XBand

Features (Extensive List)

- **Authentication. Authorization and Accounting Gateway**
  Passport provides a mechanism which allows user on a closed network to gain rights to use network services as defined in the profile created for the particular user.
  It will authenticate a user on the basis of
  1. IP /Mac/User id
  2. Type (administrator/user)

- **Bandwidth Control**
  This module basically features on controlling the bandwidth requirements of the Network/Users. This also deals with dynamically setting up of bandwidth requirements. This will be done accordingly
  1. By defining bandwidth requirements on a particular user/IP/Pool/Time/Protocol*.
  2. Restrictions on bandwidth requirements for upload and download data transfer.
  3. Should also give the total bandwidth status of bandwidth available/used on the passport server. Since passport is directly on the Internet backbone & the LAN is further connected a cumulative status of bandwidth on passport is desirable to see the overall status of the network.

- **Network Security**
  Restricting the traffic on the basis of
  1. Specific/Generic URLs, Source –IP, Destination-IP, Source Port, Destination Port, Expressions, Phrases.
  2. Blocking the NetBIOS and NetBEUI traffic.
  3. Ability to deal with Denial of Service Attacks*
  4. Reduction of Network Congestion *
  5. Restricting the traffic of a particular application at any point of time for e.g. restricting the FTP/mails during times when its critical (i.e. virus attacks etc)
  6. Scheduled access control. This will be used to configure to allow or deny access at specific periods. For example, this could be used to limit the amount of time staff can browse the web during the working day.
  7. Stateful inspection: Stateful Inspection architecture intercepts, analyzes, and takes action on all communications before they enter the operating system of the gateway machine, ensuring the full security and integrity of the network and the gateway itself. Any traffic not explicitly allowed by the security rules is dropped by default and real-time security alerts and logs are generated, providing the system manager with complete network status.
  8. Logging: Firewall events can be selectively logged to physical medium. This will detect and log range of denial of service attacks including SYN and FIN flooding, ping of Death, Smurf Packets and port scans.
  9. Anti virus Solution support: it should be open to loading of AV solutions like Symantec AV corporate edition where in the server takes care of the viruses in the network servers & workstations (including mobile users)

from the main machines. This would ensure a virus free environment in the complete network

- **Network Connectivity**
  Should be able to support connectivity through:
  1. Ethernet LANs.
  2. Wireless LANs.
  3. Cable Modems.
  4. DSL Networks.
  5. Tel Lines of Data compatible EPABX through RAS.

- **Interface for Users**
  Facilitate the user interface with following facilities
  1. Change of password
  2. Change of Secret Questionsh
  3. View Profile
  4. View Statistics

- **Accounting**
  1. Payment details (mode of payment, payment type, amount)
  2. Package details (package name, type)
  3. Flexible Billing – Usage by Time and Data Transfer
  4. Billing Cycle.
  5. Provision of integrating Payment gateway in future i.e. the passport server interact directly with a web interface & e-commerce can take place can take place.

- **Messaging and Brand Image**
  This includes creation, sending and management of messages for
  1. For various notifications
     Package expiry, Renewal Details, network problems, package details and Modifications. These messages exemplify the above module
     a. You have been deactivated by the Administrator
     b. You have been disconnected by the administrator
     c. You are not allowed to login from this machine
     d. You have used up your allotted surfing time, so you have been disconnected from the Internet
     e. Wrong username/password

  2. For troubleshooting
  3. For advertisement

  This applies to a particular user, group of users and all users.

- **Network Trouble Shooting and Monitoring Wizard**
  This module is used by the administrator for:
  1. Monitoring the bandwidth usage on daily/weekly/fortnightly/monthly and yearly basis.
  2. The Passport administrator could control and monitor its passport customers by storing their information in a management information base (MIB) .Now using SNMP and these MIB values it can control, administer, and troubleshoot his customers remotely.
  3. Checking the status of Passport Server, Gateways, DNS Servers, and Cache Server.
  4. Checking the status of Users (Active, Inactive, Online, and Offline).

5. Troubleshooting a particular user.
6. Real Time Web Based Monitoring.

- **Package Management**

  This module deals with the creation and the management of the packages which include
  1. Creation of new packages where we can define Surfing policies, Access Policies, Bandwidth policies, Price, Payment type.
  2. Managing and editing the existing packages.
  3. Ability to charge on the usage pattern
  4. Based on days and Hours
  5. Restriction based on Time, Services and Groups and username.

