# Table of Contents

[Table of Contents 1](#_Toc436395294)

[Task 1 6](#_Toc436395295)

[Introduction 6](#_Toc436395296)

[Management of Threats 6](#_Toc436395297)

[Vulnerability 6](#_Toc436395298)

[IT Department Staff Leaving Organization 6](#_Toc436395299)

[Spyware 7](#_Toc436395300)

[Spam 7](#_Toc436395301)

[Security Policies 7](#_Toc436395302)

[Review and management 7](#_Toc436395303)

[Access to system 7](#_Toc436395304)

[Vetting of staff 7](#_Toc436395305)

[Impact on productivity 8](#_Toc436395306)

[Legal proceeding 8](#_Toc436395307)

[Estimating Risk 8](#_Toc436395308)

[Penetration Testing 8](#_Toc436395309)

[Contingency planning 9](#_Toc436395310)

[Summary 9](#_Toc436395311)

[References 10](#_Toc436395312)

[Task 2 11](#_Toc436395313)

[Introduction 11](#_Toc436395314)

[Proposed Network Design 11](#_Toc436395315)

[Impact of Proposed Network Design 12](#_Toc436395316)

[Social Impact 12](#_Toc436395317)

[Organizational Trust 12](#_Toc436395318)

[Public relations management 12](#_Toc436395319)

[Law enforcement involvement 12](#_Toc436395320)

[Impacts on productivity 13](#_Toc436395321)

[Losses 13](#_Toc436395322)

[Summary 13](#_Toc436395323)

[References 13](#_Toc436395324)

[Task 3 14](#_Toc436395325)

[Current and common threats 14](#_Toc436395326)

[Awareness 14](#_Toc436395327)

[Update 14](#_Toc436395328)

[Patches 15](#_Toc436395329)

[Access Policies 15](#_Toc436395330)

[Maintenance of System 15](#_Toc436395331)

[Summary 16](#_Toc436395332)

[Task 4 17](#_Toc436395333)

[Introduction 17](#_Toc436395334)

[Technologies 17](#_Toc436395335)

[Domain Controller 17](#_Toc436395336)

[Role of DC in designed solution 17](#_Toc436395337)

[Read Only Domain Controller 17](#_Toc436395338)

[Role of RODC in the Solution 18](#_Toc436395339)

[DNS Server 18](#_Toc436395340)

[Role of DNS in designed solution 18](#_Toc436395341)

[Secondary DNS 18](#_Toc436395342)

[Role of DNS in the Solution 18](#_Toc436395343)

[Web Server: IIS 19](#_Toc436395344)

[Role of IIS in designed solution 19](#_Toc436395345)

[Network Policy Server (NPS): Radius Server 19](#_Toc436395346)

[Role of NPS in designed solution 19](#_Toc436395347)

[Dynamic Host Configuration Protocol (DHCP) 19](#_Toc436395348)

[Role of DHCP in the Solution 20](#_Toc436395349)

[FTP Server 20](#_Toc436395350)

[Role of FTP server in the solution 20](#_Toc436395351)

[VPN Server 20](#_Toc436395352)

[Role of VPN in designed solution 20](#_Toc436395353)

[IPsec Policy 20](#_Toc436395354)

[Role of IPsec Policy in designed solution 21](#_Toc436395355)

[Certificate Authorities 21](#_Toc436395356)

[Role of Certificate Authority in designed solution 21](#_Toc436395357)

[Firewall: MS Firewall 21](#_Toc436395358)

[*Network Components* 22](#_Toc436395359)

[IP addressing 22](#_Toc436395360)

[User 22](#_Toc436395361)

[Organizational Units and Groups 23](#_Toc436395362)

[Designed Solution [2.1] 23](#_Toc436395363)

[Design Evaluation 24](#_Toc436395364)

[Task 6 25](#_Toc436395365)

[Introduction 25](#_Toc436395366)

[System Test Logs 25](#_Toc436395367)

[**What was tested:** ***Web Server Policy [IIS]*** 26](#_Toc436395368)

[Summary 32](#_Toc436395369)

[Task 7 33](#_Toc436395370)

[Interlocution 33](#_Toc436395371)

[Access Control 33](#_Toc436395372)

[Logical Access Control: System Access 33](#_Toc436395373)

[ACL 33](#_Toc436395374)

[Group Policies 35](#_Toc436395375)

[Password 36](#_Toc436395376)

[Account Restriction 37](#_Toc436395377)

[Physical Access Control: Physical Access 37](#_Toc436395378)

[Audit 37](#_Toc436395379)

[Physical Access Audit 37](#_Toc436395380)

[Logical Audit 38](#_Toc436395381)

[Summary 38](#_Toc436395382)

[Task 8 39](#_Toc436395383)

[Introduction 39](#_Toc436395384)

[System Monitoring 39](#_Toc436395385)

[Traffic 39](#_Toc436395386)

[Load 40](#_Toc436395387)

[RAM Monitoring 40](#_Toc436395388)

[Server Monitoring 41](#_Toc436395389)

[Ongoing Network Management 41](#_Toc436395390)

[WireShark 41](#_Toc436395391)

[PRTG Network Monitor 41](#_Toc436395392)

[Summary 42](#_Toc436395393)

[Task 9 43](#_Toc436395394)

[Introduction 43](#_Toc436395395)

[Self-Evaluation 43](#_Toc436395396)

[Devices 43](#_Toc436395397)

[Recommendation 43](#_Toc436395398)

[Router 43](#_Toc436395399)

[Switch 44](#_Toc436395400)

[Groups 44](#_Toc436395401)

[Recommendation 44](#_Toc436395402)

[Services 45](#_Toc436395403)

[Recommendation 45](#_Toc436395404)

[Mail server (Email Server) 45](#_Toc436395405)

[Additional Recommendations 45](#_Toc436395406)

[Physical Security 45](#_Toc436395407)

[Move to Cloud 46](#_Toc436395408)

[Conclusion 46](#_Toc436395409)

[References 47](#_Toc436395410)

# Task 1

**Evaluate** a currentsystem’s network security. [1.1, M1]

# Introduction

Nepal Commercial Investment Bank is a joint venture between Nepalese and French partners. It has dedicated information and technology department that manages IT infrastructure of the bank. This document evaluates various components of network security. Evaluation emphasize on management of threats, various security policies, security’s impact on productivity and risk estimation process.

# Management of Threats

Any network implementation process goes through threat analysis process. Threats imposed on network infrastructure can be addressed via various threat management techniques. For that, various threats on the system need to be identified evaluated. Following are the various commonly found threats on any network environment.

## Vulnerability

According to an article by monster dot com (n.d.) vulnerability in the system is a great threat to system. There is possibility of exploiting vulnerability of the system to cause damage in the system. Here vulnerability refers to weaknesses or flaws of the system. Flaws in hardware or software of the system causes weaknesses in the security of overall network. Sometimes, vulnerability can be created by improper security configuration in the system. Network environment of the NCIB will be monitored and analyzed regularly to identify potential vulnerabilities of the system.

## IT Department Staff Leaving Organization

This is a great threat to security structure when a worker that knows too much about institute leaves their job. Worker leaving organization due to disagreement may want to take revenge on organization by providing critical information to rival companies. Ex-worker can leak company policies, client details, account details and network details to rival that may lead to serious loss of organization. An article by Dorbian (2014) published in CFO, tech laborers have utilized their passwords to hurt an ex-boss — decimating information, acquiring client data and purchasing products and administrations utilizing client account. To control this, it is important to disable accounts of ex-works. If he is from IT department, it is nice practice to change administrative passwords and other security measurements.

## Spyware

According to Rouse (n.d.) spyware is program that gathers user’s information and transmit them to someone else. This types of program monitors internet activities and remains hidden from the user. What makes spyware a genuine threat is that it can gather information about email addresses and password or even credit card details. In critical sector like bank, spyware can steal critical information. This type of program can be downloaded from emails, instant messaging or USB drives.

## Spam

Nowadays, spam is a common threat to computer system. It is basically electronic version of junk mails (Kaspersky, n.d.). These mails come as advertisement but it can deliver viruses, spywares etc. which can steal user information. Anybody should not publish private email address publicly.

# Security Policies

## Review and management

According to CONTROLRISK (n.d.) security review accesses network system environment, methodologies and approaches to identify required resources for the security. This is process of identifying security related issues in the system. This process analyze required security policies for the optimal security of the network infrastructure. Following are the review and management approach practiced by current system:

## Access to system

Security of network environment depends on security policies that allows or deny access to resources. This process analyze who/how/when should be granted access to system and what should not be granted. Proper implementation of access policies greatly enhances the security of system. COMPTECHDOC (n.d.) writes, security policies determines security configuring of both hardware and software and defines what should be done or what should not be done to optimize system security.

