

Betrouwbaar- beschikbaarheid van uw data



Volgens het CIA-model

Inventariseer volgende onderwerpen:

Autorisatie / Toegangsrechten

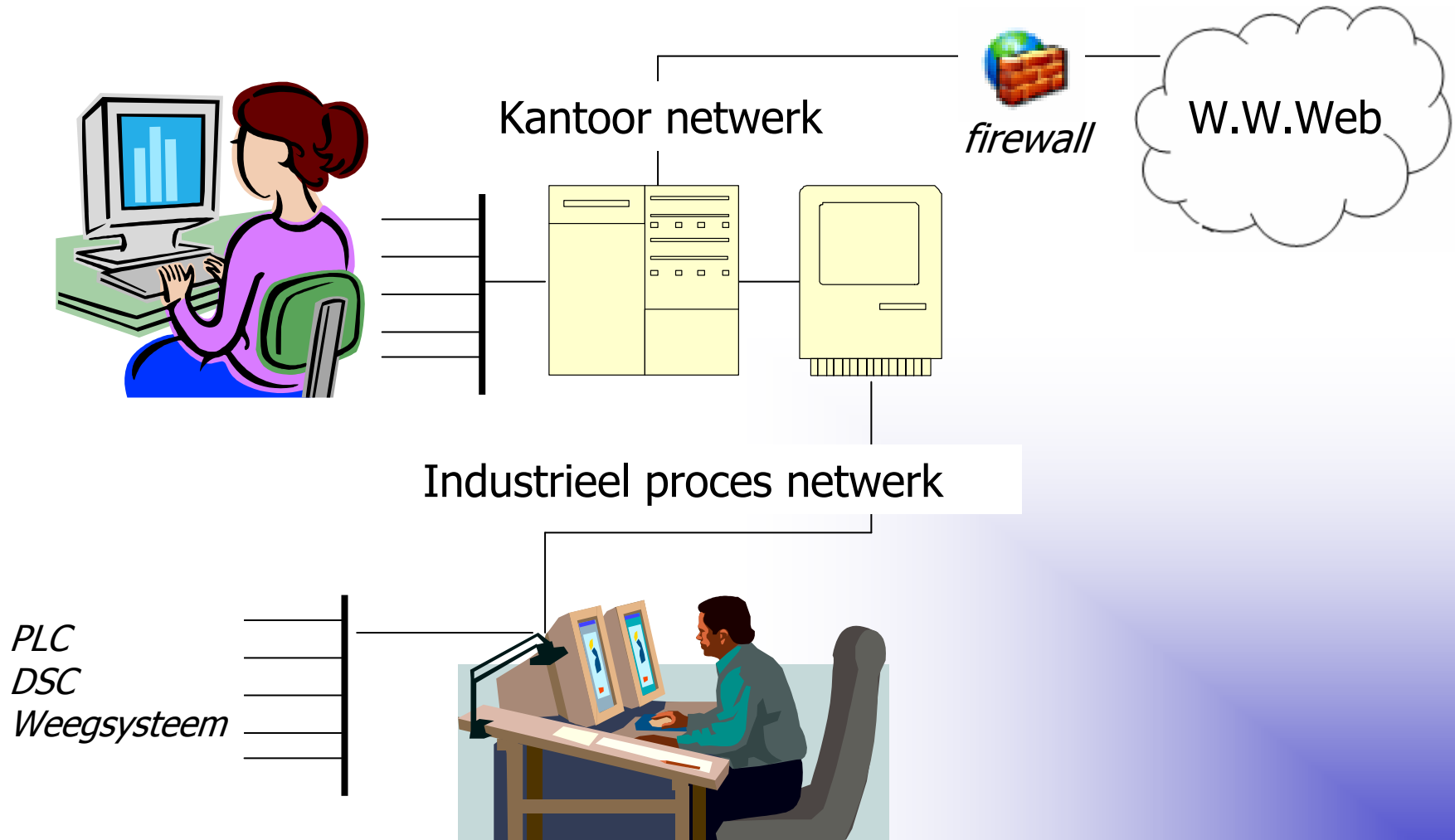
mag je bij de informatie?

Beschikbaarheid

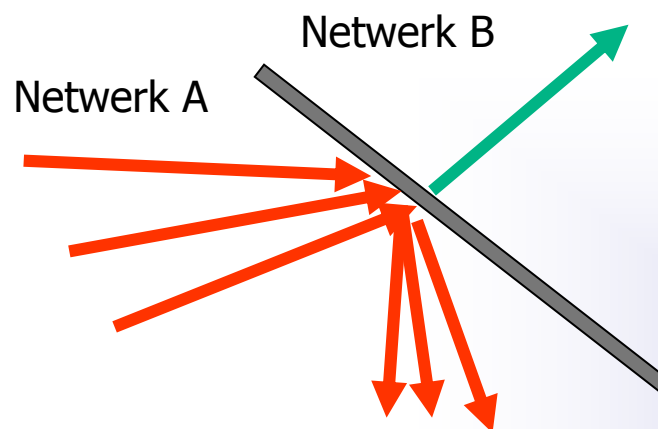
Is de informatie beschikbaar?

