معهد العراب العالي للتدريب

مقدمة في أمن الشبكات

م. ميسون الرحماني

أمن الشبكات "Network Security"

يعتبر هذا المقرر مقدمة للمفاهيم الأمنية الأساسية لأمن الشبكات، حيث يتم التعرف على التهديدات وهجمات الشبكة الشائعة، ثم التدرب على تأمين أجهزة الشبكة ومنح الصلاحيات، وتطبيق بروتوكول الثقة وتقنية التعرف على الهوية وسلامة المعلومات، وكيفية صد الاختراقات باستخدام جدار حماية، وكذلك التعرف على أنظمة منع الاختراق، كما يتم التدرب على تأمين الشبكات المحلية.

الهدف العام:

يهدف هذا المقرر إلى اكساب المتدرب المعارف والمهارات الأساسية اللازمة لتأمين الشبكة وصد الاختراقات باستخدام جدار الحماية وأنظمة منع الاختراق.

الأهداف التفصيلية:

أن يكون المتدرب قادرًا على أن:

١- يصف أنواع مختلفة من أدوات الهجوم المستخدمة من قبل المخترقين
٢- يصف البرمجيات الخبيثة
٣- يشرح هجمات الشبكة الشائعة
٤- يصف الأساليب والإمكانيات اللازمة لحماية الشبكات
٥- يصف التقنيات المستخدمة للحد من هجمات الشبكة الشائعة
٦- يهيئ الوصول الإداري الأمن لأجهزة التوجيه
٧- يعد خاصية الثقة وتقنية التعرف على الهوية
٨- يهيئ الخواص الأمنية لجدار الحماية
٩- يهيئ الخواص الأمنية في جهاز أنظمة منع الاختراق
١٠- يهيئ الخواص الأمنية المتعلقة بالشبكة المحلية

الحفاظ على السرية ليس كافي، يجب أيضًا
ضمان التوافر والنزاهة

معهد العراب العالي للتدريب

01

المحاضرة الأولى

2024

محتويات المحاضرة

1. التعرف على أمان الشبكة
2. إدارة مخاطر الشبكة
3. أنواع هجمات الشبكة
4. Intrusion Detection Systems
5. أنواع (VPN)

أمان الشبكة

أمان الشبكة
هو حماية البنية التحتية للشبكات الأساسية من الوصول غير المصرح به أو سوء الاستخدام أو السرقة، يتضمن إنشاء بنية تحتية آمنة للأجهزة والتطبيقات والمستخدمين للعمل بطريقة آمنة.
يجمع أمان الشبكة بين طبقات متعددة من الدفاعات على الحافة وفي الشبكة، تقوم كل طبقة أمان شبكة بتنفيذ السياسات وعناصر التحكم.
يحصل المستخدمون المصرح لهم على حق الوصول إلى موارد الشبكة، ولكن يتم حظر الجهات الفاعلة الضارة من تنفيذ الاستغلال والتهديدات.

إدارة مخاطر الشبكة

قياس المخاطر
مخاطر منخفضة
مخاطر متوسطة
مخاطر عالية
على سبيل المثال: يحتوي النظام الداخلي على ثغرة أمنية في نظام البريد الخاص به
من الخارج يجب على المهاجم العثور على النظام من خلال جدار حماية الإنترنت.
لا يمكن الوصول إلى النظام عبر نقطة الوصول هذه ، لذلك لا يوجد خطر.

التهديد

هو إجراء أو حدث قد ينتهك أمن بيئة نظم المعلومات،
هناك ثلاثة مكونات للتهديد: الهدف والعملاء والأحداث.

المخاطر

هي المفهوم الأساسي الذي يشكل الأساس لما نسميه "الأمن"
الخطر هو احتمال الخسارة التي تتطلب الحماية، إذا لم يكن هناك خطر فلا داعي للأمن.

القاعدة العامة للأمن المادي هو ضرورية الحماية المادية للأصول مثل السجلات الورقية والإلكترونية.

COMSEC(أمن الاتصالات) - ضروري لحماية المعلومات أثناء النقل والتداول.

EMSEC(أمن الانبعاثات) - يحمي من مراقبة وإعتراض الإشعاعات الكهرومغناطيسية.

COMPUSEC (أمن الحاسبات) – ضروري للتحكم في الوصول إلى أنظمة الكمبيوتر الخاصة بنا.

NETSEC(أمن الشبكات) - يؤمن الاتصالات عبر الشبكات.

INFOSEC (أمن المعلومات) - نهج شامل لحماية أصول المعلومات.

أنواع هجمات الشبكة

أنواع هجمات الوصول:

- التنصت
- التطفل

كيف يتم تنفيذ هجمات الوصول؟

يمكن استخراج المعلومات وتخزينها من خلال مصادر متنوعة، مثل:

- ملفات النظام والمستندات المخزنة على أجهزة الكمبيوتر
- الذاكرة المؤقتة والبيانات المتبقية في الطابعات
- التخزين طويل الأجل كالأقراص الصلبة والوسائط الأخرى

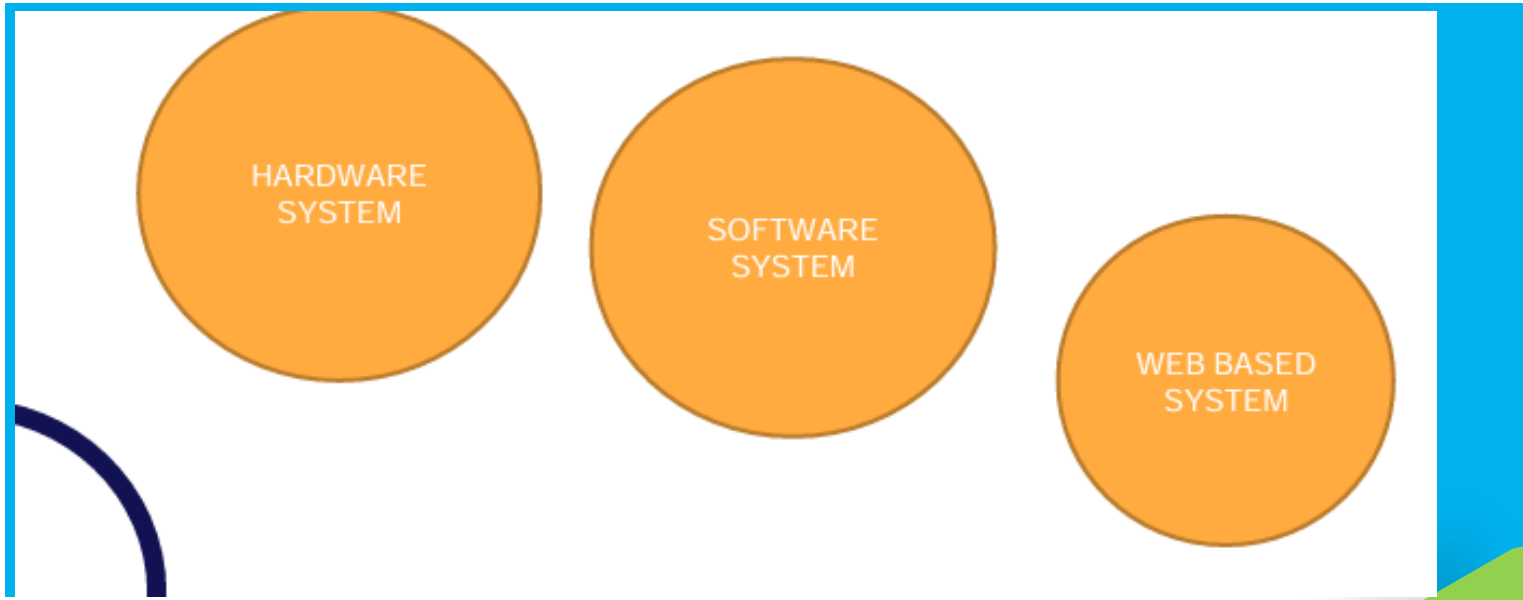
وبالتالي فإن هجمات الوصول تستهدف الحصول على هذه المعلومات دون تصريح.

Intrusion Detection Systems

أنظمة اكتشاف التسلل

قد تشمل التدابير المضادة ما يلي:
-جدران الحماية، برامج مكافحة الفيروسات، ضوابط الوصول، أنظمة المصادقة الثنائية، الشارات، القياسات الحيوية قارئات البطاقات للوصول إلى المرافق، الحراس، عناصر التحكم في الوصول إلى الملفات، التشفيرالموظفون المدربون تدريبًا جيدًا، أنظمة كشف التسلل، أنظمة إدارة التصحيح الآلي والسياسة.
ومن أجل الرقابة منع الموظفين الداخليين من الدخول إلى الشبكة خلال الفترات الأمنية.
تقديم A presentation to management about risk
يجب أن يظهر الضرر الذي قد تتعرض له المنظمة.

أنواع VPN(virtual Private Network)



سؤال و إجابة

1- حماية البنية التحتية للشبكات اللاسلكية من الوصول غير المصرح به أو سوء الاستخدام

A. امن الشبكات

B. الحوسبة السحابية

C. الافتراضية

2- إجراء أو حدث قد يهدد أمن بيئة نظم المعلومات.
فالثلاثة مكونات هي: الهدف والعملاء والأحداث

A. التهديدات

B. المخاطر

معهد العراب العالي للتدريب

شكرًا

معهد العراب العالي للتدريب

مقدمة في امن الشبكات

م. ميسون الرحماني

معهد العراب العالي للتدريب

02

المحاضرة الثانية

2024

محتويات المحاضرة

1. Security CIA
2. إدارة مخاطر الشبكة
3. تصميم امن الشبكة

ما هو امن الشبكة

أمان الشبكة هو حماية البنية التحتية للشبكات الأساسية من الوصول غير المصرح به أو سوء الاستخدام أو السرقة. يتضمن إنشاء بنية تحتية آمنة للأجهزة والتطبيقات والمستخدمين والتطبيقات للعمل بطريقة آمنة. يجمع أمان الشبكة بين طبقات متعددة من الدفاعات على الحافة وفي الشبكة. تقوم كل طبقة أمان شبكة بتنفيذ السياسات وعناصر التحكم. يحصل المستخدمون المصرح لهم على حق الوصول إلى موارد الشبكة ، ولكن يتم حظر الجهات الفاعلة الضارة من تنفيذ الاستغلال والتهديدات.

- **الخصوصية:** "هل نظامي محمي من هجمات العالم الخارجي، و الدخول الغير مصرح؟"
  - حماية البيانات من الوصول الغير مصرح لها، فقط من يملكون الصلاحية يستطيعون رؤيتها.

- **النزاهة:** "هل تم التلاعب في بياناتي أو إفسادها أو تأثرها من تهديد خارجي؟"
  - التأكد من صحة المعلومات و عدم التحريف فيها وأن مصدر المعلومات حقيقي.

- **الإتاحة:** "هل يمكن الوصول بسهولة الى أنظمتي وبياناتي للإستخدام اليومي؟"
  - المعلومات متاحة للأشخاص المصرح لهم.

الخصوصية	النزاهة	الإتاحة
Encryption - التشفير إدارة عملية الدخول: • المعرف - الأسم • المصادقة - الرقم السري • تفويض - الإذن Steganography - اخفاء البيانات: • الرسائل الخفية داخل الموقع • الرسائل الخفية داخل الملفات و الصور	**التأكد من عدم العبث بالبيانات** **التشفير** إنشاء كود مشتق من خلال خوارزمية، اذا تم تغيير البيانات، فسيتم تغيير الكود في المستقبل ايضًا **توقيع رقمي، شهادة** ارسال توقيع رقمي فريد، بتوضيح من ارسل الرسالة ومن يسمح للمستلم بقراءتها	**ضمان إمكان استرداد البيانات عند الحاجة إليها** • أي فشل في SPOF يتوقف النظام بإكمله عن العمل • تكرار القرص • تكرار الخوادم • النسخ الإحتياطية • الطاقة البديلة • التوقي

