

CCNA - Security

# CCNA SECURITY

210 – 260

# Lec 1

CCNA - Security

## Chapter//1

بسم الله الرحمن الرحيم

بخصوص منهج ccna security هناك مصطلحات في بداية الامر وهي التالي :

لو كان لدينا شبكة ووجد بها

1 - **Vulnerability** – وتعني أن هنالك ثغره يمكن من خلالها اختراق الشبكة من قبل Attackers (قابلية الاختراق) ويجب علينا ان نعالج هذه الثغره .

2 - **Threats** – وتعني تهديد والتي تأتي من بعد وجود ثغره في الشبكة والتي كما قلنا تسمى Vulnerability .

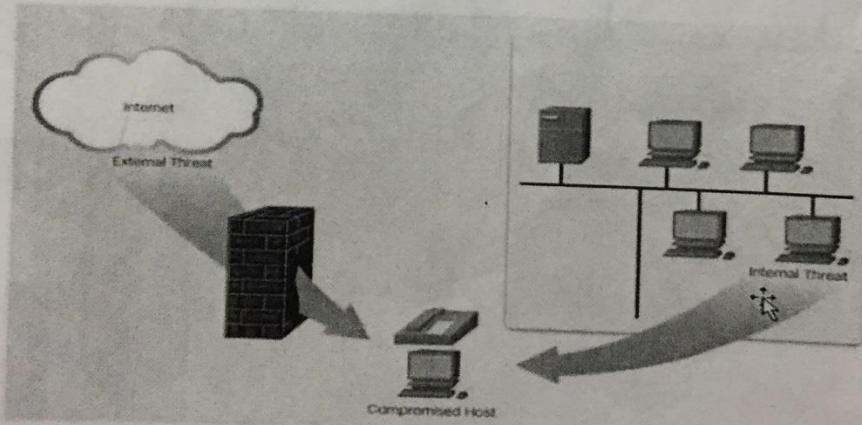
3 - **Risk** – في حال وجد ثغره في الشبكة وهذا يؤدي الى وجود تهديد من قبل Attackers وهذا سوف يضع الشبكة في دائرة الخطر Risk .

4 - **Mitigation** – وتعني حماية الشبكة من نوع معين من الأختراق .

\* أنواع الـ Attacks هي :

- 1 - عن طريق WAN اي عن طريق الانترنت .
- 2 - عن طريق LAN اي عن طريق الشبكة الداخلية للشركة مثلا .

### Vectors of Network Attacks



الموضع الرئيسي

المعروف المفهوم

النهايات اطعمة

اللاحقة اهم

\* الفرق بين hacker والattacker

• هو الشخص الذي يستعمل برامج ماهنة ل القيام بعمليات القرصنة  
• هو الشخص الذي يبني برامج القرصنة ويستخدمها في عملية القرصنة

CCNA - Security

في ما مضى كان أغلب الاختراق يكون عن طريق الانترنت ولكن في مرور الزمن أصبح التهديد الرئيسي من داخل الشبكة الداخلية اي احد الموظفين مثلاً يعمل داخل الشركة حيث أصبح هذا الاختراق من الانواع المنتشرة حالياً بسبب ان المخترق يعرف ماهي مكونات النظام داخل الشبكة وماهي نقاط ضعف ايضاً للشبكة.

\* البيانات التي يمكن ان تحدث لها مشكله اثناء الاختراق هي :

### Data Loss

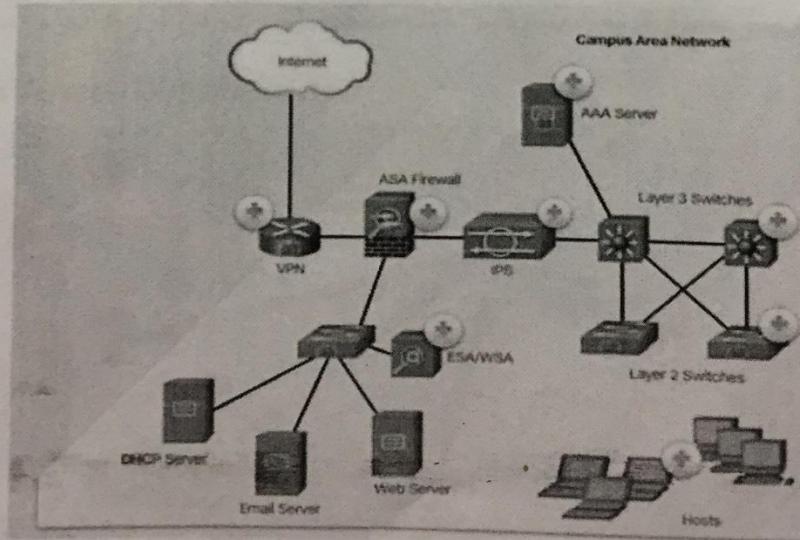
#### Vectors of data loss:

- Email/Webmail
- Unencrypted Devices
- Cloud Storage Devices
- Removable Media
- Hard Copy
- Improper Access Control

\* لكي نفهم بشكل جيد أنواع الاختراق للشبكات يجب علينا فهم تصاميم كل شبكة وأنواعها  
كالتالي :

: Campus Area Network ( LAN ) – 1

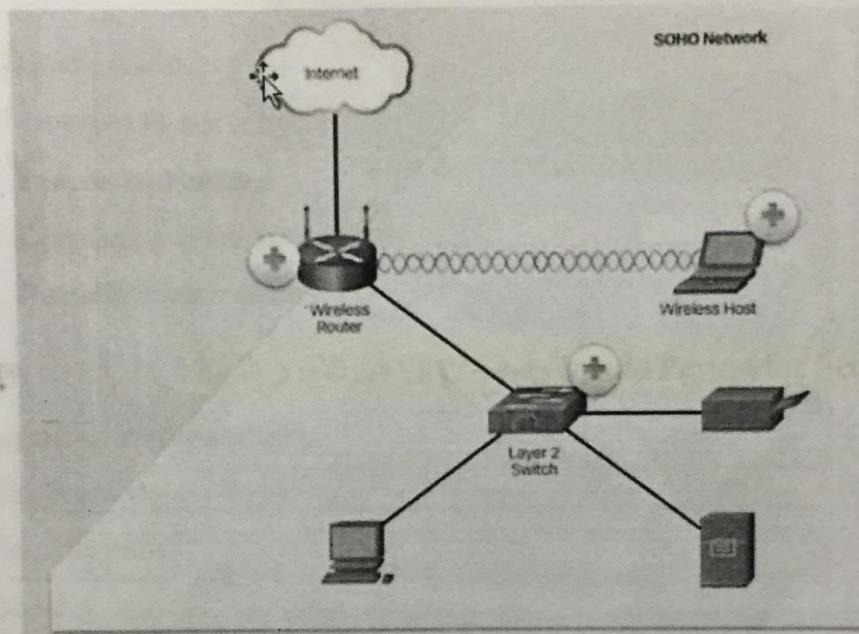
### Campus Area Networks ( Local area Network )



## 2 – النوع الثاني : Small Office & Home Office Network

تعني شبكات صغيرة أي داخل البيت أو شركة صغيرة .

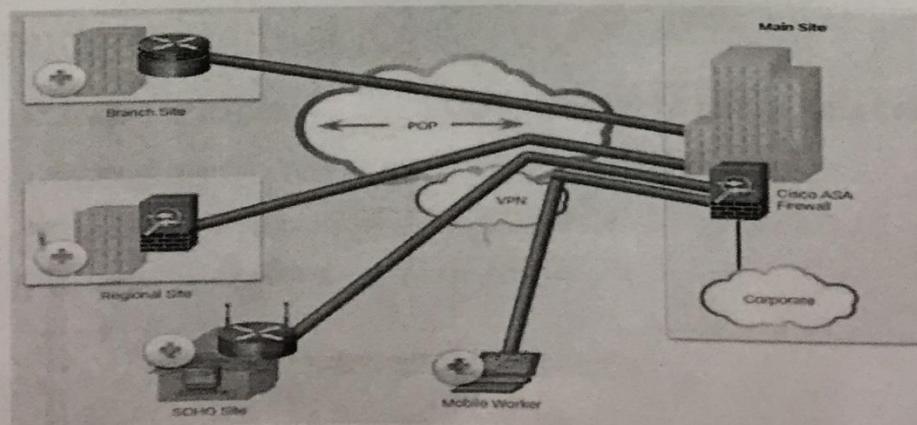
### Small Office and Home Office Networks



## 3 – النوع الثالث : Wide Area Networks

وتكون من مجموعة من الراوترات والسوتجات ومثالها مجموعة من فروع لشركة معينة

### Wide Area Networks



#### 4 - النوع الرابع : Data Center

اي احد انواع الشبكات لشركات ضخمه تقدم خدمات للزبائن كمثال شركات الاتصالات الهايفيه وخدمات الانترنت ويجب ان تكون الحمايه لهذا النوع على قسمين وهما :

##### Outside Perimeter Security – 1

###### Outside perimeter security

- On-premise security officers
- Fences and gates
- Continuous video surveillance
- Security breach alarms

##### Inside Perimeter Security – 2

###### Inside perimeter security:

- Electronic motion detectors
- Security traps
- Continuous video surveillance
- Biometric access and exit sensors (بجهة الوجه وفتحة الماء)

#### 5 - النوع الخامس : Cloud & Virtual Networks

وهذ من الانواع المنتشره حاليًا بشكل كبير

## Cloud and Virtual Networks

### VM-specific threats:

- Hyperjacking
- Instant On activation
- Antivirus storm

### Components of a secure data center:

- Secure segmentation
- Threat defense
- Visibility

الشركات الكبيرة تستخدم  
بعروفة ومحضها وتستخدم كل  
لخدمة سيرفرات  
كبير على Server وتقسيمة الـ VM لخواص معينة  
server

## CCNA - Security

من انواع الـ Attack الذي يستهدف هذا النوع وهو :

الماكنة

\***Hyperjacking** وهو عباره عن انشاء virtual machines ليوهم المستخدم بأنه ~~الجهاز~~ الرئيسيه للاتصال ومن خلال هذا العمليه يتم الاختراق ويسمى هذا الـ VM التابع للمخترق **Rouge VM**

\*سبب انشاء هذه المكنه هو استخدام الشركات للـ VM في شبكات الـ Cloud بشكل كبير اي استخدام أجهزه وهميه محاكيه للأجهزه الحقيقية .

## 6 - النوع السادس : The Evolving Network Border

### The Evolving Network Border

Critical MDM functions for BYOD network:

- Data encryption
- PIN enforcement
- Data wipe
- Data loss prevention
- Jailbreak/root detection

و هو من انواع الشبكات التي تسمح لاستخدام الأجهزه الخاصه بالموظفين وليس اجهزة الشركة نفسها والتي تسمى **BYOD(Bring Your Own Device)** اي بامكان الموظف استخدام الlaptop الخاصه به والعمل بها على شبكة الشركة ولكن ضمن صلاحيات وامور امنيه يحددها الادمن كمثال لو كان هناك موظف اراد استخدام الشبكة الخاصه بالشركة فيجب أن توفر هناك امور امنيه للشبكة يجب ان تتوافق في جهاز الموظف لكي يتمكن من الدخول الى الشبكة وهنا اوجدت شركة سسکو جهاز يسمى **NAP(Network Access Protection)** ويعمل هذا الجهاز على التحقق من جهاز الموظف هل يحوي على Anti-Virus وهل هو محدث الى الأصدار الأخير وغيرها من الأمور الواجب توفرها في جهاز الموظف لكي يتم السماح له من الدخول الى الشبكة وأن كان لا يملك أحد هذا الخواص المطلوبه فسوف ينقل اتصاله الى منطقة تسمى **Limitation Area** اي منطقة الحجر الصحي كاسم تقريبي وفي هذا المنطقة سوف يتم تضييق جهاز المستخدم لما تتطلب الاجراءات لكي يتمكن من الدخول الى الشبكة وهذه العملية تكون بصورة اوتوماتيكية .

\*لو فرضنا انه هنالك شخص غير موظف في الشركة واراد استخدام الانترنت الخاص بالشركة فسوف يكون اتصاله ضمن منطقة تسمى **Guest Area** والتي تسمح له باستخدام الانترنت دون الدخول الى الشبكة الداخلية للشركة ..

### \*التهديدات التي تتعرض لها الشبكات :

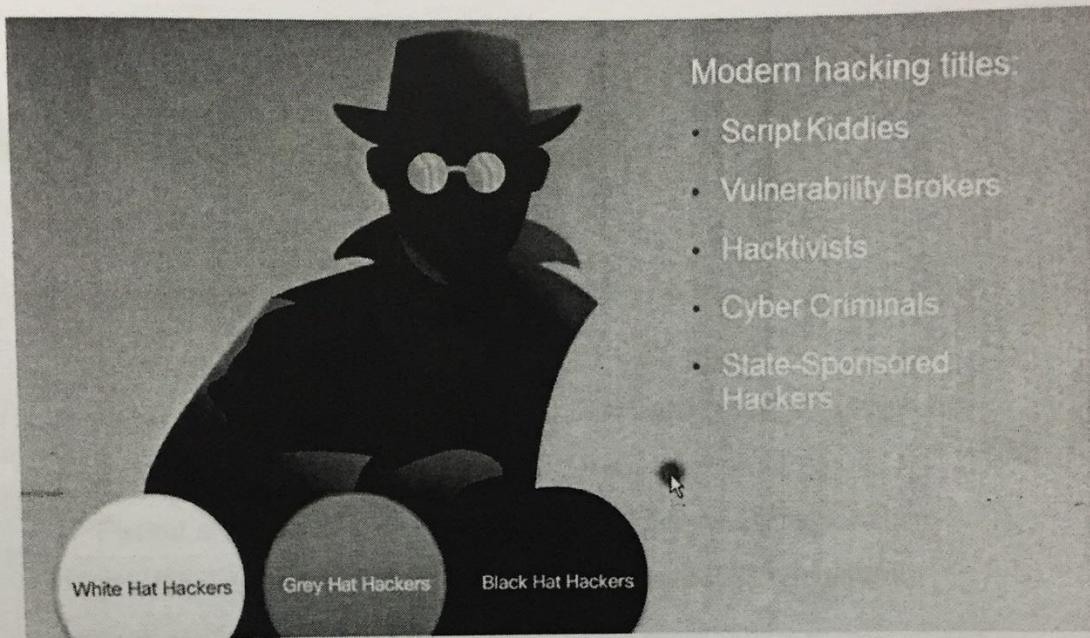
## Network Threats

Upon completion of the section, you should be able to:

- Describe the evolution of network security.
- Describe the various types of attack tools used by hackers.
- Describe malware.
- Explain common network attacks.

## \*أنواع الـ Hackers :

### The Hacker & The Evolution of Hackers



ينقسم الهاكرز الى ثلاثة أنواع وهم :

#### : White Hat Hackers – 1

وهم الهاكرز الذين في الصدفة يجدون ثغره في احد البرامج او الشبكات ويقومون بتثبيط الأدمن او مبرمجي البرامج بهذه الثغره لكي يتمكنوا من تجاوزها .

#### : Gray Hat Hackers – 2

وهم الهاكرز الذين يتم التعامل معهم من قبل الشركات لكي يعملوا على ايجاد الثغرات في البرامج او الشبكات الخاصه بهذه الشركات ولكي تتمكن الاداره من التخلص من هذا الثغرات بمساعدة هولاء الهاكرز ولكن هنالك مسالة عدم ثقه من قبل الشركات مع الهاكرز لانه لا توجد ضمانات احيانا بأنهم هم من سوف يحاولون الهجوم على شبكات او برامج الشركة .

#### : Black Hat Hackers – 3

وهم الهاكرز الذين يبحثون عن الثغره في البرامج او الشبكات لكي يتمكنوا من اختراقها والعبث بهذه البرامج او الشبكات .

\*الأدوات التي يمكن استخدامها لكي نعرف ما هي الثغرات لدينا في الشبكة :

## Evolution of Security Tools

Penetration testing tools:

- Password crackers
- Wireless hacking
- Network scanning and hacking
- Packet crafting
- Packet sniffers
- Rootkit detectors
- Fuzzers to search vulnerabilities
- Forensic
- Debuggers
- Hacking operating systems
- Encryption
- Vulnerability exploitation
- Vulnerability Scanners

هناك أدوات يمكننا استخدامها لكي نتمكن من التعرف على الثغرات التي توجد لدينا في الشبكة ولكي نتمكن من تجاوزها وحلها والتي مبيه في الجدول اعلاه .

## \* فئات او اصناف الـ Attacks :

### Categories of Attack Tools

Network hacking attacks:

- Eavesdropping
- Data modification
- IP address spoofing
- Password-based
- Denial-of-service
- Man-in-the-middle
- Compromised-key
- Sniffer

٤

#### : Eavesdropping – 1

وهو أحد أنواع الهجمات والتي تعمل على التجسس والتنصت على المكالمات الهاتفية .

#### : Data Modification – 2

وهو التعديل على البيانات المشفرة والتي لا يفهمها المهاجم وانما يعدل عليها لغرض تدميرها وعدم فه مها من المستلم في حال استلامه لهذه البيانات .

#### : IP Address Spoofing – 3

وهو أحد أنواع الهجمات وهي التحايل على المستلم على ان المهاجم هو المرسل الصحيح للبيانات .

