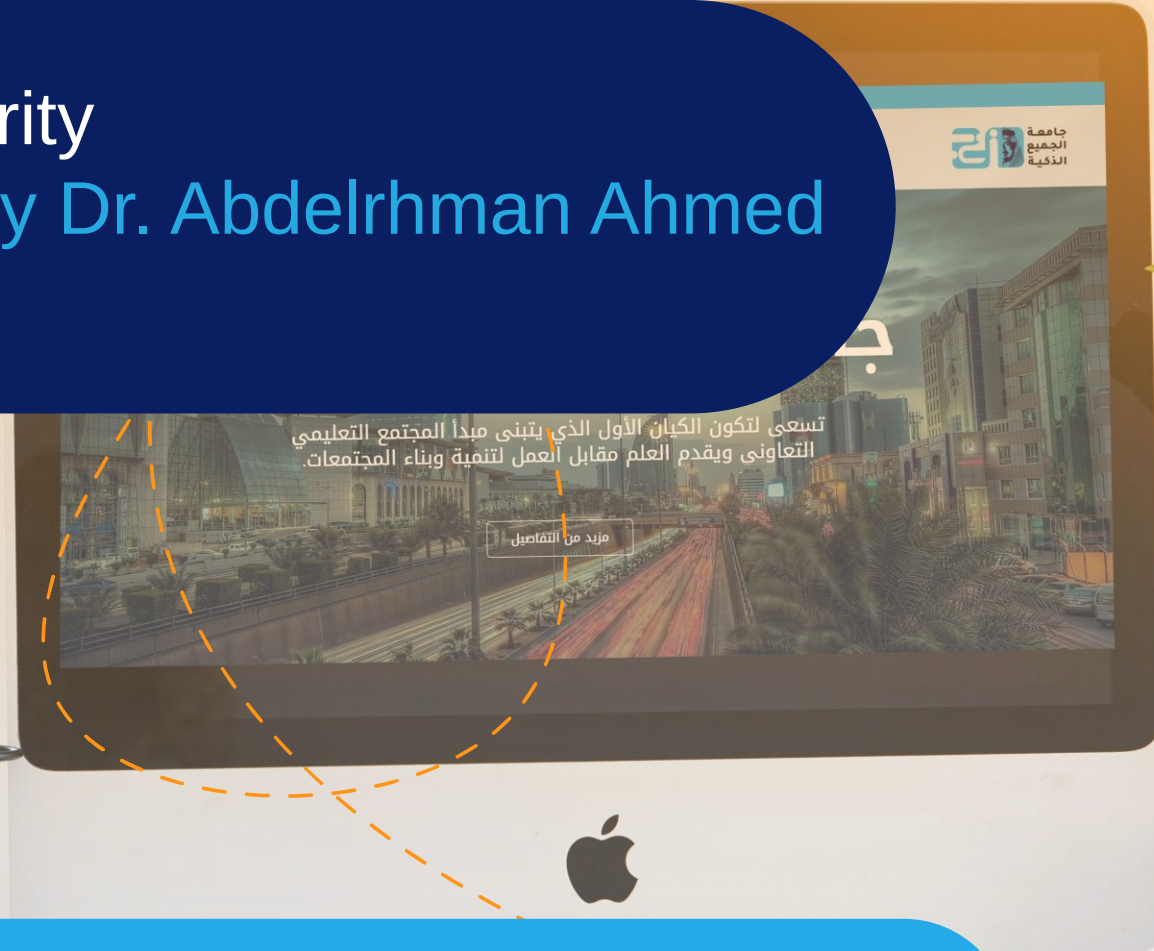


HCIA Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 8



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Overview of Intrusion Prevention

- **Currently, malware is the most common form of security threat, while the impact of greyware is increasing and security threats correlated to crimes have been critical to network security.**
- **Instead of dealing with only virus attacks, users now have to fend off combinations of network threats, including viruses, hacker intrusions, Trojan horses, botnets, and spyware. Current defense mechanisms struggle to mitigate such attacks.**
- **This course explains what intrusion is and describes to what degree Huawei USG products support intrusion prevention.**



Objectives

- **Upon completion of this course, you will be able to:**
 - ☐ **Describe the different types of intrusion prevention.**
 - ☐ **Deploy network antivirus policies.**

- Network threats, such as viruses, no longer only target computer systems. Instead, they are also used for financial gain, etc. This is causing conventional computer viruses and other network threats to evolve into interest-driven, all-round network threats.
- Malware is the most common security threat, and includes viruses, worms, botnets, rootkits, Trojans, backdoor programs, vulnerability exploit programs, and wap malicious programs. Besides malware, the impact of greyware is increasing and security threats correlated to crimes have been critical to network security.
- Instead of facing only virus attacks, users now have to fend off combinations of network threats, including viruses, hacker intrusions, Trojan horses, botnets, and spyware. Current defense mechanisms struggle to mitigate such attacks.



