experience.
b. Guest/contractor access must be provided (internet only).
c. User/visitor should able to bring their devices and at least get internet access.
d. Wi-Fi enables office, so that users are able to move frequently in their office and still connected to the network.
e. Wired and wireless network must be combined to get unified experience.
f. Users are able to use VoIP softphone in their machine via wireless network.

4.4 Centralized networking management and monitoring

Proposed network solution must include relevant network management (OSS) tool-set. OSS should have the function to facilitate provisioning, operation, administration, maintenance, and control of all the network elements. Such functions should be accessible at minimum from all corporate locations, but various cloud-based OSS extensions can be considered as well.

Critical OSS core elements can be placed into a preferred target company data centers, but possible needed sub-systems may be distributed to other centers or as mentioned above, to cloud as well.

5 DIFFERENT VENDOR SOLUTIONS

The target company has received a solution proposal from five different vendors. After the preliminary analysis, the company decided to test three different vendor solutions. Those three vendors were Juniper Networks, Fortinet and Aruba networks. Below we will delve into more detail of those vendors' solutions.

5.1 Juniper network

The Juniper networks SRX series is an all-in-one device solution providing consolidated network and security. The SRX series for the branch runs Junos OS, which is used by the top 100 service providers around the globe and is a very reliable and proven operating system. The SRX series devices can be managed by the easy unified management system. Figure 7 shown Juniper STRM series security threat response managers system. The Junos single OS platform for all SRX can help businesses reduce time and effort to plan, deploy and manage. It also provides stable delivery of new functionality in a steady time manner. The Juniper Networks' Network and Security Manager (NSM) is very useful for large-scale deployment. (Juniper Network, Inc., 2014).

Figure 7. Juniper STRM Series Security Threat Response Managers System (Juniper, 2009)

5.1.1 SRX Features and Benefits

The Juniper SRX series is a feature rich appliance. It is a fast, highly available switching, routing, security, and applications control capability in a single device. Figure 8 shown Juniper SRX series UTM device. Some of the features are as follows:

a. Security: The SRX appliance has a firewall, police based VPN, IPS, AppSecure, antivirus, enhanced web filtering and antispam capabilities in one product.
b. Routing and switching: Routing features such as RIP, OSPF, BGP, Multicast, IP4 and IP6 are included. There is also J flow, RPM, Layer 2 switching and OPE options available.
c. Wireless LAN and 3G/4G WAN: To support the business user's needs, there are wireless LAN and 3G/4G WiMax and LTE features available.
d. Physical interface: Ethernet, serial port, T1/E1, DS3/E3, xDSL are all available options for WAN or Internet connectivity to securely connect to the corporate network.
e. Managing network: It is possible to manage the corporate network using a command- line interface, scripting capability and also with a web based graphical user interface (Juniper Network, Inc., 2014).

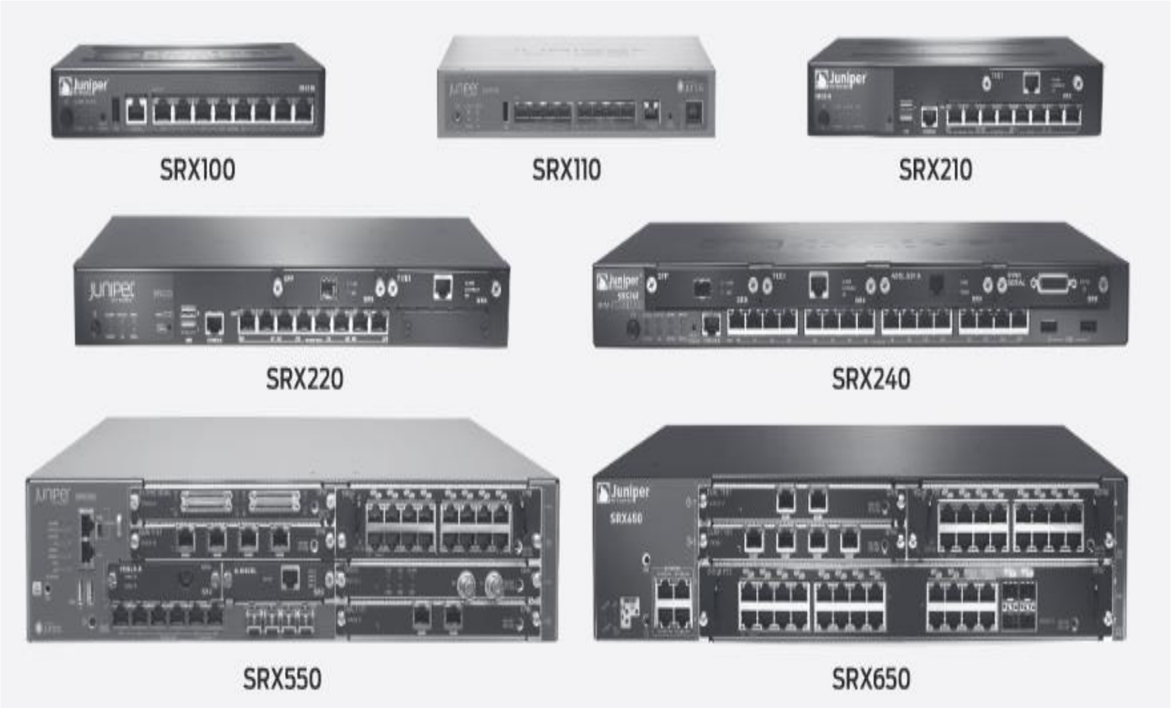
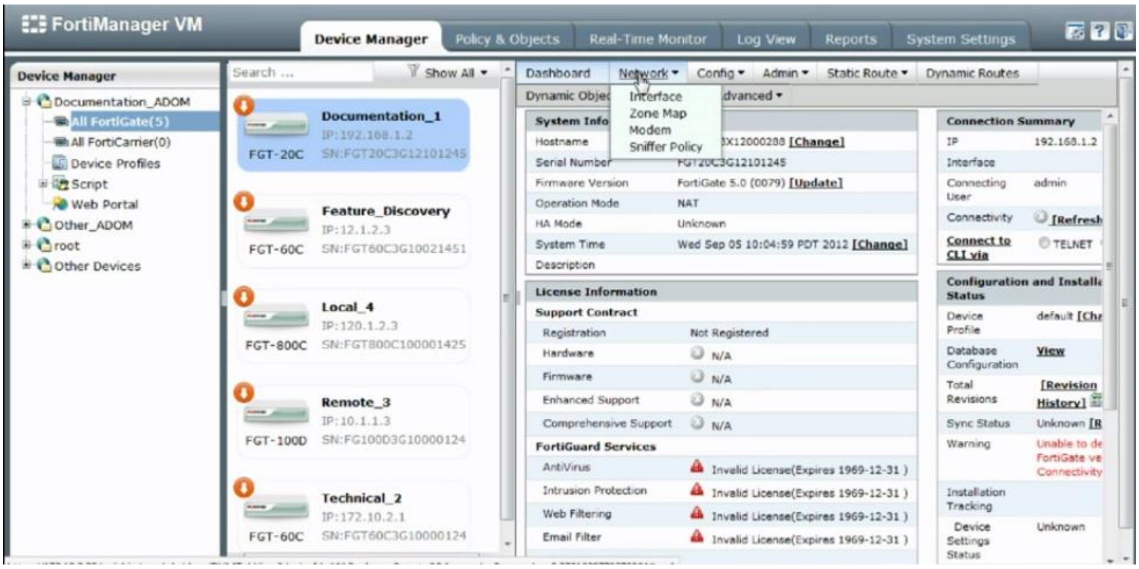


Figure 8. Juniper Network SRX Series Gateway (Juniper Network, Inc., 2014).

5.2 Fortinet

Fortinet offers a wide range of products to the service provider, large enterprises and small/medium branch offices. In this thesis, we only discussed about the FortiGate products that the target company used for their POC project. The FortiGate product is an all-in-one network security appliance, which combines firewall, IPSec and SS- VPN tunnel, application control, intrusion prevention, anti-malware, antispam, P2P security and web filtering into a single appliance (Fortinet, Inc., 2015). Smaller FortiGate (see Figure 11) devices are available with a built-in wireless access point. This gives instant WLAN for small offices, where the device can be located so that adequate wireless coverage is achieved (Fortinet, Inc., 2015).

FortiGates and FortiClents can be centrally managed with FortiManager and it is shown in Figure 9. FortiManager allows the network management team to use centralized configuration templates, making it easy to deploy standardized configurations on a large number of appliances. FortiAnalyzer is used for centralized logging and reporting. It gives visibility throughout the network infrastructure (Fortinet, Inc., 2014).



