

Convergence



THE POSSIBILITIES ARE INFINITE

The Information and Communication Technology (ICT) Journal

Volume 2

Issue No. 02

<http://convergence.fpi.com.ph>

Second Quarter 2003

Practical Technology Solutions from
Fujitsu Philippines, Inc.



2Q- 03

CONTENTS

- Using Linux to set up a low cost Internet infrastructure.....page 2**
By Arnaldo Trinidad, WeSolv Open Computing, Inc.
In difficult times, expansions or investments in new technology projects that require big budgets are hard to justify. Emphasis on cost effectiveness is one of the priorities of top management that makes Open Source technology appropriate in this area. This article will give you an idea on how to apply Open Source solutions as a low cost alternative to setting up an Internet Infrastructure.
- Best practices in deploying Open Source software.....page 5**
By Manolito David, WeSolv Open Computing, Inc.
Adopting Open Source Software into the enterprise requires careful consideration. As with any technology adoption that an organization takes, proper policies and procedures must be established to maintain control and fluidity. Gartner Group suggests that establishing a best practices process is essential in ensuring the protection of the enterprise's technology systems when incorporating Open Source Software as part of a diversified environment.
- Setting up a secure network – A case study.....page 7**
By Mark Anthony Jastia, WeSolv Open Computing, Inc.
Having a proxy server only to separate the internal network from the public network can create intrusions to a company's corporate network. Such intrusions can compromise information that can be used against the company or that can be sold to competitors. To address the security requirement of the company, a secure network infrastructure using firewall, Intrusion Detection System, vulnerability assessment, and anti-virus software, is ideal.
- How to avoid serious data loss.....page 11**
By Joseph Sta. Brigida, Fujitsu Philippines, Inc.
Today, organizations are getting ready for the inevitable "disaster". It can happen to any organization, perhaps due to fire, flood or human error. This article will help you plan and prepare your organization for any threats such as calamities and other events by using precautionary measures and tools, from simple backup utility software to the most complex data protection software available in the market.
- Going back to the basics of TCP/IP – Part 2.....page 13**
By Conrado Catindig, WeSolv Open Computing, Inc.
In part one, the definition of TCP/IP and what it does, including protocols used, were discussed. Part two details how TCP/IP designers devised ways and options to address limitations of IP addresses. It also defines the routing function of routers, which serves as the LANs gateway to the outside world, and their routing protocols. The Ethernet protocol, which most networks use today, and its use are also discussed. Finally, there are several computer services that can be provided by TCP/IP but not part of its protocol suite.
- From the Publisher: "Article to be submitted by FRM"page 15**

Using Linux to set up a low cost Internet infrastructure

By Arnaldo Trinidad

The Internet market is growing incredibly fast and companies of all sizes need their own Internet infrastructure to gain a competitive edge in increasing their employees' productivity and in meeting their clients' demands.

Companies advertise their products and services on the Internet to reach as many potential customers as possible. Employees need to connect on the network to collaborate with co-employees, to browse the Internet for research work and global access, to send and receive email for quick business transactions, and to share files and printers to increase office productivity. One way of satisfying all these needs is to set up their own Internet infrastructure.

Investing on infrastructure, however, is a major issue for companies that have tight budgets during hard times. Putting up their own Internet infrastructure would mean additional investment on hardware, software, and skills. Moreover, companies also experience difficulties in expanding their existing infrastructure due to the high cost of acquiring additional licensed software.

With a multi-user environment, Linux is an excellent platform for development and an outstanding low-cost alternative for expensive operating systems.

This article will address the companies' needs with cost-effective solutions without sacrificing flexibility and reliability using open source applications on Linux environment. These needs include web serving to reach more customers by publishing services and products on the Internet, proxy services to provide Internet browsing to employees for global access, file and printer sharing, firewall to protect from internal and external unauthorized access, DNS to be used by the web and email service in resolving names to an IP address, and DHCP to provide IP configurations to client computers with ease.

Low Cost Solution

A low cost Internet infrastructure solution may be composed of open source applications running on a Linux environment. Linux is an operating system that is similar but not identical to UNIX. It runs on a multi-user environment and is an excellent platform for development. Linux-based information systems are also known to offer better security, reliability, and flexibility.

Linux can be downloaded from the Internet and can be used by anyone for free. In addition, it offers significant cost savings in software license fees. These factors make Linux an outstanding low cost alternative to expensive operating systems.

