E-Commerce Infrastructure

The diagram below shows an example of an e-commerce infrastructure. It shows clients, customers, partners and suppliers to the left and how they may connect to an Internet company to the right through the Internet.

Clients and partners, using computers, telephones, etc., can connect to the Internet through dial-up lines to the ***public switched telephone network*** (PSTN). Through the PSTN ***Internet Service Providers*** (ISPs) can be reached. The ISPs can also be reached through dedicated lines, as well as switched dial-up and dedicated lines from LANs, routers, hubs and PBX and other switches on the Customer Premises, i.e. the premises of the clients, partners, etc.

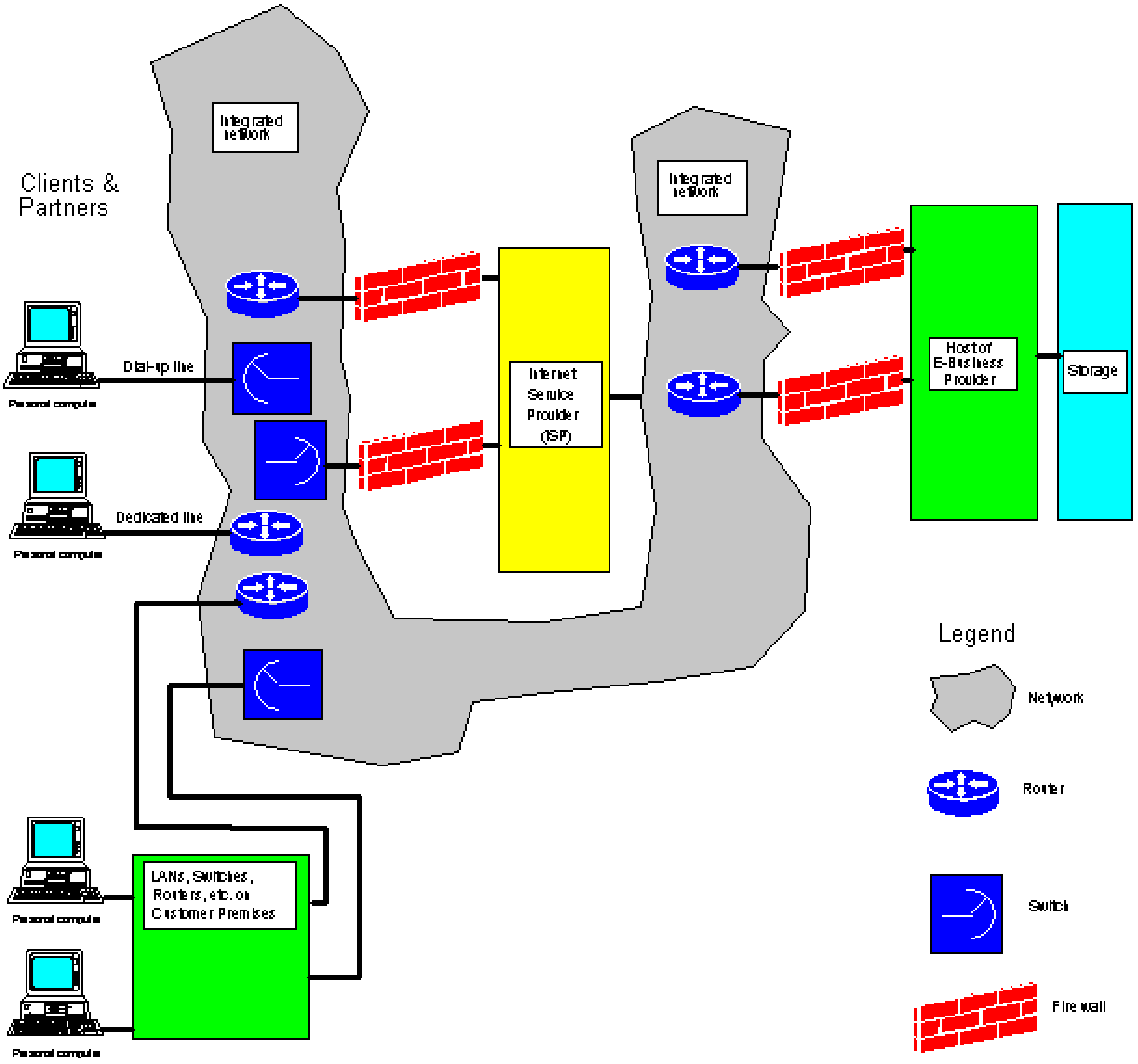
The PSTN is integrated with other networks, including packet switched public data networks (PSPDNs) that use routers and similar switching/directing devices.

On the other side of these networks you will find the host computers of the product/service provider or seller. These people may have co-located or outsourced storage facilities. The latter are data warehouses containing information on products, services, clients, partners, suppliers, billing, payments, etc.

Security is of a major concern. This includes concerns about the following, among many other security problems:

- Credit card numbers, expiration dates, and owner information getting in the wrong hands.
- Orders being accepted from the wrong clients.
- Payments being made to the wrong sources or goods and services being delivered to the wrong people.
- Viruses being allowed to pass through the system.

To prevent some of these security problems firewalls are installed at critical interfaces. The firewalls are supposed to filter the traffic, inhibit transmission of unwanted information (including viruses), and prevent malicious or criminal actions by outside persons. However, a firewall cannot by itself prevent misuse of credit card numbers or identity fraud.



Encryption is a way of improving security. You as a user can encrypt your messages in an end-to-end fashion and having your correspondent at the other end convert the message back into the original clear-text. Encryption can also be used on individual links in the transmission chain.

There has always been a competition between users and "authorities." Users want secure encryption end-to-end, and government (law enforcement) agencies want to be able to read your messages and in particular illegal ones. These agencies may be part of your own government or foreign governments. We all agree that the traffic of drug dealers, terrorists and similar persons should be controlled. Some countries make all encryption illegal, and others, like the U.S. Government, put restrictions on the complexity of the encryption permitted.

Severe problems in the conflict between users and government arise when the users are conducting businesses in the multimillion dollar range with governments. Examples of such users are manufacturers of telecommunications networks, airplanes, as well as construction companies, etc. You hear all of them talking about cases where their messages with their local agents regarding terms and prices end up in clear-text on the desks of their (government) customers even before their agents receive the messages. This may mean that the capabilities of government security agencies (like the U.S. National Security Agency) have been used to intercept and decrypt messages. Since national security agencies lost most of their "jobs" after the end of the cold war, some countries are considering using the security capabilities of these agencies to promote civil business.

The U.S. Government recently relaxed its restrictions on the export of advanced encryption technology. But, the capabilities of the U.S. National Security Agency is still ahead...