إدارة مخاطر الشبكة

- Assets الاصول
- Vulnerability الثغرات
- Threats التهديدات
- Impact التأثير

- Assets

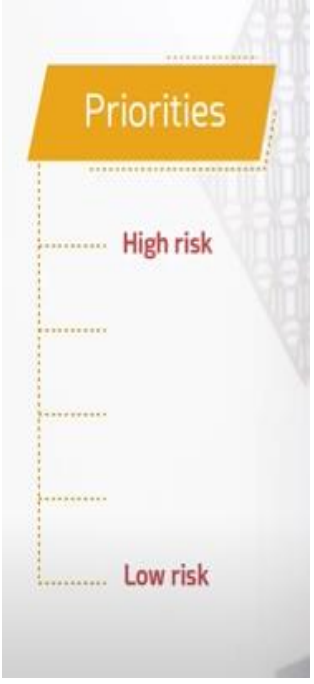
- Vulnerability

- Threats

- Impact

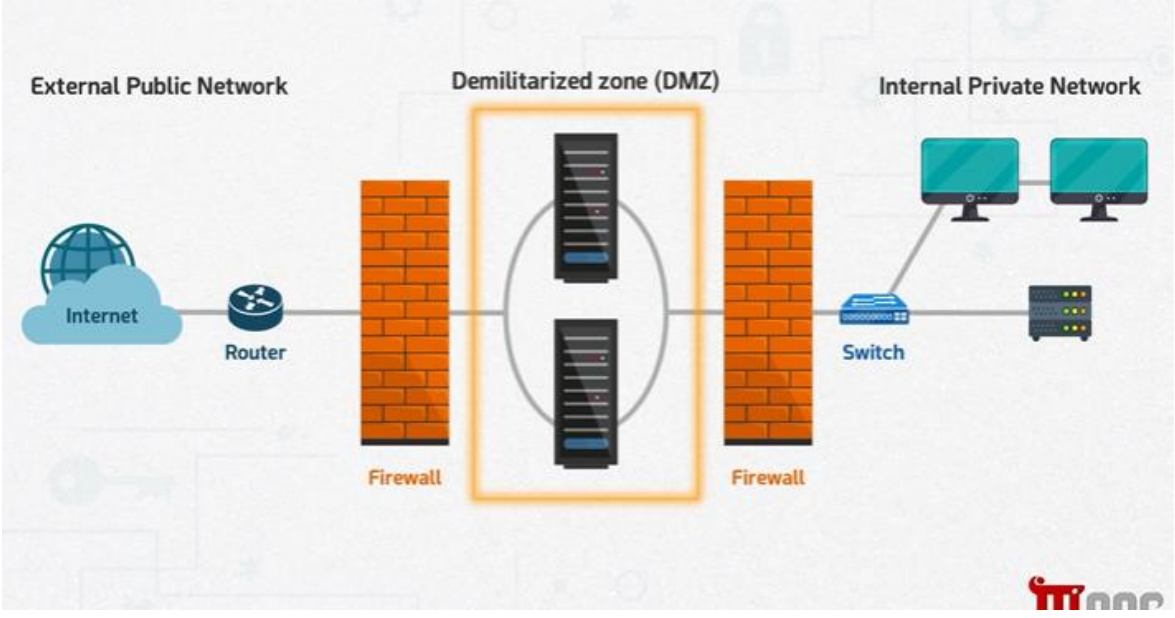
حساب RISK


Risk
=
Threats
×
Vulner-
-ability
×
Impact

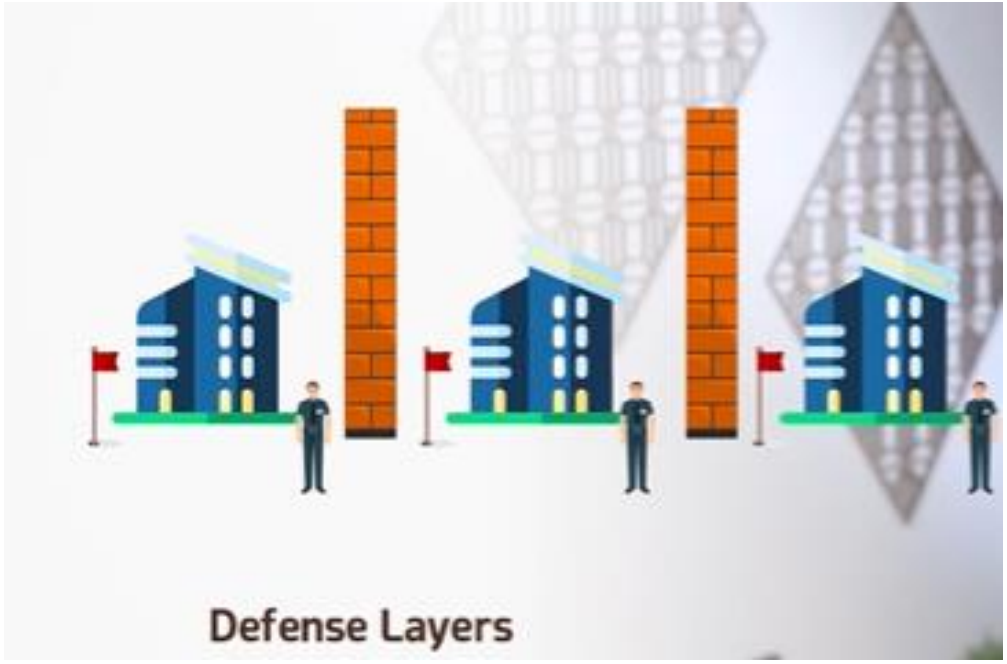

Priorities
High risk
Low risk

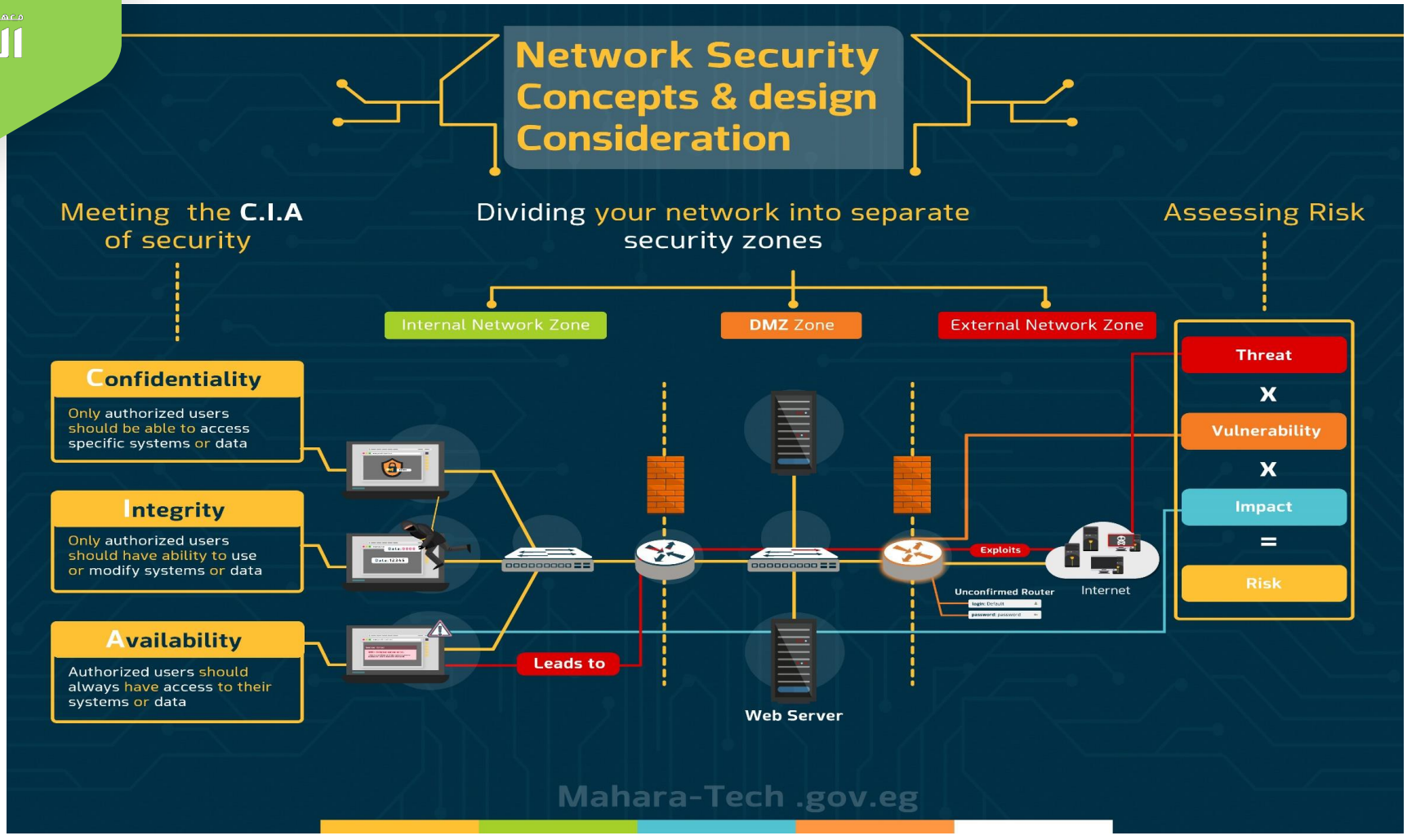
تصميم امن الشبكة

1- تقسيم الشبكة



2- الدفاع في العمق




Network Security Concepts & design Consideration
Meeting the C.I.A of security
Dividing your network into separate security zones
Assessing Risk
Internal Network Zone
DMZ Zone
External Network Zone
Confidentiality
Only authorized users should be able to access specific systems or data
Integrity
Only authorized users should have ability to use or modify systems or data
Availability
Authorized users should always have access to their systems or data
Leads to
Exploits
Unconfirmed Router
Internet
Web Server
Threat
X
Vulnerability
X
Impact
=
Risk
Mahara-Tech .gov.eg

معهد العراب العالي للتدريب

مقدمة في امن الشبكات

م. ميسون الرحماني

معهد العراب العالي للتدريب

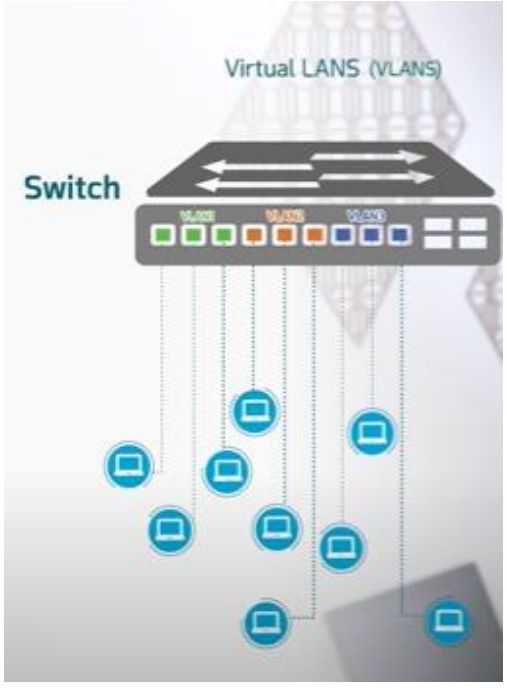
03

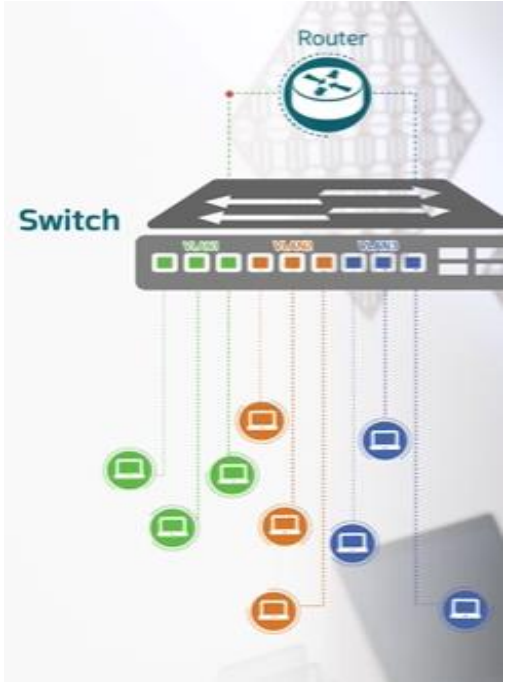
المحاضرة الثالثة

2024

Network segmentation and monitoring

Segmentation

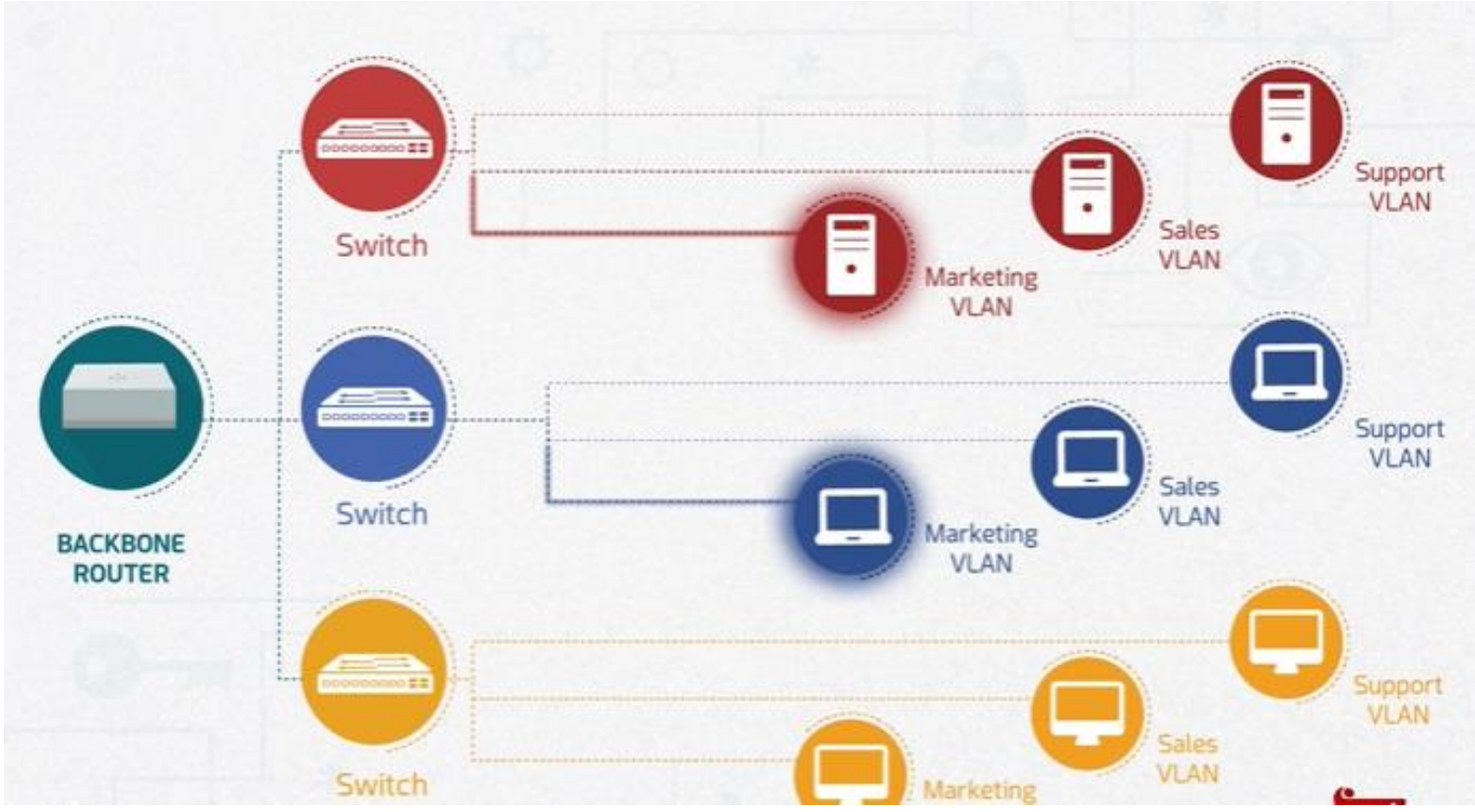




Vlan

Intervlan

- On-Sticky
- legacy


Switch
Marketing VLAN
Sales VLAN
Support VLAN
BACKBONE ROUTER
Switch
Marketing VLAN
Sales VLAN
Support VLAN
Switch
Marketing
Sales VLAN
Support VLAN

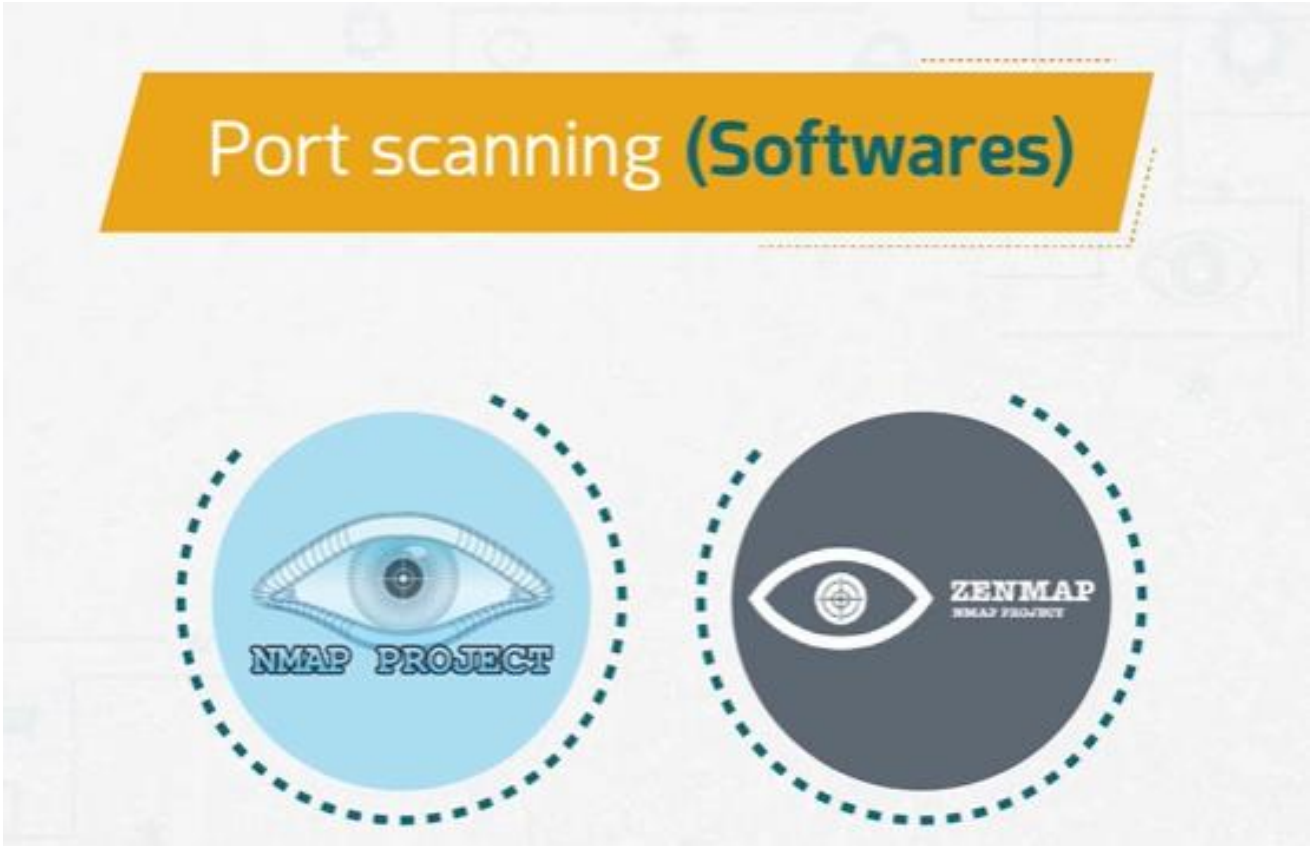
Monitoring:

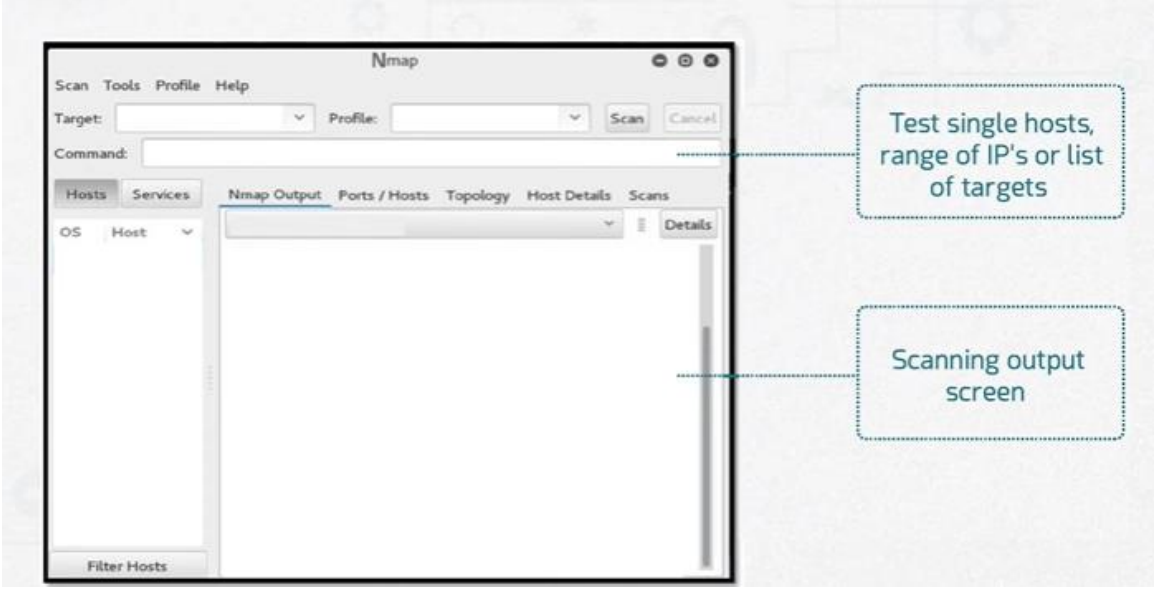
- Port Scanning and tools.
- Sniffing.