#### : Password Based – 4

وهو التلاعب بكلمة المرور للبيانات المشفرة وعدم مقدرة المستلم من القدرة على فك التشفير بالباسورد الصحيح .

: DOS(Denial-of-Service) - 5

وهو أحد أهم أنواع الهجمات والذي يكون على نوعين :

### DOS(Denial-of-Service) – A

هذا النوع من الهجمات يكون على ثلاثة أنواع وهي :

## Ping Flood – 1

وهي عملية استغلال كل Session موجود على سيرفر معين والمستمرار بارسال Ping على هذا السيرفر الى حين استفاده كل Session عليه وايقافه (التوقف يكون لفترة معينة).

## Mail Bomp – 2

وهي عملية ارسال ايميلات وهمية الى اميل معين وتدمير الInBox لدى صاحب الاميل .

## Syn Attacks – 3

وهي العملية التي نعرفها والتي تتمثل بالـ 3 Way Hand Shake وهي فتح قناة اتصال مع سيرفر معين والسيرفر سوف يرد بأكشن Ack ويرسل Syn للحاسبيه ترسل Ack وهذا هو العادي لهذه العملية ، لكن في عملية الهجوم الحاسبيه ترسل Syn وبالتالي سوف يرد السيرفر بـ Ack ويرسل Syn وبعدها تستمر الحاسبيه بارسال Syn والسيرفر يرد الى ان يتوقف السيرفر ايضا

وهو النوع الأخطر من **Attacks** حيث ان المهاجم سوف يستغل حاسبة احد الاشخاص من خلال حاسبته ويقوم بالهجوم على سيرفر معين او شبكته من خلال حاسبة الشخص دون علم وتكون هذا العمليه هي استغلال الثغرات الموجودة داخل نظام احد الاشخاص . ويسمى **Zombie** **Man In The Middle - 6**

نـعـف كـيـفـة الـاهـمـهـ بـهـذـا الـطـرـيـقـ

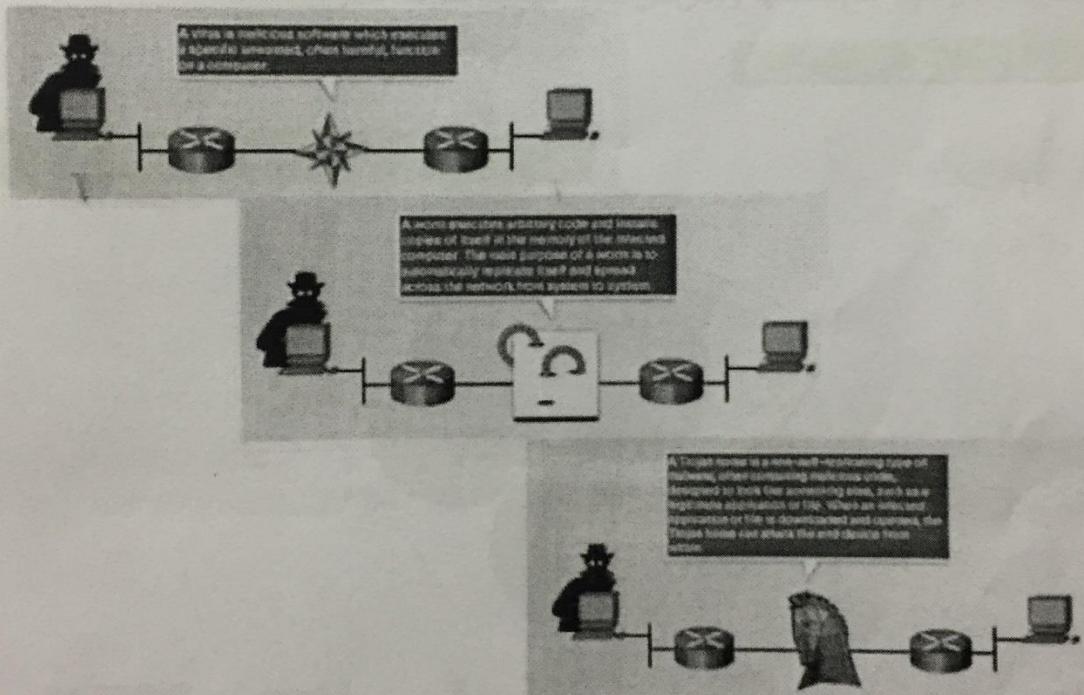
وهي عملية استغلال بروتوكول HTTP وانشاء صوره من الموقع الذي يرغب المستخدم الدخول له ولكن في الحقيقة المستخدم قد دخل الى موقع اخر غير الموقع المطلوب وذلك باستغلال المهاجم عملية Key – Compromised اي ارسال مفتاح للموقع بشكل خطا ووهبي .

: Sniffer – 8

وهي عملية تتبع البيانات في الكيل الخاص بشركة ما كمثال هو برنامج Wildshark الذي يعمل Capture للبيانات الماره من خلال كيل معين او لاين معين .

## البرامج الخبيثة\*: Malware\*

### Various Types of Malware



الـMalware تعني برامج خبيثه وتكون على ثلاثة أنواع هي :

Virus – 1

نقصد هنا بالفايروس هي إنشاء برنامج يعمل على تدمير الشبكة او مجموعه من الحاسبات ولنفرض ان هنالك فلاش يحوي على هذا الفايروس وتم تشغيل ذلك الفلاش داخل احد الحاسبات فسوف ي العمل الفايروس مباشرة داخل الشبكة الداخله لشركة ما وي العمل على تدمير بيانات او اي شيء تم انشاء هذا الفايروس لكي ي عمله .

## 2 – Worm

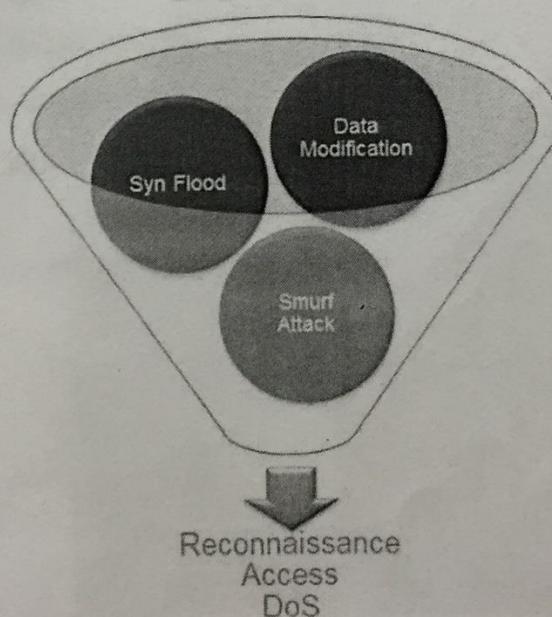
وهي عباره عن فايروس ايضا يعمل على ايذاء الشبكة والحسابات وكان اول من انشاء هذه النوع هو شخص اسمه موريس وتم تسمية الفايروس على اسمه موريس وورم حيث استغل في البدايه انظمة اللينكس القديمه لكي ياذيها من خلال التغيرات التي كانت تحويها هذه الاجهزه .  
اي انه برنامج ينسلخ من الشبكة ي مجرد اعمال الغلاش بالاسه دون فتح الغلاش

## 3 – Trojan Horse

وهو فايروس يسمى حصان طرواده ويكون على شكل برنامج عادي يمكن تنصيبه على اي حاسبه ولكن داخل هذا البرنامج يوجد هذا الفايروس والذي يعمل ايضا على ايذاء الشبكة والحسابات المرتبطة مع بعضها ولنفرض شبكه داخليه لشركة ما .

## \* انواع الهجمات على الشبكات :

## Types of Network Attacks



وتكون الهجمات على الشبكات على ثلاثة أنواع وهي :

## Reconnaissance Attacks – 1

وتعني حب استطلاع ومن خلاله يعمل المهاجم على الشبكة على معرفة معلومه هو يريدها مثل معرفة الحد المستخدم من الاي بي داخل الشبكة وما هو الاي بي الفعال حالياً ويعمل عليه Ports Lookup وهي عملية منعرفة اي البورات المفتوحة داخل هذه الحاسبه مثلاً وهذا كله حب استطلاع لدى المهاجم .

ولكن لو استغل المهاجم هذه العملية لكي يستخدمها بهجوم اكبر هنا سوف تكون مشكله كبيره  
ويجب غلق هذه البورت بعد عملية اعادة البحث عن الثغرات داخل حاسبة المستخدم لكي يتم  
غلقها .

## Reconnaissance Attacks

- Initial query of a target
  - Ping sweep of the target network
  - Port scan of active IP addresses
  - Vulnerability scanners
  - Exploitation tools



للتعرف على موقعة IP address من خلال نفع الـ Whois Lookup على الموقع المزبور

في الحقيقة إذا اتفق لم يتم ~~التحقق~~ ~~التحقق~~ على الحاله اريد ان انتبه في حين  
نخاف من اتفاق التعامل مع ادار admin (ie) المفزع بوكاً لل  
Whois lookup

## Access Attacks – 2

وهي عملية الاستفاده من المعلومات التي تم جمعها بصفة حب الاستطلاع لكي يتم الهجم على الشبكة من خلا لاستغلال تلك المعلومات ومن هذا الهجمات هي :

### Access Attacks

A few reasons why hackers use access attacks:

- To retrieve data
- To gain access
- To escalate access privileges

A few types of access attacks include:

- A • Password
- B • Trust exploitation
- C • Port redirection
- D • Man-in-the-middle
- E • Buffer overflow
- F • IP, MAC, DHCP spoofing

ولنفرض تم معرفة الباسورد **(A)** للشبكة ولكن كان هذا الباسورد بصيغه مشفره ويريد الهاكرز فك تشفير هذا الباسورد فهناك طریقتين لهذه العملية هما :

### Brute Force Attack – 1

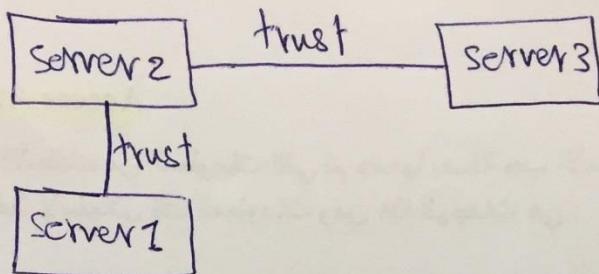
في هذا النوع يوجد مثلا موقع تعمل على فك تشفير الباسورد المشفر بطريقة MD5 حيث سوف تعمل على خوارزميه معينه لفك التشفير هذا بمنهج الصواب والخطأ في عملية البحث .

### Rainbow Attack – 2

وهو عباره عن فرض هناك كلمات شائعه يستخدمها صاحب الباسورد ويتم وضع هذه الكلمات ضمن جدول حيث يقوم برنامج معين على مطابقة الباسورد المشفر مع هذه الكلمات لحين الوصول الى الكلمه الصحيحه .

### (التجسس) Trust exploitation (B)

الشبكة المترابطة (trust topology) هي الشبكة التي



لوكان يمكن أن يكون بين S3 و S2 و S1 في trust relationship.  
ولوكان يمكن أن يكون بين S3 و S1 في distrust relationship.  
ذلك في النوع من الاتaccoن يقوم S1 بـspoofing attack على S3 و S1 يتحقق ذلك لأن S1 هو بين S3 و S1 و يدخل S3 كـmid-node.

### : Port redirection (C)

يمكن لوكان أن يحول port من server إلى user أو يحول port من user إلى server.  
ويمكن لوكان أن يحول port من attacker إلى victim أو يحول port من victim إلى attacker.  
أو يحول port من victim إلى another server.

### : man-in-the-middle-attack (D)

attacker ي Intercept traffic between victim and server -> Buffer overflow (E)  
syn attack / die attack

destination يخترع ويتحقق أن الأطلاع على victim ->  
victim يتحقق أن الأطلاع على victim

- IP spoofing
- MAC spoofing
- DHCP spoofing

client يتحقق أن victim يرسل DHCP request أو IP أو victim يتحقق أن victim يرسل DHCP request

# Social Engineering Attacks

- Pretexting
  - Phishing
  - Spearphishing
  - Spam
  - Tailgating
  - Something for Something
  - Baiting

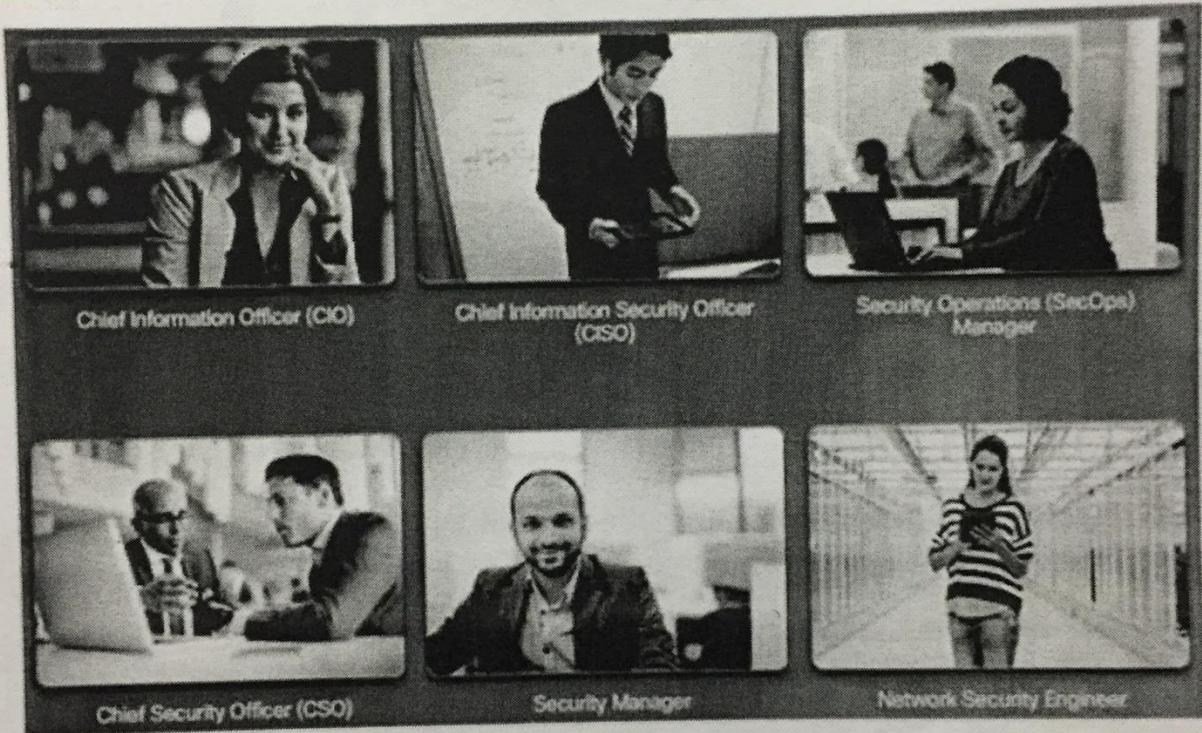


وهو من أخطر انواع الهجمات ويقصد به عملية التحايل على أدمن لشركة ما وايهامه بأن الشخص الهاكرز هو موظف في شركة اخرى يريد بعض المعلومات عن اجهزة الشركة وطريقة الربط (المساعدته لا اكتر) ولكن بهذه الطريقة هو اخذ معلومات بصورة غير مباشرة والاستفاده منها بعملية الهجوم .

### \*طريقة الحماية من الهجمات (الهاكرز) :

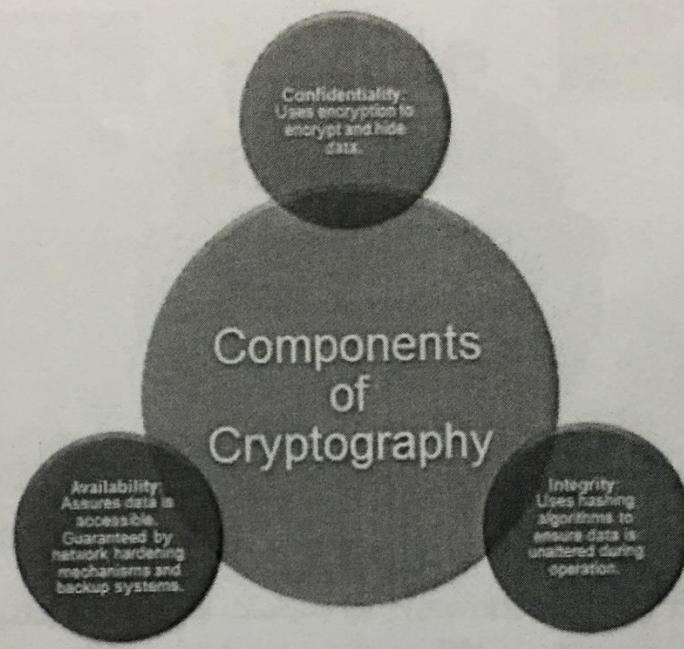
في بداية الامر هنالك مصطلحات للمقيمين على امنية الشبكات وهي تسميات تطلقها شركة سسکو على العاملين في مجال امنية الشبكات :

## Network Security Professionals



\* اي نظام امني يجب ان يحوي على الثلاث امور التالية :

## Confidentiality, Integrity, Availability



### :Confidentiality

وهي الحفاظ على المعلومات من الاختراق اي ارسالها دائمًا مشفرة

### :Availability

وهي عملية ابقاء الشبكة دائمًا متاحة للمستخدم من بيانات وما الى ذلك

### :Integrity

وهي عملية ضمان عدم التلاعب بالبيانات أثناء ارسالها الى هدف معين من خلال عملية ال Hashing التي تكون كمثال بال MD5

## Network Security Policy



يقصد هنا بالـ Network Security Policy هو السياسات التي يضعها القائمين على الشبكة كمثال بالنسبة لكلمة المرور يجب ان لا تقل عن 8 رموز وهذا حسب الامور التي يحددها الأدمن .

