IN
PARTNERSHIP
WITH
PLYMOUTH
UNIVERSITY

Name: A.A. Yasiru Heshan Perera

Student Reference Number:10602294

Module Code: CNET233SL	Module Name: NETWORK SECURITY

Coursework Title: CNET233SL Project Report

Deadline Date: 9th April 2018	Member of staff responsible for coursework: Mr. Saliya Patabandi

Programme:

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.

10602294- A.A Yasiru Heshan Perera

10602165- R.Jegatheshan

10601896- B.M.U.S Basnayake

10601909- R.G.K.Dilshan

10601886- C.Shan Aluwihare

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 reg relating to Assessment Offences and that I am aware of the possible penalties for any breach 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 ha 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___________**

Acknowledgement

It’s our greatest pleasure to express our gratitude and appreciation towards everyone who has helped us and guided us into achieving successful completion of the project and gather knowledge. This has been a great experience we tackled and without the support and guidance, would have been an impossible task.

Firstly we would like to express our sincere gratitude to our member of staff who’s responsible for this module Mr.Saliya Patabandi for his active guidance and knowledge that was given to complete this report successfully.

Furthermore, we are extremely grateful for this wonderful opportunity, learning materials and facilities given by the NSBM and Plymouth University which was immensely helpful in carrying out this task.

Contents

Introduction

Purpose :

NSCS is a university which is located in Homagama and having branches in Colombo and as well as Kandy has many users. Therefore NSCS university wants to implement security devices and technologies that are required to secure all NSCS networks.

As the network security consultants for the university 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 centre 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.

What is network security?

Any activity designed to protect the usability and integrity of data is called network security. which includes hardware and software technologies. An effective network security manages access to the network and targets a variety of threats to stop them from disabling or corrupting the network.

How does network security work?

Combination of multiple layers of defences at edge and in network which each layer containing controls and policies. Only authorized users are allowed access to the network and the malicious acts are blocked from making exploits or threats.

Types of network security

- Access Control
- Antivirus and antimalware software
- Application Security
- Behavioural analytics
- Data Loss Prevention
- Email Security
- Firewalls
- Intrusion prevention systems
- Mobile device security
- Network segmentation
- Security information and event management
- VPN
- Web Security
- Wireless Security