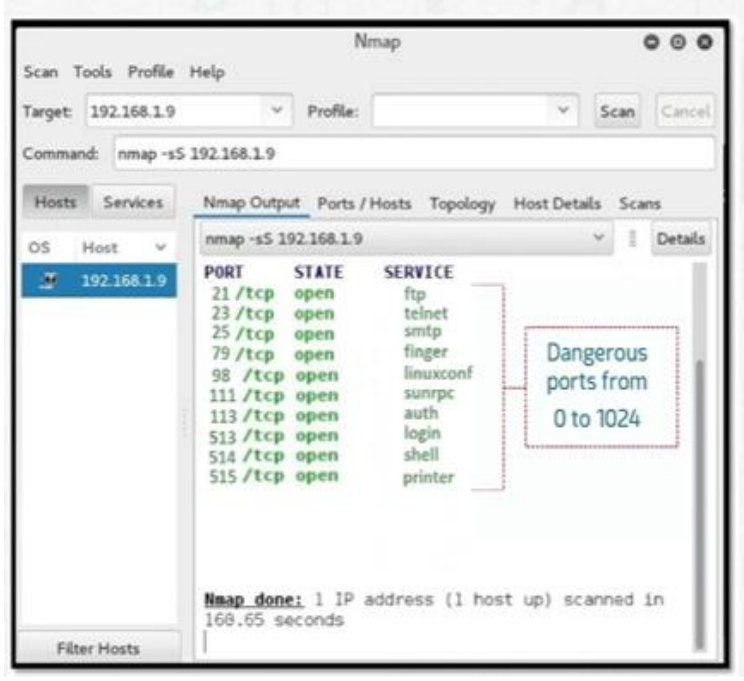
Port scan

- الهجوم السلبى
- الهجوم الإيجابي

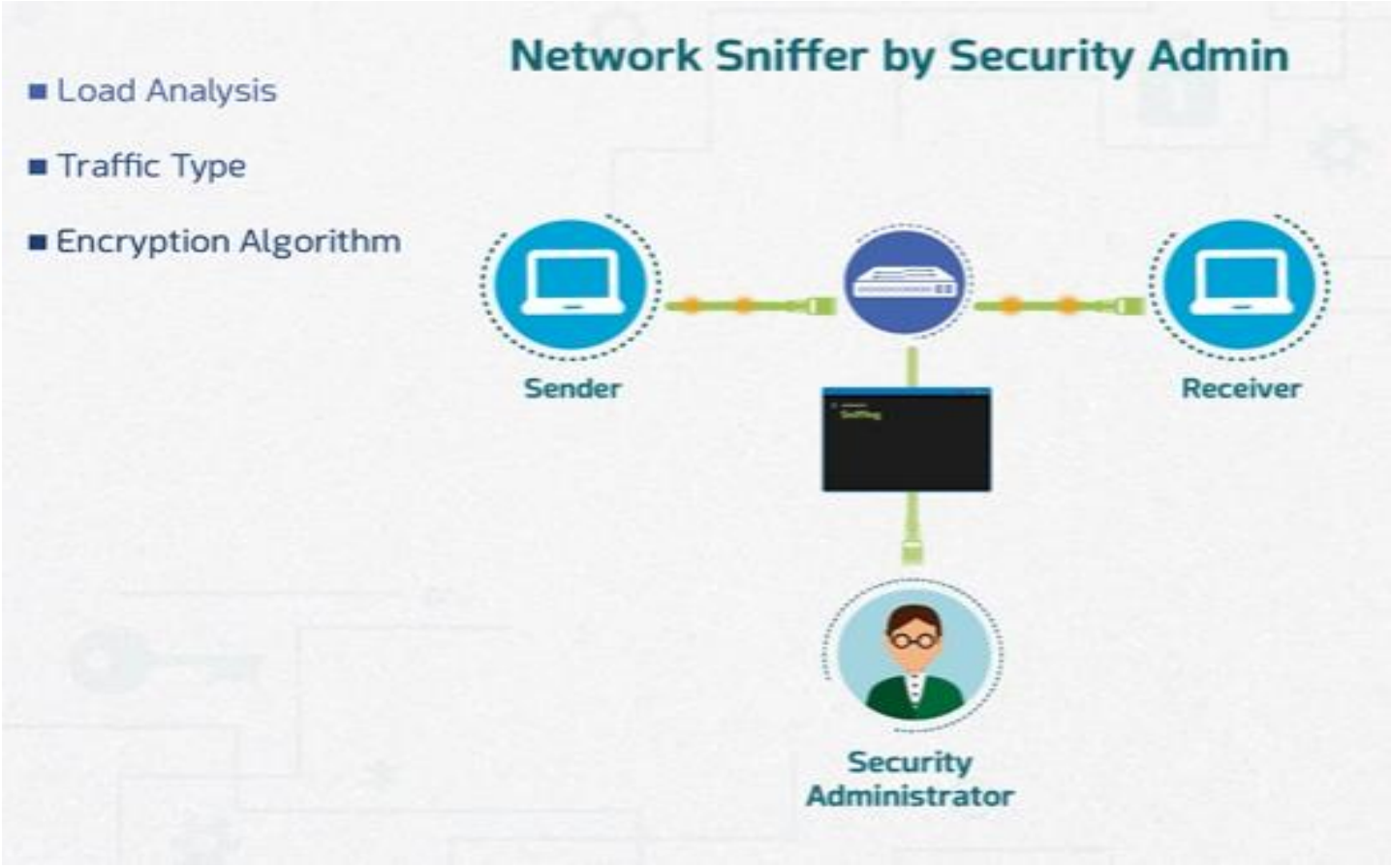
Download Zenmap




Nmap
Scan Tools Profile Help
Target:
Profile:
Scan
Cancel
Command:
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
Details
Filter Hosts
Test single hosts, range of IP's or list of targets
Scanning output screen


Nmap
Scan Tools Profile Help
Target: 192.168.1.9
Profile:
Scan
Cancel
Command: nmap -sS 192.168.1.9
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
192.168.1.9
nmap -sS 192.168.1.9
Details
PORT STATE SERVICE
21 /tcp open ftp
23 /tcp open telnet
25 /tcp open smtp
79 /tcp open finger
98 /tcp open linuxconf
111 /tcp open sunrpc
113 /tcp open auth
513 /tcp open login
514 /tcp open shell
515 /tcp open printer
Dangerous ports from 0 to 1024
Nmap done: 1 IP address (1 host up) scanned in 160.65 seconds
Filter Hosts

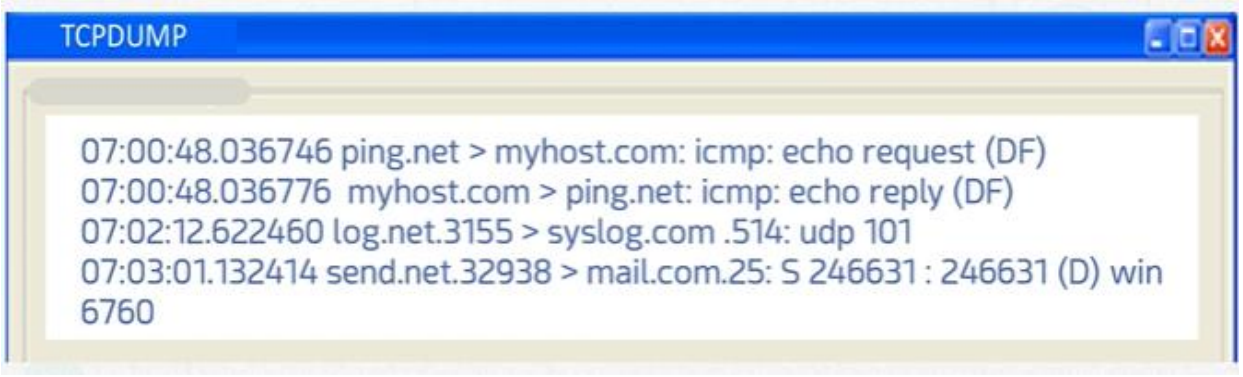
Sniffing التنصت



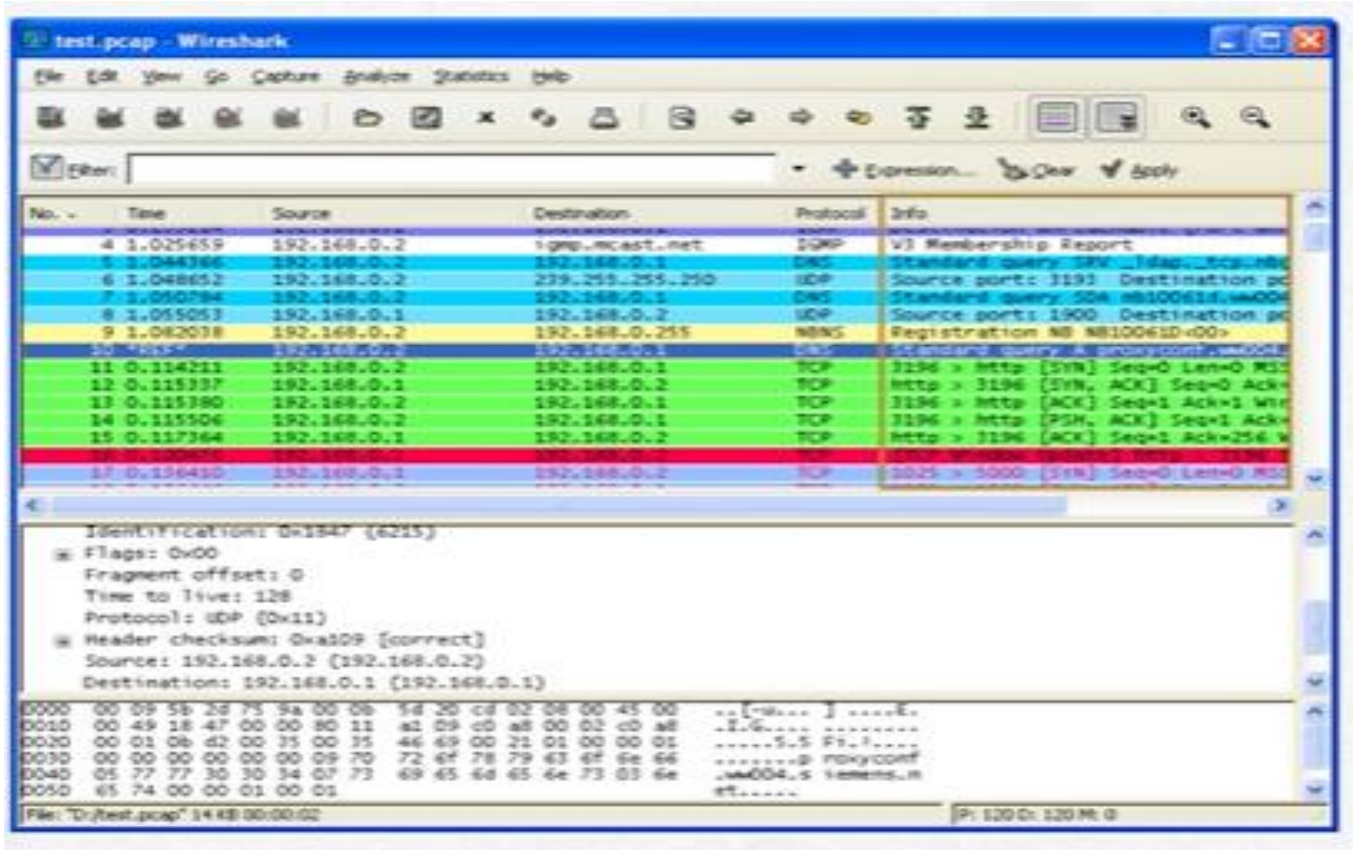
Sniffing Tools

TcpDUMP


TCPDUMP
IP source address
IP destination address
TCP Protocol
Packet


TCPDUMP
07:00:48.036746 ping.net > myhost.com: icmp: echo request (DF)
07:00:48.036776 myhost.com > ping.net: icmp: echo reply (DF)
07:02:12.622460 log.net.3155 > syslog.com .514: udp 101
07:03:01.132414 send.net.32938 > mail.com.25: S 246631 : 246631 (D) win 6760

Wireshark


test.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
4 1.025659 192.168.0.2 igmp.mcast.net IGMP V3 Membership Report
5 1.044366 192.168.0.2 192.168.0.1 DNS Standard query SRV _ldap._tcp.nb
6 1.048652 192.168.0.2 239.255.255.250 UDP Source port: 3193 Destination po
7 1.050794 192.168.0.2 192.168.0.1 DNS Standard query SOA nb100610.ww004
8 1.055053 192.168.0.1 192.168.0.2 UDP Source port: 1900 Destination po
9 1.082038 192.168.0.2 192.168.0.255 NBNS Registration NB NB100610<00>
10 1.109474 192.168.0.2 192.168.0.1 DNS Standard query A proxycomf.ww004
11 0.114211 192.168.0.2 192.168.0.1 TCP 3196 > http [SYN] Seq=0 Len=0 MSS
12 0.115337 192.168.0.1 192.168.0.2 TCP http > 3196 [SYN, ACK] Seq=0 Ack=
13 0.115380 192.168.0.2 192.168.0.1 TCP 3196 > http [ACK] Seq=1 Ack=1 Win
14 0.115506 192.168.0.2 192.168.0.1 TCP 3196 > http [PSH, ACK] Seq=1 Ack=
15 0.117364 192.168.0.1 192.168.0.2 TCP http > 3196 [ACK] Seq=1 Ack=256 W
16 0.130475 192.168.0.1 192.168.0.2 TCP [TCP Window Update] http > 3196
17 0.136410 192.168.0.2 192.168.0.1 TCP 3025 > 5000 [SYN] Seq=0 Len=0 MSS
Identification: 0x1947 (6215)
Flags: 0x00
Fragment offset: 0
Time to live: 128
Protocol: UDP (0x11)
Header checksum: 0xa1D9 [correct]
Source: 192.168.0.2 (192.168.0.2)
Destination: 192.168.0.1 (192.168.0.1)
0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00 ..[-u...] .....E.
0010 00 49 18 47 00 00 80 11 a1 d9 c0 a8 00 02 c0 a8 .I.G.... ....
0020 00 01 0b d2 00 35 00 35 46 69 00 21 01 00 00 01 .....5.5 Fi.!....
0030 00 00 00 00 00 00 09 70 72 6f 78 79 63 6f 6e 66 ....p roxycomf
0040 05 77 77 30 30 34 07 73 69 65 6d 65 6e 73 03 6e .ww004.s iemens.n
0050 65 74 00 00 01 00 01 et.....
File: "D:\test.pcap" 14 KB 00:00:02
P: 120 D: 120 M: 0

Network Scanning & Segmentation

Network Scanning

Type: Port Scanning | Sniffing

Definition

Scanning network with no permission by a hacker

The process of:

- Identifying open TCP/UDP ports on a system.
- identifying the operating system running on a host (OS fingerprinting)

The process of scanning and monitoring of the captured data packets passing through a network using sniffers.