## Vetting of staff

Staff recruitment process has great influence on security of any organization. As competition is high, organization can choose staff from number of candidates. When recruiting a staff for an important role, it is not only necessary to look into his/her qualification but also look into his/her background. This includes checking his criminal records, credit records, verification of certification etc. It is important to look for staff with clean background especially for critical department such as IT.

According to Anderson (n.d.) while vetting a staff it is important to follow legal guideline of the country. Employer cannot ask for reports or certificates forbidden by law of that country. It is always nice practice to have candidate sign consent form before vetting them. Nepal commercial investment bank has prepared and follows organizational policy while vetting of staffs.

# Impact on productivity

Any threat on network security has impact on productivity of organization. Attack on system can damage information, steal information or damage whole network. When this happens, as discussed earlier, it has social impact leading loss of clients which ultimately makes impact on economy of organization.

Organization needs to recover data or system after such attack which makes direct impact on productivity. Recovery period can be from some hours to some days, during these period organization cannot work smoothly and causes both social and economic loss. Breach of security in network of NCIB would have great negative impact on service and productivity of NCIB. It will eventually cost NCIB loss of customers, image, service etc.

## Legal proceeding

Legal proceeding procedure practiced by organization to seek assistance from law and order. It is necessary for any organization to follow required legal proceeding to secure system from cyber-crime losses. Legal proceeding offers organization legal preparations to fight against losses caused by attack on system.

# Estimating Risk

Just like security review and management optimizes security of network environment, it is essential to estimate risks imposed by various vulnerabilities on system. This process helps to prevent potential threat on the system. Risk estimation and planning is done through identification, analyze and evaluation process of the system review. NCIB network will go through various test procedures to identify potential risks. Current system practices following risk estimation techniques:

## Penetration Testing

CORESECURITY (n.d.) defines penetration testing as process of testing a system by safely attempting to exploit system vulnerabilities of OS, configuration, implementation approach, flaws in resources etc. Penetration testing includes testing of user behavior that can be exploited to gain unauthorized system access. Both manual and automated techniques are practiced to perform penetration testing. Logs created during testing are critically evaluated to identify potential risk on the security of the IT infrastructure.

## Contingency planning

MINDTOOLS (n.d.) suggests, for any displeasing events like loss of data, customer, supplier etc. contingency plan allows to recover from the loss. Evaluation of risk estimation helps to identify potential risk and develop contingency plan. Example of contingency plans includes effective data backup plan, system restore plan, data recovery plan, read-only servers etc. Good contingency plan helps to improve productivity by limiting impact of security breach. Contingency plan for NCIB will be planned and managed to minimized impact of security threats. Data backup, alternative data routes etc. should be managed to secure the network.

# Summary

This document evaluated various network security threats and security management related measurements of the network. Various security threats has been evaluated. Vulnerabilities of network system allows hackers/attackers to get unauthorized access to system through weaknesses in system. Various testing and monitoring tools are used for analyzing and identifying potential risks in the system. Network environment utilizes security policies to mitigate potential risks. Security of the network environment has such significance due to its impact on productivity. Any security catastrophe will cause huge impact on services provided by bank. To provide optimal service quality and secure service, bank will require to design and implement proper network environment.

# References

* CONTROLRISK (n.d.) Security Reviews and Audit [Online] Available: <https://www.controlrisks.com/en/services/security-risk/security-risk-consulting/security-reviews-and-audit> Accessed [11/25/2015]
* CORESECURITY (n.d.) Penetration Testing Overview [Online] Available: <http://www.coresecurity.com/penetration-testing-overview> Accessed [11/25/2015]
* Dorbian, I. (2014) Vengeful Employees an Increasing Threat to Network Security [Online] Available: <http://ww2.cfo.com/technology/2014/09/vengeful-employees-increasing-threat-network-security/> Accessed [11/25/2015]
* Kaspersky (n.d.) Understanding Spam and Phishing Scams [Online] Available: <http://usa.kaspersky.com/internet-security-center/threats/spam-phishing#.VleApOJpVf4> Accessed [11/25/2015]
* MINDTOOLS (n.d.) Contingency Planning [Online] Available: <https://www.mindtools.com/pages/article/newLDR_51.htm> Accessed [11/25/2015]
* Monster (n.d.) Computer Threats [Online] Available: <http://hiring.monster.com/hr/hr-best-practices/monster-training/security-center/avoid-computer-threats.aspx> Accessed [11/25/2015]
* Rouse, M. (n.d.) spyware [Online] Available: <http://searchsecurity.techtarget.com/definition/spyware> Accessed [11/25/2015]
* Vengeful Employees an Increasing Threat to Network Security

# Task 2

**Discuss** potential impact of proposed network design. [1.2]

# Introduction

Nepal commercial investment bank plans to achieve its main mission of being leading bank of Nepal by integrating state of are networking environment. This document proposes network design for the bank to satisfy their business requirements. Proposed system design utilizes various server technologies to enhance its quality service.

# Proposed Network Design

Proposes network design plans to centrally manage users and resources through Domain server. Network will consist of DNS server to provide domain name service. To achieve business requirements of the bank, proposes design consist of web server. IIS server will serve as web server to publish and support web application. To securely connect with branch offices and distribute its services through ATMs, VPN server is utilized. Appropriate router, switches and firewalls are used in design to support network infrastructure.

Bank has critical information that need to handle with extensive care. Administrator will enforce various security policies and utilize technologies to enhance security of the network. Administrator will user Network policy server to impose security policy on the network environment. To optimize security of the network, various certificates will be installed. Radius server and IPsec policies are planned to secure VPN connection. Proposed design emphasize on quality service and network security, potential impacts of this network design is discussed in this document.

# Impact of Proposed Network Design

# Social Impact

## Organizational Trust

Organizational trust is how organization trust their employees and how employees trust organization. Peppers (2013) explains, organization trust signifies how an employee can rely on his/her fellow manager/co-worker. Proposed network design plays role in organizational trust within NCIB. Proposed system centrally and securely manages user account information and resources. Each employee will have their own user account and this will secure their privacy. Enhanced privacy security and data security will make positive impact on employee’s trust on organizations and fellow co-workers. Proposed design allows data sharing, resource sharing etc. which enables staffs working together, eventually increasing organizational trust. Optimized quality service and data security also enhance bank’s profile to build corporate trust and financial trust.

## Public relations management

Proposed network design emphasize on the quality of service as well as information security. Fast and quality service helps organization to develop better public relation. Enhanced bank’s profile will make positive impact on customer’s view toward bank. As network design has VPN server to allow secure connection with bank, customer will be able to gain banking service through brank office too. Public can rely on bank’s network security.

## Law enforcement involvement

Proposed network design has strict security policies. When a staff tries to take advantage of his/her position to gain access to system for wrongdoing, law enforcement involvement is imminent. Security monitoring will keep track of network security and in the event of cybercrime from inside or outside, organization can rely on law and order to seek justice and punish the guilty person. Fighting cybercrime will make positive impact on society.

# Impacts on productivity

Proposed network design is based on satisfying business requirement of the bank. Network design will provide secure and quick service to its customers which will make positive impact on productivity of the bank. Additionally, design supports branch extension and ATM centers which allows extend service area.

## Losses

There are various types of losses that influences productivity. Proposed network is designed to make positive impact on these potential losses. Improper design can led to losses such as service loss, data loss, loss of goodwill etc. To reduce impact of these losses, proposed design has allows data backup, system back up. To prevent service loss, network design utilizes technologies like read-only servers. Through positive organizational trust and public relation loss of good will can be prevented.

# Summary

This paper discusses various types of impact due to threat on the system. To discuss the impacts, a network design for NCIB has been planned. Analyzing the planned network security system helps to identify possible impacts of threats on the system. Different aspects of both social and economic impact of the threats on the

# References

Pepper, D. (2013) *the five keys to a successful Google team* [Online] Available: <https://www.linkedin.com/pulse/five-keys-successful-google-team-laszlo-bock> Accessed [11/26/2015]

# Task 3

**Discuss** the current and common threats and their impact. [1.3]

# Current and common threats

In context of computer system, threats are anything that has potential to cause harm to the system or network. If these threats are not taken seriously, computer system or whole network can become easy target for hackers, attackers.These hackers or attackers perform unauthorized access to system to gain access to private data and cause damage to the system. This document discusses available methods to medicate threat impact on the system. Impact of such methods are also discussed.

## Awareness

Educating employees about threat and their impact is one of the key and most common phase to minimize threat impact. Employees tends to become victim of spam and phishing attack due to lack of awareness about network security threats. They become prey by clicking attracting links, failure to separate fake or genuine sites or installing suspicious software in the system. NCIB must organize awareness program to make staffs aware about various threat and their impact on organization. Awareness program also teaches about social engineering, how they work and how they can avoid them. Awareness program on the network security of the bank will enable employees to understand the significance of network security in the bank.

