

IDRBT's Working Paper No. 8

Enterprise Network Security

- V. P. Gulati and V. Radha

ABSTRACT

This paper maps out the need for Enterprise Network Security, an area of concern in this networked world, and explains how to go about achieving it.

Stressing on the process of building an Enterprise Network, it details the various possibilities of interconnecting Networks and Application Servers, the possible threats and mitigating them, and connecting an Enterprise Network to Internet.

1.0 Introduction

Communication is the foundation for every activity, be it financial, commercial, social or that of the government. Internetworking has drastically changed the way we communicate, so much so that Computer Networks and Web Browser technology is fast gaining acceptance as the de-facto standard of communication. Internet Technology along with TCP/IP protocol has changed office automation and business processes radically. TCP/IP is an Internetworking protocol, capable of interconnecting different networks like LAN and WAN.

Most of the Banks have either set up or are in the process of setting up LAN and WAN for their own intra-bank activities. The INdian Financial NETwork (INFINET), managed and operated by the IDRBT can also be used for intra-bank communication.

1.1 INdian Financial NETwork (INFINET)

The INdian Financial NETwork became operational in June 1999. It started off as a VSAT-based network on extended C band with 1/8th of a transponder on Insat 3B and was upgraded to a full transponder by August 2000. The Network now has over 1000 VSATs spread across the country, and has three 512 kbps out-routes and 48, 128 kbps in-routes. The Network would shift to Insat 3C shortly.

1.2 Integration with Leased Line Network

The need to strengthen the VSAT based network by alternate, high bandwidth communication media led to its expansion with Leased Line circuits. Now, the INFINET is a blend of VSATs and Leased Lines, providing users better quality and high availability.

Twenty-one major cities of the country are connected through Leased Lines with the RBI offices and the IDRBT as the nodes. These nodes, in-turn, can extend the communication link further to the banks. The Voice over IP facility on the Leased Line Network is facilitating voice communication between all the offices connected through the Leased Line Network.

1.3 Network Management System

INFINET is spread across the length and breadth of the country, and manning the network is a daunting task. The whole network is remotely configured, and monitored from the IDRBT and the RBI, Central Office, Mumbai, using TNG-Unicentre, the network management software.

This Network Management System (NMS) is capable of monitoring the network, providing the requisite alerts and has high quality reporting features.

1.4 The Road Map

Plans are afoot to upgrade the VSAT Network to increase its bandwidth and make it more effective. The specific areas of focus include:

- Interconnection and integration with the present extended C-band VSAT service providers.
- Strengthening the Leased Line Network by connecting some more places, increasing bandwidth and providing backup links

1.4.1 Disaster Recovery and Back Up

1.4.1.1 Back Up: Plans are in place to set up a similar kind of Hub as in IDRBT, Hyderabad, at Pune, because it is the most unlikely location to be hit by natural disasters.

1.4.1.2 Remote Branches: Presently, in case of satellite/VSAT failure, remote branches with VSAT connectivity cannot communicate to INFINET, though INFINET has Leased Line connectivity, as the remote branches may not be able to afford the Leased Line. Allowing ISDN and PSTN dial-in to a leased line node (RBI Office), or to the IDRBT hub, can act as a back up for such remote branches.

Back Up links can also be provided to the existing leased lines by using ISDN links and parallel leased lines from different communication service providers.

1.5 Members of INFINET

Initially, INFINET started as a Closed User Group with the RBI and Public Sector Banks as its members. Owing to the demand from a wide variety of financial applications running on

INFINET, and their users, the Network has been opened up for Primary Dealers, Satellite Dealers, Foreign Banks, Private Sector Banks, Financial Institutions and Cooperative Banks etc.

Mission critical business applications like SFMS, ATM, CBS, EFT, Forex, PDO-NDS and back-office applications like Mail Messaging, Intranet, and MIS etc are ported and running successfully on the INFINET.

1.6 Present Scenario

- Many banks are connected to the INFINET through VSATs.
- INFINET is expanding in terms of capacity, availability, accessibility and redundancy. Leased Lines have already been integrated with the VSAT network, making it a blend of communication technologies.
- At some locations, banks have connected their Local Area Networks to the INFINET through a Router, NAT, Proxy or a Firewall.
- Many banks are communicating over the INFINET, and it is the backbone for their intra-bank communications.
- Some banks are using INFINET as the backbone for inter-city communication and are augmenting the Network with intra-city Leased Lines.
- Some banks have also set up their own Private Network using Leased Lines and ISDN Lines. These Private Networks are also being connected to INFINET.

1.7 Future Scenario

- Banks may like to access Internet through their own Private Network for various bank/business applications.
- Banks may also like Internet (External network) to access a location of their Private Network for Internet Banking, i.e. Banks may open up the services over the Internet.

There is a great deal of confusion prevailing on how to connect all these networks in a secured manner. Though INFINET is a Closed User Group, it has always been an issue whether the security provided is good enough, or the banks should go in for their own security set up, taking into consideration their specific business requirements.

This paper discusses how to connect these networks, segregate security levels, and counter the risks involved.

2.0 A Bank's Enterprise Network

In order to carry on their day-to-day business and the related back office administration smoothly, banks have to set up Local Area Networks at their major branches. These branches then need to be connected with their own enterprise private network to collect and disseminate MIS for fast decision making and to allow anywhere banking. Banks may have to connect some of these locations to INFINET for inter-bank applications and to Internet for Internet Banking or for providing service to their business partners.

2.1 Emerging Scenarios

The following diagram illustrates the various scenarios that are emerging as choices for the banks to build their own enterprise networks using various communication services.

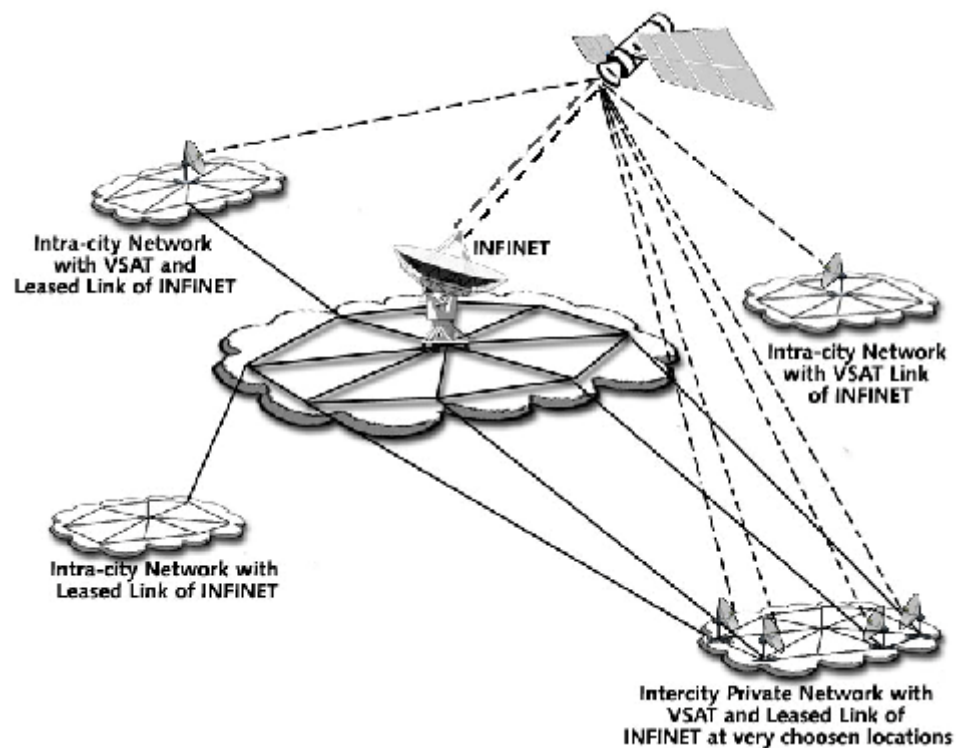


Fig 1: ENTERPRISE NETWORK SCENARIOS

2.1.1 Enterprise Network with INFINET as Backbone

In this scenario, the INFINET acts as the backbone for the bank's enterprise network. All the remote locations of the bank are connected to the INFINET links, either through Leased Line or VSAT. The following diagram illustrates such a scenario.