Hacker intrusion

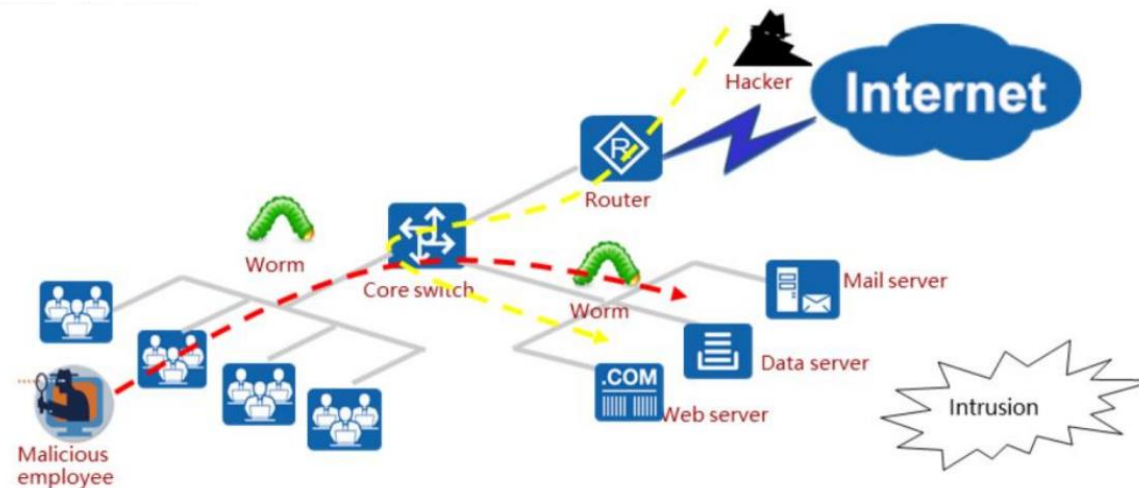
Denial of Service (DoS)
attacks

Virus and malware

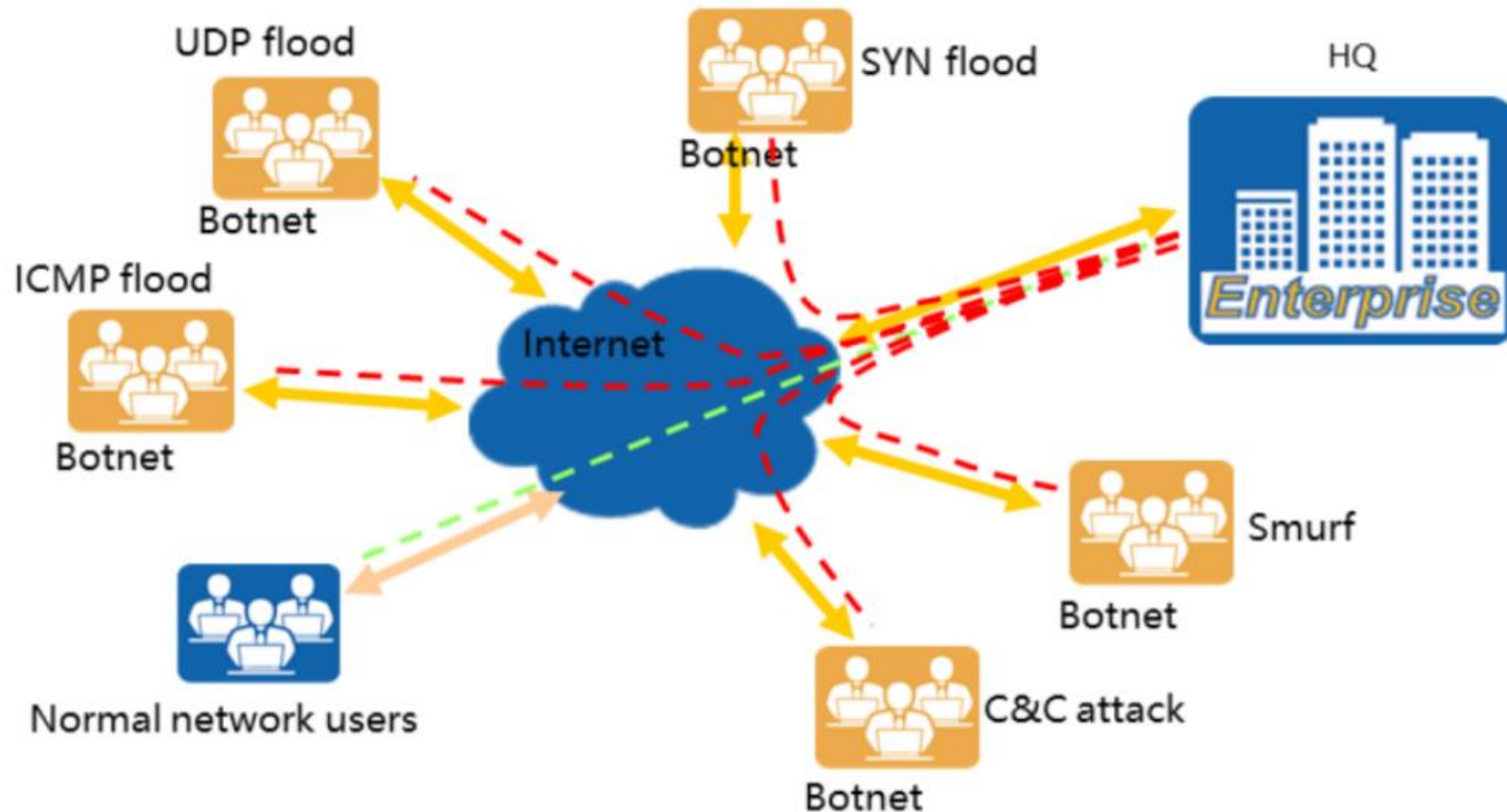
Hackers and malicious employees may exploit system and software vulnerabilities to intrude into servers, putting the security of data from key services at risk.

- Vulnerabilities lead to severe security risks:

- ❑ Application software running on the enterprise intranet may have vulnerabilities.
- ❑ The Internet helps vulnerabilities in application software spread rapidly.
- ❑ Worms spread by exploiting application software vulnerabilities, consuming network bandwidth and damaging important data.
- ❑ Hackers and malicious employees target vulnerabilities to intrude into enterprise servers and tamper with, destroy, or steal confidential information.