## Update

An update is a product file that contains fixes for issues found by different clients or the product engineer. Update fixes the problem and keeps the issues from happening the system. Quite often updates are free as they are built the fix problem in application brought by client. When update or patches for a software is officially release, it comes with security and performance enhancement. Updates generally targets to improve known vulnerabilities of the system. There are various type of update system that need to be utilized by NCIB ensure enhanced security and performance. Service pack update addresses issues related with application service and performance. Hotfixes are updates that addresses specific issue of the product and security update is used for enhancing security aspect of the product.

Each day attacker tries to find new vulnerability in the system and if updates are not applied to the system, we leave our system vulnerable to attack. Technical of NCIB should always test updates and patches on virtual system before deploying in the system as some updates are not compatible with existing hardware and software causing system instability. Technical team should send emails to all user regarding update and maintenance schedule.

## Patches

Patches are files that is used for fixing issues with application. When beta version of system is released to users, and later official release is done. Users find bugs in the system and report to developer. Now to address those bugs, developer provide patches which is similar to hotfix. Though patches is not the best solution as sometimes it cannot fix all bugs, developer addresses the bug in next release of the system.

## Access Policies

Maintaining policy to allow access to network resources one of the most common threat prevention technique. Technical team should perform critical security analysis to evaluate access policy for the organization. Access policies such as not allowing an untrusted user to connect to account computer or account network can improve resource security. Use of proper configuration on router, firewall can also prevent unwanted situation. There are two types of access control policies that can be practiced to improve network security. System access control maintain security of the network on system level by deploying policy configurations whereas physical access control maintains security of the system by deploying physical security tools and techniques.

NCIB should always deploy access policies on both software and physical level to manage network security threat. It is necessary to plan proper access policy for physical access too. As physical damage on IT infrastructure can create problems in the network.

## Maintenance of System

System should be maintained on regular basis as unmanaged system are vulnerable to attack. Updates/patches should be applied on system on regular basis (sooner as possible). Recognizing requirement of system upgrade is also another important part. Older system can reduce performance capacity of the network. If system is attacked somehow, maintenance of the system should be done as soon as possible to get network back to safe position. Giving importance to system maintenance can mitigate threat and their impact. NCIB will use various monitoring tools and techniques to analyze system activities and identify need of maintenance of the system. Maintaining the system for NCIB will help to ensure optimal security of the system as well as optimal service quality.

# Summary

When network security of an organization is breached, it makes some serious impact on the organization and network. Organizations such as bank, data centers etc. loses their corporate/individual trust. Managing public relation on during these situation is really hard as trust is highly dependent on network security. This may result loss of large number of client and damage in organization reputation.

It is organization’s responsibility identify, evaluate and plan proper threat management policy to mitigate threat impact on network. Organization should aware its staffs about network potential threats and their impact. Administrator should take advantage of system monitor tools to identify maintenance requirement. And lastly, security and service updates/patches should be applied as soon as possible.

# Task 4

**Design** a network security solution to meet given specification. [2.1]

**Evaluates** the design and **analyze** the feedback **for** improvements [2.2, M2]

# Introduction

Nepal commercial investment bank is has existing network environment to support their business. Now it wishes to upgrade their IT infrastructure by implementation of more secure and reliable network design. This document designs a network security solution for NCIB and justifies its selection.

# Technologies

Different tools and techniques has been utilized while planning and designing secure network environment for NCIB. Each components of the designed network has been evaluated to potential improvement feedback has been provided.

# Domain Controller

Hosts accessing the resources of system are managed through a controller, called Domain controller. Active directory service of domain controller is a repository that stores network object information such as user accounts, groups, computer etc. User needs to provide right combination of username and password to access a system, these information are stored in active directory. Administrators can enforce various policies to enhance security of system. A user can only perform those activities within a network that are allowed by domain controller. Security policies such as user right and privilege, group policies are applied through domain controller.

## Role of DC in designed solution

Designed network security solution of NCIB utilizes domain controller technology to maintain and secure the network environment. Domain controller in the network is in control of lots of things like providing access rights, planning and implementing group policies and maintaining user account, group, and OU information.

# Read Only Domain Controller

Read only domain controller (RODC) is read only copy of domain controller. Client can't compose changes in RODC and it gives ordinary active directory functionality for branch offices. As its name says it’s naturally Read-only duplicate of the organization DC. So the progressions making on branch site RODC won't influence DC operations. So basically its keep all the information about the DC characteristics in Branch-DC as read-only duplicate.

## Role of RODC in the Solution

Association between branch office and focal office can break whenever, for example, regular catastrophe, power disappointment, or issue in ISP system and so forth. In cases branch office still needs to up and running and here is the RODC is helpful. RODC would recreate the fundamental DC and sets up the space system without primary DC. Also RODC can be utilized as security layer as a part of bank as changes made by assailants in RODC is not spared in Domain. Other part of RODC in branch is to introduce secondary DNS to give DNS service even if there is an occurrence of system disappointment with main **DNS**.

# DNS Server

To provide name resolution service in the network DNS server technology has been utilized. DNS server in the network will convert machine readable IP address of resources into user-friendly names. Hosts that are part of domain system will have human friendly FQDN (fully qualified domain name). These names are not case sensitive.

## Role of DNS in designed solution

Designed network solution for bank has utilized DNS server to convert host machine’s IP addresses into human friendly names. This will allow administrator to access resources using names and apply privilege and policies. For example, printer1 with IP address of 10.10.10.10 will have friendly name like printer1.ncib.com.

# Secondary DNS

Like RODC and DC, Secondary DNS is read only duplicate of DNS server. It is just read only duplicate means DNS records can't be composed to it straightforwardly. It handles DNS questions from clients when main DNS server is down.

## Role of DNS in the Solution

Proposed design solution has secondary DNS servers in branch offices. This is to ensure host machine can use DNS service even in situation of main DNS server failure.

# Web Server: IIS

A web server is used for publishing web pages that can be accessed by intranet users. In designed network for NCIB, IIS server has been chosen as webserver. IIS is short form for Internet Information Server which is Microsoft’s web server and runs in Windows NT system. IIS server includes web platforms including IIS, ASP.Net, WCF, and SharePoint services. IIS server enables sharing information through internet, intranet or extranet.

## Role of IIS in designed solution

1. IIS server will allows publishing bank’s ASP.NET based web application within the secured intranet.
2. Banks Official website will be published for customers to provide information and internet banking

# Network Policy Server (NPS): Radius Server

Network Policy Server (NPS) can be used for authorizing, authenticating, and accounting radius users by implementing NPS as Remote Authentication Dial-in-user Service (RADIUS) server. Radius users can be various servers such as access server, dial-up server, radius-proxy or wireless access point. It provides central authorization and authentication service for all radius client’s access request. All request and accounting record are stored in local log. This information can also be store in MySQL database for further analysis.

## Role of NPS in designed solution

1. Radius server in designed network will be used for implementing more secure VPN.
2. It tracks access request to from various radius clients which will help analyzing traffic and user behavior to identify potential risks.

# Dynamic Host Configuration Protocol (DHCP)

A DHCP server is administration supplier that consequently allot IP addresses to clients. Moreover, DHCP can appoint subnet mask, IP address and DNS address to client. This administration diminishes the effort requires for manual configuration of all clients. Hosts with DHCP enabled, can automatically ask for DHCP server to appoint setting related to IP addresses. Manual configuration of IP address to all resources can be time consuming and can create complications sometime only due to small mistake.

## Role of DHCP in the Solution

Manual assignment of IP address, gateway address, DNS address etc. to all resources and clients in NCIB bank would require large amount of time and effort. And there are chances of assigning same IP address multiple time by mistake. Current system would use DHCP server to allocate IP addresses to client computers.

# FTP Server

FTP is short form of File transfer protocol. It is the standard Internet convention for exchanging document between client and server. FTP is a piece of the TCP/IP protocol suite. TCP/IP is the protocol convention that runs the entire Internet. There are various smaller conventions that keep running on top of TCP/IP, for example, email, HTTP, and Telnet. FTP is one of these. Its sole capacity is to move a document from a server to a customer (download) or from a customer to a server (upload).

## Role of FTP server in the solution

In NCIB network, FTP is used for file transfer between computers in network. NCIB can utilize FTP to trade records between PC records, exchange documents between a record and a desktop PC

# VPN Server

To connect to a system remotely and securely, VPN technology is utilized. It enables connection with remote network through public network such as Internet. It is very common method to securely connect to office network from home. While connecting with VPN, data are encrypted and are travelled through VPN tunnel which helps to secure data from hackers. Only authentic receiver can decrypt and access the information.

