2007

White Paper

Integration with VPN

BoxesOS Managed Hosting Services

This document explains how your organization can outsource the hosting of BoxesOS to Epazz and still receive all of the integration benefits.

Table of Contents

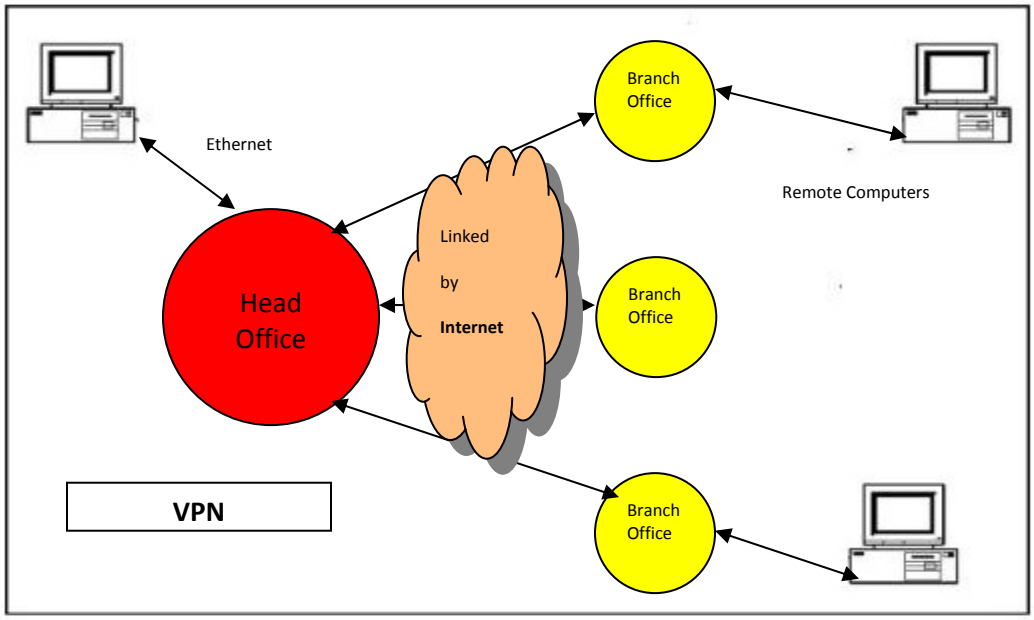
What is VPN?

In this age of globalization businesses have expanded, dealing not only with the local and the regional markets, but also the markets throughout the world. The global business houses have the main or the corporate office located at a particular place and the branch offices located in various other parts of the country or the world. Many businesses have their representatives moving globally. The executives and the high level managers have to travel to various places meeting with the clients for getting the projects and solving the problems.

One of the major problems with the branches or people spread in remote locations is the communication with the corporate office. It is crucial for the remote offices and the representatives to remain in constant contact with the corporate office to get the details of the work and related instructions. In many cases, especially the software development companies, a lot of data has to be transferred between the corporate office and the remote offices. This can be in tera bytes at times.

The corporate office and the offices scattered globally have their own network of computers. The individual users work for the company from a particular location, home, or while traveling by using the laptop. This is where the Virtual Private Network (VPN) plays the dominant role. The virtual private network provides the remote offices and individual users with secure access to their organization's network by using the telecommunication infrastructure such as the Internet.

VPNs links the local area networks (LANs) of the remote offices, form the wide area networks (WAN), and create intranets and extranets. The LANs of the remote places are connected by using the public Internet infrastructure. It does not require dedicated E1 or DDN lines, and it uses only the dedicated equipment already available at the site.



All that is required to use the VPN is the Internet and some hardware. Since the cost of building the VPN infrastructure is quite less, it is very suitable for small and medium enterprises.

With the help of VPN, the remote offices are connected to the corporate office 24 hours a day while the individual users can connect at any time as per the requirements. This helps in maintaining the close and live communication between the remote offices and the corporate office. For the remote office personnel and the individual, VPN is just the extension of the LAN.

