Contents

1. Introduction

Golden Bank is the largest financial institution operating in mainland Tivoli. GB business processes rely on a combination of systems including Internet, IPX/SPX, SNA and ICT related services with a very complex ICT infrastructure in place seen by the GB board of directors as problematic for the sustainability and further GB business growth. There is a little room for the network infrastructure improvement. And there needs to be a change and re-provisioning of its ICT infrastructure to remain competitive. As part of this change, the transition to interoperability should be achieved in a smooth manner and leverage in the latest advancements in secure network infrastructure. There should not be any problems while migration. The bank is expected to grow by 30% in the next 4 years. In terms of security, the new system should safeguard the appropriate access and use of ICT resources; ensure unauthorized and malicious internal and external network attacks are properly blocked. The findings of this report are founded in various websites that are dealing with network security. Lot of network security features is discussed in this paper that can be used to fulfill the requirements of the banks network infrastructure expansion.

2. Project Scope:

- To prepare a security plan for Golden Bank
- Investigate the Existing Infrastructure
- Planning the design of the new infrastructure
- Policies needs to be framed for the network security

3. Statement of Work:

In this project Golden Bank management recruited us to investigate and find out the details about the present infrastructure, Plan the design of the new infrastructure and the required network policies to be framed to migrate the infrastrure with less downtime.

4. Current Security Environment:

GB has 28 branch offices around Tivoli and two remote branch offices in the islands of Greenland and Faroe. GB has three major facilities, all located in mainland Tivoli: Headquarters, Operations and Backup. The Headquarters facility is located in a downtown office that houses the administrative staff. The Operations facility is located in a warehouse near an industrial area in the outskirts of Tivoli. The Operations building located 60Kms from the headquarters houses the back-office technical functions, the data centre and the GB IT staff. Finally, the Backup facility, located in the country area of Tivoli about 100km from the headquarters is used as a warm-site facility which can take over within minutes in the event that the Operations facility fails.

5. Security Policies

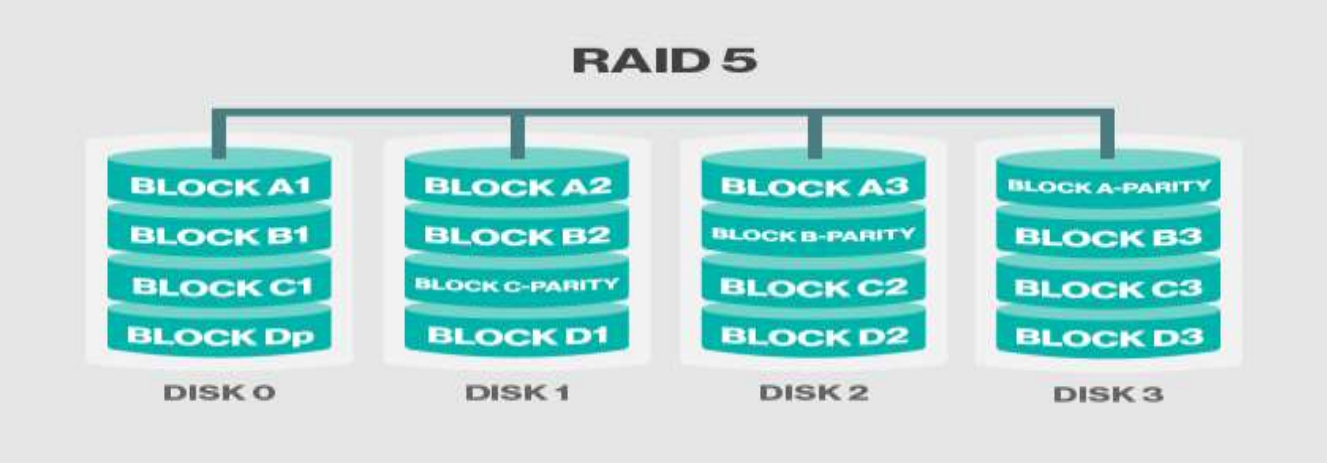
Security policies are discussed in many places in this project. Mainly Golden Bank should have the following password policy.

Mandatory Requirements for Password are 10 minimum password length, No spaces in between, one letter between A-Z, One letter between, one numerical characters between 0-9, One special character.

6. Disaster Recovery and Business Continuity Plan

6.1 RAID

RAID is a short form for redundant array of inexpensive disks and also redundant array of independent disks. It is a virtualization technology for the storage. In RAID multiple drivers are combined together. The combination will form a logical unit. Data redundancy is the main purpose of RAID. RAID is used for performance improvement also. RAID level explains how the data is spread across the drives. Up to what level capacity, availability, reliability and performance parameters are combined together is decided by RAID levels. Golden Bank can use Raid 5 for their servers.



Block level stripping but distributed parity. Parity data also distributed among the drives. If single drive is failed then the read will happen with the help of parity. So read operation will not be affected because of the single drive failure. It requires at least 3 disks. This is very widely used in all commercial applications. Performance is very excellent and fault tolerance also very good. When write intensive application is used Raid-5 cannot be recommended as it will

calculate parity in all times and this will affect the write performance. When one hard disk fails the entire system will go to degraded mode and performance also will have a hit. Rebuild will take lot of time. And second hard disk failure also possible in this. Read performance is good in this level. Good aggregate transfer rate. Controller design is very complex. Raid-5 is used in File and Application Servers, Database servers, Web, Email and News servers, Intranet servers and etc.

6.2 Microsoft and Veritas Clusters

We will be going with Microsoft windows failover clusters for the critical applications. If we want to have very stable cluster applications then we can go for VERITAS cluster technology. One standard Veritas design is given in the appendix. This design features can be used in our Veritas cluster design.

Cluster technologies can be used for high availability. For load sharing we can go for DNS round robin technologies and for application servers we can go for network load balancing technologies.

6.3 High Availability of DNS:

DNS can be classified as Primary and secondary. Primary server will be having master copy of the DNS records whereas secondary will be having the copy of the primary. Any time the secondary can be converted as primary when need arises. We can go ahead with active director integrated DNS which will be always primary. Further all the servers will be having primary DNS servers and so there won't be any DNS downtime.

7. Risk Management Plan

Switches will be kept in a switch rack of each and every room and the switch rack will be kept in 8 feet high on the wall. Only the status lights of the switches will be visible. Users can not touch the switch. The switch rack is very solid rack, able to withstand and protect the switches from extreme temperatures, high humidity, theft, vandalism, and arson, spilled drinks, overloaded electrical outlets, and bad plumbing.

There will be a server room with 24x7x365 hours AC. The servers will be kept in this room and these servers will be connected with a layer-2 switch (Distribution Switch #10). These servers will be connected with the internet through a router. The server room will be always locked from outside. Only server administrators and management people will be having the access to the server room.

VLAN technology will be used while configuring the switches. Same department users will be connected with same VLAN. This ensures smooth network traffic between the end users and

internal network protection. The desktops of two different departments cannot communicate each other as they are connected with two different VLANs.

There will be an anti-virus server for the entire network. Anti-virus clients will be installed in all the desktops and authorized laptops and Anti-Virus server will keep monitoring those desktops and servers.

There will be a software proxy for the entire network. All the users will be connected with the proxy for internet browsing.

There will be Active directory server for windows domain environment. All the users need to login to the network using windows domain user account only.

For accessing the internet the network configuration of the end users PC will be configured with proxy settings as shown below. In these settings 192.168.200.200 is the proxy servers IP address and 8080 is the port number through which the internet service is delivered to the clients.

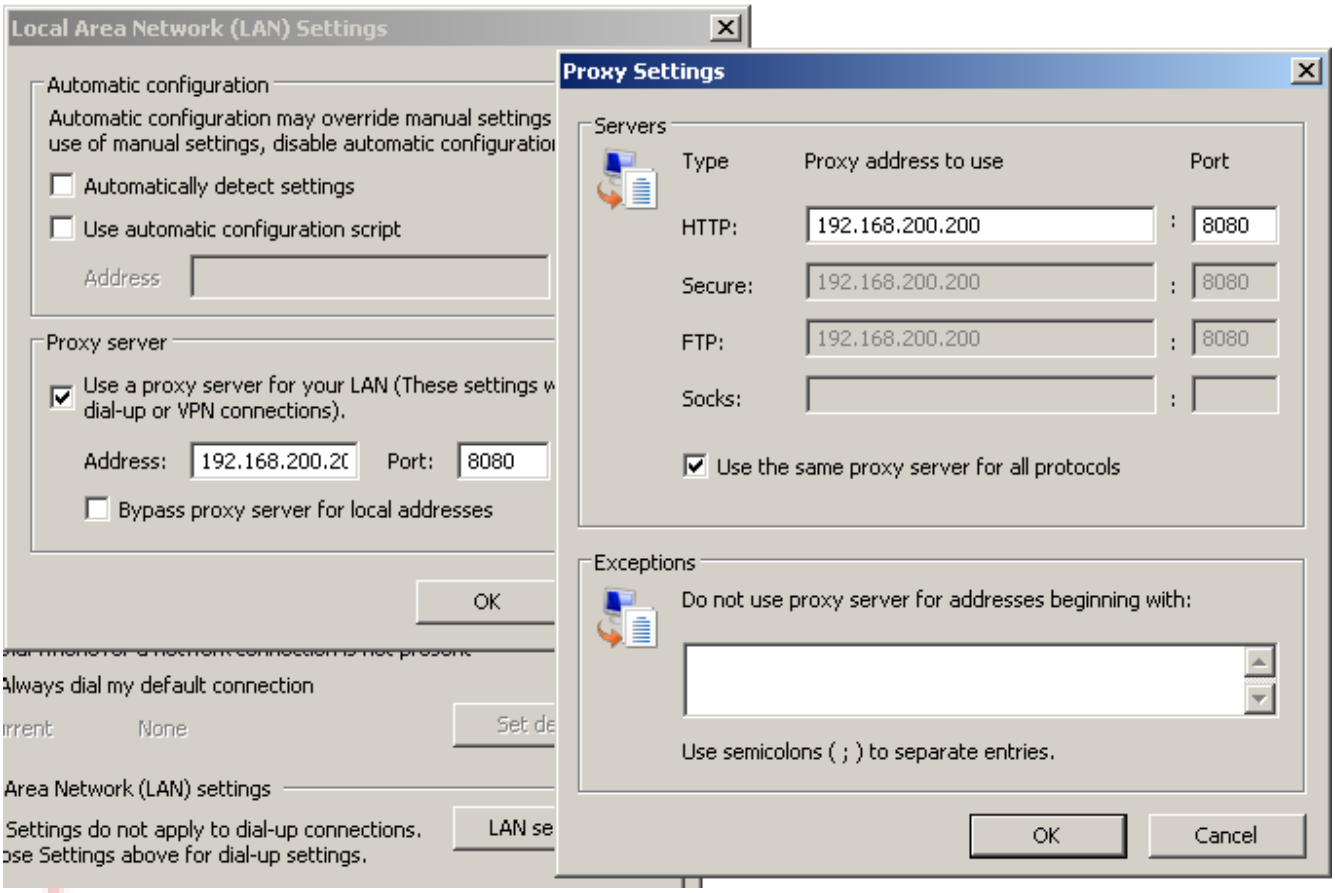
8. Basic Network Security to the network

There are no much detail given about the placement, Datacenter locations and etc.

The following security aspects should do as early as possible.