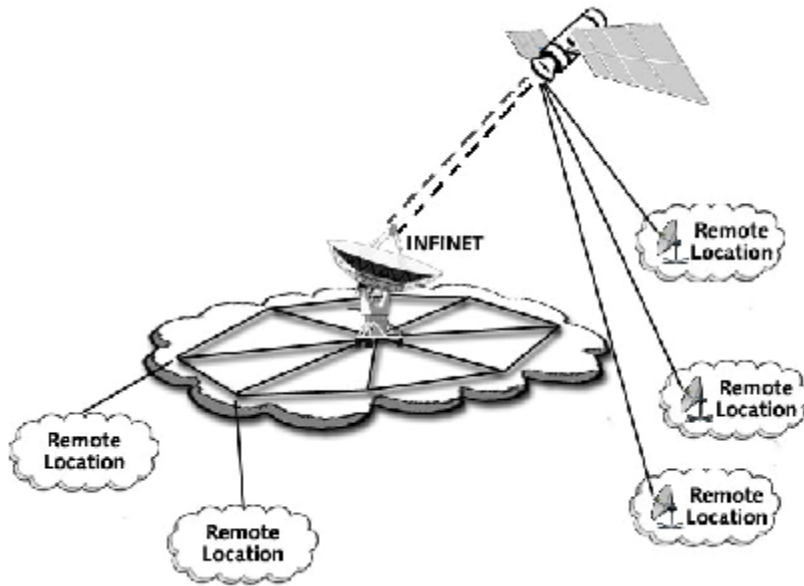


Fig 2: INFINET AS BACKBONE

2.1.2 Enterprise Network with INFINET as Backbone and Augmented by Intra-city Lines

In this scenario, the INFINET acts as the backbone for a bank’s enterprise network for Inter-city communication. For branches within a city, the bank uses either Leased Line or ISDN etc and all the remote cities of the bank are connected through the INFINET, using Leased Line or VSAT.

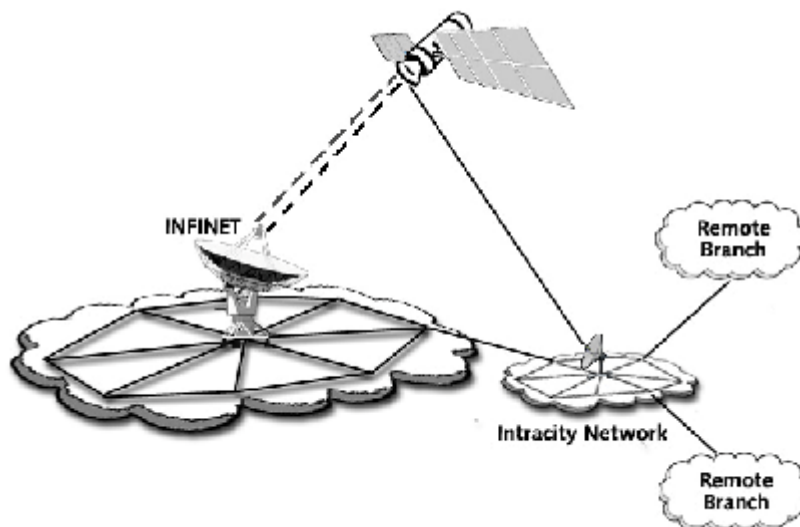


Fig 3: INFINET INTEGRATED WITH INTRA-CITY NETWORKS

2.1.3 Enterprise Private Network connected to INFINET

In this scenario, the INFINET acts as the backbone for a bank's enterprise network only for inter bank applications, as a back up for crucial locations and as a link for remote locations. Here, the bank has used either a Leased Line or ISDN etc to set up its own Private Wide Area Network across cities and only a select few branches are connected to INFINET.

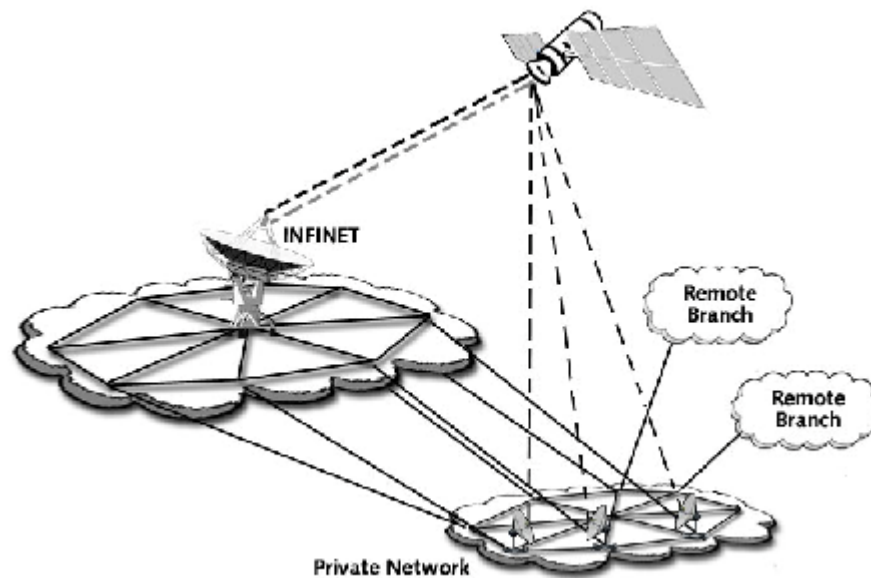


Fig 4: PRIVATE NETWORK AND INFINET

2.2 Communication Links to set up Enterprise Network

Let us consider the enterprise network of a bank as a Wide Area Network, which connects all/many geographically widespread locations of the bank. A bank can set up its enterprise network by using different media from different service providers such as:

- Leased Line Network – Lines taken from MTNL, BSNL and other service providers.
- INFINET Connection - VSAT, Leased Lines of INFINET
- ISDN – From MTNL, BSNL
- PSTN/Dial-up
- Radio Modems etc

The choice would depend upon the availability, manageability, reliability and assured uptime of each media link at various locations. Banks can connect their branches through these media

links seamlessly, as all the service providers provide only dedicated physical links and allow the banks to design their own enterprise network with their unique IP addressing scheme.

However, IDRBT recommends using INFINET IP addressing scheme for the VSATs or Leased Lines connected to INFINET, as the INFINET is a CUG and its chief focus is inter-bank communication.

2.3 Select the Right Network Link

In a scenario with choices galore, it is important to choose the best. Before arriving upon any connection, it would be prudent to group the locations based on remoteness, business, and whether the location should be connected to Inter-bank Applications etc. The network connections should take into account every factor.