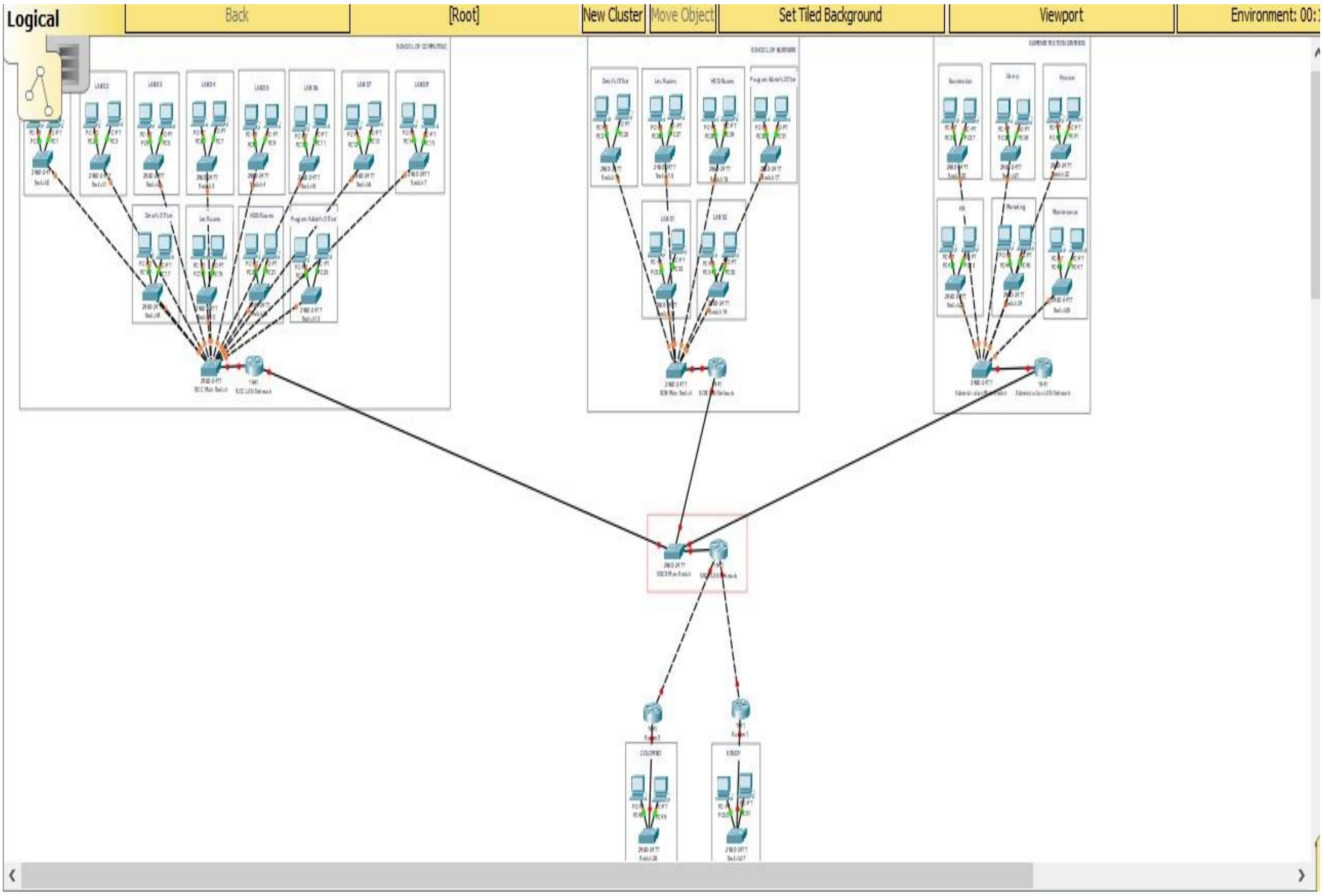
NSCS organization

Network infrastructure:

The NSCS has established their marketing office in Colombo 7 and Kandy and the main concern in whole is the concern of security networks within University premises. The management of NSCS is looking to give full control over ICT facilities and shares them between its marketing branches, so that services are made available for marketing offices.

The university concludes the School of Computing and the School of Business together with the Administration unit.

Current Network Diagram.