Documentation_1 IP:192.168.1.2 FGT-20C SN:FGT20C3G12101245

Feature_Discovery IP:12.1.2.3 FGT-60C SN:FGT60C3G10021451

Local_4 IP:120.1.2.3 FGT-800C SN:FGT800C100001425

Remote_3 IP:10.1.1.3 FGT-100D SN:FG100D3G10000124

Technical_2 IP:172.10.2.1 FGT-60C SN:FGT60C3G10000124

System Info	
Hostname	3X12000288 [Change]
Serial Number	FGT20C3G12101245
Firmware Version	FortiGate 5.0 (0079) [Update]
Operation Mode	NAT
HA Mode	Unknown
System Time	Wed Sep 05 10:04:59 PDT 2012 [Change]
Description	

License Information	
Support Contract	
Registration	Not Registered
Hardware	N/A
Firmware	N/A
Enhanced Support	N/A
Comprehensive Support	N/A
FortiGuard Services	
AntiVirus	Invalid License(Expires 1969-12-31)
Intrusion Protection	Invalid License(Expires 1969-12-31)
Web Filtering	Invalid License(Expires 1969-12-31)
Email Filter	Invalid License(Expires 1969-12-31)

Connection Summary	
IP	192.168.1.2
Interface	
Connecting User	admin
Connectivity	[Refresh
Connect to CLI via	○ TELNET

Configuration and Installa Status	
Device Profile	default [Ch
Database Configuration	View
Total Revisions	[Revision History]
Sync Status	Unknown [R
Warning	Unable to de FortiGate ve Connectivity
Installation Tracking	
Device Settings Status	Unknown

Figure 9. Fortinet Management Portal Called FortiManager (Fortinet, 2012).

5.2.1 FortiGate Features and Benefits

FortiGate is a simple, powerful, secure appliance that has lots of features and benefits available. However, we will only discuss a few of the key features and how they are useful to the business network.

a. Application control: Helps the organization determine which application generated traffic on the business network, along with the ability to control the business application.
b. Advance threat protection: The FortiGate appliance has an on device and cloud based detection mechanism that is able to block Advanced Persistent Threats (APT) that can aim to target specific employees or business functions within an organization.
c. Web/content filtering: Web content filtering lets an organization control what kinds of web traffic a user may view. By using web content filtering, the business can highly decrease their employees' exposure to spyware, phishing, pharming, and inappropriate web sites.
d. Integrated wireless LAN controller: Every FortiGate can act as a wireless controller, so it is possible to manage FortiAP thin access points and FortiWiFI thick access point through the FortiGate appliance. In addition, comprehensive threat management and same policy enforcement can be implemented in both wired and wireless network and it shown in Figure 10.
e. Intrusion prevention system: The system can monitor packet logging, identify malicious activities and be able to block those activities.

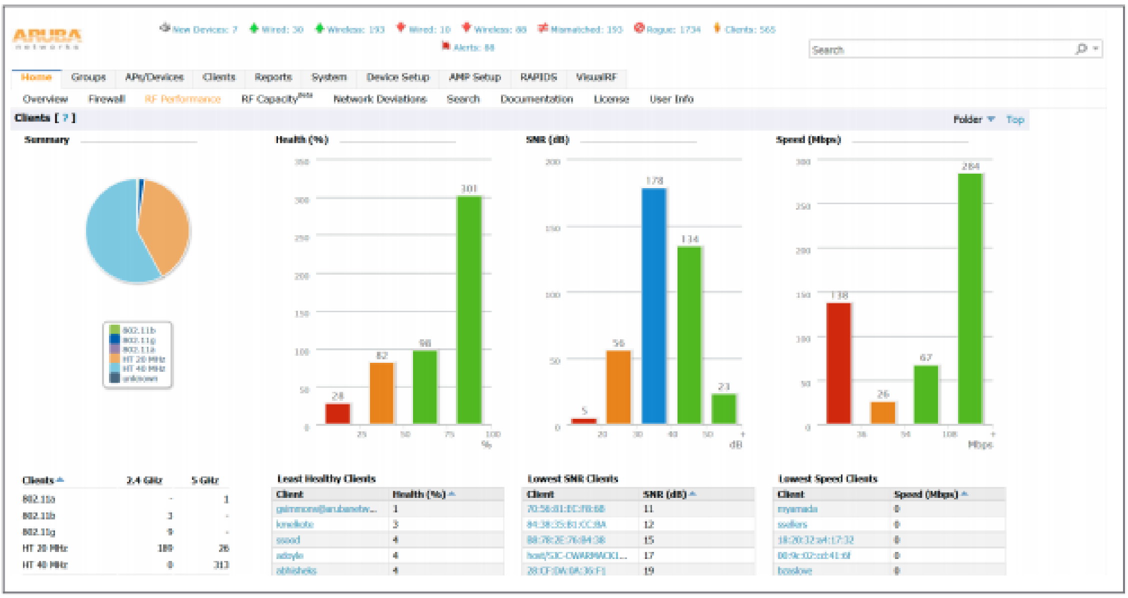
f. Anti-malware: The FortiGate appliance has the capability to do real-time monitoring and protection against the installation of malicious software (Fortinet, Inc., 2014).

Figure 10. FortiGate 800-600 Series (Fortinet, 2015)

Figure 11. FortiWiFI 60D and FortiGate 60D-POE Appliances (Fortinet, 2015)

5.3 Aruba network

The Aruba network provides a high- performance mobility solution to an enterprise, which enables employees' secure access to their data corporate network, voice and video applications across wireless and wireline networks. The company's main products are remote access points, mobility controllers and network management software, which they named AirWave management (Wikipedia, 2015), which shown in Figure 12.



Clients	2.4 GHz	5 GHz
802.11a	-	1
802.11b	3	-
802.11g	9	-
HT 20 MHz	189	26
HT 40 MHz	0	313

Least Healthy Clients

Client	Health (%)
gsimmons@arubanetw...	1
kmelkote	3
ssood	4
adoyle	4
abhisheks	4

Lowest SNR Clients

Client	SNR (dB)
70:56:81:EC:F8:68	11
84:38:35:61:CC:8A	12
88:7E:2E:76:84:38	15
host/SJC-CWARMACK1...	17
28:CF:DA:0A:36:F1	19

Lowest Speed Clients

Client	Speed (Mbps)
myamada	0
swilkes	0
18:20:32:a4:17:32	0
00:9c:02:cd:41:6f	0
bswlowe	0

Figure 12. Aruba AirWave Management Platform for Wireless, Wired and Remote Networks (Aruba Networks)

5.3.1 Mobility controller features and benefits

The Aruba mobility controller is a simple, compact and affordable solution for the corporate network. Figure 13 shown Aruba mobility controller and Figure 14 shown remote access point from Aruba network. The mobility controller not only manages access points, but it is also capable to handle many different kinds of operations that were usually handled by some dedicated network hardware devices. The controller acts as an IPsec virtual network private network tunnel concentrator for site to site and client based VPNs. Some of the mobility controller features are as follows (Aruba network, Inc., 2010).

a. Its acts as a user role-based firewall.
b. Centralized security, control and management
c. The Mobility controller is working as layer 2 switching and layer 3 routing.
d. Identity-based security gateway
e. It is able to detect and block unsafe traffic.
f. It provides separate guest access.
g. The Mobility controller has advanced radio frequency services with adaptive Radio management and spectrum analysis.
h. Seamless integration with existing corporate VPNs
i. Easy to deploy and expend without interruption to the wired network
j. Able to provide location services and has a radio frequency “heat map” feature

Figure 13. Aruba 3000 Series mobility Controllers (Aruba network, 2010)

Figure 14. Aruba RAP-5WN Remote Access Point(Aruba Network, 2011)

5.4 Vendor sections decision matrix

As we discussed in chapter 5 after a preliminary analysis, the target company decided to test three vendor's hardware devices for this proof of concept project. However, selecting the right vendors would not be easy if the company does not have any standard vendor selection guidelines. So based on the project requirements, the project team came up with a list of test criteria, which need to be performed during the implementation time as well as on the live network. A more detailed breakdown of the vendor selection matrix is shown in Table 1.