Controle

Is de informatie betrouwbaar?

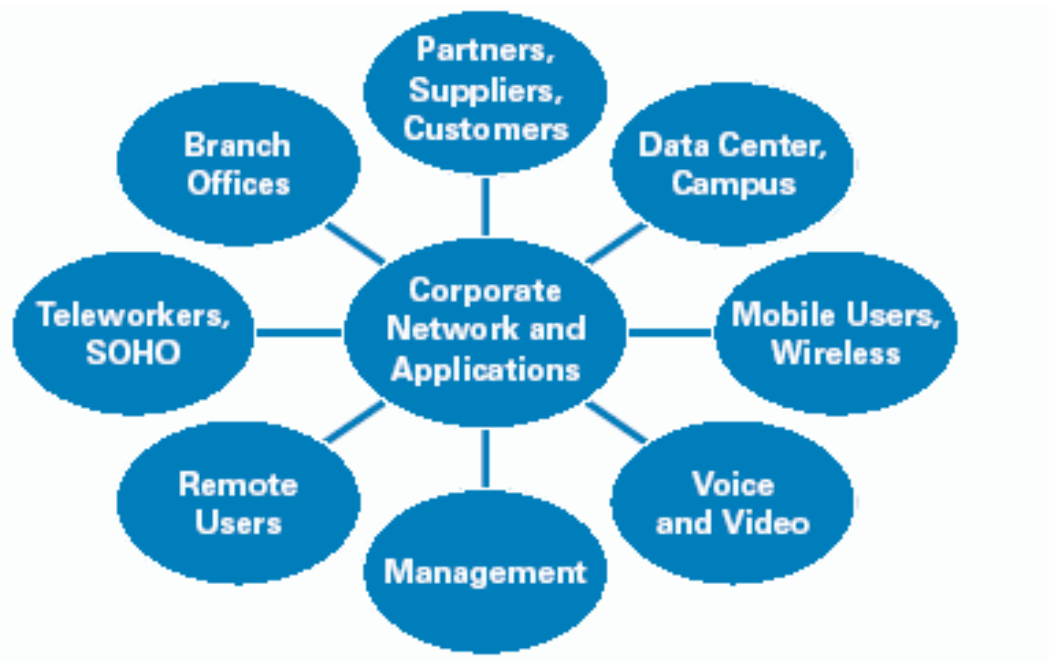


Firewall routers toegepast als filter, toezicht op welke protocollen het netwerk betreden of verlaten!



Multi-platform, multi layer security protocol

Ik heb toch maar 1 netwerk?



Multi-platform, multi layer security protocol

Eén systeem voor communicatie tussen verschillende computer systemen opgebouwd uit:

Hubs: laagste verbindingspunt, verbind alles aan alles.

Switch: verbindingspunt met simpelste netwerk management opties, verbind alleen aan elkaar “geadresseerde” apparatuur met elkaar. Werkt als data filter.