A possible choice could be:

- Follow separate IP addressing scheme for Private Network.
Ex: 172.16.x.x IP addressing scheme for LAN
192.168.x.x IP scheme for WAN
10.x.x.x IP scheme for INFINET
- Connect remote locations either by Leased Line, ISDN, PSTN or radio-modem
- Make use of INFINET VSAT connections from IDRBT for very remote locations, where other communication media is not available or is unreliable.
- Make use of Leased Line INFINET connections not only for Inter-bank application locations but also for locations wherever crucial backbone business servers are hosted as this allows the remote locations, with only INFINET connection or only Private Network connection to access these servers

2.4 Segregating Networks

A group of connected computers form a computer network, and the number of such groups may vary. These groups can be segregated by:

- Physical Links: Like hubs and switches on the LAN
- Logical Links: Here the focus is on IP design. This can cross the LAN and cover much geographical spread, connected through many kinds of physical media like ISDN, Leased Line, Radio Modem etc. By proper IP design, setting up routers, and firewalls, one can group the computers as LAN, Bank's own Private Network, INFINET and Internet.
- Control: Who should control the network? For example, the Local office IT personnel control the LAN, the bank controls the Private Network, IDRBT controls the INFINET and many control the Internet.

The security levels should be decided based on who is controlling which network. One has to carefully look into and decide which computers/servers should fall in which group. Often servers can fall into more than one group, as they have to be accessed from many networks. Similarly, normal desktops may fall into a single group in a LAN, as outsiders need not access them. However, the desktops/clients may have to access their Private network, INFINET or Internet depending on the need.

We suggest that a Bank first conduct an in-depth study and then segregate the computers, servers, networks etc, instead of connecting every computer to every network. This would also help in monitoring and controlling the network. As a first step:

- Follow different IP schemes for different networks.
- Make sure unnecessary traffic doesn't flow from LAN to WAN or vice-versa.
- Connect these networks wherever required with router, NAT, Proxy, and Firewall etc.
- Deploy security scanners, Firewalls, Intrusion Detection Systems at crucial connectivity places.

2.5 Connecting Two Networks

LANs at every branch/zonal office etc of a bank can be connected together to make a WAN–Enterprise Private Network. For example, a bank with LANs in each of its locations might choose to connect all these LANs together to make its own Private Network. Once this is done, employees at the different locations would be able to share information across the network. But to do business with other banks or other enterprise customers, the Private Network needs to be connected to INFINET and/or Internet.

2.5.1 Group Hosts/Computers Based on the Services/Access

- Servers that participate in Interbank applications should be accessed from the INFINET
- Servers that participate in the bank's business only, like ATM should be accessed from both the Private Network and INFINET. This is essential as Private Network points may not be available at some locations.
- It should be decided which servers should be accessed from the Internet, INFINET and Private Network
- It should be decided whether a branch has to access Internet, INFINET, or Private Network
- It should be decided which servers (ex: Groupware and office automation) should be on the LAN, but also be visible on the INFINET and the Private Network for

occasional data transfer. These servers are placed on LAN as they generate more traffic for LAN than for other networks.

Based on these groups, specific IP address/es should be allotted to each server. If a server has to be accessed from more than one network, it should be assigned IP addresses belonging to each of that network IP schemes.

2.5.2 Network-to-Network Access

In this simple scenario, a LAN computer is allowed to access the bank's Private Network and the security risk associated here is low.

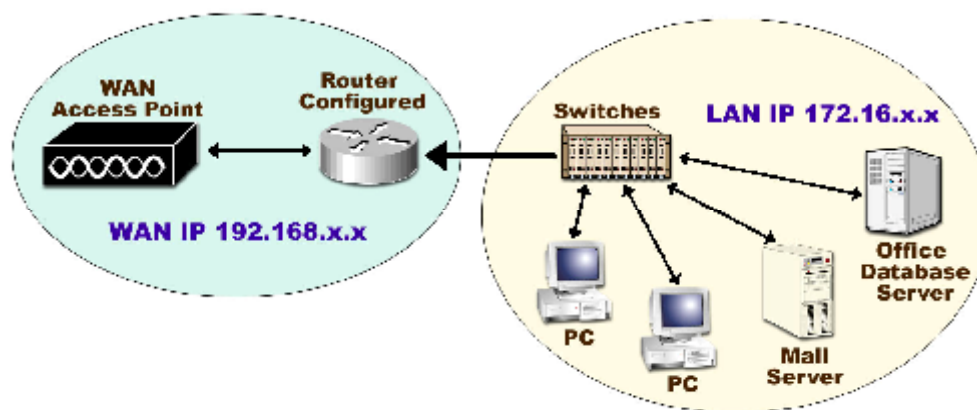


Fig 5: A ROUTER CONNECTING LAN & WAN

- Even a normal server with basic Operating Systems like Windows, Unix or Linux, with 2 NIC cards can act as a router for relatively small offices.
- These servers are capable of allowing/blocking specific traffic based on Source and Destination IPs, ports and a combination of both. Ports are logical numbers against which application services listen to service the requests.
- In all the computers of the LAN that access the Private Network, the default gateway has to be specified as the router.
- The router should be configured in such a way that the underlying network topology of the LAN is not visible to the Private Network.

2.5.3 Publishing an Application Server to Other Network

The above configuration allows only the computers on the LAN to access the WAN. It doesn't allow any one from the WAN to come inside the LAN and access a server. Publishing a server to a network means allowing access from that network to the server. An example is Mail server.

Not only does the mail server send mails outside, but other offices too need to send mails to this mail server and for that, the mail server has to be assigned a WAN IP.

This can be done in the router by configuring the NAT (Network Address Translation). The NAT translates a WAN IP into LAN IP and vice versa. If the mail server's LAN address is 172.16.0.20 which is mapped to WAN IP, i.e. 192.168.0.20 in the router, any packet from WAN with destination IP address as 192.168.0.20 would be received by this router. The router then rewrites the destination IP as 172.16.0.20 and sends it to the mail server. Similarly, packets from mail server to WAN travel with source the IP as 192.168.0.20, instead of 172.16.0.20.

NAT has become a very primitive security and privacy mechanism, hiding the network infrastructure of Private Networks.

Depending on the level of security required and the importance of the server that is being exposed to other network/s, a firewall can be deployed. **It is always advisable to set up a firewall whenever a server is being exposed.**

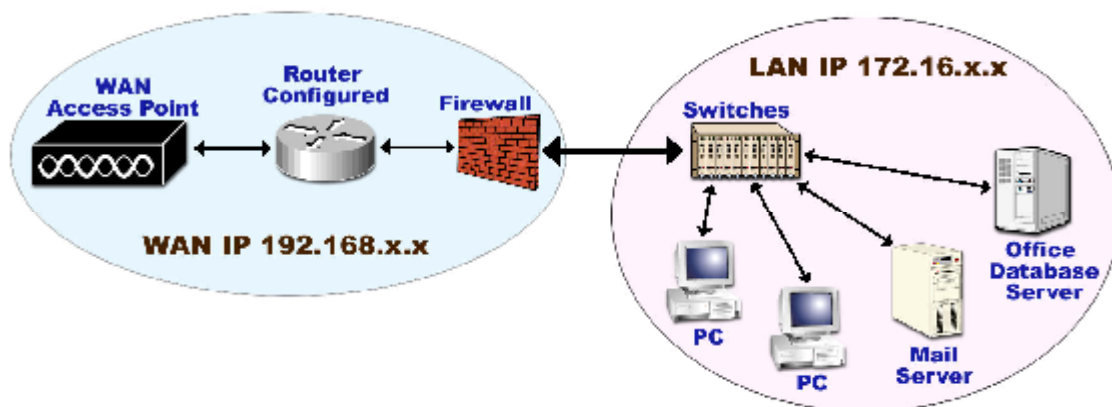


Fig 6: A FIREWALL CONNECTING LAN & WAN

2.5.4 Communication between INFINET and Private Network

In this section, we describe the various possible ways of communication between INFINET and a Private Network.