Software tools

1. **NMAP PROJECT**

Features:
port scanner tool
Service identification
IP address detection
operating system detection
Supported by many operating systems (Unix, Windows, Linux)

2. **ZENMAP**

Features:
Newer version with GUI

1. **TCPDUMP**

Features:
Runs primarily on Unix
Helps in the analysis of network traffic (TCP, UDP, ICMP)

2. **WIRESHARK**

Features:
Protocol analyzer and sniffer
Capture and identify TCP/UDP traffic

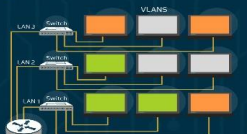
Countermeasures

Scanning network with permission by security administrator

- Security administrator should run a port scanning tool to detect and stop any port scanning activity on the network.
- The firewall should carry out stateful inspection to examine the packet header.
- Only needed ports should be kept open, unused ports should be closed.
- Security administrator should use sniffing tools to be aware of what potential attackers can see on the network.
- Using strong encryption methods.

Segmentation

More protection can be provided by separating the critical systems on the network through VLAN



A virtual LAN (VLAN) takes a large physical switch and regardless of where systems are plugged in, segment them into different networks based on function or access required.

So if a single system becomes infected, you can prevent it from connecting to critical networks and stop it from spreading to a large number of hosts through VLANs.

معهد العراب العالي للتدريب

مقدمة في أمن الشبكات

م. ميسون الرحماني

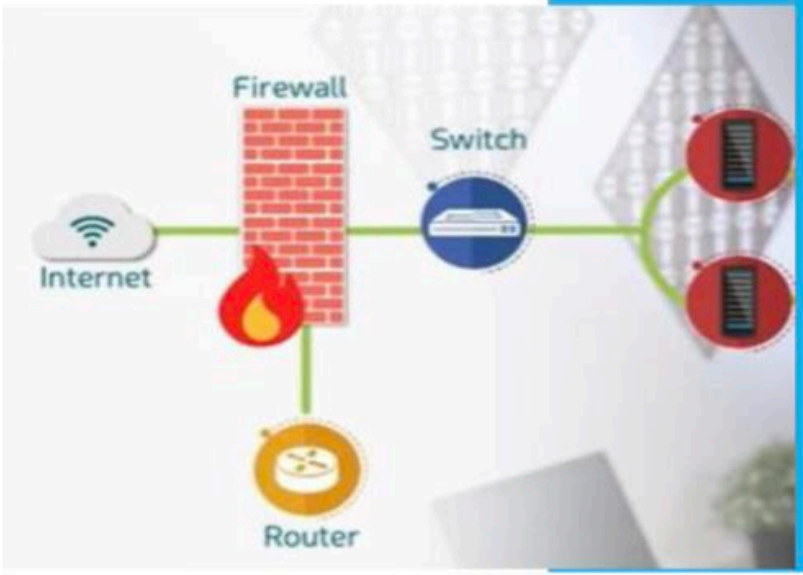
معهد العراب العالي للتدريب

المحاضرة الرابعة

04

2024

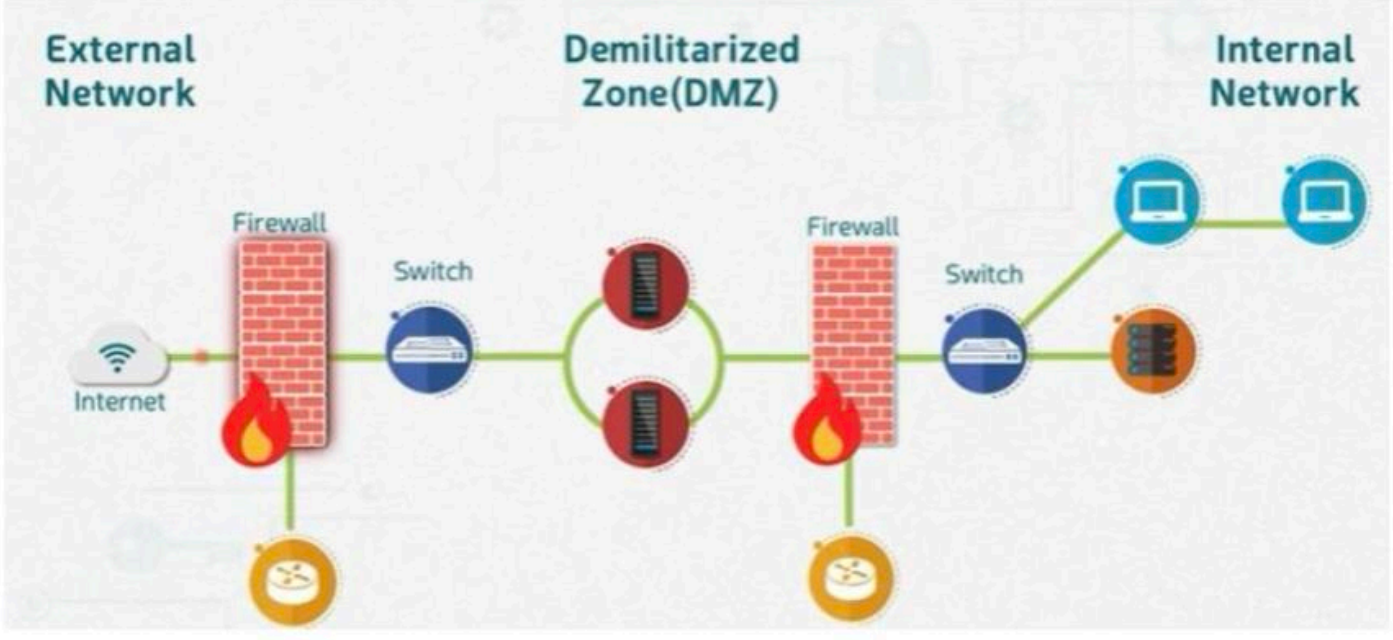
Firewalls

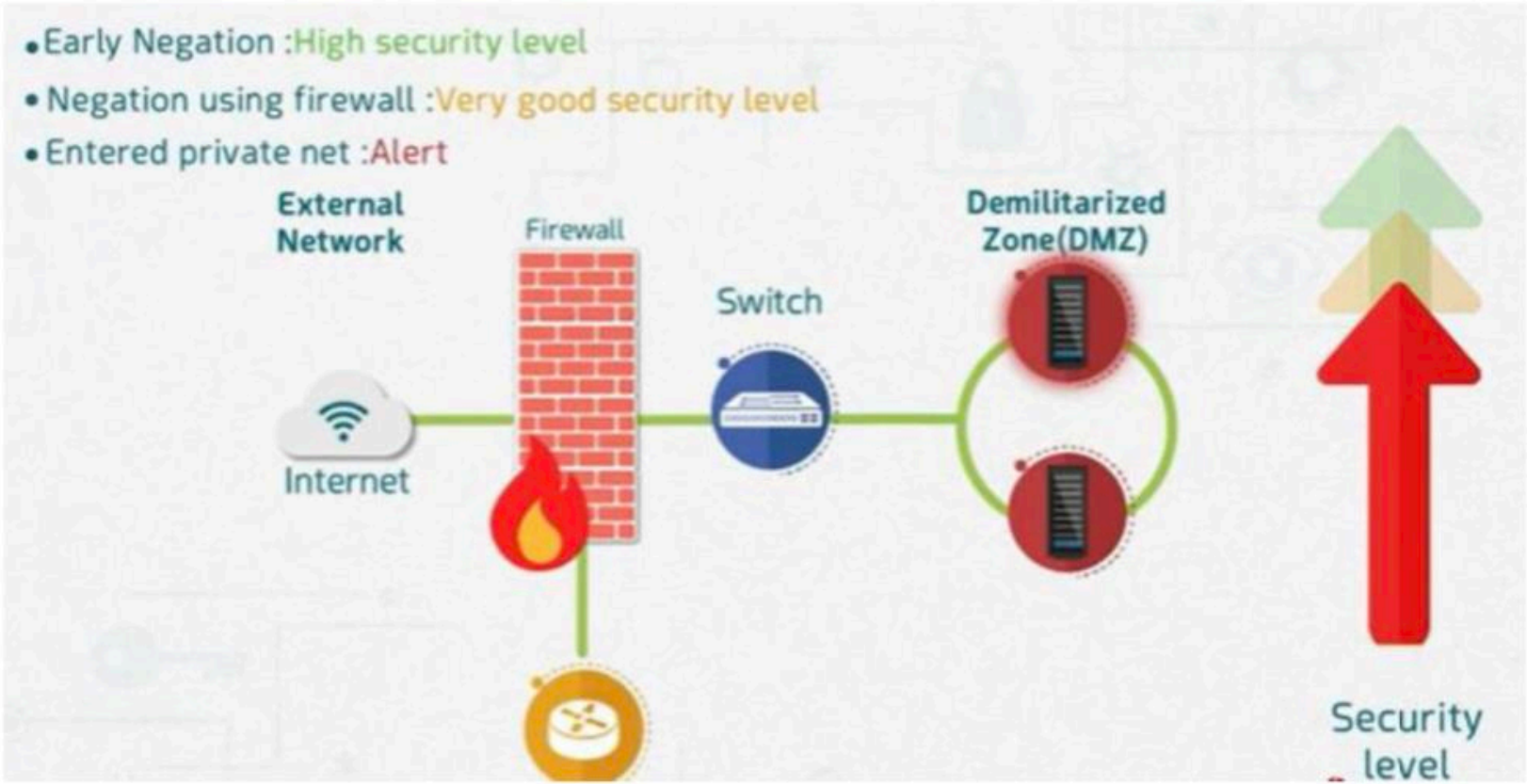


جدران الحماية هي حدود أو بوابات تدير حركة نشاط الإنترنت المسموح به والمحظور في شبكة خاصة. يأتي هذا المصطلح من مفهوم الجدران المادية كونها حواجز لإبطاء انتشار الحرائق حتى تتمكن خدمات الطوارئ من إخمادها. عند المقارنة، جدران حماية أمان الشبكة مخصصة لإدارة حركة مرور الإنترنت تهدف في العادة إلى إبطاء انتشار تهديدات الإنترنت.

أنواع Firewall

- Host-based
- Network-based

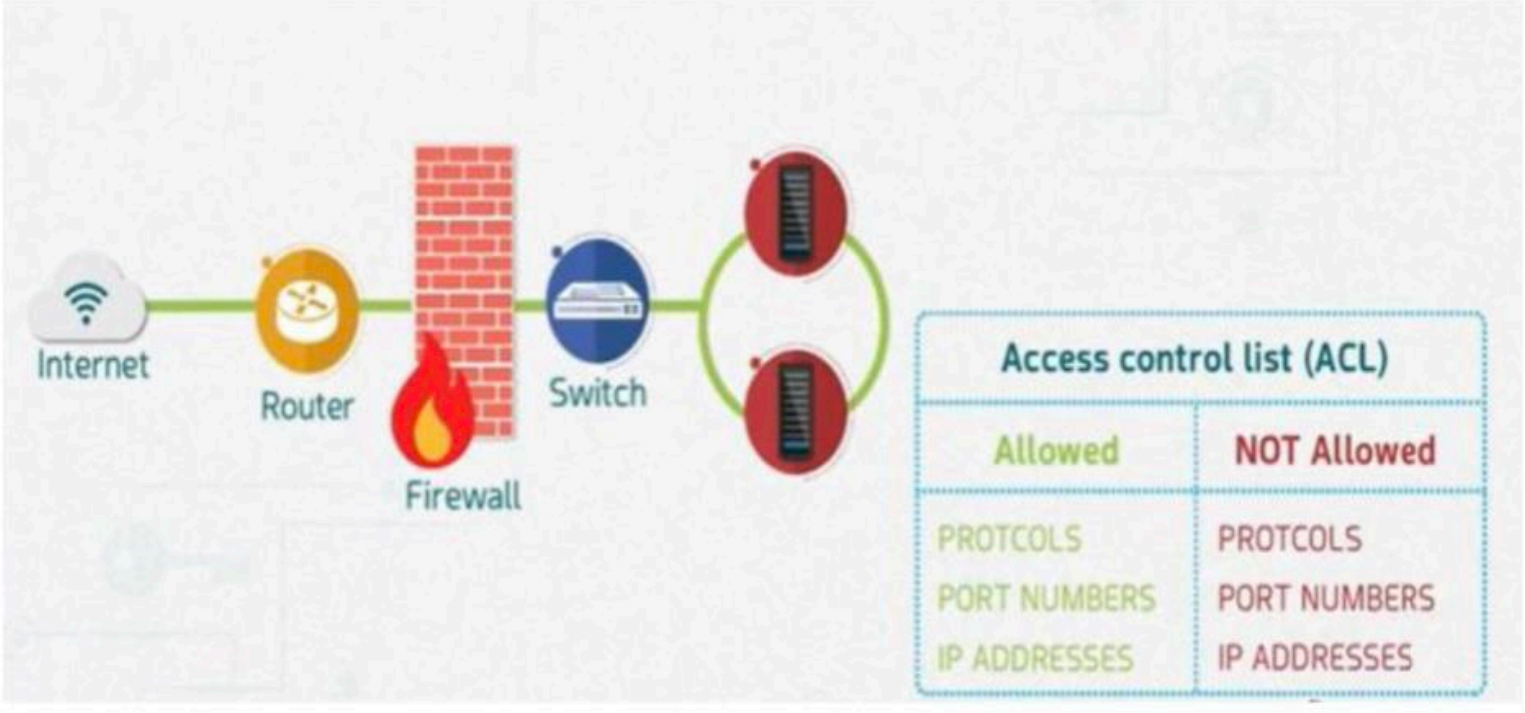


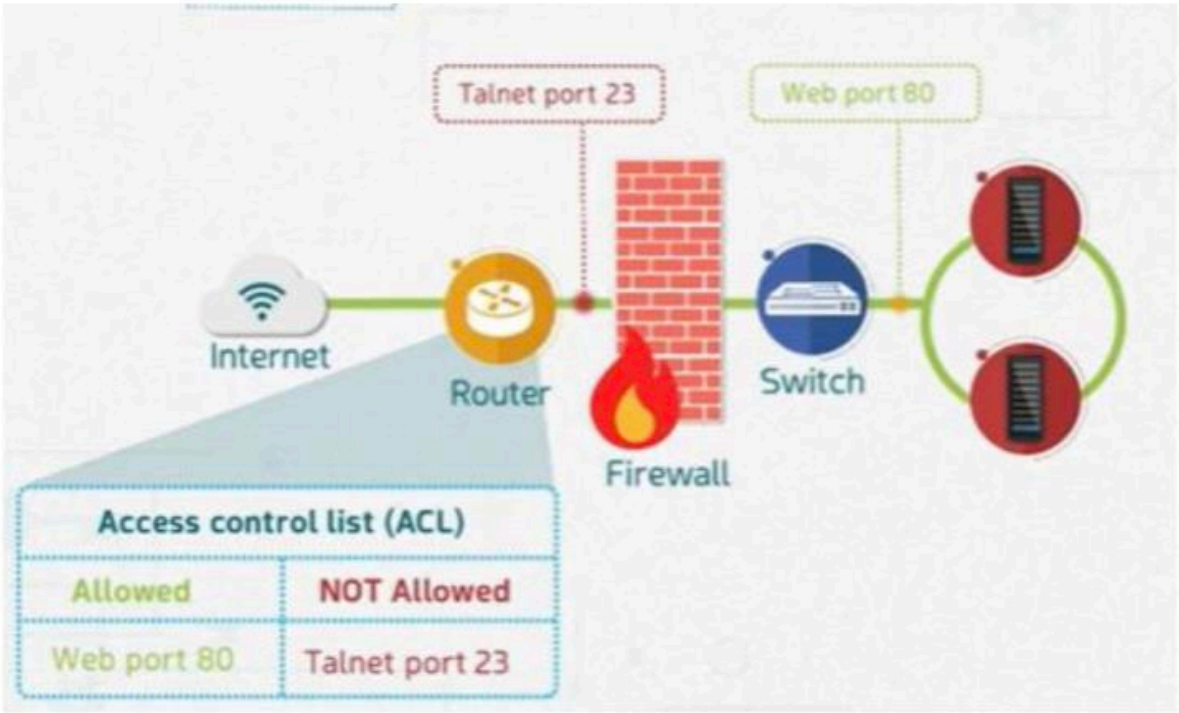

•Early Negation :High security level
• Negation using firewall :Very good security level
• Entered private net :Alert
External Network
Firewall
Switch
Demilitarized Zone(DMZ)
Internet
Security level