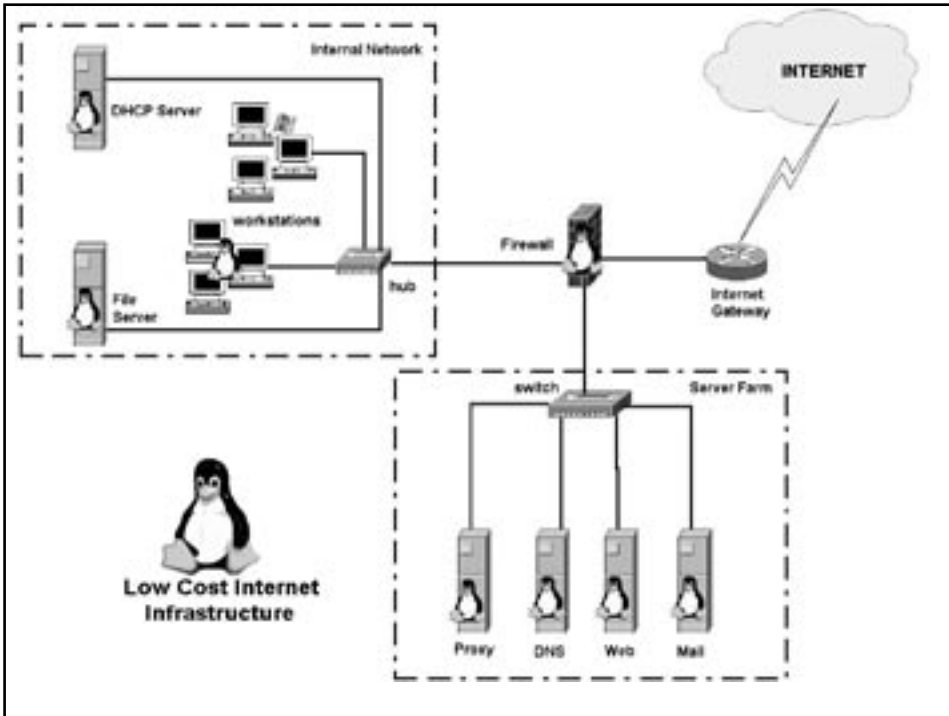
Internet Services

Basic Internet services may include email, web serving, web proxy, file and printer serving, firewall, DNS and DHCP to name a few. These services or applications are included with the Linux distribution or are freely downloadable. It means companies don't need to buy additional software to deliver the basic services mentioned.

Function of the servers and services

Proxy Server

A proxy server acts as a gateway for users to access the Internet simultaneously and has caching capabilities to increase access speed and reduce network traffic. A Linux based Web Proxy Caching supports most popular web protocols such as HTTP, FTP, gopher etc. One example of an open source proxy server is the Squid Proxy Server. Squid is a high-



PCs running Windows operating systems are widely used as client machines. Thus, sharing of files and printers between Linux and Windows machines is very important. Be sure to address these issues when implementing a Linux environment.

performance proxy-caching server for web clients, supporting FTP, gopher, and HTTP data objects. Squid operates on most modern UNIX operating systems including Linux.

File and printer server

A file server is a system dedicated to store files while a printer server is a system that manages one or more printers.

Windows operating systems are widely used as client machines and implementing a Linux-based solution would surely need to interact with the existing Window-base machines. Thus, sharing of files and printers between Linux and Windows machines are very important. A Linux-based file and print sharing system provides Windows-based workstations access to Linux-based servers and workstations via the standard Network Neighborhood.

A low cost file and print server on Linux by using an Open Source application called Samba can be implemented. Samba is a file and print server for Windows-based clients using TCP/IP as the underlying transport protocol. It can also support SMB/CIFS-enabled clients.

Web Server

Web servers are systems where the web site resides and provides HTTP service.

One of the most popular Open Source web servers is the Apache web server. Apache is fully compatible with Linux environment and is considered as one of the fastest, most efficient, and most functional web server available in the market today.

DNS Server

DNS stands for Domain Name System. It is a distributed Internet directory service used mostly to translate between domain names and IP addresses, and to control Internet email delivery. Internet services rely on DNS. And if the DNS fails, web sites cannot be located and email delivery will not be functional.

The open source model gives the client freedom to choose from different suppliers without a proprietary tie-in. This helps drive support costs down to a reasonable level and become market-driven.

Some Linux distributions include BIND package that is used on a vast majority of name serving machines on the Internet. BIND is also freely downloadable if it is not included in the Linux distribution or if you wish to have a copy of the latest release.

DHCP Server

DHCP stands for “Dynamic Host Configuration Protocol”. DHCP reduces the work to administer large IP network by distributing configurations such as IP address to individual computers who request for information. The overall purpose of DHCP is to reduce the work necessary to administer a large IP network.

Some Linux distributions include the DHCP package that can turn your Linux machine into a DHCP server in an instant without additional cost. If the DHCP package is not included in your Linux distribution, it is freely downloadable on the Internet.

Email Server

Email servers handle the delivery of mails. The Mail Transport Agent (MTA) is the program responsible for delivering email messages. It stores the messages and analyses the recipients and either delivers it or forwards it to another MTA upon receiving the message from the Mail User Agent (MUA) known as the mail client.


There is a number of Open Source mail server software that companies can use on the Linux environment such as Sendmail, Postfix, etc. Sendmail, normally included in most Linux distributions, is loaded with more than enough features for putting up a simple Linux mail server. With Open Source, the possibilities are infinite. Nothing stops a company from integrating Open Source applications like database, directory server, calendaring and web mail can be integrated to improve the performance, usability, and accessibility of the mail server.

Firewall Server

Firewall provides advanced perimeter defense against Internet and Intranet crackers. It is designed to prevent unauthorized access to or from a private network. All messages entering or leaving the Intranet pass through the firewall that examines each message and blocks those that do not meet the specified security rules.

To turn your Linux machines into an instant firewall server, one needs to use IPCHAINS or IPTABLES services, which are freely downloadable on the Internet or come with the Linux distribution. Don't forget to implement the right set of rules. Without the right set of rules, the firewall server will not be effective.

Overall, Linux is worth considering for most types of Internet infrastructure deployments given its low cost and flexible licensing requirements, high level of security, and general stability and usability that makes it a successful business solution.