## Cisco Network Foundation Protection Framework\*

### Cisco Network Foundation Protection Framework



هو عملية تامين كل Data التي تمر من خلال كيبل معين وكما نعرف ان اي Traffic يتقسم الى ثلاثة أنواع :

Control Plane - 1 : قتل او Removal of protocols updates مثل STP او EIGRP او OSPF في الاتصال

Data Plane - 2 : وهم ابيانات المسندة والمسلطة

Management Plane - 3 : وهم البروتوكولات المستخدمة في الادارة

المفروض هو عملية تامين كل نوع من هذا الانواع

النوع الاول يتم تامين البيانات التي تتبادلها السوتجات والراوترات كالتحديث وما الى ذلك

النوع الثاني هو تامين البيانات وجعلها مشفرة

النوع الثالث هو تامين عملية الاتصال كالاتصال عن بعد مثل Telnet و SNMP و SSH

## Lec 2

CCNA - Security

### Chapter // 2

#### : CCP (Cisco Configuration Professional)\*

هو عباره عن برنامج يمكن التحكم برواترات وسوتجات شركة سيسكو من خلاله وهو عملية تسهيل ارسال الايمايل من اوامر من هذا البرنامج الى الرواتر مثلا وتطبيق تلك الاوامر على الرواتر سيتم شرح عملية التنصيب لهذه التقنيه .

\*بالنسبة لـ Chapter 2 سوف يضم المواضيع التالية :

## Lec 3

### Chapter Outline

- 2.0 Introduction
- 2.1 Securing Device Access
- 2.2 Assigning Administrative Roles
- 2.3 Monitoring and Managing Devices
- 2.4 Using Automated Security Features
- 2.5 Securing the Control Plane
- 2.6 Summary

• تفعي ادخال احصار الاعدادات على المراوتر Configuration by CLI

بعودة بيرفيت كاعملنا ان ندرس

administrator pc : وتفعل انتا نطبب برنامج على المراوتر  
(CC P) : وتفعل ادارات يحصلة على المراوتر وتدخل البرنامج ومن خلال البرنامج الاعدادات  
كالى سلسلة (فقط اختيارات ) ويقوم CC P بتنفيذ هذه الاختيارات التي اولها  
دارجها على المراوتر  
30 امر في المراوتر ولكن بواسطه او  
(CC P) تتحكم في المراوتر  
فقط اختيارات تكسسات ونحوها الامثلية

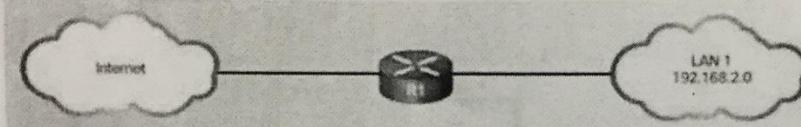
### : Securing Devices Access\*

في هذا الموضوع سوف نتكلم عن طريقة تامين مختلف الأمور في اي شبكة ممكن ان نعمل عليها .

عند تصميم اي شبكة فهناك ثلات سيناريوهات للتصميم وهم :

## Edge Router Security Approaches

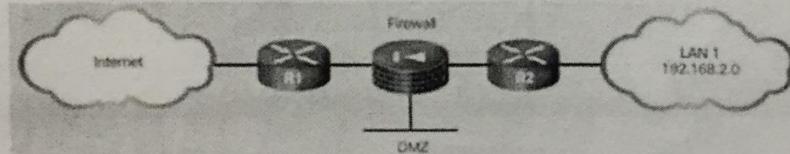
Single Router Approach



Defense in Depth Approach



DMZ Approach



### : Single Router Approach – 1

وهي طريقة التصميم العادي وهي ربط انترفيس بال-LAN وانترفيس آخر بال-WAN

### : Defense in Depth Approach – 2

وهي طريقة وضع كما يسمى بالجدار الناري Firewall لحماية الشبكة والطريقة كما مبينه بالشكل الثاني للربط .

\*في ما يخص الـ Firewall ويخلص كالتالي :

هناك نوعين من الـ Firewall وهو اما ان يكون سوفت وير او يكون هارد وير

: انواع الـ Software Firewall – A

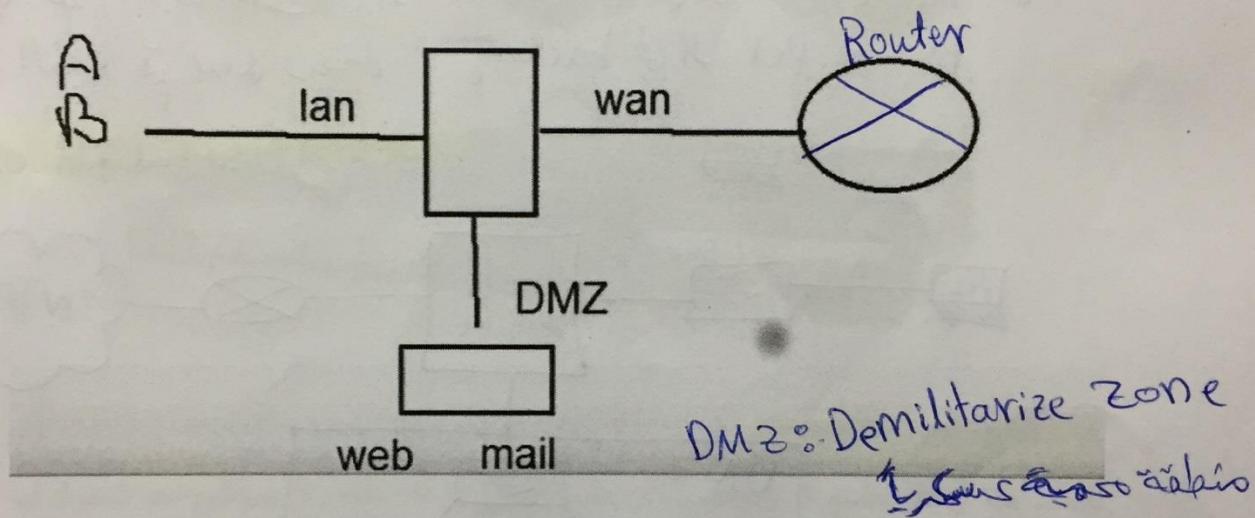
FIREWALLD / IPTABLES / IPCHAIN / TMG / ISA من انواعه /  
Firewall لعمل كل الـ Network

: انواع الـ Hardware Firewall – B

ASA Cisco / PIX Cisco من انواعه /

: DMZ Approach – 3

يقصد بالـ DMZ (Demilitarized Zone) وكما موضحه بالشكل اعلاه والشكل التالي :

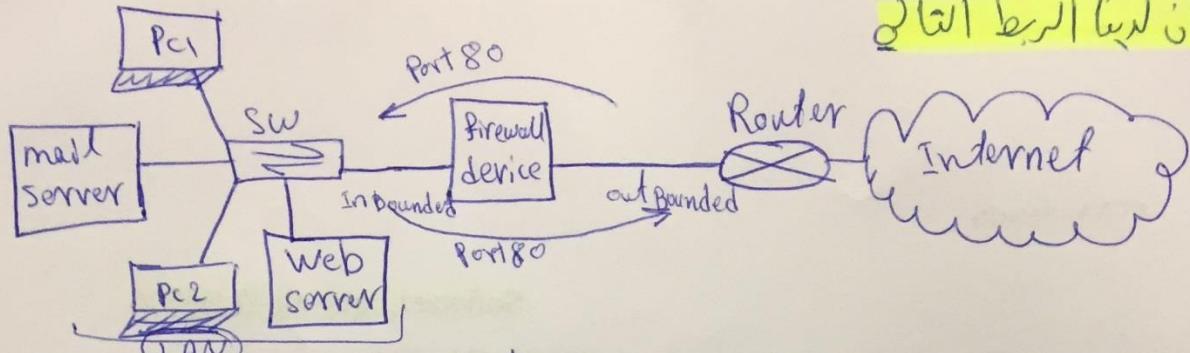


عندما يريد احد الاتصال بالويب سيرفر فيجب ان يكون الپورت 80 مفتوح في داخل Firewall ومن الاناحه الامنيه تم وضع الويب سيرفر في المنطقه المعنوزله التي يطلق عليها بالـ DMZ لكي تحمي الشبکه الداخلية من الاختراق .

. من المسائل المفضلة وضع 2 جدار ناري بالتتابع في الشبکه لكي تتم الحمايه بشكل عالي . (⊗)

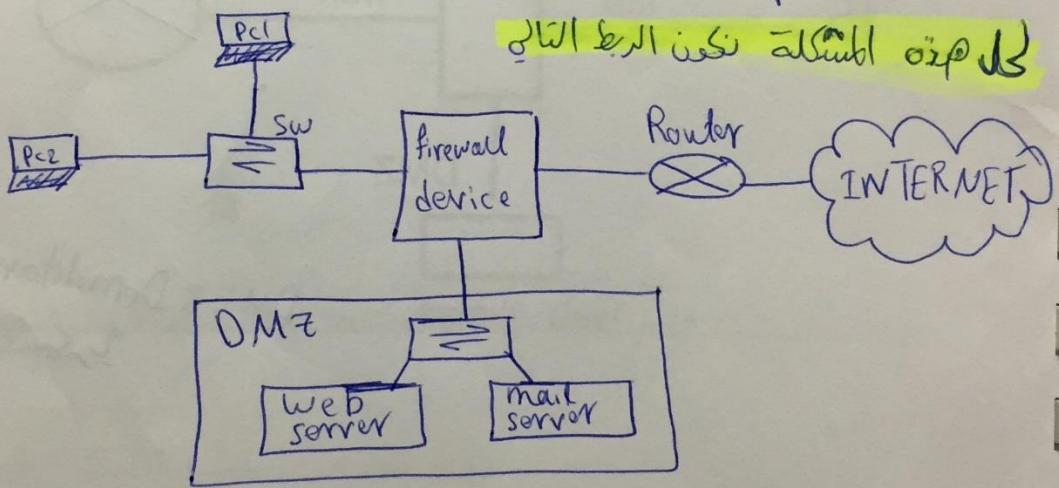
ملاحظة حول DMZ

كما نعلم ان الـ Firewall device يحتوي على 2 LAN و 1 WAN . واصبح يمكنه بالـ Router باتجاه الـ WAN واخفريله بـ LAN .



لو كان ليناً الربط الآتي  
فإن PC1 و PC2 يفتحان بفتحة 80  
port = 80

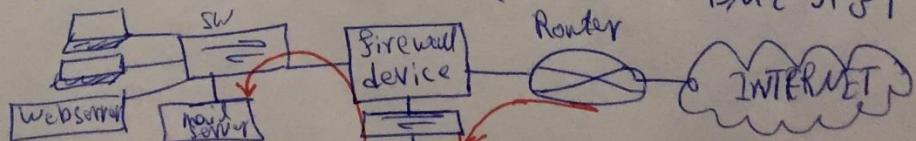
mail server أو web server في Internet OUT أو IN في Firewall  
وأيضاً هي users التي تدخل من هنا  
IN أو OUT في Firewall device port 80 أو 180  
mail server في Internet يفتح بفتحة 80  
ما يسمى بـ "IP spoofing"  
PC1 أو PC2 في hacking داخل DMZ



وهي نفس الربط السابق ولكن نفع في LAN (مزودة بـ DMZ)  
DMZ هي المكان الذي يدخل فيه switch أو servers وينتهي في switch

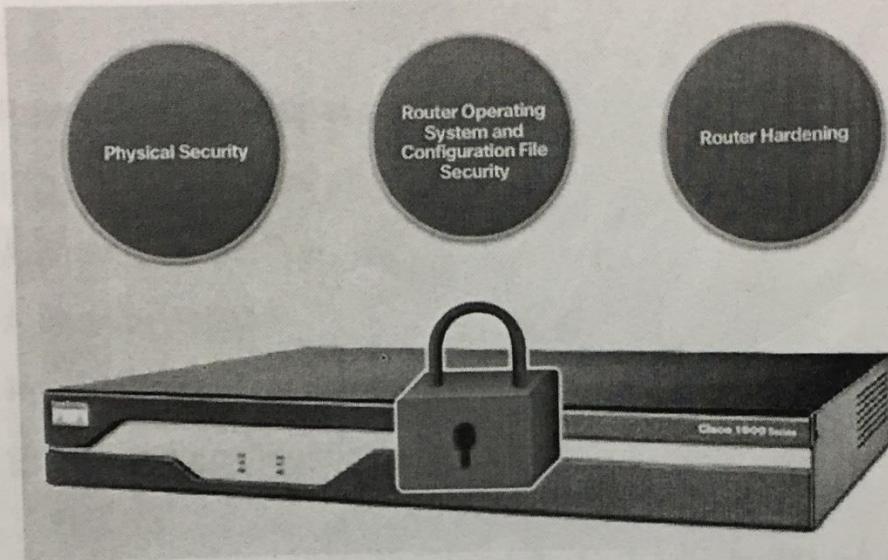
- DMZ والRouter يفتحان Port 80  
ونفتح 80 في DMZ والوصول إلى DMZ  
web server أو mail server أو PC1 أو PC2  
لأنها كانت المكان الذي يفتح فيه المخدم

Software على LAN يفتح المخدم  
WAN DMZ على Portal قارئ PC على  
mail server على Portal يوماً ما  
يمكن أن يفتح المخدم على WAN



\*المناطق الواجب تأمينها في الشبكة :

## Three Areas of Router Security



### :Physical Security – A

نقصد هنا ان يتم وضع الرواوترات بمكان مأمن اي في غرفه مغلقه ولا يستطيع احد الدخول لها الا من هم مصرح لهم .

### :Router Operating System & Config File Security – B

كمثال لو أحد أراد مسح او التلاعب بالكونفريشن سوف لن يستطيع (سيتم شرحها لاحقاً) .

### :Router Hardening – C

لو أردنا الاتصال والدخول على الرواوتر فيجب أن يكون الاتصال عن بعد مأمن وباستخدام SSH وأطفاء اي Services غير مطلوبه .

## Secure Administrative Access

Tasks:

- Restrict device accessibility
- Log and account for all access
- Authenticate access
- Authorize actions
- Present legal notification
- Ensure the confidentiality of data

- 1 – ليس أي أحد قادر على الدخول على الراوتر فقط الأدمين المصرح له بذلك .
- 2 – أعطاء صلاحيات مختلفة لكل مستخدم وفي حال احد المستخدمين عمل خطأ فسوف يظهر لنا Log Message .
- 3 – الـ Authenticate وهي التحقق من المستخدم في حال طلب الدخول الى الشبكة .
- 4 – الـ Authorize وهي اعطاء الصلاحيات التابعه لكل مستخدم بعد التتحقق .
- 5 – أظهار Log Message لكل حدث سوف يحصل في الشبكة .
- 6 – التأكد من سرية البيانات داخل الشبكة .

\*في ما يخص كتابة كلمات المرور هناك أمور يجب مراعاتها أثناء تهيئة كلمة المرور وهي :

## Strong Passwords

### Guidelines:

- Use a password length of 10 or more characters.
- Include a mix of uppercase and lowercase letters, numbers, symbols, and spaces.
- Avoid passwords based on easily identifiable pieces of information.
- Deliberately misspell a password (Smith = Smyth = 5mYth).
- Change passwords often.
- Do not write passwords down and leave them in obvious places.