Firewall Filtering Techniques عملية الفلترة

- Packet filtering
- Stateful inspection
- Proxy firewall

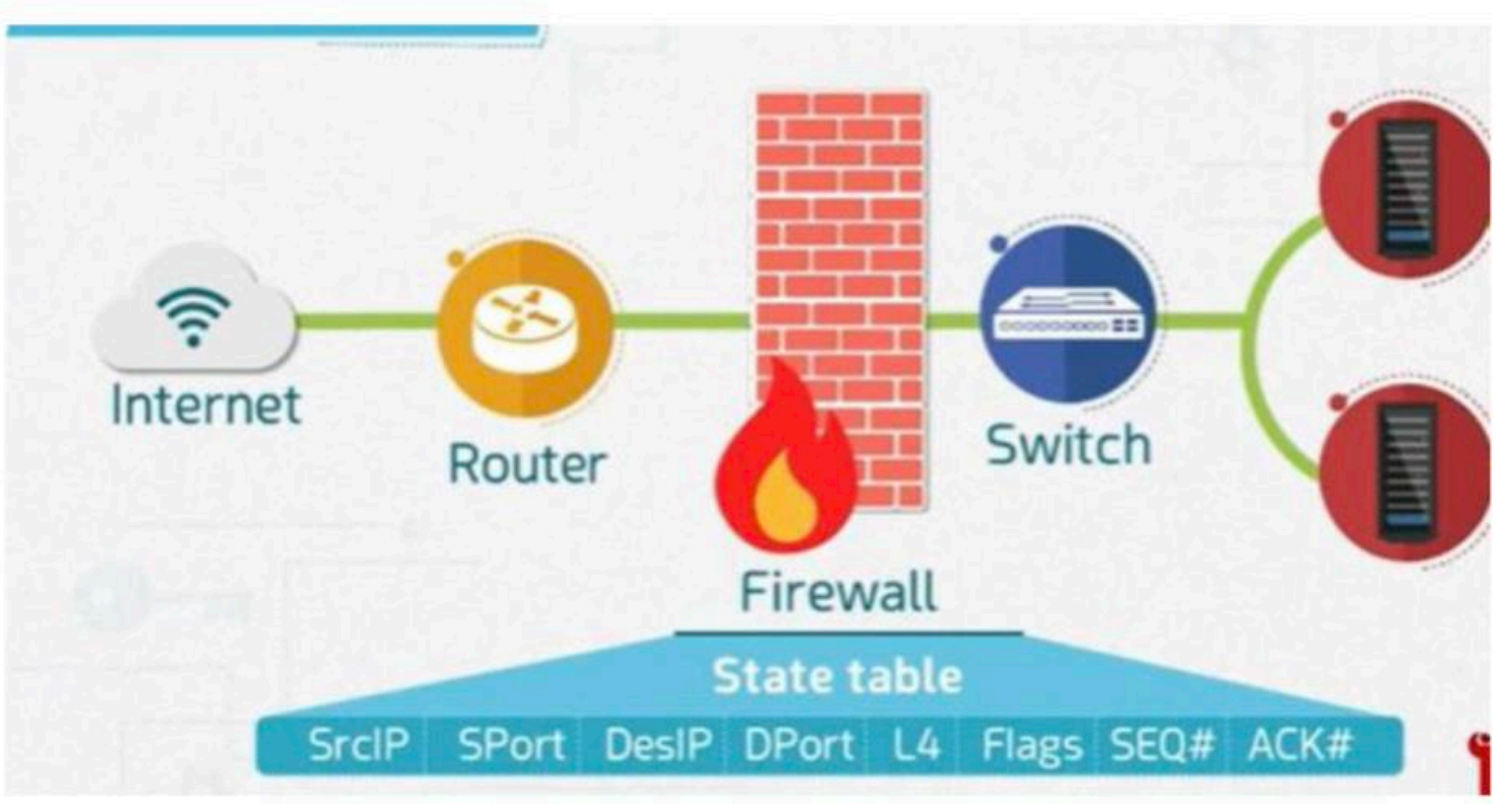
Packet filtering

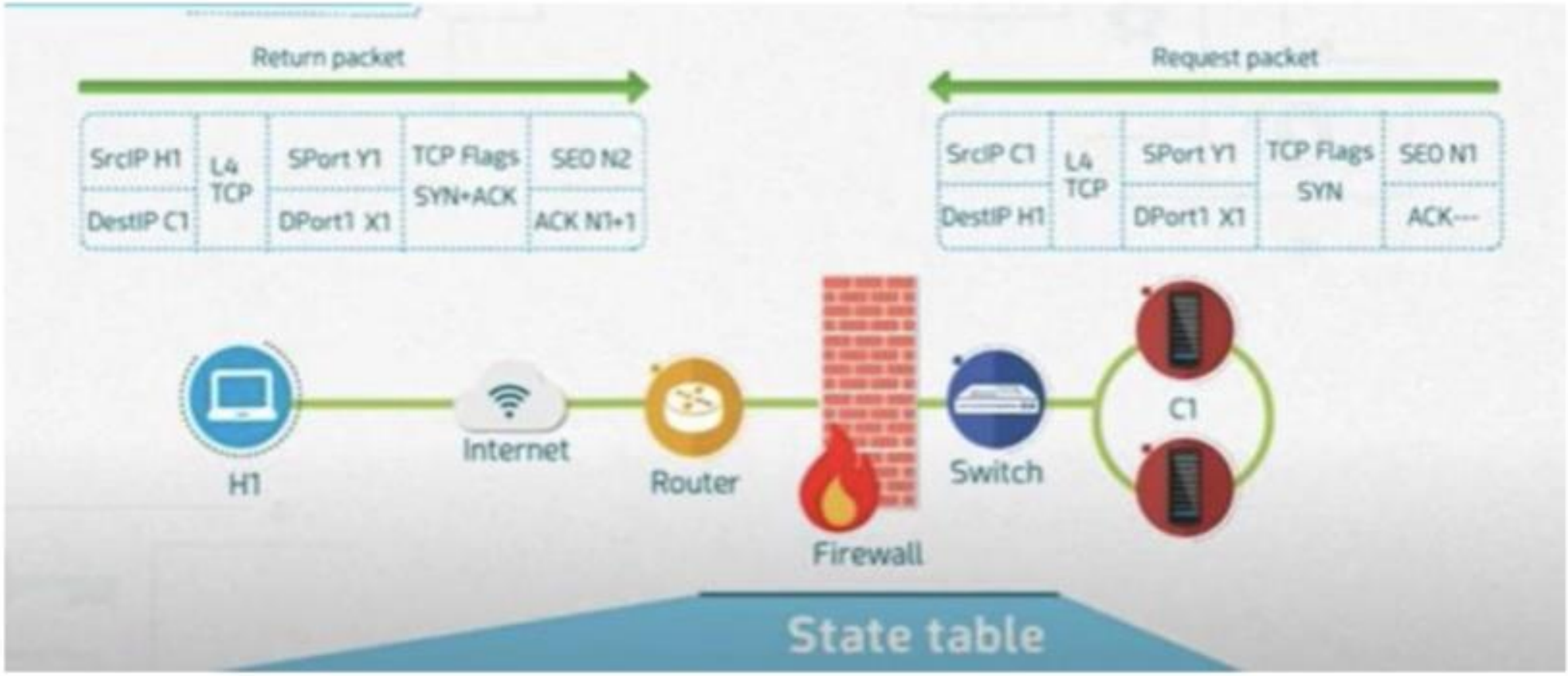


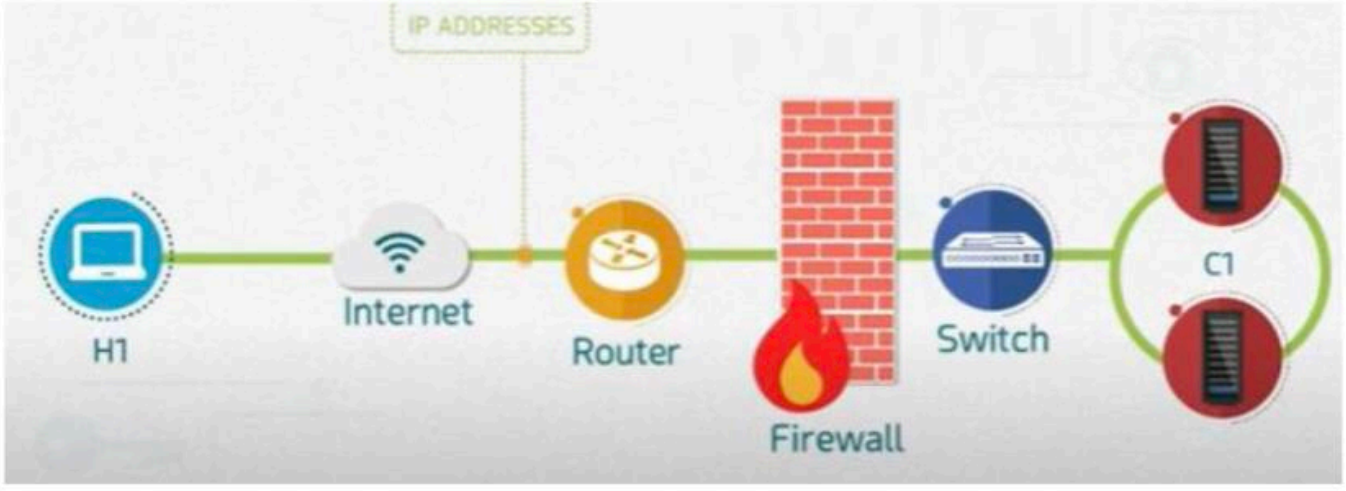


العيوب: ان القواعد توضع من شخص فاذا كانت فيها مشكلة او ناقصة يحدث مشكلة واختراق

Stateful inspection

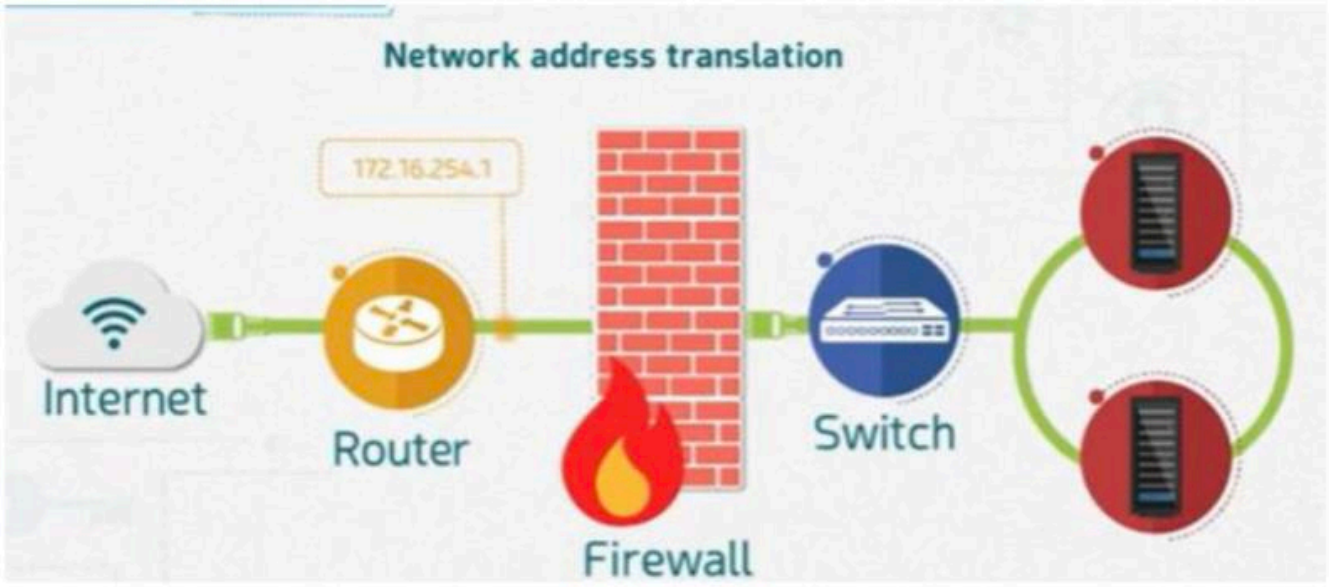



Return packet
SrcIP H1
L4 TCP
SPort Y1
TCP Flags SYN+ACK
SEQ N2
DestIP C1
DPort1 X1
ACK N1+1
Request packet
SrcIP C1
L4 TCP
SPort Y1
TCP Flags SYN
SEQ N1
DestIP H1
DPort1 X1
ACK---
H1
Internet
Router
Firewall
Switch
C1
State table



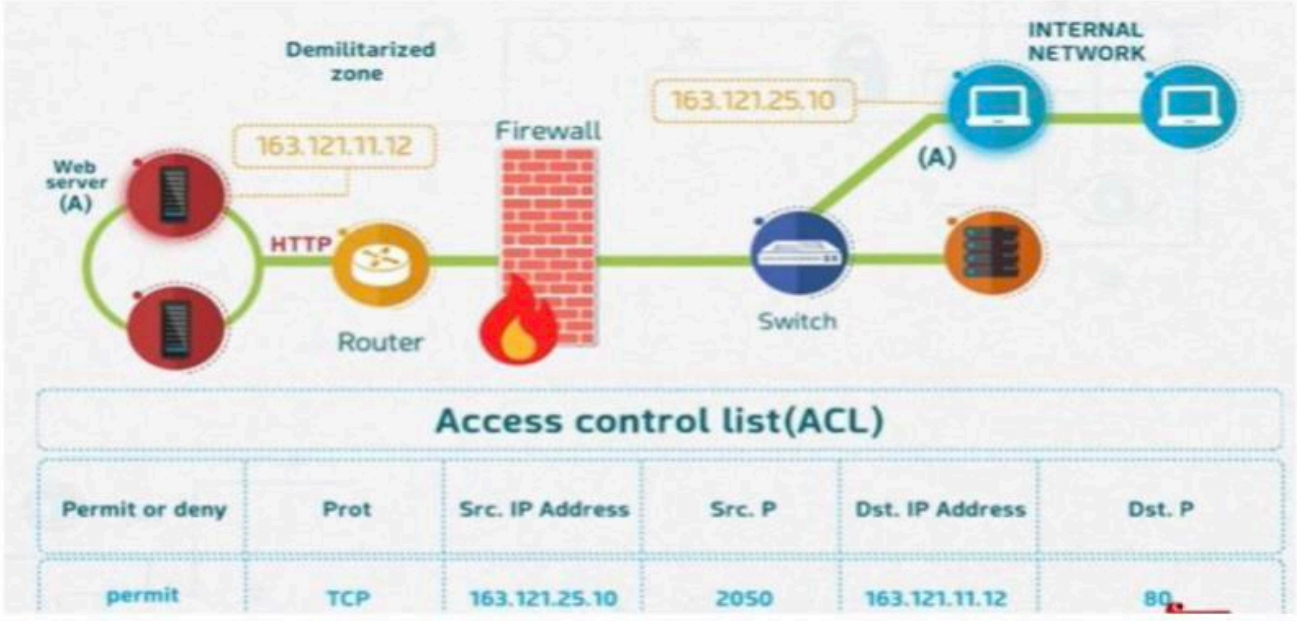
العيوب: في حاله الاتصال المباشر بيتم كشف العنوان الخاص بالشبكة الداخلية وهذا خطر