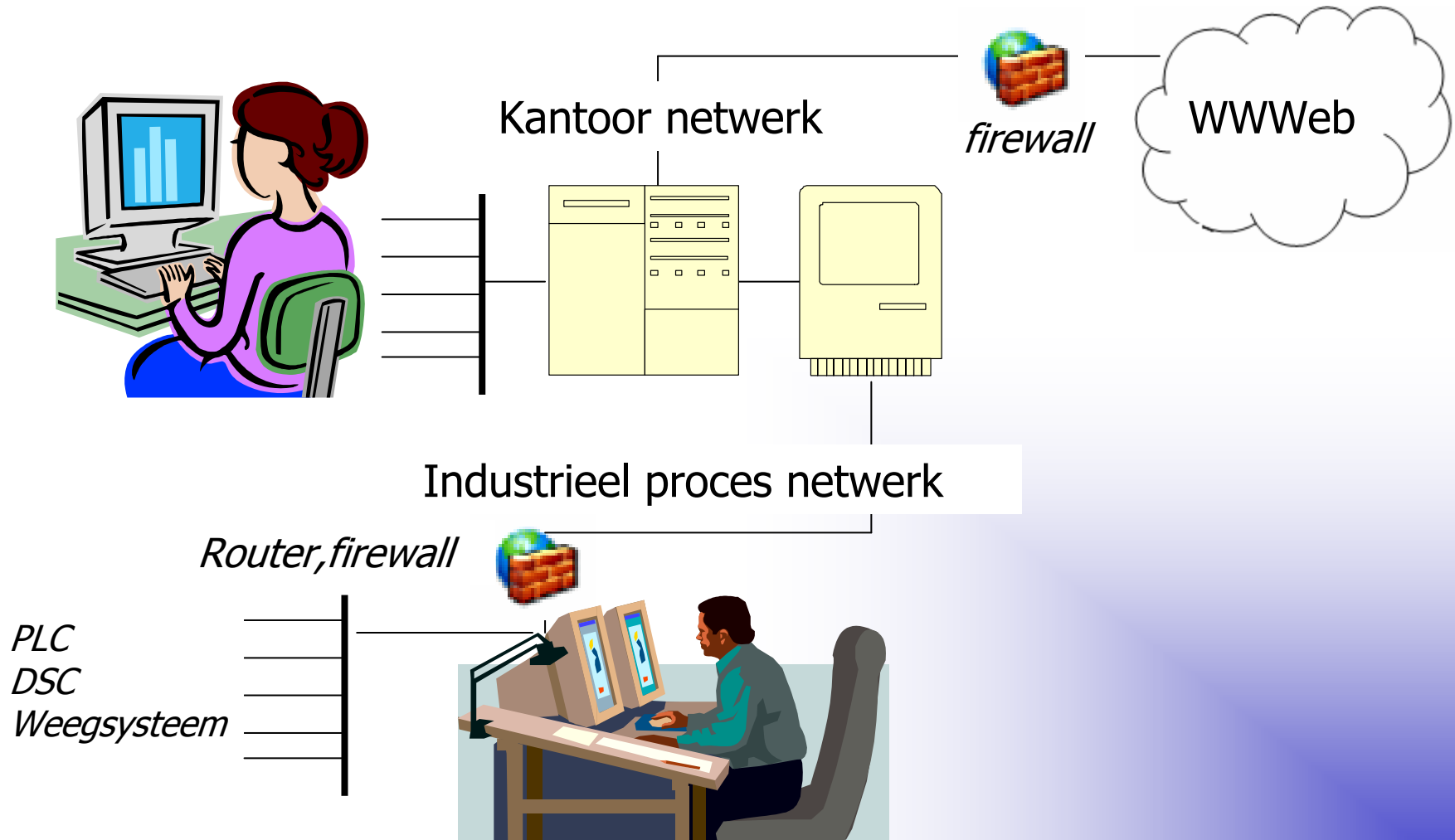
Bridge: (netwerk)switch toegepast om netwerk segmenten (gefilterd) te koppelen.

Router: een computer dienende als verbindingspunt om netwerken te koppelen, met aanvullende functie mogelijkheden als bv. gateway, firewall, NAT (IP adres scheiding)

Eén systeem voor communicatie tussen verschillende computer systemen opgebouwd uit:

Vlan: Local Area Netwerk opgesplitst in 2 of meer “conflicterende” domeinen (kantoor, proces), waardoor virtuele netwerken ontstaan.

Vlan is software op daarvoor bestemde hardware als routers of switches. Vaak krijgt elk virtueel netwerk een eigen server. Door Vlan toepassing lijkt het of de apparatuur welke zich op het Vlan netwerk bevinden d.m.v. 1 netwerkkabel i.p.v. het gehele netwerk verbonden zijn, waardoor Server en cliënts verspreid over het gehele netwerk kunnen zijn.



Verschillen zitten hoofdzakelijk in de hardware:

- Robuustheid (Mechanisch)
- Trilling gevoeligheid
- (Stof/vocht/ chemische)dichtheid (IP)
- Omgevingstemperatuur (>25 graden C)
- Storingsgevoeligheid (EMC)

- (Redundante) Ringbekabeling i.p.v. stervormige “vaste” bekabeling.

We kunnen nog veel leren van onze kantoor netwerken!

Industrie sector moet volgende nog leren toepassen:

- Firewalls
- Routers
- Anti-virus toepassingen
- VPN protocollen
- VLAN mogelijkheden

Wensen:

We willen gegarandeerd, gecontroleerd communiceren met een bekende, bevestigde bestemming zonder dat externe hier toegang toe krijgen.

