ELECS425F Computer and Network Security

Lec 07

Virtual Private Network (VPN)

VPN Introduction

It is used to secure end-to-end private network connections over a public network infrastructure.

Data is tunneled, but it appears as if information is sent over a dedicated private line.

More secure than traditional Internet transport

Inexpensive substitute for leased lines

VPN Design Requirements

Basic premise – secure transfer of data across a public network

Security of tunnel requires that its endpoints are authentic (must have accurate authentication scheme)

Must ensure that data has not been modified in transit (integrity)

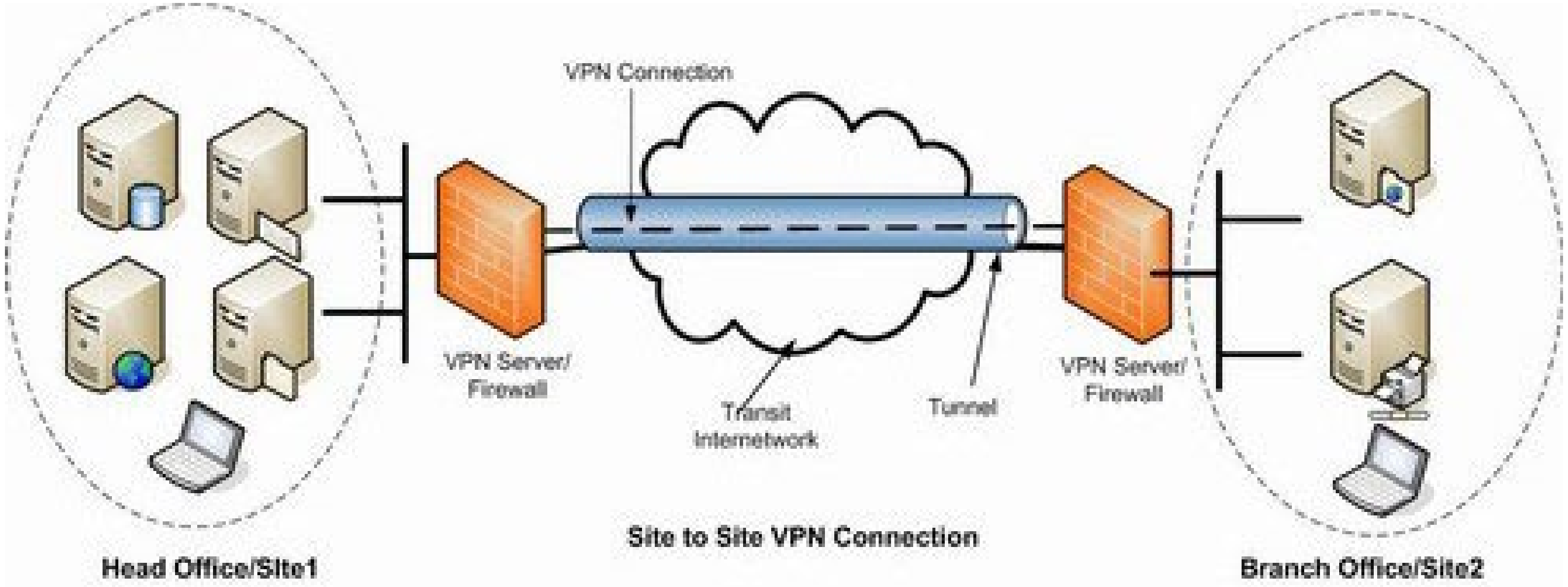
Must be able to manage both the establishment and operation of VPN tunnels

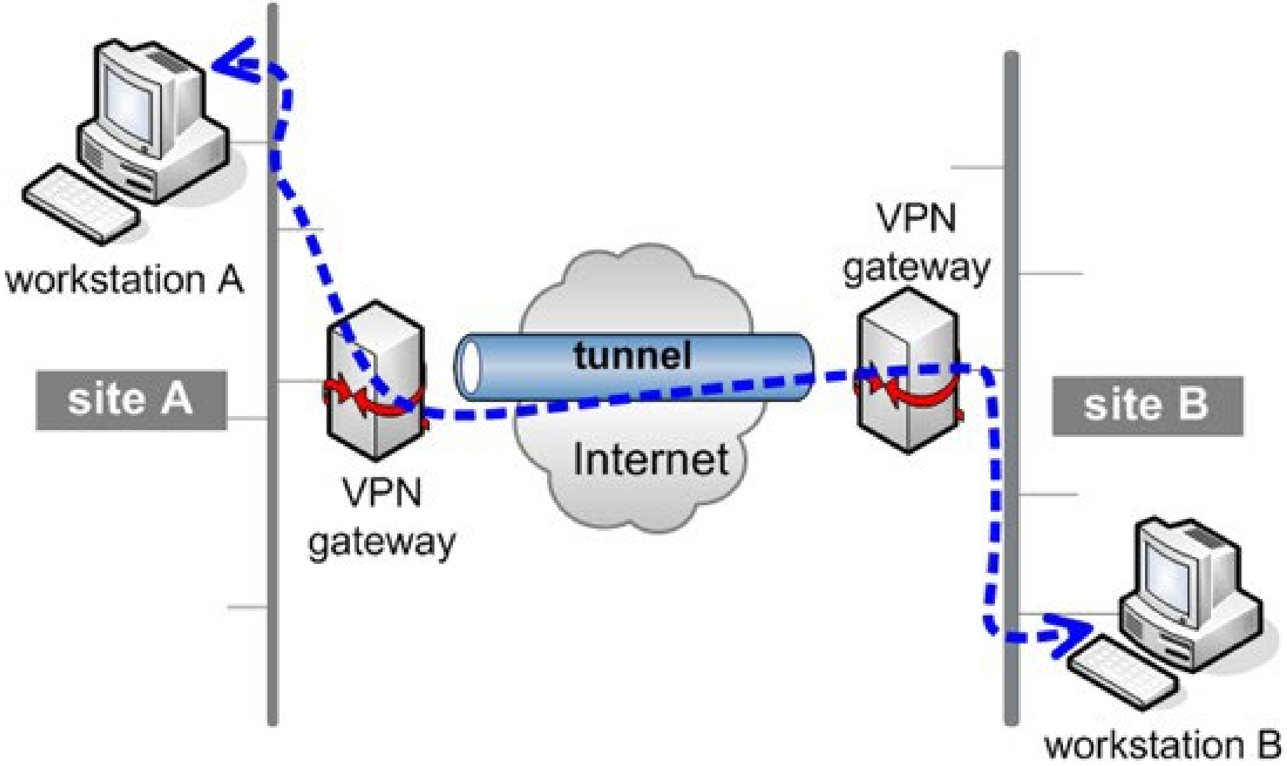
Must be able to restrict unauthorized access to your network (access control)

Must be able to prevent viewing of data as it traverses the network (confidentiality)

Two modes of use

1) LAN-to-LAN internetworking
(Site-to-site VPN, Intranet VPN)