Types of VPN

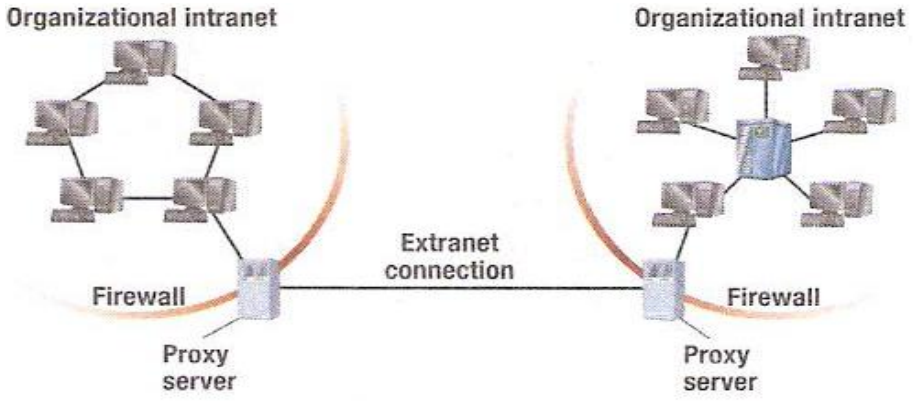
There are two main types of VPN:

1) **Remote Access VPN**: For a company having many employees in remote places who should be able to connect to its network, a user-to-LAN connection called remote-access or virtual private dial-up network (also called VPDN) is suitable. Remote access to the company resources is provided, keeping the information private. In these cases, the company out-sources the VPN service to an enterprise service provider (ESP) who provides hardware in the form of a network access server (NAS) and desktop client software for the computers of the remote users. With the help of the toll-free number, the users can reach the NAS, while the software enables them to enter into the company's network.

2) **Site-to-Site VPN:** In the Site-to-Site type of VPN, various remote offices can be connected to the corporate office by using local dedicated equipment and large scale encryption over the public network-like Internet. In this case, merely a connection to the local ISP is required, and just by using the internet, the VPN software creates the virtual private network between the user and the corporate VPN server. Thus, no dedicated lines are required, and no long distance calls or toll free calls to a corporate outsourced NAS are required. Calls only to the local ISP are required.

There are two possibilities for this arrangement:

a) Intranet: In this system, various remote locations or the branch offices of the company having independent LAN can connect to the LAN of the corporate office.
b) Extranet: Many companies want to share the data and information with the partners, suppliers, customers, students (for educational institutions) and others. Extranet is the VPN that allows connecting the LAN of more than one organization.



Implementation of BoxesOS over VPN

On the VPN of the organization, one can find browsers, websites, and web pages just like the Internet. VPN has greatly helped in developing the channels of communication between remote offices and the individual users and the corporate office. But in this age of communication, a lot more is desired.

The individual users placed not only in the remote locations but also in the corporate office have to remain in constant contact with each other. They have various tasks to be completed, meetings with clients and colleagues, a number of emails to access and reply, meet certain deadlines and much more. To increase the productivity, it is also very important to impart new trainings to the employees. All this has to be done in a real-time manner as if the employees were located at a single place. In short, the effects of the distance should be seamless.

All this communication has to be made between all the employees located at the corporate office as well as the remote office. The VPN provides us the channel for the communication, but the BoxesOS™ from Epazz provides a platform for the communication between the employees.

BoxesOS™ is a Web Infrastructure System (W I S) for the enterprise community. It is designed to maximize communication, functionality and operations for the key stakeholders (employees, senior management, clients, partners and suppliers), providing one-stop access, secure, Internet-enabled real-time integration to administrative operating systems. BoxesOS™ enhances stakeholders' experiences with your company, thereby fostering relationships.

BoxesOS™ enables the user to immediately enhance communication between the stakeholders. There is improvement in administrative utility irrespective of whether they are on legacy platforms or recent ERP implementations (such as PeopleSoft, MS Dynamics, DataTel, SCT, Oracle, and SAP). With BoxesOS™ 3.0, you can connect multiple databases over VPN.