For more information, go to squid proxy (<http://www.squiq-cache.org>); samba (<http://www.samba.org>); sendmail (<http://www.sendmail.org>); postfix (<http://postfix.org>); DNS (<http://www.isc.org>); and, Apache Web Server (<http://www.apache.org>). 



About the author:

Arnaldo T. Trinidad is a Senior Technology Service Engineer at WeSolv Open Computing Inc., the networking and communication subsidiary of Fujitsu Philippines, assigned to the Enterprise Systems Management Group (ESMG). He is one of the pioneer members of the Linux Core Team (LCT) of FPI. He also provides technical support and does systems administration for various operating systems such as Windows, Solaris, and Linux.

Best practices in deploying Open Source software

By Manolito David

Organizations looking to incorporate Open Source Software (OSS) into their businesses have to craft a carefully considered OSS best practices policy. This is a guideline on what, when, where, why, and how OSS can be integrated into an organization's infrastructure.

According to Gartner Group, not having a proper OSS policy in place may lead to future problems in the enterprise. By 2005, it's possible that 70 percent of large organizations may fail to implement an adequate OSS policy. Without such, 90 percent of these organizations will deploy poorly documented, "unauthorized" systems running OSS or combinations of OSS and commercial code.

Adopting OSS into the organization means that new processes must be created to support it. These processes should be designed to quantify and qualify OSS packages into fields of use. These fields may be the different business units of the organization or its markets of engagement. This will enable the organization to put systems in perspective by creating a streamlined implementation approach that may assist in the deployment and maintenance of OSS in the enterprise.

Screening process

When selecting an OSS package, it is important to have an adequate screening process in place for this. Setting up a pilot team or test lab is ideal in qualifying OSS packages before deployment. The team must run through all feasible scenarios for use, interoperability, modification, and upgrade.

It is advised that software be categorized into different application areas. These categories may be servers (production and test environments), development platforms, administration tools, security, and productivity software among others. These software groups will help in identifying functional characteristics that the OSS package must address.

In the case of office productivity, the suite must be able to inter-operate with other file formats (file types), and provide features that the business unit requires. One business unit may be a heavy user in word processing, and another unit for spreadsheets. In this sense, it may be possible to define different software of the same category to different business groups based on required functionality. It is also advised to research the nature of the authors that created the OSS package being tested. It may be helpful to know their long-term plans and support practices.

A multitude of OSS packages usually come bundled with the OS distribution. This will at least alleviate the process of selection. Another good thing about this is that bundled OSS packages are usually pre-tested on the OS distribution, which offers a guarantee that it works. Moreover, the OS distribution may offer support for these packages.

Modifying OSS

According to Gartner Group, do not employ a Blanket Policy (outright rejection or acceptance) as this may carry risks in itself in the form of missed opportunities or costs and loss at the end.

When selecting an OSS package, it is important to have an adequate screening process in place. It is advised that software be categorized into different application areas.

We invite interested ICT practitioners to share their experiences in the field by contributing stories to Convergence.

The author/s should submit the following requirements:

1. The article with a maximum of 1,200 words; longer works may be accepted for publication in two parts
2. A 70-word summary of the article
3. A 60-word biography of the author
4. A 2 x 2 photograph of the author
5. At least two original illustrations (soft copy: letter size at least 200 dpi, JPEG or TIFF file format) with captions

Send all correspondences to:

The Editor
Convergence ICT Journal
Marketing Administration Division

FUJITSU PHILIPPINES, INC.
2/F United Life Building,
837 A. Arnaiz Ave. Legaspi Village,
Makati City
Tel: 812-4001; 894-8529
Fax: 817-7576
Email: b.jose@fpi.fujitsu.com

Organizations that find it necessary to modify OSS packages to suit specific or targeted business needs should consider the following: will the modification/enhancement affect the support agreement of the package (if any); will the package be incorporating a similar feature in the future as part of the package author's directions/plans; will the changes pose as a hindrance to future upgrades of the package; and will the changes still be applicable?


It's also important to consider that most OSS packages employ the GNU General Public License, which states that changes made to an OSS package must be made freely available if the package is redistributed.

Licensing standards

Depending on the type of application being modified, it may be a good idea for the organization to participate in the Open Source Community, provided that the organization is willing to share and make available its modifications to the community. Gartner recommends a "code licensing and definition committee" whose purpose is to make sure that projects utilizing OSS codes comply with licensing standards and legal company restrictions.

But in order to properly prepare the organization for an eventual OSS adoption, an adequate training plan should be developed. Staff skills should be accounted and depending on the nature or type of OSS to be used for particular business units, the corresponding skills should be developed. The organization should help protect their staff against gaps in the business' overall knowledge.

The following questions may help in identifying the areas of concern when adopting OSS in the enterprise:

- 1) What type of application is required?
- 2) What is the objective of the application in terms of assisting the business?
Should the package be specific to the business unit and industry?
- 3) What distribution is the package going to run on, should there be certifications from the distribution regarding the package desired?
- 4) Will there be a need to customize or modify the package to fit specific business processes now or in the future?
- 5) If so, will the modifications be in conformance with any legal standards in place for the package and the company?
- 6) What skills are required to support the package/technology?
- 7) How will the package be deployed and maintained? 