Network Design	What security the design provides to the network
Switches will be kept in a switch rack of each and every room and the switch rack will be kept in 8 feet high on the wall. Only the status lights of the switches will be visible. Users can not touch the switch.	People cannot touch the switches. So there will be a physical security for the switches. The switch rack is very solid rack, able to withstand and protect the switches from extreme temperatures, high humidity, theft, vandalism, and arson, spilled drinks, overloaded electrical outlets, and bad plumbing.
There will be a server room with 24x7x365 hours AC. The servers will be kept in this room and these servers will be connected with a layer-2 switch (Distribution Switch #10). These servers will be connected with the internet	People cannot touch the servers. So there will be a physical security for the servers. The servers rack is very solid rack, able to withstand and protect the servers from extreme temperatures, high humidity, theft, vandalism, and arson, spilled drinks, overloaded electrical outlets, and

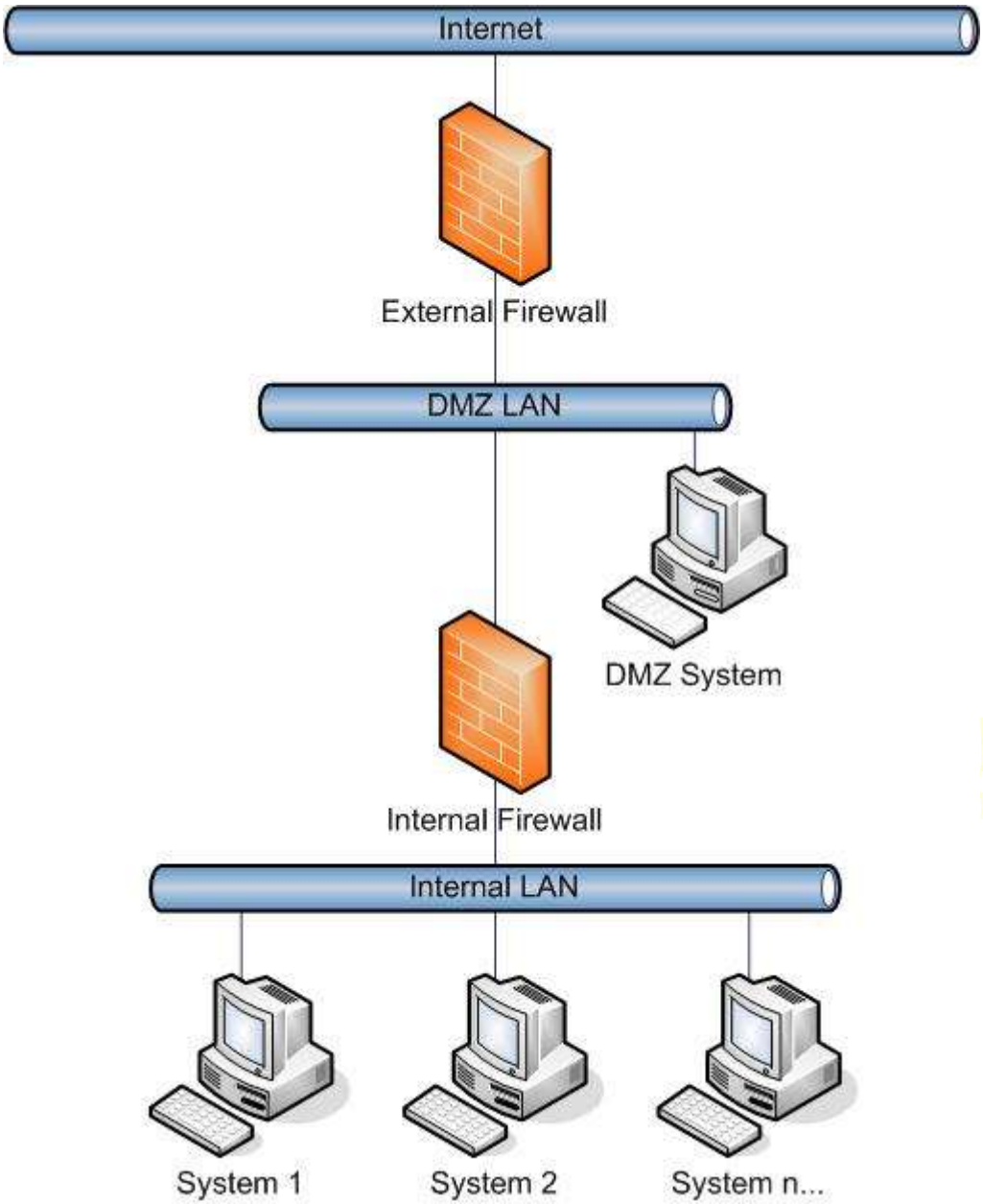
through a router. The server room will be always locked from outside. Only server administrators and management people will be having the access to the server room.	bad plumbing. Since servers are isolated from the end users area physical access to the servers is restricted to only server administrators. So there will not be any data theft will be there.
VLAN technology will be used while configuring the switches. Same department users will be connected with same VLAN.	This ensures smooth network traffic between the end users and internal network protection. The desktops of two different departments cannot communicate each other as they are connected with two different VLANs.
Install anti-virus in all the clients and servers	This will protect the servers and desktops from viruses, adware , spyware, Trojans and etc.
There will be Active directory server for windows domain environment. All the users need to login to the network using windows domain user account only.	All the users' login time and their activities can be monitored. Un-authorized users cannot come into the network and cannot access the network resources like file server, webserver and internet. If the user tries to do hacking, tried to do file sabotage, unauthorized copying then the user will get caught easily?
There will be a software proxy for the entire network. All the users will be connected with the proxy for internet browsing.	Proxy will control the internet access to the users who are members of the domain. The username password will be the domain user name and password for the internet access through the proxy. If the password is wrong then proxy will not allow internet access.
For accessing the internet the network configuration of the end users PC will be configured with proxy settings as shown below. In these settings 192.168.200.200 is the proxy servers IP address and 8080 is the port number through which the internet service is delivered to the clients.	Controlled internet flow is possible. Each user's session can be monitored. The bandwidth usage of the users, Types of files downloaded, download duration and all web download properties can be controlled.



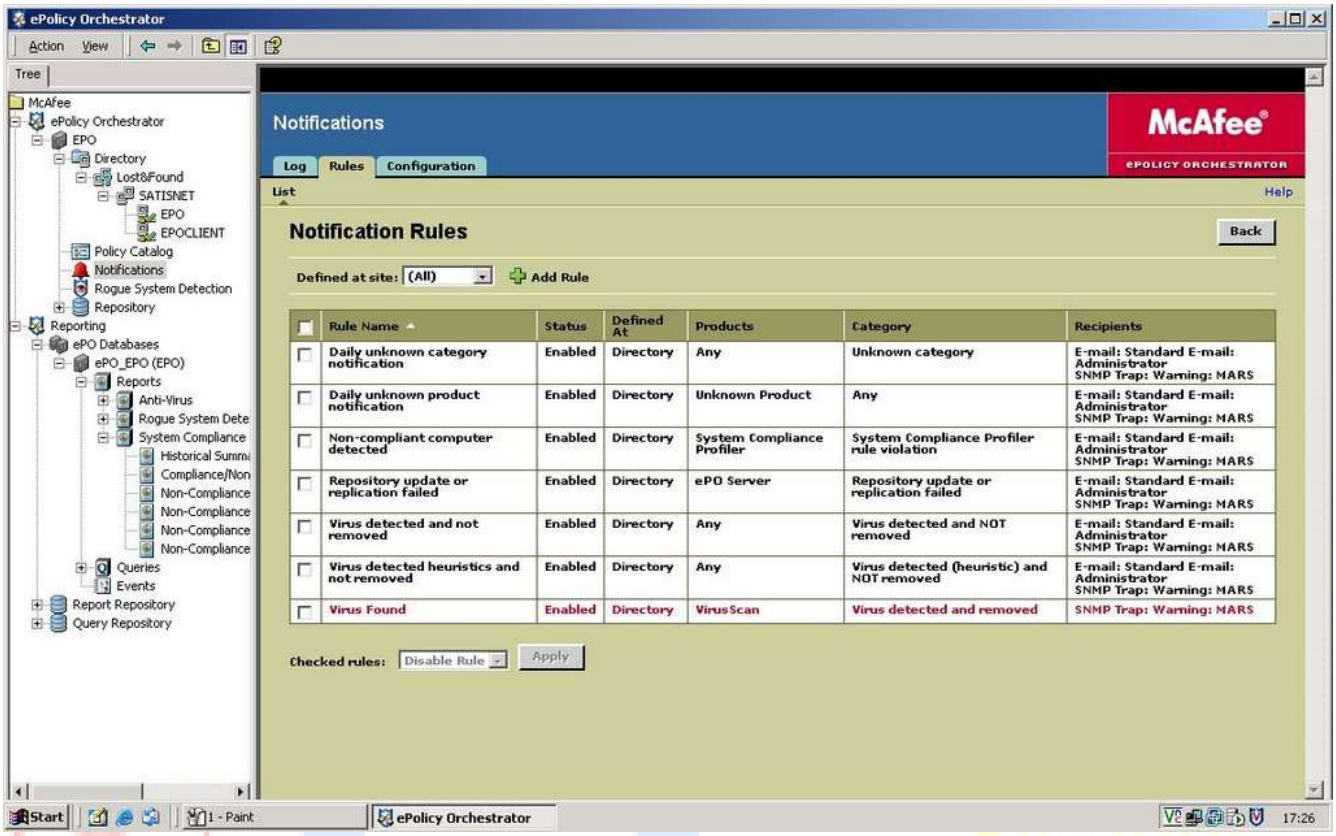
9. Further Security Procedures

1. The above network doesn't have firewalls except windows firewalls. Two firewalls can be purchased and a De-Militarized Zone can be formed. (DMZ)

2. The public facing servers like Web Server and FTP servers can be put in these DMZ zone. In the pictures shown below DMZ systems are web servers and FTP servers. These servers will be accessed from internet and as well as from intranet (Local LAN). So there should not be any link between external world (WAN) and the internal world (LAN).



3. There will be an anti-virus server for the entire network. Anti-virus clients will be installed in all the desktops and authorized laptops and Anti-Virus server will keep monitoring those desktops and servers and keep scanning them. We need not install the clients in each and every PC and need not check the threat level in each every PC.

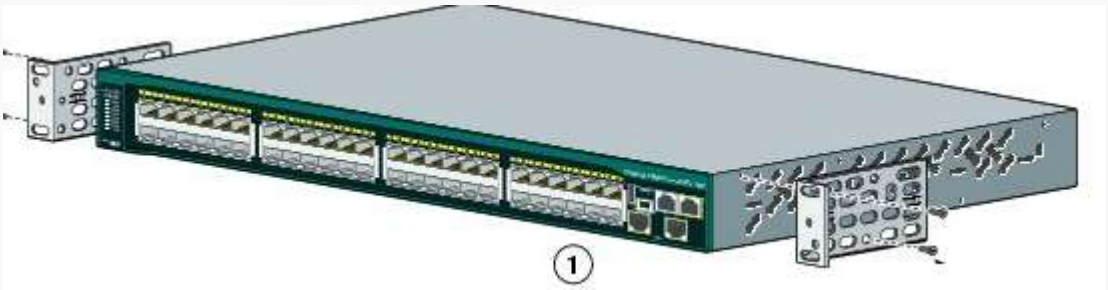


The above network solutions tested. The following components were selected.