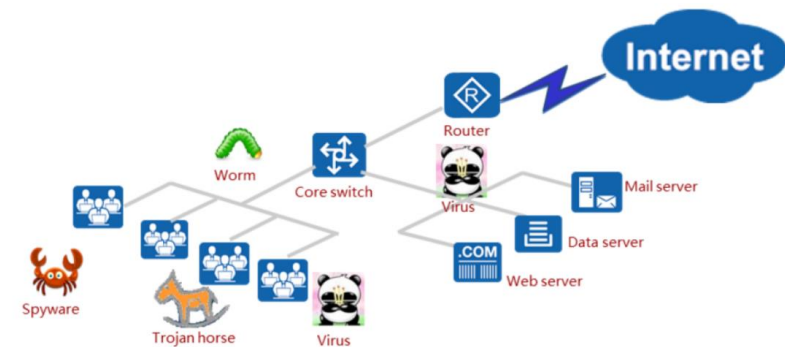
DDoS attacks launched for financial gain continuously disrupt the normal operation of enterprises, and these attacks are becoming increasingly harmful.



- **DDoS attacks:**

- **There is now a global black industry chain based on DDoS attacks that has the aim of financial gain. Also, there is a huge number of botnets on networks.**
- **DDoS attacks may be launched for blackmail or disrupting competitors.**
- **DDoS attacks will occupy bandwidth to bring the network down and exhaust server resources to prevent the server from responding to user requests or to crash the system, ultimately causing services to fail.**

- An increasing number of enterprise service applications depend on the IT information system. The operation of services is under threat from viruses, Trojan horses, and spyware.
- A virus is a type of malicious code that infects or attaches to application programs or files and spreads through protocols, such as email or file sharing protocols, threatening the security of user hosts and networks.
- Viruses perform various types of harmful activities on infected hosts, such as exhausting host resources, occupying network bandwidth, controlling host permissions, stealing user data, and even corrupting host hardware.
- Virus and malware:
 - ❑ Viruses, Trojan horses, and spyware invade an intranet mainly through web browsing and mail transmission.
 - ❑ Viruses can crash computer systems and tamper with or destroy service data.
 - ❑ Trojan horses enable hackers to steal key information on computers as well as crash them. Spyware collects, uses, and transmits sensitive information on enterprise employees, disturbing normal services.
 - ❑ It's difficult for desktop antivirus software to globally prevent the outbreak of viruses.



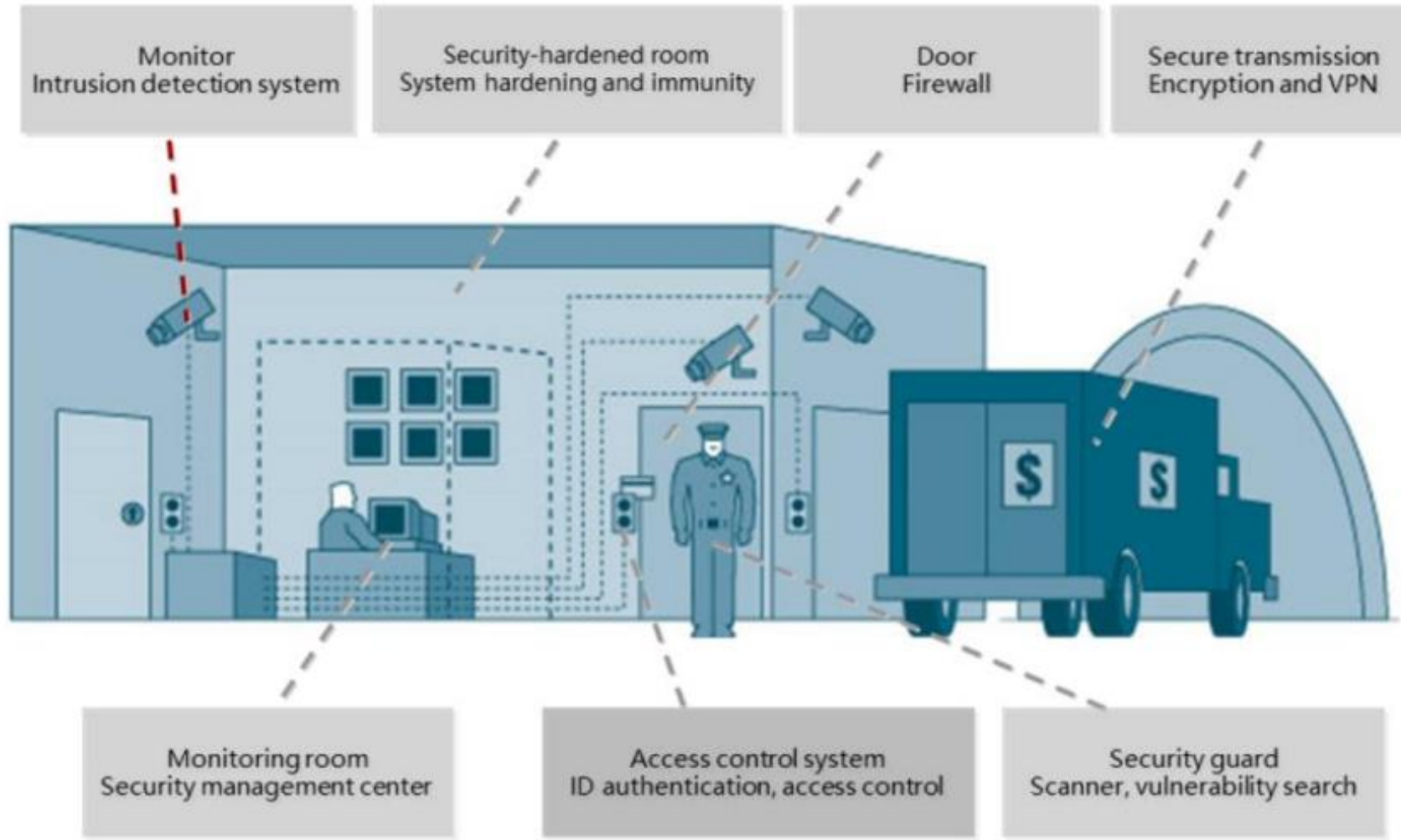
- What are the similarities of the preceding network threats?