Reference:

A Linux Open Source Best Practices Guide: Applications, Gartner/TechRepublic.com



About the author:

The author is the Linux/Open Source Software evangelist at Fujitsu Philippines and part of the Linux core team that promotes awareness on Linux-based solutions. He was the acting department head and information systems architect for the E-Business Solutions Department of WeServ Systems International, Inc., the software services subsidiary of FPI. He was also the lead designer of the open platform content management system and other community-based web services.

Setting up a more secure network - A Case Study

By Mark Anthony Jastia

Network security has become a vital part of companies' overall mission-critical Information and Communications infrastructure as transactions and the amount of data exchanges grow each day. This article discusses how Fujitsu assisted a certain manufacturing company to implement a more secure ICT infrastructure using efficient network security solutions.

The company's current ICT infrastructure, as shown in fig. 1, is basically composed of a number of hubs, which act as concentrators, a proxy server connected to the Internet using a dial-up connection, a RAS server that allows remote access from different branches, a number of workstations and a server that hosts the application.

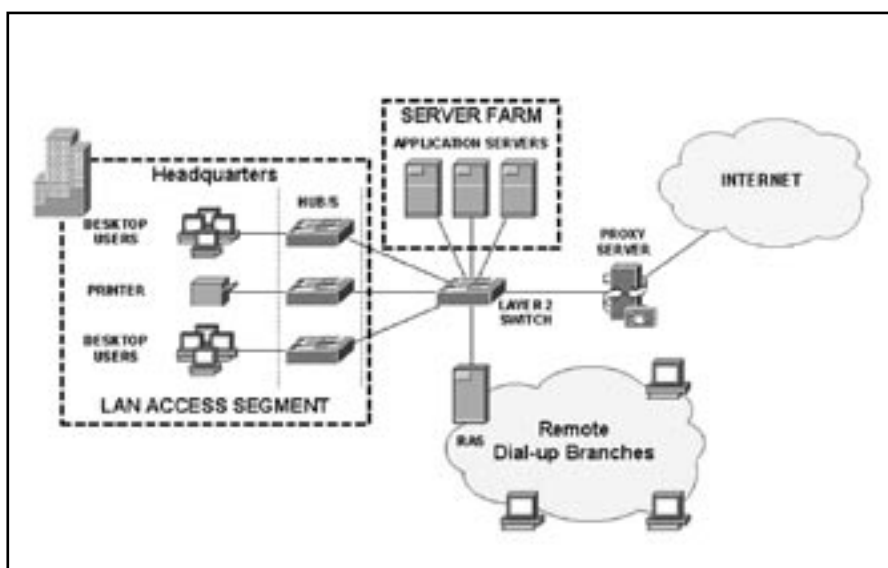


Figure 1 indicates the Open Access Internet model using a proxy server to separate the internal segment from the public network.

Figure 1

To address the security requirements of the company, a secure network infrastructure design was proposed (see fig. 2). Four security solutions were recommended: the firewall, Intrusion Detection System, vulnerability assessment, and an anti-virus solution.

Firewall

The proposed firewall solution integrates the "CheckPoint" firewall at the gateway of the company's corporate network. Based upon the premise that any connection not passing through the firewall is not a secure connection, the "CheckPoint" firewall is strategically placed at the heart of this security set-up to filter all inbound and outbound traffic. It acts as the gateway where all Internet requests are filtered.

The CheckPoint firewall is configured with five separate networks; the Public, DMZ1, DMZ2, Secure Operations Center (SOC), and Internal network.

The Public segment connects the Internet router to the external interface of the firewall. This ensures that all inbound requests from the Internet are filtered before they are transferred to its corresponding destination. Fujitsu recommended implementing stricter rules for the public segment, as this segment is vulnerable to aggression. Requests coming from the Internet are allowed access only on the public servers, such as DNS, SMTP, FTP, and Proxy servers. In this way, only relative ports are opened for every session while other

services are filtered, blocked, and logged on the firewall.

The DMZ1 segment separates the “publicly” accessible servers from the Public and Internal networks. These servers are primarily accessed from the outside, thereby creating the risks of being attacked. Separating these servers from the entire network will confine and isolate those attacks. Proper policies are enforced between the DMZ1-Public and DMZ1-Internal networks to mitigate the risks of being insecure.

The DMZ2 segment separates the remote access connection from the branches and the internal network. A local telephone provider is controlling part of the remote access connection. Thus, stricter policies must also be enforced between the Internal and the DMZ2 segment.

The Secure Operations Center segment separates the different Security Management servers from unauthorized access. Policies are defined to give authorized access to the firewall administrator.

The Internal segment connects the desktop users and mission-critical servers to the internal interface of the firewall.

All segments, except the public segment, are using private IP addressing scheme so that there is no way that the company can be accessed from the Internet through normal network connection.

Network Intrusion Detection System

ISS RealSecure Network Sensors are deployed on the Internet Router Segment and the Internal network’s switch. Both network sensors are running on a Nokia IP330 hardware appliance.

RealSecure for Nokia is an appliance-based intrusion detection sensor designed for easy deployment, featuring a hardened operating system, plug-and-play technology and excellent performance.

All segments, except the public segment, have to implement private IP addressing scheme so that the company’s network will not be accessed from the Internet through normal network connection.

All incoming packets from the Internet to any of the two DMZs are thoroughly monitored by the network sensor located at the Internet Router segment. The same way, the Internal Network Sensor monitors all outgoing packets from the Internal Network to any destination.