Weak Password	Why it is Weak	Strong Password	Why it is Strong
secret	Simple dictionary password	b67n42d39c	Combines alphanumeric characters
smith	Mother's maiden name	12^h u4@1p7	Combines alphanumeric characters, symbols, and includes a space
toyota	Make of car		
bob1967	Name and birthday of user		
Blueleaf23	Simple words and numbers		

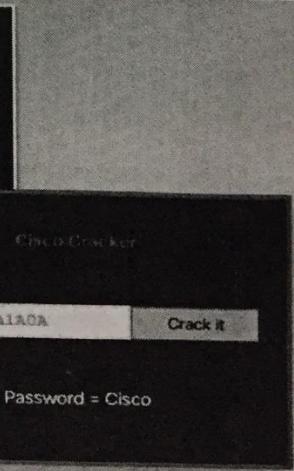
## Increasing Access Security

```
R1(config)# security passwords min-length 10
R1(config)# service password-encryption
R1(config)# line vty 0 4
R1(config-line)# exec-timeout 3 30
R1(config-line)# line console 0
R1(config-line)# exec-timeout 3 30
```

```
R1(config)# service password-encryption
R1(config)# exit
R1# show running-config

<output omitted>

line con 0
  exec-timeout 3 30
  password 7 094F471A1A0A
  login
line aux 0
  exec-timeout 3 30
  password 7 094F471A1A0A
  login
line vty 0 4
  password 7 094F471A1A0A
  login
```



**CCNA - Security**

```
R1(config)#  
R1(config)#  
R1(config)#security passwords min-length ?  
    <0-16> Minimum length of all user/enable passwords  
  
R1(config)#security passwords min-length 8  
R1(config)#us  
R1(config)#username Abawy pa  
R1(config)#username Abawy password 12345678  
R1(config)#
```

الأوامر أعلاه هي لتحديد طول كلمة المروور والتي تكون رموزها بين الـ 0 الى الـ 16

```
R1(config)#enable ?
  algorithm-type  Algorithm to use for hashing the plaintext 'enable' secret
  password        Assign the privileged level password (MAX of 25 characters)
  secret          Assign the privileged level secret (MAX of 25 characters)

R1(config)#enable algorithm-type ?
  md5      Encode the password using the MD5 algorithm
  scrypt   Encode the password using the SCRYPT hashing algorithm
  sha256   Encode the password using the PBKDF2 hashing algorithm

R1(config)#enable algorithm-type scrypt secret 123
R1(config)#[
```

- الأمر أعلاه هو لتشغيل **Enable Password** والذى يكون على ثلاثة أنواع كما

میں اعلاہ و ہم :

پسورد وسم: MD5 - 1

وهذا يكون Level 9 وهو أقوى انواع التشفير Scrypt – 2

Scrypt وهذا يكون Level 8 ويكون بعد الـ SHA256 – 3

```
R1(config)#username abeer algorithm-type ?  
  md5      Encode the password using the MD5 algorithm  
  scrypt   Encode the password using the SCRYPT hashing algorithm  
  sha256   Encode the password using the PBKDF2 hashing algorithm  
  
R1(config)#username abeer algorithm-type sha256 secret 123  
R1(config)#[
```

لأجل الأمان، يتم تشفير كلمة المرور لأسم المستخدم وتم استخدام الشا256

عندما ندخل على الـ Router أو Switch ندخل على him بـ Username و Password

الرقمي & passwords II من الـ

Router أو Switch أو IPsec مع \*

R(config)# security passwords min-length [no. of letters]

الـ enable password مع Password of username first \*

enable Password SSH و telnet

R(config)# username [username] password [password]

Privileged mode II II User mode II we will password has \*

- R(config)# enable password [password]

الـ enable password  
عنوان، وكلمة سر

- R(config)#enable secret [password]

الـ enable password has

Level 8 ← Sha56 , level 9 ← script , MD5 لـ

R(config)# username [username] algorithm-type

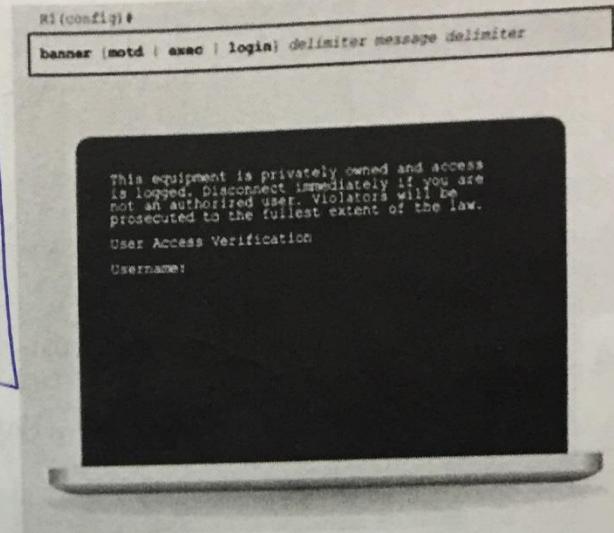
MD5
script
sha56

secret [password]

## Enhancing the Login Process

### Virtual login security enhancements

- Implement delays between successive login attempts
- Enable login shutdown if DoS attacks are suspected
- Generate system-logging messages for login detection



\*لتحسين الأمان في الدخول الى الراوتر عن بعد فهناك اوامر مهمة ومفيدة لهذه العملية وهي:-

الأمر التالي :-

```
R1(config)#login block-for 60 attempts 3 win  
R1(config)#login block-for 60 attempts 3 wit  
R1(config)#login block-for 60 attempts 3 within 30  
R1(config)#[
```

- نقصد بالأمر اعلاه هو في حال حاول احدهم الدخول الى الراوتر عن بعد وادخل الـ Password بصوره خطأ 3 مرات خلال 30 ثانية فاؤقف عملية الدخول لهذا الشخص لمدة 60 ثانية.

وهو نوع من العقاب في حالة اهلا حاول

Broad force attack او Router يغلق

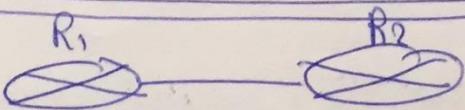
حالة طلاق اتفاقاً على وثائق VTY

R1(config)# line VTY 0 4

R(conf-line) # login local

R(cront) # user name mohammed password 123

Rc.conf) # login block-for 60 attempts 3 within 30



R<sub>2</sub> و محمل افرادی telnet like

R, # Show Login

اداً اعْلَمُنَا امْر

Router present in  Normal-mode  
Router present in Quiet-mode

سُوقِ الْأَنْطَلِ

username & password (لیے لئے) :- ونجیان الگیا Normal-mode

يُواصَفُ بِالْعَدَدِ الْكَبِيرِ وَيُجَاهَنُ بِهِ الْمُهَاجِرُونَ إِذَا دَخَلُوا إِلَيْهِمْ مِنْ أَنْوَارِ الْأَرْضِ

وتحتاج اجهزة في حالة حفظ لمرة 60 دقيقة Quiet mode

وزمله لخلاق المثل اعلاه

يمكن تطبيق الامر التالي:

```
R1#show login failures
Total failed logins: 9
Detailed information about last 50 failures

Username      SourceIPAddr    IP Port Count TimeStamp
f             10.0.0.2        23   1     14:05:38 UTC Sat Nov 12 2016
fd            10.0.0.2        23   1     14:05:40 UTC Sat Nov 12 2016
h             10.0.0.2        23   1     14:05:42 UTC Sat Nov 12 2016
tg            10.0.0.2        23   1     14:07:24 UTC Sat Nov 12 2016
s             10.0.0.2        23   3     14:11:52 UTC Sat Nov 12 2016
d             10.0.0.2        23   1     14:11:54 UTC Sat Nov 12 2016
q             10.0.0.2        23   1     14:11:57 UTC Sat Nov 12 2016
```

والذي نستفاد منه لمعرفة عدد مرات الفشل في الدخول الى الراوتر من قبل المستخدمين .

\* الاوامر الأخرى التابعة للـ Login هي :

```
R1(config)#login ?
block-for  Set quiet-mode active time period
delay      Set delay between successive fail login
on-failure Set options for failed login attempt
on-success Set options for successful login attempt
quiet-mode Set quiet-mode options

R1(config)#login on-success log
R1(config)#login on-f
R1(config)#login on-failure log
R1(config)#[
```

- لطبقنا الأمر Login on-success وفائدته هو اعلامنا بمن هو الذي دخل الان ويظهر لنا اسم المستخدم ووقت الدخول وإذا عمل خروج ايضا سوف تظهر لنا معلومات

حول الخروج من الراوتر . (هذا الامر يشمل او telnet & console)

- لطبقنا الأمر Login on-failure وفائدته هو اعلامنا بمن هو الذي اراد الدخول الى

الراوتر ولم يستطع ذلك بسبب عدم معرفته بكلمة المرور او اسم المستخدم (هذا الامر يشمل telnet & console)

- لطبقنا امر Login delay (time in second) وفائدته عـ وقت مـسـقطـعـ بـيـنـ

محاـولةـ دخـولـ وـاـخـرـىـ حـسـبـ وـقـتـ يـتمـ تحـديـدـهـ مـنـ قـبـلـ الأـدـمـنـ .ـ (ـاـيـ مـذـكـرـةـ Pa~as~word~ وـصـاحـوةـ كـمـيـةـ Pa~as~word~ أـخـرـىـ)

- لطبقنا امر (Login quiet-mode+Acc) (ـعـاـمـنـاـ نـسـعـ يـدـهـفـلـ)

الـ Rـ 1ـ telnetـ كـ usersـ الـ Blockـ فيـ عـاـلـةـ اـفـلـ

الـ Usernameـ & passwordـ اـكـثـرـ مـرـدـدـ صـرـةـ بـالـ طـاـلـاـ بـالـ فـيـ هـذـاـ النـفـعـ

عـقـطـ نـجـلـعـ الـ Rـ 1ـ يـعـاقـبـ الـ usersـ الـ يـعـقـدـ بـ الـ اـسـمـ الـ اـسـمـ

R1(config)# login quiet-mode access-class 1

R1(config)# access-list 1 permit 10.0.0.0 0.0.0.255

R1# show login failures

## Remotely login ( او حماية الـ login )

في حالة نجاح تسجيل الدخول user في حالة ادخاله 3 مرات خاطئة في 30 ثانية فانه يفتح بعدها 60 ثانية ثم يفتح بعدها 30 ثانية

R(config)# login block-for 60 attempts 3 within 30

لما يتحقق كل هذه الشروط ينقطع الدخول

R(config)# login delay

لتحقيق ذلك يدخل الرفتر وتحت الرفع وتحت آخر من الاوصاف التي تدخل الرفع للاستفادة

R(config)# login on-success log

لتحقيق ذلك الراتس يتم تشغيله على كل بوابة

R(config)# login on-failure log

لتحقيق ذلك يجب تعيين رفع على الـ Remote access

R# Show login failure

## Steps for Configuring SSH

### Example SSH Configuration

```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

R1(config)#
*Feb 16 21:18:41.977: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# ip ssh version 2
R1(config)# username Bob algorithm-type scrypt secret cisco54321
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# end
R1#
```

### Example Verification of SSH

```
R1# show crypto key summary rsa
* Key pair was generated at: 21:18:41 UTC Feb 16 2015
Key name: R1.span.com
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
30819730 0D6092A 86488E87 00010101 05000301 8D003081 89028101 00CF35DB
A58A1BDB F7C78600 F189CF3 2E06E584 0923E25B 71841D98 B5472A03 D19CD620
ED125829 5A58412B B7F29234 0E2A1B09 6C421AC3 07F298E6 80DE149D 2A2E2E13
748880AF CAC8F197 B11111AF A413E76F EC157CDF DEFE0082 2961B58C BE1CAD21
176E82B9 5081F933 06E66C93 94E1C908 88746276 90AC63CE 5E169845 C1020301 0001
* Key pair was generated at: 21:18:42 UTC Feb 16 2015
Key name: R1.span.com server
Key type: RSA KEYS
Temporary Key
Usage: Encryption Key
Key is not exportable.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B0C 30680261 00AB914D 8172DFBE
DE57AC49 1B944219 1F3985942 3943ACD F5487746 3995CF54 E68C1961 8A44FEB3
IA019F27 D9E71AAB FC71F423 A59CB9F5 50289272 3392CEBC 4C3CB060 DB9231DE
90019CAD 79D58165 423JA862 FD1CRABZ 7AB059DC 2490C795 ED020301 0001
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# crypto key zeroize rsa
* All keys will be removed.
* All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
R1(config)
```

## Configuration of SSH

R(config)# IP domain domain name ex: CISCO.COM

R(config)# crypto key generate rsa generate-keys modulus key size ex 1024

R(config)# IP ssh version 2

R(config)# username new algorithm-type scrypt secret 123

R(config)# login vty 0 4

R(config)# transport input ssh ← Set default line

SSH J1 S1/2

## Privilege Configuration

## Privilege Levels :-

Lee u

If is used to define what particular command a user can run or they logged into device.

نیز ممکن است که هر کاربر کوچکتر از سطح کاربر ادمین (admin) باشد و در این صورت می‌تواند تنها برخی از قابلیت‌های سطح کاربر ادمین را داشته باشد. این مفهوم به عنوان سطوح امتیازات (privilege levels) نیز شناخته می‌شود.

There are three modes in CISCO devices

- User EXEC mode >
  - Privilege EXEC mode #
  - Configuration mode (conf) #

## Privilege Levels Name

$(0, 1, 15)$  ← by default  $\text{env}[\text{levels}] = \text{K}[\text{levels}]$

By default

- user Exec mode → Level 0

- User EXCL mode → level  
where level 0 contains exit → to exit from this level

- ④ help → to identify meaning of command
  - ④ enable → to move to privilege mode

- Privilege Exec mode → Level 1

Where level 1 contain all test command and remot access  
④ Show -

- ④ Show -  
④ telnet

- Configuration mode → Level 15

Where level 15 contains all commands can be done in the device

the device

١٤) يُمكِّنُ ان تكتنُ Levels من ٢ ← اجهزة لـ Set مُستوى المُخدر لـ حافظة / يُمكِّنُ  
the device

## \*تفعيل الصلاحيات عن طريق الـ Privilege Configuration

```
R3(config)#privilege exec ?  
    all    All suboption will be set to the samelevel  
    level  Set privilege level of command  
    reset  Reset privilege level of command  
  
R3(config)#privilege exec level 0 ?  
    LINE  Initial keywords of the command to modify  
  
R3(config)#privilege exec level 0 show run int f0/0
```

\*يقصد هنا هو تفعيل الصلاحيات بالنسبة للأوامر كمان Show وتحويله من مود الى مود آخر بالإضافة لأوامر **Privilege Model** التي في المقدمة مثل exec في الأمر اعلاه تم تمكن المستخدم من Level 0 من أمكانية فعل أمر Show على **exec mode** **Enable Mode**

```
R3(config)#  
R3(config)#username abeer priv 0 pass 123  
R3(config)#
```

\*في الأمر اعلاه تم وضع اسم المستخدم وكلمة المرور في **Priv 0**.  
ملاحظة: يمكن رفع الأوامر من مود الى مود اخر او من مود أعلى الى مود ادنى وكما نعرف ان في اجهزة سيسكو هذا لايك 15 مود.

## القائمة الأساسية في ار (Hierarchical Privilege Level)

يسمح ان يدخل كل اد اسفله **Level 10** the **Levels** التي تحته **Level 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10**, **Level 10** يسمح ان يدخل اد اسفله في **Level 6** فقط

عندما نقوم بعمل level 15 في الواقع level 15 ليس له أي صلاحيات  
 level 15 يقوم بنسخ level 1 في كل الأحوال

### Level (15)

- router ospf 1
- access-list

### Level (1)

- show run
- telnet

### Level (0)

- enable
- exit

Making new Level (7)

### Level (15)

- router ospf 1
- access-list

### Level (7)

- access-list
- telnet

### Level 1

- show run

### Level 0

- enable
- Exit

### Configuration of Privilege Level

R1

Router configuration mode  
level 15

R2

R(conf)# privilege [EXEC  
Configure  
Interface] level [From  
e→15] [Command]

EXEC → means this command under Exec mode (user or privilege)

configure → means this command under major configuration mode

Interface → means this command under interface mode

(admin) user N password → username تكون

R(conf)# username [username] privilege [e→15] password [password]

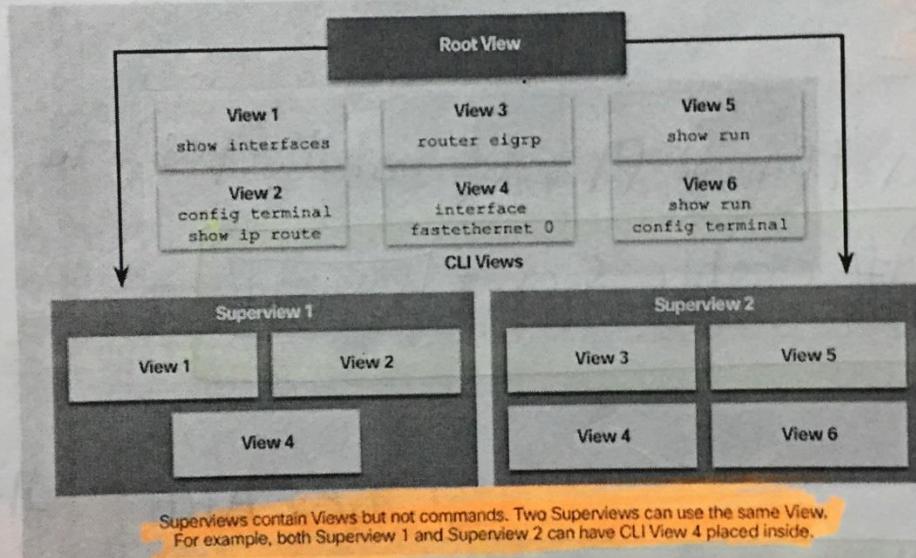
عندما ندخل إلى level 15 لا يظهر ping command في terminal  
 level 15 لا يظهر ping command في terminal  
 level 15 لا يظهر ping command في terminal  
 level 15 لا يظهر ping command في terminal

## Configuring Role-Based CLI



هناك طريقة أخرى أفضل وتعمل على الأصدارات الحديثة من نظم تشغيل الروتارات والسوتجات تسمى بالـ Parser View وتسمي أيضاً Configuring Role – Based CLI

## Role-Based Views



طريقة عمل CLI او ان صح التعبير طريقة تفكيرها هي ان هناك Root View رئيسي يعمي فيه كل الاوامر ويمكن عمل انشاء تحت هذا الروت Superview وتحت السوبر يمكن انشاء View صغيره ويمكن ربطها مع مستخدم حسب الحاجه كمثال ربط View 1 مع مستخدم محمد و View 2 مع المستخدم احمد وهكذا . **ولو وظفحت View 1 و View 2 في Superview محمد** في حالة تم حذف View 1 و View 2 فانه لا تختلف Superview في حال حذف Views التي تحويها .

