

Network Topology

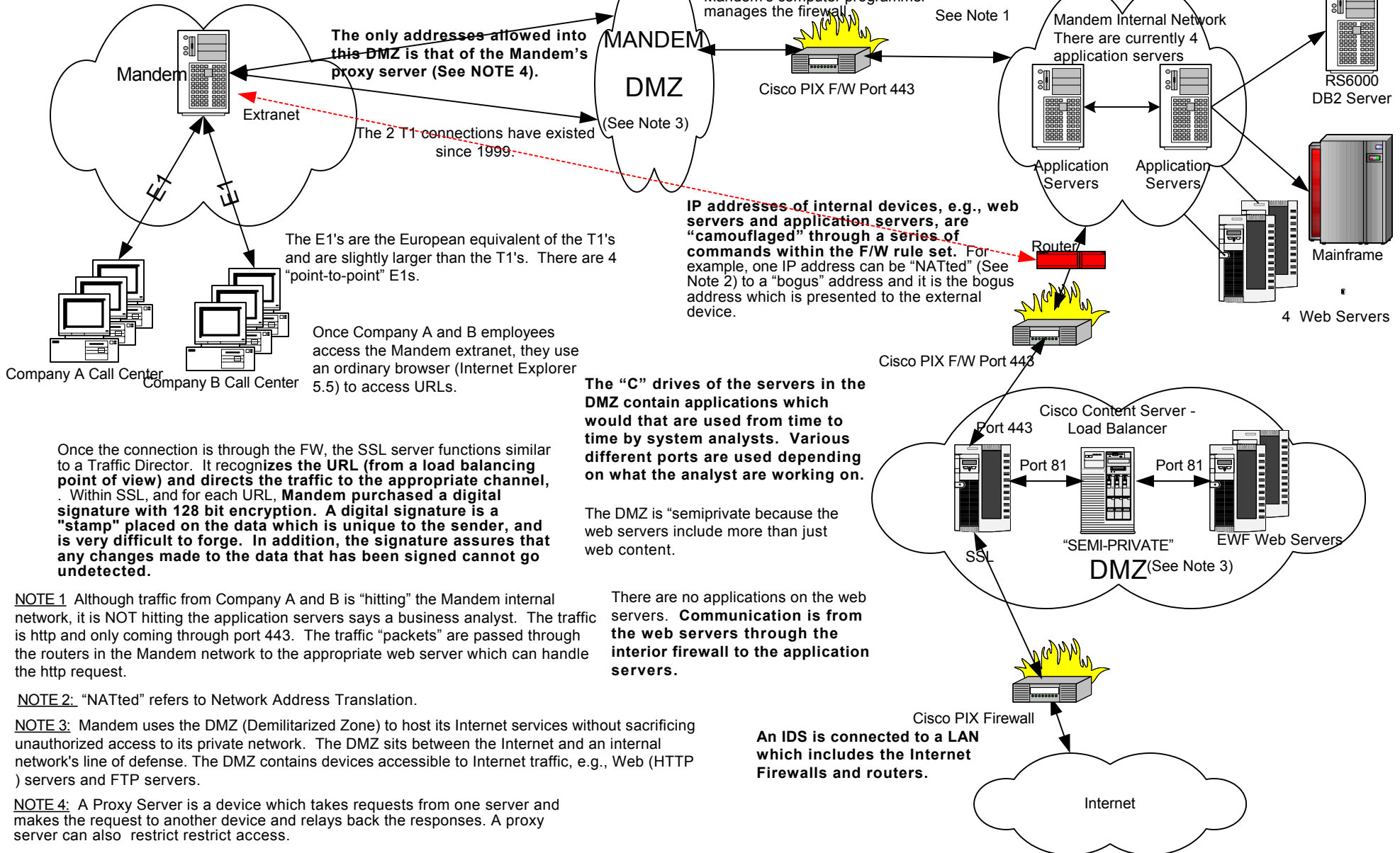
The extranet is an intranet that is partially accessible to authorized outsiders. Whereas Mandem's intranet resides behind a firewall and is accessible only to people who are authorized, the extranet provides various levels of accessibility to outsiders. **When Client A and B employees authenticate themselves to their own network, they bring themselves into the Mandem's Extranet.**

The DMZ contains 2 Cisco 2600 routers, 2 Catalyst 2900 switches and 1 PIX 520 firewalls.

The firewall (FW) opens a **secure hypertext transfer session (https) with the SSL server (a specific site address)**. The FW is programmed with either specific allowable IP addresses or a specific range of allowable IP addresses. In addition, traffic is restricted based on port number, e.g., port 443. Mandem's computer programmer manages the firewall.

Another content server and Web server are located within the Mandem Internal Network

The user password is not encrypted and is rarely compared to the encrypted password in the DB2 database which resides on the internal network and is accessible by internal application servers. If there is a match, the source is considered to be "trusted" and access through the web page to the application server is permitted. Problems generally happen in the production environment and so the DBAs usually resolve issues and clean up database crashes on the fly.



The only addresses allowed into this DMZ is that of the Mandem's proxy server (See NOTE 4).

The 2 T1 connections have existed since 1999.

The E1's are the European equivalent of the T1's and are slightly larger than the T1's. There are 4 "point-to-point" E1's.

Once Company A and B employees access the Mandem extranet, they use an ordinary browser (Internet Explorer 5.5) to access URLs.

IP addresses of internal devices, e.g., web servers and application servers, are "camouflaged" through a series of commands within the F/W rule set. For example, one IP address can be "NATted" (See Note 2) to a "bogus" address and it is the bogus address which is presented to the external device.

The "C" drives of the servers in the DMZ contain applications which would that are used from time to time by system analysts. Various different ports are used depending on what the analyst are working on.

The DMZ is "semiprivate because the web servers include more than just web content.

There are no applications on the web servers. **Communication is from the web servers through the interior firewall to the application servers.**

Once the connection is through the FW, the SSL server functions similar to a Traffic Director. It recognizes the URL (from a load balancing point of view) and directs the traffic to the appropriate channel. Within SSL, and for each URL, Mandem purchased a digital signature with 128 bit encryption. A digital signature is a "stamp" placed on the data which is unique to the sender, and is very difficult to forge. In addition, the signature assures that any changes made to the data that has been signed cannot go undetected.

NOTE 1 Although traffic from Company A and B is "hitting" the Mandem internal network, it is NOT hitting the application servers says a business analyst. The traffic is http and only coming through port 443. The traffic "packets" are passed through the routers in the Mandem network to the appropriate web server which can handle the http request.

NOTE 2: "NATted" refers to Network Address Translation.

NOTE 3: Mandem uses the DMZ (Demilitarized Zone) to host its Internet services without sacrificing unauthorized access to its private network. The DMZ sits between the Internet and an internal network's line of defense. The DMZ contains devices accessible to Internet traffic, e.g., Web (HTTP) servers and FTP servers.

NOTE 4: A Proxy Server is a device which takes requests from one server and makes the request to another device and relays back the responses. A proxy server can also restrict access.

NOTE: Bolded text indicates a control identified by the Network Administrator