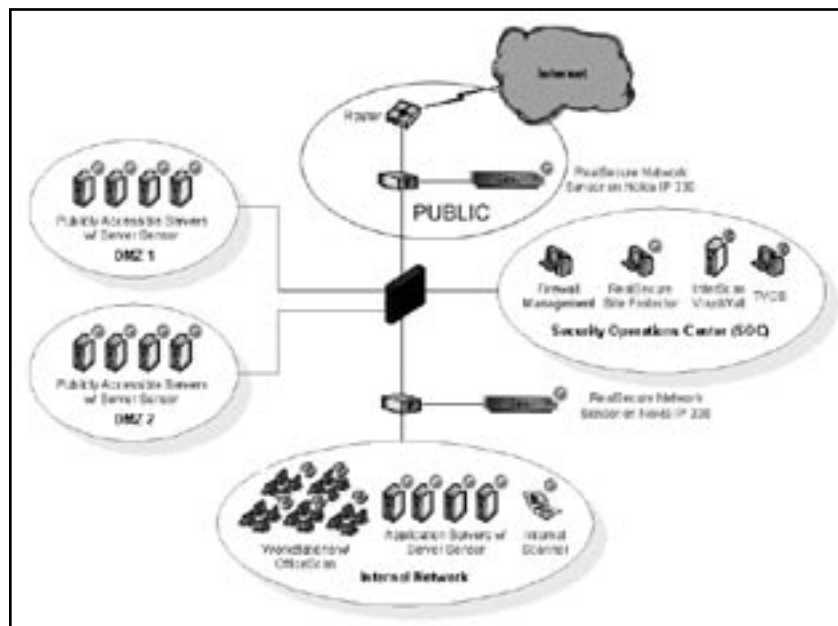
The manner of which these two Network Sensors are positioned covers both potential sources of an attack (since reaching the two DMZs means passing through either one of the Network Sensors). The Network Sensor thoroughly monitors all network activities and responds with appropriate action against any signs of suspicious or malicious activity.

Once triggered, Real Secure can respond in various ways such as sending alerts of the ongoing attacks to administrators, terminating the attack session, recording the attack in real-time for playback forensic evidence and even reconfiguring Check Point firewall to totally block out any external-based attacks.

The interface, which listens to the network segment, are configured in a stealth mode. This is to hide the network sensor from hackers/attackers scanning networks for systems such as an IDS. The other interface of the server is connected to the RealSecure SiteProtector located on the Secure Operations center.

Host Intrusion Detection System

Figure 2 shows a network security infrastructure using an Enterprise Firewall/VPN to secure the perimeter. The perimeter is a combination of network and host sensors to provide 24 x 7 response and monitoring, a vulnerability assessment tool to provide the current security posture, and an enterprise anti-virus to provide a last level of defense from virus attacks.



ISS RealSecure Server Sensors are installed on mission-critical servers of the company. The RealSecure Server Sensor provides broad-based detection, prevention, and response for attacks and misuse directed at these servers.

In addition, RealSecure Server Sensor inspects network traffic at multiple points in the network stack, allowing it to monitor and act on traffic that may have been encrypted by the network. Centrally managed from the RealSecure SiteProtector management platform, RealSecure Server Sensors quickly adjust for different network needs, including user specified alerting, tuning of attack signatures, and creation of user-defined signatures.

Internet Security Systems' RealSecure SiteProtector application provides scalable, centralized security management for RealSecure deployments that significantly reduce demands on operational resources. SiteProtector's unified command, control, and monitoring system scales easily, and enables the use of vulnerability assessment information to automatically configure RealSecure installations against newly discovered threats.

SiteProtector's interface helps administrators work more efficiently through flexible views built around asset grouping and event aggregation. Event prioritization and correlation create real-time attack and misuse tracking. Powerful filters screen for event exceptions and false alerts.

In addition, SiteProtector automates RealSecure Protection System deployment, and enables multi-site management via secure remote administration. ISS is an OPSEC Certified partner whose products work seamlessly with the existing Check Point VPN-1/FireWall-1 implementation.

Vulnerability Assessment

The solution also includes a vulnerability assessment tool also from ISS. The Internet Scanner probes all devices on the network for vulnerabilities, simulating various network attacks. It then takes note of all devices that react to these attacks and sorts them by severity, whether high, medium or low risk vulnerabilities.

The Internet Scanner based on the vulnerabilities found on the network can then generate

a report. The Internet Scanner resides on a portable computer for better mobility when transferring the Internet Scanner to scan different network segments. The SiteProtector located on the SOC can also manage the Internet Scanner.

Anti-Virus

Anti-virus, which is another essential part of security, is also integrated in this security solution. Trend Micro's InterScan VirusWall is installed on a dedicated NT server on the SOC segment that provides a gateway anti-virus system.

Anti-virus solutions are essential parts of security. Trend Micro, for instance, has come up with a variety of effective anti-virus software such as InterScan VirusWall installed on NT servers, OfficeScan for workstations, and Server Protect for Windows-based servers are popular examples.

This anti-virus system works in conjunction with the existing Check Point VPN-1/FireWall-1 server to detect and clean viruses on e-mail attachments (SMTP), Trojans and malicious codes on downloaded WEB pages (HTTP), and assorted file viruses on files in transit (FTP).