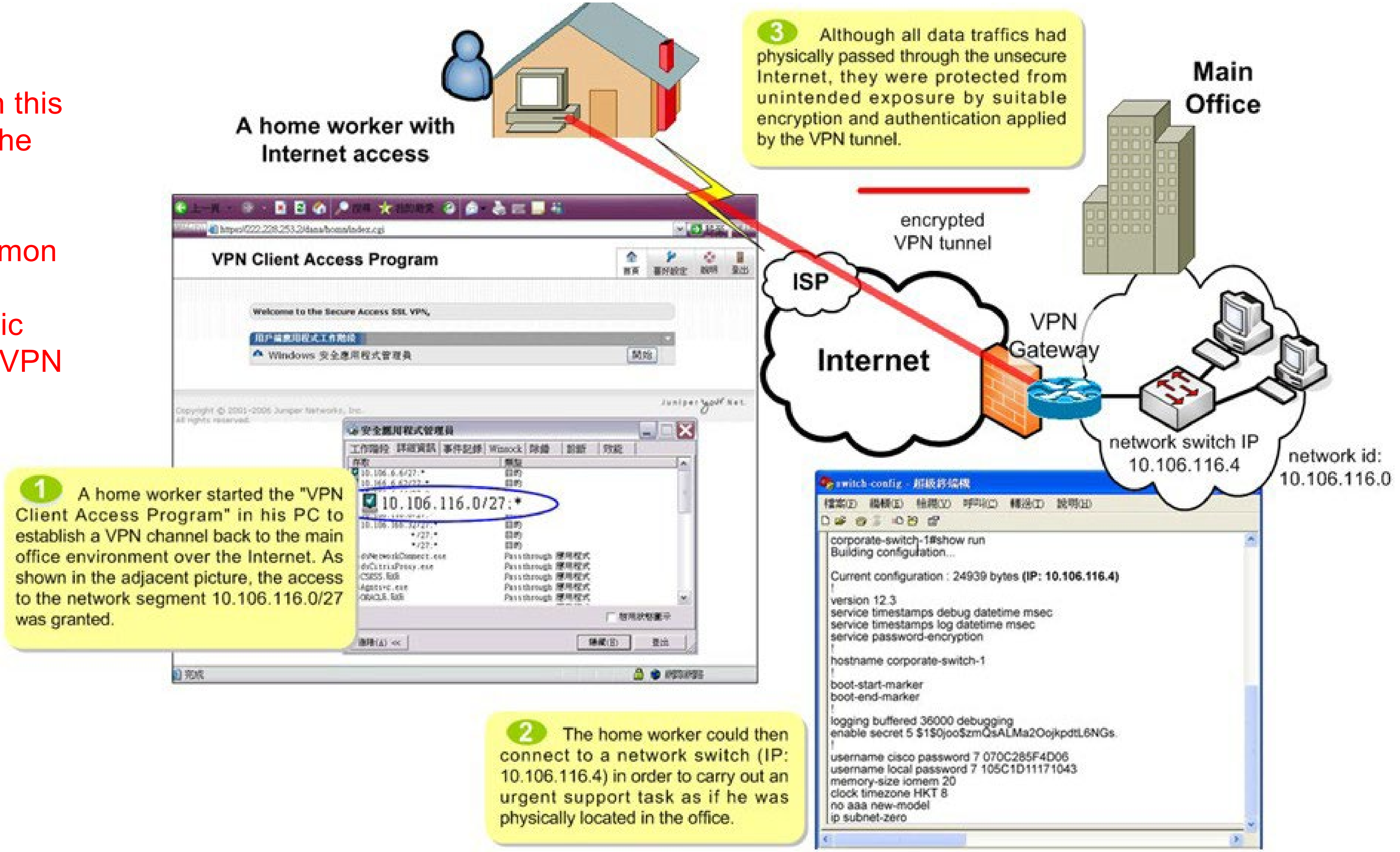


2) Remote access VPN

Access the VPN anywhere with Internet access (Remote access for the mobile workforce)

The VPN usage in this figure: to access the intranet.

Another very common usage:
Access other public networks thought VPN server


A home worker with Internet access
Main Office
encrypted VPN tunnel
ISP
Internet
VPN Gateway
network switch IP 10.106.116.4
network id: 10.106.116.0
VPN Client Access Program
Welcome to the Secure Access SSL VPN.
Windows 安全應用程式管理員
開始
Copyright © 2001-2006 Juniper Networks, Inc. All rights reserved.
安全應用程式管理員
10.106.116.0/27:*
switch-config

1 A home worker started the "VPN Client Access Program" in his PC to establish a VPN channel back to the main office environment over the Internet. As shown in the adjacent picture, the access to the network segment 10.106.116.0/27 was granted.

2 The home worker could then connect to a network switch (IP: 10.106.116.4) in order to carry out an urgent support task as if he was physically located in the office.

3 Although all data traffics had physically passed through the unsecure Internet, they were protected from unintended exposure by suitable encryption and authentication applied by the VPN tunnel.

```
corporate-switch-1#show run
Building configuration...

Current configuration : 24939 bytes (IP: 10.106.116.4)
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname corporate-switch-1
!
boot-start-marker
boot-end-marker
!
logging buffered 36000 debugging
enable secret 5 $1$0joo$zmQsALMa2OojkpdtL6NGs.
!
username cisco password 7 070C285F4D06
username local password 7 105C1D11171043
memory-size iomem 20
clock timezone HKT 8
no aaa new-model
ip subnet-zero
```

VPN Technologies and Protocols

PPTP - Point-to-point tunneling protocol
L2TP - Layer-2 tunneling protocol, or, **IPSec** - IP Security

	PPTP	**L2TP**
Basic Info	Basic & first VPN protocol supported by Windows.	Tunneling protocol that uses IPSec for security/encryption and works via UDP.
Compatibility	Built-in support for a wide array of desktops, mobile devices, and tablets.	Built-in support for a wide array of desktops, mobile devices, and tablets.
Encryption	128 bit keys	256 bit keys
Usage	via device/OS built-in client, using username + password + server address	via device/OS built-in client, using username + password + server address and pre-shared-key
Stability	Comparatively unstable, but very stable and accepted by most Wi-Fi hotspots.	Proven stable on various kinds of devices, networks and operating systems
Supported Devices/OS	Windows, Mac OSX, Linux, Android, DD-WRT, etc.	Windows, Mac OSX, Linux, iOS, Android, DD-WRT, etc.
Security	Basic encryption	Very secure. Data integrity checking, encapsulates data twice.
Advantages	Easy setup/configuration, good speeds, supported by a large number of devices.	Easy setup/configuration, easily bypasses restrictions by networks or ISPs.
Disadvantages	Stability may vary depending on network. Does not offer government level security. Easy to be blocked.	Slower Speeds
Conclusion	PPTP is easy to setup and use with decent speeds. Less secure than other VPN protocols.	L2TP usually achieves lower speeds than other protocols, but its ability to bypass network restrictions and strong security make it a good choice.
Best For	High-speed browsing, streaming or downloading	Security-specific tasks like online shopping, using public Wi-Fi, etc.,

https://www.purevpn.com/blog/difference-between-pptp-and-l2tp-protocols/

IPSec (Internet Protocol Security)

a framework that helps us to protect IP traffic on the network layer.

Security Features

Confidentiality: by encrypting our data, nobody except the sender and receiver will be able to read our data.

Integrity: we want to make sure that nobody changes the data in our packets. By calculating a hash value, the sender and receiver will be able to check if changes have been made to the packet.

Authentication: the sender and receiver will authenticate each other to make sure that we are really talking with the device we intend to.

IPSec Introduction

IPSec is the IP Security standard from the IETF (the people that standardize the Internet)

IPSec is a protocol suite for secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

IPSec consists of two different protocols

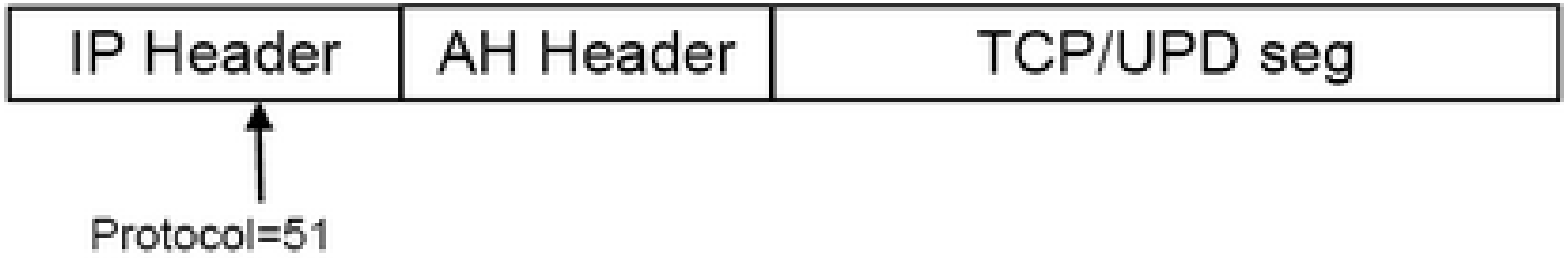
1)Authentication Header (AH)
2)Encapsulating Security Payload (ESP)

Both protocols assume the peers using the protocol have a shared key.
share authentication information.

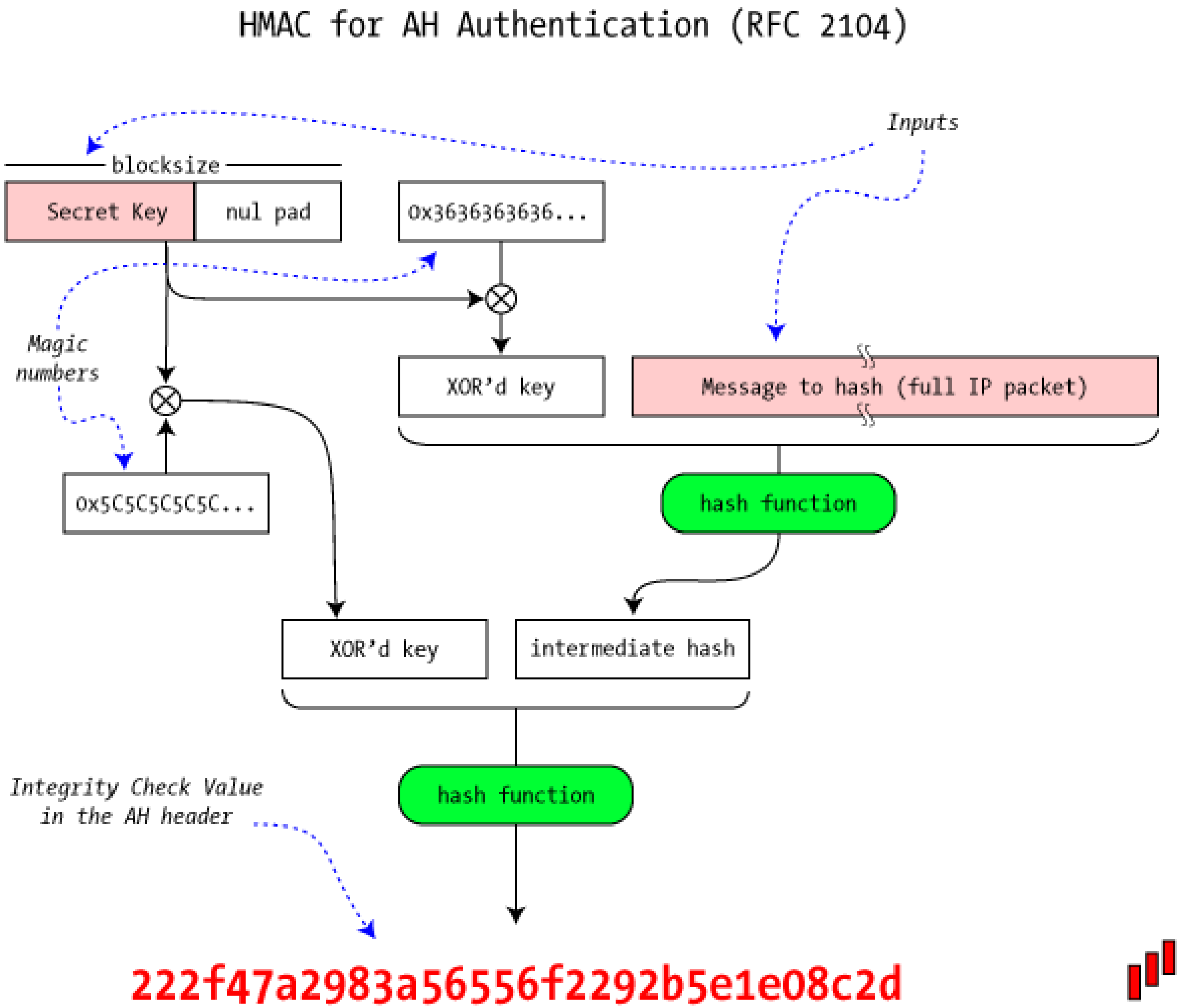
IP Authentication Header (AH)