Feature Threat	Unauthorized Access	Unauthorized Tampering	Unauthorized Damage
Hacker Intrusion	√	√	√
DoS Attack	√		√
Virus and Malware	√	√	√

- An intrusion is an unauthorized attempt to access information system resources, tamper with system data, and paralyze the system.
- The purpose of an intrusion is to compromise system integrity, confidentiality, availability, and controllability.

- **Typical intrusions:**
 - ☐ **Tampering with web pages**
 - ☐ **Cracking system passwords**
 - ☐ **Copying and viewing sensitive data**
 - ☐ **Obtaining user passwords using network sniffing tools**
 - ☐ **Accessing servers without authorization**
 - ☐ **Obtaining raw packets with special hardware**
 - ☐ **Implanting Trojan horses in hosts**

Positions of Security Devices in a Security System



- In the security system, the intrusion detection system (IDS) takes on the same role as a surveillance camera. It monitors and analyzes traffic across key nodes in the information system and learns of ongoing security events. The system administrator can use the IDS to obtain and analyze the traffic of key nodes for discovering and reporting anomalies and suspicious network behaviors.
- Intrusion detection inspects various operations as well as analyzing and auditing data and phenomena to detect intrusion behaviors in real time. It is a proactive and dynamic security defense technology that covers various authorized and unauthorized intrusion behaviors.
- The IDS can immediately start relevant security mechanisms once detecting security policy violation behaviors or evidence that the system is being attacked.
- Firewalls and IDS:
 - Firewalls are usually deployed in serial mode and are capable of rapid forwarding but not in-depth detection.
 - Firewalls can neither correctly analyze malicious code in application data flows nor detect malicious operations or mis operations of intranet users.
 - Firewalls perform coarse-grained access control, whereas the IDS provides fine grained detection, allowing the administrator to monitor the live network even more accurately.
 - The IDS can interwork with a firewall and switch to serve as a helpful assistant of the firewall for controlling interzone access.
 - The IDS can be manually or automatically updated, and its policies can be easily configured.

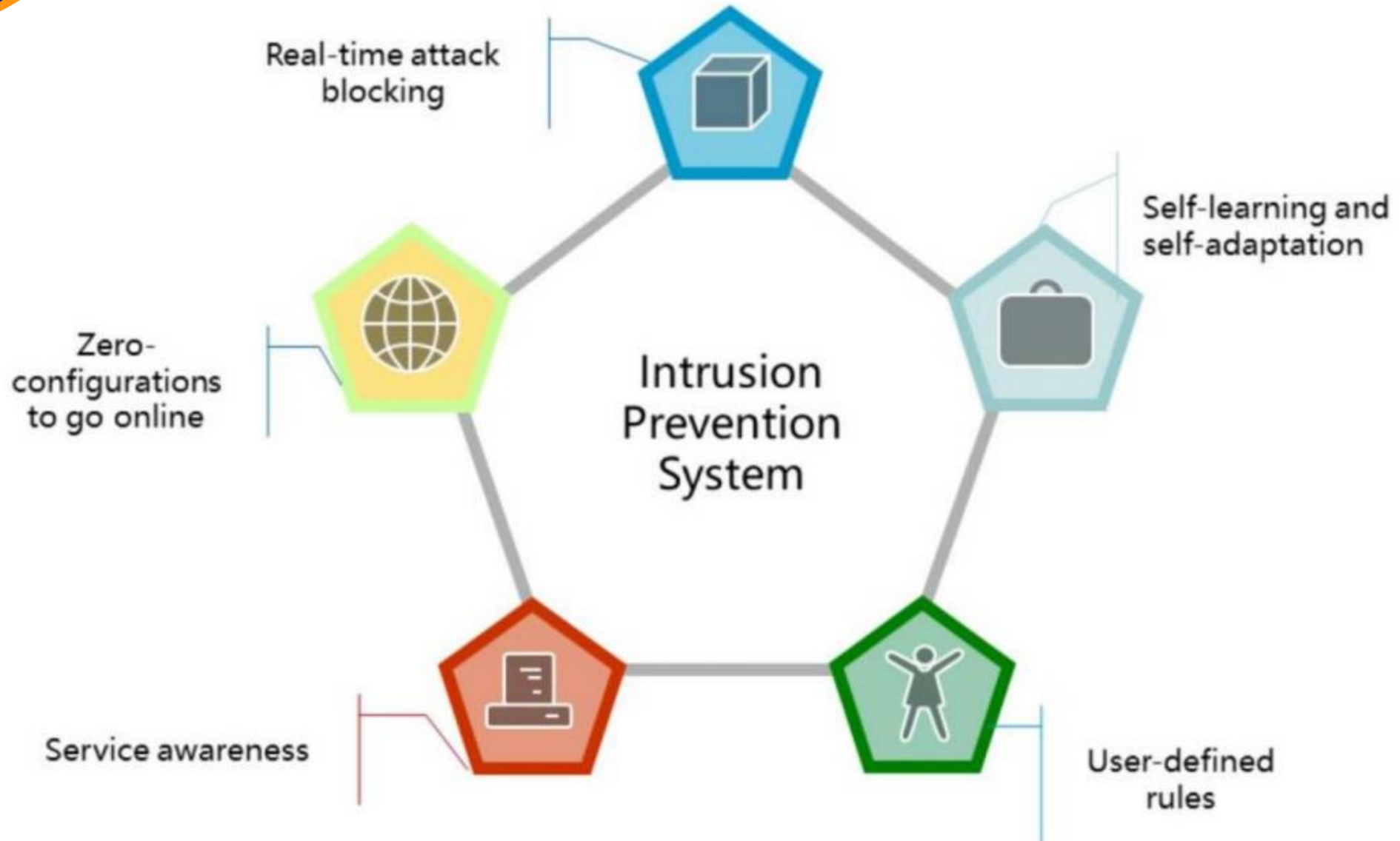
- The intrusion prevention system (IPS) is an intelligent intrusion detection and prevention product. As well as detecting intrusions, it also prevents and terminates intrusion behaviors using certain ways of responding, protecting the information system in real time against substantial attacks.
- The IPS can be deployed in the following modes:

Off-line

Deployed on the switch to perform port mirroring through the switch.