## Role of VPN in designed solution

NCIB bank has number of branch offices and ATM centers all over the country. It is impossible for head office to physically connect with all those branch offices. With implementation of VPN, head office can connect to its branch offices through Interne and act as if they are connected locally. This will allow Domain controller to control all branch network centrally. With broad service reach, NCIB will have access to larger potential customers.

# IPsec Policy

IPsec policy basically set rules of for administrating networks via use of IPsec protocol. IPsec protocol uses Public Key Encryption to secure TCP/IP packets traveling in the network. IPsec is mainly used for enhancing security of network environment. IPsec Policy enables management of IPsec implementations. In domain based network, IPsec policies can be applied using Group policy object.

## Role of IPsec Policy in designed solution

IPsec Policy in NCIB is utilized for securing the network and securing critical information. One of the key disadvantage of using IPsec is it use encryption and decryption to secure information which causes extra CPU load and requires more time due to larger packet size and encryption/decryption process. Hence while choosing hardware component IPsec requirement also need to be considered.

It is also essential to keep in mind that older IPsec algorithms are no more secure method hence administrator should use suitable and secure algorithms. Following are the need of IPsec in designed network security system:

1. Access from untrusted computers can be prevented with help of IPsec policy.
2. Critical information can be encrypted before transmission.
3. IPsec policies will help monitoring and securing all incoming and outgoing traffics along with firewall

# Certificate Authorities

Certificate Authorities also abbreviated as CA is an organization that issues digital credentials. This digital credentials (certificates) allows companies, people or devices to represent their authentic online identity. Millions of certificates are issued by CA each year, used for securing communication, transactions and protecting information.

## Role of Certificate Authority in designed solution

CA helps to guarantee that the two parties trading data are actually who they claim to be. In designed network, Certificate authority verifies identity of user, machines or applications. Bank can use active directory certificate service to enhance security for webservers. CA uses information stored in active directory such as user accounts and security groups.

# Firewall: MS Firewall

Firewall system monitors and control both incoming and outgoing network traffic. Firewall is either hardware or software. It prevents access from untrusted resource. Both hardware and software Firewall is utilized. Hardware firewall is used before connection with public network where windows firewall is used for securing network internally. Various servers in network will use windows firewall to allow or deny access from other computers. This will block access to server computer from unauthorized computer and create complications. Use of firewall will enhance network security both internally and externally.

# Network Components

## IP addressing

IP addressing is process of allocating IP addresses to network resources. In NCIB network, dynamic IP address is distributed to client computers. For server computers, static IP address is allocated for the system stability. IP address plan for the system in given below.

|  |  |  |
| --- | --- | --- |
| **Head Office** |  |  |
| **Machine** | IP **Address (Range)** | **Subnet Mask** |
| Domain Controller | 10.10.10.1 | 255.255.255.0 |
| DNS | 10.10.10.2 | 255.255.255.0 |
| VPN | 10.10.10.3 (Adapter 1)  192.168.1.1 (Adapter 2) | 255.255.255.0 |
| DHCP | 10.10.10.5 | 255.255.255.0 |
| IIS Server (Web Server) | 10.10.10.6 | 255.255.255.0 |
| CA Server | 10.10.10.9 | 255.255.255.0 |
| FTP Server | 10.10.10.7 | 255.255.255.0 |
| Client Computers | 10.10.10.10-10.10.10.254 | 255.255.255.0 |
| **Branch Office** | | |
| **Machine** | IP **Address (Range)** | **Subnet Mask** |
| RODC | 192.168.1.5 | 255.255.255.0 |
| VPN | 10.10.10.101 (Adapter 1)  192.168.1.2 (Adapter 2) | 255.255.255.0 |
| Read-Only DNS | 192.168.1.6 | 255.255.255.0 |
| DHCP | 192.168.1.7 | 255.255.255.0 |
| Client Pcs | 192.168.1.10-192.168.1.1254 | 255.255.255.0 |

## User

User accounts will be created and maintained in Domain Controller through active directory according to requirement.

## Organizational Units and Groups

Following are the OU/and groups planned for the network. Additional groups can be create in future if required.

|  |  |
| --- | --- |
| **OU/Group** | **Description** |
| HR | This is security group consisting user accounts of staffs for HR department |
| IT | This is security group consisting user accounts of staffs for IT department |
| Sales/Marketing | This is security group consisting user accounts of staffs for Sales and marketing department |
| Finance | This is security group consisting user accounts of staffs for Finance department |

# Designed Solution [2.1]

Network security solution for the given scenario is prepared in separate page below.

# Design Evaluation

To design proper network security system for NCIB various server technologies and security technologies are identified and utilized. Domain controller is employed to control the network and store user account information using active directory. DC also used for applying various security policies to enhance network security. Design also consists of IIS, DNS server and VPN server to satisfy business requirement of NCIB. In addition, design also utilized security components such as firewall, polices, IPsec and Certificate Authority to secure the network environment.

# Task 6

Systematically **test** the complex network security solution and then **document and analyze** the test results. **[3.2, 3.3, D1]**

# Introduction

Propose network security design for the NCIB has been implemented. Before handling the system to the bank and before bank move to the new system, it is must to carryout test on implemented system. Testing the network will enable to study the status of the network environment. If there is any misconfiguration issue with any policy setup, service or server setup, testing will help to identify them and report them as a test log. This document tests the newly implemented system and analyzed the test results.

# System Test Logs

|  |  |  |  |
| --- | --- | --- | --- |
| **What was tested: *IPsec Policy*** | | **Date: 2015-11-27** | |
| **S.N.** | **Expected Output** | **Actual Output** | |
| 1. | Two system should able to ping each other when IPsec policy is not enabled | Ping successful | |
| E:\ISMT\4th Sem\Network Security\Assignment\ScreenShots Task 5\before using ip sec policy.JPG | | | |
| 2. | Ping fail should occur when IPsec policy blocks the pinging | Ping Failed | |
| E:\ISMT\4th Sem\Network Security\Assignment\ScreenShots Task 5\after using ip sec policy.JPG | | | |
| **Analysis:** IPsec policy can be enforced to a host of a domain network to ensure secure connection between client and server. To test IPsec policy status in the developed system, Port used for pinging was blocked using IPsec. Before test client was able to ping the server. And after enforcing the IPsec rule, pinging failed replying request time out. This test shows IPsec policies are working correctly in the new domain network environment. | | | |
| **What was tested:** ***Web Server Policy [IIS]*** | | **Date: 2015-11-27** | |
| **S.N.** | **Expected Output** | **Actual Output** | |
| 1. | Published website should be accessible if any policy is not enforces | Website access successfull | |
|  | | | |
| 2 | User authentication should after implementation of  Windows authentication method | Website asked for user authentication | |
|  | | | |
| 3 | Website should be accessible after correct authentication | | Website is accessible |
|  | | | |
| **Analysis:**  A webserver is a server that publishes webpages. Developed system uses IIS server as Web server to provide web services. To test configuration of the web server and its security, first website was published with anonymous authentication and client was able to access the system. To test the security, window authentication was enabled. Now, client required to provide authentication information to visit the website. This test demonstrated that both webserver and web server security is configured correctly. | | | |
| **What was tested: *Certificate Authority*** | | **Date: 2015-11-27** | |
| **S.N.** | **Expected Output** | **Actual Output** | |
| 1. | Should show report of certificate being installed | A massage displayed with successful certificate installation | |
|  | | | |
| **Analysis:**  Most often people implement network designs with firewall system and does not care about internal network. What they have to understand is intruders can breach firewall security (through malware application). For this sort of unpleasant situation, internal network should be encrypted as much as possible. Developed network system user certificate to indemnify identity of client users. Test was carried out to view certificate installed which was successful. This test demonstrates successful configuration of Certificate Authority. | | | |
| **What was tested: *Security Policies*** | | **Date: 2015-11-27** | |
| **S.N.** | **Expected Output** | **Actual Output** | |
| 1. | All group policies should be displayed in Group Policy Management | Group policy management displays all group policies | |
|  | | | |
| 2. | Accessing Run menu should be disabled for users from Finance group | Users are not allowed to access run menu | |
|  | | | |
| 1. | Users are only allowed to access system during Monday-Saturday(8AM-5PM) | Accessing the system is not allowed in denied time | |
|  | | | |
| **Analysis:**  Various security policies has been managed in then newly implemented network. To test each policies, extreme condition was chosen. Trying to access the system while policy forbids it showed denying access to user showing warning massage. Similarly, trying to access denied service resulted warning massage. All test results were positive which means, network is configured correctly to support security policy management. | | | |
| **What was tested: *FTP Server*** | | **Date: 2015-11-27** | |
| **S.N.** | **Expected Output** | **Actual Output** | |
| 1. | FTP site should be accessible while any policy is not enforces | FTP is accessible | |
|  | | | |
| 2. | User authentication should require after implementation of windows authentication | Access required user authentication | |
|  | | | |
| 3. | After providing right authentication information access to FTP should be allowed | Access allowed | |
|  | | | |
| **Analysis:**  FTP server is used for file transfer between computers through web browser. Implemented system uses IIS service to provide FTP service. To test the system, FTP was published without any security policy and all client were able to access the system. Then implemented authentication system, FTP access required user authentication. Test results shows FTP server and FTP server security has been configured correctly. | | | |
| **What was tested: *VPN Server security with NAP*** | | **Date: 2015-11-27** | |
| **S.N.** | **Expected Output** | **Actual Output** | |
| 1. | VPN connection should be allows when no deny policy applied in NAP | VPN is accessible | |
|  | | | |
| 2. | VPN access should be denied when NAP policy denies the user/group to use VPN | Access Denied | |
|  | | | |
| 3. | VPN connection should be allowed when NAP policy to allow the user/group VPN connection is created | VPN connection allowed | |
|  | | | |
| **Analysis:**  VPN Server is used in developed network to provide secure connection between branch and main office. To enhance the VPN security, NAC (Radius) policy has been implemented. To test VPN and security, first user was allowed to access the VPN with no policy in which connection made successfully. Then NAC was used to create and implement policy to block particular user from connecting to VPN. Now trying to connect through VPN failed. This showed VPN and Radius server was installed successfully. | | | |