Proxy firewall

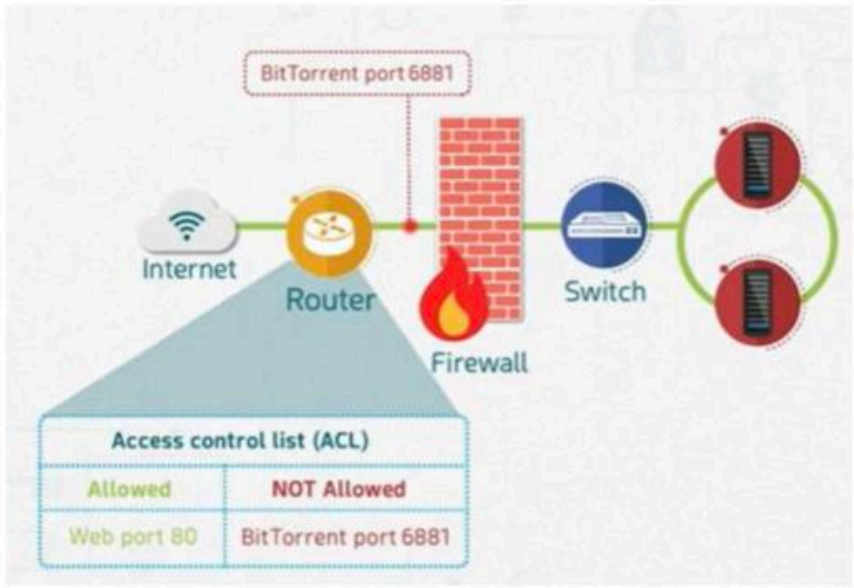


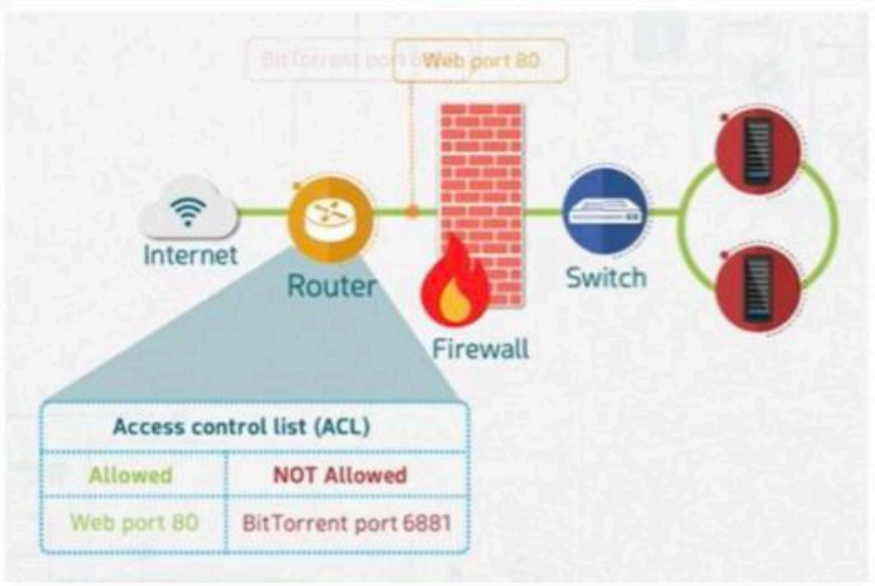
Configuring Firewall Rules

Example

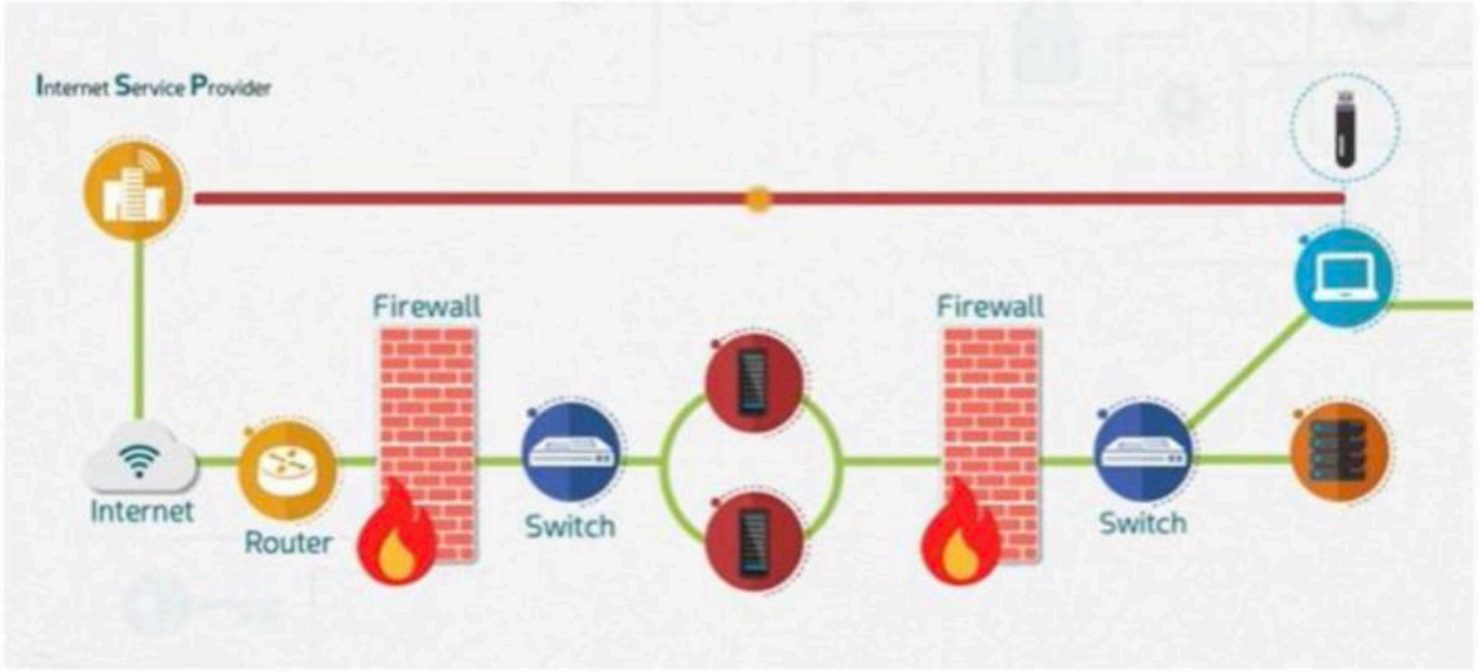

Demilitarized zone
INTERNAL NETWORK
163.121.25.10
163.121.11.12
Firewall
Web server (A)
(A)
HTTP
Router
Switch
Access control list(ACL)
Permit or deny
Prot
Src. IP Address
Src. P
Dst. IP Address
Dst. P
permit
TCP
163.121.25.10
2050
163.121.11.12
80

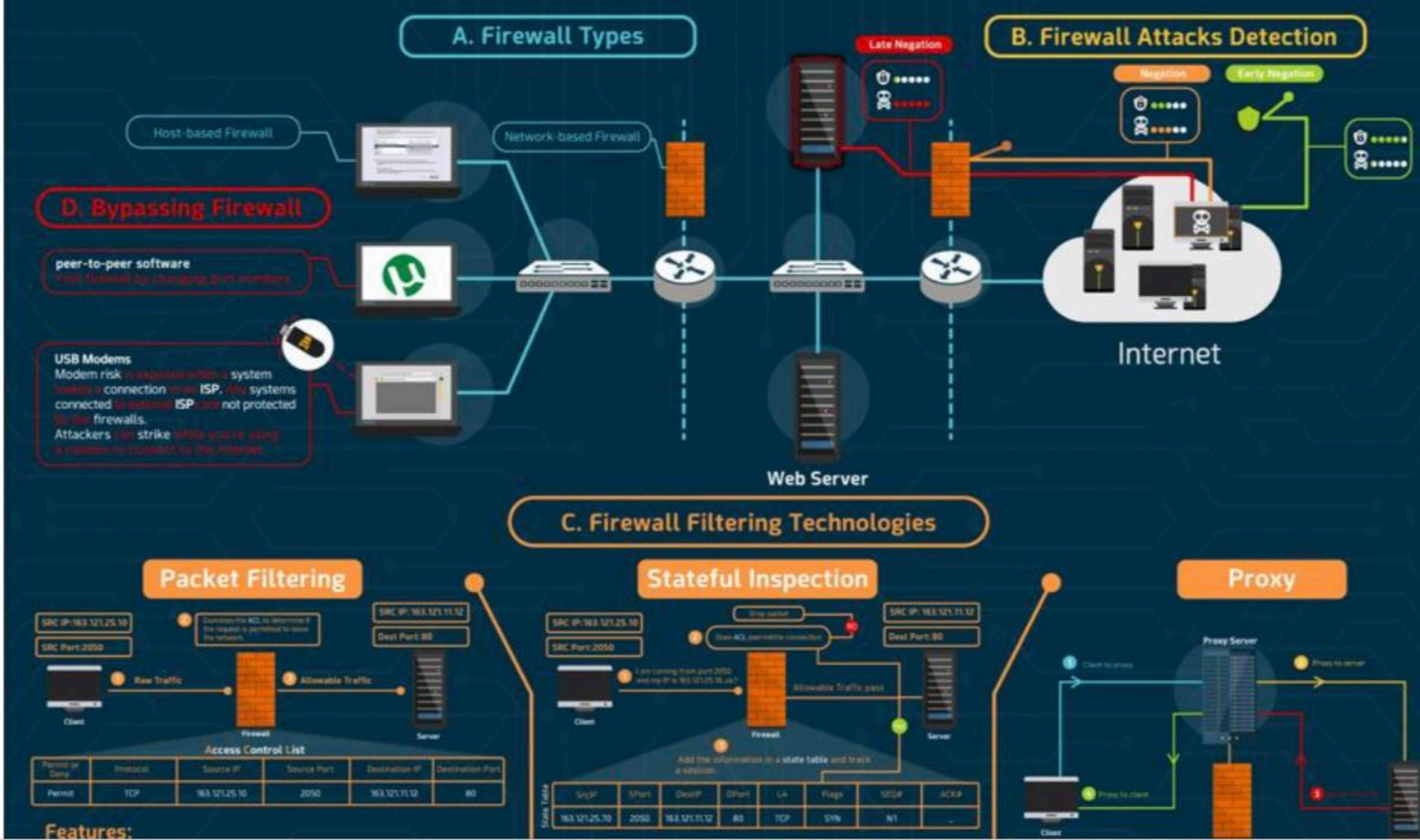
Bypassing Firewall


BitTorrent port 6881
Internet
Router
Firewall
Switch
Access control list (ACL)
Allowed
NOT Allowed
Web port 80
BitTorrent port 6881


Web port 80
Internet
Router
Firewall
Switch
Access control list (ACL)
Allowed
NOT Allowed
Web port 80
BitTorrent port 6881

التقييد Restrictive




A. Firewall Types
Host-based Firewall
Network-based Firewall
B. Firewall Attacks Detection
Late Negation
Negation
Early Negation
Internet
Web Server
D. Bypassing Firewall
peer-to-peer software
USB Modems
Modem risk
system
connection
ISP.
systems
connected
ISP
not protected
firewalls.
Attackers
strike
C. Firewall Filtering Technologies
Packet Filtering
SRC IP:163.121.25.10
SRC Port:2050
Dest IP: 163.121.11.12
Dest Port: 80
Raw Traffic
Allowable Traffic
Client
Firewall
Server
Access Control List
Permit or Deny
Protocol
Source IP
Source Port
Destination IP
Destination Port
Permit
TCP
163.121.25.10
2050
163.121.11.12
80
Features:
Stateful Inspection
Allowable Traffic pass
Add the information in a state table and track a session
State Table
SrcIP
SPort
DestIP
DPort
L4
Flags
SEQ#
ACK#
163.121.25.70
2050
163.121.11.12
80
TCP
SYN
N1
Proxy
Proxy Server
Client to proxy
Proxy to server
Proxy to client
Client

معهد العراب العالي للتدريب

شكرًا

معهد العراب العالي للتدريب

مقدمة في أمن الشبكات

م. ميسون الرحماني

معهد العراب العالي للتدريب

05

المحاضرة الخامسة

2024

ACL

- Standard
- Extended

standard

- فقط باستخدام IP source
- Access-list (الرقم) (permit/deny) (العنوان)

Extended

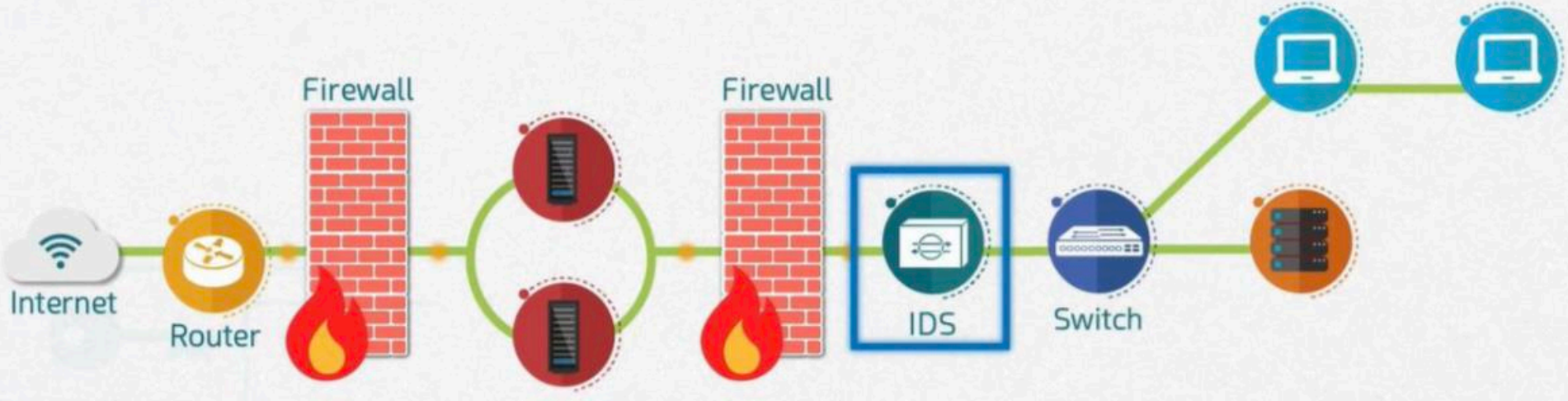
- Access-list (الرقم) (permit/deny) (البرتوكول) (source Ip) (dist. Ip)

- Ip access-group (الرقم) (in out)

العناصر الاساسية

- **Intrusion Detection and Prevention Systems**

INTRUSION DETECTION SYSTEMS(IDS)

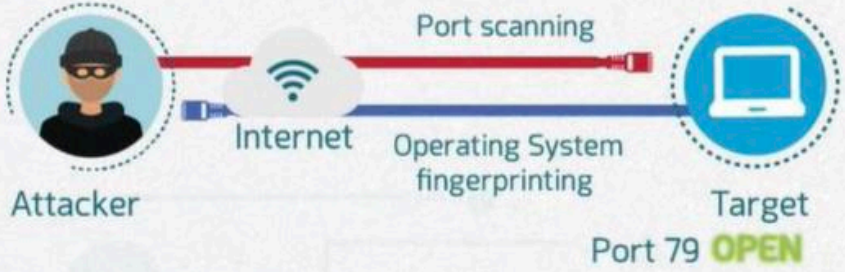


نظام كشف التدخل IDS

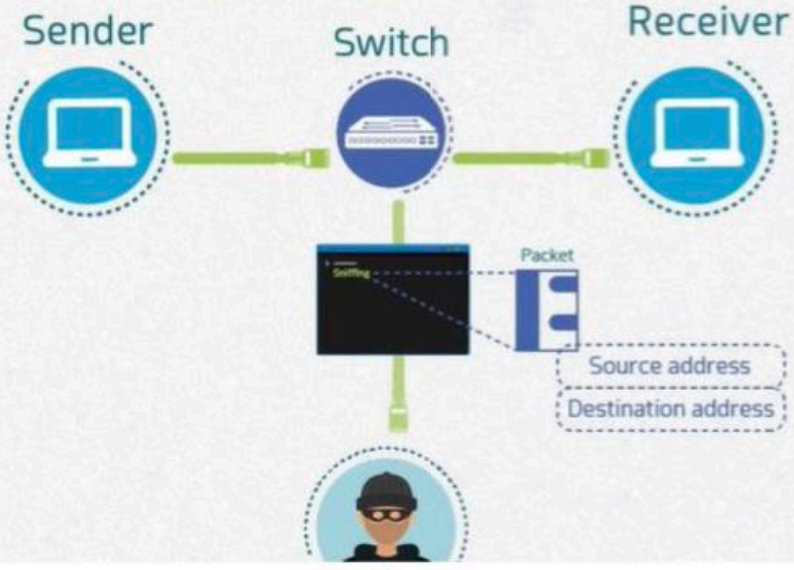
- دورة مراقبة الشبكة وعمل تحليل لحركة المرور خلالها وعند رصد أي تهديد او خطر يقوم بأطلاق انذار
- هي اشبه بكاميرات المراقبة
- ليس دورة وقف او اخذ أي اجراء، ولكن انذار وعلى المسؤول اخذ الإجراءات