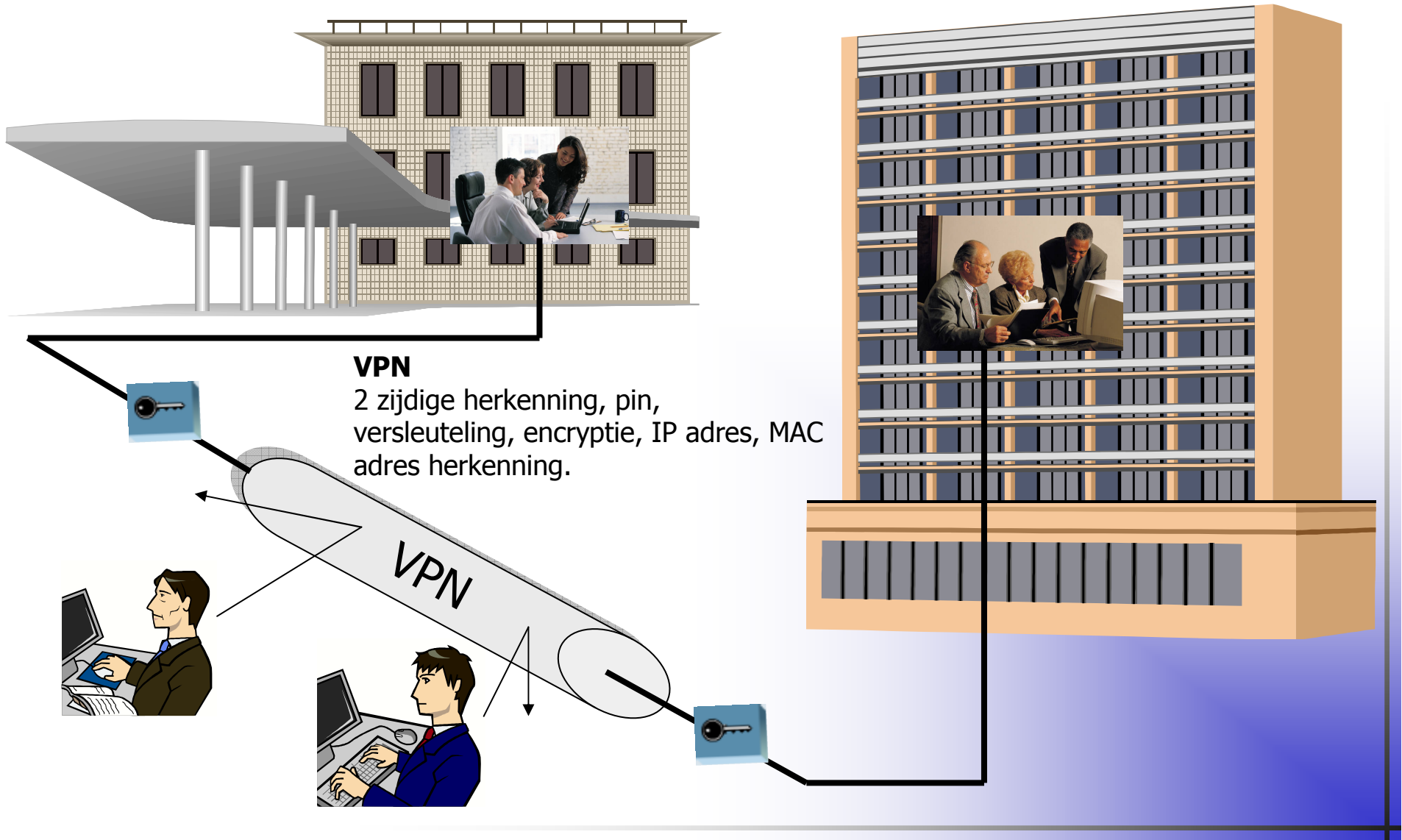
VPN (Virtual Private Network)-verbinding:

Een veilige “tunnel” verbinding (over publieke verbinding als bv het internet) welke computers verbind (veilige bestand deling) zonder het gevaar van ongeautoriseerde interruptie.

Door middel van firewall technologieën kunnen bepaalde communicatie poorten worden geopend voor geautoriseerde gebruikers (vaak enkel van bekende systemen). Ongeautoriseerde “zien” de geautoriseerde systemen niet en krijgen geen verbinding!

Toegepast beveiligingsmethoden:

- Gebruiker herkenning (encryptie)
- IPsec (IP beveiliging)
- PPTP (point-to-point tunneling protocol)