حيث ان Parser View هي الـ **惟一** View يمكن لنفس الممر تحت عدة Views اذا **بقيا** معاً **بكل View**

## Configuration Parser View

### Privilege Mode

R> enable ← Privilege mode

R> enable view → Root View

password view رسمياً privilege view وال root view دعك

~~الكلمات السرية~~

### Part one

(secret password) Privilege mode في Password mode ١

R(conf)# enable secret [password]

R(conf)# aaa new-model

Root view على نفس الـ user mode

privilege mode على نفس الـ GNS3 ٢

enable على نفس الـ user mode

enable على نفس الـ user mode

\*طريقة تفعيل هذه التقنية بالأوامر التالية:

```

1 R2(config)#enable se
R2(config)#enable secret 123
R2(config)#aaa
R2(config)#aaa n
R2(config)#aaa ne
R2(config)#aaa new-model
R2(config)#enable secret 123
R2(config)aaa new-model
R2(config)exit
[redacted]
*Jan 22 16:47:42.359: %SYS-5-CONFIG_I: Configured from console by console
R2>disable
R2>enable
R2>enable vi
R2>enable view
Password:
R2#
*Jan 22 16:48:14.883: %PARSER-6-VIEW_SWITCH: successfully set to view 'root'.
R2#

```

enable secret او Enable password

aaa new-model

exit -3

4- تطبيق أمر enable view وب مجرد ضغط enter سوف يطلب كلمة المرور التي وضعناها في enable view

لـ Root View (نحو ٣ خط)  
لو طبقنا امر show parser view سوف يبلغنا بانتهاء Root View

ملاحظة: في الـ Parser View سوف يكون لكل مستخدم enable Password مرتبطة بها.

## Part two

حيث view شناس

part one الذي وضعته في view root من الـ User mode ثم ندخل المودي

```
R>enable view
Password: [password]
```

لـ viewParser يدخل view

```
R# show Parser View
```

نحوه View Mode secret password & View 2

R(conf)# Parser View Abawy

R(conf-view)# secret password

نحوه View Mode list view ایجاد 3

R(conf-view)# command Exec  
Config { Include  
Exclude  
Include-exclusive } Command

View Mode list view - Include

View Mode list view - Exclude

View Mode list view - Include-exclusive

### Part three

نحوه AAA authentication local  
local view authentication local

R(conf)# aaa authentication login default local

Either

R(conf)# line con 0

R(conf)# login authentication local  
line

or

R(conf)# line VTY 0 4

R(conf-line)# login authentication local

## Supper View

Views کو جو اسکرین کرنا ہے اسے View کہا جاتا ہے اسے ان نکھل کر View کہا جاتا ہے

• Supper View پیش کیا جائے

- Max View (show ip, ping, telnet)
- abeer View (router, show crypto)

لوگوں کی لئے

(Abeer View → Max View) اسے سمجھو

### Configuration of Supper View

R(conf)# Parser View Ahmad Supperview

→ start

Supper View || secret password وضعیت

R(conf)# secret [password]

R(conf)# View Max

Supperviews Views اخراجی

R(conf-view)# View abeer

ذکر کردیں Views || اسکے Supperviews کیلئے ایسا Supperviews

R(conf)# No Parser View Ahmad Supperview

ذکر کردیں View گزینہ User ہے

R(conf)# username [username] view [view name] Password [password]

## lec 6

### CCNA - Security

#### : IOS Resilient Configuration \*

Using  
Packet tracer  
(Router 2911)

```
R2(config)#secure ?  
boot-config Archive the startup configuration  
boot-image Secure the running image
```

هذه الخاصية تستفاد منها لحفظ نسخة من Config ونسخة من IOS التي لدينا في  
الـ Flash: *وتخزن بعثرة حقيقة في الـ Flash*

boot - config - 1

هي لخزن config على الـ Flash

boot - image - 2

هي لخزن نسخة IOS على الـ Flash

```
IOS1#show secure bootset  
IOS resilience router id 2048001  
IOS image resilience is not active  
IOS configuration resilience version 15.4 activated at 12:42:00 UTC Tue Jan 24 2  
017  
Secure archive unix:.runcfg-20170124-124200.ar type is config  
configuration archive size 1566 bytes
```

الأمر أعلاه يبين لنا بأننا أخزننا نسخة من config والـ IOS ووضعناها في الـ Flash

#### : SCP بروتوكول Configuration Secure Copy\*

### Configuring Secure Copy

Configure the router for server-side SCP with local AAA:

1. Configure SSH
2. Configure at least one user with privilege level 15
3. Enable AAA
4. Specify that the local database is to be used for authentication
5. Configure command authorization
6. Enable SCP server-side functionality

R# dir flash: ↴ not able flash . It's seeable when \*

لتحفظ خفته في الملايين configuration او IOS او IOS configuration لـ R# dir flash: ملك

الخطوة في الفلاش يعوّه حفنة config او IOS مثلاً لرقة او IOS \*

حيث تغير تفاصيل عن ما هو مطلوب

R# Show secure

الخطوة اولاً

او IOS او config

• **will** في configuration & IOS لـ save، like از **\***  
• configuration او IOS **in** حالة ابرد ترتيب **in** **configuration**

- بالنتيجة Configuration : بدهان تم خزنها في الـ flash فنجد ان نسختها صرفة افريانا بواسطه الـ وادر الـ ٦٠٨٩:

Configuration ملخص امنیتی R# Show Secure تاپ

(Rconf)# secure boot-config restore flasho: config will pt

no startup Running-config > [ctrl+f] flash write <local copy file>

R# copy flash: [edit] running-config

- النسمة لتنمية ملف ISO: الموجودة في `src/main/resources` بواسطه المعايير العالمية.

Reload keyf electronic keyboard ای میکرو میکروفون common mode میکروفون و کنترلر را باعث ایجاد نمایند // R# Reload میکروفون

Ctrl + S CrLk  
Rommon mode kurde گزینی keyboard چهارم  
Rommon ۱ > سریع شدن

Romm on 2) dir flash:

نحو اسم IOS فنكتب اسفل الالى لنسخة IOS config files flash و ايها كل اسفل IOS الموعدة في اسفل

Rommel 3 > boot

Ios 11.1.1

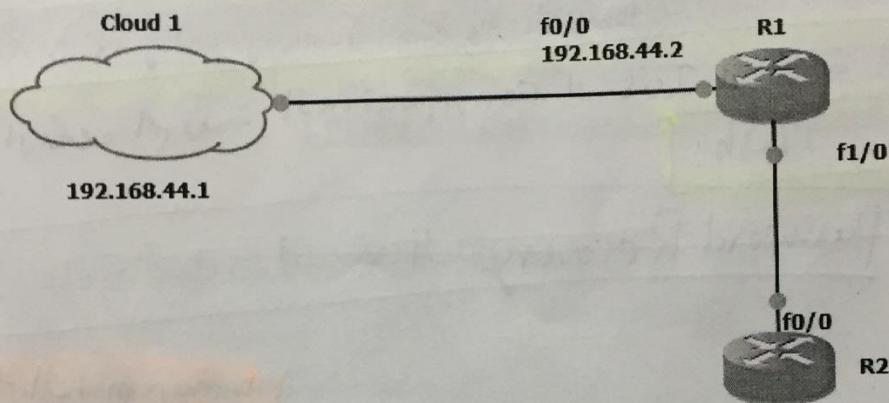
# Secure copy protocol (SCP)

CCNA - Security

IOS

بروتوكول SCP فائدته هو أخذ نسخة من config من راوتر ووضعها في الكمبيوتر كنسخة احتياطية ونريد بأن تكون البيانات التي تنقل بأمان أي Secure .

كما في المثال التالي :



بعد إنشاء الربط أعلاه وربط Cloud مع الكمبيوتر الخاص بنا سوف نقوم بنقل config من الراوتر R1 إلى الكمبيوتر .

الأوامر التي نعملها على الراوتر هي :

```
interface FastEthernet0/0
ip address 192.168.44.2 255.255.255.0
```

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
```

```
line vty 0 4
```

```
username abawy privilege 15 password 123
ip domain name cisco.com
ip scp server enable
```

الامر الاخير هو لتفعيل SCP .

C Partition في PSCP يتيح admin@PC to Command Line من PC GUI view لفتح الفايل اى مفهوم

C:\>PSCP.exe -SCP [username] [address of destination] : [filename] [Save destination]

username will be running-config حال لورى ان تغير اى اى داتا running config will change the config file XX will be (IP of ahmed 192.168.88.2) and (Ahmed)

C:\>PSCP.exe -SCP Ahmed192.168.88.2 : running-config d:\xx.txt

soft اسلوب IOS او configuration R# dir flash: يمك ان تغير الملف

Password Recovery حمله على الـ flash

Rommon mode [not Jeesh]

electronic keyboard Jeesh

Rommon Mode [not Jeesh] control + lock screen [not Jeesh] Reboot [not Jeesh]

- Configuration register [not Jeesh]

0x8102 :- normal router operation. When the router startup. It loads the startup configuration into RAM and became running-config

0x2102 :- Blank Router operation. When the router startup. It loads the startup configuration into RAM but does not copy it to the running-config.

soft اسلوب mode || mode in configuration register [not Jeesh]  
- From Router  
- From Rommon

R(config)# config-register [Value off]  
Rommon # config-reg [Value off]

Established running config → startup config || if 0x8102 || 8 - 11:00  
so the router is running at established startup config || if 0x8102 || 8 -

soft اسلوب في الـ config register [not Jeesh] R# show version

ادا استعمل المودم وتحتاج الى ادخال اعدادات او تغير اعدادات او تغير داتابس او تغير المودم  
وتحتاج المودم بريدي وتحتاج داتابس او تغير اعدادات او تغير داتابس او تغير المودم  
recovery mode (0x8002)

Reset the Router to factory setting if there is no password on the router :-

R# write erase  
R# Reload

الخطوات التي يجب اتباعها لـ NVRAM

وبذلك تم تفريغ المودم من جميع البيانات

Reset The Router to factory setting if there is unknown enable Password or unknown Secret Password :-

Rommon1 > confreg 0x8002  
Rommon2 > Reset

الخطوات التي يجب اتباعها لـ Rommon

وبذلك تم تفريغ NVRAM من جميع البيانات

R[conf]# config-register 0x2102

وبذلك ندخل في mode (0x2102)

R# write erase  
R# Reload

وبذلك تم تفريغ NVRAM من جميع البيانات

وبذلك تم تفريغ المودم من جميع البيانات

Recovering a Router Password :-

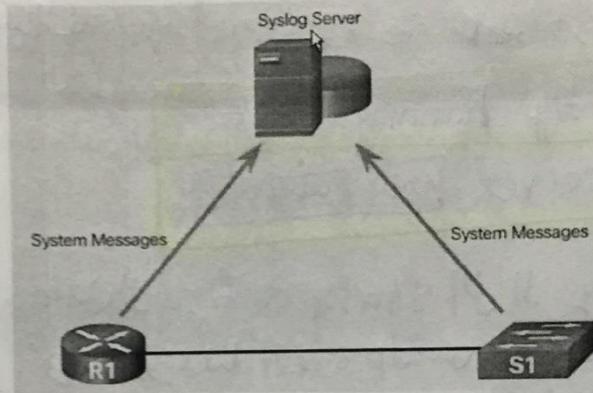
لو كان لدينا راتر وفقد اعدادات مخزنها في اور NVRAM  
وتحتاج password او config او enable secret او enable password  
ان نقوم بفتح Password Recovery mode في المودم  
وكل هذه الخطوات التالية :-

لذلك اعد اعدادات المودم

## lec 6

CCNA - Security

### Introduction to Syslog

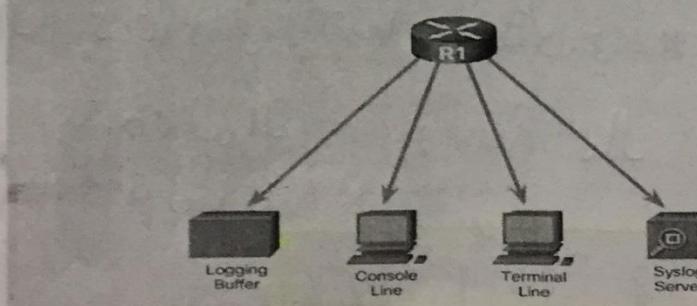


في هذا الجزء سوف نتكلم عن رسائل Syslog التي تظهر في الراوتر او السوچ وكما مبين  
أعلاه ان رسائل Syslog ترسل الى سيرفر مسؤول عن اظهارها للمستخدم اي الادمن  
. Syslog Server ويسمى

### Syslog Operation

severity level  
↓

```
R1(config-if)# no shutdown
R1(config-if)#
000047: *Feb 19 11:36:47.779: %LINK-3-UPDOWN: Interface Serial0/0/0, changed
state to up
000048: *Feb 19 11:36:48.779: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
```



# Recovering a Router Password

Configuration register  $\Rightarrow$  من الممكنRommon mode

الخطوة 1:  $\text{J1 J2 J3}$  على  $\text{0x2102}$

Rommon 1)  $\text{confreg 0x2102}$

Rommon 2)  $\text{reset}$

وسيتم تغيير الـ Configuration register

• running config  $\Rightarrow$  startup config  $\Rightarrow$  new password

R# copy startup-config Running-config

R(config)# enable secret newpassword

• running config  $\Rightarrow$  startup config  $\Rightarrow$  copy newpassword  $\Rightarrow$  newpassword  $\Rightarrow$  newpassword

ويمكننا دخول running config  $\Rightarrow$  go startup config  $\Rightarrow$  view password  $\Rightarrow$  newpassword  $\Rightarrow$  newpassword

• Configuration register  $\Rightarrow$  Normal mode

R(config)# config-register 0x2102

Shutdown  $\Rightarrow$  new interfaces  $\Rightarrow$  new IP

• startup config  $\Rightarrow$  running config  $\Rightarrow$  copy  $\Rightarrow$  reload

R# copy Running-config Startup-config

R# Reload

•  $\text{ip password-encryption}$   $\Rightarrow$  disable  $\Rightarrow$  enable  $\Rightarrow$  password recovery

password  $\Rightarrow$  auto  $\Rightarrow$  enable password recovery

R(config)# no service password-recovery

•  $\text{enable}$   $\Rightarrow$   $\text{ip packet-trace}$   $\Rightarrow$   $\text{Guzz}$   $\Rightarrow$   $\text{show ip route}$

شكل الرسالة هو كما في الصورة اعلاه وقد مر علينا هكذا رسائل اثناء دراستنا لمنهج ccna ولكن هناك معلومه ظاهره في بداية الرسالة والمتمثله بالرقم 000047 وهذا الرقم يسمى sequence Number ويتم تفعيلها عن طريق تفعيل Service موجوده على الرووتر او السوچ حسب حاجة الأدمن ويتم تفعيلها بالأمر التالي :

```
R1(config)#service sequence-numbers
R1(config)#end
R1#
000033: *Nov 12 16:04:36.231: %SYS-5-CONFIG_I: Configured from console by abeer on console
```

وكما نلاحظ هنا ان ال Sequence Number قد ظهرت في بداية رسالة اللوك .  
بالنسبة لرسائل Log Message تصنف كما نعرف كالتالي :

## Syslog Message

### Security Levels

	Level	Keyword	Description	Definition
Highest Level	0	emergencies	System is unusable	LOG_EMERG
	1	alerts	Immediate action is needed	LOG_ALERT
	2	critical	Critical conditions exist	LOG_CRIT
	3	errors	Error conditions exist	LOG_ERR
	4	warnings	Warning conditions exist	LOG_WARNING
	5	notifications	Normal but significant condition	LOG_NOTICE
	6	informational	Informational messages only	LOG_INFO
Lowest Level	7	debugging	Debugging messages	LOG_DEBUG

### Example Severity Levels

Syslog Level and Name	Definition	Example
0 LOG_EMERG	A panic condition normally broadcast to all users	Cisco IOS software could not load
1 LOG_ALERT	A condition that should be corrected immediately, such as a corrupted system database	Temperature too high
2 LOG_CRIT	Critical conditions; for example, device errors	Unable to allocate memory
3 LOG_ERR	Errors	Invalid memory size
4 LOG_WARNING	Warning messages	Crypto operation failed
5 LOG_NOTICE	Non-error conditions that may require special handling	Interface changed state up or down
6 LOG_INFO	Informational messages	Packet denied by ACL
7 LOG_DEBUG	Messages that contain information that is normally used only when debugging a program	Packet type invalid

وكما قلنا سابقاً أنّي أقل رقم (Severity) اي مثلاً رقم 7 وهم المسج الأقل خطوره وكما موضح تفصيل شكل رساله اللوك :

## Syslog Message (Cont.)

Column 1	Column 2
1 seq no	Stamps log messages with a sequence number if service sequence-numbers is configured.
2 timestamp	displays if service timestamps log is configured
3 facility	denotes the source or the cause of the system message
4 severity	levels 0 - 7
5 MNEMONIC	text string that uniquely describes the message
6 description	text string containing detailed information about the event being reported

طريقى تفعيل Syslog كما ذكرناها في المناهج السابقة تلخص بالتالي :

## Configuring System Logging

### Step 1

```
Router(config)#
```

```
logging host [hostname | ip-address]
```

← IP of Syslog SERVER

### Step 2 (optional)