In-line

Deployed in serial mode to block the attacks in real time.



- The IPS has the following technical features:

- ❑ **Real-time blocking:** The IPS detects and blocks network attacks in real time, whereas the IDS can only detect attacks. Therefore, the IPS improves system security to the maximum extent.
- ❑ **Self-learning and self-adaptation:** The IPS minimizes the rate of false negatives and false positives through self-learning and self-adaptation to reduce the impact on services.
- ❑ **User-defined rules:** The IPS supports the customization of intrusion prevention rules to give the best possible response to the latest threats.
- ❑ **Service awareness:** The IPS can detect exceptions or attacks at the application layer.
- ❑ **Zero-configurations to go online:** The system provides a default intrusion prevention security profile that can be directly referenced.

Log

- Traffic Log
- Threat Log**
- URL Log
- Operation Log
- System Log

Threat Log List

Export Customize

View	Time	Threat Type	Risk Level	Threat ID	Threat Name
	2018/07/05 10:41:45	Intrusion	Low	1540	Cisco Common Services Frame...

[View Threat Log Details\(Intrusion\)](#) ?

Common Log Field

Time: 2018/07/05 10:41:45

Protocol: TCP

Security Policy: [untrust_trust](#)

Application Category: Network

Application Subcategory: Infrastructure

Application: [HTTP](#)

Threat

Threat Type: Intrusion

Intrusion Subtype: Attack intrusion

Threat Name: [Cisco Common Services Framewo...](#)

Threat ID: 1540

Occurrences: 1

Profile: [strict](#)

Action: Alert

Severity: Medium

Risk Level: Low

Target Type: Server

Operating System: all

Attack Category: XSS

Accessed Content: [/cwhp/device.center.do?device=sc...](#)

Source

Source Zone: untrust

Source Region: [unknown-zone](#)

Source Address: 172.16.8.47

Source Port: 2882

Destination

Destination Zone: trust

Destination Region: [unknown-zone](#)

Destination Address: 172.16.8.102

Destination Port: 1741

• Intrusion log information includes: virtual system, hit security policy, source and destination addresses, source and destination ports, source and destination Zones, user, protocol, application, hit intrusion prevention security profile, signature name, signature sequence number, event count, intrusion target, intrusion severity, operating system, signature category, and signature action. Of these, the following are particularly important:

- Profile: Hit intrusion security profile.
- Threat name: IPS signatures describe attack behavior features. The firewall compares the features of packets with the signatures to detect and defend against attacks.
- Event count: The field is used for merging logs. Whether logs are merged is determined by the merge frequency and conditions. The value is 1 if logs are not merged.
- Intrusion target: Indicates the attack target of a packet detected based on the signature, which can be:
 - server: The attack target is the server.
 - client: The attack target is the client.
 - both: The attack targets are the server and client.

- ☐ **Intrusion severity:** Indicates the severity of the attack caused by the packet detected based on the signature, which can be:
 - **Information**
 - **Low**
 - **Medium**
 - **High**

- ☐ **Operating system:** Indicates the operating system attacked by the packet detected based on the signature, which can be:
 - **All: all systems**
 - **Android - iOS**
 - **Unix-like**
 - **Windows**
 - **Other: other systems**

- ☐ **Signature category:** Indicates the threat category to which the packet attack detected based on the signature belongs.

- **Signature action, which can be:**
 - ☐ **Alert**
 - ☐ **Block**

- **Computer virus**

- **A computer virus is a set of self-replicable instructions or program code compiled independently or embedded in computer programs to adversely affect a computer's use by damaging its functions or data.**

- **Malicious code**

- **Malicious code is a program that covertly inlays code into another program to run intrusive or disruptive programs and damage the security and integrity of the data on an infected computer.**

- **Ways of categorizing computer viruses:**

- **By functions of malicious code: virus, worm, and Trojan horse**
 - **By transmission mechanisms: mobile media, network sharing, network scanning, email, and P2P network**
 - **By infected objects: operating system, application, and device**
 - **By carriers: executable file, script, macro, and boot area**

Item	Viruses	Worms	Trojan Horses
Existence	Parasitic	Independent	Parasitic
Replication Mechanism	Inserts into host programs	Self-replicating	Not self-replicating
Means of Infection	Running on host programs	System vulnerabilities	Based on carriers or functions
Infected Target	Mostly local files	Other computers on the network	Zombie hosts
Triggering Mechanism	Computer users	Programs	Remote control
Affected Target	File system	Network performance, system performance	Information theft, denial of service
Prevention Measure	Removing from host programs	Patching	Preventing Trojan horse implantation

- The relationships between viruses, worms, and Trojan horses are as follows:
 - A virus is a segment of malicious code that is parasitic on a normal program. When a user enables the normal program, the virus is also started, damaging the system's file system.
 - A worm is a variant of the virus. It is an independent entity that does not need to be parasitic. It can replicate itself and spread by exploiting system or intentional vulnerabilities, impacting the performance of the entire network and the computer system even more severely.
 - A Trojan horse is a kind of malicious code that is parasitic by nature, and is extremely covert. Hackers can usually control a host through a Trojan horse and make the host become a zombie. In addition, a Trojan horse can be used to monitor and obtain key information of a victim, such as a bank account password.
- When we talk about using an antivirus, we are referring to the mitigation of malicious code.

- Based on Zones, there are two types of antivirus technology:

- Single device antivirus
- Network antivirus

• Single-device antivirus can be implemented by installing antivirus software or professional antivirus tools. Virus detection tools detect malicious code, such as viruses, Trojan horses, and worms. Some detection tools can also provide the recovery function. Norton Antivirus from Symantec is a common antivirus software program, and the Process Explorer (see figure) is a professional antivirus tool.