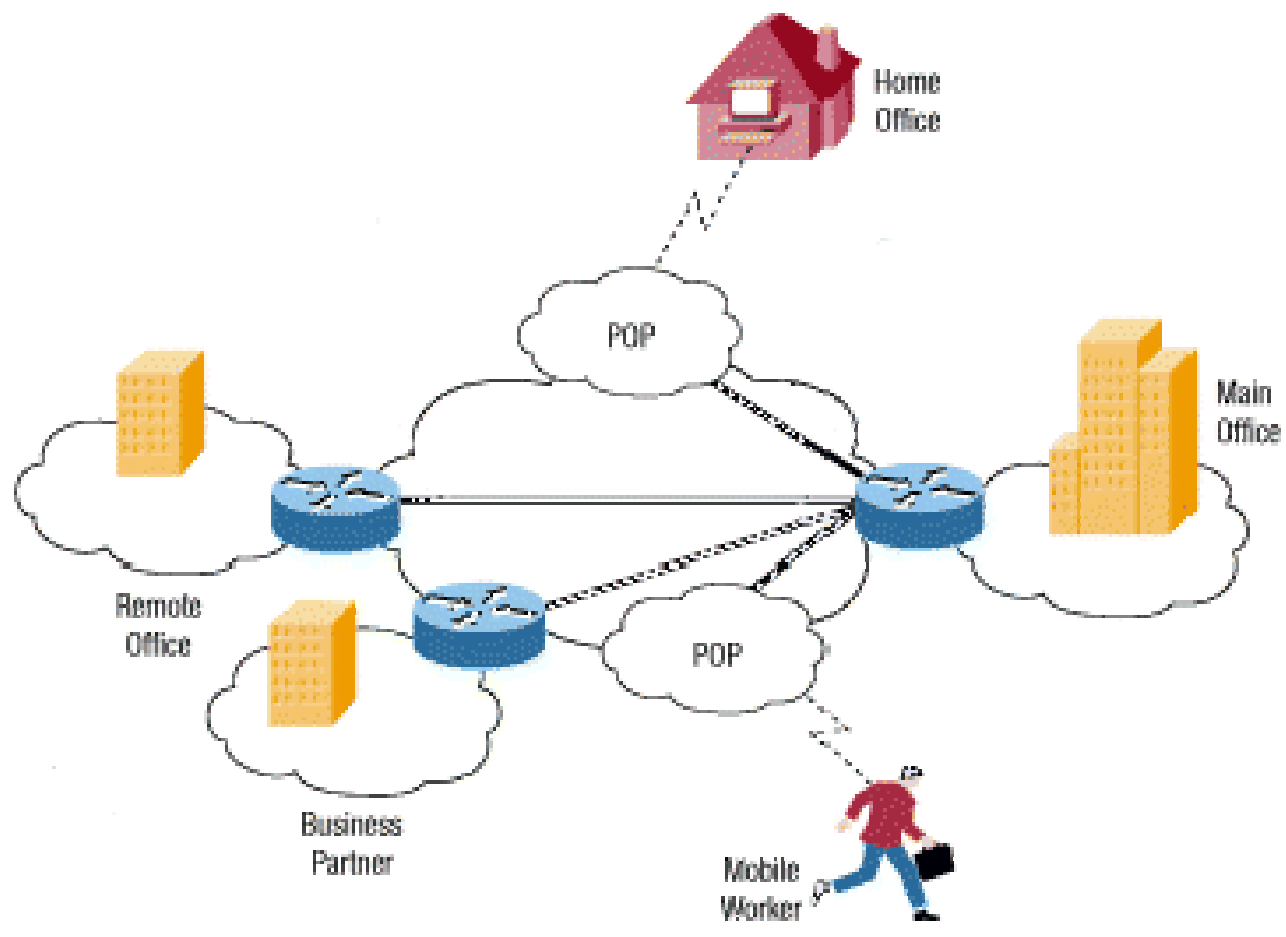


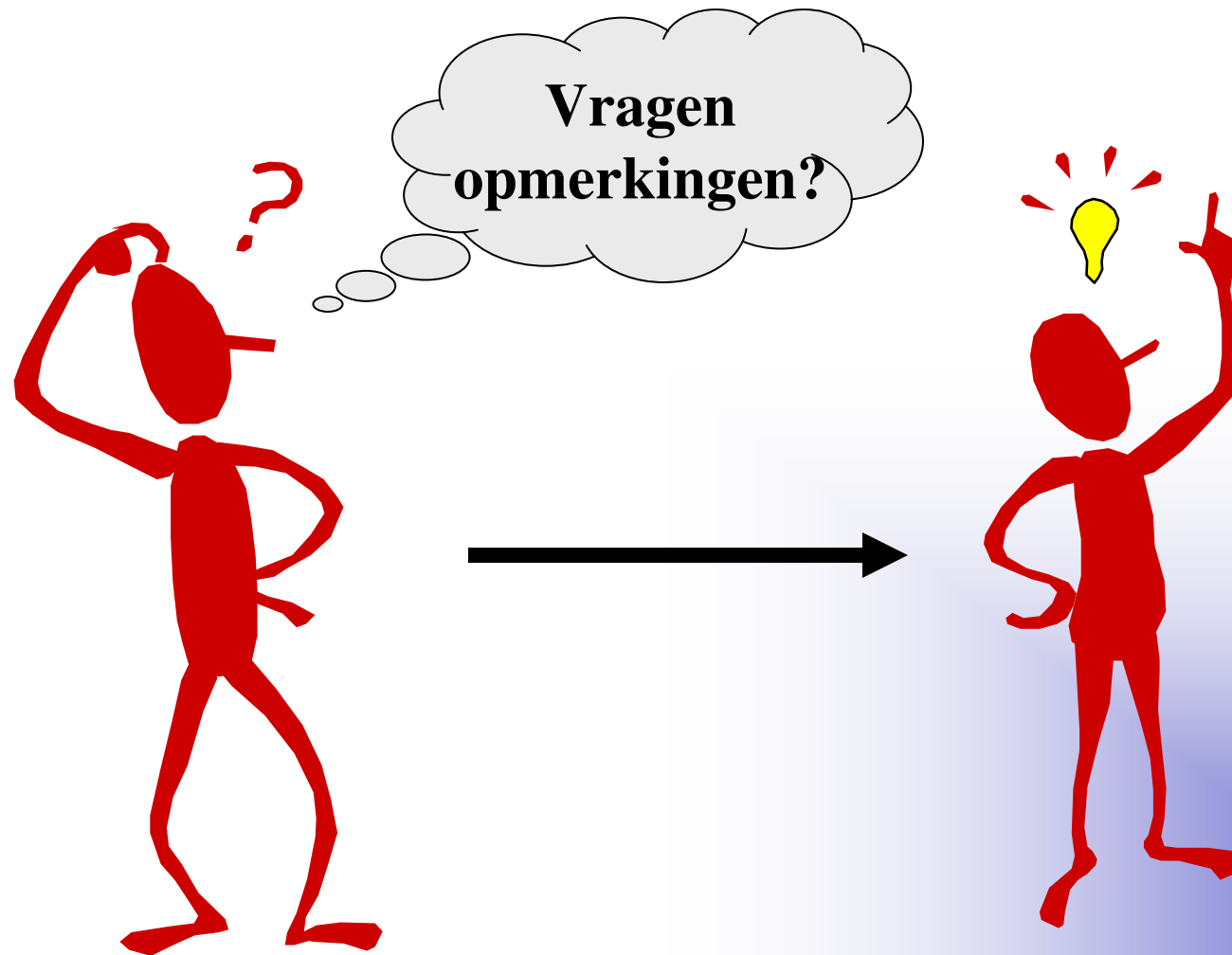
VPN (Virtual Private Network)-verbinding:

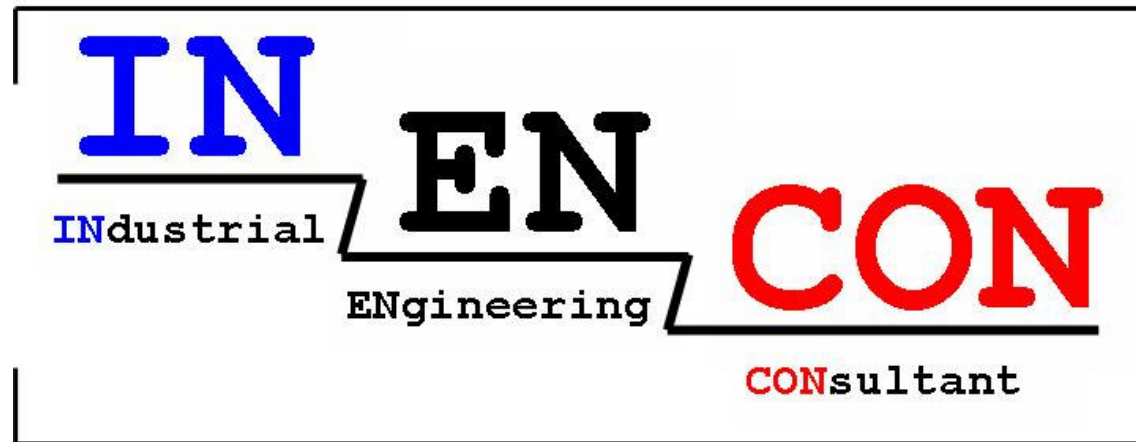
Een VPN kan onder meer gebruikt worden om een beveiligde connectie te creëren tussen de werkplek en server, tussen twee firewalls of tussen werkplek en firewall.

De meest voorkomende VPN's zijn die van bedrijven met meerdere vestigingen op verschillende lokaties. De netwerken worden middels de tunnels over het internet gekoppeld zodat de eerst losstaande netwerken, een groot netwerk vormen. Daarnaast is het de ideale oplossing voor Telwerk-/remote user koppeling met een intern bedrijfsnetwerk zonder dat er ingebeld hoeft te worden

VPN-verbinding mogelijkheden







Adres: Annie Romeinstraat 51, Venray

Tel: 0478 – 69 07 73

Fax: 0478 – 69 21 35

Email: ton.ariaans@inencon.com

Website: [http: // www.inencon.com](http://www.inencon.com)

adware Software installed with some shareware or freeware, that displays web-based advertisement usually via a pop-up window, on a user's computer.

