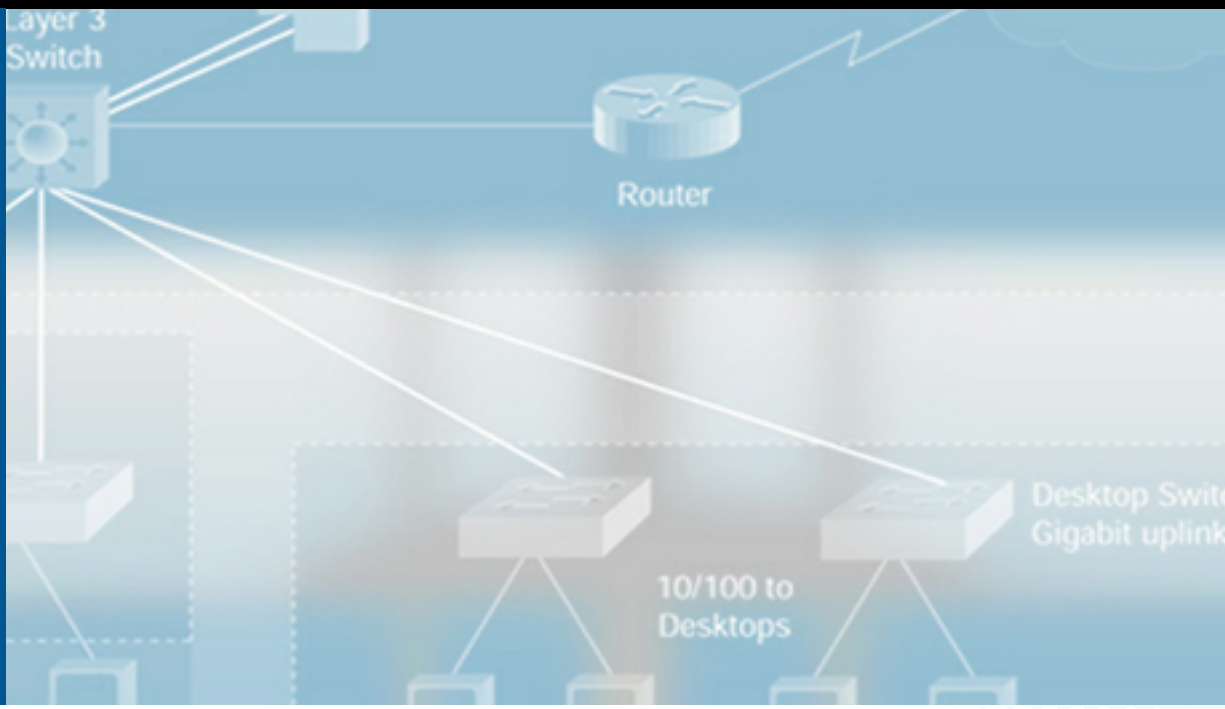
Cisco Systems

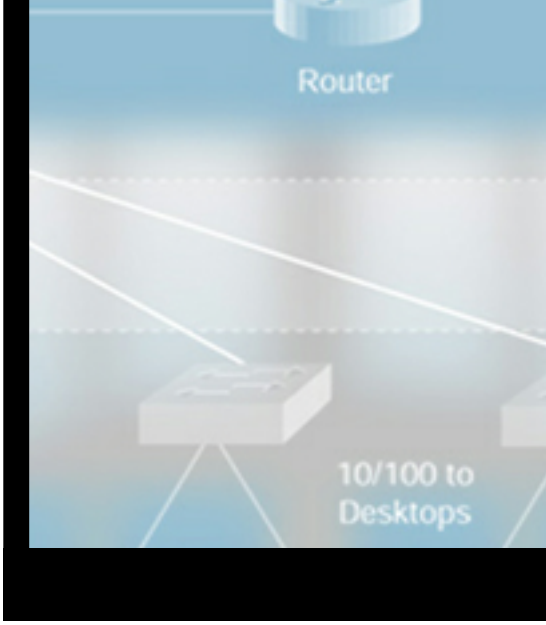
E-Seminar



Network Security

Internet Technical Solution

Seminar



Network Security

Internet Technical Solution

Seminar

Welcome

Welcome to the Technology E-seminar on Network Security.

With the growth of the Internet and business applications such as e-commerce, computer networks are increasingly vulnerable to a wide range of security threats. The business impact of security breaches can be catastrophic.