- Network antivirus technology refers to deploying antivirus policies on a security gateway.

The screenshot shows the Windows Process Explorer window. Callouts point to specific columns: 'Process name' points to the 'Process' column, 'Capable of identifying any desktop program' points to the 'Process' column, 'Process description' points to the 'Description' column, and 'Process company' points to the 'Company Name' column.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	96.68	0 K	24 K	0		
System	0.18	48 K	1,228 K	4		
smss.exe	0.89	0 K	0 K	n/a	Hardware Interrupts and DPCs	
csrss.exe		284 K	824 K	284		
wininit.exe	< 0.01	1,432 K	3,448 K	384		
services.exe		956 K	3,376 K	440		
svchost.exe		4,440 K	7,688 K	564		
WmPvSE.exe		3,812 K	8,368 K	688	Host Process for Windows S...	Microsoft Corporation
WmPvSE.exe		8,236 K	13,256 K	2720		
unsecapp.exe		1,340 K	4,040 K	2884		
WmPvSE.exe		2,360 K	5,348 K	5876		
svchost.exe		5,172 K	9,072 K	768	Host Process for Windows S...	Microsoft Corporation
svchost.exe		18,776 K	19,652 K	856	Host Process for Windows S...	Microsoft Corporation
audiodg.exe		12,040 K	11,848 K	5168		
svchost.exe	< 0.01	5,888 K	12,316 K	920	Host Process for Windows S...	Microsoft Corporation
dmn.exe		1,552 K	4,312 K	2380	Desktop Window Manager	Microsoft Corporation
svchost.exe	0.06	28,116 K	33,084 K	948	Host Process for Windows S...	Microsoft Corporation
svchost.exe		6,180 K	11,860 K	1044	Host Process for Windows S...	Microsoft Corporation
svchost.exe		13,592 K	16,932 K	1176	Host Process for Windows S...	Microsoft Corporation
rdpclip.exe	0.03	2,672 K	6,892 K	1632	RDP Clip Monitor	Microsoft Corporation
spoolsv.exe		6,432 K	12,120 K	1304	Spooler SubSystemApp	Microsoft Corporation
svchost.exe		9,364 K	11,180 K	1344	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	9,284 K	14,104 K	1484	Host Process for Windows S...	Microsoft Corporation
ccSvcHst.exe	0.58	33,764 K	17,964 K	1540	Symantec Service Framework	Symantec Corporation
WmPvSE.exe	< 0.01	4,864 K	4,508 K	3964	Symantec Service Framework	Symantec Corporation
WmPvSE.exe	< 0.01	1,824 K	4,528 K	1668		
vmtoolsd.exe	0.18	73,268 K	79,908 K	1768	VMware Tools Core Service	VMware, Inc.
msiexec.exe		2,876 K	6,696 K	2144	Microsoft Distributed Transa...	Microsoft Corporation
ispvnc.exe		8,896 K	14,576 K	3148	Microsoft Software Protectio...	Microsoft Corporation
SearchIndexer.exe		29,028 K	24,472 K	3232	Microsoft Windows Search I...	Microsoft Corporation
taskhost.exe		7,900 K	7,664 K	3112	Host Process for Windows T...	Microsoft Corporation

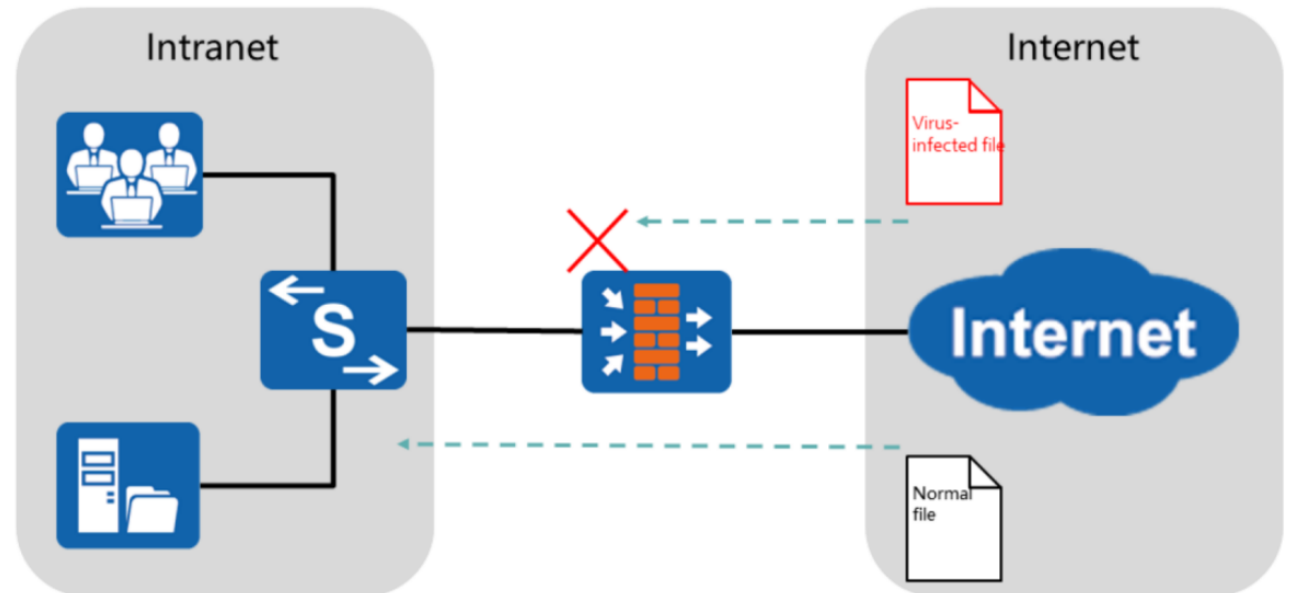
At the bottom of the window, system statistics are displayed: CPU Usage: 3.32%, Commit Charge: 19.90%, Processes: 42, Physical Usage: 42.00%.