# Summary

This document planned and completed test on newly implemented network solution designed for Nepal Commercial Investment Bank. Various services, servers, security policies were tested to verify the configuration. Output during test was analyzed with expected results. Test log was used to document all test procedure. Now, as it is confirmed that network is configured correctly, system is ready for later phases of network implementations.

# Task 7

**Manage** the network security solution that you have implemented in task 4. [4.1, M3]

# Interlocution

Implemented network security design for Nepal Commercial Investment Bank (NCIB) is thoroughly tested and test results were analyzed to find any performance and security issue. To secure a network environment, successful implementation of network design is not enough, various access control plans need to be managed in the developed system. This document identifies and manage various access control plans for the developed network security system.

# Access Control

In network security, Access control is method used for control who or what can have access to network resources. Access control can be implemented in two different method. And they are logical access control and physical access control.

## Logical Access Control: System Access

Logical access control is used for controlling access to network and information. It grants an individual access to system after confirming their identity. This process is called authentication. To confirm identity, system may accept login credentials as username and password, biometric scan, PIN number etc. Once authentication is done access control approve or deny individual access to system based on permission associated with that individual. If administrator has authorized that individual to access the system then access control give approval to access the system. In NCIB, an individual may use username and password to access a system.

Administrator can give access permission to users, groups from active directory. For example, let’s say administrator creates a user account and authorized him/her to user printer1 and denied printer2 for this user then that user can use provided username and password to access printer1 and access control would allow it. If same user tries to access system using wrong username or password system deny access as it will fail to authenticate the user. And if user tries to use printer2, access control would again deny it as this user is not authorized to access printer2. In NCIB various methods are used for implementing logical access control to enhance security of network.

## ACL

Access control list (ACL) is table that defines while type of access authorization a user has on a specific system object. Each system object has access control list defined by its security attributes. This list describes various system user’s access freedom on that object. Permission ranges from read only which allows user to execute the object to full access where user can do anything with object. Whereas access denied permission simply denies user from performing any action on that object. Here are some the access control list currently being managed in developed network system for NCIB.

|  |  |  |  |
| --- | --- | --- | --- |
| OU/Group/User | Rule | Permission Description | Remark |
| Administrators | Access Control List | Full Control on any document | To implement and manage network security |
| HR/IT/Sales/Marketing | Access Control List | * Full Control on files/directory they own them-self * Read-only to public documents * Permission to printer | To enhance system security by limiting access to system object |

Here is example of how ACL is managed in NCIB network. Users from IT\_DAY\_SHIFT group has read and execute access permission on document but does not have modify permission. Hence they are not allowed to modify or delete to document.

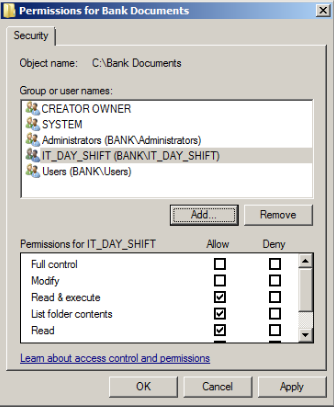


Figure 1 Access control list in NCIB



Figure 2ACL denied the action

## Group Policies

Group policy is a method used for applying security policies on system with help of active directory. It provides centralized management system allowing administrator to enforce rules from domain controller rather than going to each system to apply rules. GPO (group policy object) is created which is linked with objects in active directory. GPO is then edited to change policy settings using group policy management editor. In network implemented for NCIB, administrator uses group policy to set various security policies to user/groups.

|  |  |  |  |
| --- | --- | --- | --- |
| Group/User/computer | Rule | Description | Remark |
| Account | Group Policy | * Disable command prompt * Disable Run * Run accounting software at logon * Maximum Password age * Minimum password length | Enhance security by blocking batch file and asking to change password in each 30 days  Ensure account is locked if suspicious login attempt is made |
| HR/IT/Sales/Marketing | Group Policy | * Disable command prompt * Maximum Password age * Minimum password length | Enhance security by blocking batch file and asking to change password in each 90 days |
| Temporary Staff | Group Policy | * Disable command prompt * Maximum Password age * Account lock down | Ensure account is locked down once contract is finished/ staff leave the organization |

Here is example of management of group policy in NCIB to enhance network security. Here user from account group tried to user RUN menu which is disable by administrator using group policy.