2.5.4.1 Mail Application

It would be better if the bank computers communicate as per the application requirement. Every branch hardly requires access to every other branch. Though every user has to send and receive mails, it's not essential that every computer be connected to every network. If the servers are connected and they can communicate, and local users communicate to the local server, it is good enough. Here is an example of how Mail servers at different locations on different networks communicate.

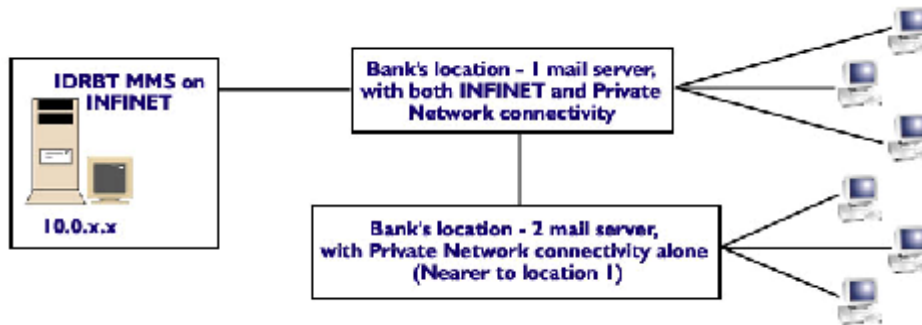


Fig 7: CONNECTING MAIL SERVERS

In the above example,

Incoming Mails

- IDRBT MMS sends inward mails for both the locations of the bank to Location -1
- The Location-1 mail server in turn sends the mails for Location-2, to the location-2 mail sever.

Outgoing Mails

- The Location-2 mail server forwards outgoing mails to Location-1
- Location-1 mail server forwards them to IDRBT.

In a way, the servers that have both INFINET and Private Network connections act as relay servers for locations that are connected to Private Network but not connected to INFINET. Connectivity design varies from Application to Application as per specific requirements.

2.5.4.2 ATM Connectivity

Let the centralized ATM switch be accessed both from the INFINET and Private Network and branches with INFINET connection be allowed to communicate over INFINET. Branches with Private Network connection can be allowed to communicate over Private Network. Here is how the conceptual diagram would be:

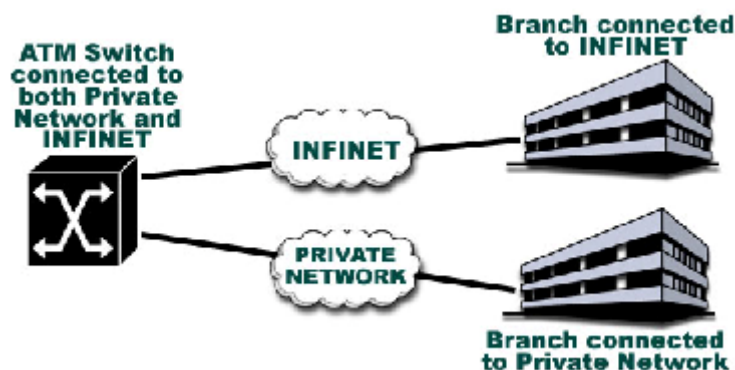


Fig 8: ATM CONNECTIVITY

2.5.4.3 Publishing a Private Network Server on to INFINET

In this scenario, the application server is in a location, which is connected to Private Network, but not to INFINET but the requirement is to access this server from both the networks.

We suggest that this scenario be avoided as it is more complicated and may not be required at all. However, if the situation doesn't leave any other option, one can implement it as shown below. Here Location-1 is connected to the Private Network through Router A; and Location-2 is connected to both INFINET and Private Network through Router B.

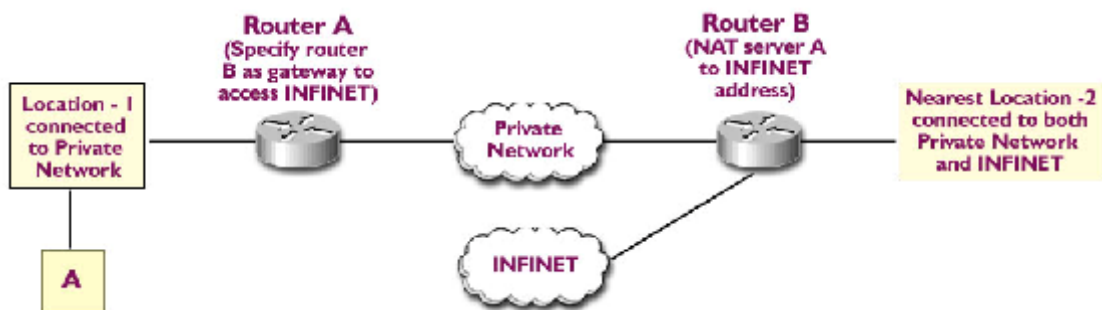


Fig 9: PUBLISH PRIVATE NETWORK SERVER ON TO INFINET

Make sure that the router doesn't send the route information of INFINET to Private Network and vice versa. This is highly important.

2.5.4.4 Publish INFINET Server on to Private Network

Even this scenario should be avoided and if essential, the earlier concept can be used as illustrated below.

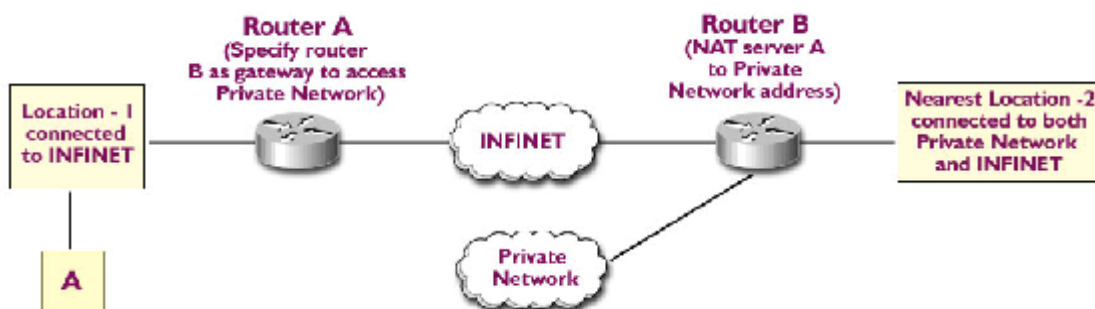


Fig 10: PUBLISH INFINET SERVER ON TO PRIVATE NETWORK

2.5.4.5 Publish Critical Business Services on to both INFINET and Private Network

Instead of complicating the issues both in terms of connectivity and manageability, as explained earlier, identify the servers and services that have to be accessed by almost everybody. Place these servers at a secure location (data center) and apply strict security policies at all levels like physical, application access, system access, router, firewall and end users.

2.5.4.6 Load Balancing the Network Connections

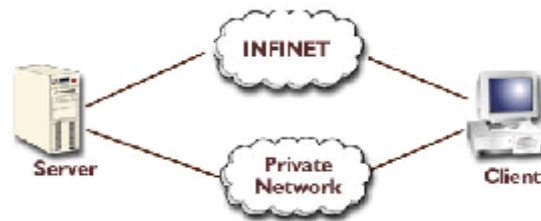


Fig 11: NETWORK LOAD BALANCING

The two connections in the above conceptual diagram can be treated as two different service access points and one can use any of the following methods.