```
Router(config)#
```

```
logging trap level
```

### Step 3

```
Router(config)#
```

```
logging source-interface interface-type interface-number
```

← sourceint. conf  
system management

### Step 4

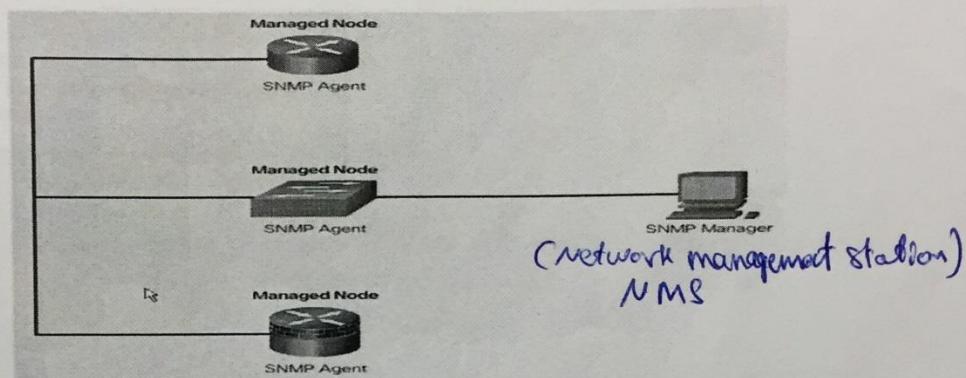
```
Router(config)#
```

```
logging on
```

## Using SNMP for Network Security

هنا سوف نستخدم الـ SNMP تم شرحه سابقاً ويكون شكل عملية الـ SNMP كالتالي :

### Introduction to SNMP



وهنالك عدة اصدارات للـ SNMP وتلخص بالشكل التالي :

## SNMP Versions

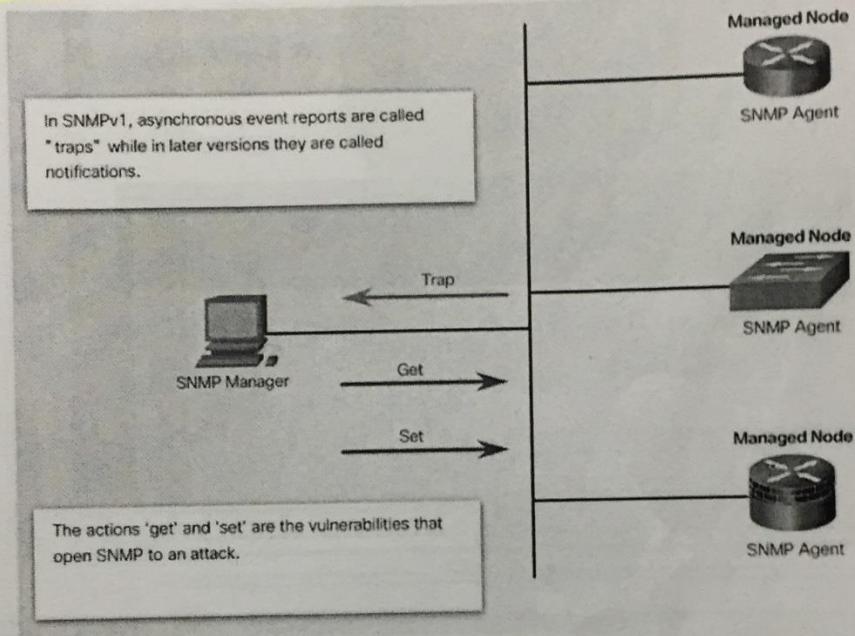
Model	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication (an improvement over SNMPv2c).
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3	authPriv (requires the cryptographic software image)	MD5 or SHA	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms: <ul style="list-style-type: none"><li>• DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.</li><li>• 3DES 168-bit encryption</li><li>• AES 128-bit, 192-bit, or 256-bit encryption</li></ul>

Community string أو user name



في ما يخص المتبادل بين SNMP Manager والـ SNMP Agent :

## SNMP Vulnerabilities



## Using NTP

استخدام بروتوكول NTP في ضبط الوقت داخل الشبكة :

### Network Time Protocol

```
R1# clock set 10:28:00 DEC 16 2008
R1#
*Dec 16 10:28:00.000: %SYS-6-CLOCKUPDATE: System clock
has been updated from 16:07:17 UTC Tue Dec 16 2008 to
10:28:00 UTC Tue Dec 16 2008, configured from console
by console.
R1#
```

تكون أعدادات NTP Server كالتالي :

### NTP Server

#### Sample NTP Topology

I am the NTP master with IP address  
10.10.10.1, and I will provide all other  
devices with a synchronized time source.

Sample NTP Configuration on R1

```
R1# conf t
R1(config)# ntp master 1
R1(config)# ^z
R1#
R1# show clock
13:01:15.735 UTC Tue Dec 16 2008
R1#
```

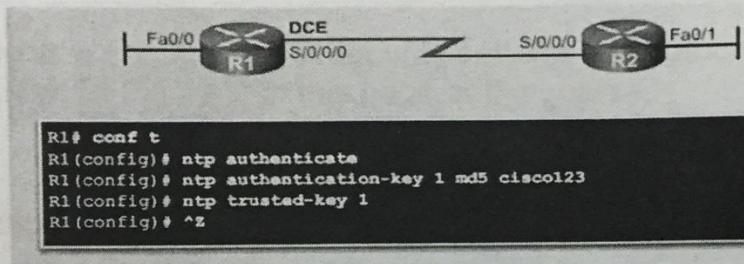
اداً لم نحدد الـ stratum 8 فالـ default خالياً

Sample NTP Configuration on R2

```
R2# conf t
R2(config)# ntp server 10.10.10.1
R2(config)# ^z
R2#
R2# show clock
13:01:41.986 UTC Tue Dec 16 2008
R2# show ntp status
Clock is synchronized, stratum 2, reference is 10.10.10.1
nominal freq is 250.000 Hz, actual freq is 249.9992 Hz, precision is 2**18
reference time is CCE2253E.5DC2A53B (13:01:50.356 UTC Tue Dec 16 2008) clock
interval is 0.0002 seconds, offset is -0.41 ms, dispersion is 0.000000 ms
last update was 13:01:41.986 UTC Tue Dec 16 2008, leap is normal
```

بالنسبة لزيادة الأمان تم عمل الـ Authentication في NTP و تكون كالتالي :

## NTP Authentication



Lee F

## Performing a Security Audit

في هذا الجزء مراجعه بسيطه حول :

## Discovery Protocols CDP and LLDP

```
R1(config)# lldp run
R1(config)# end
R1# show cdp neighbors detail
-----
Device ID: S1
Entry address(es):
  IP address: 192.168.1.254
Platform: Cisco WS-C2960-24TT-L, Capabilities: Switch IGMP
Interface: GigabitEthernet0/1, Port ID (outgoing port): FastEthernet0/5
Holdtime : 164 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
<output omitted>
R1# show lldp neighbors detail
-----
Local Intf: Gi0/1
Chassis id: 0022.9121.0380
Port id: Fa0/5
Port Description: FastEthernet0/5
System Name: S1

System Description:
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
<output omitted>
```

والذان نستفاد منهما في معرفة الـ Neighbor وكما نعرف أن الـ CDP هو اصدار لسسكو ومفعل By default في الجهاز اما الـ LLDP وهو ستاندرد وغير مفعل . هناك بعض الامور الواجب الانتباه عليها لتأمين الاجهزه والشبكه بشكل عام :

## Settings for Protocols and Services

There is a detailed list of security settings for protocols and services provided in Figure 2 of this page in the course.

Additional recommended practices to ensure a device is secure:

- Disable unnecessary services and interfaces.
- Disable and restrict commonly configured management services.
- Disable probes and scans. Ensure terminal access security.
- Disable gratuitous and proxy ARPs
- Disable IP-directed broadcasts.

كمثال اطفاء اي خدمة غير ضورريه حاليا او لسنا بحاجتها وما الى ذلك وكما نعرف ان هناك الكثير من الخدمات مفعله بالراوتر بصورة اوتوماتيكية ونحن لسنا بحاجتها ولا يمكننا طبعا اطفاء واحد واحده لأجل زيادة الامان ولكن هناك خدمة تسمى بالـ Auto Secure

## Locking Down a Router Using AutoSecure

الـ Auto Secure وهي خدمة يمكن من خلالها غلق او فتح خدمات حسب حاجة المستخدم ولها اكثر من Mode واشهرها :

Full – 1

no interact – 2

بالنسبة للـ **Full Mode** هو انه سوف يتم سؤالنا عدة اسئله وعلى ضوء اجاباتنا سوف يتم اعداد الراوتر او السوتج .

اما بالنسبة للـ **No Interact** فانه سوف يغلق خدمات بأكملها وسوف تحتاج الى ان نفتح الخدمة المطلوبه ببنفسنا .

طريقة تفعيل هذه الخدمة هو من على **Enable Mode**

```
R1#auto secure ?
  firewall          AutoSecure Firewall
  forwarding        Secure Forwarding Plane
  full              Interactive full session of AutoSecure
  login             AutoSecure Login
  management        Secure Management Plane
  no-interact      Non-interactive session of AutoSecure
  ntp               AutoSecure NTP
  ssh               AutoSecure SSH
  tcp-intercept    AutoSecure TCP Intercept
<cr>
```

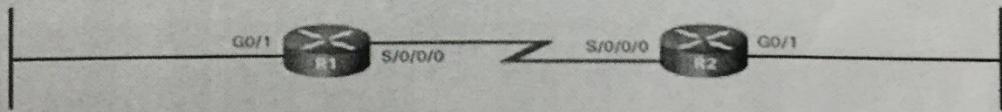
## Securing the Control Plane

Upon completion of this section, you should be able to:

- Configure a routing protocol authentication.
- Explain the function of Control Plane Policing.

ونقصد هنا تامين الشبكة بين الراوترات وغيرها مثل **Update** وما الى ذلك ومثال عليه هو **OSPF Authentication** في **OSPF** ويتم كالتالي :

## OSPF MD5 Routing Protocol Authentication



```
R1# conf t
R1(config)# interface s0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 cisco12345
R1(config-if)# ip ospf authentication message-digest
R1(config-if)#
000209: Feb 20 13:59:35.091 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)#
000210: Feb 20 14:01:09.975 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Serial0/0/0 from
LOADING to FULL, Loading Done
-----
R2# conf t
000137: Feb 20 13:59:35.091 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Dead timer expired
R2(config)# interface s0/0/0
R2(config-if)# ip ospf message-digest-key 1 md5 cisco12345
R2(config-if)# ip ospf authentication message-digest
R2(config-if)#
000138: Feb 20 14:01:09.975 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done
R2(config-if)#

```

ويتم التشفير بواسطه MD5 ولكن الان هذا النوع من التشفير أصبح ممكناً أن يتعرض للـ Prod Force Attack ولذلك ظهر نوع التشفير SHA وتفعيله كالتالي :

## OSPF SHA Routing Protocol Authentication

work only on  
New IOS (FOU)

Step 1: Specify an SHA authentication key chain.

```
Router(config)# key chain name
Router(config-keychain)# key key-id
Router(config-keychain-key)# key-string string
Router(config-keychain-key)# cryptographic-algorithm hmac-sha-256
Router(config)# send-lifetime start-time {infinite | end-time | duration seconds}
```

key [max]

Step 2: Assign the authentication key chain to the desired interfaces.

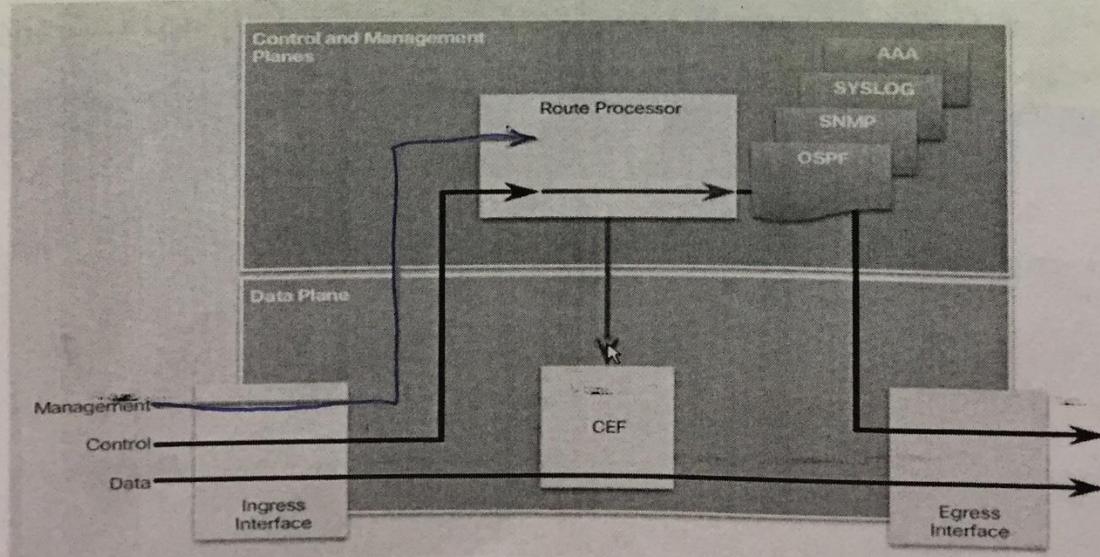
```
Router(config)# interface type number
Router(config-if)# ip ospf authentication key-chain name
```

key

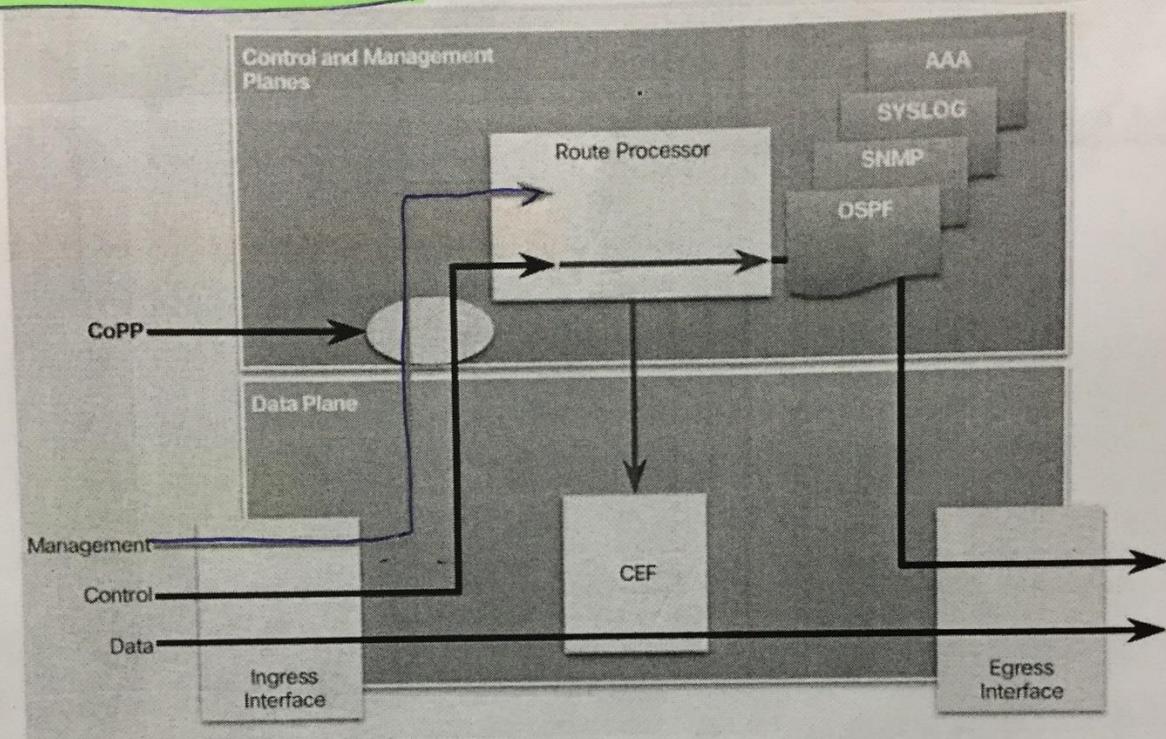
## Control Plane Policing

هنا سوف نعرف كيفية وضع Policy معين على Data Plane

## Network Device Operations



## CoPP Operation



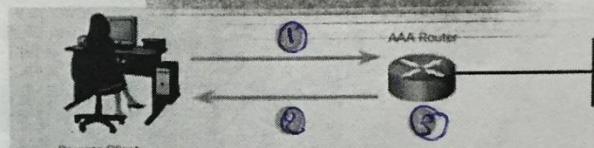
كما نعرف ومبين في الشكل اعلاه انني اي معلومات خاصة بال—Control Plane فسوف تمر على—the Processor ولنفرض انه كان هنالك هجمه من خلال—the DOS فان هذه الهجمه سوف تادي الى حمل عالي على البروسيسنك لذلك تأتي هنا فائدة COPP(Control Plane Policing) والتي تحمي من هذا اللود اي نضع منهجه للراوتر بأنه اي Data خاصه بال—Control Plane اذا تجاوزت حد معين فطبق عليها—the Policy . Drop - Data

## Authentication, Authorization, and Accounting

: AAA \*

### Authentication Modes

#### Local AAA Authentication



1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using the local database and the user is authorized to access the network based on information in the local database.

- 1> the client established a connection using Console or remontaccess
- 2> AAA Router ask the user for username & password
- 3> the Router ~~authenticates~~ authenticates the username and password using Router Local database also authorize the User using Local database

#### Server-Based AAA Authentication



is same as Local AAA authentication

but database of authentication

will be saved on another server

هناك نوعين من الموديل كما مبين في الصورة أعلاه :

#### Local Based – 1

اي تكون قاعدة البيانات بالنسبة للمستخدمين داخل الراوتر (يمكن عملها في حال كانت الشبكة ليست كبيرة جدا).

#### Server Based – 2

اي تكون قاعدة البيانات في داخل سيرفر مستقل (يُنصح باستخدامه في حالة كانت الشبكة كبيرة جدا).

بالنسبة للمستخدم في حال اراد الدخول فسوف يكون في البداية عملية تحقق Authentication بعدها في حال سمح له بالدخول يطبق عليه الصلاحيات Authorization حسب كل مستخدم بعدها في حال تم طلب مراقبة هذا المستخدم فسوف يطبق عليه الـ Accounting . طريقة الأوامر كالتالي :

نحو اسفل (Local Data Based) - 1

```
Router(config)# aaa new-model  
Router(config)# aaa authentication login {default | list-name} method1[method2...]  
Router(config)# line [aux | console | tty | vty] line-number [ending-line-number]  
Router(config-line)# login authentication [method1[method2...]]
```

## **AAA Authentication Login Methods**

Keyword	Description
enable	Uses the enable password for authentication.
krb5	Uses Kerberos 5 for authentication.
krb5-telnet	Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router. If selected, this keyword must be listed as the first method in the method list.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
groupradius	Uses the list of all RADIUS servers for authentication.
grouptacacs+	Uses the list of all TACACS+ servers for authentication.
groupgroup-name	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaagroup server radius or aaa group server tacacs+ command.