Table 1. List of Test need to Performed During Implementation and Testing Period

Test Field	Site Type	
Implementation test	Hub and satellite office	Line up
Implementation test	Hub and satellite office	Preconfigure equipment installed
Implementation test	Hub and satellite office	IPSec connection
Implementation test	Hub and satellite office	LAN connection
Implementation test	Hub and satellite office	Wireless connection
Implementation test	Hub and satellite office	SAP application
Implementation test	Hub and satellite office	Web based tendering application
Implementation test	Hub and satellite office	CAD/CAM document management application
Implementation test	Hub and satellite office	VoIP and video
Implementation test	Hub and satellite office	Intervention planning application
Implementation test	Hub and satellite office	Sharepoint
Implementation test	Hub and satellite office	Browsing
Implementation test	Hub and satellite office	External email
Implementation test	Hub and satellite office	SaaS application (mainly saleforce.com)
WAN performance	Hub office	Reducing the pressure on the MPLS connection by using internet gateway "load"
WAN performance	Hub office	Reducing the pressure on the MPLS connection by using internet gateway "max bandwidth"
WAN performance	Hub office	Latency in MPLS and Internet
WAN performance	Hub office	Reducing the pressure on the MPLS connection by using the internet gate Hub office way "less discard out"
WAN performance	Hub office	Reducing the latency to reach the datacenter over the IPSec tunnel
WAN performance	Hub office	Network traffic from the satellite office to MPLS

		connection over Internet
WAN performance	Hub office	Internet breakout statistics
WAN performance	Hub and satellite office	Core application statistics, ping, timeout
WAN performance	Hub and satellite office	Outage length (timeout)
User acceptance	Hub and satellite office	Internet access first impression (bad, even, better)
User acceptance	Hub and satellite office	Application performance (bad, even, better)
User acceptance	Hub and satellite office	Network availability (bad, even, better)
User acceptance	Hub and satellite office	IP telephony (bad, even, better)
Firewall performance	Hub and satellite office	Don't allow any incoming and only outgoing traffic
Firewall performance	Hub and satellite office	Antivirus
Firewall performance	Hub and satellite office	Content filter/ app filtering
LAN performance	satellite office	Wireless (easy to configure)
LAN performance	satellite office	Printing over LAN and WAN
Vendor Comparison	Hub and satellite office	Cost of solution per office
Vendor Comparison	Hub and satellite office	Easy to implement and move
Vendor Comparison	Hub and satellite office	Scalability
Vendor Comparison	Hub and satellite office	Monitoring capability and reporting
Vendor Comparison	Hub and satellite office	Remote configuration (deploy and configure from anywhere)
Vendor Comparison	Hub and satellite office	Easy to troubleshoot

6 NETWORK REDESIGN CASE STUDY

The basic idea of this proof of concept project was to reduce MPLS network usage by providing local, secured internet access at all levels. In small offices, MPLS can be completely replaced with Internet. This is done by the deploying vendor's solutions at all offices, providing secure Internet access along with a VPN connection and MPLS access.

6.1 High level view of network design for POC

Before deploying any larger scale of an Internet breakout solution into the corporate network, it is a good idea to test the vendor's devices to see how well they perform in the real world network. For this proof of concept project, the target company decided to test the Juniper network, Fortinet and Aruba network solution (discussed in chapter 5) in three countries within eight different cities. Due to the project time constraints, not all vendor solutions could be tested at every location, so the company decided to test the Juniper network solution in China, the Aruba network solution in Finland and the Fortinet solution in the United Kingdom. It is discussed in more detail for each country's test network setup in later sections in this chapter.

To successfully test those new devices and at same time not interrupt everyday business operations, all test locations received new Internet connections for Internet breakout and for the IPSec tunnel. The plan was to check if any problems occurred during the implementation or testing period, so that the office network could fall back to an old connection that has been working previously to help minimize risk. Therefore, the smaller branch offices (discussed in chapter 3.6), where not so many users were working will only have an Internet connection, and at regional offices or headquarter offices, it will complement the MPLS network and Internet connection. At larger offices with both Internet and MPLS connections, critical traffic and applications which were hosted in the datacenter such as SAP, Voice over IP, and SharePoint are routed through the MPLS network. Noncritical traffic, Internet access like email, browsing, YouTube, and saleforce.com will send though Internet line. This can be achieved either through regular routing or through policy routing. These VPN connections can be also act as backup connection for the MPLS network to increase network reliability. Automatic failover of connections can be achieved either through dynamic routing or through static multipath routing with link failure detection. Internet bound traffic is naturally sent directly to the Internet.

6.2 Finland test plan

The target company has selected two small branch offices as test locations for the Aruba network solution. Each location had around seven users. It was the company's internal decision to test Aruba devices only for small offices where no more than 10 users were located and the office does not perform any critical operations. For this project, each location had one new business class Internet connection. Deploying the Aruba Remote Access Point (RAP) in small branch offices was easy (discussed in chapter 6.2), but installing the Aruba mobility controller in the datacenter was a bit difficult because of datacenter's own firewall. Once that was sorted out, it worked very well and is discussed further in chapter 5.3. The Aruba mobility controller had a firewall feature but in this project, the firewall feature was not tested.

Previously, all small branch offices connected through the IPSec tunnel to the datacenter. To access Internet and corporate applications, small offices had to travel through the datacenter and from there access Internet and corporate applications. There was no Internet breakout from each country, as all Internet breakouts happened from regional datacenters. The small branch offices are the ones affected by poor network performance because of a long distance path to datacenters and low bandwidth connections.

In this architecture, a Remote Access Point (RAP) device provides similar functionality to a VPN client but allows for shared access to multiple devices through wired and wireless LAN interfaces. The mobility controller, which was located in the datacenter, acts in an analogous manner to a VPN concentrator. Each RAP communicates with the controller over one or more WAN or more secure, encrypted IPSec tunnels. This communication provides access to the devices/users connecting through the RAPs to the company's core network and to the applications and services that exist there. The connection between the controller and RAPs are shown in Figure 15.

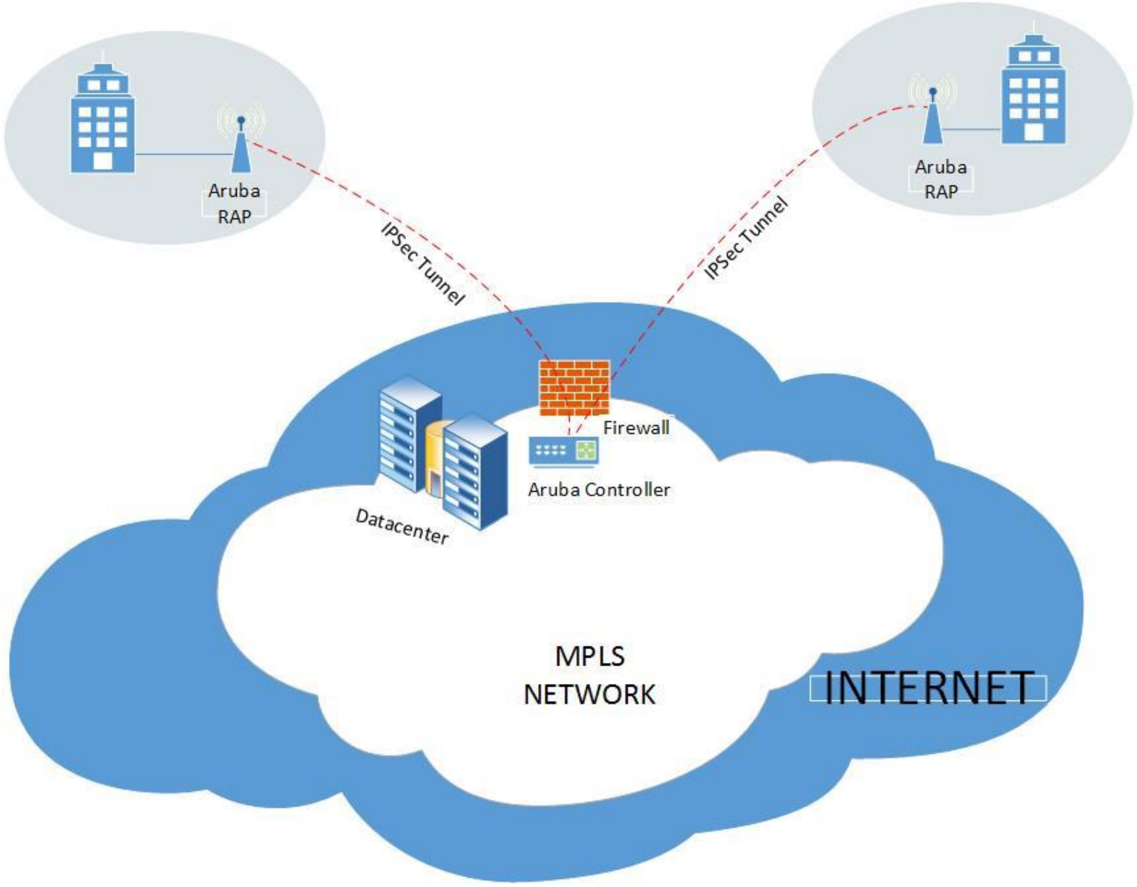


Figure 15. RAPs are Communicating with the Controller over WAN

6.3 United Kingdom test plan

With the current company network architecture, satellite offices had a single Internet connection. As mentioned in chapter 6.2, not every country had their own Internet breakout or datacenter. All small offices that were connected through the IPSec tunnel had to go through a long path to the regional datacenter to access Internet and corporate critical applications. All regional offices or corporate office's network traffic went through a MPLS connection to reach the datacenter or half-datacenter to access hosted applications and for accessing Internet and cloud based services. This is discussed in chapter 3.2.1.