AP (application programming interface). A standardized interface whereby an application program can use services provided by the operating system or subsystems.

applet Specifically, Java programs. An HTML-based program that uses a web browser to provide a user interface.

attack vector The route or means used by a hacker to carry out an attack.

Use present virus remove tool (download from internet by McAfee)

- Clean** To remove a virus or other malicious software from a computer, file or disk.
- Cold Boot** To start the computer by cycling the power. A cold boot using a rescue disk (a clean floppy disk with boot instructions and virus scanning capabilities) is often necessary to clean or remove boot sector infectors.
- FDISK /MBR** If you have MS-DOS version 5.0 or later, the command FDISK /MBR can remove viruses which infect the master boot sector but do not encrypt it. Using this command can produce unexpected results and cause unrecoverable damage.

backdoor

A backdoor is a secret or undocumented method of accessing a computer. It can also be the software that uses such a means to penetrate a system. Some software has a backdoor placed by the programmer to allow them to gain access to troubleshoot or change the program. Software that is classified as a "backdoor" is designed to exploit a vulnerability in a system, and open it to future access by an attacker.

port

A communications channel on a computer identified by a number known as a Port Number. Hackers often use an open port to gain unauthorized access to a computer.

exploits

An exploit is a way of breaking into a system. An exploit takes advantage of a weakness in a system in order to hack it. Exploits are the root of the hacker culture. Hackers gain fame by discovering an exploit. Others gain fame by writing scripts for it. Most exploits can be classified into categories including buffer overflow, directory climbing and Denial of Service.

key logger

(Keystroke Logger) A program that runs in the background, recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker. The attacker then peruses them carefully in the hopes of either finding passwords, or possibly other useful information that could be used to compromise the system or be used in a social engineering attack.

cookie

A small file containing data about a visitor to a website. It's main purpose is to identify users when they return to that website. Cookies might contain login or registration information, "shopping cart" information or user preferences.

worm

Classified as a type of virus. A self-replicating program that propagates by attacking other machines and copying itself to them. It can be destructive or harmless, depending on its payload. A worm may replace files but does not insert itself (as happens with a virus).

Worms are parasitic computer programs that replicate, but unlike viruses, do not infect other computer program files. Worms can create copies on the same computer, or can send the copies to other computers via a network. Worms often spread via IRC (Internet Relay Chat).

**network
worm**

A program or command file that uses a computer network as a means for adversely affecting a system's integrity, reliability or availability. A network worm may attack from one system to another by establishing a network connection. It is usually a self-contained program that does not need to attach itself to a host file to infiltrate network after network.

virus

A computer program file capable of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission. Some viruses attach to files so when the infected file executes, the virus also executes. Other viruses sit in a computer's memory and infect files as the computer opens, modifies or creates the files. Some viruses display symptoms, and some viruses damage files and computer systems, but neither symptoms nor damage is essential in the definition of a virus; a non-damaging virus is still a virus.

There are computer viruses written for several operating systems including DOS, Windows, Amiga, Macintosh, Atari, and UNIX, and others.

**macro
virus**

A virus containing a malevolent macro. Depending upon the way the virus is delivered it may sometimes be known as a Trojan, or a Worm.

Multipartite viruses use a combination of techniques including infecting documents, executables and boot sectors to infect computers. Most multipartite viruses first become resident in memory and then infect the boot sector of the hard drive. Once in memory, multipartite viruses may infect the entire system. Removing multipartite viruses requires cleaning both the boot sectors and any infected files. Before you attempt the repair, you must have a clean, write-protected Rescue Disk.

**spy
ware**

Software installed with some shareware or freeware that collects and transmits information about users browsing habits to a third party and usually without their knowledge or consent.

Trojan

[horse] Either, (a) any program designed to do things that the user of the program did not intend to do or that disguises its harmful intent or (b) a program that installs itself while the user is making an authorized entry; which is used to break-in and exploit a system. Unlike viruses and worms, Trojans do not replicate.

A Trojan horse program is a malicious program that pretends to be a benign application; a Trojan horse program purposefully does something the user does not expect. Trojan horse programs can be destructive.

Many people use the term to refer only to non-replicating malicious programs, thus making a distinction between Trojans and viruses.