- **User Data Backup and Restore facility**
- **Local Support/Entertainment Portal**
  - Email Support: should have the ability to support emails for the users on the network i.e. a mail server can be integrated with Passport for the passport users.
  - Space on Passport Server for Users of Passport
  - Paid Audio/Video on Demand
  - Online Gaming
  - News and Normal Announcements
  - Support site
    - Downloadable Software
    - User Manual
    - FAQ's
    - Brochure/Manuals

- **Migration tool for 24 online subscribers**

  This module will automatically transport the user database of 24 online subscribers to the passport's database making it completely transparent to the user.

- **System Services Modules**

  This module will manage and configure various system services which Include
  1. Configuration and management of Routing, DNS servers, Cache Server, DHCP Server, Passport Server.
  2. Starting and Stopping of remote services.
  3. Supporting Multiple Gateways.
  4. Cache Management

- **User Management**

  This module will be dealing with creation, management and editing of user and user pools.
  1. Assigning a zone to a user.
  2. Assigning priorities to the services provided to the user.
  3. Assigning package policies to the user which includes bandwidth policies, surfing policies access policies.

- **Prioritization Module**
  This module will assign priorities to different types of traffic according to
  1. The IP Pool/IP.
  2. The Protocol/Service.
  3. Definition of classes and assignment of priorities and bandwidths to each class.

- **Search Module**
  This module will search the information on the basis of
  1. Pool
  2. User Name/IP/Mac/User ID/User Type

- **Modular Integration and facility to hold plug-ins**
  Passport provides user extensibility via dynamically loadable software components (plug ins). The use of plug-ins allows users to activate only the needed ones depending on the specific situation where passport is being used. It may also be beneficial in the up gradation of the software.

- **Extensive reporting (Graph and Tabular)**
  This module will generate reports on the basis of
  1. User wise.
  2. Zone wise.
  3. Pool Wise.
  4. Package Wise

  Reports will be of following types
  1. Web Surfing.
  2. Internet Usage.
  3. Bandwidth Usage
  4. MIS
  5. Audit Trail

For each host, passport records the following information:

- **Data sent/received**: The total traffic (volume and packets) generated or received by the host classified according to network protocol (IP, IPX, AppleTalk, etc.) and, when applicable, IP protocol (FTP, HTTP, NFS, etc.).
- **TCP session's history**: The list of currently active TCP sessions established/accepted by the host and associated traffic statistics.
- **UDP traffic**: The total amount of UDP traffic (volume and packets) sorted by port. It is worth noting that it is possible to recognize simple port scan and protocol scan (e.g., an SNMP manager issued SNMP requests to a given host) when the host has received packets at a specified port but has sent no data.
- **TCP/UDP used services**: The list of IP based services (e.g., open and active ports) provided by the host with the list of the last five hosts that used them.
- **Operating system (OS) type**: The operating system of the host is identified.
- **Used bandwidth percentage**: Actual, average, and peak bandwidth usage.
- **Traffic distribution**: Local (subnet) traffic, local vs. remote (outside specified/local subnet), remote vs. local.
- **IP traffic distribution**: UDP vs. TCP traffic; relative distribution of the IP protocols according to the host name.

- **Local network usage**: Statistics about open sockets, data sent/received, and contacted peers for each process running on the host.

In addition, passport reports **global traffic statistics**, including:

- **Traffic distribution**: Local (subnet) traffic, local vs. remote (outside specified/local subnet), remote vs. local.
- **Packet distribution**: Total number of packets sorted by packet size, unicast vs. multicast vs. broadcast, and IP vs. non-IP traffic.
- **Used bandwidth**: Actual, peak, and average bandwidth usage.
- The list of **active TCP sessions** for each known host.
- **Protocol utilization and distribution**: Distribution of the observed traffic according to both protocol and source–destination (local vs. remote).
- **Local subnet traffic matrix**: 2D matrix where each cell (X, Y) contains the traffic sent by host X to host Y, where X and Y are hosts that belong to the local subnet of the host where passport is running.
- **Network Flows**: Traffic statistics for each user-defined flow.
- **Use of duplicate IP addresses**.
- **Identification of all the subnet routers** so that it is possible to find out whether a misconfigured host wrongly believes it acts as a router for the local subnet or a host is using a wrong netmask for the actual network.
- **Protocol misuse:** Identification of those computers that speak unnecessary protocols. For instance, the Windows OS installs by default protocols such as NetBEUI and IPX, while most people use just TCP/IP.
- **Excessive network bandwidth utilization**: In organizations where the Internet connection has limited bandwidth, it is important to detect the hosts/users that use most of the available bandwidth. For instance, this can be done by either tracking traffic values for certain protocols (i.e., HTTP or FTP) or identifying hosts with connections established with remote hosts.