It provides authentication and integrity of payload and header.

It does not provide confidentiality of payload.



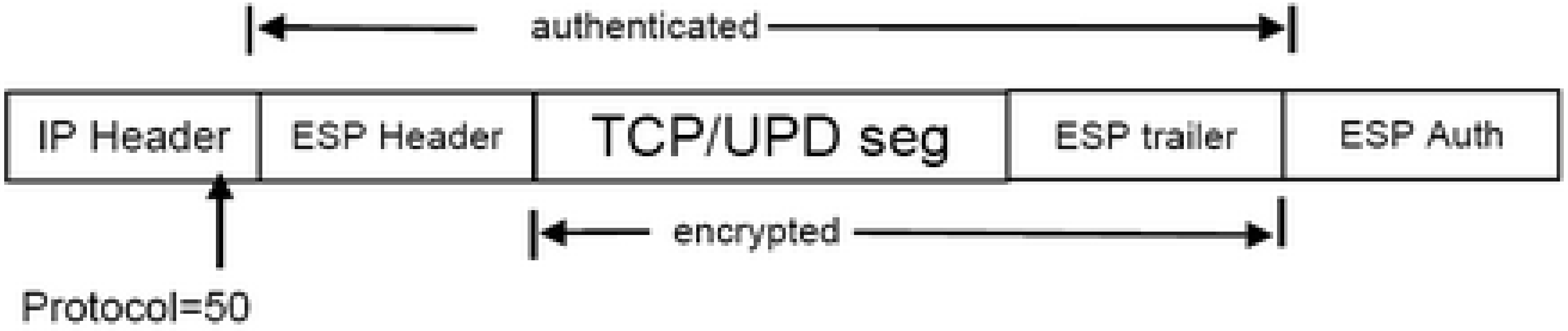
An example of Integrity Check Value (ICV) generation over the IP packet's contents



HMAC for AH Authentication (RFC 2104)

IP Encapsulating Security Payload (ESP)

It provides integrity, authentication, and confidentiality of an IP packet.



IPSec supports Transport and Tunnel modes for encryption.

IPSec Transport Mode

The Transport mode processes only the data portion of the IP packet. (It does not protect the IP header,)

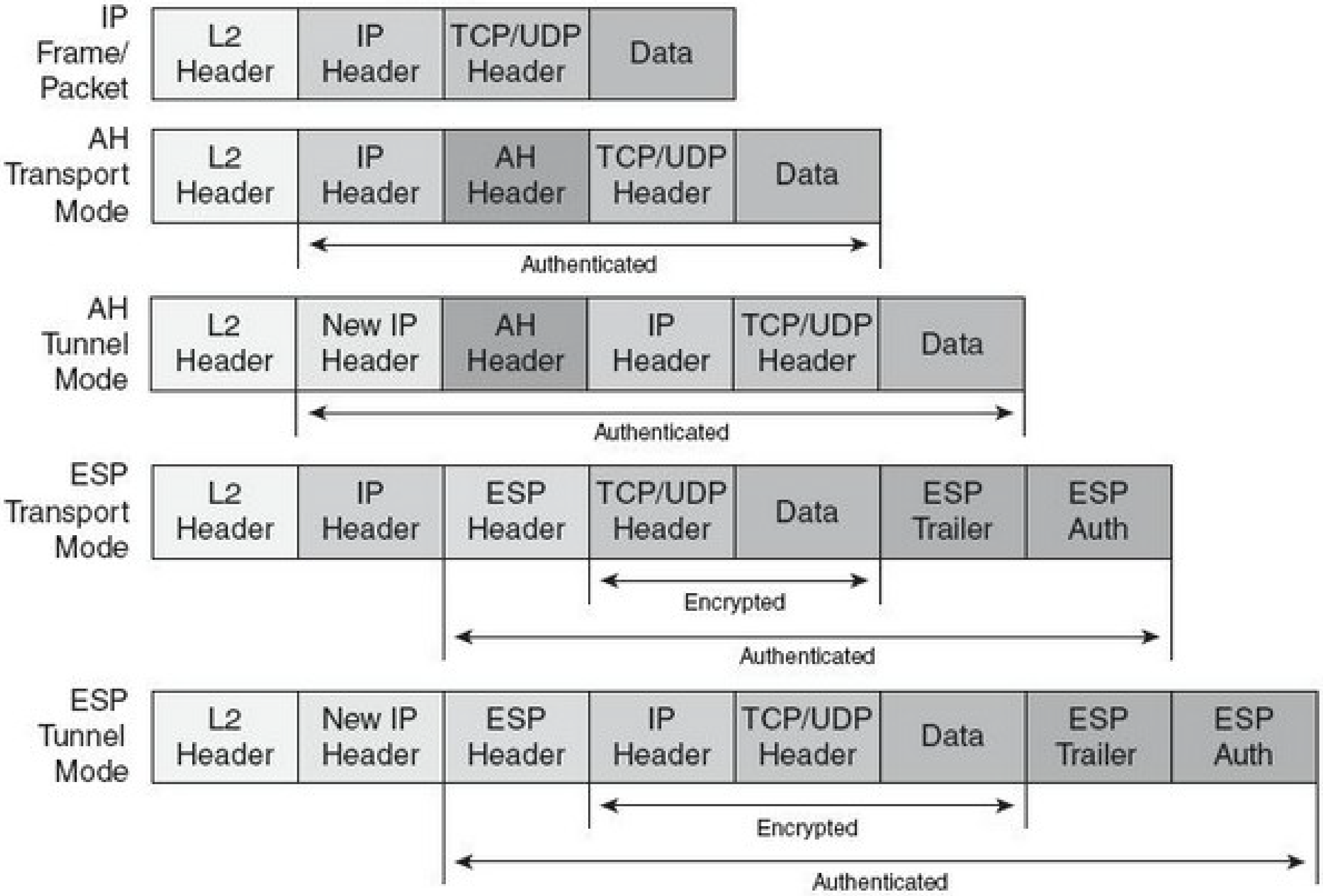
The Transport mode is commonly used for data transfer between two hosts in the same private site.

IPSec Tunnel Mode

The Tunnel mode encrypts both the data and the header portions of the encapsulated packet hiding more information about the underlying communications.

Tunnel mode is used for data transfer between two private sites, linked by a less secure channel, e.g. the public Internet.

Tunnel mode needs a new IP addressing space on top of the original IP addressing space.



IP Frame/ Packet: L2 Header | IP Header | TCP/UDP Header | Data

AH Transport Mode: L2 Header | IP Header | AH Header | TCP/UDP Header | Data

Authenticated

AH Tunnel Mode: L2 Header | New IP Header | AH Header | IP Header | TCP/UDP Header | Data

Authenticated

ESP Transport Mode: L2 Header | IP Header | ESP Header | TCP/UDP Header | Data | ESP Trailer | ESP Auth

Encrypted

Authenticated

ESP Tunnel Mode: L2 Header | New IP Header | ESP Header | IP Header | TCP/UDP Header | Data | ESP Trailer | ESP Auth

