

Firewall Security

SECURITY ON-LINE SHOULDN'T BE ANY DIFFERENT
THAN A LOCKED FILE CABINET...

One of the chief goals of TOSHIBA's technology is to ensure that schools are able to maintain their established goals and practices, even in the face of using new Internet technology.

Schools have always had the ability to ensure that private information was viewed solely by members of the school administration. It was relatively easy to maintain the security of this information when it was recorded on paper files and kept on-site in administrative offices.

Going on-line should present no compromise to this type of security, and that is why the INTERNET SELECT includes an integrated firewall along with its other features, all of which ease the technology transition. The INTERNET SELECT's powerful firewall ensures that information on your internal network cannot be accessed from the outside—just like in the traditional model of paper file cabinets.

TOSHIBA's Internet Select provides built-in security against intrusion: a firewall integrated into our total solution for schools. This powerful system prohibits unwanted access into the protected network while still allowing users within your network to receive information from the Internet. Consider the illustration while you read

how the INTERNET SELECT implements security.

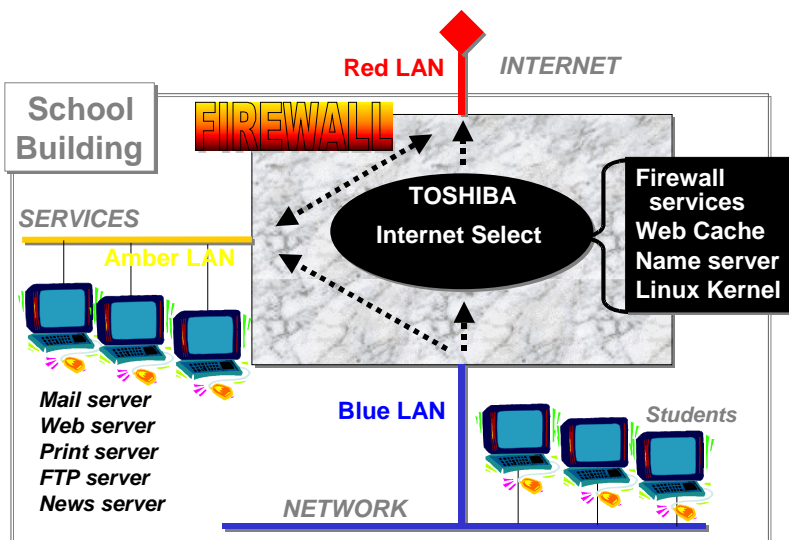
Basic Security

TOSHIBA has developed a unique approach to Internet security, designed to afford protection of your internal network and its sensitive information. This unique approach to firewalling is accomplished through a secure 'multiple LAN' configuration. Each LAN represents a distinct Ethernet interface. This inventive configuration ensures that school networks remain closed off from the outside world, while still allowing them to enjoy all of the Internet services they need. Using three distinct LAN segments, schools are also able to employ public email, Web service, FTP, or Usenet news servers—without compromising the security of their internal network.

The three LAN solution that maintains a school's security is as follows:

The **RED LAN** represents the connection to the Internet. There is no restriction on the information contained within this LAN.

The **BLUE LAN**—the network containing your most sensitive information—is protected behind the firewall. TCP/IP packets with originating Blue LAN addresses can receive email from the Amber LAN, and can request the TOSHIBA Internet Select to display Web pages on a browser. However, these requests *must* originate from a packet within the Blue LAN. This configuration thoroughly prohibits access to the internal network from anywhere beyond the firewall.



The **AMBER LAN** only allows requests to well-known services while blocking obscure ports to heighten security. It is open enough to pass information back and forth between the Internet and the Blue LAN. Services contained on the Amber LAN can include mail, Web, print, etc.

In this scenario, all information that passes through the INTERNET SELECT can only originate from requests within the Blue LAN. Thus security is maintained.

Other Avenues

In addition to communication out from the protected network, the TOSHIBA Internet Select allows communication between the Internet and the Amber LAN if using one of the approved services (email, FTP, etc.). The INTERNET SELECT will allow packets to pass from the Red LAN or the Blue LAN to the Amber LAN if the information request originates in the Blue LAN.

For example, if a computer on the internal network requests mail, the INTERNET SELECT sees that as a legitimate request because it originated from an address on the Blue LAN. Access is approved and information is exchanged.

No Spoofing Here

Spoofing is a technique whereby a deceptive request is sent from the Internet to a server. It fools the server into thinking that the request originated from an IP address on the internal network; the server thinks the request is legitimate, and carries out the request.

The INTERNET SELECT virtually eliminates the possibility of IP spoofing: if the incoming packet from the Red LAN contains an address from the internal network, the INTERNET SELECT drops the request. Thus, no request can appear as if it is coming from inside the firewall when it's really coming from the Internet.

Please Translate...

Routers relay packets of information through the giant web of computers that comprise the Internet. For security purposes, modern routers throughout the world will routinely block passage of packets that appear to be coming from any network behind a firewall. This is accomplished through the use of network address translation.

The three LAN approach that TOSHIBA has pioneered alters the originating IP address so that routers will pass requests from behind the firewall. This virtually eliminates the possibility of an illegitimate request being passed through Internet routers.

Other Security Features

- The INTERNET SELECT firewall automatically defragments all packets going through the firewall. This protects the computers behind the firewall from so-called 'IP fragment attacks.' It also prevents attacks that try to use overlapping fragments of TCP packets. This security feature stops attempts to get at the information within your protected network.
- IP packet filtering decides whether packets of information arriving at the INTERNET SELECT are allowed to pass, another firewall security feature. "Stateful, kernel-level, IP packet-level filtering" is employed in the INTERNET SELECT. It's a mouthful, but this sophisticated operation works on the concept of forwarding packets based on algorithms. These rules let packets pass through the INTERNET SELECT based on the source and destination IP address, source and destination port numbers, the protocol being transported, among other considerations.
- An application-level proxy is employed within the INTERNET SELECT. This feature is used to disrupt the connection between the Internet and the internal network—a basic firewall principle. Connections are made via a proxy process to a host, that will in turn establish a connection to the destination (if appropriate) and handle communications between the two connections. The advantage of using an application-level proxy is that it can intercept application protocols, such as FTP, HTTP, IRC, etc., and apply stronger authentication mechanisms to them without adversely affecting the operation of the network.

TOSHIBA is working continually to ensure that the latest

The Future

Internet Select continues to meet schools' needs in the area of network security. Stay tuned for more developments in this area...

TOSHIBA

BASCOM[®]
Internet Productivity For Schools