Routers – Cisco 17xx, 18xx, 26xx, 28xx, 36xx, 38xx, 72xx, 76xx

Switches: Cisco 19xx, 35xx, 36xx, 40xx, 45xx, 65xx

Anti-Virus : McAfee ePO Orchestrator

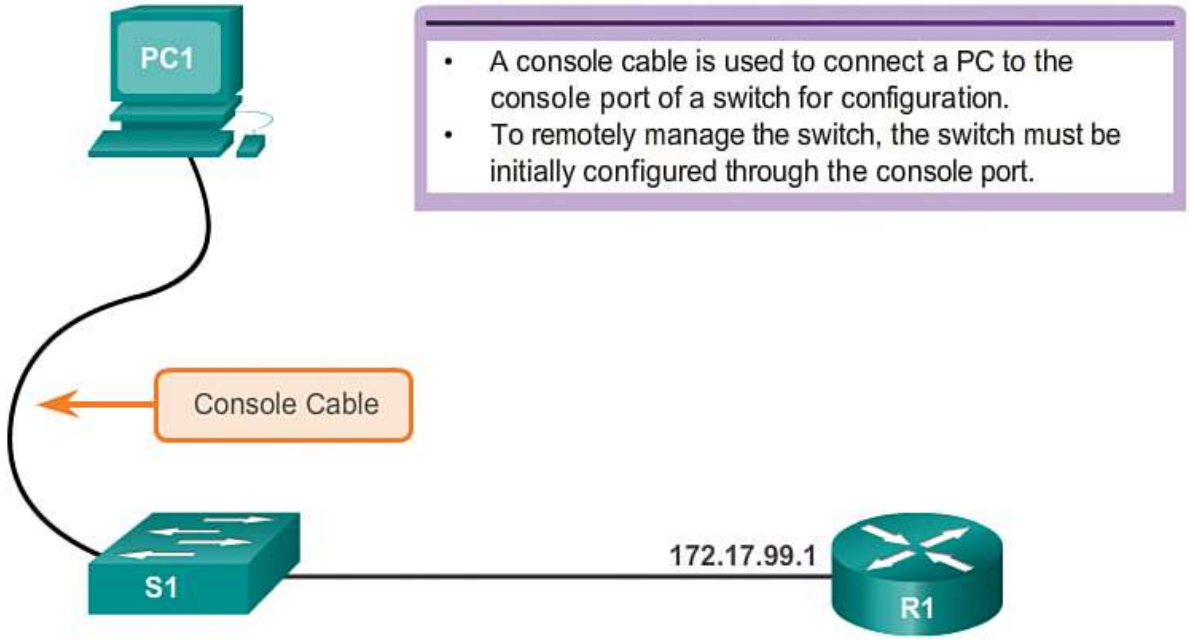


Switch Rack for Cisco Switches

Router Rack for Cisco

9.1 Managing the switches and routers

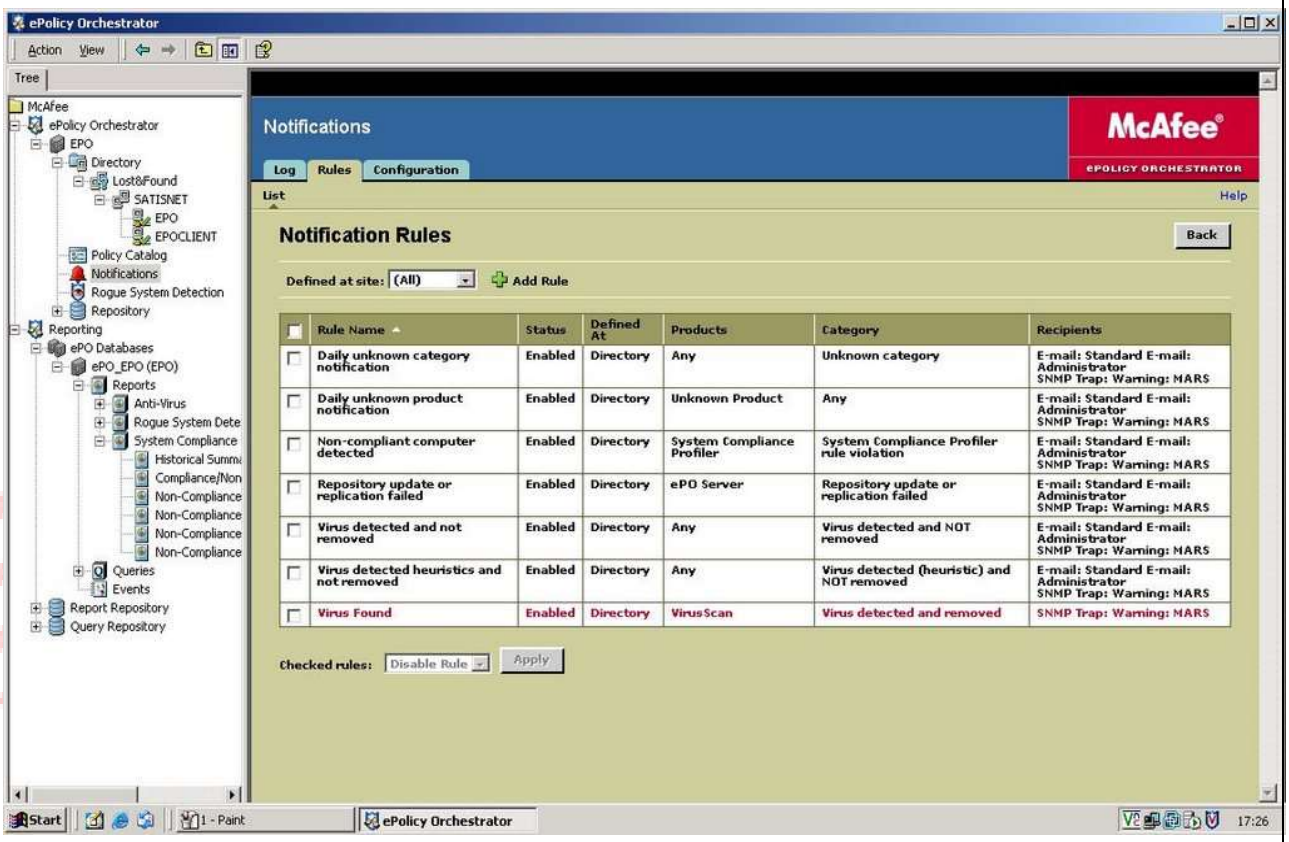
- Managing switches and routers will be done by connecting a console cable to the switch/router to the desktop. We can connect to switch/router using terminal application from the windows.



Connect a Terminal to Catalyst Switch

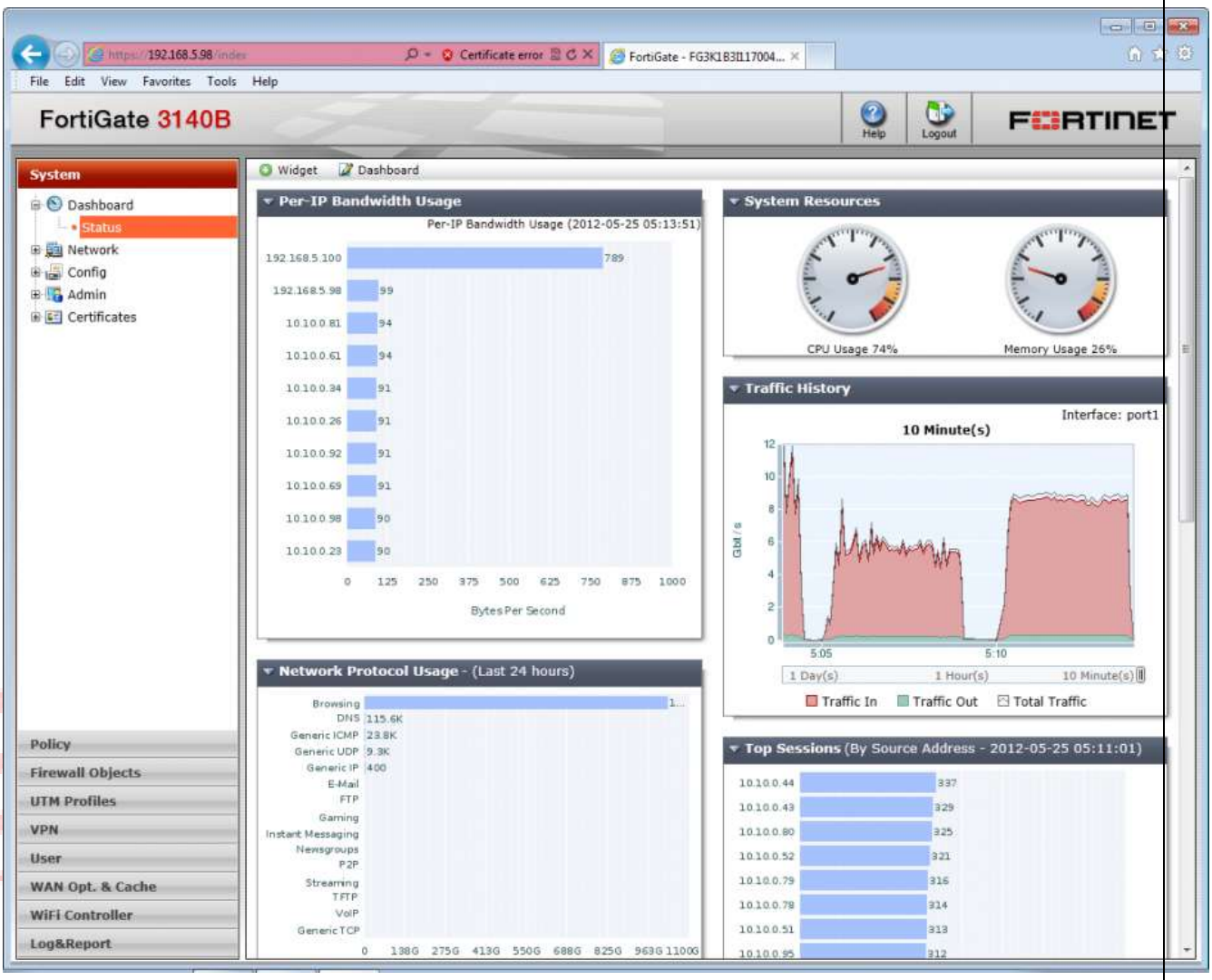
9.2 Managing MacAfee Anti-Virus

McAfee Anti-Virus can be managed from ePolicy Orchestrator. Using this interface we can add the client pc into the anti-virus domain, push the anti-virus agent into the PC, and bring the PC into the scanning control of anti-virus server.



9.3 Managing FortiGATE Firewall

FortiGATE Firewall can be managed from the web interface. In this web interface we can set rules, allow the ports, block the ports, block the services, allow the services and etc. The whole network will be behind the safe region.



9.4 Managing a Windows Proxy server.

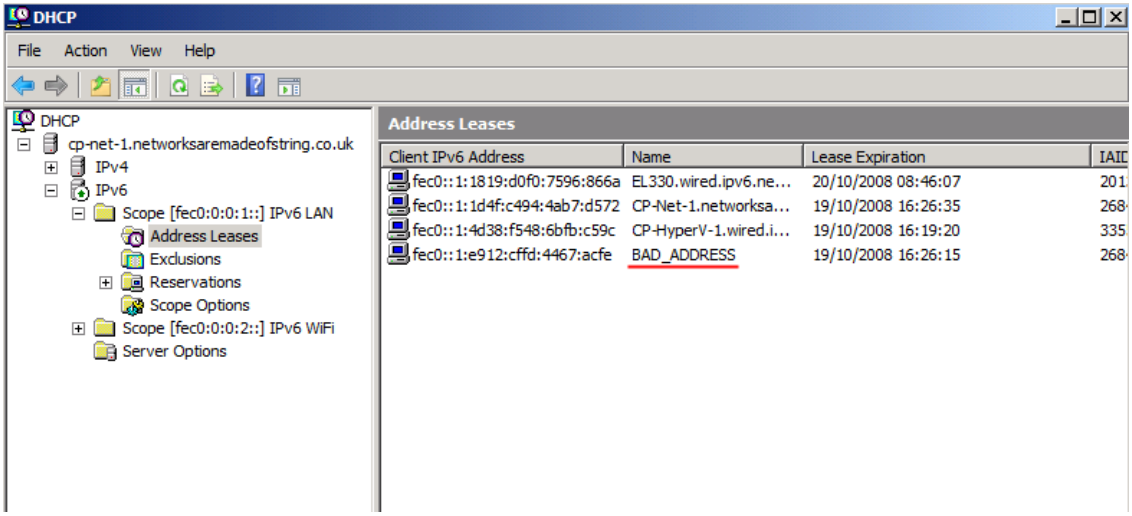
We can manage the proxy server through a proxy management consol.

As shown in the above picture we can do user management, web managements and network activities

9.5 Managing DHCP Server

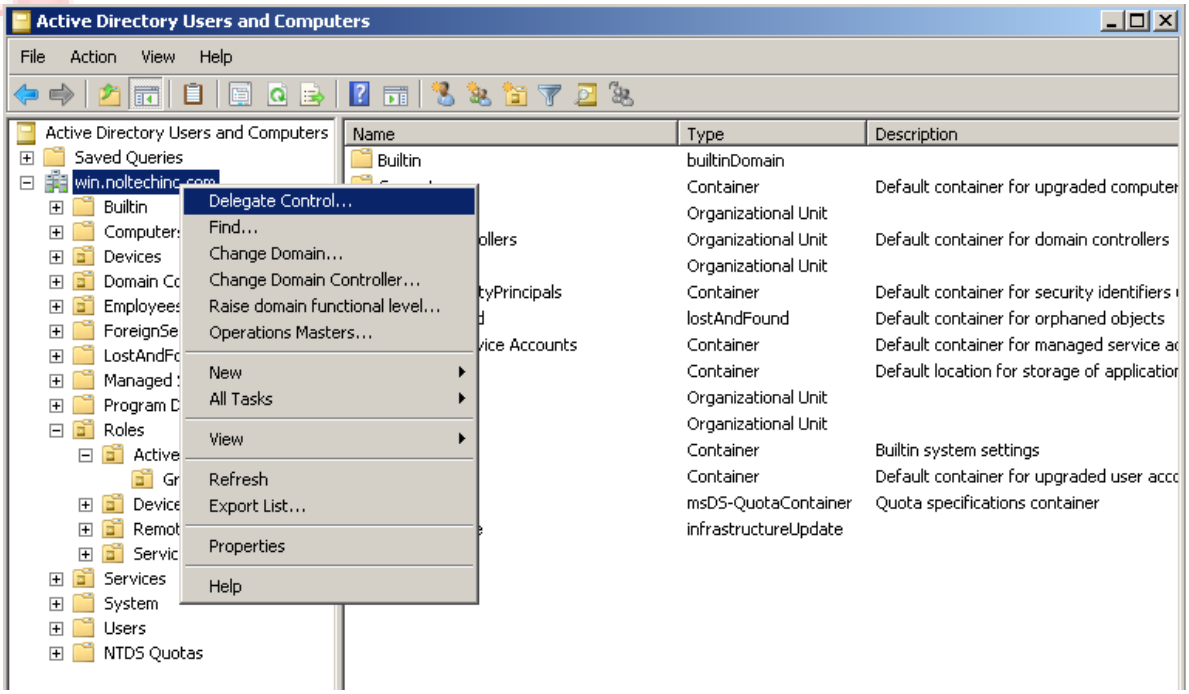
DHCP Server can be managed from DHCP Server consoles that are available in the windows'.

Start – Run → DHCPMGMT.MSC will give the DHCP Server consol.



9.6 Managing Active Directory Users and Computers

Active directory users and computers will be managed from Active Directory Users and Computers console in the domain controller servers.



9.7 Network security policies and practices you could implement

There will be a governing policy under which technical policies and end user policies are formed.

Governing Policy

Governing Policies: This policy is the high level treatment of security concepts. These policies are important to the company

End User Policies: This policies answer the what, who, when and where questions at an appropriate level for an end user.

Technical policies: Technical people use these policies. They carry out their security responsibilities of the system

A lot of policies will be defined under technical policies

Example Policy: Server Configuration and Access Policy

- Proper server configuration policy should be maintained by appropriate people.
- Servers must be registered within the company's EMS. Server details should cover the following
  - Server Sl No
  - Server OS
  - Main functions and applications
- Operating System Configuration will be as per the InfoSec recommendations.
- Unnecessary Services and Applications must be disabled
- Access to servers and services should be logged
- Timely security patching should be done
- Trust relationships needs to be created only if it is necessary.
- Server should be physically located in an access control environment.

Good Practices to be followed

Keep the server and switch environments dust free
Don't use hubs or bridges. Use layer 2 /layer 3 switches
Don't use unmanaged switches. Use managed switches.
Use VLANs.

Don't bring laptops without preapproval from the InfoSec team.
Install anti-virus in the laptops
Don't connect the laptops with the corporate network without the permission from InfoSec
Don't misuse company internet
Switches and servers should be kept in appropriate places. Human activity should be less nearer to the switches and servers.