As mention earlier in chapter 6.1, FortiGate appliances have planned to test in the United Kingdom. The target company selected one large office, which is called the hub office and three other branch offices that were called satellite offices for this project. Previously, two branch offices had one IPSec connection each and another branch office had one MPLS as primary connection and an

IPSec connection as a backup. The hub office had two MPLS connections; one was for a primary connection and another was for a backup connection. For this project, a new Internet connection was installed in the hub office from a local ISP provider for Internet breakout and for the IPSec tunnel to satellite offices. A new Internet connection was installed in all satellite offices from the same ISP provider for the IPSec tunnel to the hub office.

With the Fortinet solution, each country will have at least one Internet breakout point, which will to reduce latency to access service from the Internet. The target company also wanted to test how much network performance improves when using the same ISP vendor connection for all offices. The company expected that if all offices were on the same ISP network, satellite offices would have less hops to reach the hub office. Therefore, a new Internet connection was installed from the same ISP vendor for each test location. As mentioned in chapter 6.1, the satellite office's user network traffic will go through the hub office. From hub office it will decide, if network traffic is Internet or cloud based services, it goes directly to the Internet using local internet breakout and if network traffic is corporate applications or hosted applications at the datacenter, it will use the hub office MPLS connection to reach the corporate network. The same network traffic rules are applied for the hub office users. Figure 16 is illustrated United Kingdom test network setup.

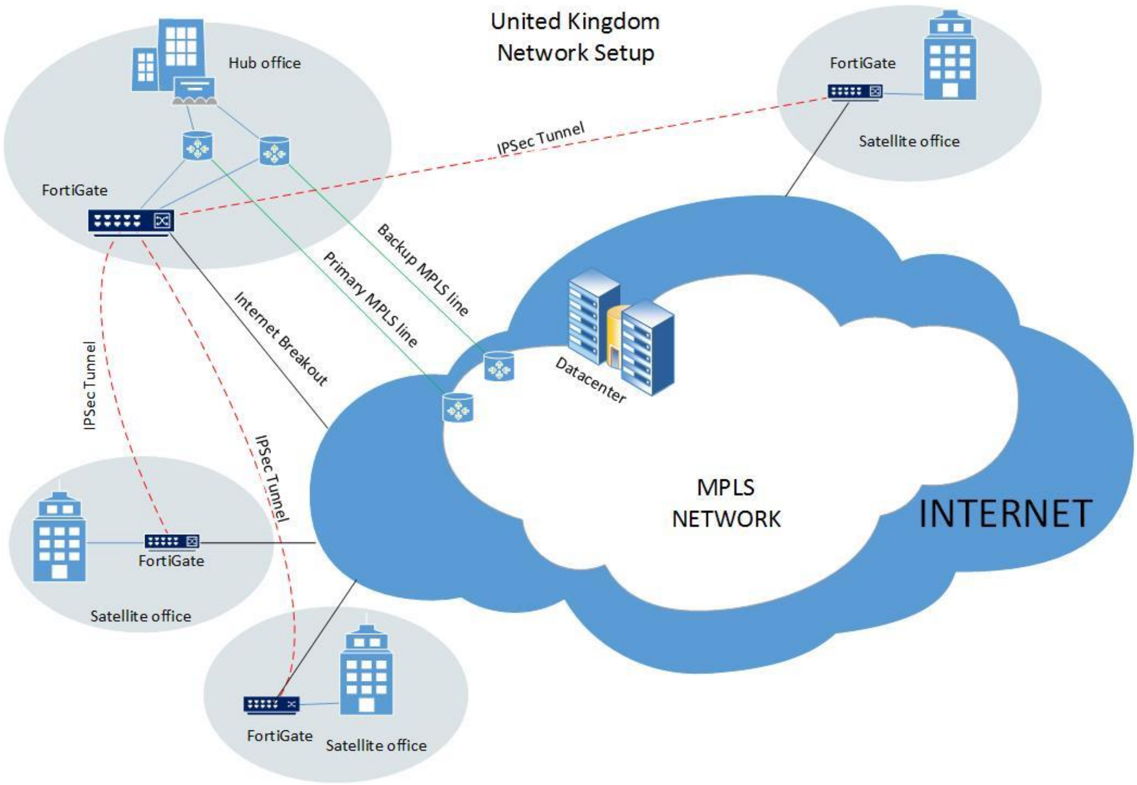


Figure 16. Test Network Setup for Fotinet Solution in United Kingdom.

6.4 China test plan

In China, the company has decided to test the Juniper network solution in two different locations. One large office acted as a hub office and it had over 300 users and a small branch office acted as a satellite office that had 30 users. Previously, the hub site had two MPLS connection, one for the primary connection and another was for backup. The satellite office had only one MPLS connection and no backup connection.

To test the juniper devices, both locations received a new Internet connection from the same ISP vendor. The idea here was to replace the MPLS connection by an IPSec tunnel and check how well it would perform. This way, the target company could replace no mission-critical branch offices that had MPLS connections and replace them with cheaper IPSec connections. It will be a huge network operation cost savings for the company. With a similar network design to the United Kingdom (discussed in chapter 6.3), users' corporate related network traffic from the branch office will travel through to the hub office and from there to the corporate network. If that traffic is Internet related, they will use local Internet breakout on location and direct access the Internet and if the users try to accessing corporate applications which were hosted in the datacenter, it will use the hub office MPLS connection to connect to the datacenter and it shown in Figure 17.

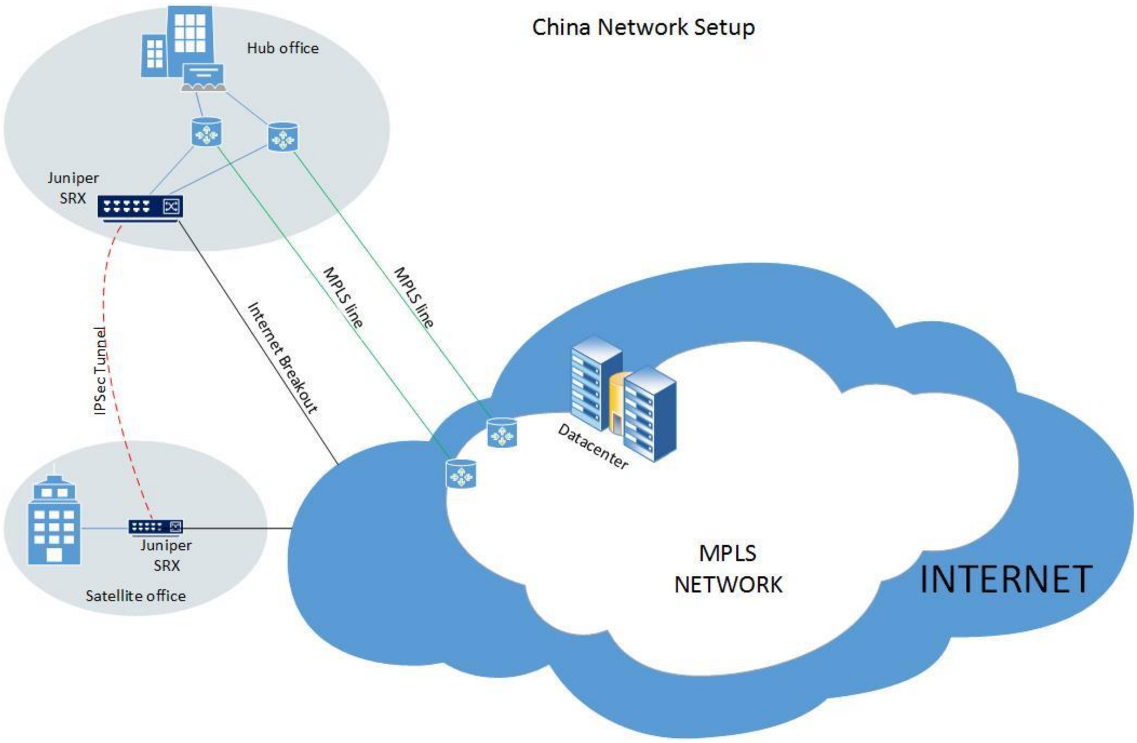


Figure 17. Test Network Setup for Juniper Solution in China

6.5 Test result

A general conclusion can be made after implementing those new vendor devices to corporate network for couple of months. First of all, Internet breakout worked perfectly as we expected and users have seen huge improvements of application performance, especially when they tried to access Internet and cloud based applications. The results of each country are discussed in the following section.

6.5.1 Test result analysis for Finland

The Aruba mobility controller was not a full feature UTM device like Juniper and Fortinet. Though the Aruba controller has a firewall capability as mentioned in chapter 6.2, testing the Aruba firewall was not part of this project scope. It was very easy to provision a new remote access point through the Aruba management portal called AirWave management. It was possible to apply different user group polices, application access policies and many other features through the management portal. The AirWave management portal helped the company add more visibility to their network with real time monitoring and reporting, which was not the case for previous vendor solution. They did not have any monitoring system where the target company can monitor small branch office's network traffic and because of this, there were always a problem when it came to troubleshooting network related issues for branch offices.