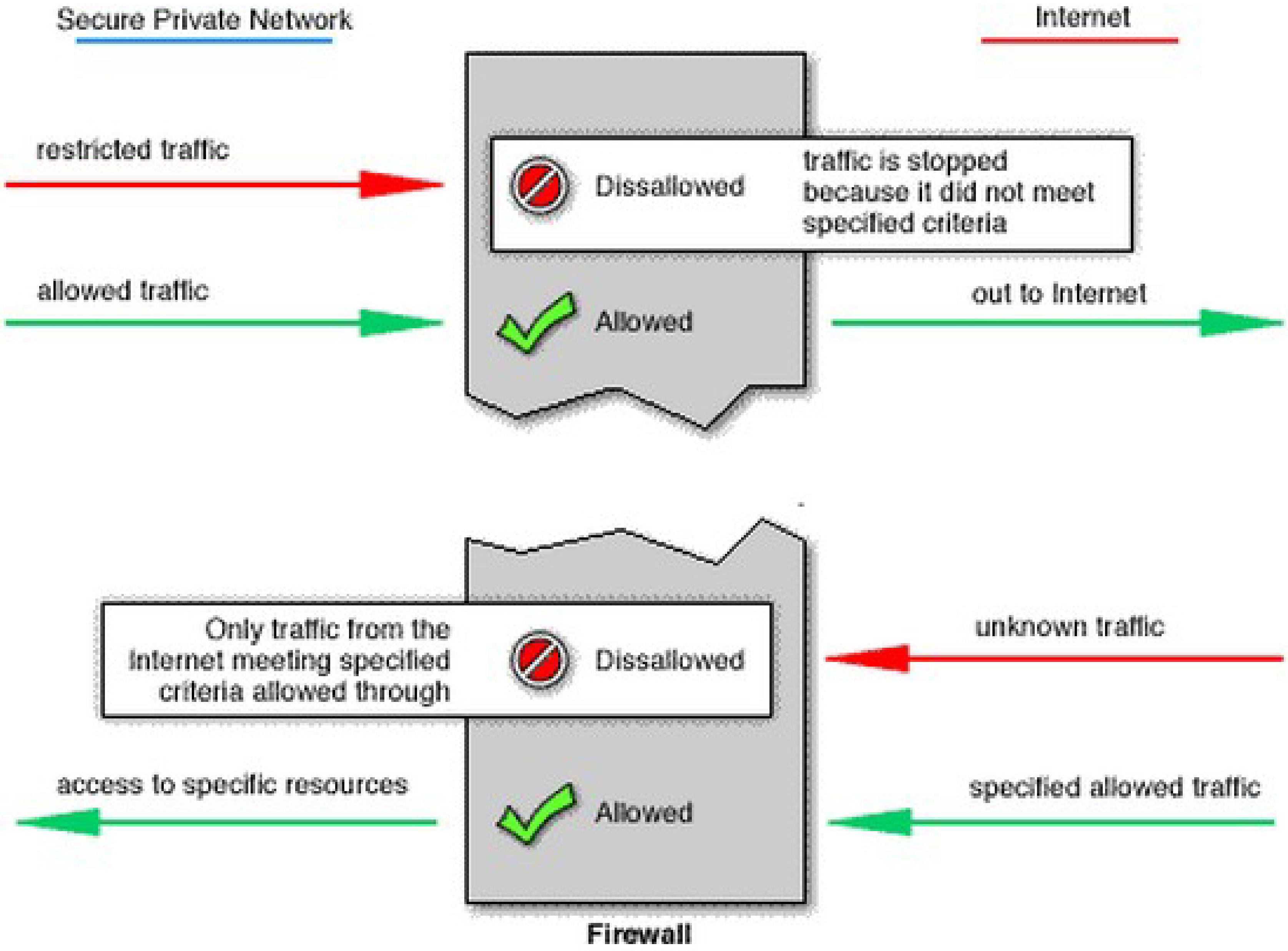
Encrypted

Authenticated

Reading: IPsec (Internet Protocol Security) from NetworkLlessions.com: https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security/

Firewalls

- Firewalls are hardware and/or software designed to prevent unauthorized access to or from a private network.
- They are placed at the junction or gateway between the two networks, which is usually a private network and a public network such as the Internet.
- Firewalls examine all messages entering or leaving the Intranet and block those that do not meet the specified security criteria.

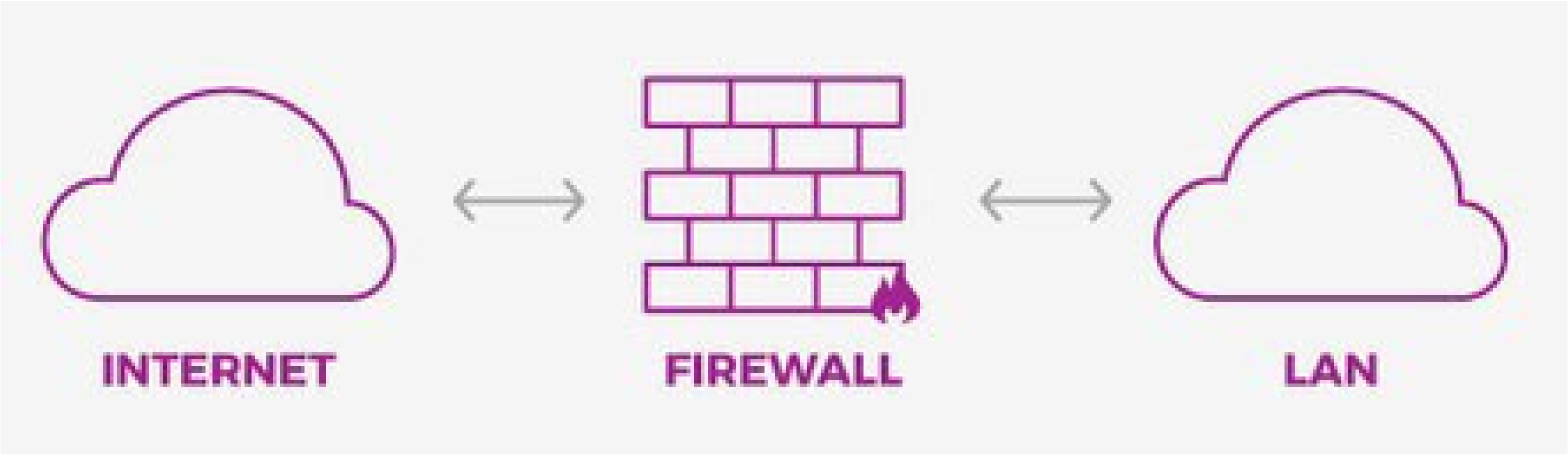

Secure Private Network
Internet
restricted traffic
Dissallowed
traffic is stopped because it did not meet specified criteria
allowed traffic
Allowed
out to Internet
Only traffic from the Internet meeting specified criteria allowed through
Dissallowed
unknown traffic
access to specific resources
Allowed
specified allowed traffic
Firewall

Firewall Architecture / Firewall Topologies

Bastion Host

The most common option of use for firewalls, especially in small environments, is called a bastion host. Through this topology, the firewall is placed between the internet and the internal network segment.

Traffic entering or leaving the network passes through the firewall. It has two interfaces

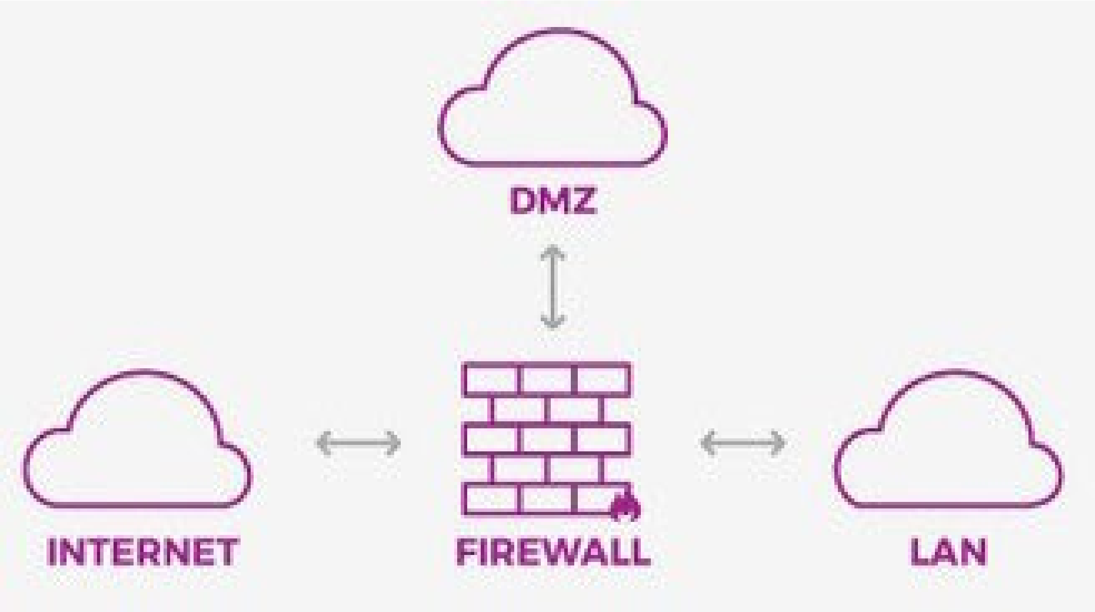


Screened Subnet

The firewall has at least three communication interfaces, so that it can isolate the Internet, protected networks, and finally, create a so-called DMZ.

The screened subnet or DMZ (DeMilitarized Zone) contains hosts that offer public services.