10. The following are all some of my recommendations for general security

- Ensure the basics are taken care of. Such as OS and driver updates are up to date.
- Ensure that the Personal firewall is active
- Ensure that the anti-virus is running and updated
- Passwords are set as per the pre-approved security policy
- Use disk stripping in the hard disk where multiple disks will be combined together and one logical volume will be formed. Data will be stripped and put inside the hard disk
- Cleanup network protocol. Remove old network protocols if they are installed and not in use
- Adjust TCP/IP settings, particularly window size.
- Implement WAN bandwidth savings models like terminal servers, content networking and web services.
- Perform auditing and mapping.
- Keep the network up-to-date
- Physically secure the servers and switches
- Implement VLANs to segregate traffic
- If wireless networks are used then don't use WEP encryption. Use WPA/WPA2 for authentication.
- When contacting the servers from outside of the LAN use VPN and encrypt the entire network

11. Possible Threats and Their Mitigations

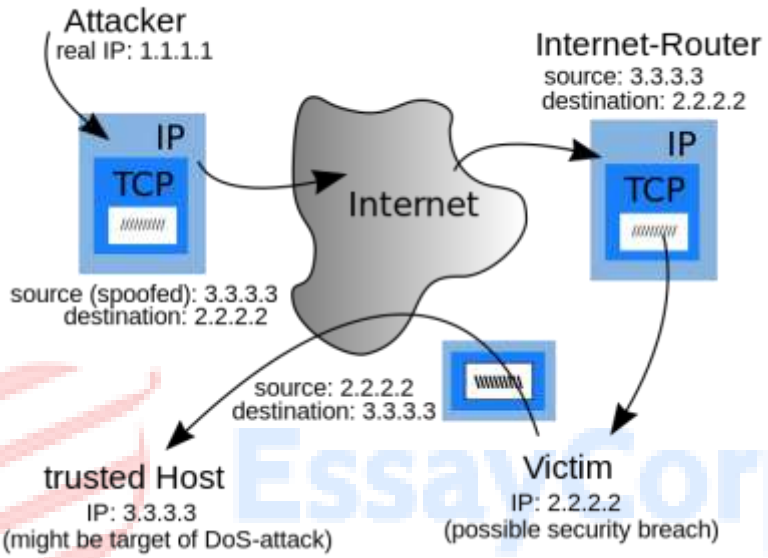
11.1 Spoofing Attacks

In this attack one program or person will act as other by falsifying data and getting access to the protected system.

11.2 Email spoofing

Spam and phasing emails mainly uses this spoofing mechanism. The sender address of the email will be spoofed and the target person will think that email has come from some important places.

11.3 IP Address Spoofing



In this spoofing the IP Pockets will be generated with the source IP, to hide the original IP of the system. IP Spoofing is mostly used by the hackers while performing DDoS attacks. In DDoS attack the victim system will be flooded with lot of request pockets with in sort time. The victim will try to respond for the requests and reach their maximum capacity very soon. Due to this attack the genuine services will get affected. The IP address spoofing affects any service that uses IP Address information. RPC Services, XWindow System and rlogin and rsh services. IP Spoofing attacks can be prevented by using Pocket Filtering.

11.4 Prevention from IP Spoofing

Many tools and practices are there.

Use Pocket filtering

Avoid trust relationship: Trust relationship should be minimized. Trusts are based on IP and hence prone to IP Spoofing.

Use Spoofing Detection Software

Use cryptographic network protocols like TLS , SSH, HTTPS protocols can be used to secure communications

11.5 ARP Spoofing Attack

ARP stands for Address Resolution Protocol. ARP is used to resolve the IP address to MAC address. The hacker sends a spoofed ARP pockets to the LAN where the victim is connected. Switching devices will think that, that the hacker is the correct person to send the data and will send the data. These types of attacks are mainly used for information steeling.

11.6 DNS Server Spoofing Attack

DNS = Domain Naming System. It maps the domain names with IP addresses.

In this attack the hacker will send spoofed DNS pockets and so the requests will be re-directed to some other servers which the hackers control. This server will be having spyware and malware. This type of attacks happens mainly for spreading viruses and computer worms.

11.7 Google Dorking

It is a practice of using advanced search techniques. In this specialized search parameters are used and very sensitive information will be taken out but the hackers. Usernames and passwords, email lists, bank account details can be stolen using this attack.

11.8 Trojans, Key loggers and Spyware Attacks

Trojan is a malware program. It contains malicious code which carries out lot of black hat actions determined by the nature of the Trojan. Loss of data and system harm will happen due to Trojans. Sometimes these Trojan will open back doors using which the affected systems will be controlled by hackers. It is not easy to find out backdoors but computers will run slowly due to backdoor utilization.

Net bus Advance System Care, Sub seven or Sub7, Back Orifice, Beast, Zeus, Flashback Trojan, Zero Access, Koobface, Vundo are the well known trojans.

11.9 Purpose of the Trojan

User screen watching, Users webcam watching, controlling the victim computer system from a remote place.

Encrypting files; a ransom payment may be demanded for decryption, as with the Crypto Locker ransom ware

System registry modification and converting the victim computer as proxy and making use of it to do illegal activities and/or attacks on other computers.

Fully Infects entire Network information and other connected devices

Payment Data theft, confidential files Theft, industrial espionage, usernames and passwords theft

Changing or deleting of files, multiplication of files

Downloading/uploading of virus affected files for various purposes

Downloading and installing commercial advertisement software(adware), including third-party malware and ransom ware

Keystroke logging and may Crashing the computer with blue screen of death (BSOD)

Data corruption and formatting disks and thus destroying all contents

11.10 Key Loggers

Keyloggers can be software or a device that is used by logging the keys typed. Key loggers can be used to spy people and also to monitor the people like in Parental control.

Keyloggers will log all the user typed keys and store them locally or send them to the remote hacker. Once hackers get the info about the bank username and bank passwords, they can transfer the money from the infected users account to remote persons account. Cyber frauds are using key loggers, phishing and social engineering as the methods to create maximum harm to the innocents.

Major theft of users data prevented by police in London, Married couple who were involved in industrial espionage in Israel, The theft of over $10 million from banking client accounts at the major Scandinavian bank at Nordea, Major incidents that happened due to key loggers are the major incidents happened due to key loggers.

The lot of financial benefits from the key loggers inspired lot of hackers and they started creating lot of applications.

11.11 How the Key loggers spread

Key loggers spread via emails as attachments
Key loggers spread via PTP networks
Key loggers spread due to a web page

11.12 There are many software based key loggers are there

Hypervisor-based, Kernel Based, API Based, Form grabbing based, Memory injection based Pocket Analyzers, Remote access software Keyloggers

11.13 Hardware based key loggers

Firmware based , Keyboard hardware , wireless keyboard sniffers, Keyboard overlays, Acoustic Keyloggers, Electromagnetic emission, Optical surveillance, Smartphone sensors

Figure - Hardware based Key Loggers

11.14 Prevention from Key Loggers

Use good anti-virus with very recent database
In banking transactions use two times authentically and one time password Use virtual keyboard

11.15 Spyware Attacks

Spyware is malicious software. It collects the users' info covertly. This information will be utilized for commercial purposes. Spywares are mostly used to monitor the internet users and offer them targeted advertisements. System monitors, adware, trojans and tracking cookies all will come under spyware only. Spyware gets installed itself by deceiving users or using software vulnerabilities. Spyware is making use of loopholes that are available in internet explorer.

Spyware affects the computers which are already affected by many infections. Once spyware got infected we can see lot of performance issues in the system. A spyware infection can create significant unwanted CPU and Memory utilization, long system boot timings, application crash, blue screen of death, applications freezing and etc.

Some spywares disables the anti-virus, will not allow installing anti-virus, will not allow opening goggle page, will stop the firewall, will decrease the security options of the internet explorer and etc. Some spywares remove the equivalent competitor spywares.

In vista all the activities are happening as a user. This prevents spyware activities up to some extent.

Movieland,WeatherStudio,Zeng,CoolWebSearch,FinFisher,HuntBar,Internet,Optimizer,Zlob Trojan are some of the spywares.

11.16 Password Cracking Attacks

Passwords are the entry tickets to IT and other enterprise resources. They provide access to the files, shares, printers, VPN, e-mail servers, and the network. Hacker may crack the passwords and misuse them. Lot of password theft is happening in the internet only. Within the organization internal thefts also happening. Social engineering made the internal password theft as an easy job. Nearby people can hear the passwords, may see the passwords and make use of them when the password owner is not there. One should not write the password and keep in anywhere in the house or office. Keeping the passwords on the laptop and desktops, emailing passwords to some group of users in the office are bad practices.

11.17 Weak Passwords and Strong Passwords

Easily hack able and crack able passwords are bad passwords or week passwords. Using the user account parameters like first name, last name, Spouse name, street address, your mobile

number are bad ideas and the passwords can be easily cracked. Having password sequence or letter sequence which are all mentioned in the password cracking dictionary are bad ways of selecting the passwords. For easily remembering people sued to take simple passwords made up of English lowercase letters. That also not a good idea. The passwords like 123456789 , Password, 0123456789, Qwerty, Abc123456, abc123456789, aaa111111, aaa1234567, hiIloveu, adobe123, 123123, Admin, 1234567890, Letmein, Photoshop, 1234,Monkey, Shadow, Sunshine, 12345 are the mostly used passwords by vulnerable people.

Passwords that are having more than six characters without the user name partially or fully, without having any personal information, combination of upper and lower case letters, special characters like @#$%^&* are not easily crack able and if any one hacker tries to hack the strong password
It will take years.

To prevent password thefts the week passwords should be converted into strong passwords as shown below.

Original Weak Password:	**New Strong Password:**
LouvlleSlgr	**L*6v11E5Lgr**
AcmeIT	**aC&3i7**
QwERty	**Y7#RQ^e**
BJones25	**890NEs2%**
1TechRepublic1	**T3CH&R3pU8Lic**

Hard passwords are hard to crack but it is possible. Length of time to crack passwords of varying complexity is tabulated below.

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:

k – Thousand (1,000 or 10^{-3})
m – Million (1,000,000 or 10^{-6})
bn – Billion (1,000,000,000 or 10^{-9})
tn – Trillion (1,000,000,000,000 or 10^{-12})
qd – Quadrillion (1,000,000,000,000,000 or 10^{-15})
qt – Quintillion (1,000,000,000,000,000,000 or 10^{-18})

Table Length of time to crack passwords of varying complexity

12. Implementation

12.1 Introduction

This projects focus on the Network design, implementation and securing communication of Golden Bank enterprise infrastructure.

12.2 Project Areas / Skills / Environments

- Virtual LANs
- Inter-VLAN Routing
- WAN technologies
- Network Security
- Network Troubleshooting
- Security policy
- Firewalls
- Proxy servers
- Encryption
- Virtual Private Networks
- Intrusion Detection technologies
- DMZ
- Authentication Systems

12.3 Deliverable

- Working configuration
- Overall Banks Network Architecture
- Network Architecture Brief
- Datacenter LAN Network overview
- WAN network flow for Bank branches
- IP network schema
- DC Connectivity schema
-

12.4 Solution

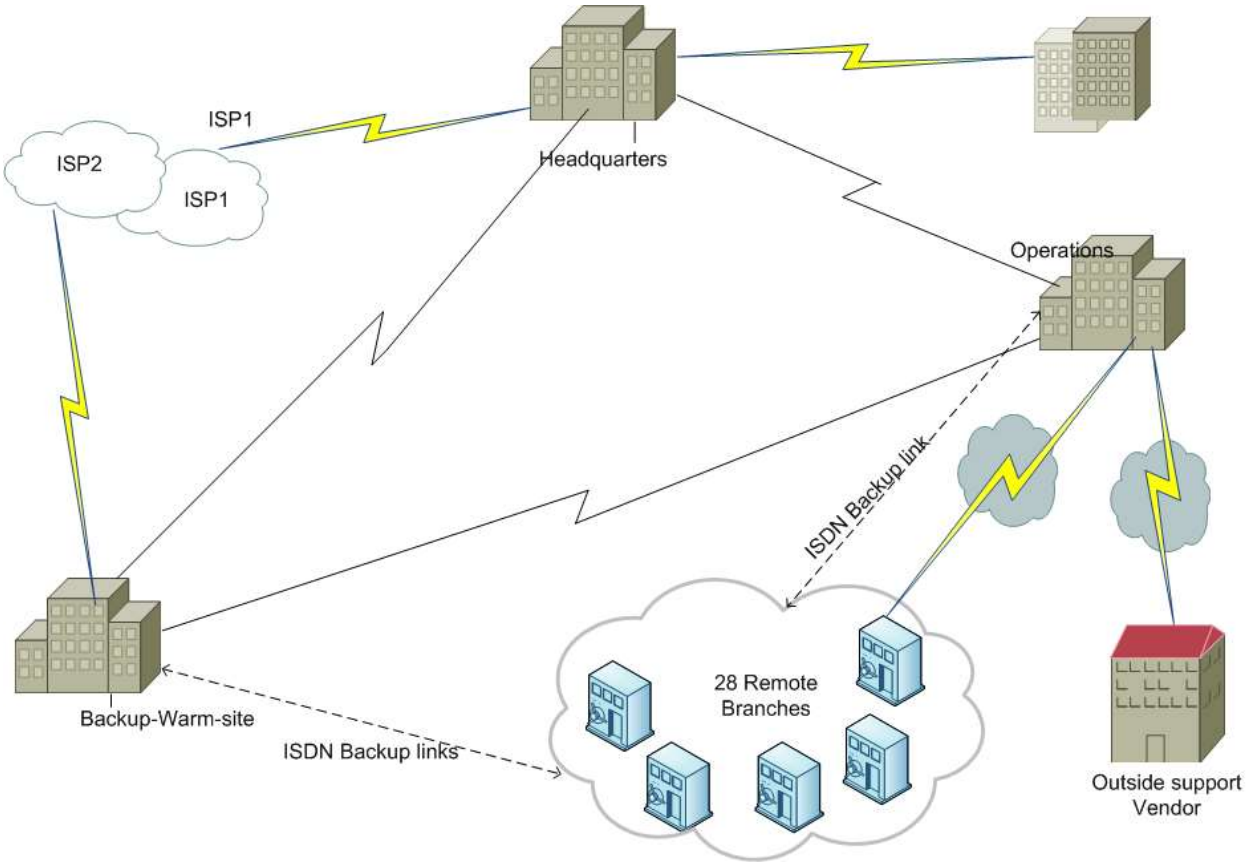
The proposed IT Infrastructure Modification Plan (the "IT Plan") has been developed in accordance with the industry standard Information Technology Infrastructure Library ("ITIL") model