```
R(config)# aaa authentication login mohammed enable local
```

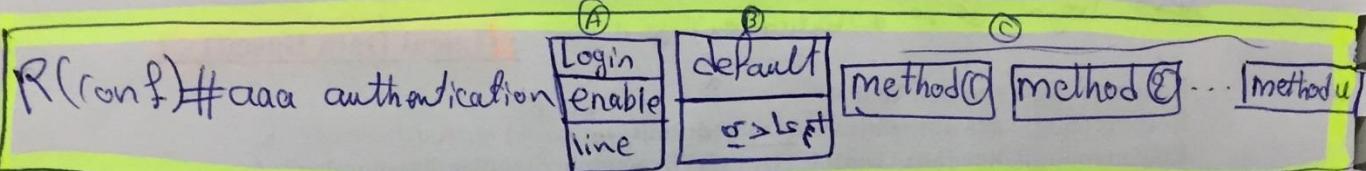
enable login with enable password if user login then it will ask for password.

## AAA using local database الاعداد او دورة اوضخ للكتابة

R(config)# AAA new-model

AAA الجديدة

- ١) تحدد سقوف الـ Login او enable password او line password
- (line) يتحقق من line password
  - تحدد اذا تكون default او غيرها
  - تحدد الخطوة الفعلية ماذا لو يوجد enable password local database



- Methods are enable, krb5, line, local, ... .

Local username & password او line VTY password او enable password

R(config)# Username [username] Password [password]

او ننكرى ان يكون [local username & password] كالتالي

R(config)# Username [username] Privilege [level] Password [password]

## Fine-Tuning the Authentication Configuration

Command Syntax	Command	Description
<code>aaa local authentication attempts max-fail [number-of-unsuccessful-attempts]</code>		Number of unsuccessful authentication attempts before a connection is dropped and the user account is locked.
<code>Display Locked Out Users</code>	<code>show aaa local user lockout</code>	Shows the number of failed login attempts for each user account.
<code>Show Unique ID of a Session</code>	<code>show aaa sessions</code>	Shows session details including unique ID, user name, IP address, and idle time.

الامر اعلاه هو لتحديد عدد مرات الفشل للمستخدم أثناء ادخال كلمة المرور واسم المستخدم

وفي حال مثلا تم وضع Max Fail على 3 مرات فان المستخدم لن يتمكن من الدخول الى  
الراوتر وسوف تكون حالته .  
lockout

`R#clear aaa local user lockout` لـ unlock user

### Troubleshooting Local AAA Authentication

من اجل حل مشكلات Lock user و privilege level user

#### Debug Options

##### Debug Local AAA Authentication

```
R# debug aaa ?
  accounting          Accounting
  administrative      Administrative
  api                 AAA API events
  attr               AAA Attr Manager
  authentication      Authentication
  authorization       Authorization
  cache               Cache activities
  coa                AAA CoA processing
  db                 AAA DB Manager
  dead-criteria      AAA Dead-Criteria Info
  id                 AAA Unique ID
  ipc                AAA IPC
  mlist-ref-count    Method list reference counts
  mlist-state         Information about AAA method
                      list state change and notification
  per-user            Per-user attributes
  pod                AAA POD processing
  protocol           AAA protocol processing
  server-ref-count   Server handle reference counts
  sg-ref-count        Server group handle reference counts
  sg-server-selection Server Group Server Selection
  subsys             AAA Subsystems
  testing            Info. about AAA generated test packets
```

يمكن استخدام امر `Debug AAA` لمعرفة المشكله ان وجدت في الـ .

## Server-Based AAA

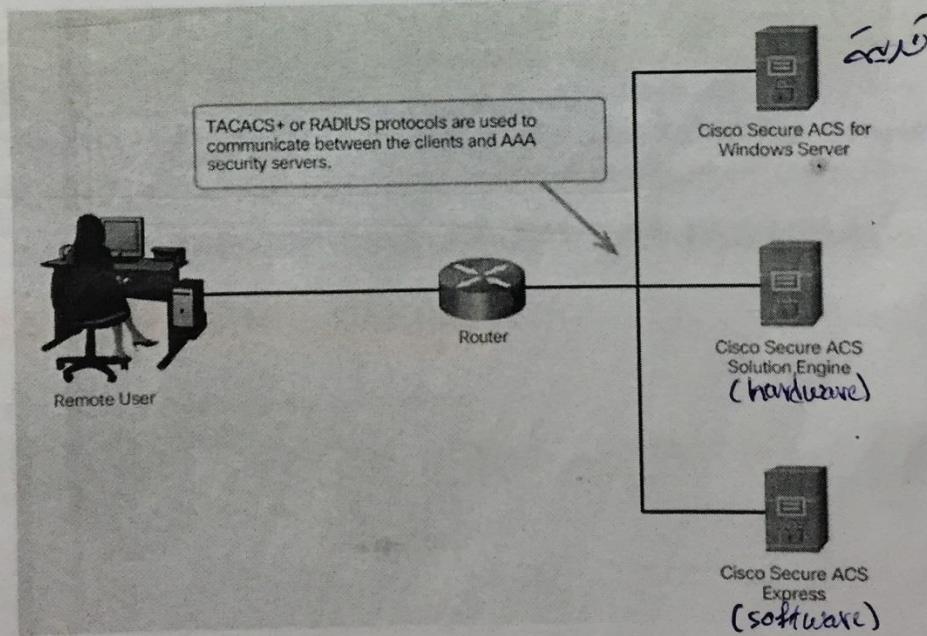
Upon completion of this section, you should be able to:

- Describe the benefits of server-based AAA.
- Compare the TACACS+ and RADIUS authentication protocols.

### : (Server Data Based) - 2

بالنسبة للسيرفر ياما ان يكون جهاز او برنامج يثبت على كمبيوتر معين

## Introducing Cisco Secure Access Control System



بالنسبة لأجهزة سisco يسمى ACS او ISE ويكون هذا السيرفر Active directory التابع لمایکروسوفت او برنامج مجاني يمكن تثبيته .

ابع لسکو یجب تطبيق عليه احد البروتوكولات التالية والتي مر ذكرها في  
هي :

## Introducing TACACS+ and RADIUS

	TACACS+	RADIUS
Functionality	Separates AAA according to the AAA architecture, allowing modularity of the security server implementation	Combines authentication and authorization but separates accounting, allowing less flexibility in implementation than TACACS+
Standard	Mostly Cisco supported	Open/RFC standard
Transport Protocol	TCP	UDP
CHAP	Bidirectional challenge and response as used in Challenge Handshake Authentication Protocol (CHAP)	Unidirectional challenge and response from the RADIUS security server to the RADIUS client
Protocol Support	Multiprotocol support	No AAA, no NetBEUI
Confidentiality	Entire packet encrypted	Password encrypted
Customization	Provides authorization of router commands on a per-user or per-group basis	Has no option to authorize router commands on a per-user or per-group basis
Accounting	Limited	Extensive

**RADIUS protocol:** It combines authentication and authorization into one service using UDP port 1645, and the accounting service uses UDP 1646.

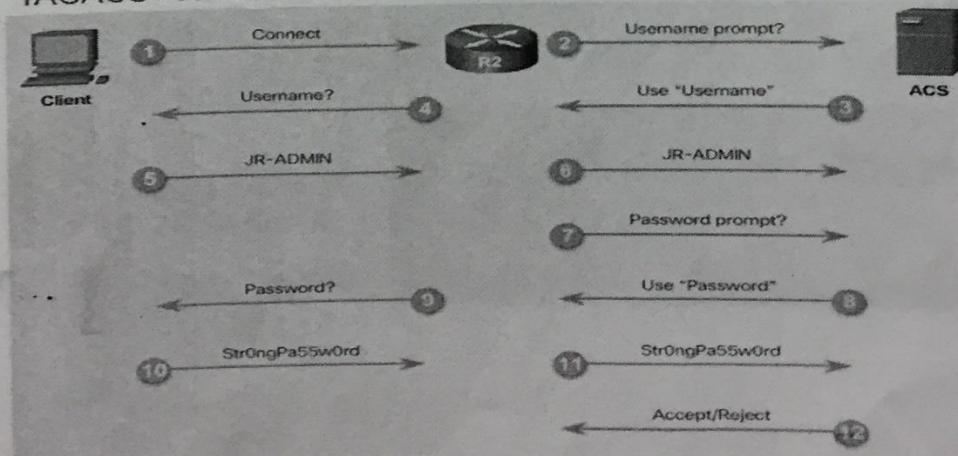
**TACACS+ protocol:** TCP port 49

فيما يلي ملخص عمل تأمين تسلسل العمل :  
الخطوة الأولى : التأمين (Auth) ، التأكيد (Acc) و التحكم (Auth) .  
حيث يتم التأمين من قبل Router (R2) ، التأكيد من قبل ACS (Auth Server) و التحكم من قبل Router (R2) .  
بالنسبة للمقارنة بين النوعين فتظهر لنا بالصورة أعلاه .

طريقة عمل TACACS تلخص بالشكل التالي :

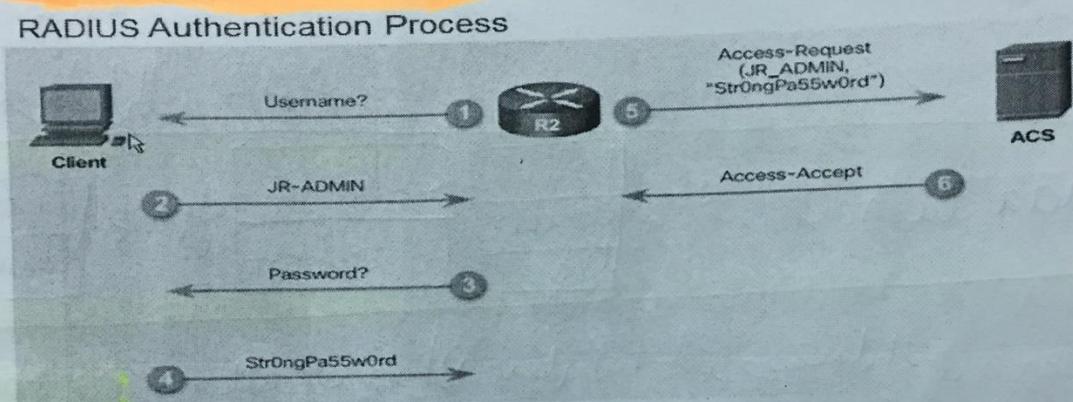
## TACACS+ Authentication

TACACS+ Authentication Process



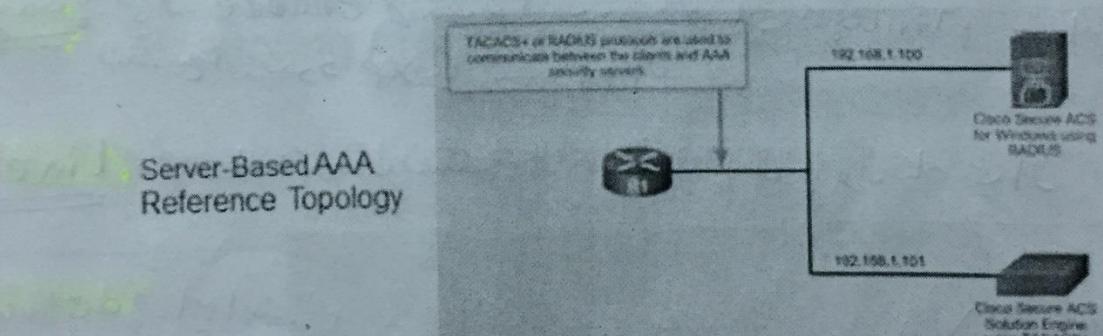
اما طريقة عمل الـ RADIUS تلخص بالشكل التالي :

## RADIUS Authentication



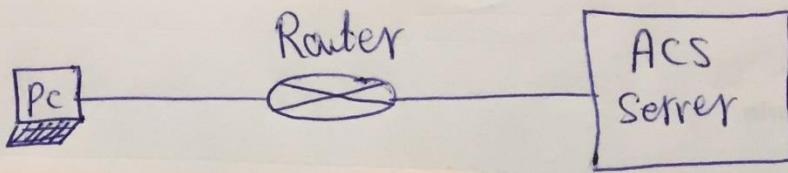
بالنسبة لأوامر التفعيل للـ TACACS كال التالي :

## Configuring the CLI with TACACS+ Servers



## Configure a AAA TACACS+ Server

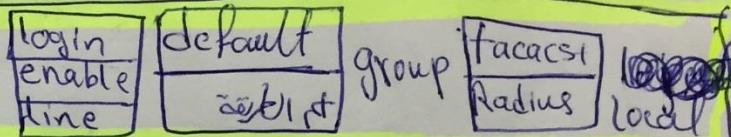
## Configuration of AAA TACACS+ Servers :-



```
R(config)# aaa new-model
```

AAA نظریہ ۱

R(config)# aaa authentication



-فُحْكَةِ إِبْرِيرِ الْيَنْهَلِيِّ الرَّادِرِ وَسَهْلِ الْوَرَدِ enable -  
لِعُونِ مُخْرُونِهِ لِعُوَارِ daa Setrey

- في حالة اهتزاز المدخلات على الرابط يواصـة Login -  
Username & password

**مُخَصَّصٌ**: خواص مُخْصِّصةً enable privileges بمعنى آخر أن نحدد مُخَصَّصات privileges لـ login.

VTY : لحالات اثنان يستخدم الـ password الذي وضحته في اول Line -

and it always Verify the address of the user - المطلوب:-

local database & faces+ the طبق نسخه ای انسف group server

لـ authentication ای سوچنیم ای tacacs+ server ای tacacs+ local database ای سوچنیم ای tacacs+

خطوة ٣: - في حالة أنك لا تدخل أو لا تعرف لا ينفع  
أي طريقة لفتح باب الـ local database على سيرفر sql server .  
• السيرفر new user ||

Radius of influence or facecast 4 methods of cell to cell local database

## Configure Authentication to Use the AAA Server

## Command Syntax

```

#110config# aaa authentication login default ?
cache          Use Cached-group
enable         Use enable password for authentication.
group          Use Server-group
krb5           Use Kerberos 5 authentication.
krb5-telnet    Allow logins only if already authenticated via Kerberos V
                Telnet.
line           Use line password for authentication.
local          Use local username authentication.
local-case     Use case-sensitive local username authentication.
none          NO authentication.
password-expiry enable the login list to provide password aging support

#110config# aaa authentication login default group ?
radius         Use RADIUS hosts.
tacacs         Use TACACS hosts.
tacacs+        Use TACACS+ hosts.

```

## Configure Server-Based AAA Authentication

```

R1(config)# aaa new-model
R1(config)#
R1(config)# tacacs server SERVER-T
R1(config-server-tacacs)# address ipv4 192.168.1.100
R1(config-server-tacacs)# single-connection
R1(config-server-tacacs)# key TACACS-PassWord
R1(config-server-tacacs)# exit
R1(config)#
R1(config)# radius server SERVER-R
R1(config-radius-server)# address ipv4 192.168.1.101 auth-port 1812 acct-port 1813
R1(config-radius-server)# key RADTUS-PassWord
R1(config-radius-server)# exit
R1(config)#
R1(config)#

```

## Monitoring Authentication Traffic

## Troubleshooting Server-Based AAA Authentication