To implement BoxesOS™ in your VPN environment, you need to utilize the turnkey solution from Epazz. This is comprised of software, content services, integration services, customization services, maintenance services, marketing services and hardware. It is an immediate user-group utility accompanied by secure and administrative functionality and can easily cut over to new administrative platforms. The implementation team will help customize BoxesOS™ into the company's requirements and network environment.

Epazz has significant years of experience in deploying enterprise-level web base systems. Epazz BoxesOS™ has been more than five years in design and testing among more than tens of thousands of members of five key user stakeholder groups to carefully incorporate desired design, features and functions.

BoxesOS™ allows the institution to start-up by implementing elegant web-enabled information dashboards for each stakeholder group. Functionality with administrative systems can be swiftly completed using connectors to legacy administrative platforms. Administrative operating systems that require upgrading can be upgraded on a prioritized basis as desired and easily linked to BoxesOS™ and

its personal information system. The highly-functional stakeholder information dashboard can be customized to meet your specific requirements.

Applications of VPN

Before going into the security measure and other requirements of VPN, look at some applications of VPN.

1) ***Internal Office Networking:*** Suppose yours is a big educational institute teaching a number of technical courses in different buildings which may be beside each other or across the street. Let us suppose there is a central computer located in the computer department. There are also other computers in the computer department and other buildings conducting different courses.

   Suppose data is to be exchanged between the different buildings; you can set up the connection between various LANs of the buildings by creating the VPN by using the cheap Internet connection from your telephone lines. You don't need the special and expensive leased lines.

   You get high quality data at fast speeds with maximum security. In fact, the data security provided by VPN makes it ideal for internal data privacy.

   VPN can also be created between various departments of the company. In such cases, a VPN device like a router, switch or server is placed between the departmental computers and the main network backbone.

   Here, BoxesOS™ from Epazz can further help bring close communication between the stakeholders. It also provides additional functionalities like web designing, training of the employees, scheduling, and more.

2) ***External Office Networking:*** Suppose there is a big company having a number of branch or group offices or individuals located in remote places. There has to be a lot of data exchange between its offices. In addition, the company has customers, vendors, and some partners who need access to the data.

   Whether the offices are local, interstate or international, an extranet atmosphere with VPN will be perfect for them. This allows fast access of data for all the authorized offices and individuals. All that will be needed in the offices is the Internet connection by using the dial-up or broadband connection.

   The VPN client authenticates itself to the VPN server on the corporate network; at the same time, the VPN server must authenticate itself to the client. This establishes point-to-site networking with ensured security.

Security of VPN

Since the LANs of remote places are connected by the Internet, it is possible for the public to access the data of the corporate as well as the remote office. The transfer between the remote location and the corporate office takes place in the form of a secure and encrypted tunnel. Only the authorized users can access the data, and it cannot be read by other Internet users.

Firewall

The firewall prevents the organization's VPN from the common threats of the Internet. It is comprised of the hardware and the software that prevent unauthorized users from entering the company's network. Typically, it consists of a special computer (called a proxy server) that acts as the "gate keeper". You should not use the VPN without the proper firewalls in place.

Data Encryption

To prevent the public from accessing the VPN data over the Internet, the data traveling from one network to the other is encrypted. In this system, the encrypted data sent from one computer can be decrypted by only the computer to which the data is sent. No one else has access to this data.

There are two common types of encryption systems: public-key encryption and symmetric-key encryption. In public-key encryption there are two keys – a public key and a private key. The private key is known only to a specific computer that can send it to another computer that wants to communicate securely. To open the data, the computer needs the public key sent by the originating computer and its own private key.

In the symmetric-key system, each computer in the network is provided with a secret key that enables it to encrypt the packet information, before it is sent to the computer over the other network. Any computer that wishes to communicate with any other computer should know its key. Each of the two computers should know its key so as to communicate.

Tunneling

The data travels through the VPN in the form of encrypted packets. This private data travels through the public Internet, but it is encapsulated within a small portion of connection known as a tunnel. Actually, tunneling is placing the entire packet in another packet and sending it across the network. The tunnel interfaces (i.e. the starting and the ending points) of points of the network and the network itself understand the protocol of the outer packet. The process of the creation of tunnels requires various protocols to be followed which ensure proper flow of the packets and its security.