Attacks

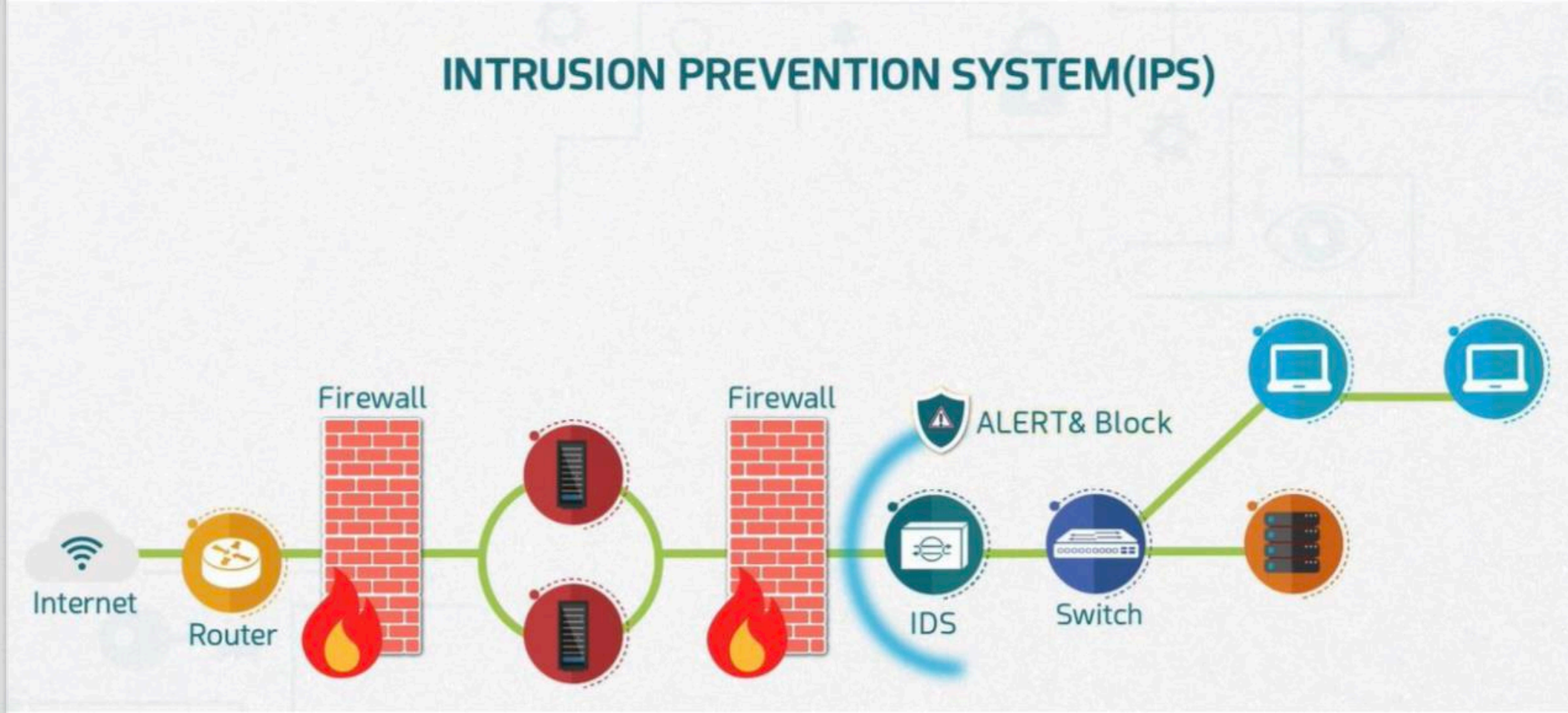
Port scanning



Sniffing



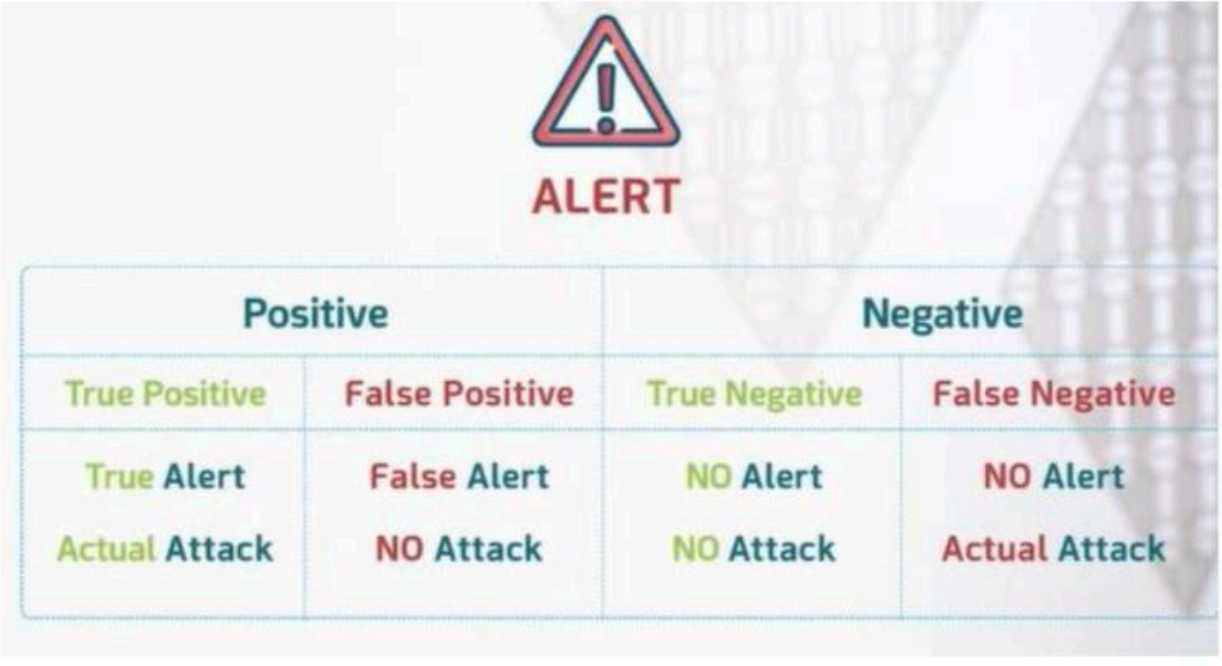
INTRUSION PREVENTION SYSTEM(IPS)

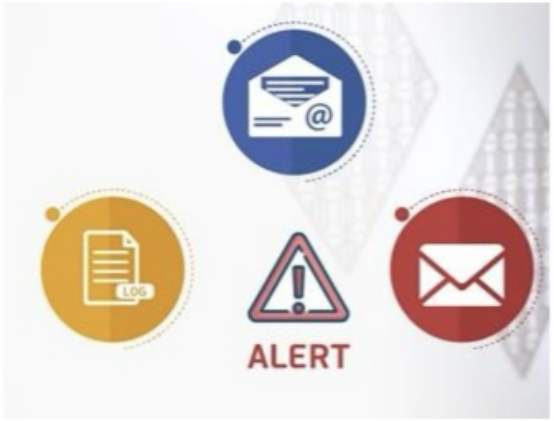


نظام حماية التدخل IPS

- خطوة اعلى وهى اتخاذ اجراء مع إعطاء انذار

أنواع الانذارات



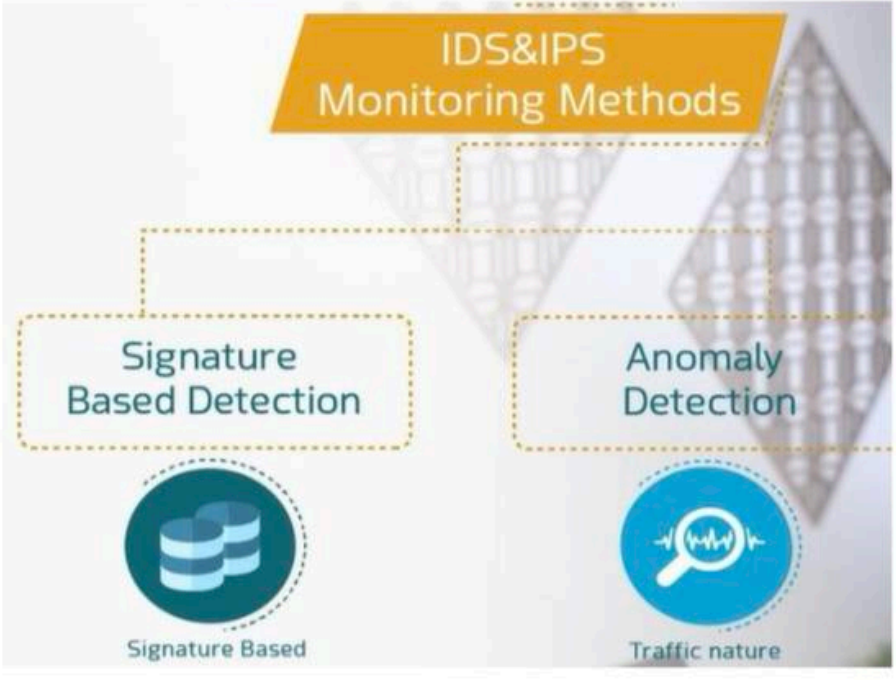

LOG
ALERT

IDS&IPS Monitoring Methods طرق مراقبة

- الطريقة الأولى :

هي من خلال وجود قاعده بيانات متعرف فيها أشهر الهجمات والتهديدات وكل تهديد له توقيع خاص به ويتم مقارنته مع حركة المرور

عيوبها : انه يظهر تهديدات جديدة كل يوم وهناك فجوة وقتية من وقت ظهور التهديد ووقت تعرف النظام عليه وتطبيقه



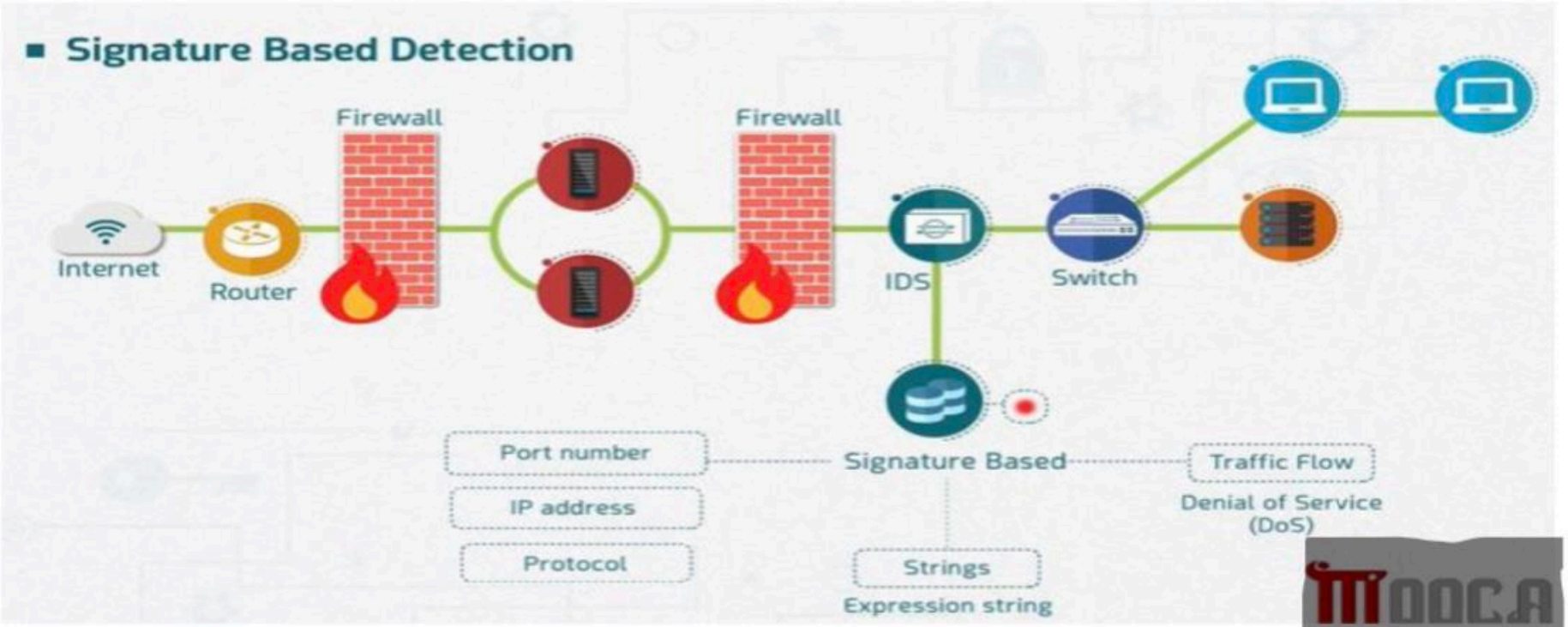
- الطريقة الثانية:

وضع تصور طبيعي للشبكة واي شيء اخر يعتبر تهديد

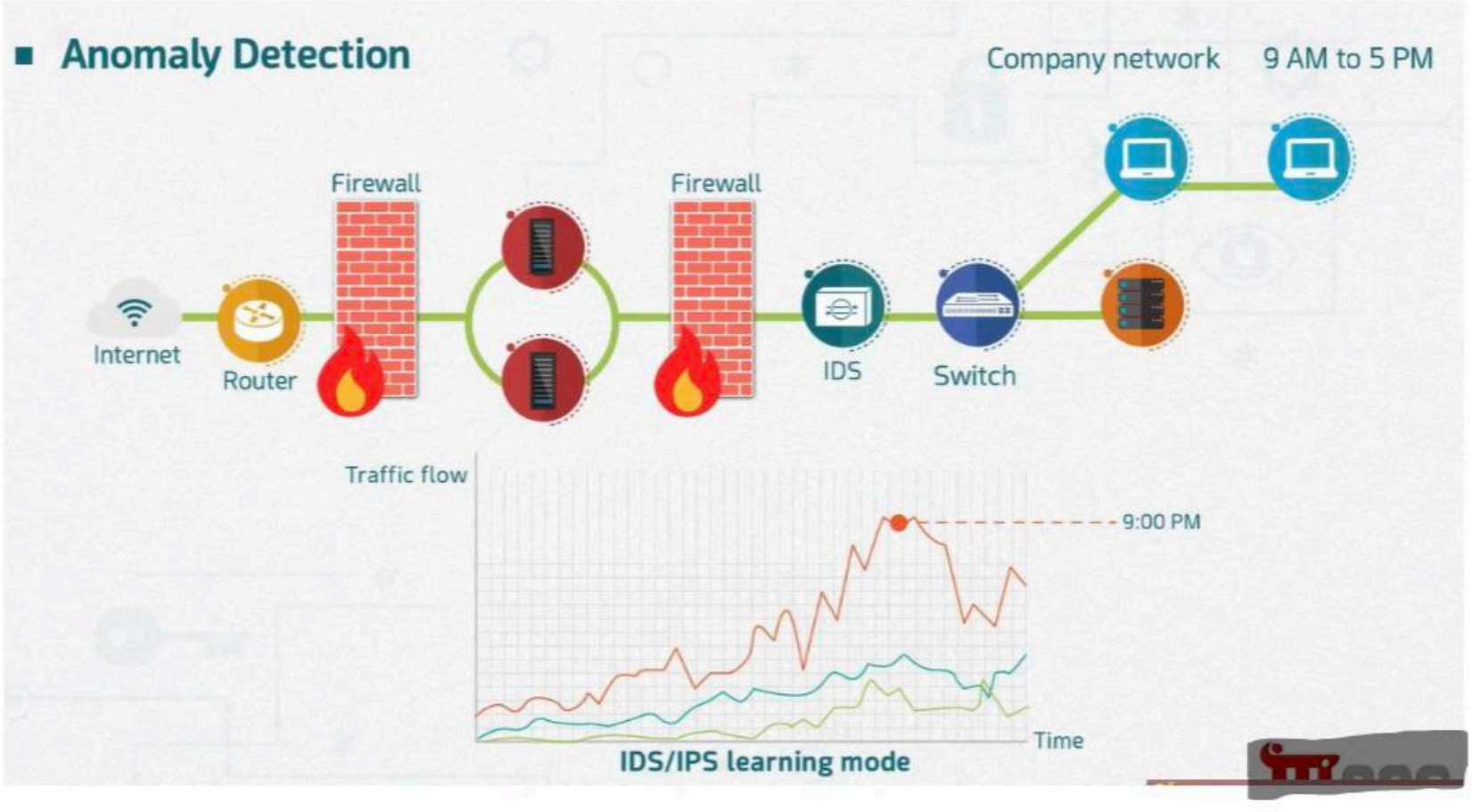
ميزاته: يقدر يتعرف على التهديدات التي يتم تعريفة عليها من قبل