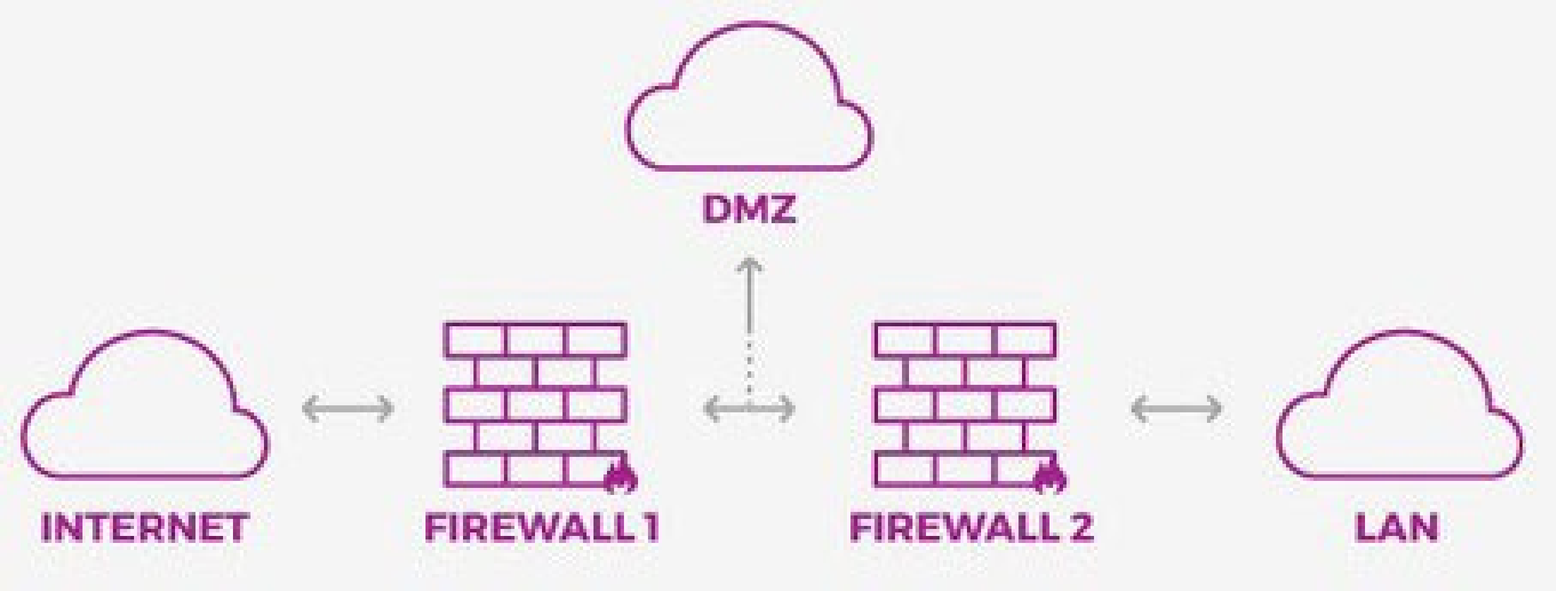
Public network services, such as web servers, e-mail servers, and others, are strategically positioned in the DMZ. If an attacker compromises the access of some of these servers, it will still not have direct access to the protected networks because the firewall is interposed in this architecture.



Multi-homed Firewall

In addition to the Screened subnet topology, multi-homed architectures are composed of several connections that allow segmenting of various networks.

In addition, in many cases these architectures work with two distinct devices, further enhancing the security of the environment, since the compromise of one of them does not mean access to the protected networks.



Types of Firewalls

Hardware Firewall

A hardware firewall is either a dedicated stand-alone hardware device or it comes as part of a router.

The network traffic is filtered using the packet filtering technique.

It is used to filter out the network traffic for large business networks.

Software Firewall

A software firewall is a software program installed on a computer, just like normal software. It is

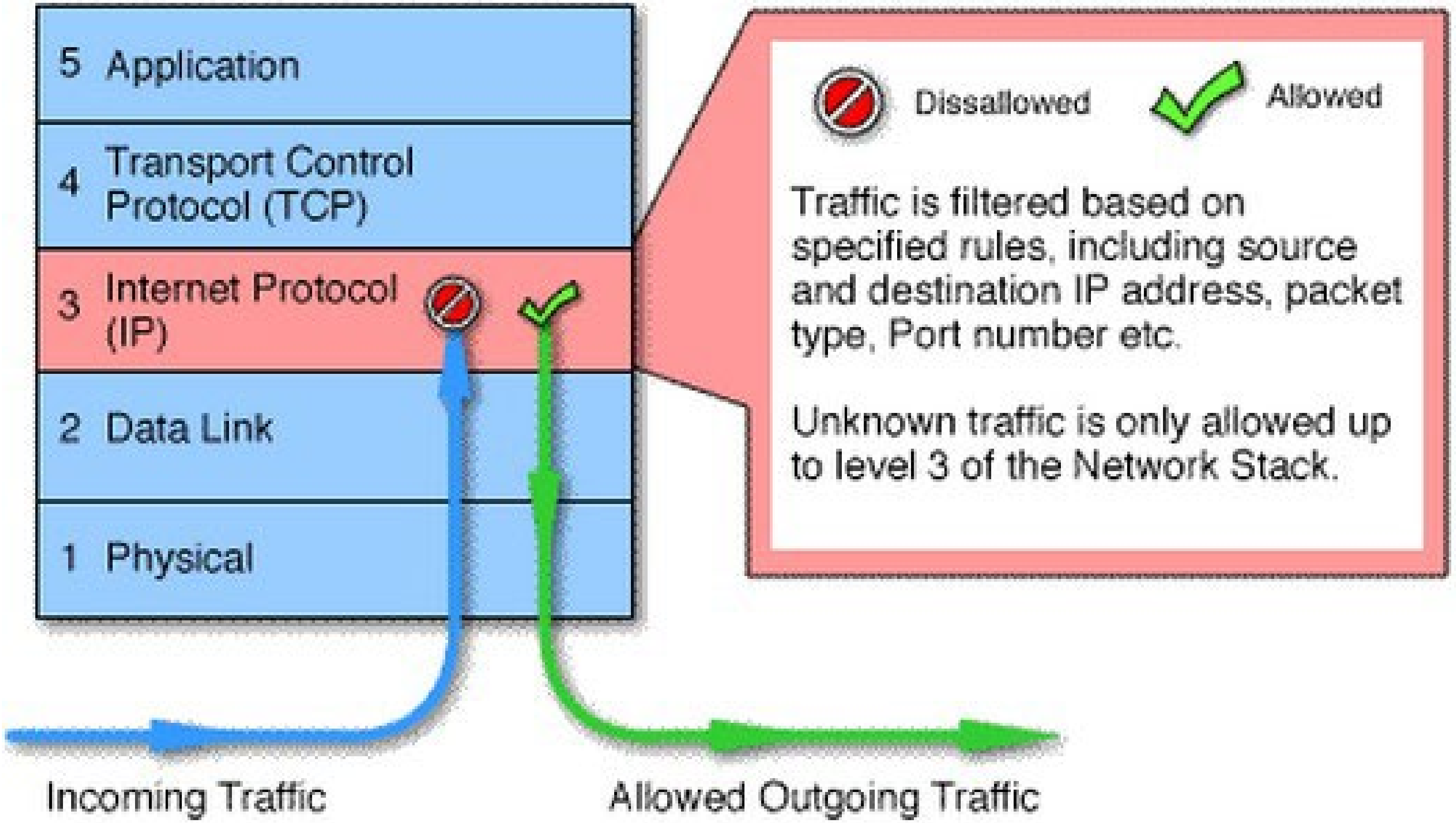
generally used to filter traffic for individual home users.

It only filters traffic for the computer on which it is installed, not for the network.

Example: **iptables** (the Default Linux Firewall)
Reference: https://www.cyberciti.biz/tips/linux-iptables-examples.html

Firewall Technologies

- **Packet Filtering**


5 Application
4 Transport Control Protocol (TCP)
3 Internet Protocol (IP)
2 Data Link
1 Physical
Dissallowed
Allowed
Traffic is filtered based on specified rules, including source and destination IP address, packet type, Port number etc.
Unknown traffic is only allowed up to level 3 of the Network Stack.
Incoming Traffic
Allowed Outgoing Traffic

Packet filtering firewalls work at the network layer of the OSI model, or the IP layer of TCP/IP. (They are usually a part of a router.)

In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded.

Depending on the packet and the criteria, the firewall can drop the packet or forward it, or send a message to the originator.

Rules can include the source and the destination IP address, the source and the destination port number, and the protocol used.