Several benefits that will result from the implementation of the IT Plan follows:

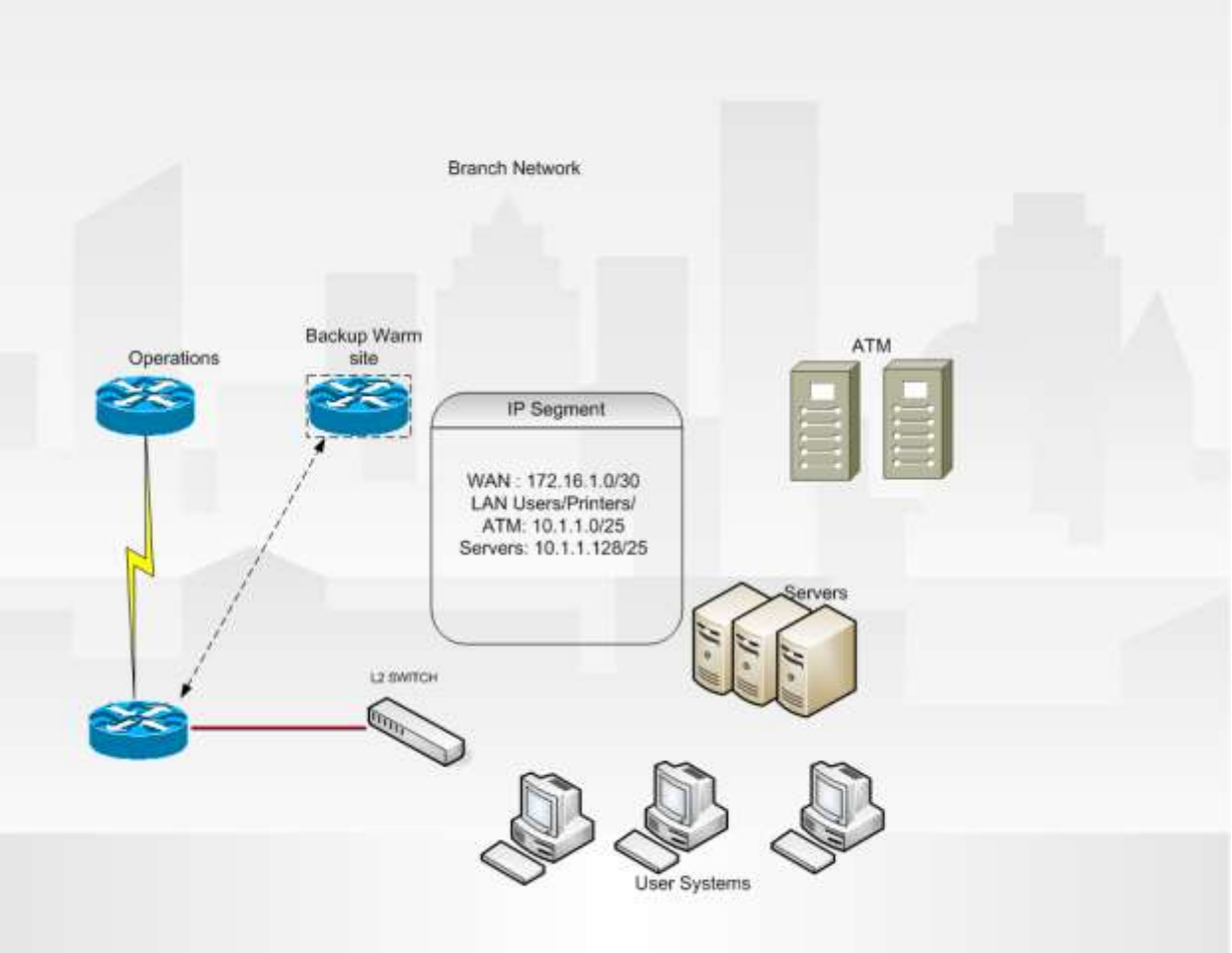
1. Improve security and management of data across the network
2. Provide Network failover for all Remote Branches and applications across the network
3. A significant reduction of IT support costs for Network management
4. Improved disaster recover tools included at no additional cost because they are built-in to many of the server based software products

12.5 Network Design:

12.5.1 Network Topology Diagram



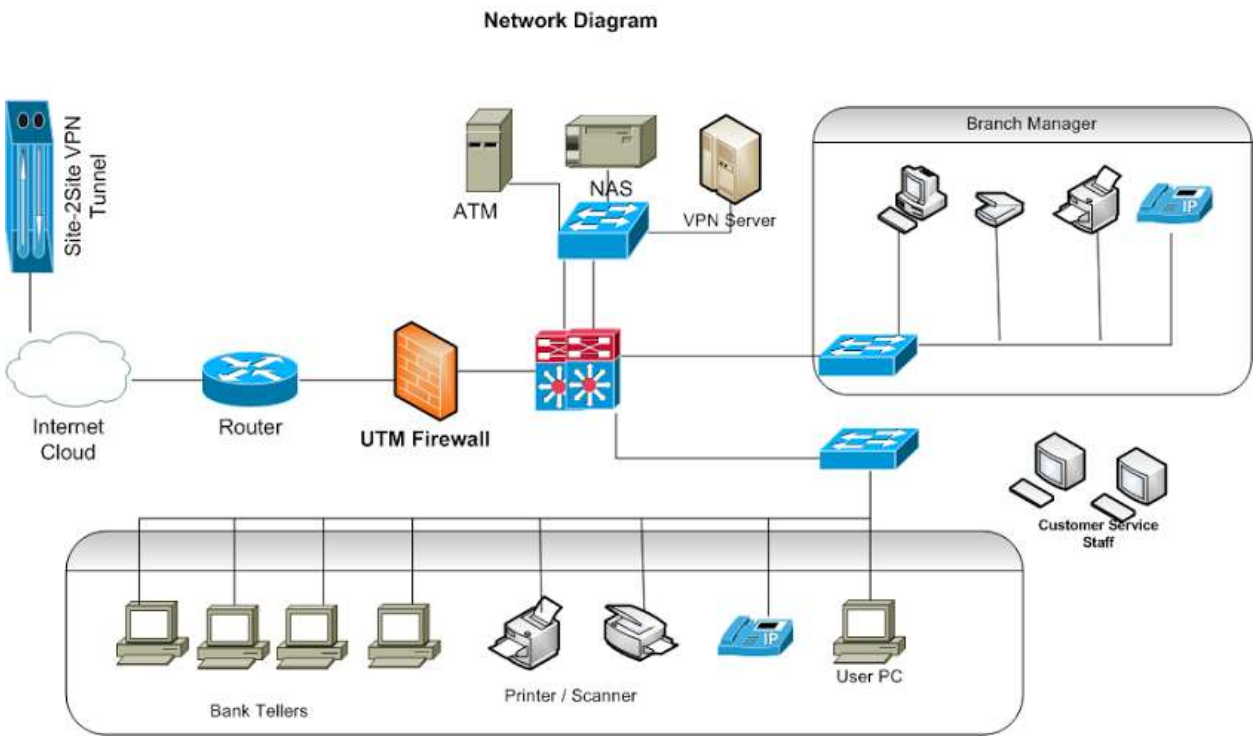
12.5.2 Sample Layer-3 diagram



The VSD file for L3 Diagram is attached here.

BranchL3Diagram.vsd

12.5.3 Proposed Security Design for Golden Bank



The VSD file is attached here

Proposed Security Design for Golden Bar

12.6 Proposed Security Design

The following investigation and design are based on the topology diagram as the topology diagram explains the requirements of the proposed design well. Branches are connected to Operations via 2-mbps links depending No. of users in the branches the WAN bandwidth can be increased. Implemented multiple redundancies for WAN as well as LAN. Connectivity between branch and Operations and Backup warm site is encrypted with IPsec 3des for banking application traffic. Centralized network management, monitoring and access control has been implemented.

There are lots of Branch LAN infrastructures available. They provide connectivity to the end devices to access the GB Operation through frame relay link. ISDN backup terminated at all remote locations which can be used when the primary link fails. ISDN link can be used for Operations and backup warm site connectivity for backup purpose.

12.7 VLANs requirements

The branch locations have multiple VLANs,

i. Management
ii. Servers
iii. End hosts – Users,printers,ATMs

This provides for private IP address space. These addresses will never be allocated by IANA (Internet Assigned Numbers Authority) as public addresses and are therefore not routable on the Internet. The private address ranges available, with the number of networks and hosts they support are:

Branch network setup

Private IP ranges are as below:-

- ➔ Class A 10.0.0.0 - 10.255.255.255
- ➔ Class B 172.16.0.0 - 172.31.255.255
- ➔ Class C 192.168.0.0 - 192.168.255.255

The private IP (RFC1918) ranges are used in the each branch locations. Depending on the branch size and no of users the subnet has been used at the Branch.

Static and dynamic IP address used at Branches

Static IP address are used for Network devices, Servers, Printers and ATM's

Dynamic IP address used for end hosts like users systems

Branch user can connect to backing application over the WAN link based on the Branch size WAN bandwidth allocated.

The banking application use 12kbps per user to working on day by day activities.

Internet access for branch users can be done through proxy server in Operations and Backup Warm-site and Internet access has been restricted for the Branch users.

All the branch location configured with IPsec tunnel with Operations and Backup Warm-site. IPsec connections would provide secure communication between Branch systems and server which are located Operations and Backup Warm-site
The end-to end communication for banking data encrypted through IPsec tunnel.

Now a day banking farms are hit with virus and malwares. To product the systems from the virus and malwares we deployed antivirus on all end hosts which will get latest definitions from the antivirus servers hosted in Operations and backup warm-site. The antivirus servers in the Operations and Backup warm site will getting latest updates get from the internet repository servers.

12.8 Network Connectivity

- Operations and Backup Warm site are fully redundant with high performance, highly available, scalable network
- All branch office has direct connectivity with Operations and backup warm-site with primary connections of frame-relay circuits and ISDN backup links
- The deployment includes of third level backup for all remote branch with ISDN connectivity to backup Warm site, this third level backup used when the Operations site it totally isolated are major outage on the primary site.
- GB business processes rely on a combination of systems including Internet, IPX/SPX can used in the WAN
- The Golden Bank network used for dynamic protocol used in the WAN for better performance and easy troubleshooting purpose
- Using the dynamic network protocol automatic failover will be triggered for the WAN locations. The primary link to Operations fails the frame-relay circuit will automatically ISDN link will be established with Operations site the delay of the complete

establishment is around 20 seconds. As soon as the primary frame-relay link restores the ISDN link will be idle ad will be in standby state in next 30 so there will be not transaction failure for the end used and remote locations

- The circuit of frame-relay and ISDN connectivity failure to Operation office. The remote branch can fire the ISND to backup warm-site further the traffic can reach the Operation through Backup warm site. This is called as a third level backup for branch. This network design provide 100% uptime to the Golden bank business
- The traffic over the frame-relay and over the ISDN will be encrypted with IPsec tunnel for the better security of the data
- Access control list has been applied on the each branch LAN to avoid known network attacks
- Operations and Backup Warm site has Distributed core network architecture deployed in Golden bank typically interconnected to other data center, remote location branch offices, headquarter office and third party vendor sites.