عيوبه: فترة التعلم

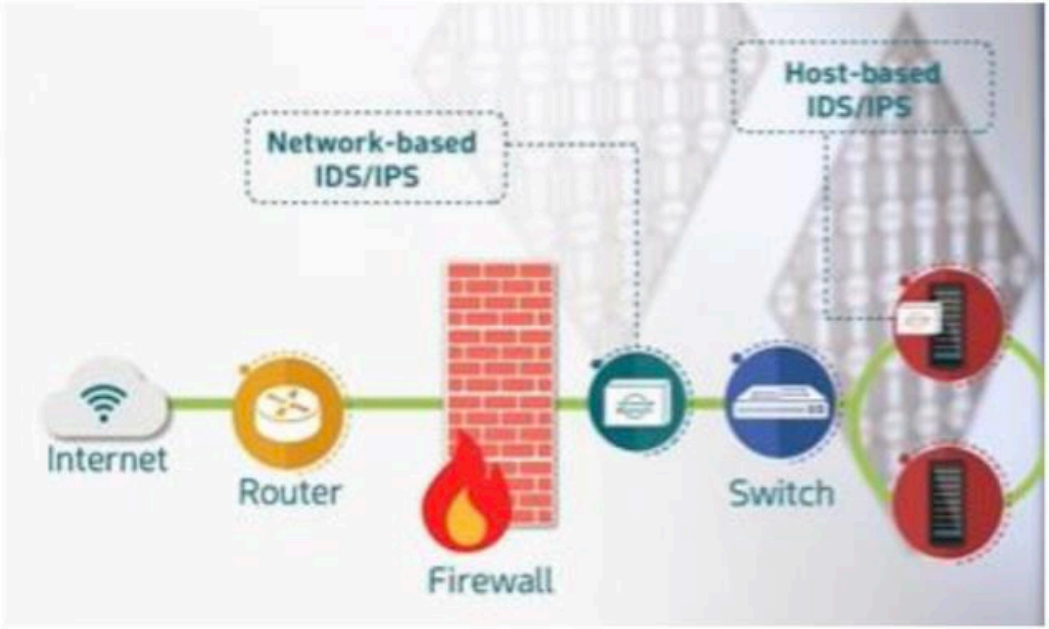
Signature based detection



Anomaly detection

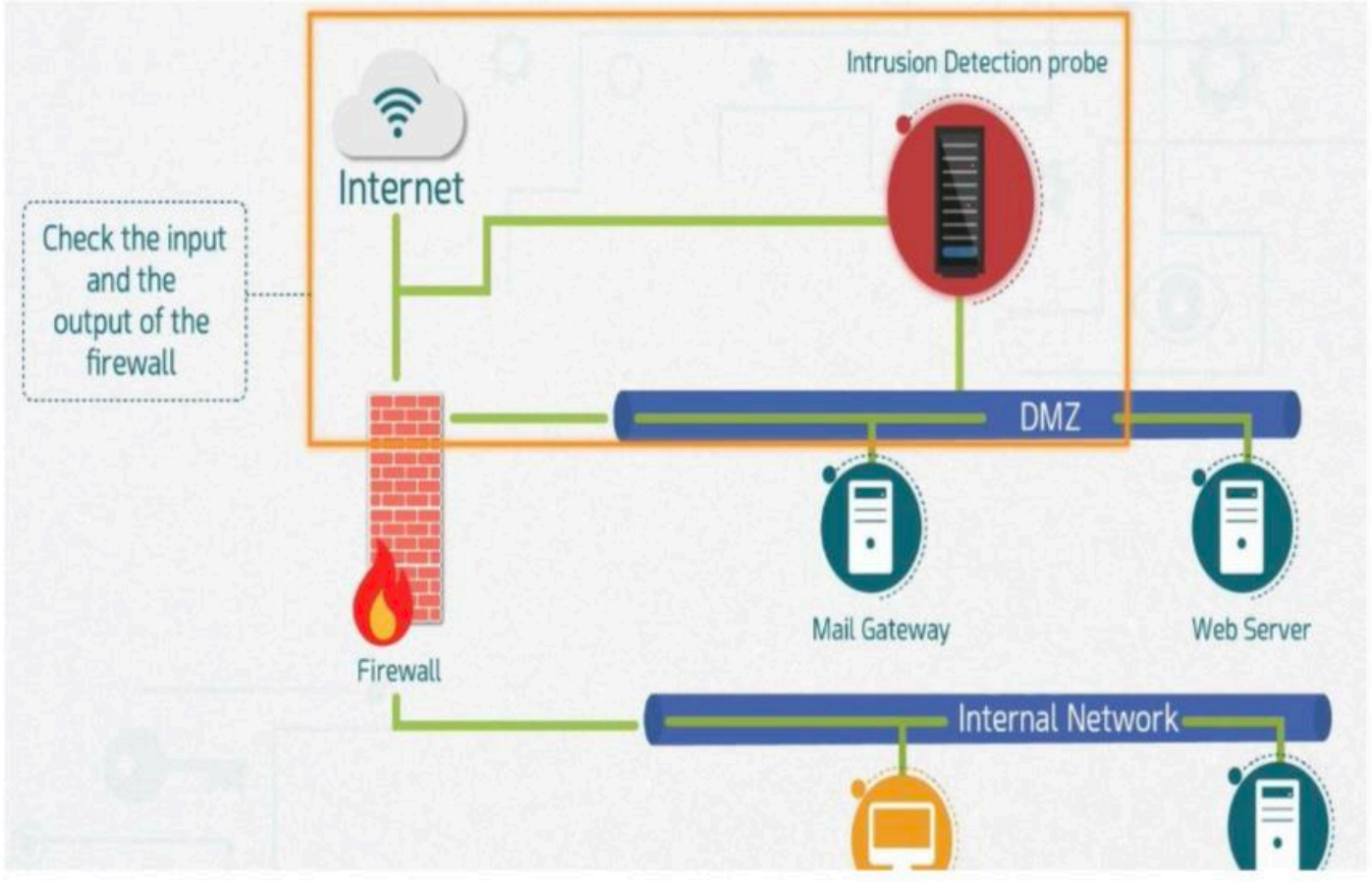


أماكن وضع IDS\ IPS

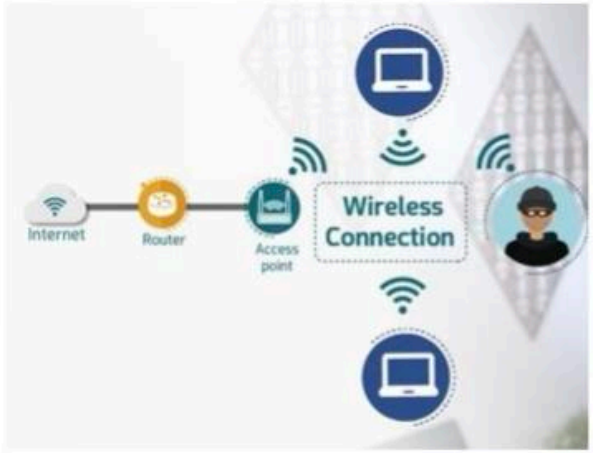


1- على الجهاز وهنا يراقب المرور لهذا الجهاز
2- على الشبكة

مثال


Intrusion Detection probe
Internet
Check the input and the output of the firewall
DMZ
Mail Gateway
Web Server
Firewall
Internal Network

Wireless Security Standards

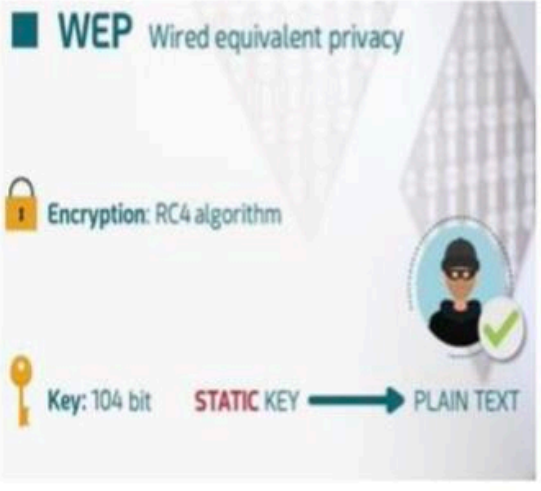


- أنواع برتوكولات تشفير اللاسلكي:

A. WEP

B. WPA1

C. WPA2

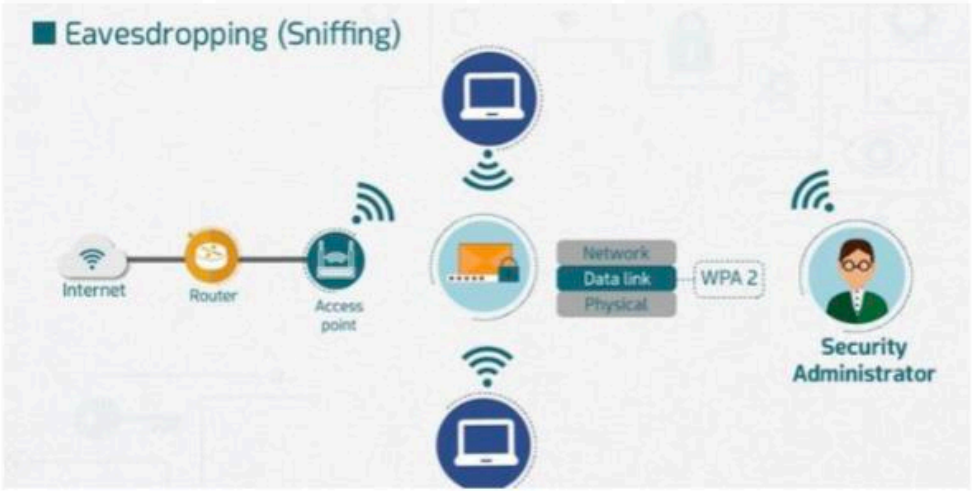

WEP Wired equivalent privacy
Encryption: RC4 algorithm
Key: 104 bit
STATIC KEY
PLAIN TEXT


WPA 1 (Wi-Fi protected access)
Encryption: RC4 algorithm
Key: PSK (PRE- SHARED KEY)
Data integrity

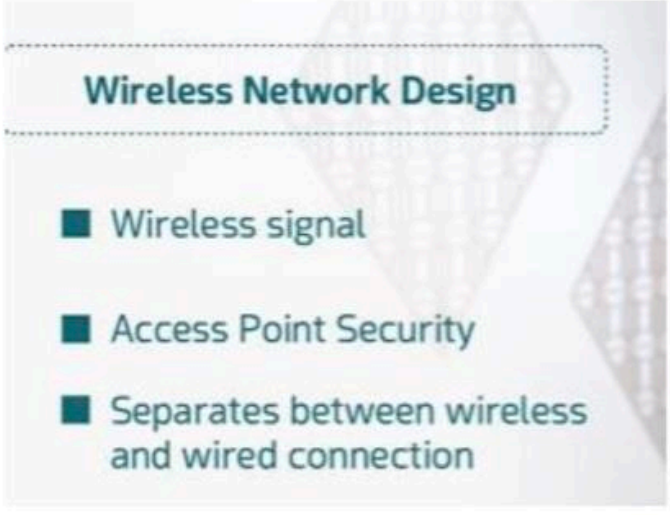

WPA 2 (Wi-Fi protected access)
Encryption: AES advanced encryption standard
Key: PSK (PRE- SHARED KEY)
Changeable KEY

Wireless Threats and Attacks

- Sniffing WPA2/ encryption
- Spoofing المصادقة
- Daniel of service DOS IDS



تصميم الشبكة اللاسلكية Wireless Design



1- الإشارات اللاسلكية
- التغطية داخل المبنى فقط
- التغطية قوية داخل المبنى

2- حماية AP (access point)
- إخفاء SSID
- عمل فلترة لحركة المرور

3- الفصل بين السلكي واللاسلكي
- استخدام firewall
- استخدام سويتش منفصل للجزء اللاسلكي

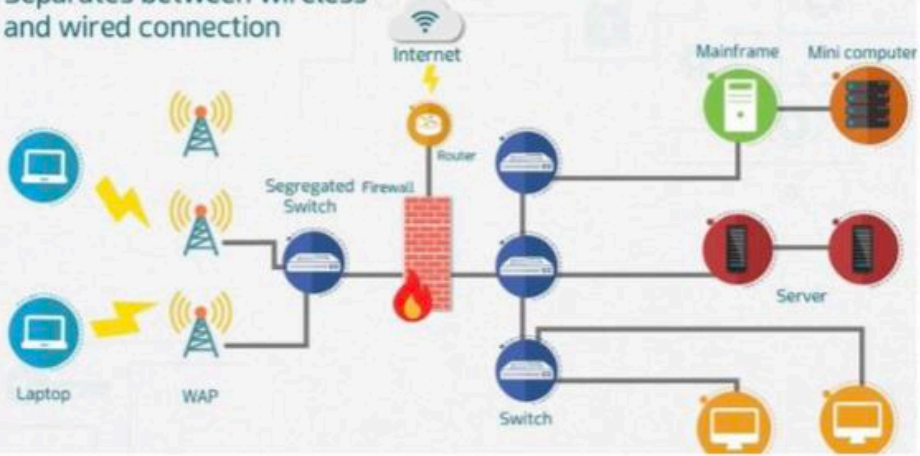
Access Point Security

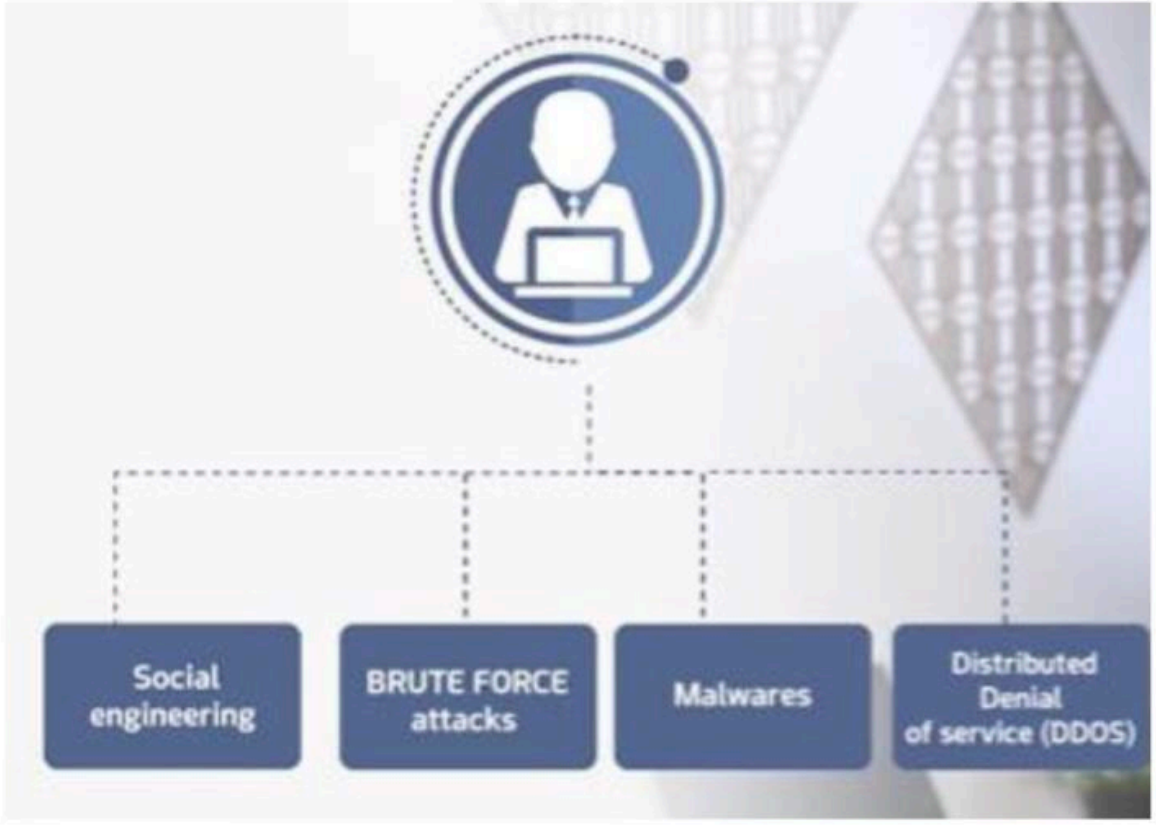
1- (SSID) service set identifier: **Hidden**

2- **Access point filtering**

Permit or deny	Src. Mac Address	Src. IP Address	Src. P	Dst. Mac Address	Dst. IP Address	Dst. P

Separates between wireless and wired connection




Social engineering
BRUTE FORCE attacks
Malwares
Distributed Denial of service (DDOS)

معهد العراب العالي للتدريب

شكرًا