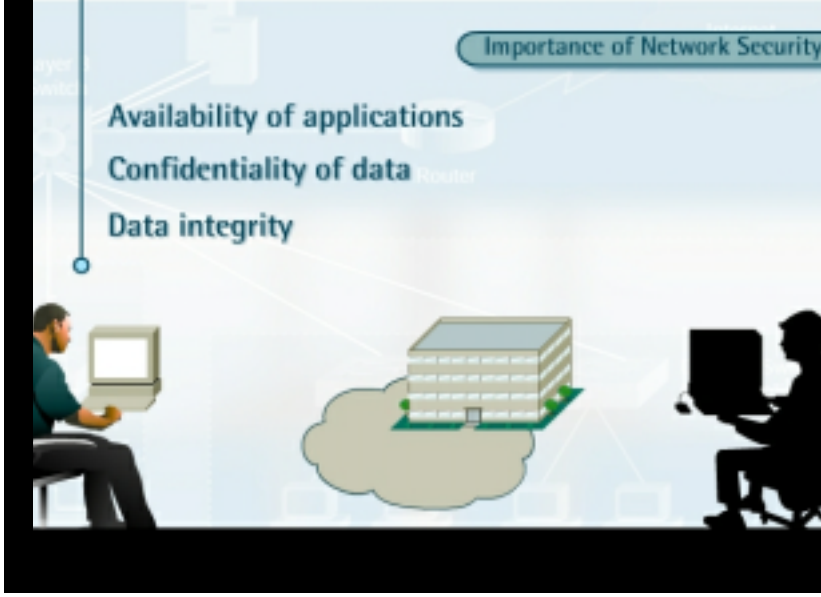
To combat these threats and to ensure that e-business transactions are not compromised, security technology plays a key role in today's networks.

Objectives

In this seminar, we will discuss the technical aspects of Network Security.

BY the end of the seminar we hope you will have a good understanding of the different network security hazards and the technologies that exist to protect your company networks.

We will also address how to implement network security technologies in your company



Importance of Network security

Internet Business Solutions require mission-critical networks such as E-Commerce, Supply Chain Management and Web Marketing enable companies to improve their efficiencies, reduce costs and increase revenues. Such applications that accommodate voice, video and data traffic.

These networks need to be scalable to support increasing numbers of users and the need for greater capacity and performance.

However, as more applications are enabled and become accessible to increasing numbers of users, networks become ever more vulnerable to security threats a wider range of.

Network attacks compromise availability of applications. Furthermore, confidentiality of company data may be compromised by unauthorised external access. Or data integrity of documents compromised could be by, for instance, hackers modifying the content or databases.

Elements

Network security AIMS to protect networks and their applications against such attacks. To achieve this, companies * approach network security by creating a security policy and designing a network security architecture. based on this policy,

This architecture should take the following elements of network security into account.

First, you should know the identity of who's on the network and what access they are allowed to have.

Secondly, controlled access to critical network applications, data and services should be so, that only legitimate users and information can pass through the network. This is often referred to as perimeter security.

Data privacy or secure network connectivity can be achieved by implementing Virtual Private Networks or VPNs, which allow companies to extend their secure company network to remote offices, teleworkers or extranet partners. Encryption technologies ensure that data travelling across a VPN cannot be intercepted or read by unauthorised recipients.

Security monitoring tools allow you to monitor, recognize and test vulnerabilities in your network infrastructure, so you can address them before intruders exploit them.

Finally, as networks grow in size and complexity, it will be necessary to use Security Policy Management tools, that can centrally administer the security elements we HAVE JUST mentioned.

AAA

Let's now focus on some of these security elements.

Identity methods and technologies allow to accurately and positively identify network users. They ensure that authorised users gain access to the company computing resources they need, while unauthorised users are denied access.

The framework used to control access to a computer network is commonly known as A-A-A, also known as "triple-A", which stands for Authentication, Authorisation and Accounting.

Authentication refers to the method of identifying users, through steps such as a login and password dialog. It basically verifies "who you are".

Authorisation is checking and controlling what a user is permitted to do within the network. This permission could range from a one-time authorization to a specific level of authorization for each network service.

And accounting enables you to track the services users are accessing, as well as the amount of network resources they are consuming. Accounting assists in the monitoring of security, and checks "what you did" within the network.