There are two methods of tunneling. In the voluntary tunneling method, the client at the remote office develops the connection with the service provider. Once the connection is developed, the VPN client creates the tunnel to the VPN server. In the compulsory tunneling method, it is the service provider who manages the VPN connection and facilitates the connection between the VPN server and the client.

Tunneling requires the three protocols mentioned below:

1) Point-to-Point Tunneling Protocol (PPTP): This allows IP, IPX, or NetBEUI traffic to be encrypted and then encapsulated in an IP header to be sent across the Internet.
2) Layer Two Tunneling Protocol (L2TP): This allows IP, IPX, or NetBEUI traffic to be encrypted and then sent over any medium that supports point-to-point datagram delivery such as IP, X.25, Frame Relay, or ATM.
3) IPSec tunnel mode: This allows IP packets to be encrypted and then encapsulated in an IP header to be sent across the Internet.

Protocols on VPN

Since the security of data transfer through the VPN is of utmost importance, protocols are followed for the data encryption on VPN. The commonly followed protocols are:

1) ***Internet Protocol Security Protocol (IPSec):*** This is the most widely deployed protocol developed by IETF for the security of packets transferred through VPN at the IP layer. IPSec provides strong encryption algorithms and comprehensive authentication for the users. Two encryption modes supported by IPSec are: tunnel and transport. The transport mode helps by encrypting the data portion (payload) without touching the header. The tunnel mode is more secure, as it encrypts the payload as well as the header. On the network where the data is to be received, there are IPSec compliant devices which decrypt each packet. Thus, to take the advantage of this protocol, it is essential that all the systems used in VPN are IPSec compliant.

   Further, for the working of the IPSec, it is essential that the sending and the receiving devices share a public key. This is accomplished deploying a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley). This enables the receiver to get the public key to authenticate the user to use the digital certificates.

2) ***Point-to-Point Protocol (PPTP):*** This new technology for the creation of VPN has been developed by Microsoft, U.S. Robotics, 3COM, Ascend and ECI Telematics, together known as PPTP Forum. This protocol keeps the data safe, as it is transferred over the public Internet, allowing only the authorized users to access it. The user can easily connect to the corporate network by using the Internet. However, it is important to note that PPTP by itself will not encrypt the data, but it ensures that the data transferred is encrypted. Using a protocol called Microsoft Point-to-Point Encryption (MPPE), PPTP supports multi-protocol VPNs with 40-bit and 128-bit encryption.

3) ***Layer Two Tunneling Protocol (L2PT)/ IPSec:*** This is comprised of the best features of Layer two Tunneling and IPSec protocol. It is the outcome of the combined partnership of PPTP forum, Cisco and the Internet Engineering Task Force (IETF). This combined protocol is commonly used with the VPNs working on the Windows 2000 operating system, as it provides native IPSec and L2PT to the client. For dial-up users, the ISPs provide an L2PT

connection, encrypting the traffic between their access point and the remote office server with IPSec.