- Clearly demarcate the services application wise, either to be accessed through Private Network or INFINET.
- Allow servers to be accessed from both INFINET and Private Network.

In this case, the server could be accessed from both the networks. If a remote location has both the connections, it can use both to access these servers, by using simple methods from DNS Round Robin Load Balancing and Network Load Balancing offered by specific operating systems like Windows, Sun Solaris etc; to complex Load Balancing offered by high end network specific products like Linkproof, Stonesoft etc. All these techniques, basically allow both the connections to be utilised, but differ in their intelligence quotient. Selection of the solution should depend on how really these features are required.

3.0 Security – the Major Concern of the Networked World

Internetwork, along with its benefits like fast communication across an organization, business partners etc, also brings in lot of risks. The more the number of networks connected, the more the complications.

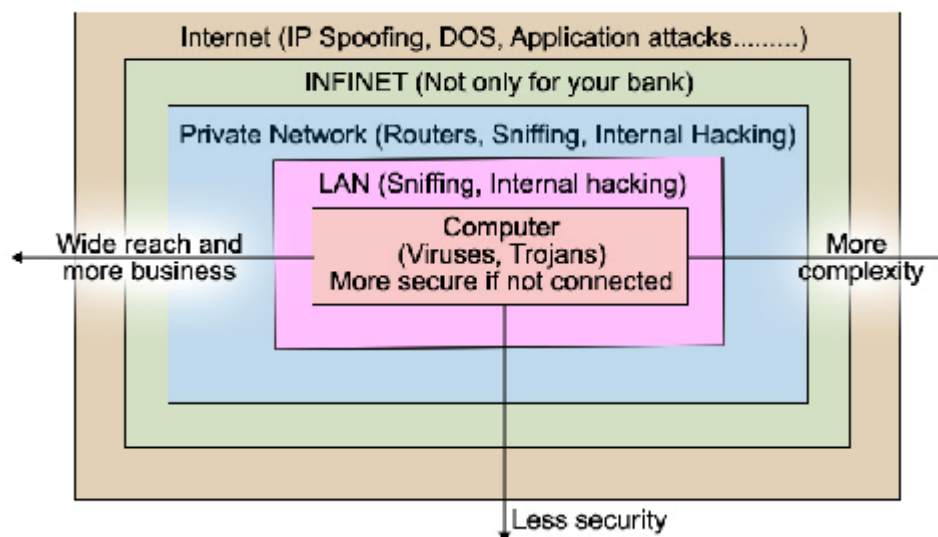


Fig 12: SECURITY LEVELS

If we keenly observe the complete process of users communicating over a network, we come across these crucial components.

- Users and their desktop (Note: Any entity, which is being serviced as a User can be considered. It can be yet another service/application.)
- The communication devices and their protocols
- The applications or rather the services

All these components are developed keeping only a specific goal in mind and without looking at the whole scenario of providing an end-to-end solution – i.e. offering a secure, authentic, non-tampered and uninterrupted service to the users. For ex. the client software is designed and developed keeping the (G)UI in mind and security becomes secondary. The Communication Protocols are more worried about “how to deliver the data to the destination”, than privacy, confidentiality, integrity and security of the data.

The applications are built to suit the business logic, performance of system etc in mind. Many application developers are not even aware of the basic Operating System on which their application runs, and the communication protocols that carry their business data to the end user.

These three loosely integrated components, along with buggy software are the major sources of today’s computer threats. In this very complicated scenario, the major issues that need to be looked at include:

- Protecting the Desktops and Servers
- Protecting the Network, be it Private Network, INFINET or Internet or any other network
- Ensuring that one’s network/systems do not become a launch pad to attack other connected networks.

These three rules should be applied at every system, network (LAN, MAN, WAN, INFINET, Internet) level appropriately.

3.1 Threats

Threat	Cause	Solution
Loss of data integrity	Trojan on Server, client, Sniffing and changing the data on transmission	1. Harden the Server 2. Virus Scanner on both Server and Client 3. Use Digital certificates to encrypt and sign the data
Loss of confidentiality		
Repudiation		
Unauthorized access	Trojans, Password Cracking, Negligence; Poor network and computer access policy	1. Harden the Server 2. Virus scanner 3. Password Policy 4. Use Smart cards 5. Deploy firewalls, IDS 6. System Integrity Checkers
Fake Servers and Services	DNS Spoofing and IP Spoofing	1. Use SSL 2. Use DNS Sec 3. Use IP Sec 4. Router ACL policy
Server unreachable	DOS	1. Harden the Server 2. Virus Scanner on both Server and Client 3. Router ACL policy 4. Firewalls
Service unavailable	Trojans	
Network unreachable	DDOS	
Internal Abuse	Lack of planning, Vigilance and Coordination	Audit and Security Policy; Physical Access Controls

3.2 Need for Security

The threats/risks listed above are not very exhaustive and new threats keep cropping up every now and then. Security in a networked environment is a process that can ensure confidentiality, and integrity of information; availability of services; protection of information assets from unauthorized access; and protection of users from being misled.

We discuss here a “defense-in-depth” security approach, i.e. implementing multiple layers of security to mitigate the risk.

3.3 Desktop Security

Often, desktops are the most neglected lot when it comes to security, for the entire security team concentrates on servers, firewalls etc. But these very small computers can become a gateway for serious attacks. Email and malicious code on web pages are currently the top

distribution mechanism for the world's most dangerous electronic viruses and Trojans, which do not even require human intervention to be activated. The system can be made foolproof by:

- Educating users on usage of computers; the virus threats; importance of information; protection of information by passwords, smart cards, digital certificates etc
- Defining and implementing computer security and usage policies.
- Deploying virus scanners, personal firewalls etc.
- Using various security software and updating them regularly
- Applying security patches of operating system, and application software at regular intervals
- Any Enterprise Network Management Solution like SMS, TNG-Unicentre can be used to install and update software for a wide network of desktops.

3.4 Server Security

Servers are special computers that offer services to users, and more importantly, to the users of the outside world. Many a times, it is this specific service through which attackers sneak into the network, though there are other vulnerabilities like default configurations, unnecessary software etc. Such attacks can be avoided by:

- ◆ Placing critical servers on a separate network segment
- ◆ Building a server profile and procedures for documenting installation, troubleshooting and maintenance.
- ◆ Performing server hardening by following the vendor specific security checklists
- ◆ Understanding the system completely by meeting and questioning the administrators about the system's health, and any changes that took place etc
- ◆ Allowing very limited access that is required to complete day-to-day operations to administrators
- ◆ Removing unnecessary software or disabling the unnecessary default services
- ◆ Enabling computer, file, directory and service access control and auditing
- ◆ Configuring the system to write logs on to a remote computer too.
- ◆ Monitoring the logs and taking immediate actions if any alerts are found
- ◆ Installing and configuring integrity checkers like Tripwire, which can alert the administrator
- ◆ Scanning the servers for well-known vulnerabilities by using security scanners like Nessus, ISS etc
- ◆ Never allowing opening of any mails or browsing activities etc. on servers
- ◆ Never allowing remote server administration from public networks. Even if remote administration is allowed from internal network, the communication must be fully encrypted
- ◆ Conducting regular system audits and penetration tests

3.5 Application Security

While the operating system's software is general-purpose software, application software is that which reflects the business logic and is specific to that particular business segment. Most of these applications software is based on the code that was never intended to be of production quality. They were "proof-of-concept" programmes that later became the basis of the production system. In order to successfully implement application security:

- Follow good software engineering methods while developing the application
- Use code testers
- Check that at no point of time, source code and database queries etc are revealed to the user by the application. Not just data validation, data boundaries too should be checked as this leads to buffer-over-flow attack, i.e. it allows a remote user to give commands as part of data.
- Purchase commercial applications from reputed vendors with on-going service and maintenance contracts
- Apply vendor specific patches at regular intervals
- The communication from the application to the user must always be encrypted and signed.

3.6 Database Security

Database servers are foundations of every e-business solution, for they hold critical information that should be protected at all costs. This can be ensured by:

- The use of complex authentication and encryption methods to protect the data
- Keeping these servers on a separate network segment, with a firewall or proxy watch guarding them.
- Putting in place an excellent backup and disaster recovery, at least for the database. This is essential even for small-scale e-businesses.

3.7 Network Security

The underlying TCP/IP communication protocol that is the basis for computer networks has no security, privacy and integrity built into it. The old TCP/IP and its associated application protocols are now being strengthened by new protocols like IPSec at the network layer, SSL at the session level and 'Digital Certificates to users' at the application level. All these mechanisms should be used whenever possible.

Since, it is not possible to use all these mechanisms at all locations due to various reasons like incompatibility between products, versions and implementations; solutions like Firewall and IDS, which provide over all security at the network perimeter, closing the security holes of desktops, servers etc by restricting access into the network need to be accorded priority.

A firewall acts as a super cop inspecting the traffic between networks. A Firewall should support the features like:

- Packet Filtering
- Secure NAT
- Application Filtering
- Content Scanning
- Virus Scanning
- Circuit Gateway
- Authentication Module
- Intrusion Detection System
- Browser Security options like downloading Cookies, ActiveX, Java Applets must be specified at the firewall level and should optionally overwrite individual browser settings

The policy of the firewall should be – ‘allow specified packet types and block any other type if unspecified’, instead of the policy – ‘block if specified and allow any unspecified’.

The three kinds of Firewalls available are Packet Filtering, Circuit Gateways and Application Proxies

- ◆ **Hardware Firewalls:** This device can be connected between public (Internet) and Private (LAN) Networks. By default, the architecture of this router device should be “don’t allow inbound connections”. The notion of public and private is relative.

Advantages of this firewall:

- Any third party s/w- cannot be installed. It is a normal tendency of administrators to install and experiment with new requirements, without looking into side affects.
 - The access/connection control could be specified clearly in black and white terms like all inbound connections are bad, so don’t allow and outbound connections are good, so allow.
 - Many hardware firewalls now allow specifying not only complex access /connection rules but also application level and user level settings.
- ◆ **Software Firewalls:** These are basically application level gateways/proxies and their major advantage is that by default they mask the LAN IP addressing scheme. These firewalls require lot of capacity planning, but allow access control, scheduling network access etc at a finer granule level. Firewalls of this nature are now available with one extra feature as web caching.

3.8 Back Up and Disaster Recovery

Computers, hard disks, hubs, switches, communication links etc do fail, and therefore a detailed local back up and replacement mechanism should be readily available. For every component that participates in the e-business, a detailed plan on how to replace it in case of failure should be in place. Moreover, hard disk mirrors, tape backups, optical storage, mirror backup servers, extra switches, hubs etc at the local level can be maintained independently.

Hardware and software can be replaced, but data has to be intact. In order to achieve this, one can look at hot sites, wherein data gets replicated to a remote server in real time. Though this is a good feature, it doesn't protect the data from corruption if the data gets corrupted at the original site. So, options for manual periodical data back ups on tape or optical storage too must be open.

Though highly unlikely, few enterprises may experience disasters like hurricanes, bombings, floods or earthquakes that can cripple them for long periods. In such a scenario, bundles of documentation will not be of any help. In such cases, what is required is a concise higher-level plan, and experienced specialists who know all about the system. Excellent rapport and co-operation among all concerned and at all levels is essential to overcome such situations.

Detailed recovery plans and various alternatives should be readily available to conquer disasters. The following options can come in handy in such a scenario

- ◆ Hot sites or computer-ready locations
- ◆ Work sites -- places that will accommodate communication lines, PCs and cubicles
- ◆ Cold sites -- empty facilities where you can house the equipment
- ◆ Reciprocal relationships to exchange space with other firms

4.0 Enterprise Networks in Complex world

The enterprise networks will soon merge with other business partner networks and then with the global open network, the Internet. This is essential for facilitating:

- Internet browsing for research and development activities.
- Sending and receiving e-mail to and from Internet. This can be achieved without Internet connection too, by switching all mails at IDRBT.
- Internet Banking – Various locations may have to be connected to Internet to allow on-line business transactions with customers.

The following section discusses how to connect an enterprise network to Internet for various purposes.

4.1 Connecting Bank's Own Enterprise to the Internet

4.1.1 Requirements/Assumptions

- The Internet access is strictly restricted to access the content on Internet.
- No services including E-mail, FTP etc. would be hosted on or made available to Internet
- Reduce load on firewall and improve performance to reduce the Internet traffic. A web-caching server can be deployed for this purpose.

4.1.2 Configuration for Office Environment with above 200 users

- ◆ ISDN/Leased-line suits such an environment.
- ◆ With the leased-line connection, your LAN is always connected to Internet with the same IP as against dial-up connection and dynamic IP
- ◆ This continuous connection to Internet itself can pose a major problem
- ◆ However, it provides for centralized overall control, making management simple and efficient
- ◆ Keeping a firewall is a must

4.1.3 The Proposed Architecture

In order to exploit both the hardware and software firewalls, architecture of the following kind can be planned.

Caching Web server: Many people accessing the same popular website is very common in any organization. Though browsers have caching features, they cache pages only locally and serve only on that computer. Each browser fetches and caches the pages independently. The same pages may be fetched dozens or hundreds of times every day. These redundant accesses may impose a significant load on the firewall system.

In order to reduce the load on the firewall and improve performance, large organizations can go in for a caching web server, the best place for which would be on the private LAN and behind the firewall.

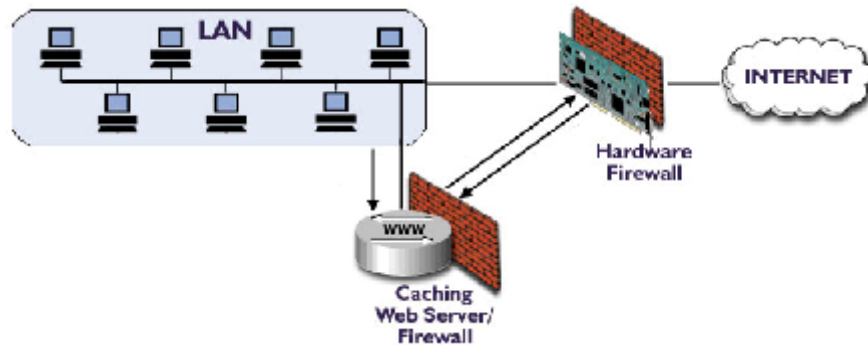


Fig 13: INTERNET CONNECTION TO ENTERPRISE NETWORK

In this configuration, all clients are configured to browse Internet through the Caching Web Server, by specifying its IP in proxy settings of the web browser. Specifying Hardware Firewall as gateway configures the caching web server to access Internet content.

1. The Hardware Firewall is dual-homed and this is the simplest configuration to set up application level Firewall. Other configurations like Screened Host, Screened Net or Demilitarized Zone Configuration can provide extra layer of security at the cost of complexity and ambiguity. If the purpose is just to access Internet without hosting any service, this simple configuration (if configured well) will suffice the requirement.
2. Since it is dual-homed, care must be taken not to route ICMP packets from Internet to LAN and vice-versa.
3. The hardware firewall can be configured for broader access policy like:
 - Which applications from Internet can be accessed – like HTTP, FTP, CHAT, TELNET etc
 - Blocking ports – Since the purpose is just accessing Internet, instead of allowing outside world to access the services hosted, all ports should be blocked.
 - All inbound connections should be blocked
 - Java Applets/ActiveX components should be blocked
4. Once configured, the h/w firewall need not be reconfigured. The modifiable security policies should be enforced through Web Caching/Software Firewall
5. The configuration of h/w firewall should be in such a way that even if a mistake happens while enforcing some policy/requirement, the h/w firewall can take care of it at a higher level as the broader security policy.
6. At the s/w firewall/web caching server, controls like the following can be enforced

- Which sites to be accessed
- Which sites to be blocked
- Who can access at what time
- Grouping of users
- Chat being very insecure/unproductive application, restrictions on who can access this service at what time
- Controlling bandwidth to certain sites
- Giving preference to certain sites
- Scheduling content download of specific sites
- Blocking certain users to access Internet
- Blocking certain IPs/computers to access Internet
- Analyzing traffic reports
- Caching and monitoring the traffic flowing from LAN to Internet etc

Minute level access controls can be imposed at this level. However, these policies should not violate the broader access policy of h/w firewall.

7. The configuration, monitoring, auditing, and managing the systems should be done by specialists with in-depth knowledge of firewalls. It would be better if separate persons manage these two firewalls. If the same person manages both, the same mistake can be committed on both. The person manning h/w firewall should always think twice before going in for some configuration change forced by the changes at s/w firewall.
8. Never install any extra s/w on these two firewalls.

4.1.4 Generic and essential Security Controls

- Block ICMP protocol
- Enforce ingress and egress filtering on routers (External/perimeter)
- Install anti-virus software on servers and desktops and update them at regular intervals
- Regularly update servers and desktops by latest patches and service packs, by using vendor specific tools like MS-Hfnet check for Windows
- Monitor server logs
- If possible, install system integrity checkers like Tripwire

5.0 Internet Banking - Opening Services to Customers & Business Partners

Internet has become the de-facto service channel. Today, almost every consumer service, be it bill payment, purchasing ticket or transferring money, is being offered over the Internet. Though there are still many restrictions on Internet Banking, banks will soon have to offer most of the services over the Internet due to the huge demand, wide-reach, new clientele and new business opportunities. The block diagram below illustrates a possible architecture for Internet Banking.

5.1 Architecture Description

The architecture is based on functional dependency and controlling issues. It is divided into:

- Database Module – Responsible for database management
- Control Module – Responsible for day-to-day management of servers, firewalls, network etc
- Preparation Module – Since there are many delivery channels like Internet, ATM, ABB etc, this module is responsible for creating the data required in the format requested by these delivery channels
- Delivery Module – This group delivers the service. Whenever it gets a request from any source, it sends the request to the preparation module, gets the response and sends it to the originator.

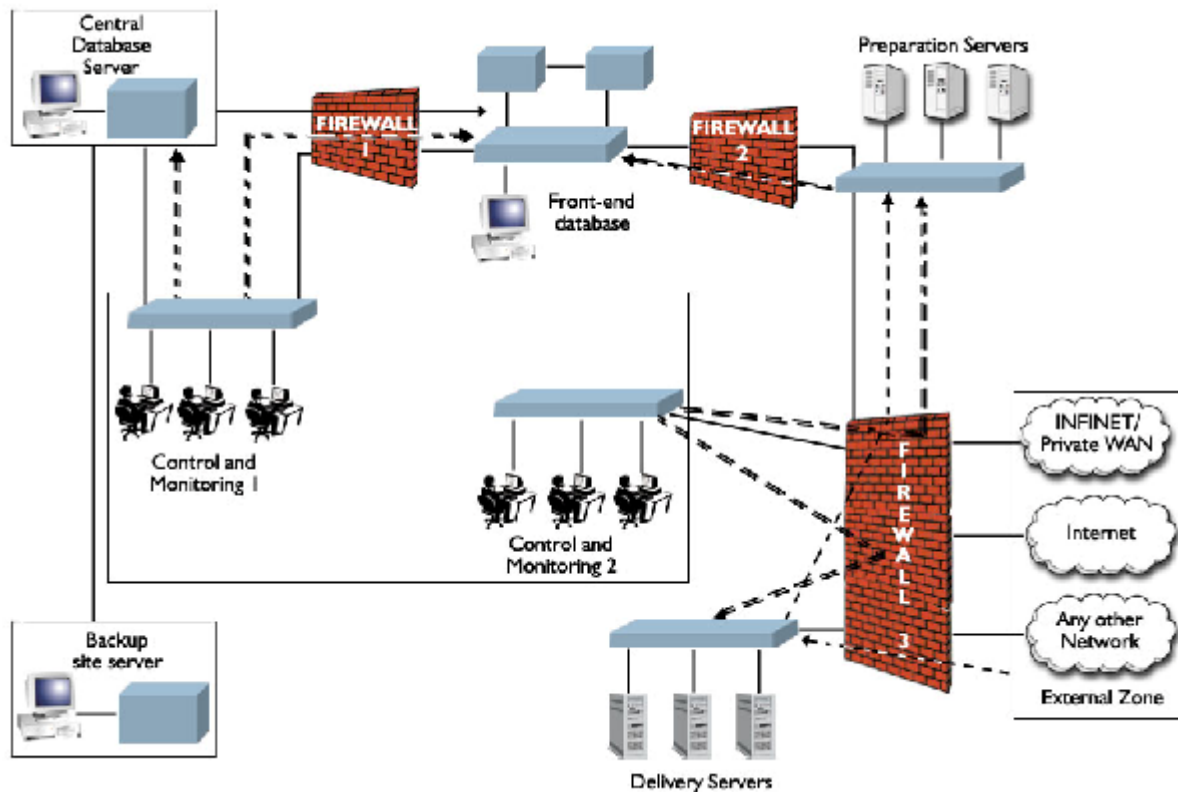


Fig 14: INTERNET BANKING ARCHITECTURE

5.2 Database Module

In any business process, it is the data that has to be protected at any cost. Therefore, data should be accorded utmost priority and it should be protected from inadvertent overwrites, loss of integrity and unauthorized access etc. This section focuses on designing a database to protect the data.

The Central Database should not be accessible by any of the components. While the Central database contains the whole data, the front-end database contains only the active portion, i.e. the minimum data required to carry out the business transactions. The Front-end database is active and should contain two types of databases - Master and Transactional.

While the Central Database only updates the master, the transactional database should be append-only, i.e. it cannot be over-written even by the super user. In a way, while one is read-only, the other is write/append-only database. So, for any particular information, the master acts as the base, and after applying all the transactions that took place after the updation of the master by the central database, it provides the current information. Even this current status also can be appended to transaction database.

Since, all transactional information is done with the front-end database, the Central database needs to get updated. This can be done in many ways such as:

1. Doing manual updates at regular intervals – it is always better to take back up before applying the update. Moreover, the updation can be done only after verifying the transactional data manually, if required.
2. Let the Central Database Server keep accessing the Front-end database at regular intervals and update its own database after taking automatic back up of the current state of the database.

Relation of Central database and Front-end database (Master, transactional)

Loop {

1. Central Database updates the master at time t1
2. Business process takes Master as the base, applies all the related transactions that took place after t1 to get current status, does transaction and appends it to transaction database
3. At time t1+schedule, Central Database takes all transactional data from Front-end database, updates it's own and master of Front-end database. Only Central Database can update the master.
4. Sets current time as t1 and proceeds to step1}

As another security and precautionary measure, one can write the Front-end database at regular intervals to a Write-Once medium.

Note: Provide only one access mechanism/data format to preparation servers, though their business logic expects it in different forms. It is the preparation servers' responsibility to convert the data taken from front-end server to suit their needs and return back the transaction data to the front-end database server in front-end database format.

Never allow many database connect plug-ins from different vendors to be installed on to the front-end database server. Try to provide access to data using database-stored procedures, than allowing programmers to write their own queries in their programmes. This is a good database design and programming practice.

5.3 Preparation Module

There could be many application servers in this module. If the application software, catering business to all delivery channels is from the same vendor, it can continue to be same, but if they are from different vendors, one may have to have different application softwares. The actual business process lies in these application servers, and moreover a lot of performance and caching techniques can be applied at this level to deliver faster service.

Preparation servers take requests from the delivery servers, check whether the requests are valid and accordingly process the request by accessing the front-end database server; applying business logic; appending the transaction and then sending back the reply (current status). In order to improve the performance, it can cache the replies in such a way that at any time if the same request comes again, it can immediately serve it without going through the whole process all over again.

No other software, except the base operating system to run the business logic application and the application software itself, is installed on these servers. Not even web service is required on these servers.

5.4 Delivery Module

These are the servers with which users from different delivery channels interact, and these servers simply act as proxies to the users and interact with preparation servers on behalf of the users. These servers should not have much business intelligence because normally these servers interact with users, who use services like the Web.

It is well known that buffer overflow and many other bugs, which can provide remote control to an outsider, are big security threats posed by web servers. To reduce such risks, all data input forms should be tested by providing huge amounts of data and checking out whether the server responds as expected or exhibits any abnormal behavior.

No caching and log information is kept in these servers, and moreover the logs of these servers should be on remote machines and be of append-only nature. This precaution is necessary because web servers reveal lot of information if the user puts in some data that is not expected by the service.

5.5 Control and Monitoring Module

These are the servers, which are responsible for monitoring the whole setup. We propose that there should be at least two groups responsible for different modules. Group 1 should be responsible for database management, since they need to look at database access control mechanisms too and Firewall 1 is totally manned by them. Since Preparation module needs to access front-end database, both the groups with mutual co-operation should manage Firewall 2, thus keeping their servers and zones safe. Group 2 mans Delivery Servers, Preparation Servers and Firewall 3.

Each group should only have the required tools installed on their servers. For ex: Group 2 need not have any database monitoring/troubleshooting tools and Group1 need not have any web service/business service monitoring tools.

5.6 Firewalls

We arrived at three firewalls because of access and control requirements based on criteria like who is managing, who is accessing etc. The firewall features as per this architecture are as follows:

1. Firewall 1 – Allows connection initiation from ‘control & monitoring’ Group 1 only to both the database servers and it does not allow connection initiation in the reverse direction.
2. Firewall 2 – Allows connection initiation from ‘preparation servers’ only to Front-end database servers.
3. Firewall3 – Allows connection initiation from external zone to “delivery servers” and from “Delivery Servers” to “Preparation Servers” only.

Note: No other connection initiation from any server to any other server is accepted as it may potentially lead to a compromise of the server. For ex: Delivery servers need not initiate any connection to External Zone at all. If that happens, it indicates that a Trozan has some how arrived onto these servers and is trying to contact its owner.

5.7 Transaction Process

A request from the external zone first hits the “delivery servers”, and they in turn make connection to the “Preparation Server” and the “Preparation server” replies immediately or gets data from front-end database, applies business logic, and sends the reply back to the “delivery server” and from there to the final user. All these connections across servers are totally independent of each other.

5.8 Essential Security Features

1. Keep security patches on all servers, firewall, routers etc. up-to-date.
2. Do not use vendor supplied default passwords on server, routers, database or applications.
3. Never give the same username and password to more than one person. Have unique accounts for every person who accesses the computer, data etc.
4. Make all configurations, system and binary files and libraries as immutable, i.e. they cannot be changed even by the super user and software updates are not allowed. So, be careful while exercising this option and you may prefer going in for the following option.
5. On all critical servers, use system, data integrity checkers like Tripwire that monitors if any sensitive file has been changed.
6. Use Host Based Intrusion Detection Systems on critical servers
7. Use Network based IDS on “Delivery Systems” network.
8. All remote control and monitoring commands and responses should be encrypted. Use SSH, one-time passwords, and kerberos authentication mechanisms.
9. All server/firewall logs should also be captured on to the remote computer.
10. Never provide administrative access from outside, i.e. External Zone.
11. Encrypt stored data
12. Encrypt data sent across networks
13. Use and regularly update anti-virus software
14. Ensure that only required ports, for ex: Ports for HTTP-80 and SSL-443 are only opened for web server from outside
15. Block ICM protocol
16. Enforce ingress and egress filtering on routers (External/perimeter)
17. Use port scanners at regular intervals to check if inadvertently some ports were open
18. Use security scanners like Nesses, which can detect well-known software vulnerabilities and alert the administrator. After all, even firewalls, routers etc are software driven and have vulnerabilities.
19. Regularly test security systems and processes.
20. Restrict physical entry by access control cards; or use thumbprints.

5.9 Other Administrative Activities

1. List all systems. Describe each machine in terms of it's OS, it's role in operation, business application softwares installed, any other software installed and it's purposes
2. List all patches installed on each machine.

3. List all virus, audit and Intrusion Detection Systems in use.
4. List all users who access the servers, their role and their access level.
5. List all commercial applications in use and describe what each application does.
6. Look at all application programs, and ensure that they do not use any database sql commands in their programs, and insist on their using database-stored procedures. List applications, the databases they access and how they are accessing, whether they are writing back data etc.
7. List all the tools/system/network/database administrators use to monitor the systems.
8. List all the system administrators, their role and the back up administrators
9. List the shutdown, startup, backup and restoration mechanism
10. Provide detailed plan of incident handling and troubleshooting escalation procedures

These activities should be repeated at regular intervals and be compared with previous lists and procedure to ensure that the system is running smoothly and there is no deviation. If any deviation is discovered, proper explanation should be provided.

References:

1. Building a Secure Internet Data Centre Network Infrastructure – Chang Born Tee – Nov 7, 2001 – <http://www.sans.org>
2. E-commerce and Defense in Depth – Clayton T. Dillard – Oct 24, 2001 – <http://www.sans.org/ecommerce/defenseindepth.php>.
3. Counter Hack Ed. Skoudis – 2002 PHI.
4. Protecting Data in today's Enterprise Environment – Marken Communications – <http://www.marken.com/docs/backupmtn08.htm>.
5. In Successful Network Protection, the Key is Recovering – Not the Plan – Marken Communications – <http://www.marken.com/docs/backup/Mtnol.html>.
6. How Safe is my Money Online – George Rapp - May 30, 2001, <http://www.sans.org>.
7. SANS Network Security Roadmap – <http://www.sans.org>.
8. Security in Banks – Cover Story – Dataquest – Oct 15, 2000.
9. Inspection Grade Card for Conducting E-commerce – Andrew Mc Allesten – Aug 27, 2001.
10. Designing Network Security – Merike Kaeo – CISCO Systems; CISCO Press
11. Network and Internet-work Security – Principles and Practices – William Stallings