A gateway anti-virus approach ensures that all incoming SMTP, HTTP, and FTP from public networks, like the Internet, are free of viruses even before they reach the intended servers and workstations. Rules are created on the firewall to check files and attachments first before accepting.

As such, the firewall first routes all pertinent packets to the InterScan VirusWall server for scanning and cleaning, only after then will these packets be allowed to pass through. Trend Micro InterScan VirusWall, being another OPSEC partner of Check Point, is guaranteed to integrate seamlessly with Check Point VPN-1/FireWall-1.

Another anti-virus solution from Trend Micro called OfficeScan is deployed on workstations on the Internal segment. OfficeScan is a complete enterprise desktop anti-virus solution that is deployed on all the internal users. It is designed for easy server-based deployment, automatic software updates, and centralized reporting – OfficeScan Corporate Edition provides ironclad corporate desktop anti-virus protection with unmatched manageability. The OfficeScan Server, which manages and pushes anti-virus agents across the network, resides on the Internal Network segment.

And to assure virus-free servers, Trend Micro's Server Protect is deployed on Windows-based servers located on the DMZ segments and Internal Network. Server Protect provides comprehensive anti-virus scanning throughout the network for file servers running on NT and Novell Netware. Trend Virus Control System (TVCS) will manage these anti-virus solutions. TVCS is a web-based management tool that allows administrators to configure, monitor, and maintain your anti-virus software from a single console. This is located also on the SOC segment. ∞



About the author:

Mark Anthony R. Jastia is a Senior Solutions Manager for the Information Security Solutions Group (ISSG) at WeSolv Open Computing, Inc., the communications and networking subsidiary of Fujitsu Philippines, Inc. He is in charge of providing efficient security solutions and services for our customers' dynamic needs. He has five years of IT working experience and has worked at FPI since graduating from college.

STAFF BOX	BOARD OF ADVISERS			
	Chairman	Fil Manalang		
	Vice Chairman	Peter Tan		
	Member	Larry Galang	Editor	Betty Jose
			Circulation	Stanley Payte
			Design	Jesse Enriquez
	EDITORIAL BOARD			
	Chairman	Jun Santos		
	Members	Suzette Santiago		
		Jimmy Castaneda		
	Carlos Haw			
	Tony Jocom			
	Lyndon Lacanienta			
	Bing Lawan			
	Romar Padilla			
	Larry Santiago			
		Convergence is a publication of FUJITSU PHILIPPINES, INC. with business office at 2/F United Life Building, A. Arnaiz Ave. (formerly Pasay Road), Legaspi Village, Makati City. For inquiries, comments, and suggestions, please email to the editor at b.jose@fpi.fujitsu.com . Visit the Convergence web site at http://convergence.fpi.com.ph		

How to avoid serious data loss

By Joseph Sta. Brigida

With the 9/11 tragedy, the world was made to realize that nobody is immune from disasters. To avoid data loss, here are some tips that can protect you:

Fire Drills - Regularly schedule “fire drills”. Such exercise can prepare you for the worst and will help you recover in case a disaster strikes your organization.

Have a generator or battery back-up system -

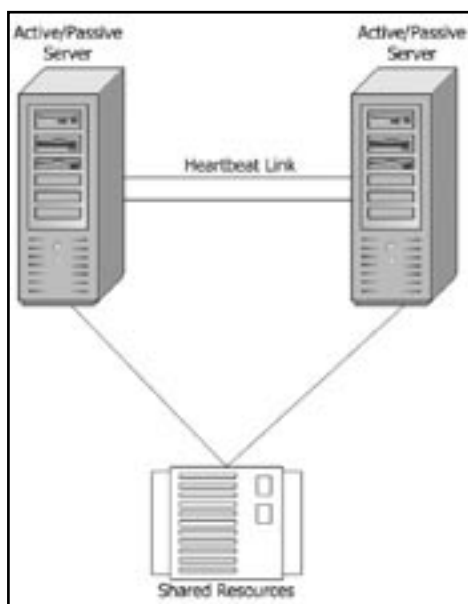
Large power surges can destroy computer equipment, but even relatively low-level bursts of energy can erase the data on hard drives. Uninterrupted power supplies give protection from power surges. A generator or battery back-up system provides stand-by energy to gracefully save data and shut down the system during an outage.

Protect equipment from static electricity - Extraneous static discharge can lead to corruptions and damage to some components. Making your data center a non-static environment will prolong the life of your equipment and will protect your data as well.

Use Virus-detection protection programs - There are software programs that can detect impending problems such as viruses, worms, and malicious codes. Using them regularly can head off problems.

Backup Regularly - Even the most reliable computer can break down eventually. Many professionals recommend that you make two, or even three back-ups of your entire file. To be especially safe, you should keep one back-up in different locations from the others. Verify the backups by actually getting the data off back-up media and restore into the computers. How often should you back up? Some companies have back-ups running

Many professionals recommend that you make two, or even three back-ups of your entire file. To be especially safe, you should keep one back-up in different locations from the others. Verify the backups by actually getting the data off the back-up media and restore into the computer.