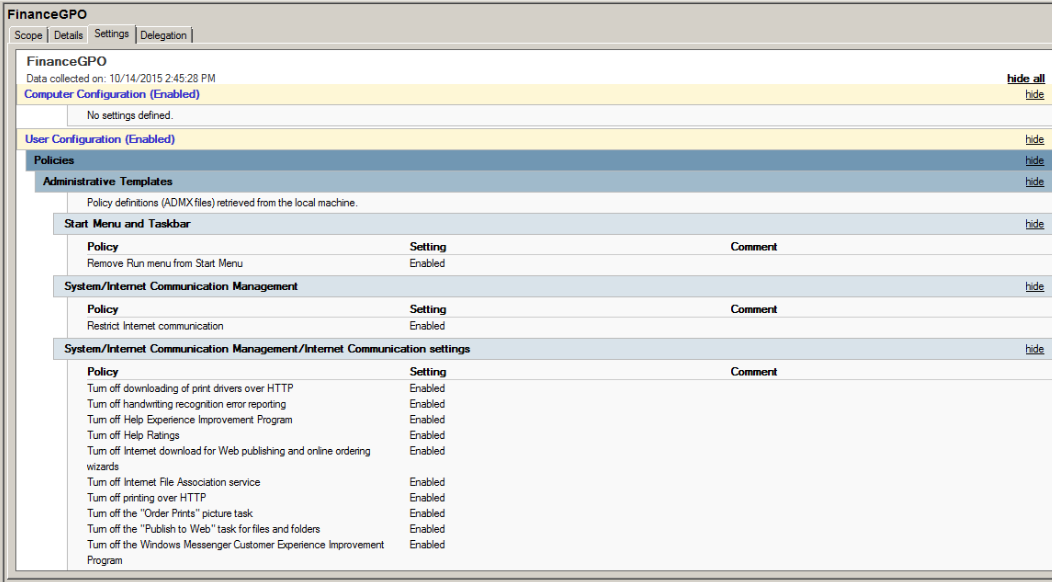


Figure 3 Group policy Object

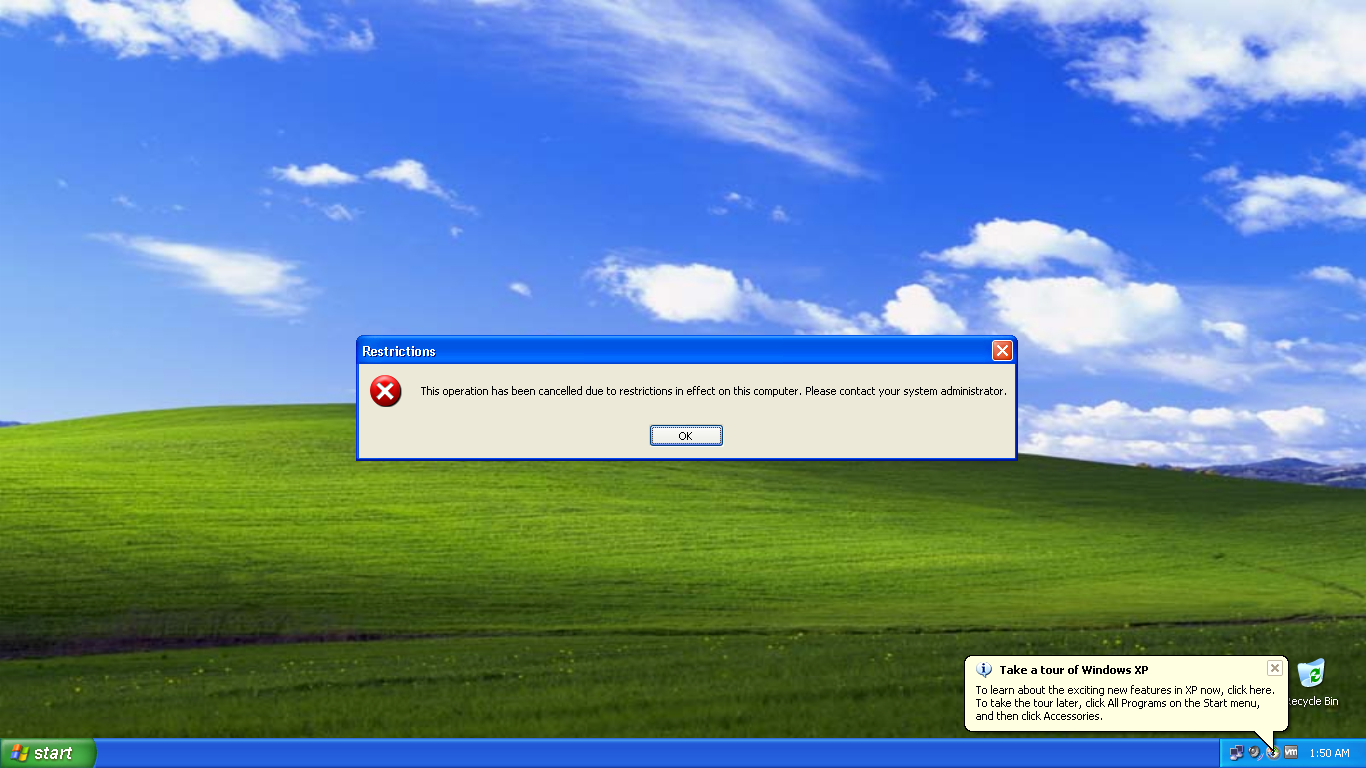


Figure 4Run menu is disable by group policy

## Password

Password is most common logical access control. But it is essential to set hard and long password so that it becomes harder to crack. Password can be hacked through brute force attack, dictionary attack, social engineering or other attack tools. Longer and harder password are tough to crack and requires longer time. In NCIB network, password policy is set through group policy. Minimum password size rule prevent short password selection making password harder to crack.

## Account Restriction

Account restriction allows administrator to prevent user from accessing system based on predefined condition. Two most common account restriction policies are time based access and time based account expiration. In NCIB network, temporary staffs are given account with prefixed account expire date to ensure their account will get expired once their contract is finished. Additionally, staffs are forbidden to access system during their off hour. This ensures hacker cannot use a staff’s credential to access the system during off-hour.

## Physical Access Control: Physical Access

Physical access control limits access to network infrastructures, network room/building to improve network security. Physical access control ensures network infrastructure is physically secured by using security tools and technologies such as surveillance system hiring security guard for IT room. In NCIB, physical access control need to be taken seriously. As this NCIB’s business is reliant on the network any harm on network can have harsh impact on productivity. Hence NCIB practices following plan to ensure physical access control.

|  |  |
| --- | --- |
| Security Provider | Description |
| Separate IT building | IT infrastructures are installed in a dedicated building/Room which makes easier to manage security and operation if IT department |
| Security Guards | Security guards for IT building/Room to ensure high security |
| Surveillance System | CCTV camera surveillance is installed in and around IT building to detect any suspicious activity. |

# Audit

## Physical Access Audit

Auditing is very important in security management. It is process of keeping record of log that can be useful for security analysis. NCIB uses auditing system to keep record of both physical as well as logical access control. These audit are analyzed to identify potential risk or used during security investigation. To keep audit of physical access control, record of each entrance/exit from IT building with time and identification is recorded. Additionally, surveillance report is also used for creating physical audit.

## Logical Audit

Administrator can record log of successful and failed system access and keep eye on all event happened in system. Administrator uses audit system to track record of files accessed by certain group/user if admin has any doubt on that user. Similarly, administrator uses audit to analyze and identify network access trend. Activities performed by various groups. NCIB network uses Event viewer system to browse the audit and analyses security logs.

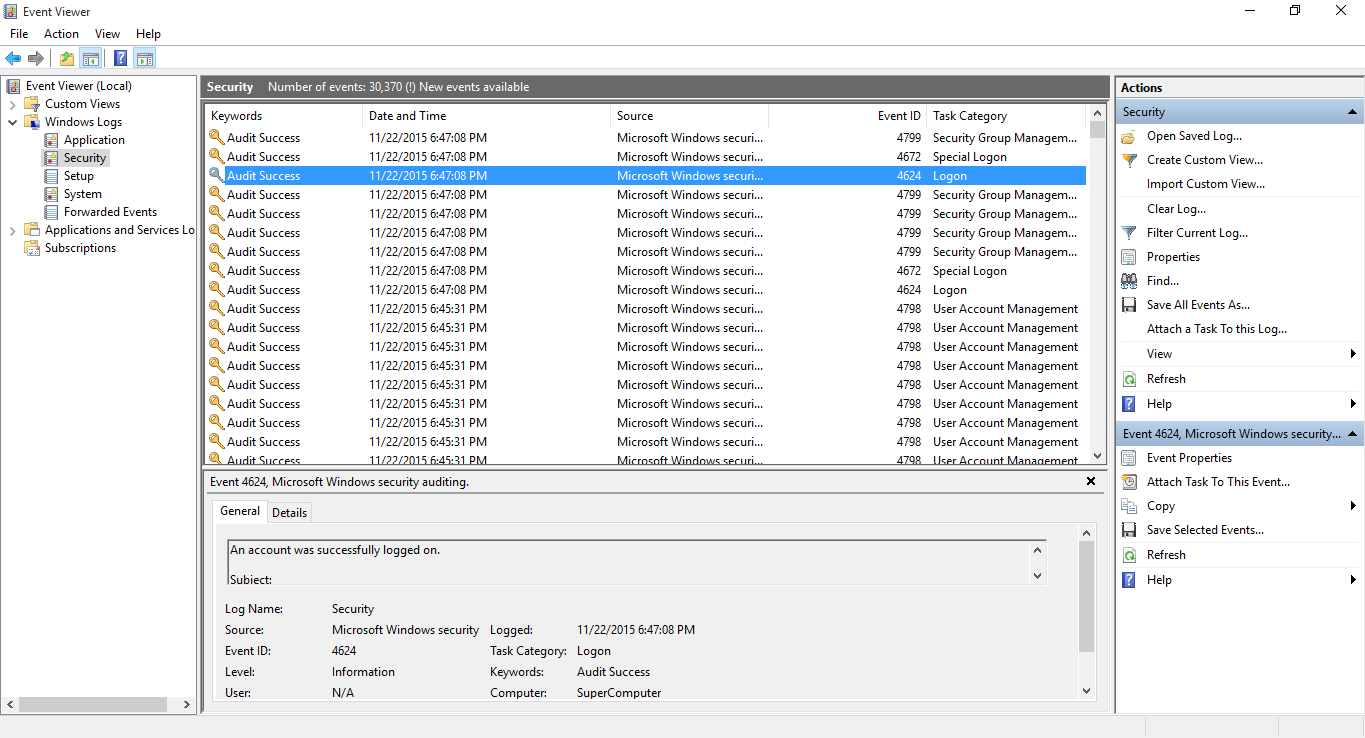


Figure 5 Logical Audit (Security Log)

## Summary

After implementation of proposed network design and test of the design, various security measurements has been managed. This paper documents those management procurements. To limit access to the system and improve security of the system, various access control mechanisms has be utilized. To enhance network security and build reliable network, system based logical access control system uses access control list, group policies, account restrictions and password policies. Each tools has been utilized in develop secure network.

In addition to logical access control, this paper also plans possible physical access control.

# Task 8

**Analyze** ongoing network security policies and practices. [4.2]

# Introduction

Secured network security environment for Nepal commercial investment bank is already designed and implemented. Security system has already gone through various tests and test results were evaluated. Newly developed design satisfies business requirements of NCIB and provides secured network environment. But then again, network need to be monitored and maintained continuously to guarantee optimal security. This report analyzes various ongoing network security policies and practices that can be utilized for securing developing network security system.