The Aruba remote access point had physical ports where the local branch office had a connected printer, IP telephone and other physical devices. The Aruba remote access point had built-in WiFi, which was very useful for the small branch office. Therefore, a user can move with their laptop inside office space and experience no hassle with cable. Previously, branch offices had a small IP-Sec tunneling(see Figure 18) device with no built-in WiFi, and that device had limited physical ports, and as a result only a limited number of devices could be connected to the corporate network, which was a big barrier. With a new network setup with the Aruba solution, branch offices had their Internet breakout within the country (see Figure 19) and now local network traffic traveled through an encrypted IPSec tunnel to the datacenter to access corporate applications and Internet. Average latency improvement was very positive in Finland, before average latency was 82ms but with new network design, it was only 10ms and that was great network performance improvement. The company plan is to deploy Aruba controllers to each country in the headquarters or regional offices or datacenter and all small branch local offices will connect to the Aruba mobility controller. The main idea was to give users more flexibility, be easy to install, first to deploy, have visibility to the network and reduce latency. All of those requirements were successfully achieved by the Aruba network solution.

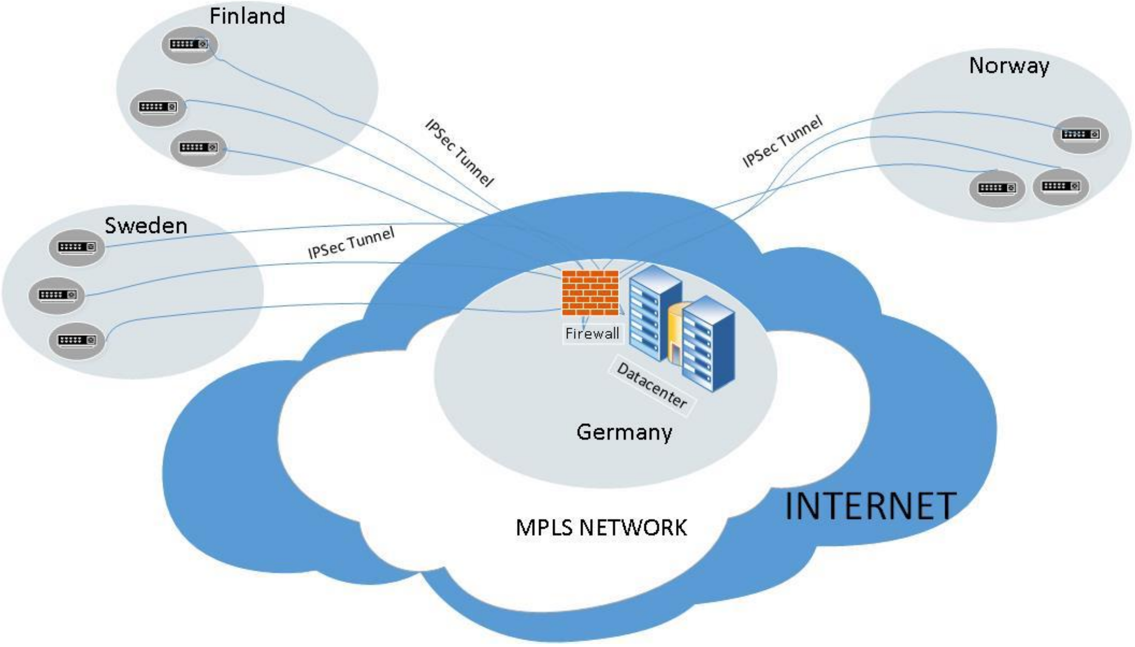


Figure 18. Shown Current Branch Offices IPSec Connection to DatacenterShown Current Branch Offices IPSec tunnel to Datacenter.

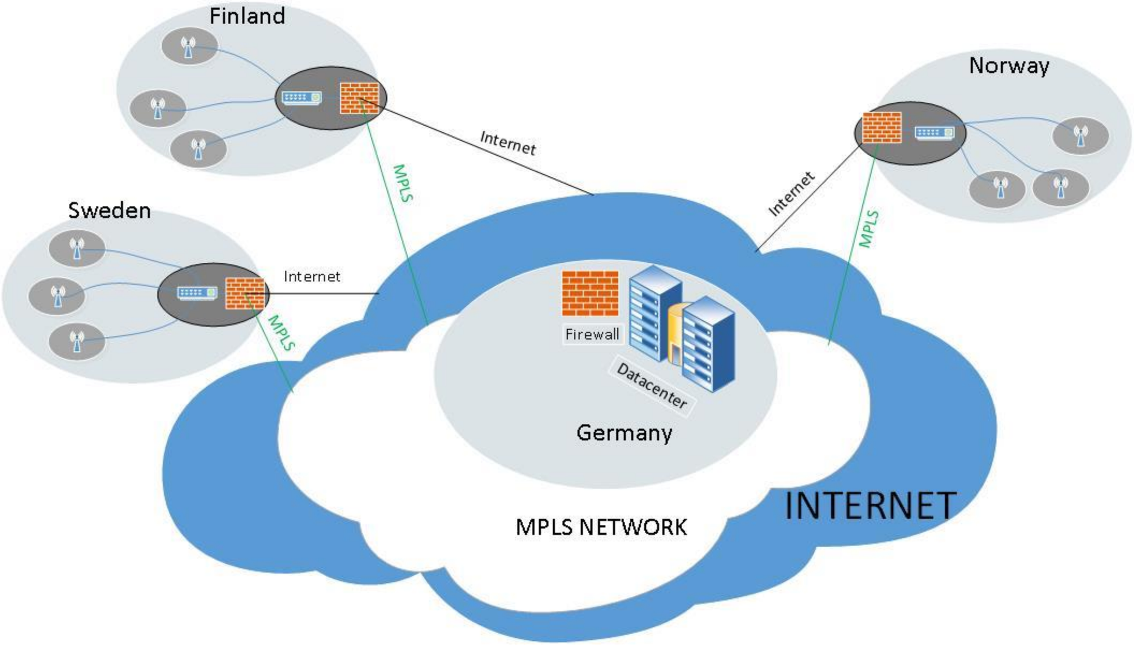


Figure 19. Shown Internet Breakout from each country for Small Branch offices when Implementing Aruba Controller and Remote Access Point.

6.5.2 Test result analysis for United Kingdom

The testing locations started to see great benefits with this new solution offloading all Internet and cloud based services traffic. Previously, the hub office UK1 used 80% of total capacity of a MPLS connection and it shown in Figure 20. That UK1 network traffic was Internet services and corporate application traffic. Because of Internet breakout, the hub office managed to save 50% bandwidth, which was used on the MPLS connection where all core corporate traffic used the MPLS connection and all other traffic used Internet breakout. This is discussed in chapter 6.3. Moreover, when the other three test satellite offices (UK2, UK3, and UK4 respectively), used UK1 MPLS connection, even then the UK1 office MPLS connection had not used as much as they did earlier. After monitoring for a while, it showed that UK1 used 40% of total MPLS Bandwidth, UK2 office used 15%, UK3 office used 3% and UK4 office used 3% MPLS bandwidth as well. In total, all four offices used only 61% of total MPLS bandwidth. Each office MPLS bandwidth uses shown in Figure 21.

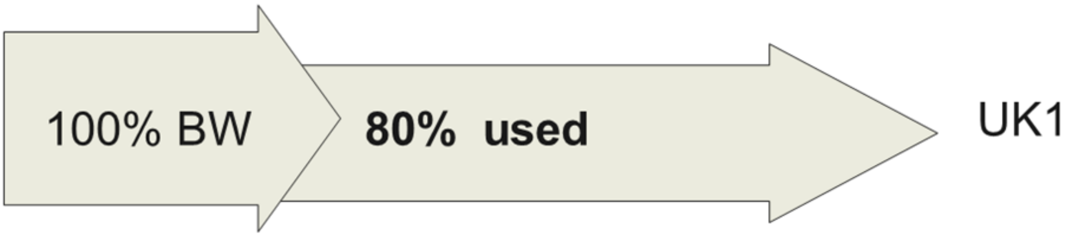


Figure 20. Shown UK1 MPLS Bandwidth used without Internet Breakout

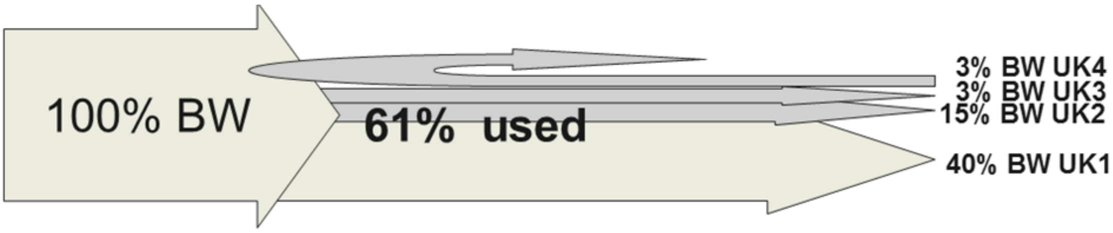


Figure 21. Illustrated MPLS Bandwidth used by all Satellite and Hub Offices when Internet Breakout is Implemented.