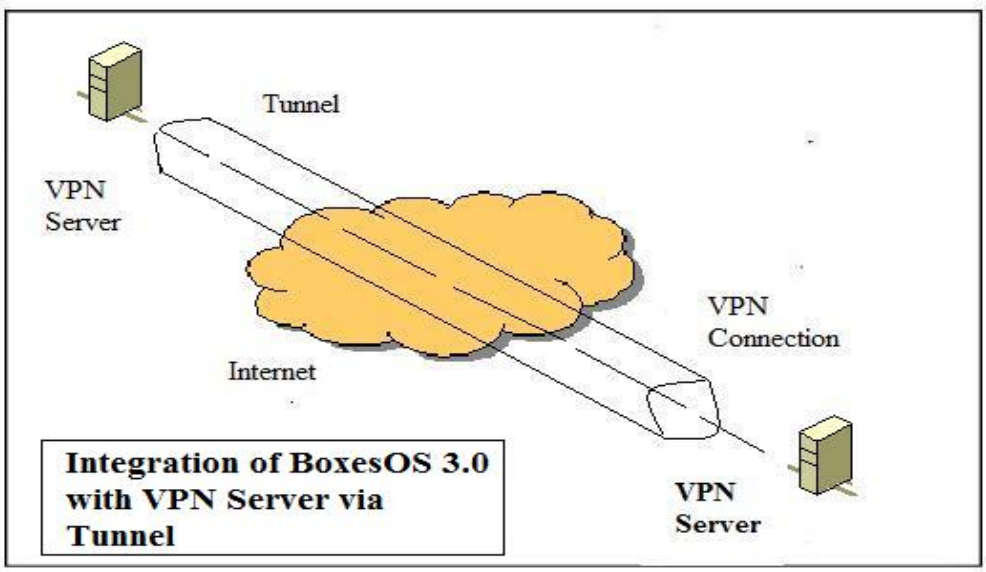
Other VPN technologies

Besides the security features of firewall, tunneling, encryption, and protocols, a number of other technologies are used on the VPN for the security and smooth functioning of the VPNs. Some of these technologies are:

1) Integrity of data: The data is encrypted over the Internet; still, it is important to confirm that the data is not altered during transition. IPSec has a built-in mechanism that can ensure that the data received in the form of packets (its header and data part) is not tampered with. If tampering is detected, the packet is dropped for security reasons. It is also important to authenticate the remote peer before allowing it access.
2) Authenticating the origin of data: It is very crucial to identify the source from which the data is sent. This is to ensure that only the authorized users are using the VPN and to avoid spammers and other hackers.
3) Authentication, Authorization, and Accounting (AAA): This is to ensure that the unauthorized users do not enter the company's VPN and access the confidential information. When a user requests a connection into the company's VPN, the VPN device prompts for a username and password. This can be authenticated locally or sent to the external AAA servers that authenticate (checks who you are), authorizes (checks what you are allowed to do) and keep your account (checks what you do).

Integration of BoxesOS™ 3.0 with VPN

Epazz Pathways is an integration suite for application enabling real-time integration with ERP and Legacy systems. BoxesOS™ initializes Pathways to create a tunnel to each database point. VPN, which has already established Pathways, sends the proper Authentication. Pathways integration suite allows for institutions to retrieve real-time data from ERPs and write data back to ERPs. Pathways provide a library of enterprise connectors and adapters accessing multi data sources in a single, secure web platform. Epazz Pathways uses open data access technologies such as ODBC, OLE DB and JDBC. Pathways help institutions be flexible on their front-end application options.



Remote Method Invocation (RMI) & Pathways : Pathways Real-time integration from BoxesOS™ to ERPs is achieved with Java Remote Method Invocation (RMI). Java Remote Method Invocation enables Pathways to create distributed Java technology-based to Java technology-based applications in which the methods of remote Java objects can be invoked from other Java virtual machines. RMI uses object serialization to marshal and unmarshal parameters and does not truncate types, supporting true object-oriented polymorphism. Pathways applications use RMI to invoke applications on the ERPs.

When a user logs in to update their address in BoxesOS™, the user clicks on the save button. Pathways senses a change which will affect the ERPs and sends a request through Pathways to RMI to invoke the program which maintains the user's address information. RMI will then execute the request, and return a confirmation message to the user that their address has been changed.

The strength of BoxesOS™ is the layer it provides to the organization's ERP. If the administrator wishes to view address changes before the address is updated in ERP, the administrator can setup an approval scheme in BoxesOS™. This way, the administrators can first view the request to change an address in BoxesOS™ before the address information is changed in ERP. The user does not access ERP. This is done by using a background account. RMI maintains the existing core security module in ERP. RMI is