# System Monitoring

System monitoring is process of keeping track of various activities around the network to identify suspicious actions and act against them. A moment of negligence can jeopardize the whole network system. For a critical institution like bank, it is necessary to keep an open eye on each network activity. Any suspicious activity should be critically analyzed and appropriate action needs to be taken before it can harm the system. For example, failure in a network resource should be handled as soon as possible based on its importance. Handling such events should be based on the priority. This report further analyzes various modules that need to be considered while monitoring a networking system.

## Traffic

Monitoring network traffic is important process in system monitoring for both small and large network system. Network traffic monitoring is process of studying, reviewing and handling network traffic for any abnormality or activity that can disturb performance or security of the network environment. Table below shows various traffic types that has to be managed for providing optimal system performance.

|  |  |  |  |
| --- | --- | --- | --- |
| **Traffic Type** | **Description** | **Limitation** | **Solution** |
| **Bursty Traffic** | Inconsistence traffic level, HTTP, FTP Download, graphics, Videos | Due to irregular traffic pressure, a peak it consumes high bandwidth | Configure to limit bandwidth access |
| **Interactive Traffic** | Real time interaction-Web Browsing, SSL transaction, IM, Telnet sessions | Vulnerable to struggle for bandwidth and results in reduced response time | Prioritize over less essential traffic |
| **Latency Sensitive Traffic** | A steady stream of traffic such as VoIP, online gaming | Vulnerable to struggle for bandwidth and results in reduced response time | Set maximum bandwidth priority range based on priority |
| **Non-Real Time Traffic** | Internet protocol such as SNTP and NNTP | Consumes bandwidth during business hours | Schedule bandwidth during non-business hour. |

## Load

Load describes how much computational tasks system is performing. During heavy traffic, running large number of services, deep packet inspection results high CPU load which causes long response time affecting the productivity of system. Monitoring load allows administrator to identify CPU usage trend and get rid of unwanted activity to improve CPU load.

## RAM Monitoring

Monitoring RAM usage in system is essential for security of the network. It enables administrator to track high RAM usage and prevent system overload. Absence of required amount of RAM in system can cause disastrous problem and impact on productivity. RAM monitoring helps to analyze system upgrade requirements.

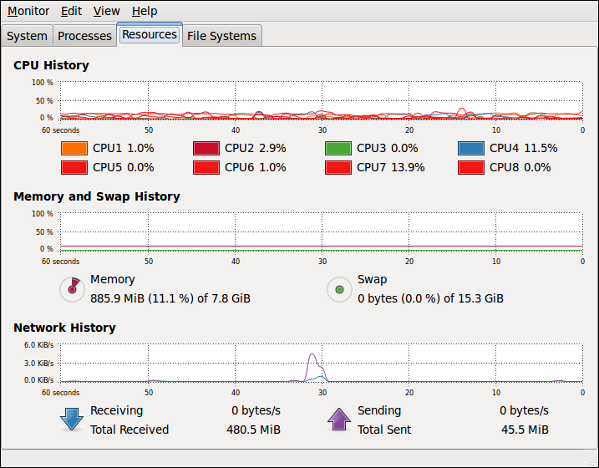


Figure 6 Load Monitoring

## Server Monitoring

Server Monitoring is process of continuous checking of uptime and detailed usage statistics of various servers in the Network. This helps to ensure all server in the network is healthy, active and showing appropriate response time. Problem in any single server can jeopardize whole network security and have negative impact on the system. Server Monitoring in NCIB network system includes IIS server, DNS server, VPN server etc.

# Ongoing Network Management

To analyze traffic, load, device behavior etc. in the network system, NCIB utilizes third party tools like wire shark, and PRTG network monitor.

## WireShark

WireShark is free network monitoring tool that analyzes network protocols. It allows you to monitor what is happening around the network. This tool allows capturing network traffic packet and browse them to analyze.

## PRTG Network Monitor

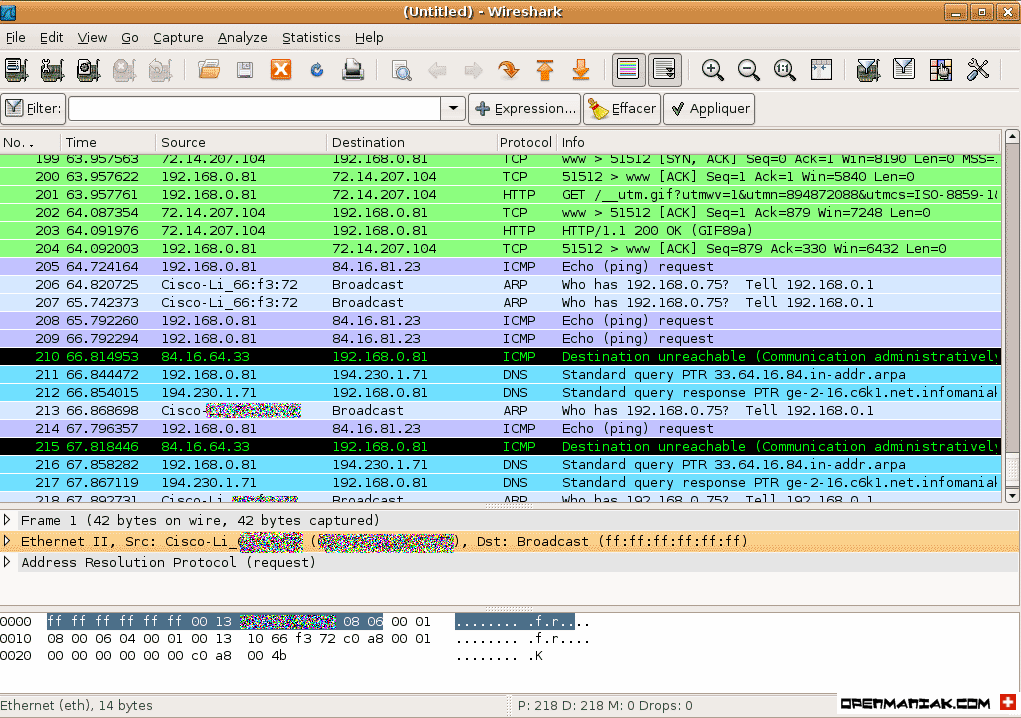
PRTG network monitoring system is world famous third party utility tool to monitor system. With this tool administrator can monitor network resources, bandwidth, servers and applications etc. It offers 24/7 automated monitoring and has feature to alert before emergency event. Administrator can keep eye on number of type of data such as: uptime, downtime, failed/success requests, CPU usage, bandwidth usage, disk space usage, utilization of firewall etc.

Figure Traffic Capture and Management using WireShark [Source: http://openmaniak.com/wireshark\_conf.php]

