

section 2

SECURE SHARED INTERNET CONNECTIONS: THE FACTS

Connecting to the Internet

Connecting to the Internet is an essential activity for any business today. With the widespread adoption of e-mail, and new technologies such as “instant messages”, the Internet is key to maintaining close ties with customers. As a vast store of knowledge, including much company-specific information on products and plans, it is essential to keeping up with industry trends and competitive developments. By setting up a web site, a global presence and identity can be established.

A recent global report showed that at the end of 2000, 414 million people had Internet access and this figure was expected to rise to 1.17 billion by 2005*.



The Benefits of Shared Internet Access

Cost Effective

Shared Internet access is less expensive than providing all users with a separate modem, phone line and Internet account. It allows PCs and laptops simultaneously to network together and share a single Internet connection.

Improved Network Security

A shared connection is easier to protect; a full-featured built-in security firewall can protect the network from hackers and intruders.

Competitive Edge

With all network users having Internet access, they can benefit from shared information and access; informed, connected users can help the company gain a competitive edge.

* Source: eTForecasts, 2001

Online Connectivity Options

Internet connections are measured by the amount of data they transmit each second. The four most practical Internet connections for small offices and branch offices are analog, ISDN, DSL, and Cable.

Dial-up

If employees receive e-mail only occasionally from outside the office or browse the web infrequently, shared dial-up is sufficient. Employees use a telephone circuit to establish a web connection and hang up when they are done.

Analog connections are the most basic form of Internet connectivity. They are available wherever there is a telephone line. The highest speed that can be reached using an analog connection is 56 Kbps, which is fine for text and e-mail files, but slow for accessing graphic-intensive web sites or downloading large files.

ISDN (Integrated Services Digital Network) delivers up to 128 Kbps performance for faster Internet access and greater productivity. An ISDN-capable access router and an ISDN line, installed by a local phone company, will be required. ISDN lines when equipped with a suitable router can support both voice and data communications.

Broadband

A broadband connection to the Internet is a high-speed, “always-on” connection.

DSL (Digital Subscriber Line) provides high-speed Internet access at up to 8 Mbps (143 times faster than analog) over ordinary copper telephone lines. Though DSL uses an existing phone line wiring, it doesn't tie it up - the Internet can be accessed while using the same line for voice communications or faxing.

Cable is a shared high-speed connection which leverages the cable TV lines, and is available primarily in residential areas. Cable modems provide speeds up to 38 Mbps downstream, 10 Mbps upstream - though this will vary depending on the number of people in the area using the cable network. The fact that cable is ‘shared’ inherently makes it less secure.

Service	56K	ISDN	Cable	IDSL	SDSL	ADSL	G.SHDSL
Availability	Everywhere	Almost everywhere	Mostly residential areas	Metro areas and suburbs	Metro areas and suburbs	Metro areas and suburbs	Metro areas and suburbs
Choice of provider	Any ISP	Most ISPs	Local Cable operator	Select ISPs	Select ISPs	Select ISPs	Select ISPs
Downstream speed to computer	Up to 56 Kbps	Up to 128 Kbps	800 Kbps to 27 Mbps	Up to 144 Kbps	Up to 1.52 Mbps	32 Kbps to 8 Mbps	Up to 2.3 Mbps
Upstream speed to computer	33.6 Kbps	Up to 128 Kbps	33.5 Kbps to 5 Mbps	Up to 144 Kbps	Up to 1.52 Mbps	32 Kbps to 1.1 Mbps	Up to 2.3 Mbps

Security

A Gartner Group survey showed that 50% of small and medium businesses would be attacked by hackers through the Internet.*

Opening a network to the Internet or the public phone system poses a serious security risk. A network becomes accessible to not only legitimate users, but also to hackers.

To safeguard sensitive data, on a network, a firewall is strongly recommended. A firewall serves as a security guard, protecting the network from unauthorized entry. The device connects between a wide area network (WAN) and a network.



What do Firewalls Protect Against?

There are a number of different types of attacks that can be used by a hacker to gain access to a network or to cause damage. The two main types of attack are:

Denial of Service: A hacker will attempt to bring down the network (in part or entirely) by causing devices to crash or rendering them inoperable.