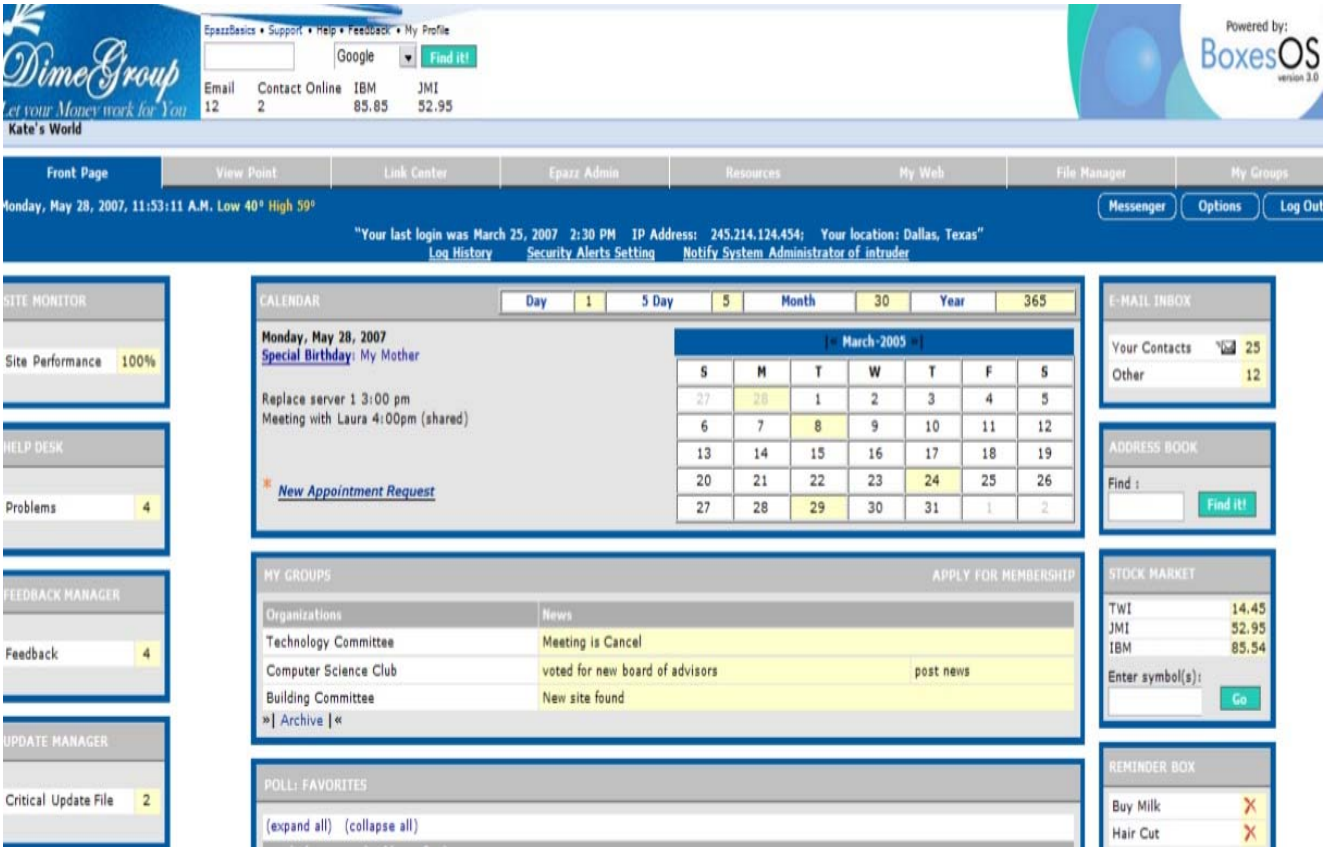
continuing to run, spawning thread for each additional request. RMI is self-healing; if the main process dies, it will be restarted automatically.

Features of BoxesOS™ on VPN

Here are only a few of the many features of the BoxesOS™ 3.0 that can be accessed on the VPN.

Web Portal Component

BoxesOS™ Web Portal Component is a gateway to all of the company's online services and information resources. The Web Portal Component provides a Personal Information System which refers to the user's entire Epazz environment - the resources, information, graphics, color, layout, and organization - all of which are customizable. Web Portal Component makes it simple for companies to create and deploy custom web applications with a common graphic user interface and connectivity to the back-end systems. BoxesOS™ will save time and resources.