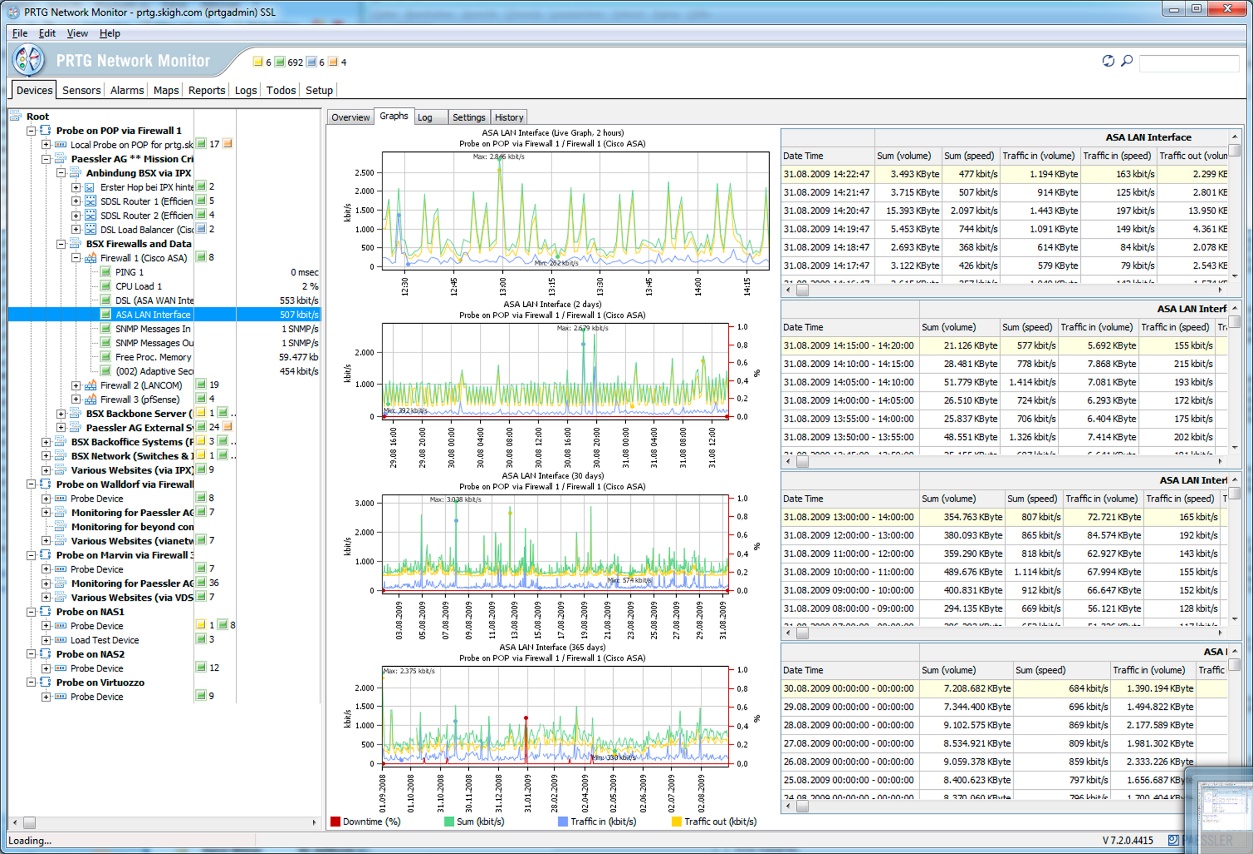


Figure 8 System Monitoring using PRTG Network Monitor [Source: http://www.healthcareguy.com/wp-content/uploads/2010/06/prtg72wingui4.jpg]

# Summary

This paper successfully analyzed several ongoing network security policies and practices. Various tools and technologies practice by NICB to monitor network traffic and system load has been analyzed. New network security solution utilizes third party tools like PRTG network monitor and WireShark to monitor traffic activities in the system. System monitoring will help NCIB to predict security as well as performance issues. Any suspicious traffic activity can be handled with help of such tools. Additionally, monitoring of RAM load and processor load will help to prevent system overload and upgrade the system before such event occurs.

# Task 9

**Recommend potential** change management [4.3, D3]

# Introduction

A new network environment for Prabhu bank based on their business requirement has been designed, implemented and tested. Various security management for the system has also been identified, managed and recommended. Now it is essential to analyze various components of the system and recommend potential change management that can enhance performance and security of the network environment. This paper evaluates different aspects of NCIB network to provide suitable recommendation.

# Self-Evaluation

To evaluate the implemented network system for NCIB various network elements such as utilized devices, user/groups, services etc. are evaluated. Limitations of the system is explored to identify change opportunities to enhance to system performance and security.

## Devices

Implemented network design is consists of various IT infrastructures such as routers, switches, printers etc. Currently, new bank network uses old routers and switches from existing system to support the system. Even though it helps organization to reduce cost of the system, it may affect the performance and security. Older system tends to have security issues compared to newer system available in market. Additionally, newer system uses latest technologies to improve their performance capability. Older routers and switch should be upgraded to newer and suitable machines available in the market as bank should not compromise with security and service performance of network.

## Recommendation

## Router

It is recommended to use highly configurable router from cisco, cisco 2951. Here are some of the features of this router that will improve the developed network system. These data are according to Cisco (n.d.) official website.

* Enhanced Security
* Hardware acceleration for VPN encryption
* Integrated threat control using firewall protection
* Enhanced Easy VPN
* High Performance

## Switch

Recommendation is made to upgrade existing switch with Cisco Catalyst 2960-Plus series. WS-C2960+24PC-L switch offers some of vast improvement over old switch used by current system. Cisco (n.d.) claims this router has following features:

* 24 Ethernet port that is suitable for head office network and branch office network
* Allows stacking of switches
* Smart Operations tool
* Energy friendly
* Highly Secure

## Groups

Network design plan phase analyzed group requirement for the system. Security group are created for each department and security policies has been enforce to those groups. Groups are based on real world department of the institution. Each group is introduced with various security policies through group policy.

During security management in the domain controller, implementation of some policies can be complicated on current group design. On this scenario, enforcing times based restriction on users based on their duty hour can be tricky. To implement time policy administrator would requirement to configure policy for each staff one by one as not user from IT group works at same time. This makes configuration process much harder than it should be. And administrators cannot take full advantage of group policy system.

## Recommendation

To solve the issues identified during evaluation, it is recommended create two/three more groups for each group to separate users based on time. For example, there will be three groups, IT\_NIGHT, IT\_EVENING, IT\_MORNING and all three groups will be member of master group, IT. By this way, administrator can set different rule for each groups. This will make system security procedure more effective and reliable.

## Services

Implemented network security system includes various server technologies to support the organization’s business requirement. But, through various feedback from staffs and self-evaluation it is identified that current network system does not have email service support. To improve service quality of the network, recommendation should be made to address this issue. Needed changes in mechanism should be made to support email service.

# Recommendation

## Mail server (Email Server)

A server that handles and delivers email over network is mail server and sometimes it is also referred as email server. A mail server has capability to receive mail from domain client and deliver them to client or other email server if required. When client sends email, program connects with mail server which is known as Simple Mail Transfer Protocol (**SMTP**). This protocol is used for delivering email from client to server or from server to client.

When client downloads mail from mail server, connection with server called POP3 is made. POP3 protocol is used this type of communication. To satisfy the requirement of staffs and avoiding dependencies on webmail, mail server should be installed on current network system. Depending on webmail for delivering critical information is not always secure as Internet is very broad and attackers may find way to crack webmail accounts.

# Additional Recommendations

## Physical Security

Physical access control in the current environment is managed. Although guard and surveillance serves well to provide physical security, there are technologies that can be utilized by NCIB to improve its security model. Information stored in banking network is very sensitive hence, any short of security improvement possibility should be taken into consideration. To improve current physical access control position, following change plan are recommended:

* NCIB should utilized biometric security system for authentication, only authorized person should be allowed to access the IT premises. Such biometric system includes finger print scanner, retina scanner etc.
* Changes should be made to improve authentication process to make sure only authentic person uses server computers. Requiring finger scan to use server computer will improve security of the network.

## Move to Cloud

According to Griffith (2015) cloud computing means putting away and getting to information and projects over the Internet rather than PC's local hard drive. The cloud is only an analogy for the Internet. As banks adjust to market changes and new innovation scenes, cloud computing is assuming a noteworthy part, giving optional approaches to access to banking technology. The spiraling expenses of conveying and keeping up complex in-house legacy frameworks, alongside the need to stay aware of clients desires, are driving banks to progressively request imaginative, adaptable and financially savvy deployment models for their banking solutions.

Cloud offers a flexible, manageable innovational demonstration that diminishes IT infrastructure, maintenance and improvement costs. This gives bank agility and flexibility to grasp new markets (TEMENOS, n.d.). For current system, it is recommended to explore in more depth for possibilities of moving to cloud. In depth evaluation of benefits of moving to cloud should be done. Moving to cloud would allow NCIB to focus on marketing and customer service and cloud based service would highly secure and industry leading banking technology without heavy expensed on internal network infrastructure and resources.

# Conclusion

This segment of the report comprises of a self-assessment of the framework which helped in recognizing the qualities and shortcomings of the framework. While the qualities of the framework helps in satisfying the necessities postured by NCIB, the shortcomings called for change administration arrange so that the shortcomings could be enhanced. Therefore, this report likewise comprises of the suggestions of progress in the arrangement of NCIB. The progressions should be made in criteria, for example, gadgets, administrations, gatherings and servers in the framework. Every segments for change has been examined and appropriate proposals has been made for enhancements. Executing the suggestion will help in making the framework secure, solid and proficient than it as of now is.

# References

* Cisco (n.d.) Cisco 2900 Series Integrated Services Routers [Online] Available: <http://www.cisco.com/c/en/us/products/routers/2900-series-integrated-services-routers-isr/index.html> Accessed [11/29/2015]
* Cisco (n.d.) Cisco Catalyst 2960-X Series Switches [Online] Available: <http://www.cisco.com/c/en/us/products/switches/catalyst-2960-x-series-switches/index.html> Accessed [11/29/2015]
* Griffith, E (2015) What Is Cloud Computing? [Online] Available: <http://www.pcmag.com/article2/0,2817,2372163,00.asp> Accessed [11/29/2015]
* TEMENOS (n.d.) Cloud Banking [Online] Available: <http://www.temenos.com/en/products-and-services/cloud-banking/> Accessed [11/29/2015]