Intrusion: A hacker enters the network and tries to gain information (passwords or access to data). This might be done without the owner of the network knowing that anyone has gained unauthorized network access.

Virtual Private Networks (VPNs)

Relying on a public infrastructure for office-to-office communication can pose security risks to a business.

What are VPNs?

VPNs offer robust security by shielding network traffic between sites in encrypted “tunnels”, making public connections appear as private leased-lines to the rest of the world. VPNs are established automatically for every remote-access session and are transparent to users.

Why Use VPNs

The most common and cost-effective way for small offices to build DSL-powered WANs is over public networks, such as the Internet or the public telephone system. Relying on a public infrastructure for office-to-office communications, poses a threat to the business. Data is travelling unprotected over an open network where it is vulnerable to hackers and others. To safeguard proprietary sensitive or business-critical communications, deploy a VPN solution.

**Gartner Research Indicates Small and Midsize Enterprises Are Vulnerable to Internet Attacks, October 10, 2000*

Gateways

A gateway is a device that interconnects networks, as in tying a private network to a public network. Today, gateways are used in small or medium-sized businesses to allow an Internet (public network) connection to be shared by multiple devices on a local (private) network. Some vendors call these devices gateway routers, because they use router functionality to bring the networks together.

Gateways generally do not provide the actual physical connection between the networks; this is done by a separate modem device often provided by the Internet Service Provider. There are many different kinds of gateways available - wired or wireless, and with varying degrees of security offered in the way of firewalls and/or Virtual Private Networking.

Access Routers

Most access routers are actually three components in one box.

Integrated Modem and WAN
Whether connecting using analog or ISDN, an integrated modem and WAN port will allow the user to connect to the internet via a telephone line or cable line.

Router
The router distributes traffic to its appropriate destination either elsewhere on a network or to the Internet.

Network Hub
The hub acts as a junction box to connect all the computers on a network.



Firewalls

What is a Firewall?

A firewall is a security system that stands between the company's network and the outside world. A firewall screens all inbound and outbound traffic according to a set of rules that is defined. Generally speaking, a firewall involves dedicated equipment or software to maintain an electronic boundary.

Hardware firewalls, or gateway products that include security are usually easy to use and maintain. These devices are suitable for small businesses with little or no in-house technical networking expertise.

Selecting a Firewall

Firewalls and security are available in different forms; hardware or software, or incorporated into another device like a router.

Routers with security (often as an upgrade) can provide a good level of security. However, the solution is generally more expensive than other options, and the performance of the router can be significantly reduced as it is not optimized to carry out a firewall function.

Dedicated software security is usually a complex application which is best suited to businesses which have a UNIX or NT/2000 Servers, and the technical expertise required to configure and maintain a complex dedicated security software.

Whatever option chosen, always check to see if the firewall performs Stateful Packet Inspection (SPI) as this ensures a high level of firewall protection.



Real Estate Company Accesses Information Through Shared Internet Access



The Challenge

A local real estate company recently joined a large real estate franchise to leverage the franchise's vast marketing and information resources. To access these resources the local real estate company needed to connect to the Internet simply and securely. Furthermore, the company had several employees who wished to work from another sales office from time to time. They also required access to the Internet but needed the flexibility to access the Internet from any point in the office.

The Solution

The company's five employees were already connected to each other via an existing Ethernet network based on the OfficeConnect Dual Speed Switch 8 Plus. The company installed an OfficeConnect Cable/DSL Secure Gateway allowing employees to share the broadband Internet connection securely and cost effectively. The OfficeConnect Wireless Cable/DSL Gateway gave shared Internet access for employees who worked from the additional sales office and also the freedom to access the Internet from anywhere in the office.

The Benefits

- Cost effective, secure shared Internet access
- Access to information and resources 24/7
- Increased employee productivity

Shopping List

- 3Com OfficeConnect Dual Speed Switch 8 Plus
- 3Com OfficeConnect Cable/DSL Secure Gateway
- 3Com OfficeConnect Wireless Cable/DSL Gateway

For ordering information, see chapter 5 of this guide