Satellite offices users also experienced great network performance improvement when they have accessed direct internet from hub office. Average latency in satellite offices also improved even though those offices corporate network traffic travel through hub office. Figure 22 and Figure 23 are illustrated between previously and newly designed network traffic path. Average latency was 150ms before, but with new internet connection from same ISP vendors it was 140ms. Moreover, between UK1 and UK2 with fast link connection average latency was only 8ms. Therefore, it gave the company very good added value to remove all MPLS connections in future from non-critical offices and replace those offices with an Internet IPsec connection which will cost less for the same amount of bandwidth and even more for the same price. In addition, it is also recommended to use one ISP vendor internet for each country to get lower latency being same network. This is very useful for future communication. The company knows that in the future, they will need more bandwidth for video, teleconferencing, social media, etc. and all the other services deployed in the cloud.

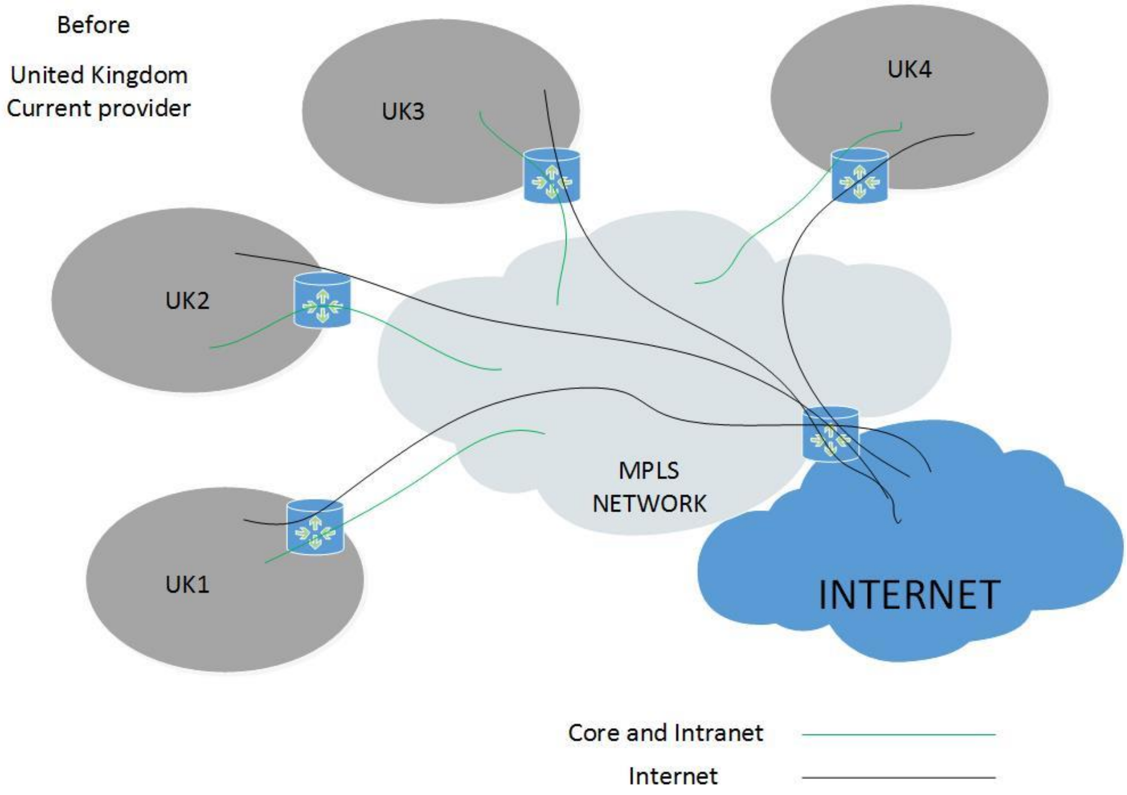


Figure 22. Network Design from Current Service Provider in United Kingdom.

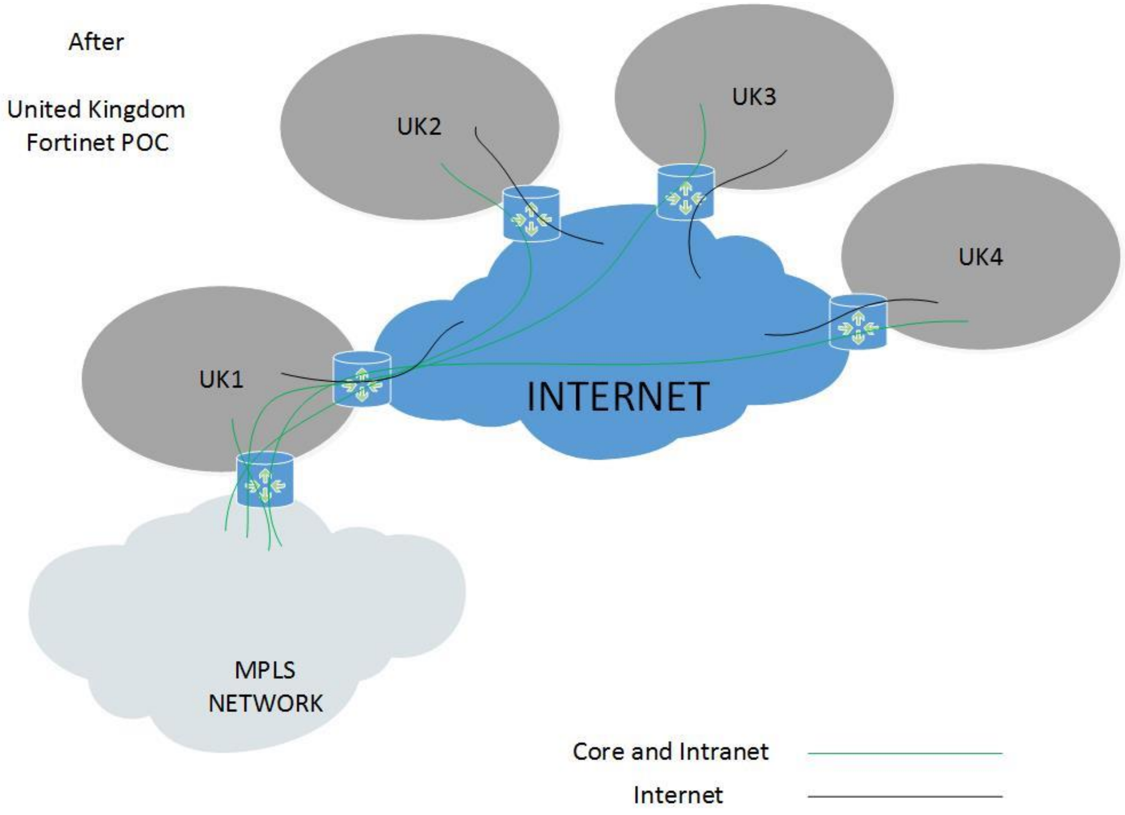


Figure 23. Future Network Design Solution In United Kingdom

6.5.3 Test result analysis for China

There were similar benefit found when implemented internet breakout in china. It worked fine as expected. There was no problem with IPsec connection from satellite office to hub office. Only surprised thing was that the company assumed the hub office would save MPLS bandwidth by offloading internet traffic from MPLS connection, which was not the case in china. In china, local office users were not using internet as much as they did in United Kingdom, not all country work same way. Maybe their corporate policy over there was not to use internet during office hours. Therefore, the result was different then what the company expected. The hub office only managed to 5% MPLS bandwidth. This was very important information for internet breakout implementation that result from one country could not be extrapolate to other country. The company will has to take every country case per case deployment of internet breakout in future.

On the other hand, the hub office users experienced faster responded when they accessed internet service. Figure 24 and Figure 25, shown difference between current network design and proposed network design solution for future in china. The test satellite office only used on average 0.3 Mbps sent traffic to hub office MPLS connection. Therefore, the target company saved operation cost by replaced MPLS connection with IPSec connection in that satellite office. In china, MPLS connections were very expensive and the company has many small branch offices there. In addition, there current growth market is china.