12.9 Branch location WAN router configuration

```
interface Loopback100

 ip address 172.240.147.38 255.255.255.255

!

interface FastEthernet0/0

 description GB BRANCH LAN

 ip address 172.20.1.1 255.255.255.128

 ip access-group 115 in

 ip access-group 115 out

 speed auto
```

```
!
interface Serial1/0
 description connectvity to Operation and Backup warm site
 bandwidth 128
 backup delay 20 30
 backup interface BRI0/0/0
 encapsulation frame-relay
 frame-relay lmi-type ansi
 frame-relay map ip 172.20.1.100 102 broadcast
 crypto map pix
!


!
interface BRI0/0
 description ISDN BACKUP
 ip unnumbered Loopback100
 encapsulation ppp
 dialer idle-timeout 3000
 dialer string XXXX xxxxxx -- Operations site
```

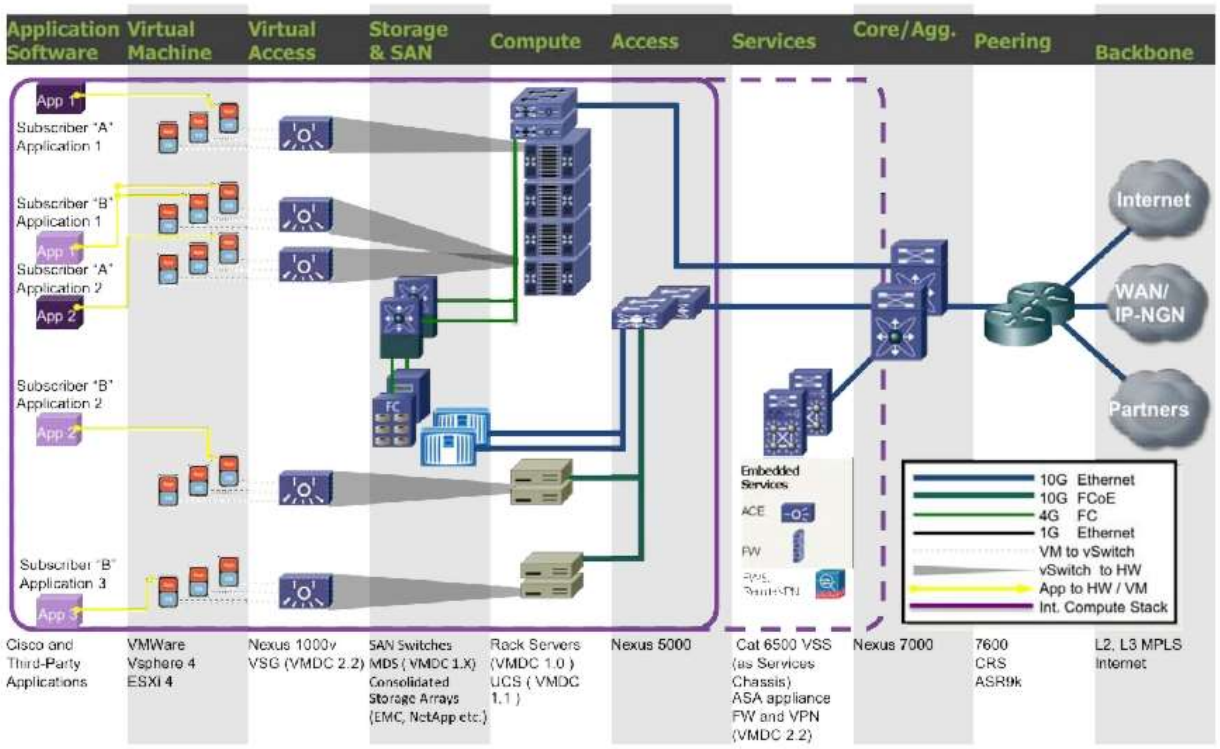
```
 dialer string XXXX xxxxxx -- Backup Warm site
 dialer-group 1
 isdn switch-type basic-net3
 ppp authentication chap
!
router ospf 1
 log-adjacency-changes
 area 30 stub no-summary
 network 172.20.1.1 0.0.0.127 area 81
 network 172.240.147.38 0.0.0.0 area 30
```

Above similar configuration used for all remote location with respective IP subnet on each location.

12.10 Data Center Overview

System overview of Operations Data center and the similar setup used for Backup warm site it is also called as Data recovery center. Data center designed as Three-Layer Hierarchical Model Core, Data center aggregation and access layer. The design hierarchical mode provides such scalability, resilience, performance, maintainability, and manageability. Redundant systems and connectivity for end to end links at each level protected from single point of failure

This design simplifies the management for entire datacenter which incudes of troubleshooting and configuration on each level



12.11 Storage Area Networks

Better performance

High availability features of Storage devices provided through multi-level redundancy

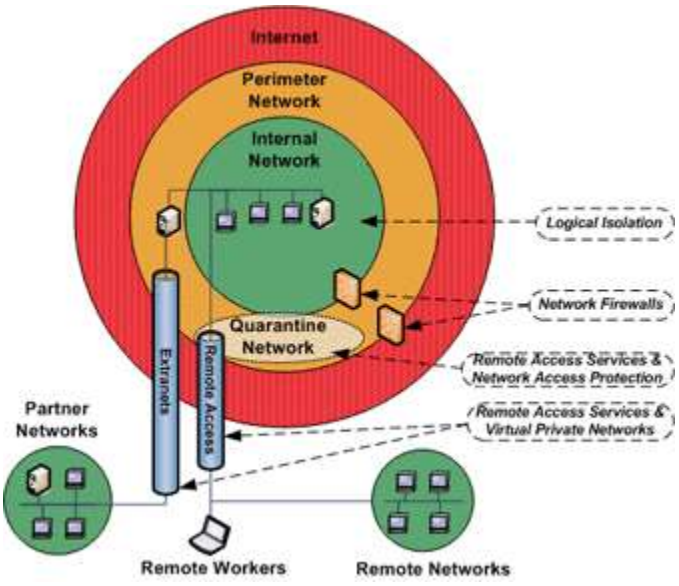
CIFS and NFS protocols used for high speed data transfer

12.12 Security infrastructure and Firewalls

Golden bank data centers secured with internal and perimeter firewalls. The Intrusion Detection System and Intrusion Prevention system deployed in Perimeter network to secure the Data center assets from the vulnerability and network attacks. The firewall policy configured to block everything except specified traffic for bank applications and limited to internet access. The IPS/IDS monitor and records every transaction of vulnerable pattern and alerts to banking security personnel. This design is highly effective in identify and restrict the vulnerable traffic of Golden bank. Traffic from internet reaching to the bank perimeter network the data pass through an IPS. IPS monitors and if found anything vulnerable it denies at perimeter level itself it also

includes of Internet-based attacks. The IPS device gets latest update from internet repository server to mitigate the latest threads

Logical security infrastructure Diagram of Golden Bank



12.13 Data backup and recovery procedures.

In the existing design NASs at the branches to back up the data generated locally, however the vast majority of data is backed up to the File Server Operations facility through the network.

The centralized backup and recovery systems are deployed at Operations and Backup warms site. The SAN used to have live data replication between data canters (Operations and Backup warm-site). Regular and daily backup are configured during the maintenance hours for banking data's. Periotic backup and recovery checks will be performed. The periotic checks will help from the failure of backup Instance, Application and Media failure due to damage of disk

12.14 Remote access solution

Remote access solution provides secure way to access Golden bank assets and line-of-banking applications from outside the bank network it include of resource access from mobile devices.

Below the Security Considerations and solution of remote access

- Two factor authentication has been implemented for User authentication
- Remote access VPN configured with Split tunneling
- Firewall policy implemented for Remote users to access Golden bank assets
- High availability and Resiliency provided for VPN devices between Operation and Backup warm site in case of failure of VPN device at Operations the still remote user can work using backup warm site VPN solution
- For the security measure Remote Access SSL VPN Gateway Sessions are Recorded with this solution

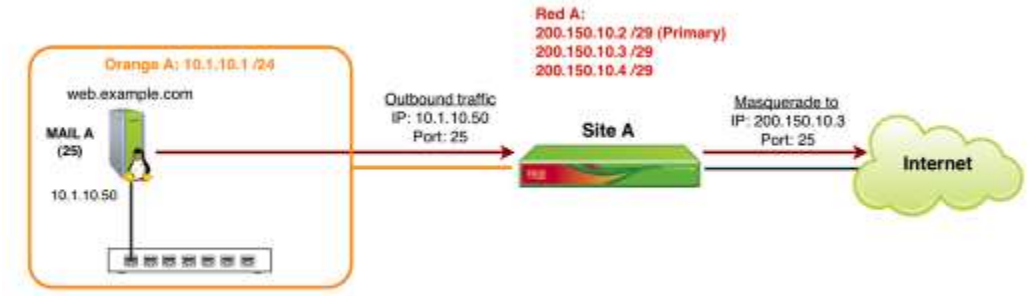
12.15 Implementation of Endian Unified Threat Management system – POC

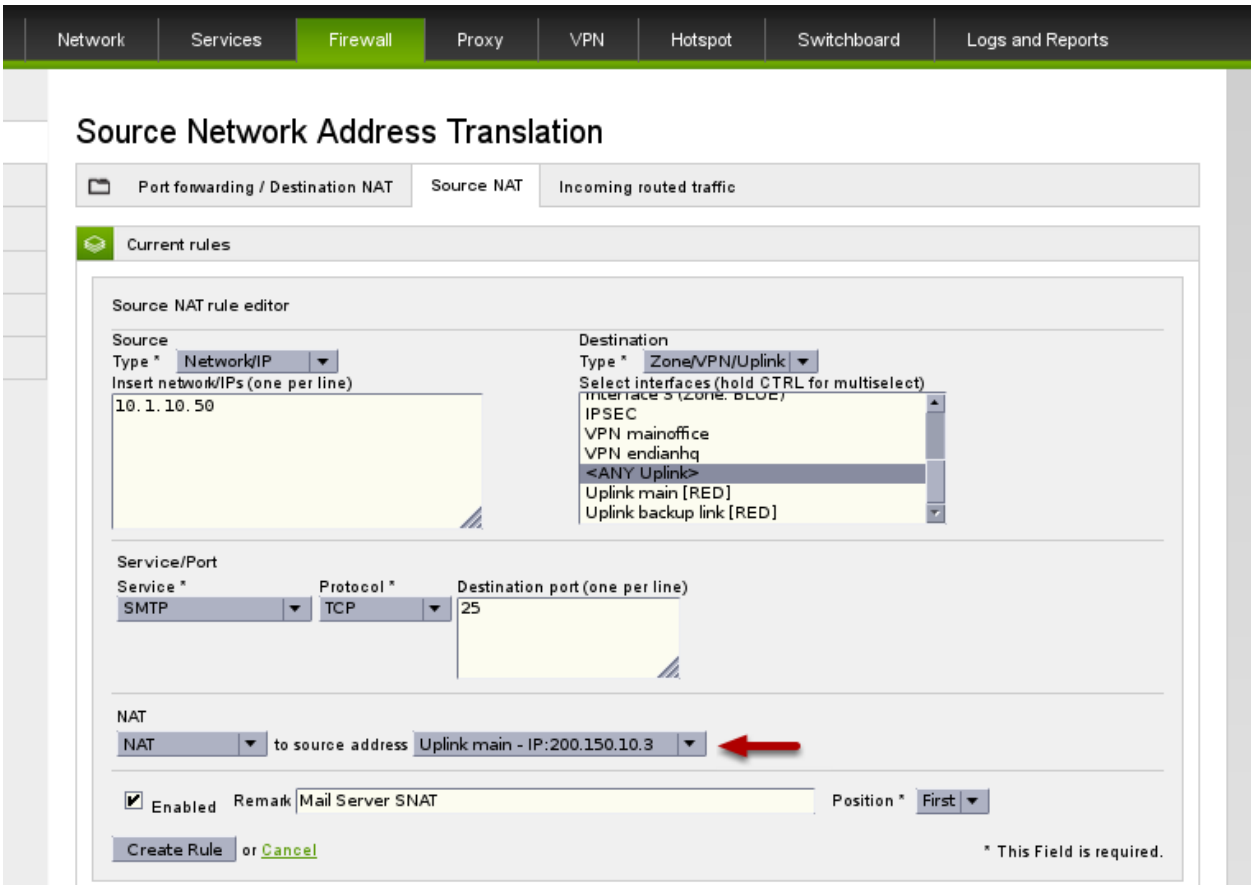
Below the process of installing and configuring the Endian Firewall, with Advanced Proxy for LDAP authentication and very granular proxy control and URL & content filtering.