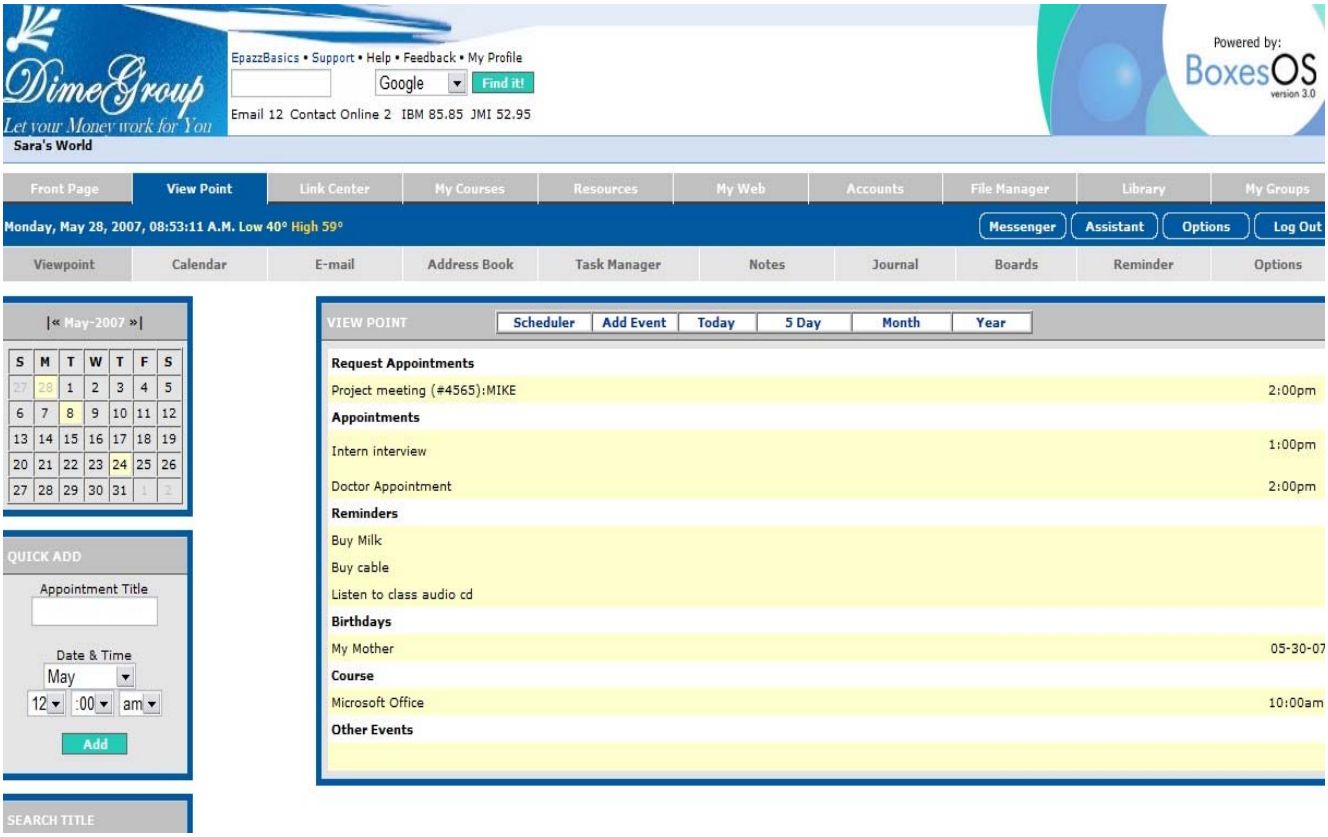


Communication, Calendaring, and Scheduling

ViewPoint is BoxesOS's communication hub that allows her to add events, schedule appointments, check e-mail and post messages on the company's board. ViewPoint is BoxesOS™ central communication, calendaring and scheduling system.

The enriched web applications provide the company with an extensive range of options. Email applications provide all of the great features you would find on Yahoo! and Hotmail. ViewPoint provides a robust threaded discussion board and chatting environment.