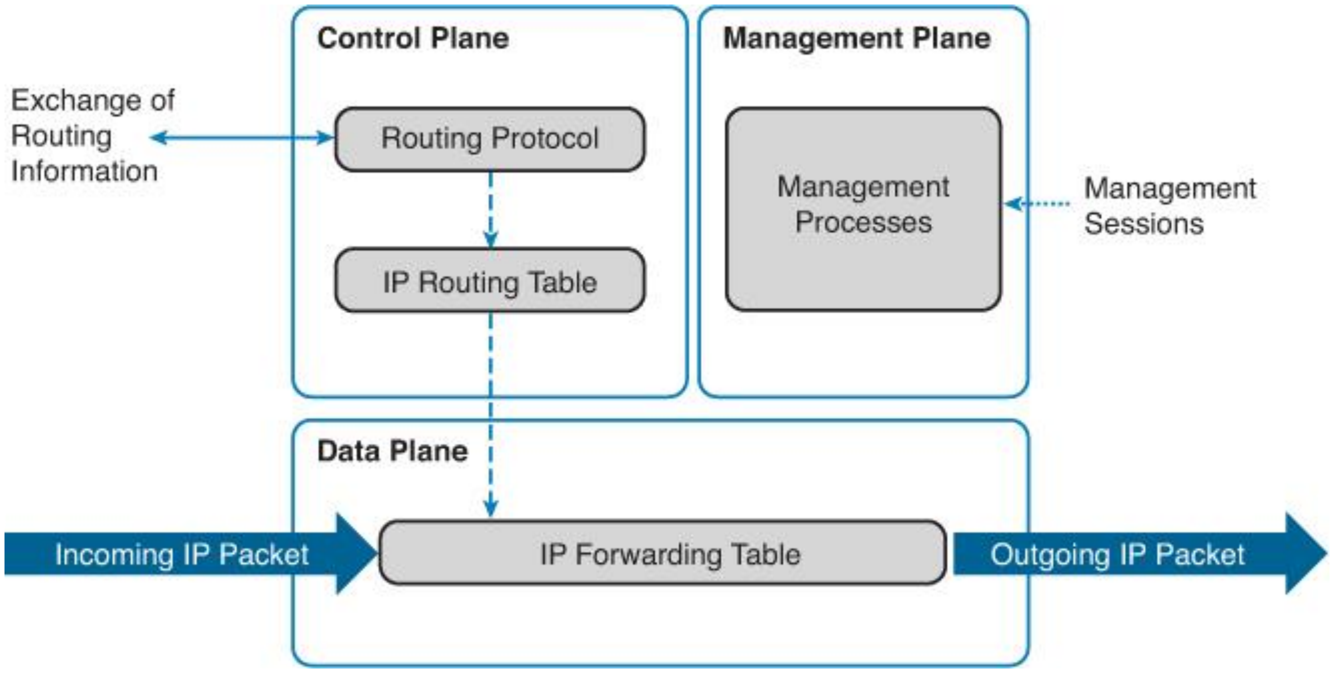


Network Foundation Protection (NFP)

NFP is a framework used to break the infrastructure down into smaller components and then systematically focusing on how to secure each of those components.

NFP is broken down into three basic planes (also called sections/areas)

- **Control plane** : Provides the capability to route traffic
- **Data plane** : Provides the capability forward traffic
- **Management plane :** Provide the capability manage devices

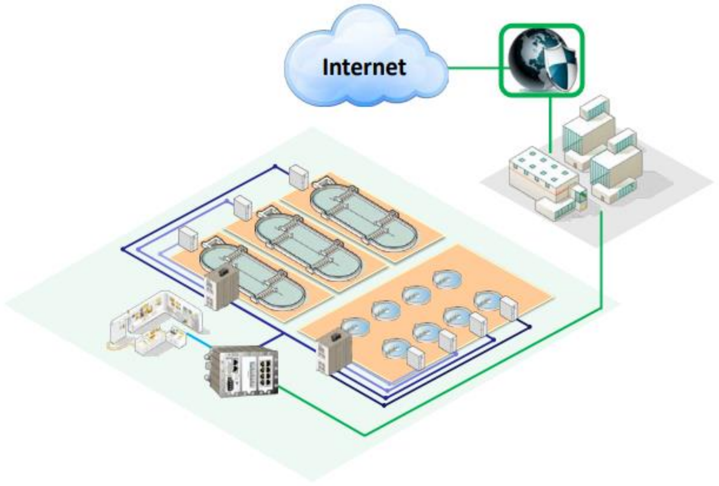


Internet Perimeter Protection

One of the most common components in a security program is identifying and protecting the outer logical and physical boundaries of an organizational location. There are different physical access controls to ensure only authorized personnel can enter.Perimeter can be present as a part of the network infrastructure.It will carry out connectivity to the internet.

There is a firewall connecting the local networks with an external network like Internet for office networks, or the office network if the local network is an industrial automation and control system (IACS).

Internet is a global system of interconnected computer networks. Otherwise can be define as collection of LAN networks working together as a wide area network and also that will content lots of unknown devices.



In this network solution a centralized internet connection is used at the headquarters and it is shared between the branches and there are a set of topographies and functions that should be applied to provide secure access to the internet.

Network architecture without perimeter security

- Flat network without segmentation
- Internal services publishing: data base
- No monitoring elements
- No inbound or outbound traffic filtering
- No malware or spam e-mail verification
- The remote client has direct access to the services Remote client

Network architecture with perimeter security

- Firewall installed
- DMZ and internal network
- Restrictive policy
- Anti-spam and antivirus installed
- NIDS installed in the three interfaces
- Segmentation of public services: Web and antivirus/anti-spam gateway
- Internal services relocated:

Firewall

- Network elements that define access policies to allow or deny traffic based on certain rules
- Two philosophies of use:

Restrictive policy (white list): denies all traffic except that which is specifically accepted

Permissive policy (black list): accepts all traffic except that which is specifically denied

Integrated Intrusion Protection System (IPS)

IPS is responsible to detect attacks based on different techniques by using their threat signature, traffic behaviour 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.