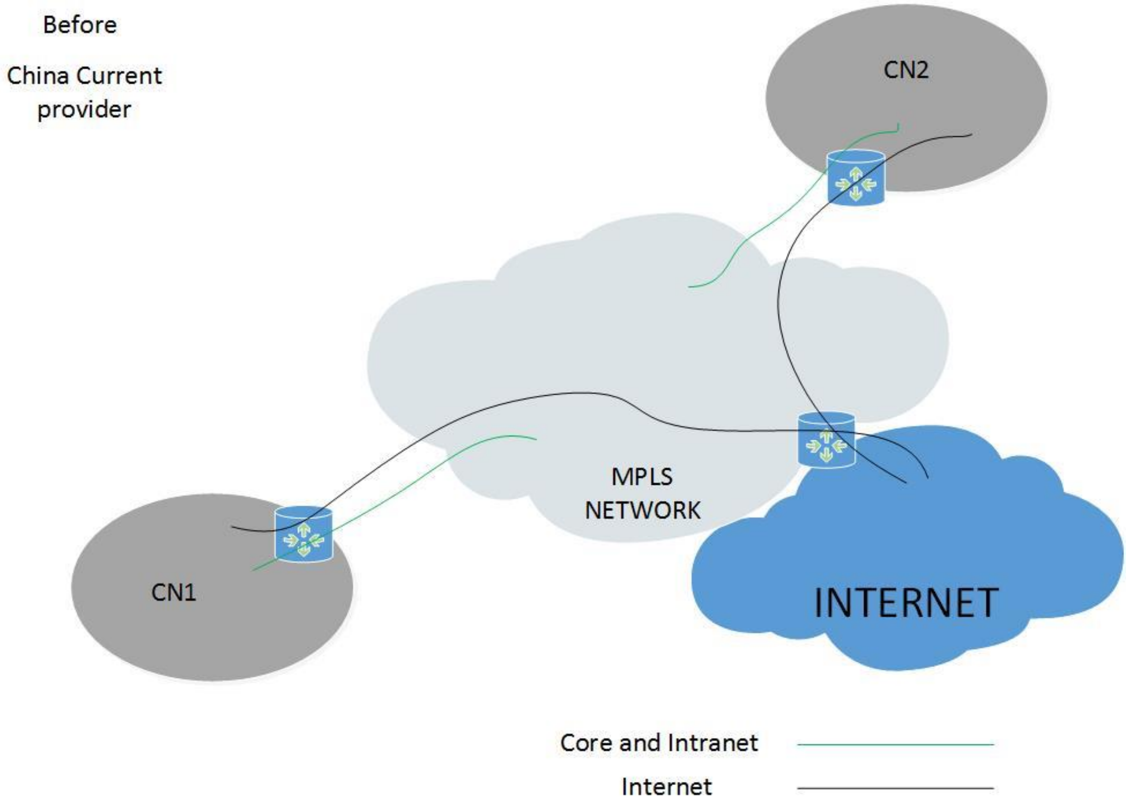


Figure 24. Current Network Setup for china from Network Service Provider

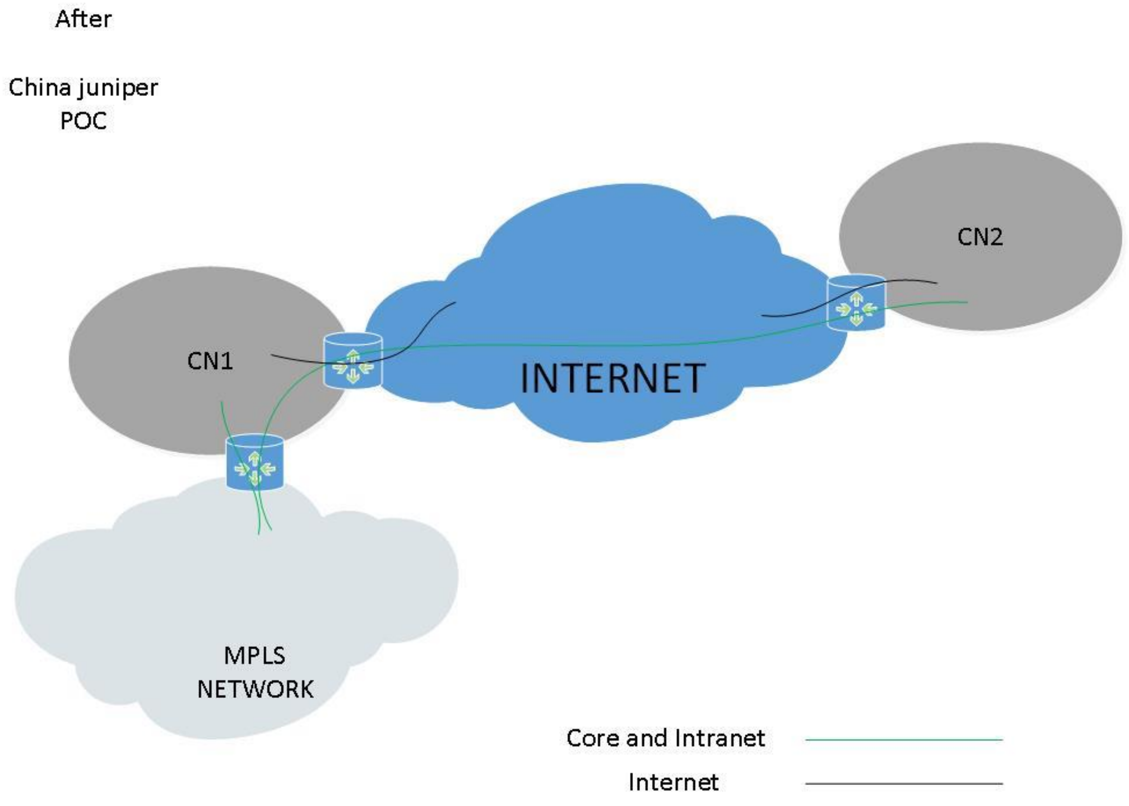


Figure 25. Internet Breakout Design Solution for China.

6.6 Project feedback

The project completed successfully without any major issue during implementation and testing period. Beginning of this project, it was little challenging to find right person whom project team could communicate, because project team was located different locations then those testing office locations. Fewer locations took little long time then other to get new internet line. Other than that, everything went efficiently as we expected.

6.6.1 Implementation

It was easy to install those new devices in different test locations. Estimation time was to roll back from new test connection to old setup was 5 to 30 min. Testing with users were very fast and they were very excited about new network solution. User gave good feedback. Every test location had one person who able to contact technical team if something goes wrong. It was easy for current network service provider to configuring their edge router for implemented those devices. Both UTM device like juniper SRX and ForTiGate appliance were easy to configure as well as Aruba remote access point. It was not very difficult to implement internet breakout using proxy on the hub office. Some of those test locations internet line delivered very fast.

6.6.2 Support

Support was done for this proof of concept by the project team, on office contact country coordinator and vendor engineer. but in future, support should be provide from central fully managed services or dedicated team. Internet support provided by local ISP provider.

6.6.3 Vendors summary

As mentioned earlier in chapter 6.5.1, Aruba mobility controller was not full feature UTM device and Aruba controller has not used as an internet breakout for this project, this is why it could not be compared with juniper or Fortinate solutions. Aruba solution used in this project as a LAN extension over WAN. Aruba solution should be considered for small offices using mainly the built-in WiFi capability to give users more mobility in office floor. Aruba remote access point (RAP) proven to be very easy to install in the office. Users were very satisfied with and gave good feedback. In future, Aruba mobility controller could be installed on outside of firewall for easier configuration and easy deployment.

On the other hand, Juniper and Fortinet hardware were great and performed very well. Both solutions were easy to install, creating new networks, VPN links and changing configuration through network management portals were easy as well. Both were very stable devices that capable to handle lots of network traffic. Offloading MPLS bandwidth and internet breakout achieved by Juniper SRX and FortiGate devices. Fortinet analyzer had pre-installed templates to analysis network traffic, which was easy to load and reporting were simple with Fortinet manager. However, to analysis network traffic with Juniper management portal, user need to be more knowledgeable but it had lots of customization available and reporting capability was very good. One of the big differences between both vendors devices were to juniper device did not have WiFi integration with their device at the time of this project whereas Fortinet device had. Therefore, on the hardware side Fortinet had something that give benefit. Both vendors devices can link to active directory, able to make group policy and access policy to internet websites. TABLE 2 is shown, Overall impression after testing vendors solution in the target company network.

Table 2. Overall Impression about Vendors Solution After Implementation

Preliminary analysis	Aruba Network	Juniper Network	Fortinet

Positive response to RFI	Yes	Yes	Yes
Built in Firewall	Yes	Yes	Yes
Internet Breakout capable	No	Yes	Yes
Built in Anti-Virus	No	Yes	Yes
WiFi for small office	Yes	No	Yes
Single vendor possible	No	Yes	Yes
Implement all office	No	Yes	Yes
Management solution	Yes	Yes	Yes
Network analysis	Yes	Yes	Yes

7 CONCLUSIONS

There are several trends that are changing the way in which corporate networks are being used. New ways of collaborative working, interaction via social networking and evolving device types like tablets and smartphones gives a fresh new possibility to access business applications, but at the same time can create overwhelming challenges for the corporation's IT department. The ability to support this change is fundamental, but requires technologies and solutions that are designed for that purpose from the ground up.