ViewPoint also offers each user a personal calendar which notifies them of scheduling conflicts and appointments priorities. ViewPoint makes it easy to create group and public calendars. With the ViewPoint scheduling system, users are able to schedule group meetings together. The scheduling system will view each user's calendar to see the next available time and date the group can meet.



Administrative Content Management

BoxesOS™ Content Management Component provides a company with enterprise level tools for creating, managing, organizing, archiving and sharing content. Content can be delivered in many forms such as web pages, e-mails, polls, documents, RSS, and hot news. Content Management Component

enables staff members with little technical skills to create web pages without needing to know any HTML.

Web Site Management is the tool all companies need to manage private and public web sites. This application allows for multiple individuals to change content on a webpage without the need for programming knowledge. Web developers can create a style sheet and assign access levels for editing, adding, uploading and deleting of information.

Central Repository

BoxesOS™ Central Knowledge Repository is a collection and indexing of shareable content. Central Knowledge Repository installs a server index application on the Windows 2003 platform to identify the company's current knowledge assets. All knowledge assets will be imported in the Dell Storage device. The server index application will import the knowledge assets into a temporary folder before moving it into a main folder. The server index application will prompt the company administrators to add detailed information about the knowledge assets into the database by using a Web form. The company would be able to group its knowledge objects by partner, client, subject, topic, employee, users, content, date, etc.

Learning Management System

My Courses is the powerful tool of e-learning which enables Carmen and other employees to learn new skills, technologies and test new company systems. The applications are created with the help of higher education institutes. These courses are a great way to increase productivity. The employees can take the course with or without the tutor and pace as per their convenience. They can take tests, download course materials and register for workshops.

My Courses provides a robust grade book, powerful authoring content tools, easy to use drop boxes, sharable folders, wide-ranging course calendar and many more features all designed to provide customization to each company, each instructor and each student.

Stakeholder Management

These are a defined group of users (stakeholders) such as employees, clients and partners. Administrators can create new stakeholders and assign rights to view the various tabs and boxes (functionalities) at the time of each stakeholder creation. Once a stakeholder logs on and is authenticated, the tabs assigned for access appear dynamically in the browser client. For example, if access to the "Viewpoint" tab is granted, then it will be available for the stakeholder on the top menu; otherwise, it will not appear.

Scalability

BoxesOS™ has been tested on 5,000 simultaneous connections. It provides high scalability to 20,000 active users. If more connections are needed, Epazz will provide additional servers. BoxesOS™ was designed for high volume traffic.

Summary of Advantages of VPN and BoxesOS 3.0

1) VPN helps communicating geographically separated LANs of offices. BoxesOS™ from Epazz is designed to maximize communication and functionality for key stakeholders located at various places.
2) VPN can easily be established over the Internet. BoxesOS™ provides the additional benefits of secure, Internet-enabled integration to administrative operating systems.
3) The staff can easily access the data over VPN. The BoxesOS™'s Open Enterprise Architecture allows the company's staff to create customized applications to BoxesOS™.
4) VPN improves productivity by providing fast and secure communication. BoxesOS™ improves productivity by enhancing communication and increasing functionality and providing new skills to the employees.
5) Setting up VPN has become comparatively easier. Similarly, to setup BoxesOS™ 3.0, all you need is a turnkey solution from Epazz.
6) VPN takes a few days to setup, and you can easily implement BoxesOS™ over it within 2-4 days. In addition, with the initial solution, you get Integration Services & Customization services.

www.epazz.com

(800) 324-9397

Epazz, Inc.
(312) 955-8161
445 E Ohio St Suite 250
Chicago, IL 60611

About Epazz, Inc.

Epazz Inc. is an enterprise-wide software company that specializes in providing customized web applications to the corporate world, higher education institutions and the public sector. Epazz's unique BoxesOS™ applications can create virtual communities for enhanced communication, provide information and content for decision-making, and create a secure marketplace for any type of commerce all through the medium of the Internet. Epazz is the answer to the increasing information technology demand of the 21st century.