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.

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.

Data Centre Protection

Physical security also plays a large role with data centres. Physical access to the site is usually restricted to selected personnel, with controls including a layered security system often starting with fencing

Data centres 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.

Characteristics in data centre protection,

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

Cisco Adaptive Security Appliances can be used to implement these security configurations to a network. Service isolation should be configured therefore only the intended group of uses can access the data centre.

Network Access Security and Control

The Network Access Security intercepts the connection requests, which are then authenticated against a designated identity and access management system. Access is either accepted or denied based on a pre-determined set of parameters and policies that are programmed into the system.

NAC (Network Access Control) used for,

- Authentication and Accounting of network connections
- 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.

Problems in Current Network

Machines are slowed by Anti-virus where users of ABC company can disable automatic updates and stop antivirus software scanning. VPN access users have the protection where provided by local firewall enforcement. There is no anti-spyware and host intrusion prevention solution deployed.

Network Access Control Solutions

- Impulse SafeConnect
- Extreme Networks ExtremeControl
- Auconet BICS
- ForeScout CounterACT
- Pulse Policy Secure
- HPE Aruba ClearPass
- Bradford Networks' Network Sentry

Cisco Identity-Based Network Services (BNS)

Using the 802.1x protocol with Cisco enhancements, the network grants privileges based on user location or device. The benefits of IBNS,

- Allows different people to use the same PC and have different capabilities
- Ensures that users get only their designated privileges, no matter how they are logged into the network
- Reports unauthorized access

Cisco Unified Wireless Network (CUWN) Integrated Security

The Cisco Unified Wireless Network end-to-end security of the entire system by using architecture and product security features to protect WLAN endpoints, the WLAN infrastructure, client communication, and the supporting wired network.

Components

- Wireless LAN controllers
- Aironet Access Points
- Management (Prime Infrastructure)
- Mobility Service Engine (MSE)

Cisco Catalyst Integrated Security Features

All security features are built-in catalyst switches made by Cisco, this security features are . set of tools and configurations that can secure access to the network.

- Strong protection against common attacks
- IP Source Guard Protection against incorrect/malicious hard coded IP Address
- Raising the Bar on Surveillance Attacks – MAC-Based Attacks
- DHCP Snooping Protection against Rogue/Malicious DHCP Server
- Dynamic ARP Inspection Protection against Recognizance/ ARP Scan's

Cisco NAC Appliance

Network administrators can use the Cisco NAC Appliance to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users before they can access the network.

With Cisco NAC Appliance,

- Recognize users, their devices, and their roles in the network
- Evaluate whether machines are compliant with security policies
- Enforce security policies by blocking, isolating, and repairing noncompliant machines
- Provide easy and secure guest access
- Simplify non-authenticating device access
- Audit and report whom is on the network

Secure Mobility

Mobile technology has changed the IT world on how people work, live, play and learn, because of that they use mobile devices to connect to the organizations internal network. Therefore, it's compulsory to safeguard organization network to make sure these mobile devices don't affect the security of the network.