The objectives of this case study were to experiment local Internet breakout in a corporate network in order to improve network performance, save MPLS bandwidth and operation costs, and have the ease of implementing the new vendor's solution. Internet breakout is a potential solution for bandwidth saving in the MPLS connection and possible to reduce number of expensive MPLS connections from the corporate network. Internet breakout can reduce the response time of Internet access, social networks and cloud based applications. It has been proven that the Internet breakout solution is possible and easy to deploy on the current corporate network.

When implementing local Internet breakout, it is recommended to order the Internet connection locally and from the same ISP provider to get better latency between offices and also possible to get a better price. For future growth such as video, voice and other critical applications, it is very useful to offload the MPLS connection and it works well for Europe. The target company needs to have strong support as well as a monitoring strategy if they implement many UTM devices in their network because UTM devices tend to have a shorter life span than other network hardware devices and face threats much faster than hardware can keep up to date.

Some concerns about this project are that the target company only selected eight locations, which represents only 1.5% of whole network, which is not good data to extrapolate for the rest of the other locations. It would be useful to analyze office network traffic and Internet line cost of each county, so that this data would be useful to extrapolate. As mentioned earlier, China does not use the Internet a lot, so Internet breakout is not as useful as in the United Kingdom.

There are a couple of main key findings of the tests performed in this thesis, which are as follows:

a) Local Internet breakout is reducing latency internet access.

b) Local Internet breakout saves MPLS bandwidth.

c) Local Internet breakout is not useful for every location.

Before implementing Internet breakout, it is important to consider the corporate culture and functionality at that location and most importantly, user network traffic because it could be different from office to office.

REFERENCES

Aruba Networks,Inc (2011). Datasheet. Aruba RAP-5Wn Remote access point . Accessed May 5, 2015
http://www.fairline.com.tw/Downloadfile/97286DS_RAP5WN.pdf

Aruba Networks,Inc. Datasheet. AIRWAVE. Comprehensive management for wireless, wired and remote office. Accessed May 5, 2015
http://www.arubanetworks.com/pdf/products/DS_AW.pdf

Aruba Networks, Inc(2010). Aruba mobility controllers and deployments models validated reference design version 5.0. Accessed May 5, 2015
http://www.arubanetworks.com.cn/downloads/pdf/technology/DG_Mobility-Controllers-Deployment-Models-5.0-VRD.pdf

Bertsekas, D. & Gallager R. (1992). Data networks (2nd Edition). Prentice Hall, New Jersey 1992, 150 p, ISBN 0132009161

Cisco system,Inc (2013, August 29th), Internetworking Technology Handbook Ethernet Technologies wiki. Accessed January 21, 2014
http://docwiki.cisco.com/wiki/Ethernet_Technologies

Cisco system,Inc (2012,October 16th), Internetworking Technology Handbook – introducing to LAN Protocols wiki. Accessed January 22, 2014
http://docwiki.cisco.com/wiki/Introduction_to_LAN_Protocols

Cisco (2014, 10th June). Cisco White paper. The Zettabyte Era—Trends and Analysis. Accessed September 24, 2014
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.pdf

Cisco system, Inc(2005, August 10th), TCP/IP Overview. Accessed January 23, 2014
http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13769-5.html

Cisco (2012, 16th October).Cisco wiki. Internetworking Technology Handbook – WAN Technologies,. Accessed September 22, 2014
http://docwiki.cisco.com/wiki/Introduction_to_WAN_Technologies

Cisco System,Inc (2012, October 16th), wiki: Introduction to WAN Technologies. Accessed September 22, 2014
http://docwiki.cisco.com/wiki/Introduction_to_WAN_Technologies

Fortinet,Inc (2015). FortiGate 100D Series. Accessed February 1, 2015
https://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-100D.pdf

Fortinet,Inc (2015). DataSheet. ForiGate/FortiWiFi 60D Series. Accessed February 1, 2015
http://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-60D.pdf

Fortinet,Inc (2014). Connected UTM . Accessed February 3, 2015
http://www.fortinet.com/sites/default/files/solutionbrief/UTM_SMB_Solution_Guide_2014_r1.pdf

Fortinet, Inc(2014). FortiManager. Accessed February 1, 2015
http://www.fortinet.com/sites/default/files/productdatasheets/FortiManager-VM.pdf

Fortinet, Inc (2012). Video. FortiMannager v5.0 Beta New Features. Accessed February 22, 2015
http://video.fortinet.com/video/25/fortimanager-v5-0-beta-new-features

Gareiss, Robin (2009, February) Search EnterpriseWAN Blog: Troubleshooting WAN performance issues. Accessed September 23, 2014
http://searchenterprisewan.techtarget.com/tip/Troubleshooting-WAN-performance-issues

Herndon, VA (2013, 2nd October).Xo communication Press release. New Independent Consulting Study Shows Value of Cloud Services Remains Elusive for Many Enterprises. Accessed September 25, 2014
http://www.xo.com/about-xo/news-and-events/press-releases/new-independent-consulting-study-shows-value-of-cloud-services-remains-elusive-for-many-enterprises/

HowStuffWorks.com, (2000, December 1st) What is a packet ?. Accessed January 21, 2014
http://computer.howstuffworks.com/question525.htm

Johanson, Till Johan (2010, May). Search EnterpriseWAN Blog: WAN performance: Application delivery, optimization and the end user. Accessed September 23, 2014
http://searchenterprisewan.techtarget.com/tip/WAN-performance-Application-delivery-optimization-and-the-end-user

Johnson, Johna till(2007, March 29th), Networkworld article : MPLS explained. Accessed September 21, 2014 http://www.networkworld.com/article/2297171/network-security/mpls-explained.html

Juniper Networks, Inc (2009). Datasheet. STRM Series Security Threat Response Managers. Accessed March 1, 2015
http://www.fr.security.wesrcon.com/documetns/23182/juniper_ficheproduit_STMR_Datasheet_ANG.pdf

Juniper Networks,Inc (2014, Sep). SRX series services gateways for the branch. Accessed February 1, 2015
http://www.juniper.net/us/en/local/pdf/datasheets/1000281-en.pdf

Murphy,Matt (2014, 18th October). Techcrunch Blog.10 Trends Transforming Enterprise IT. Accessed October 23, 2014
http://techcrunch.com/2014/10/18/big-changes-big-money-10-trends-transforming-enterprise-it/

Rouse, Margaret. (207, May).Search EnterpriseWAN Blog: virtual private network (VPN). Accessed May 12, 2015
http://searchenterprisewan.techtarget.com/definition/virtual-private-network

Rouse, Margaret. (2012, April).Search EnterpriseWAN Blog: what is an Enterprise WAN?. Accessed September 21, 2014
http://searchenterprisewan.techtarget.com/definition/enterprise-WAN

Rouse, Margaret. Search EnterpriseWAN Definition: Bandwidth Definition. Accessed May 12, 2015
http://searchenterprisewan.techtarget.com/definition/bandwidth

Rao & H.U (2010). Deploying Network Management Solutions in Enterprises. *2010 6th International Conference on Networked Computing (INC), (pp. 1-2).* Gyeongju, Korea (South). IEEE Computer Society. 11-13 May 2010
Taneja Group, Wide Area Data Services: Optimizing the Branch, [e-document], 2005, White paper [Accessed September 22, 2014] From Techworld
http://www.techworld.com/whitepapers/index.cfm?whitepaperid=4053

Wikipedia.org (2015, May 11th). Wikipedia Wiki: IPsec. Accessed May 12, 2015
http://en.wikipedia.org/wiki/IPsec

Wikipedia.org (2014, October 29th). Wikipedia Wiki: Network Delay. Accessed May 13, 2015
http://en.wikipedia.org/wiki/Network_delay

Wikipedia.org (2015, 5th may). Aruba network. Accessed May 5th, 2015
http://en.wikipedia.org/wiki/Aruba_Networks

APPENDIX 1. Office classification and capacity management guidelines

Office level	Description	Redundancy	Technology	Users
Office level 0	Data center, factory	Dual MPLS link from different carriers	MPLS	All
Office level 1	Headquarters, Call centers	Dual MPLS ending same pop	MPLS	<50
				50<x<100
				>100
Office level 2	Headquarters, Regional offices	Primary MPLS / Backup Internet	MPLS/ MPLS and IPsec	<25
				25<x<50
				>50
Office level 3	Branch offices	NO	MPLS/IPsec	<10
				10<x<25
				>25
Office level 4 and 5	Service center	NO	IPsec	<5
				5<x<10
				>10

The target company general office classification and capacity management Guidelines