Advantages:

Simplicity Transparency to users High speed

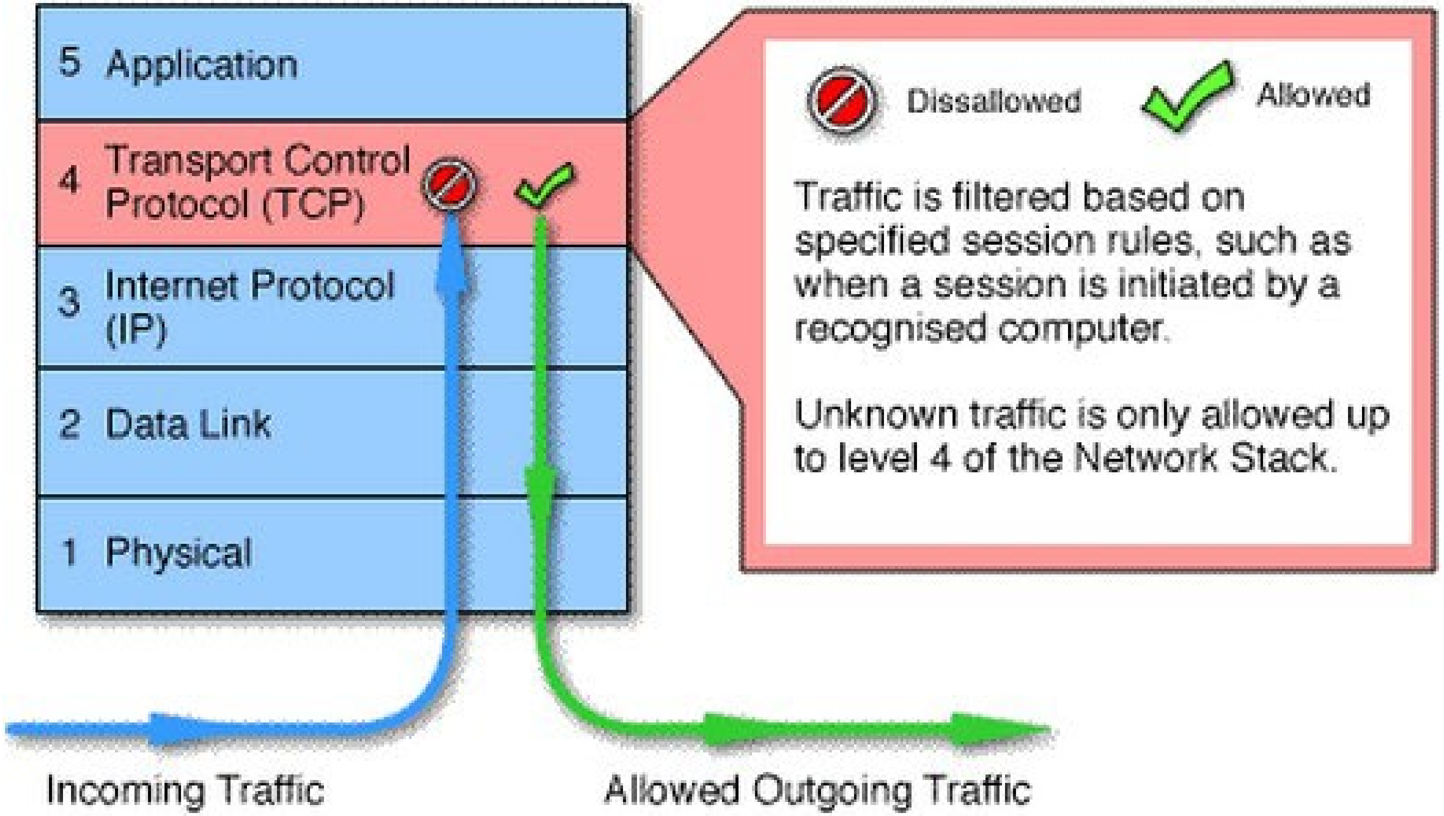
Disadvantages:

Difficult of setting up packet filter rules Lack of Authentication

Possible attacks

IP address spoofing Source routing attacks

- **Circuit Level Gateways**


5 Application
4 Transport Control Protocol (TCP)
3 Internet Protocol (IP)
2 Data Link
1 Physical
Dissallowed
Allowed
Traffic is filtered based on specified session rules, such as when a session is initiated by a recognised computer.
Unknown traffic is only allowed up to level 4 of the Network Stack.
Incoming Traffic
Allowed Outgoing Traffic

Circuit-level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP.

Information passed to a remote computer through a circuit-level gateway appears to have originated from the gateway.

They monitor requests to create sessions, and determine if those sessions will be allowed.

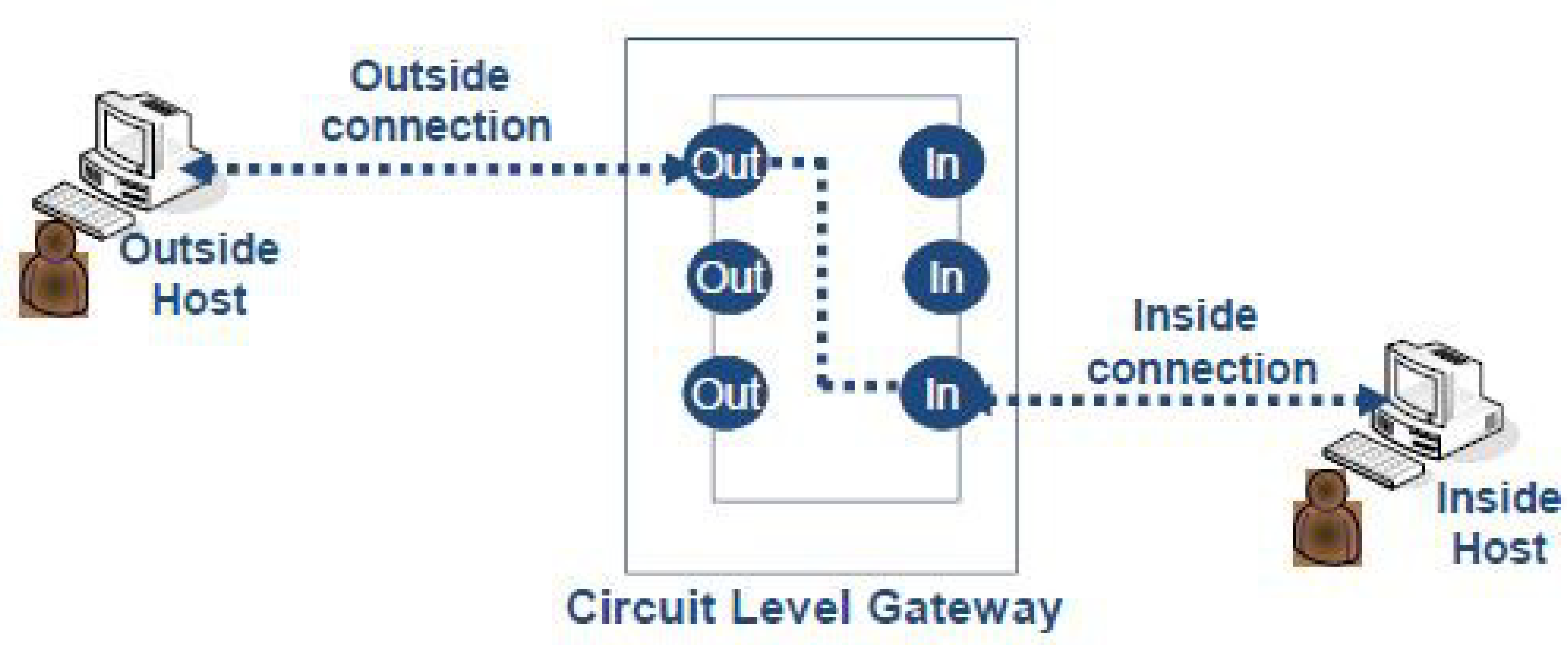
Circuit proxy firewalls allow or prevent data streams; they do not filter individual packets.

Advantages:

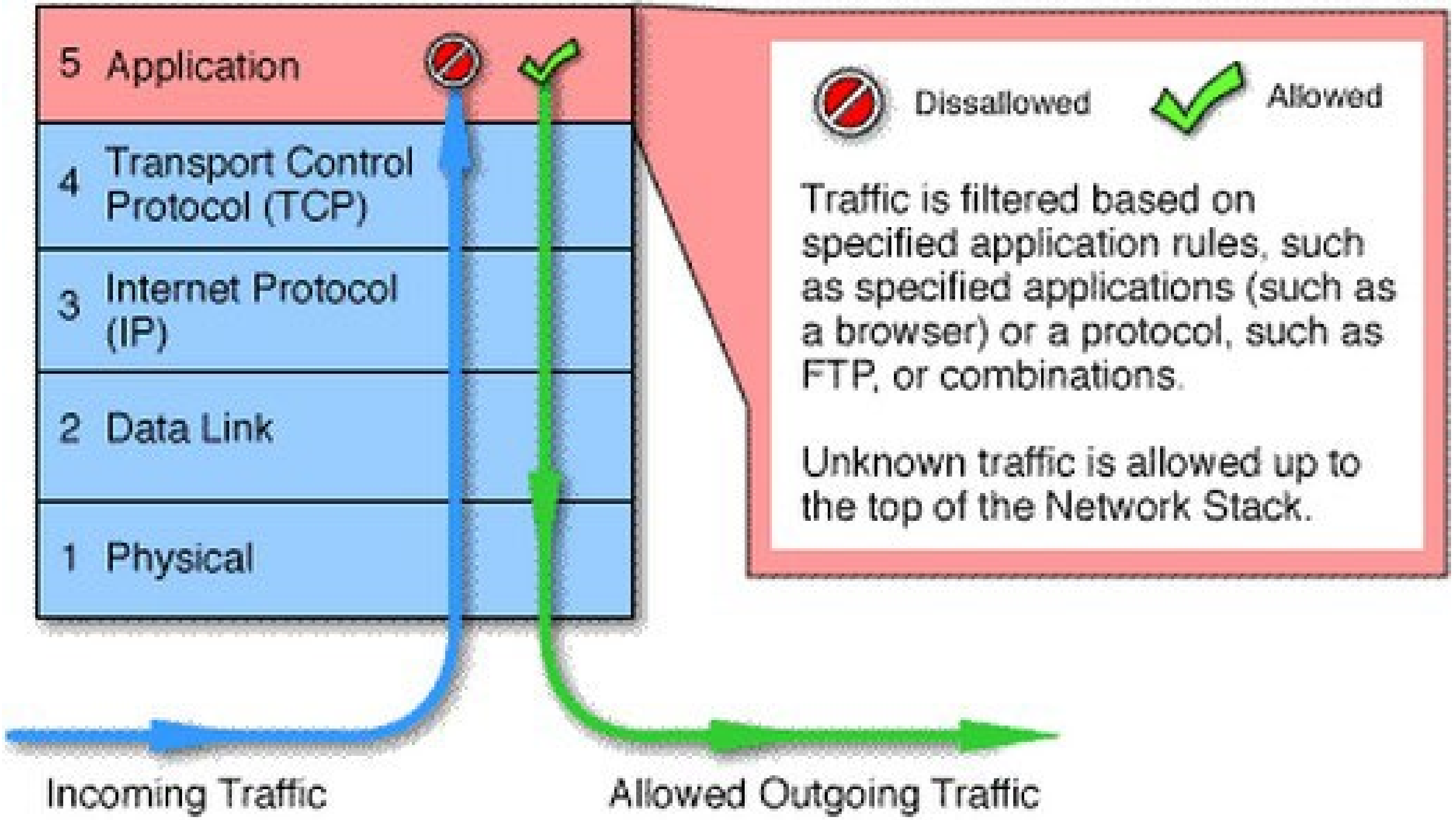
Hides private network data, doesn't need a separate proxy server for each application, simple to implement.