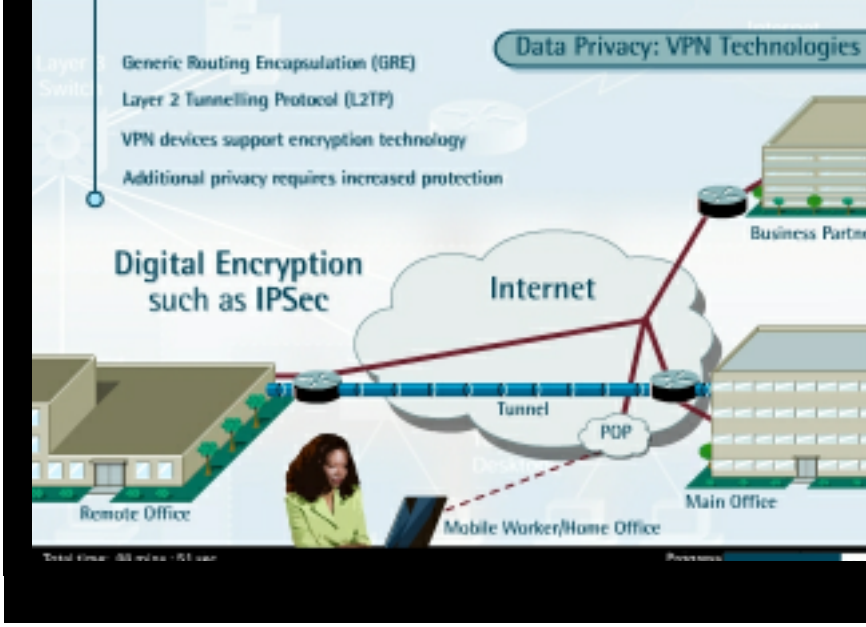
Triple-A usually relies on protocols such as RADIUS, TACACS+ [read: "tacacs-plus"], and Kerberos, to administer its security functions

Perimeter Security

Only legitimate users and information is allowed to pass through the network. This is achieved through Perimeter Security solutions, such as access control lists and firewalls.

Before a user gains access to a network, network components, such as routers or access servers, decide whether network traffic, coming from that user's computer or network, is forwarded or blocked. This decision is based on Access Control Lists, or shorter, Access Lists.

A Firewall is a specific hardware or software solution which restricts access to specific network resources, and permits only authorised traffic to pass. A Firewall can also protect against Denial of Service Attacks. These attacks do not provide intruders with access to specific data, but they tie up the computing resources by sending them large amounts of data, and as such prevent legitimate users from accessing applications.



Data Privacy

Company information must be protected from eavesdroppers, so the ability to provide authenticated, confidential communication on demand is crucial.

Virtual Private Network technology provides such private connections, by separating data into “tunnels”. In this way, a private network can be created over public networks such as the Internet, using protocols such as Generic Routing Encapsulation, or GRE, or the Layer 2 Tunnelling Protocol, or short: L2TP.

In order to provide the protection for the data they transport, hardware and software VPN devices support encryption technology. All traffic travelling through a tunnel between two points in a VPN is encrypted.

Sometimes, data separation using tunnelling technologies provides effective data privacy, for instance within a local company network. Often, however, additional privacy requires increased protection, for instance through the use of digital encryption technology and protocols such as IPSec.

Network Security Seminar

IPSec

IPSec, or the IP Security protocol, is a framework of open standards for ensuring secure private communications over the Internet. IPSec ensures confidentiality, integrity and authenticity of data communications across a public network. It is a key technology component for providing a total security solution.

This protocol can address security threats in the network infrastructure itself, without requiring expensive host and application modifications. IPSec provides encryption and authentication at the IP network layer. Because the encrypted packets look like ordinary IP packets, they can be routed easily over an IP network, such as the Internet, just like ordinary IP packets. The only devices that know about the encryption are the end points.

IPSec itself makes use of different technologies, such as DES encryption and Digital Certificates.

Encryption and Decryption

Encryption technology ensures that messages cannot be intercepted or read by anyone other than the authorised recipient.

Encryption is usually deployed to protect data that is transported over a public network, and uses advanced mathematical algorithms to “scramble” messages and their attachments.

Several types of encryption algorithms exist, but some are more secure than others. In most algorithms, the original data is encrypted using a certain encryption key, and the receiving computer or user can only decrypt the message using a specific decryption key. Encryption algorithms, such as DES, PGP or SSL, determine how these keys are constructed and exchanged.

A Network Security Architecture should be based on a Company Security Policy

A network Security Solution should include:

Authentication and Authorisation

Data Privacy

Perimeter Security

Conclusions

So let's summarise the most important aspects of Network Security.

As different levels of Internet connectivity become essential for companies to remain competitive, securing the network infrastructure becomes a key requirement.

Companies should design a network security architecture, based on a company security policy.

Instead of focusing only on one particular type of security, it is important to realise that such a complete network security solution is necessary for a company to fully protect its data and computing assets. This solution should include authentication and authorisation, data privacy and perimeter security.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www.cisco.com
Tel: +33 1 58 04 60 00
Fax: +33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Copyright © 2001, Cisco Systems, Inc. All rights reserved.
Cisco Systems and the Cisco Systems Logo are registered trademarks, and Empowering the Internet Generation is a service mark, of Cisco Systems, Inc. and its affiliates in certain other countries.