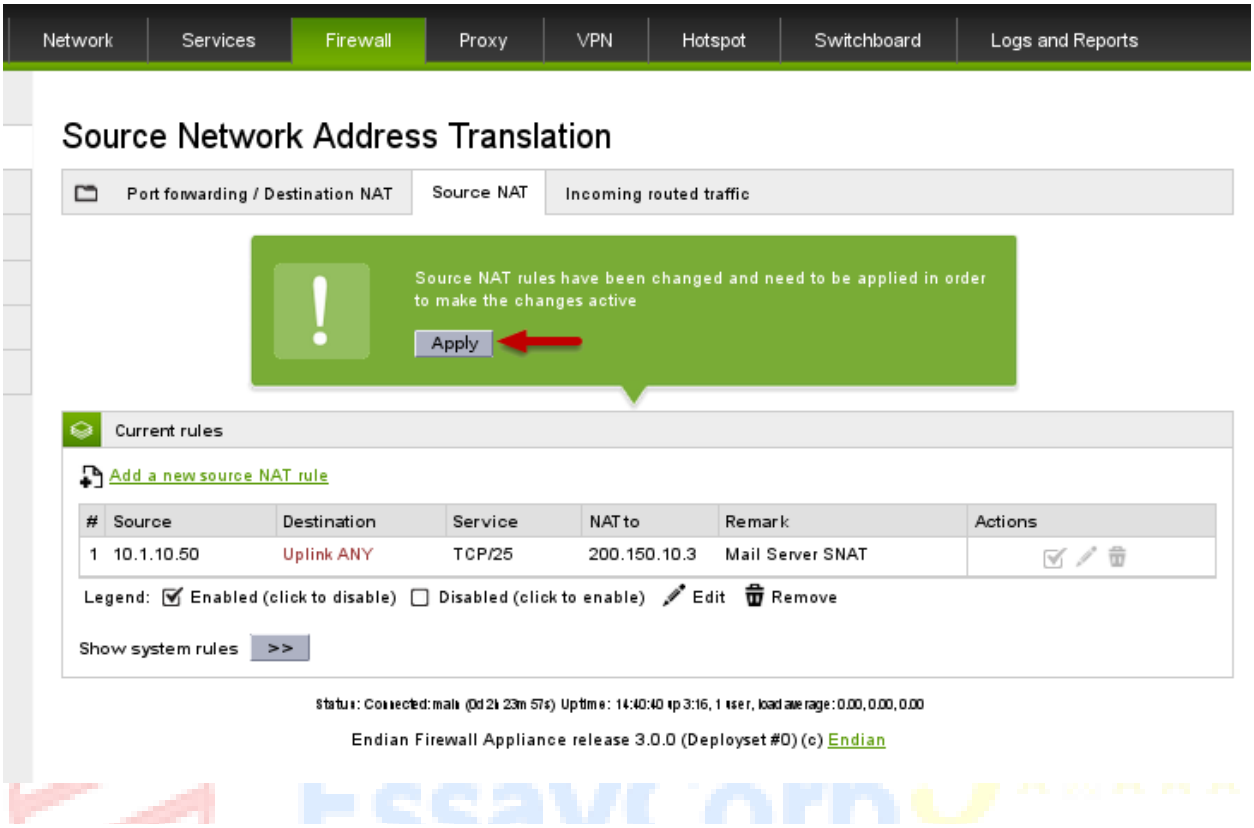
NATting configured for internal users to access internet and External vendor support. Blocked non-business related websites in firewall

Proxy service used for secure internet service and better internet performance

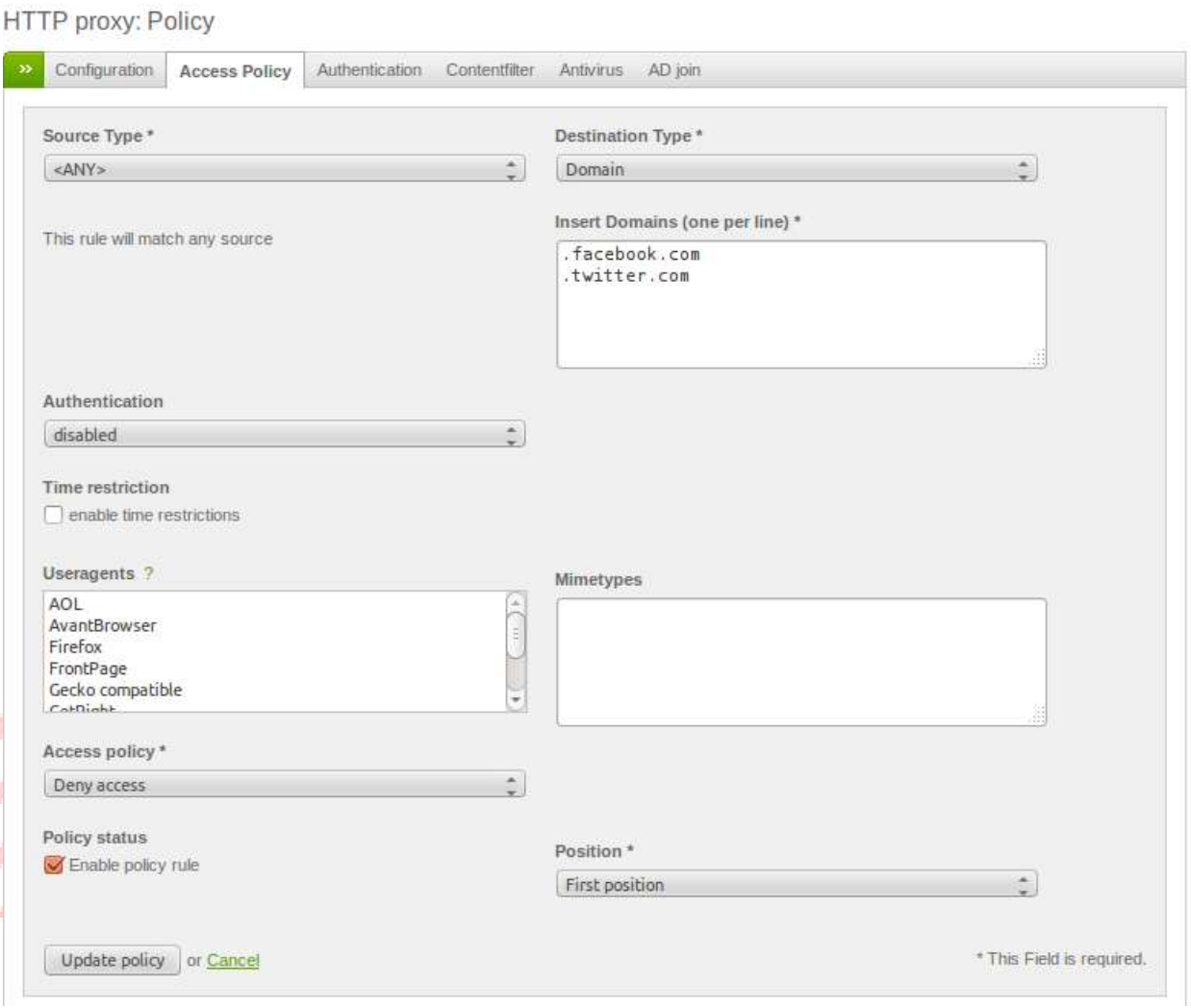
NATting configured for internal users and External vendor support


Red A:
200.150.10.2 /29 (Primary)
200.150.10.3 /29
200.150.10.4 /29
Orange A: 10.1.10.1 /24
web.example.com
MAIL A
(25)
10.1.10.50
Outbound traffic
IP: 10.1.10.50
Port: 25
Site A
Masquerade to
IP: 200.150.10.3
Port: 25
Internet


Network
Services
Firewall
Proxy
VPN
Hotspot
Switchboard
Logs and Reports
Source Network Address Translation
Port forwarding / Destination NAT
Source NAT
Incoming routed traffic
Current rules
Source NAT rule editor
Source
Type * Network/IP
Insert network/IPs (one per line)
10.1.10.50
Destination
Type * Zone/VPN/Uplink
Select interfaces (hold CTRL for multiselect)
IPSEC
VPN mainoffice
VPN endianhq
<ANY Uplink>
Uplink main [RED]
Uplink backup link [RED]
Service/Port
Service *
SMTP
Protocol *
TCP
Destination port (one per line)
25
NAT
NAT
to source address
Uplink main - IP:200.150.10.3
Enabled
Remark
Mail Server SNAT
Position *
First
Create Rule
or Cancel
* This Field is required.


Network
Services
Firewall
Proxy
VPN
Hotspot
Switchboard
Logs and Reports
Source Network Address Translation
Port forwarding / Destination NAT
Source NAT
Incoming routed traffic
Source NAT rules have been changed and need to be applied in order to make the changes active
Apply
Current rules
Add a new source NAT rule
Source Destination Service NAT to Remark Actions
1 10.1.10.50 Uplink ANY TCP/25 200.150.10.3 Mail Server SNAT
Legend: Enabled (click to disable) Disabled (click to enable) Edit Remove
Show system rules >>
Endian Firewall Appliance release 3.0.0 (Deployset #0) (c) Endian

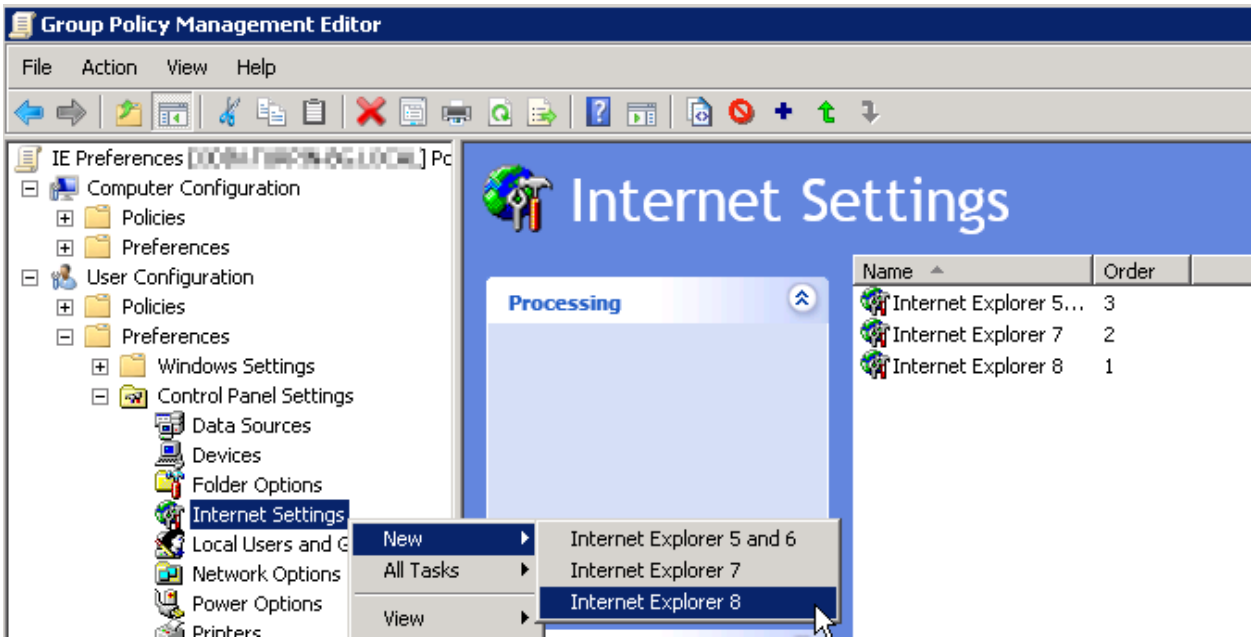

HTTP proxy: Policy
Configuration
Access Policy
Authentication
Contentfilter
Antivirus
AD join
Add access policy
Policy Source Destination Authgroup/-user When Useragent Actions
1 filter for virus ANY ANY not required Always ANY



12.16 Proxy Solution and Web proxy configuration

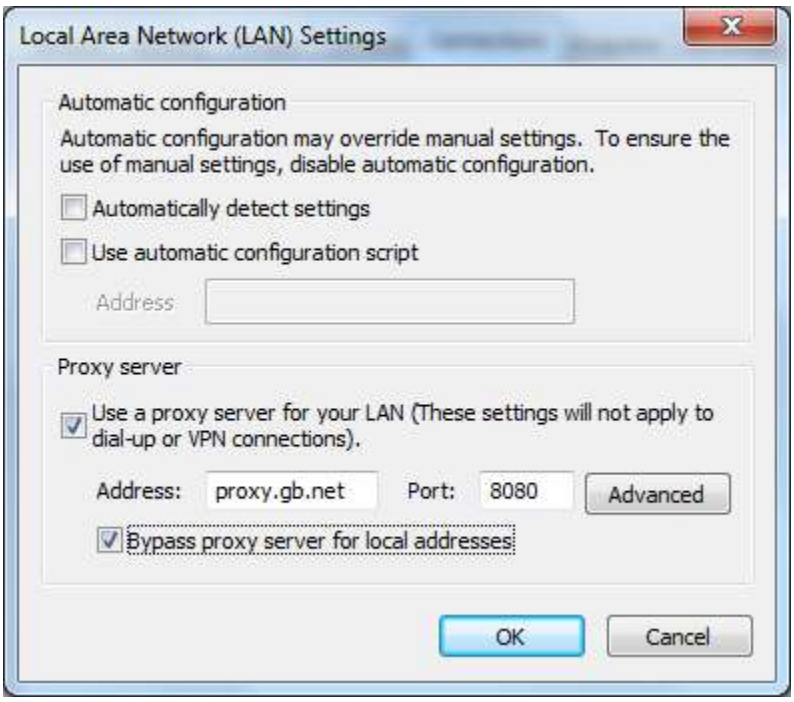
Explicit proxy solution provide for Golden bank

End host are configured with proxy server information (proxy.gb.net) on web browser to send internet request to proxy server. Users no need to configure the proxy settings manually. It has been deployed through group policy. Below the group policy template used in active directory server