- Antivirus is used for network security in the following scenarios:

- ☐ Intranet users can access the Internet and need to frequently download files from the Internet
- ☐ Servers deployed on the intranet need to frequently receive files uploaded by Internet users.

• As shown in the figure, the NIP serves as a gateway device that isolates the intranet from the Internet. There are user PCs and a server on the intranet. Intranet users can download files from the Internet, and Internet users can upload files to the intranet server. To secure the files to be uploaded or downloaded, the antivirus function should be configured on the NIP.

• After the antivirus function is configured, the NIP only permits secure files to be transferred into the intranet. If a virus is detected in a file, the NIP applies the action, such as block or alert, to the file.



- Proxy scanning mode

- All data packets passing through the gateway that require virus detection are transparently transmitted to the gateway's protocol stack for caching, and then sent to the virus detection engine.

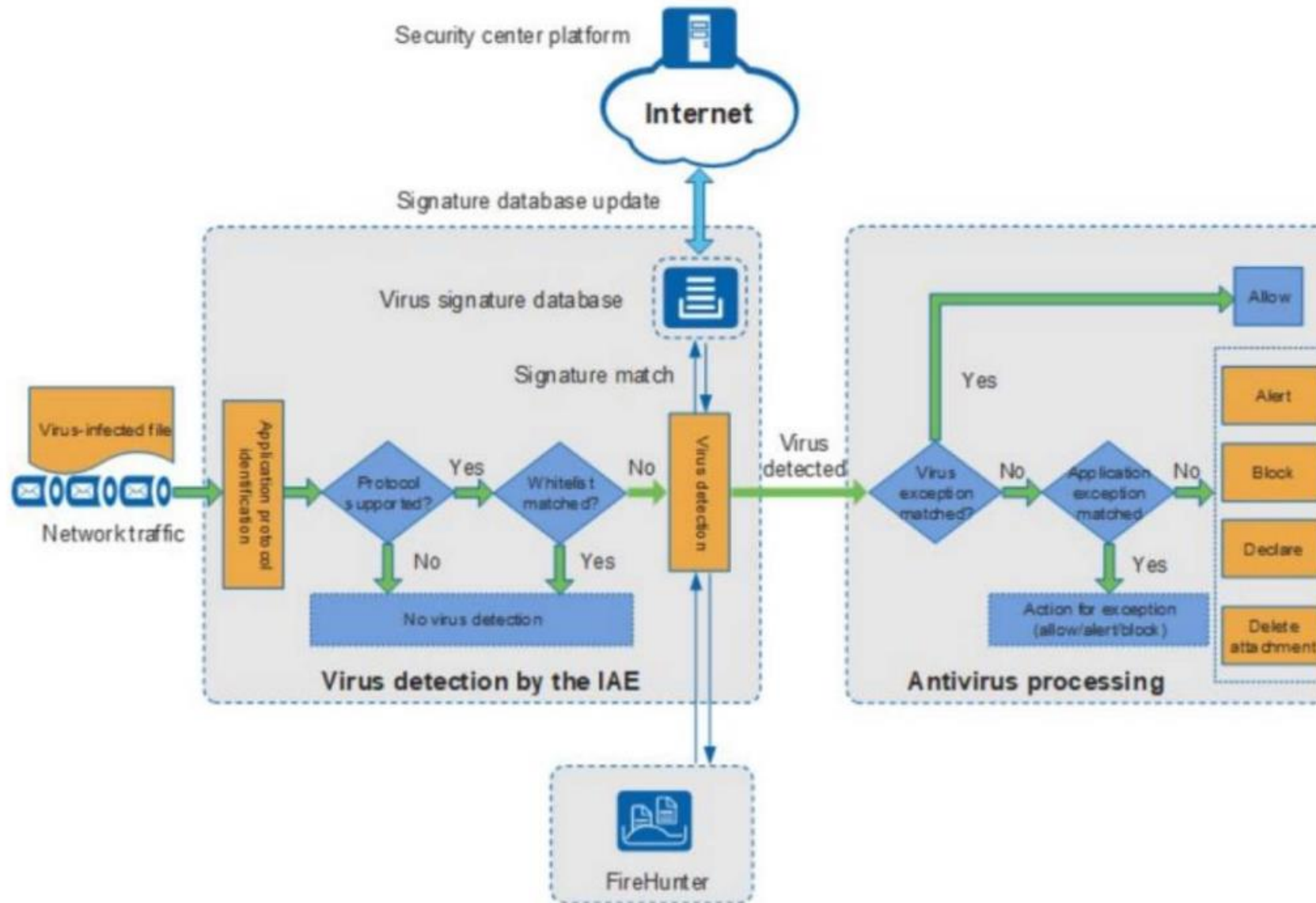
- Flow scanning mode

- File signatures are extracted for matching against the local signature database. This mode relies on stateful inspection and protocol parsing technologies.

- Currently, device vendors (including UTM and AVG) provide two antivirus scanning modes: proxy scanning and flow scanning.

- A proxy antivirus gateway performs more advanced operations, such as decompression and unpacking, with a high detection rate. However, performance and system overheads are large because all files are cached.

- A flow antivirus gateway has high performance and low system overhead but low detection rate, failing to cope with shelled and compressed files.



- **Actions taken by the firewall when a virus is detected:**
 - ❑ **Alert:** The device permits the virus-infected file and generates a virus log.
 - ❑ **Block:** The device blocks the virus-infected file and generates a virus log.
 - ❑ **Declare:** For a virus-infected email message, the device permits it but adds information to the email body to announce the detection of viruses and generates a virus log. This action applies only to SMTP and POP3.
 - ❑ **Delete Attachment:** The device deletes malicious attachments in the infected email message, permits the message, generates a log, and adds information to the email body to announce the detection of viruses and deletion of attachments. This action applies only to SMTP and POP3.