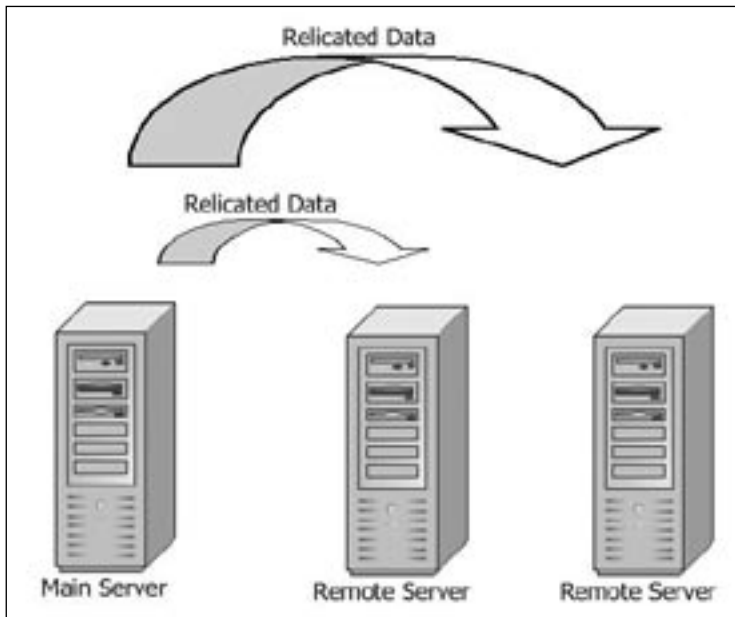


Clustering System is a high availability solution that provides failover. If any components in the Clustering System, hardware or software fail, the user may see degraded performance, but will not lose access to the service.

constantly so they can restore data to the minute. Most computer users don't have that level of need. Decide what's important to you, and then create a schedule to back up your data on a daily or weekly basis.

Backup the most important files or database

- The most important files for you are the data files you create when you operate your e-mail software, word processor, spreadsheet, database, etc. Not all files are automatically saved to your My Documents folder (in the case of Windows users) and you may have to do some investigation with your programs to find out where all your data files are. The programs themselves are not as important because, if you have a full failure of a hard drive, a restored program rarely will operate correctly. To restore your programs, you should reinstall them from the original disks.



Replication System provides synchronization of data in multiple locations. In case the primary server fails, an identical current copy of data is always available for restore operations.

Use a Tape Drive - Storing data on tapes is considerably cheaper than storing data on disk. Tapes also have large storage capacities, ranging from a few hundred kilobytes to several gigabytes. Their transfer speeds are considerably high. Fast drives can transfer as much 20MB(megabytes) per second.

Use Back-up Software - Back-up software is available in a variety of forms, both for tape and other methods. If you're not planning to use a tape back-up facility, check out some of the software titles available in computer stores. These software will allow you to schedule automatic back-up files at a frequency you select. You can use these software to reduce the data to a single back-up file of a size that will fit on some sort of removable media (Zip, Jaz, removable hard drive, Read-Write CDs, etc.) Typically, using the non-tape method, you would create a backup file on your hard drive. Once complete, copy the back-up file to your removable media.

Use RAID System - RAID (Redundant Array of Inexpensive Disks) systems are more resilient than a single hard disk. A RAID uses the capacity of extra disk to retain parity information for the other disks. Therefore, if any one disk fails, the contents of that disk can be automatically reconstructed from the contents of the other disks. Even with a failed disk, the data in the RAID can still be accessed normally.

Use Replication System - Replication does not only make copies of the database but also synchronizes a set of replicas so that changes made to one replica are reflected in all the others in case one of your servers fails. The beauty of replication is that it enables many users to work with their own local copy of a database but have the database updated as if they were working on a single, centralized database. For database applications where users are geographically widely distributed, replication is often the most efficient method of database access.

A replication system must also replicate any major hardware platform to eliminate vendor-specific systems and must also provide complete data integrity for commercial database systems.

Use Server Clustering - High availability is becoming a higher priority for organizations whose networks are hosting mission-critical application systems.

A server clustering allocates the application workload among servers, helping to optimize resource utilization. It also gives users more options for selection fail-over nodes. User can base this decision on factors such as priority (the first available system is chosen automatically), and which system supports the fewest service groups. Another factor is system load, which the software can determine by using a variety of demands and capacity assessment and calculation schemes. ∞

Clustering System, as seen in this figure, is a high availability solution that provides failover. If any components in the Clustering System, hardware or software fail, the user may see degraded performance, but will not lose access to the service.



About the author:

Joseph Sta. Brigida is a Solutions Manager of the Storage Solutions and Services Group (SSSG) at WeCare Technology Services Corp. SSSG focuses on storage software solution such as Veritas, Legato, Computer Associates, and Softek, and also provides storage services such as Storage Assessment, Consulting, and Outsourcing.

Going back to the basics of TCP/IP – Part 2

By Conrado Catindig

Part 1 of this article defined what TCP/IP is, its protocol stack, application protocols, the role of the Transport Control Protocol, as well as the User Datagram Protocol, and how TCP and UDP send datagrams to the Internet Protocol.

Internet Addresses

The IP Address - The Internet uses an addressing scheme to find destinations in the network. This scheme uses 32 bits to define the Internet address that contains a network portion and a host portion. The network portion defines the network (or group of computers) and the host portion is the ID of the machine. The 32 bits are divided equally into four.

Each division is called an “octet” which contains eight bits. IP addresses differ depending on the number of the first octet. The classes of IP addresses define which ones are for public, private, or special purposes only. These IP address classes are named Class A, Class B, and Class C.