Disadvantages:

Doesn't filter individual packets, attacker may take advantage after establishing a connection.



- **Application Level Firewall**


5 Application
4 Transport Control Protocol (TCP)
3 Internet Protocol (IP)
2 Data Link
1 Physical
Dissallowed
Allowed
Traffic is filtered based on specified application rules, such as specified applications (such as a browser) or a protocol, such as FTP, or combinations.
Unknown traffic is allowed up to the top of the Network Stack.
Incoming Traffic
Allowed Outgoing Traffic

Application-level gateways, also called proxies, can filter packets at the application layer.

Incoming and outgoing traffic is restricted to services supported by proxy; all other service requests are denied.

Application-level gateways configured as a web proxy prohibit FTP, gopher, telnet, or other traffic.

Application-level gateways examine traffic and filter on application-specific commands such as http:post and http:get.

This cannot be accomplished with either packet filtering firewalls or circuit level neither of which know anything about the application level information.

Advantages:

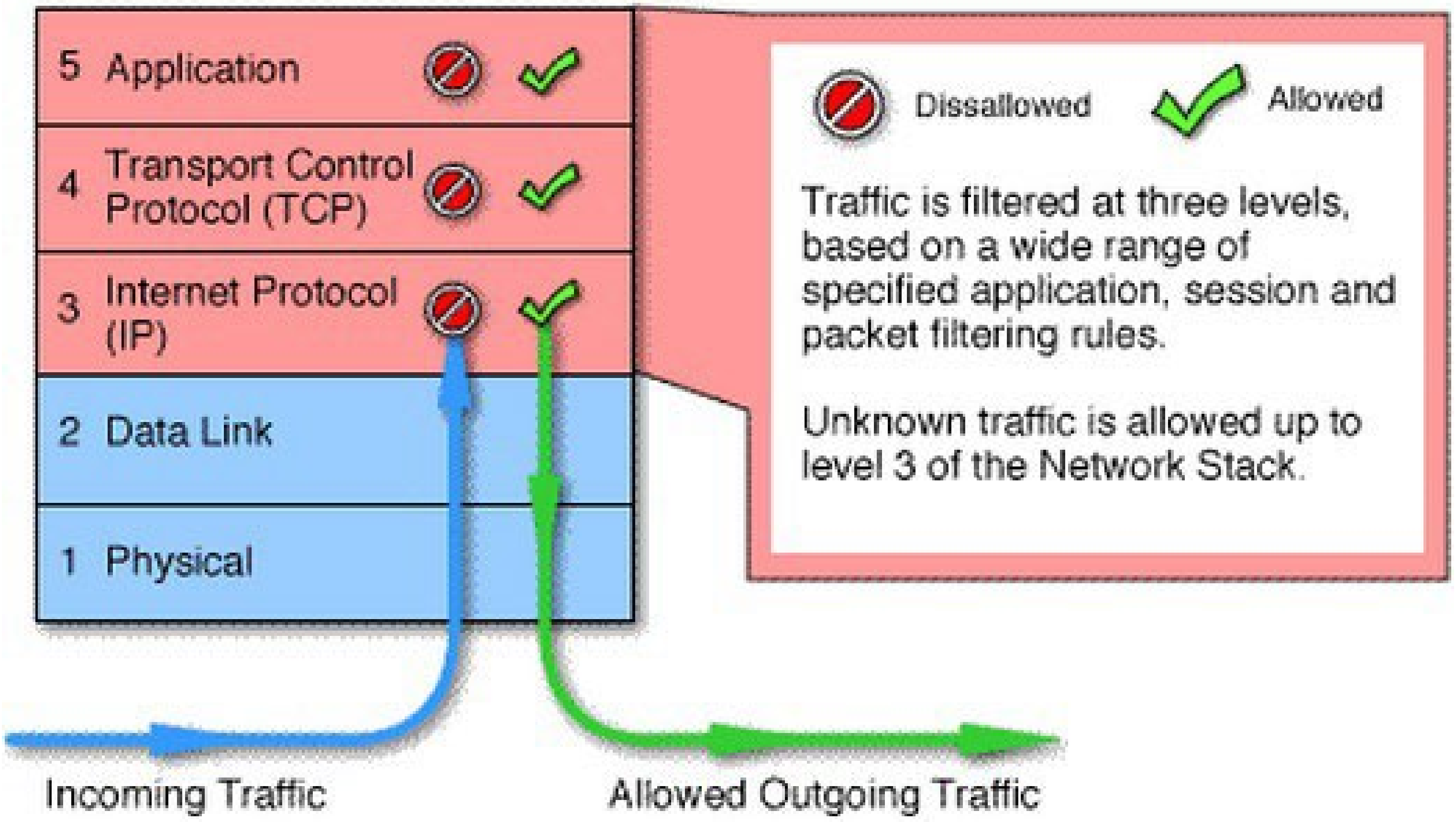
High security than packet filters

Only need to scrutinise a few allowable applications Easy to log and audit all incoming traffic

Disadvantages:

Additional processing overhead on each connection (gateway as splice point)

- **Stateful Multilayer Inspection**



Traffic is filtered at three levels, based on a wide range of specified application, session and packet filtering rules.

Unknown traffic is allowed up to level 3 of the Network Stack.

Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls.

They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer.

They allow direct connection between client and host, alleviating the problem caused by the lack of transparency of application level gateways.

They rely on algorithms to recognize and process application layer data instead of running application specific proxies.

Advantage: stateful multilayer inspection firewalls offer a high level of security, good performance and transparency to end users.

Disadvantage: they are expensive however, and due to their complexity are potentially less secure than simpler types of firewalls if not administered by highly competent personnel.

Intrusion Detection

What is **intrusion detection**?

It aims to identify potential attacks at an early stage.

It checks network traffic in real-time, monitors servers for misuse, and tries to recognise patterns of malicious action or policy abuse.

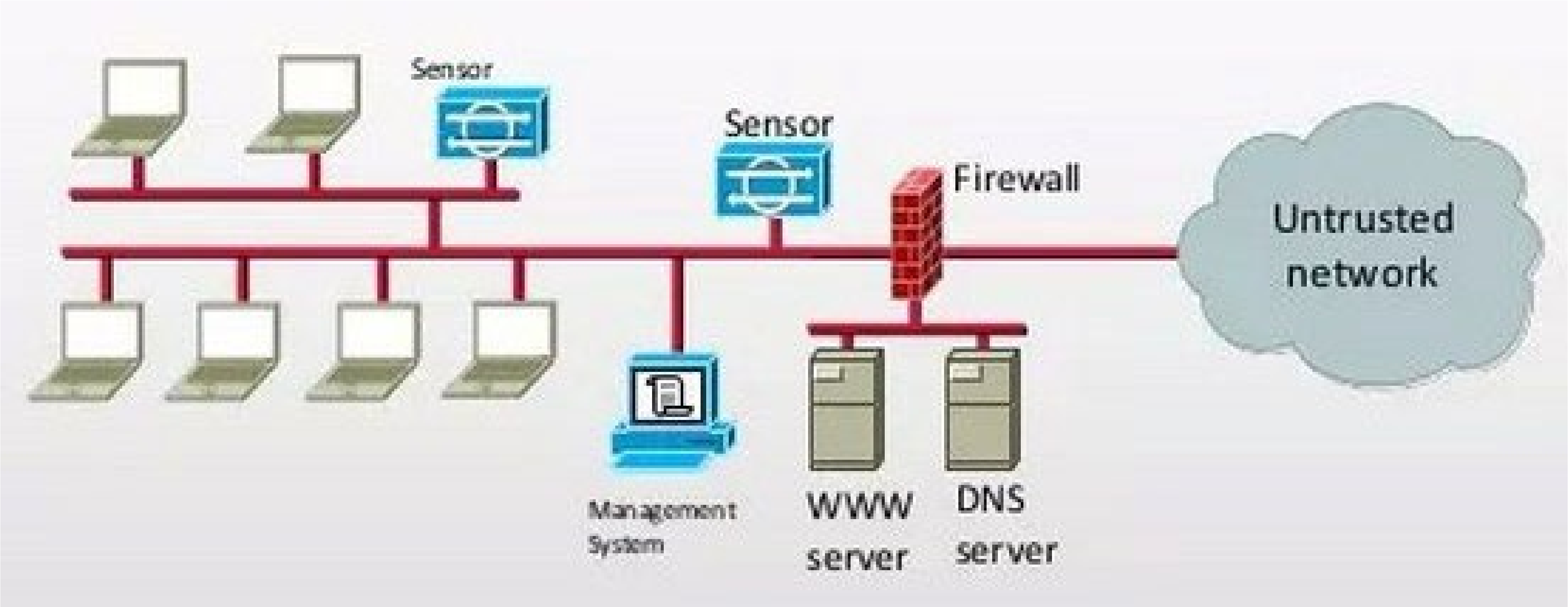
It gathers statistics, and responds to suspected attacks or breaches of usage agreements.