Trojan

Trojan horses can do anything that the user executing the program has the privileges to do. This includes:

- * deleting files that the user can delete
- * transmitting to the intruder any files that the user can read
- * changing any files the user can modify
- * installing other programs with the privileges of the user, such as programs that provide unauthorized network access
- * executing privilege-elevation attacks, that is the Trojan horse can attempt to exploit a vulnerability to increase the level of access beyond that of the user running the Trojan horse. If this is successful, the Trojan horse can operate with the increased privileges.
- * installing viruses
- * installing other Trojan horses

RAT (remote administration tool) A Trojan that when run, provides an attacker with the capability of remotely controlling a machine via a "client" in the attacker's machine, and a "server" in the victim's machine. What happens when a server is installed in a victim's machine depends on the capabilities of the Trojan, the interests of the attacker, and whether or not another attacker ever gains control of the server - who might have entirely different interests.

root Kit A collection of programs that a hacker uses to mask intrusion and obtain administrator-level access to a computer or network.

Anti-antivirus Virus Anti-antivirus viruses attack, disable or infect specific anti-virus software. Also: Retrovirus

Armored Virus An armored virus tries to prevent analysts from examining its code. The virus may use various methods to make tracing, disassembling and reverse engineering its code more difficult.

Back Orifice

Back Orifice is a program developed and released by The Cult of the Dead Cow (cDc). It is not a virus; it is a remote administration tool with potential for malicious misuse. If installed by a hacker, it has the ability to give a remote attacker full system administrator privileges to your system. It can also 'sniff' passwords and confidential data and quietly e-mail them to a remote site. Back Orifice is an extensible program--programmers can change and "enhance" it over time. See Also: Password Sniffing

Sniffer

A software program that monitors network traffic. Hackers use sniffers to capture data transmitted via a network.

checksum

A one-way function applied to a file to produce a unique 'fingerprint' of that file for later reference. The slightest change in a file changes its checksum. Checksum systems are a primary means of detecting file system tampering.

CRC (cyclic redundancy check)

A type of checksum used implement data integrity as a check against accidental changes or corruption to data.

firewall Automatically blocks hackers from accessing your PC.

A firewall prevents computers on a network from communicating directly with external computer systems. A firewall typically consists of a computer that acts as a barrier through which all information passing between the networks and the external systems must travel. The firewall software analyzes information passing between the two and rejects it if it does not conform to pre-configured rules.

The firewall is a security devices used to restrict access in communication networks. They prevent computer access between networks (for example, from the Internet to a corporate network), and only allow access to services which are expressly registered. They also keep logs of all activity, which may be used in investigations.

**personal
firewall** A firewall which is intended to run on an individual computer.

Stealth Mode

Makes your PC invisible to hackers.

Safe Sharing

Share files and printers safely with trusted people, networks, and subnets.

Program Control

Ensures that only applications you trust access the Internet. Stops spyware and hackers from stealing personal data from your PC.

Hijacking Protection

Prevents hacker tools and spyware from hijacking trusted applications by corrupting their components.

"Spoofing" Protection

Hackers can't pretend to be you and shut-off protection using fake user input.

Anti-virus Software

Anti-virus software scans a computer's memory and disk drives for viruses. If it finds a virus, the application informs the user and may clean, delete or quarantine any files, directories or disks affected by the malicious code. Also: Anti-virus Scanner

Real-time Scanner

An anti-virus software application that operates as a background task, allowing the computer to continue working at normal speed, with no perceptible slowing.

Background Scanning

A feature in some anti-virus software to automatically scan files and documents as they are created, opened, closed or executed.

Background Scanning

=

On-access Scanner

=

Virus guard

**host-
based
intrusion
prevention**

[software] Generally used to describe software installed on a system that is designed to detect and block external attacks on that system.

**host-
based
security**

The technique of securing an individual system from attack. Host-based security is operating system and version dependent.

hacker An individual whose primary aim is to penetrate the security defenses of computer systems. A skilled hacker can penetrate a system and withdraw again, without leaving any trace of activity. Proto-hackers are those who aspire to be 'true' hackers but have not yet acquired the necessary skills to get past serious security measures without setting off alarm systems. The term is also applied to individuals who do not attack or attempt to penetrate computer systems, but use their skill to hack commercially available packages. Hackers, of whatever variety, are a threat to all computer systems.

hack Any software in which a significant portion of the code was originally in another program.

cybercrime

Any criminal activity which uses network access to commit a criminal act.

Hijacking

An attack whereby an active, established, session is intercepted and used by the attacker. Hijacking can occur locally if, for example, a legitimate user leaves

domain hijacking

A type of attack where an attacker takes over a domain by first blocking access to the DNS server and then putting another server up in its place

hijacker

In software terms, some code that resets your browsers settings to point to other sites. Hijacks may reroute your information and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower.

PGP Pretty Good Privacy. Considered the strongest program for encrypting data files and/or e-mail messages on PCs and Macintosh computers. PGP includes authentication to verify the sender of a message and non-repudiation to prevent someone denying they sent a message.