A “mask” must always accompany the address. This mask tells a machine the length of the network portion in an IP address. There are different masks used in addressing depending on what scheme is implemented. For example, “default masks” are used normally for some IP addresses. Subnet masks are used to divide a major network into smaller networks.

So what are the classes for? Some are used for small networks, some for large networks, and some for special networks.

Addressing Limitations and Options - The designers of TCP/IP and the Internet somehow realized that there would eventually be a shortage in the addresses. Thus, the designers devised ways to enhance network functionality using different schemes such as: Subnetting – Dividing a major network into smaller networks of equal sizes; Classless Inter-Domain Routing (CIDR, sometimes called supernetting) – Representing, or summarizing several networks as one network; Variable Length Subnet Masking (VLSM) – Creating from one big network subnets of unequal sizes; Network Address Translation (NAT) – Translating one or more private address (es) into a public address; Support for discontinuous networks; and, IP Version 6.

The IP addresses that we are currently using are version 4. a newer version of these addresses is IP version 6. This newer version consists of 128 bits compared with version 4’s 32 bits. This version will mature and there will be mandates for this change. The reason is obvious. Although we can still work using the current version and manage to expand the IP address space with some adjustments, that space will never be enough. Yes, there are millions of Internet users today, but that number is only less than 9% of the world’s total population.

Routing

The Routing Function - Routers are network devices that find networks. It is these devices that PCs pass data to in order to reach the proper destination. In the LAN, it is the hub or switch that recognizes machines by their physical addresses. The hub and switch maintain tables containing the physical addresses of all connected machines. They know what is connected to which port and as a result they recognize who sends data and who receives it.

The router determines paths to destinations and decides which of the possible paths to a destination is the best one. It maintains a routing table in memory and uses different metrics (or factors) in deciding best paths. It comes in many shapes and sizes or may reside in different types of machines but routing is its main function. It serves as the gateway of the LAN to the outside world.

Routing Protocols - Routers need to talk with other routers in the network. The language they

The router determines paths to destinations and decides which of the possible paths to a destination is the best one. It maintains a routing table in memory and uses different metrics in deciding best paths.

use to do this is the routing protocol. This language enables routers to exchange information about local and remote networks. This exchange enables routers to recognize distant networks. Routing protocols differ in the way they send updates or routing information. They also differ in network locations where they are used. Further, routing protocols use manually defined or dynamically learned routes. There are different routing equipment in the market today. To name a few, these are Cisco, Juniper, Foundry Networks, 3Com, D-Link, Linksys, Netgear, and SMC. Some routing protocols are proprietary to some brands, while others are not. So which is the best routing protocol to use? It depends on resources, administration, geography, and sometimes politics.

The Ethernet Level

Most networks today are based on Ethernet. Ethernet is a protocol in the Data Link layer of the ISO OSI model. It specifies physical arrangements of networks, bandwidths, media types and access. Ethernet uses addresses that are more or less the physical address of the machine.

Every network device with an Ethernet card has a unique global address. A central authority manages Ethernet addresses. Ethernet is a broadcast medium, which means that anything you want to get from it, you generally broadcast it to the network.

When you send a frame to the Ethernet network, every machine sees it. Only the intended machine will process it though. Ethernet repackages packets from the IP level adding its own headers and footers to the IP packet. After repackaging the packets to frames, the frames in turn are transformed into bits (ones and zeroes) that are sent to the network.

Every network device with an Ethernet card has a unique global address. A central authority manages Ethernet addresses. Ethernet repackages packets from the IP level adding its own headers and footers to the IP packet.

Business Benefits

Some computer services that can be provided using TCP/IP are: Network File Systems; Remote Printing; Remote Execution; Name Servers; Terminal Servers; and, Network-Oriented Windows.

The list above shows examples of services available through TCP/IP. These services allow people to share printers, fax machines, and data in the office. This set-up avoids the need of one-to-one ownership of equipment and resources. Some services make network maintenance easier for administrators. For example, automatic IP addressing allows networked computers to request IP addresses over the network without manual daily manipulation by the network administrator. Some services even allow administrators to perform tasks remotely, avoiding the need to go from one device to the next.

How is it that different computer systems are able to communicate with desktop PCs? TCP ensures that there is host-to-host communication; IP is used to find computers, and Ethernet or Token Ring takes care of the physical addresses, and a host of protocols manages access.

For More Information

There are numerous materials discussing TCP/IP. Books are available in stores and lots of articles from the Internet. There are Internet-standards or RFCs (Request For Comments) defining specifications for different protocols. Many are posted in the Internet (just go find them). In any case, you can find any of these documents useful in understanding TCP/IP. TCP/IP is a complex subject, so you should only try to read these when you have the time and patience to think about it carefully. ☺

References:

Introduction to the Internet Protocols, Charles Hedrick, Computer Science Facilities Group, Rutgers The State University of New Jersey, Copyright 3 July 1987 (Internet document)
DDN Protocol Handbook, DDN Network Information Center, SRI International, 333 Ravenswood



About the author:

Conrado T. Catindig is a Solutions Manager from the Network Solutions Group (NSG) of WeSolv Open Computing, the networking subsidiary of Fujitsu Philippines. His group is responsible for providing local area and wide area network solutions. The group provides solutions to different clients and prospects in both the service provider and enterprise sectors.