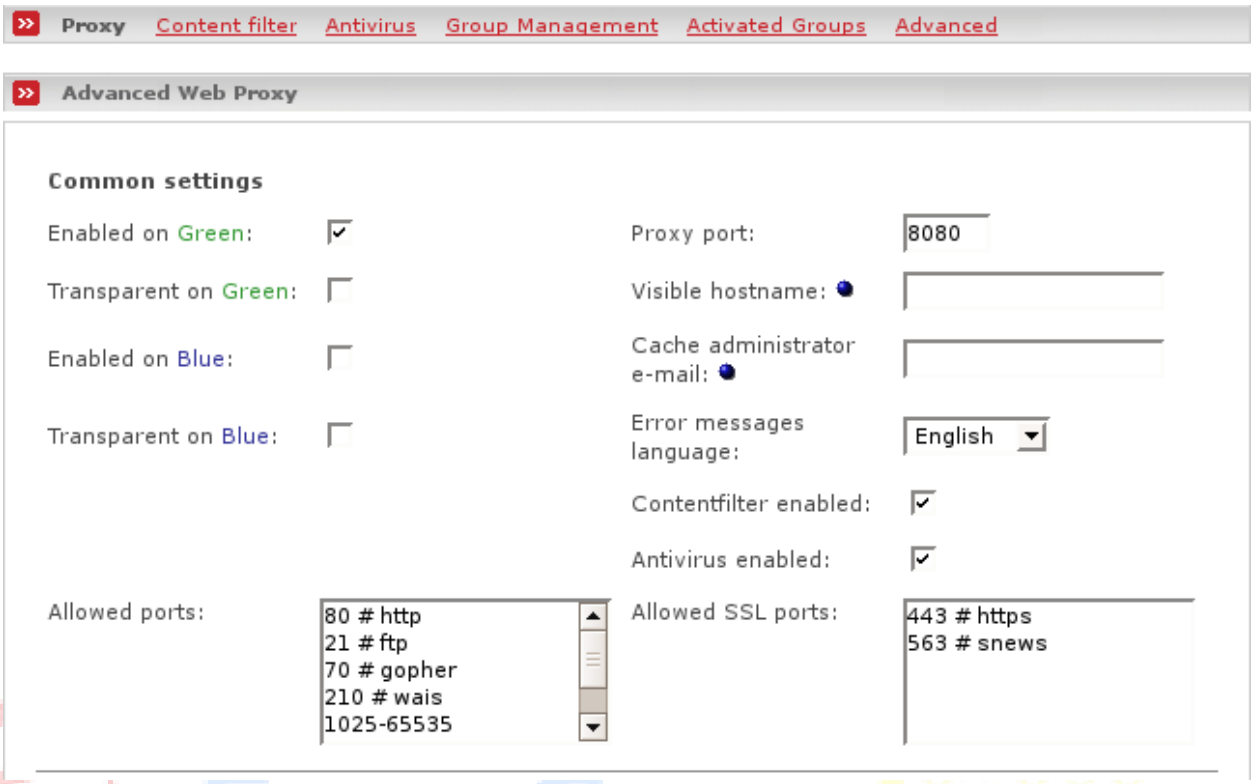


Proxy.gb.net is the proxy server deployed in Golden backup data centers.

The result of the GPO implementation the below settings will reflated at user browser settings.

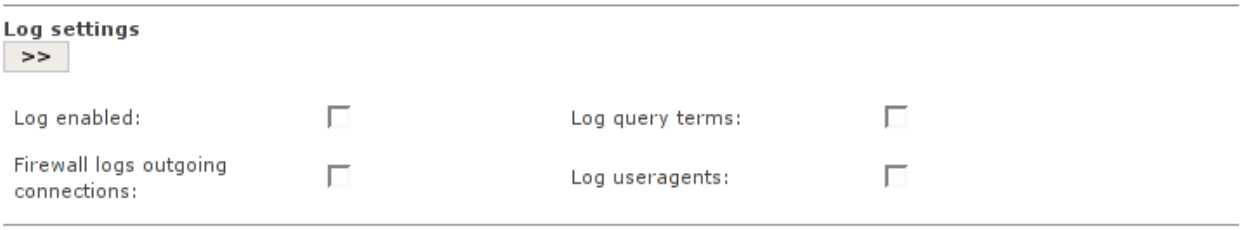


Client HTTP request will forward to proxy server through the browser. The proxy server configured with exclusion for internal networks and application so only internet request will be process in proxy server. Authentication enabled on the proxy server so the every the user attempts are monitored and recorded. The proxy server deployed in cluster for redundancy and better performance. The proxy virtual IP address applied for end hosts.

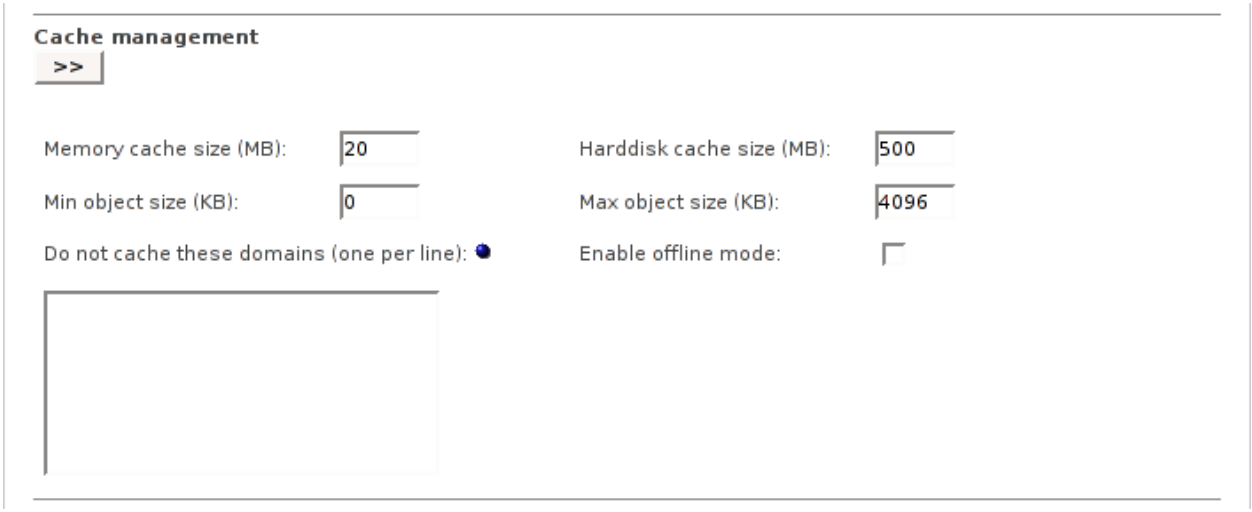


Log enabled

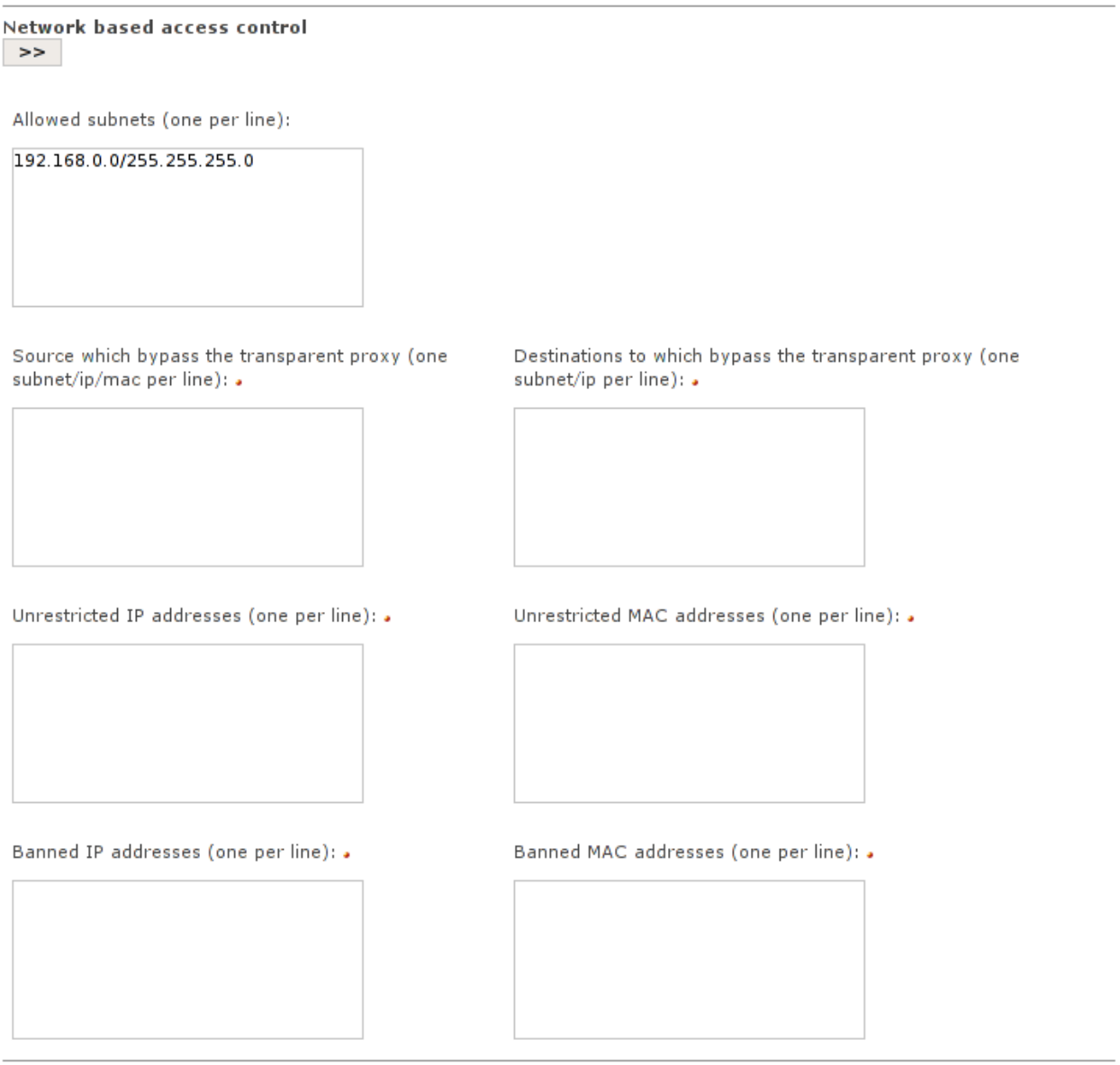
This enables the Web Proxy logging feature. All client requests will be written to a log file and can be viewed within the GUI under Logs > Proxy Logs



Cache management



12.17Network based access control


Network based access control
>>
Allowed subnets (one per line):
192.168.0.0/255.255.255.0
Source which bypass the transparent proxy (one subnet/ip/mac per line):
Destinations to which bypass the transparent proxy (one subnet/ip per line):
Unrestricted IP addresses (one per line):
Unrestricted MAC addresses (one per line):
Banned IP addresses (one per line):
Banned MAC addresses (one per line):

12.18 Network security attacks tests

After implementing the Golden bank network the testing has been carried out for security devices for following

- Known vulnerabilities
- Data leakage tests
- DDos attacks
- QoS metrics

  This test carried out for Firewalls, VPN devices, Intrusion prevention systems (IPS) and IDS devices and Antivirus

13. References

[1] 20-minute Intro to Hacking | MikeGagnon.com. 2015

http://mikegagnon.com/2013/03/17/20-minute-intro-to-hacking/

[2] Password strength - Wikipedia, the free encyclopedia. 2015.

http://en.wikipedia.org/wiki/Password_strength

[3]The guide to password security (and why you should care) - CNET. 2015

http://www.cnet.com/how-to/the-guide-to-password-security-and-why-you-should-care

[4] Phishing - Wikipedia, the free encyclopedia. 2015.

http://en.wikipedia.org/wiki/Phishing.

[5] Google Hacking: Ten Simple Security Searches That Work - EH-Net Online Mag. 2015.

https://www.ethicalhacker.net/features/book-reviews/google-hacking-ten-simple-security-searches-that-work

[6] Wireshark Network Analyzer: Review, Tutorial, Free download. 2015.

http://www.thewindowsclub.com/wireshark-network-analyzer-free-download.

[7] How to Encrypt Your Email | PCWorld. 2015. http://www.pcworld.com/article/254338/how_to_encrypt_your_email.html.

[8] A detailed guide on installing Kali Linux on VirtualBox - blackMORE Ops. 2015

http://www.blackmoreops.com/2014/04/08/detailed-guide-installing-kali-linux-on-virtualbox/.

[9] Use SQLMAP SQL Injection to hack a website and database in Kali Linux - darkMORE Ops. 2015

http://www.darkmoreops.com/2014/08/28/use-sqlmap-sql-injection-hack-website-database/.

[10] Hack Like a Pro: How to Crack Passwords, Part 3 (Using Hashcat)

http://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-3-using-hashcat-0156543

[11] How to Hide Files inside Pictures. 2015. How to Hide Files inside Pictures.

http://www.instructables.com/id/How-to-Hide-Files-Inside-Pictures/. [Accessed 28 May 2015].

[12] Phish Tank > What is phishing? (Definition of phishing, with examples). 2015.

https://www.phishtank.com/what_is_phishing.php. [Accessed 28 May 2015].

[13] How to Open Files with Unknown (or Missing) File Extensions. 2015

http://www.labnol.org/software/unknown-file-extensions/20568/. [Accessed 28 May 2015].

[14] Marco Pontello's Home - Software - TrID. 2015.

http://mark0.net/soft-trid-e.html. [Accessed 28 May 2015].

Related Topics :

Network Security Assignment Help

Computer Network Assignment Help