Mobile Device Challenges

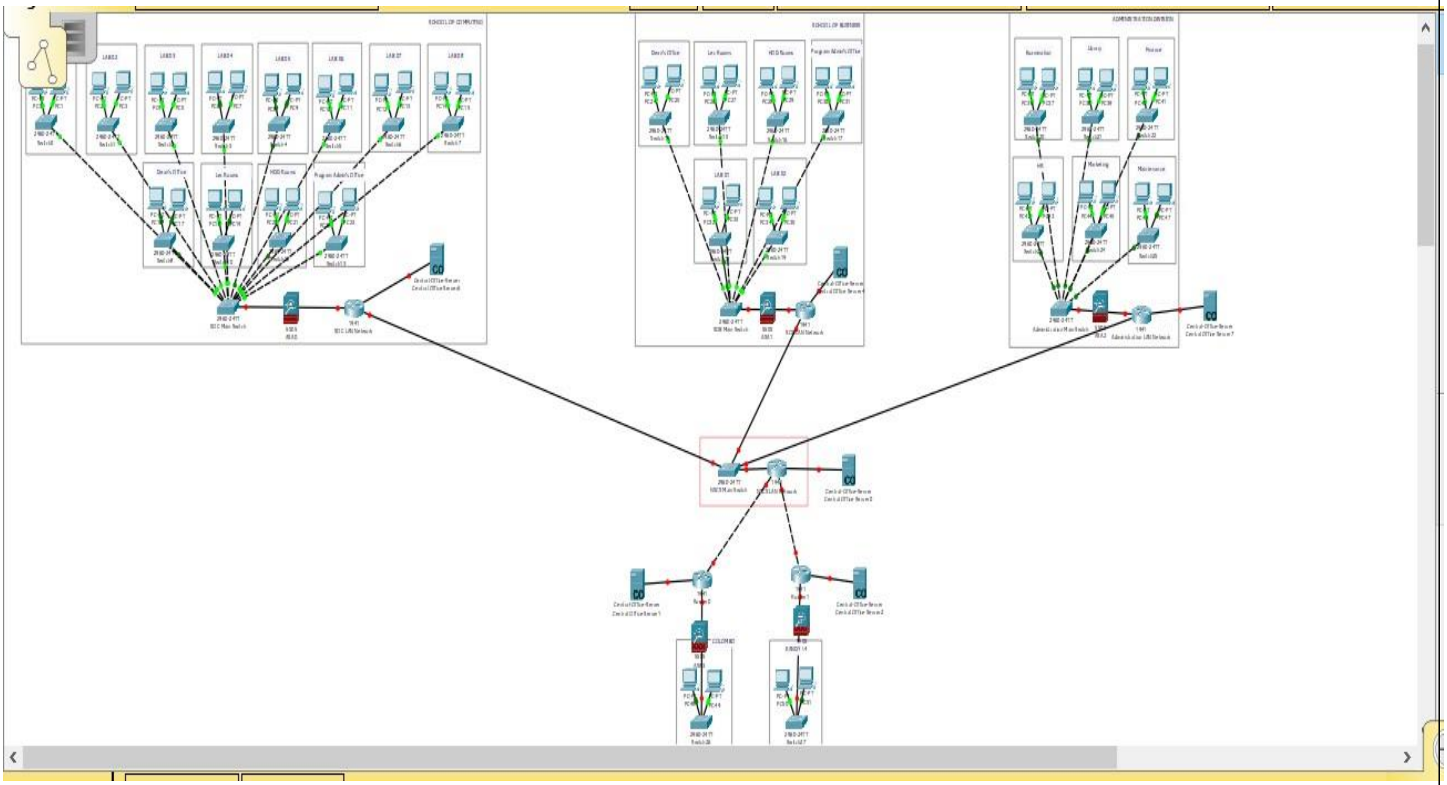
- Access policy enforcement on all devices.
- Reduce the resources needed to bring mobile devices on board.
- Delivering a great mobile business experience, even with network-heavy applications, large business customers, Mobile Phones.
- Mitigating security and privacy risks such as the loss of intellectual 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.

Solutions

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

- Produce services access and manage mobile devices and apps stores.

Suggest Secure Network



We use to implement cisco routers and switches to secure this university network, because cisco have high reputation and provide guaranteed security service for that. The branches and main University will be interconnecting using cisco devices..

We implement firewalls for each networks, because this network need to be high security and it should be filtered some web sites, viruses and malwares.

Conclusion

We've selected all the matching security features for the NSCS University network. Security of an organization network plays a vital role of its success.

All the security measures required can be achieved using the applications we've recommended on this report, implementing these standards tackles all the threats and vulnerabilities of the organizations network.

We are suggesting that the company should consider installing all of the exact proposed devices and brands to ensure that the network reaches the best security ad performance.

References

https://www.cisco.com/c/en/us/index.html

https://smbitsolutions.wordpress.com/

https://www.sap.com/index.html

https://ies.ed.gov/

https://searchcloudcomputing.techtarget.com/