Intrusion detection systems (IDS)

An intrusion detection system (IDS) is a device (or application) that monitors network and/or system activities for malicious activities or policy violations and produces reports to a managment station.

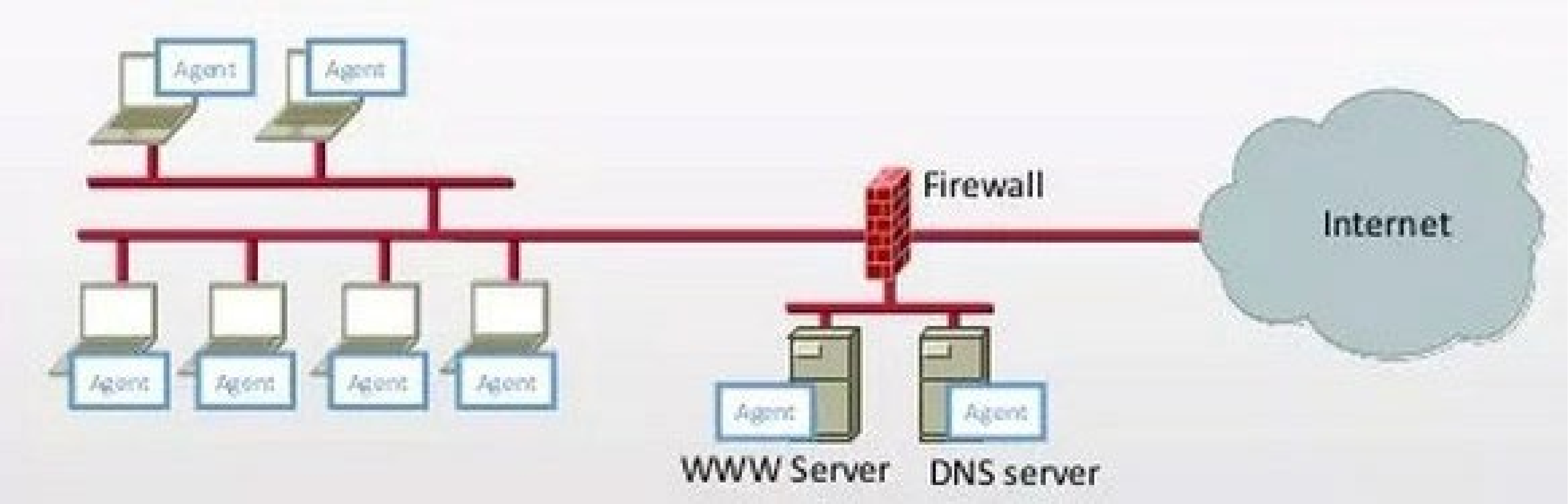
There are two types of IDS: network-based IDS and host-based IDS.

- **Network-based IDS** - to examine network packets transmitted in the network



In a network-based intrusion-detection system (NIDS), the sensors are located at choke points in network to be monitored, often in the demilitarized zone (DMZ) or at network borders. The sensor captures all network traffic and analyzes the content of individual packets for malicious traffic.

- **Host-based IDS** - to detect any abnormalities arising in a host system



In a host-based system, the sensor usually consists of a software agent, which monitors all activity of the host on which it is installed, including file system, logs and the kernel. Some application-based IDS are also part of this category.

Summary

IDS (Intrusion Detection System)

- Network-based IDS (inspecting network)
  - Snort (https://www.snort.org/)
  - Suricata (https://suricata-ids.org/)

- Host-based IDS (inspecting host)
  - AIDE (http://aide.sourceforge.net/)
  - OSSEC (https://ossec.github.io/)

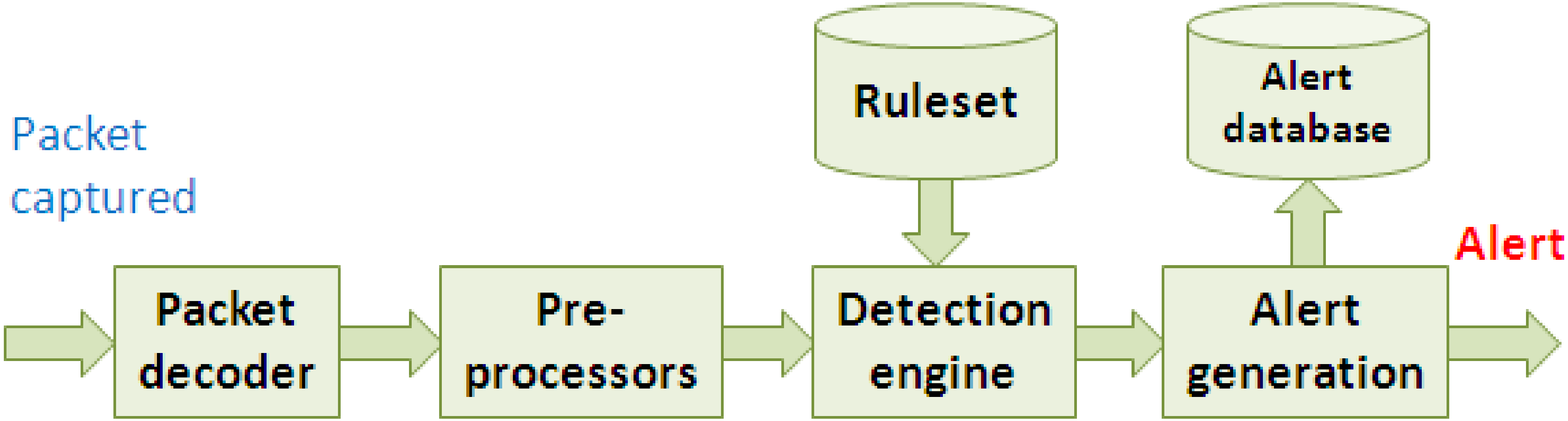
Example Host-based IDS: AIDE

AIDE (Advanced Intrusion Detection Environment) is a file and directory integrity checker. It creates a database from the regular expression rules that it finds from the config file(s). Once this database is initialized it can be used to verify the integrity of the files.

Example Network-based IDS: Snort

Snort - an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire.

Basic dataflow using Snort as an IDS



Packet Decoder: input from Ethernet, SLIP, PPP

Preprocessor:

detect anomalies in packet headers packet defragmentation

decode HTTP URI reassemble TCP streams

Detection Engine: applies rules to packets Alert generation: logging and output alert

Identification technologies for intrusion detection/prevention

Network-based intrusion detection/prevention

1) Signature-based
   Look for a perfect match

2) Anomaly-based
   Build a baseline of what's "normal"

3) Behaviour-based
   Observe and report

4) Heuristics
   Use artificial intelligence to identify

Host-based intrusion detection/prevention

1) Protect based on signatures
   constantly growing database

2) Protect based on activity
   why are you modifying that file?

References and Readings for learning more

VPNs and VPN Technologies

An Illustrated Guide to IPsec

IPsec (Internet Protocol Security)

https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security/

Video: How IPSec Site to Site VPN Tunnels Work
https://www.youtube.com/watch?v=CuxyZiSCSfc

Video: IPSec Site to Site VPN tunnels
https://www.youtube.com/watch?v=C_B9k0l6kEs

Two Types of Firewalls: Packet-Filtering Firewalls and Application/Proxy Firewalls
https://www.networkworld.com/article/2255950/lan-wan/chapter-1--types-of-firewalls.html

Network Security Course (ET1318, ET2437) at Blekinge Institute of Technology, Karlskrona, Sweden
https://www.slideshare.net/rajakhurram/lecture-4-firewalls

Firewalls - Computer Networks http://www.bankexamstoday.com/2015/12/firewalls-computer-networks.html

Intrusion Detection and Prevention Systems - CompTIA Network+ N10-006 - 1.1
https://www.youtube.com/watch?v=mmt4B60xSj0

KnowledgeShare - Firewall Q and A
http://www.vicomsoft.com/knowledge/reference/firewalls1.html