- After a virus is detected by the firewall, you can view the detailed antivirus results in the service log.
- After antivirus for HTTP and email protocol is configured, you can view relevant information in the access page or email body.

The screenshot displays the firewall's Threat Log interface. On the left, a sidebar lists log types: Threat Log (highlighted), URL Log, Operation Log, and System Log. The main area shows a table of threats with columns: View, Time, Threat Type, Risk Level, Threat ID, and Threat Name. A threat is listed with Time: 2018/08/29 15:59:23, Threat Type: Virus, Risk Level: Relatively high, Threat ID: 16424404, and Threat Name: EICAR.Test.FILE.1. Below the table, a 'View Threat Log Details(Virus)' window is open, showing detailed information in three sections: Common Log Field, Threat, and Source/Destination.

Common Log Field		Threat	
Time:	2018/08/29 15:59:23	Threat Type:	Virus
Protocol:	TCP	Threat Name:	EICAR.Test.FILE.1
Security Policy:	ftp	Threat ID:	16424404
Application Category:	Network	Occurrences:	1
Application Subcategory:	Infrastructure	Profile:	av
Application:	FTP	Action:	Block
		File Name:	eicar_com.zip+eicar.com
		File Type:	com
		Accessed Content:	
		Hash Value:	267D772D8ED87333

Source		Destination	
Source Zone:	untrust	Destination Zone:	trust
Source Region:	unknown-zone	Destination Region:	unknown-zone
Source Address:	10.1.2.100	Destination Address:	10.1.1.100
Source Port:	21	Destination Port:	58219

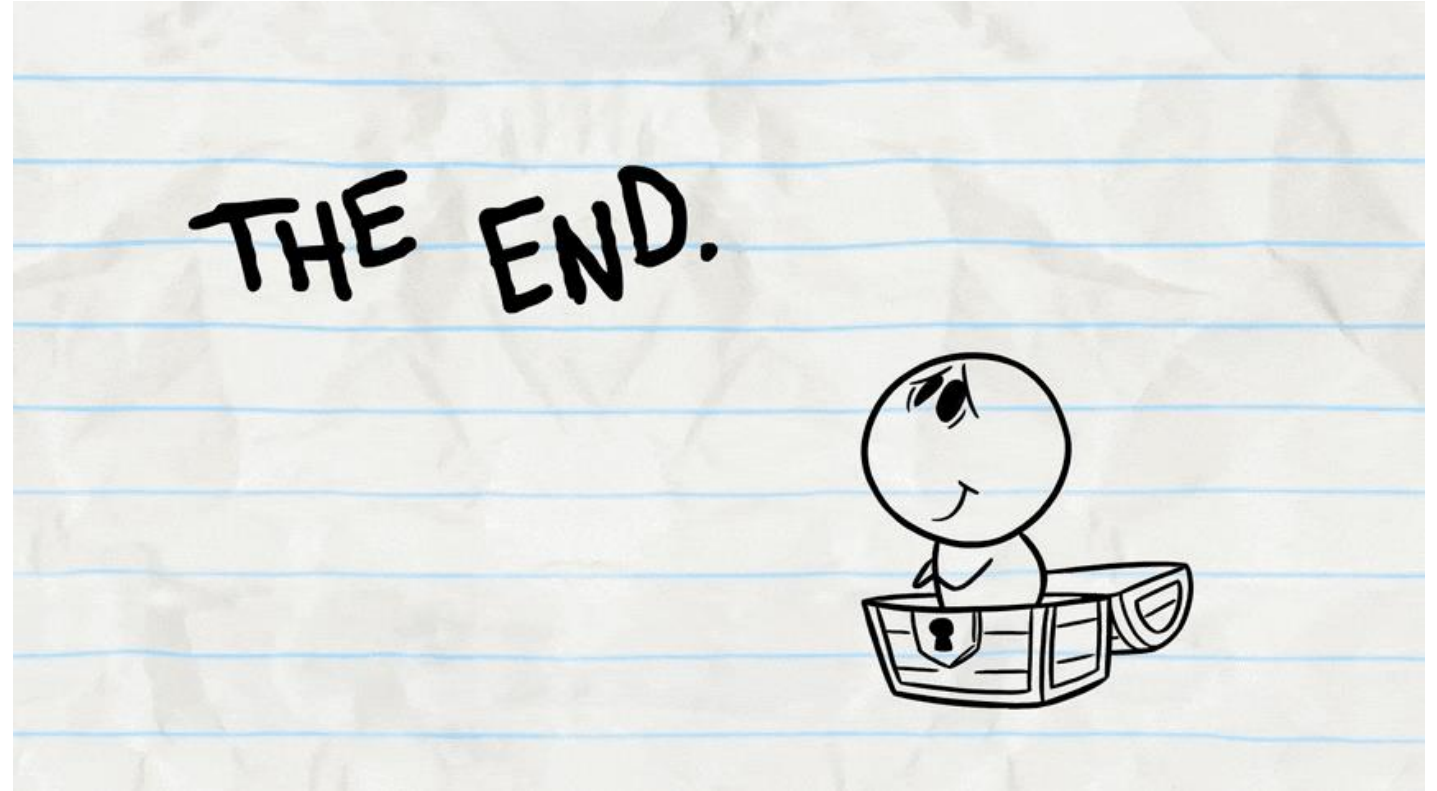
Below the logs, an email body is shown from libai@security.com to dufu, dated 2017-07-13 10:03. The email contains a warning message about a virus in an attachment. A red box highlights the warning text, and a callout bubble points to it with the text 'Mail antivirus prompt'.

Warning:
eicar_com.zip is deleted from the mail because it contains virus.

The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY