Intranets

An intranet is a portion of the Internet that is separately administered and has a boundary that can be configured to enforce local security policies. It is typically composed of *several local area networks (LANs) linked by backbone connections. Computers within an intranet may be spatially separated by any distance. They may be on different continents, in the same building, or in the same room. The network configuration of a particular intranet is the responsibility of the organization that administers it and may vary widely – ranging from one LAN on a single site to a connected set of LANs belonging to branches of a company or other organization in different countries.*

An intranet is connected to the Internet via a router, which allows the users inside the intranet to make use of services elsewhere such as the Web or e-mail. It also allows the users in other intranets to access the services it provides. However, many organizations need to protect their own services from unauthorized use by possibly malicious users elsewhere. For example, a company will not want secure information to be accessible to users in competing organizations, and a hospital will not want sensitive patient data to be revealed. Companies also want to protect themselves from harmful programs such as viruses entering and attacking the computers in the intranet and possibly destroying valuable data. The role of a firewall is to protect an intranet by preventing unauthorized data traffic leaving or entering. A firewall is implemented by filtering incoming and outgoing data traffic, for example according to its source or destination. A firewall might for example allow only traffic relating to e-mail and Web access to pass into or out of the intranet that it protects.

Some organizations do not wish to connect their internal networks to the Internet at all. For example, police and other security and law enforcement agencies are likely to have at least some internal networks that are isolated from the outside world, and the UK National Health Service has chosen to take the view that sensitive patient-related medical data can only be adequately protected by maintaining a physically separate internal network. Some military organizations disconnect their internal networks from the Internet at times of war. But even those organizations will wish to benefit from the huge range of application and system software that employs Internet communication protocols. The solution that is usually adopted by such organizations is to operate an intranet as just described, but without the connections to the Internet. Such an intranet can dispense with the firewall; or, to put it another way, it has the most effective firewall possible – the absence of any physical connections to the Internet.

Questions

1 What are typical components of an intranet?

several local area networks (LANs) linked by backbone connections

2 What is the maximum physical distance between computers in an intranet?

There is no maximum distance- they can be on different continents, in the same building or in the same room

3 What device allows intranet users to make use of services outside their intranet?

A router

4 Who, especially, will companies want to stop from accessing sensitive data?

Competing organisations or anyone wishing to gain unauthorised access.

5 Why are hospitals especially careful about network security?

Their patient data is especially sensitive

6 What criteria might a firewall use to filter messages going into or out of an intranet?

Incoming and outgoing data based on source or destination

7 According to the text, what is the most effective firewall possible?

No connection to the internet – no external danger present

8 What type of organisation might want to make use of this “firewall”?

Military, law enforcements organisations like the police, hospitals – any organisation with very sensitive data.

9 Why do they nevertheless want to use an intranet?

They want and need to share data to run their business efficiently.

Sentence structure

Construct suitable completions for these sentences using information contained in the text. Your completions must contain at least one verb.

With this task many answers are possible. The most important thing is the grammar here. My answers are only suggestions.

1 Although globally operating companies have facilities located on different continents, they can share data using their intranet

2 If the users linked in an intranet are to be able to access services located outside it, they must be connected via a router

3 Because attacks by hackers and the transmission of viruses are serious dangers, it is essential to have an effective firewall.

4 A firewall is a type of filter that filters data based on source and destination and protects the system from unwanted access by malicious users or competitors.

5 Because the National Health Service in Britain has very sensitive medical dta about patients, they chose not to connect certain systems to the internet at all.

6 Intranets with no connection to the Internet can do without a firewall because there is no external danger.

Discussion task - Large modern companies make use of both intranets and extranets. To access the data in these networks, they use search engines, in the same way as search engines are used to access data in the Internet. Work in small groups (max 5 people) and produce a short presentation on intranets for colleagues who are not especially knowledgeable about IT. One person will be chosen to present your ideas to the class next week. Your presentation should last 5-7 minutes. Be prepared to answer questions from the audience! You could consider the following points **in English**:

Please see separate suggested sample answers