```
R1# debug aaa authentication
AAA Authentication debugging is on
R1#
14:01:17: AAA/AUTHEN (567936829): Method=TACACS+
14:01:17: TAC+ send AUTHEN/CHAP packet
14:01:17: TAC+ (567936829) received authen response status = PASS
14:01:17: AAA/AUTHEN (567936829): status = PASS
```

### ٣) نعمل الخطوات التالية

④ Rconfig) # tacacs server

أحمد العسوي

(A) ندخل اسم المستخدم الذي سوف يستخدم لكي يكون اداة authentication || database

(B) R(config)# server-tacacs)# address IPv4 IP of server

نحوه الـ B Server على IPv4

© R(conf-server-faces) # key /key

٣) نفاذ key الذي سوف يقوم بالتحريك بين Server و Router

٤) إنّ الـ **faces** خبيثة كفاية لـ **User** او **Administrator** فأنه اذا  
فتحت **Session** على **Server** من **Router** وفها يطلب عملية  
الـ **authentication** وكتابة الـ **password** في الآخر مما يستخدم لـ **attack**

R(conf-server-faces) # Single-connection

لكل بروتوكول اتصال مخصوص

٥) ألا ينفع أين سف نطبق فيه العمليات

line VTY ۱۲۳ ۴۵۶ (A)

R(config)# line VTY 0-4

R(config-line)# login authentication

آنم العلیقہ

٤) في حالة اختفاء default في المحرر المالي  $\Rightarrow$  فلانكتب اسم المطريقة لأنها default

default سُفْلَكُون

R(config)# line console 0

Console & the (B)

R(config-line)# login authentication

۱۳۷

## Debugging TACACS+ and RADIUS

Troubleshooting RADIUS

```
R# debug radius ?
accounting      RADIUS accounting packets only
authentication   RADIUS authentication packets only
brief          Only I/O transactions are recorded
elog            RADIUS event logging
failover        Packets sent upon fail-over
local-server    Local RADIUS server
retransmit      Retransmission of packets
verbose         Include non essential RADIUS debugs
<cr>
```

Troubleshooting TACACS+

```
R# debug tacacs ?
accounting      TACACS+ protocol accounting
authentication   TACACS+ protocol authentication
authorization   TACACS+ protocol authorization
events          TACACS+ protocol events
packet          TACACS+ packets
<cr>
```

٦) باللحظة الراهنة لا تكون local database هي account database حتى تكون باباً يفتح في حالة وقوع الخطأ يرجع الدخن من الفحول إلى المادر ويعود إلى الأصل ويتم إعادة التأمين

R(config)# username  Username  Password  Password

او يمكن ان تكون Username & Password

R(config)# username  Username  privilege  level  Password  Password

## Configuring Server-Based AAA Authorization

### الآن نأتي لعملية الـ Authorization

والتي تعني كما قلنا توزيع الصلاحيات بالنسبة لكل مستخدم حسب وجهة نظر الأدمين.

## AAA Authorization Configuration with CLI

### Command Syntax

```
R1(config)# aaa authorization (network | exec | commands level)
[default | list-name] method1...[method4]
```

```
R1(config) # aaa authorization exec ?
WORD      Named authorization list.
default   The default authorization list.
```

### Authorization Method Lists

```
R1(config)# aaa authorization (network | exec | commands level)
[default | list-name] method1...[method4]
```

```
R1(config) # aaa authorization exec default ?
cache      Use Cached-group
group     Use server-group.
if-authenticated Succeed if user has authenticated.
krb5-instance Use Kerberos instance privilege maps.
local      Use local database.
none       No authorization (always succeeds).
R1(config) # aaa authorization exec default group ?
WORD      Server-group name
ldap      Use list of all LDAP hosts.
radius    Use list of all Radius hosts.
tacacs+   Use list of all Tacacs+ hosts.
```

### Example AAA Authorization

```
R1(config) # username JR-ADMIN algorithm-type sha256 secret Str0ng5rPa55w0rd
R1(config) # username ADMIN algorithm-type sha256 secret Str0ng5rPa55w0rd
R1(config) # aaa new-model
R1(config) # aaa authorization exec default group tacacs+
R1(config) # aaa authorization network default group tacacs+
```

## Configuring Server-Based AAA Accounting

### الآن نأتي لعملية الـ Accounting : Accounting

والتي كما قلنا الفائد منها هي المراقبة وكمثال ممكن مراقبة الشبكة اي بروتوكول الـ Point to Point Protocol اي بمعنى اننا مشغلين الراوتر كـ NAS(Network Attached Storage) Server التابع لنا ويمكن مراقبة الـ exec كاماموضح في الامر ادناه الذي يستفاد منه في معرفة متى دخل او خرج المستخدم وما الى ذلك .

## AAA Accounting Configuration with CLI

### Command Syntax

```
R1(config)#  
aaa accounting {network | exec | connection} {default | list-name}  
(start-stop | stop-only | none | [broadcast] method1...[method4])
```

```
R1(config)# aaa accounting exec?  
WORD          Named Accounting list.  
default       The default accounting list.
```

```
R1(config)#  
aaa accounting {network | exec | connection} {default | list-name}  
(start-stop | stop-only | none | [broadcast] method1...[method4])
```

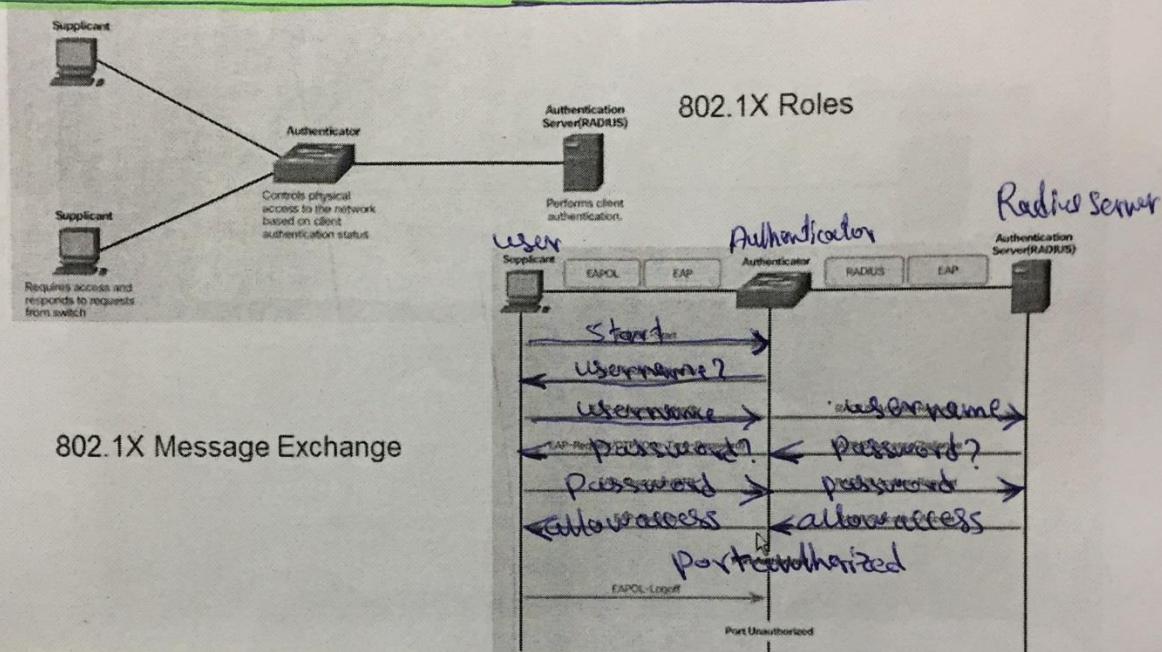
```
R1(config)# aaa accounting exec default start-stop?  
broadcast   Use Broadcast for Accounting  
group      Use Server-group  
  
R1(config)# aaa accounting exec default start-stop group?  
WORD        Server-group name  
radius     Use list of all Radius hosts.  
tacacs+    Use list of all Tacacs+ hosts.
```

```
R1(config)# username JR-ADMIN algorithm-type sscript secret Strong5xPa55w0rd  
R1(config)# username ADMIN algorithm-type sscript secret Strong5xPa55w0rd  
R1(config)# aaa new-model  
R1(config)# aaa authentication login default group tacacs+  
R1(config)# aaa authorisation exec default group tacacs+  
R1(config)# aaa authorisation network default group tacacs+  
R1(config)# aaa accounting exec default start-stop group tacacs+  
R1(config)# aaa accounting network default start-stop group tacacs+
```

### Accounting Method Lists

### Example AAA Accounting

## Security Using 802.1X Port-Based Authentication

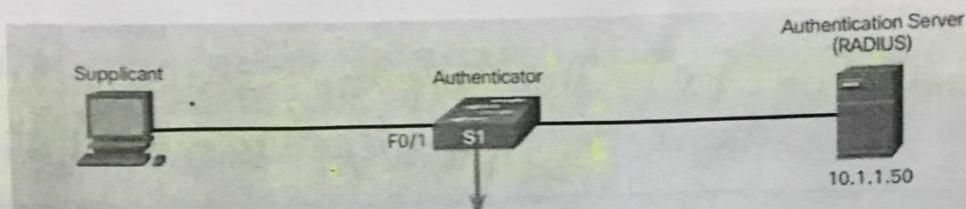


كما نعرف ان عملية تامين الشبكة تبدء من اول جهاز متصل للشبكة كمثال كمبيوتر متصل بسروج وهكذا ، وكما نعلم اننا كمنا نامن الشبكة عن طريق MAC Address اذا كان هذا الماك موجود اسمح للجهاز وبخلافه لا تسمح له .

طريقة الماك اصبحت قديمه والان بدء باستعمال بروتوكول 802.1X والذي يامن الدخول الابوجود اسم مستخدم وكلمة مرور وتم هذه العملية اي طلب اسم المستخدم وكلمة المرور عن طريق بروتوكول يسمى EAPOL(Extensible Authe Protocol Over Lan) كما مبين بالصورة اعلاه وتتوافق هذه العملية الا مع Radius Server

بالنسبة لعملية تنفيذ الأوامر كالتالي :

## Configuring 802.1X



```

S1(config)# aaa new-model
S1(config)# radius server CCMAS
S1(config-radius-server)# address ipv4 10.1.1.50 auth-port 1812 acct-port 1813
S1(config-radius-server)# key RADIUS-Pa55w0rd
S1(config-radius-server)# exit
S1(config)# aaa authentication dot1x default group radius
S1(config)# dot1x system-auth-control
S1(config)# interface F0/1
S1(config-if)# description Access Port
S1(config-if)# switchport mode access
S1(config-if)# authentication port-control auto
S1(config-if)# dot1x pae authenticator
  
```

R(conf)# aaa new-model

aaa ١١٢

Radius ٢٢٣ نحدد الطبق و اين سيرجع ال

~~R(conf)# radius-server host~~

R(conf)# aaa authentication dot1x default group radius

Radius Server ٣٣٤ نحدد

R(conf)# radius-server host [IPof server] key [Key]

dot1x ٤٤٥ نحدد

R(conf)# dot1x system-auth-control

نحوه ایجاد interface dot1x و نظریه PC

R(config)# interface [interface of switch towards to PC]

R(config-if)# switchport mode access

R(config-if)# dot1x port-control auto

یعنی اگر کسی کامپیوٹر PC را از software ایجاد کند  
آن کسی کامپیوٹر کے برای فرستینگ username & password

## Implementing Firewall Technologies

\* كما ذكرنا هناك عدة أنواع من Firewall والتي تقسم إلى قسمين وهما :

### Stateless Firewall – 1

ومن أمثلته Packet Filtering Firewall وهذا يعني انه يعمل تحقيق في Packet من اي بورتقادمه والى اي بورت ذاهبه ولكن هذا النوع يحوي على عدة مشاكل منها انه في حال كان الاتصال قادم من كلايانت معين ذاهب الى WAN مثلاً على بورت 80 ولكن في عودته من WAN يكون هناك منع لهذا البورت من قبل Firewall من الدخول الى LAN .

### Statefull Firewall – 2

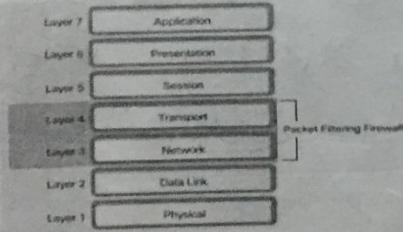
هذا النوع يعتبر اذكي من النوع السابق لـ Firewall حيث المثال عليه هو CBAC

### Application Gateway Firewall – 3

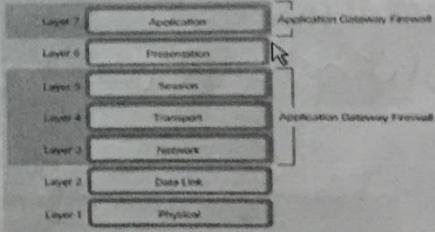
وهو من الانواع الجيدة جدا حيث انه يقوم بفحص Packet بأكمله للتأكد منه ويصل لعملية البحث الى Application Layer لليعرف ان هذا Packet لاي جهة ذاهب واي عمل سوف يقوم به .

### Firewall Type Descriptions

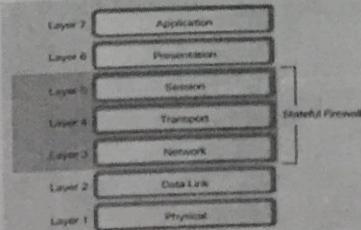
Packet Filtering Firewall



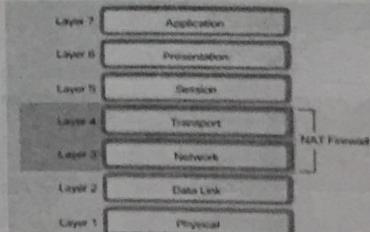
Application Gateway Firewall



Stateful Firewall



NAT Firewall



## Firewall types Description

Stateless firewall  $\nwarrow$   
transport layer  $\parallel$  ويعتمد على اللوغيراتيف  $\parallel$  (Packet filtering firewall)  
packets by Port no. او IP addresses او اينديكتور Networklayer  $\parallel$

Network layer و يقوم برقابة ال traffic stateful firewall لـ IP addresses و اذونات الملاحة  
portno. و transport layer يقوم برقابة ال traffic (الملاحة في فتح session layer بين PC و server)  
و يقوم برقابة ال traffic (فتح session layer بين client و server) لـ SSL/TLS session و غيره معاينه

في بداية هذا الموضوع سوف نأخذ شيء من المراجعه على ACL

## Configuring Numbered and Named ACLs

### Standard Numbered ACL Syntax

```
access-list acl-# {permit | deny | remark} source-addr [source-wildcard] [log]
```

### Extended Numbered ACL Syntax

```
access-list acl-# {permit | deny | remark} protocol source-addr [source-wildcard]
dest-addr [dest-wildcard] [operator port] [established]
```

### Named ACL Syntax

```
Router(config)# ip access-list [standard | extended] name_of_ACL
```

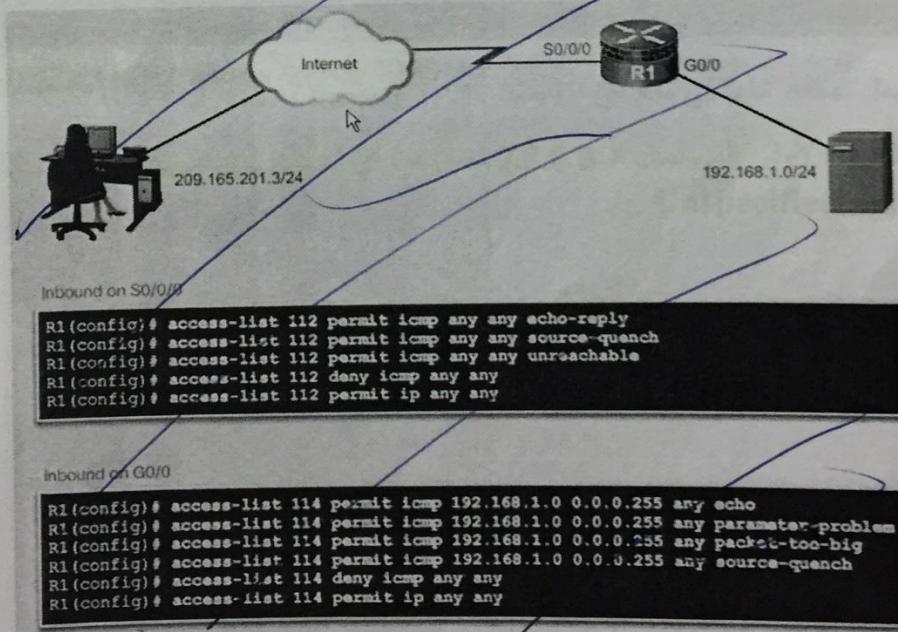
### Standard ACE Syntax

```
Router(config-std-nacl)# {permit | deny | remark} {source [source-wildcard] | any}
```

### Extended ACE Syntax

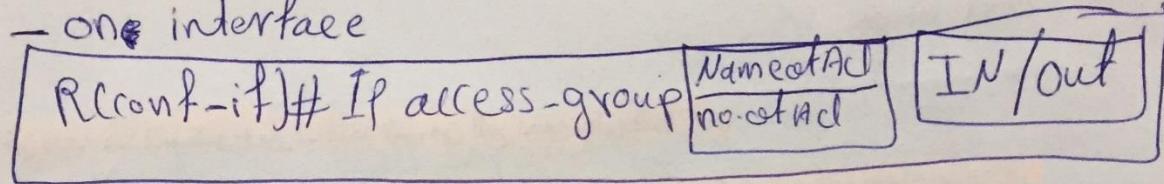
```
Router(config-ext-nacl)# {permit | deny | remark} protocol source-addr [source-wildcard]
dest-address [dest-wildcard] [operator port]
```

## Mitigating ICMP Abuse

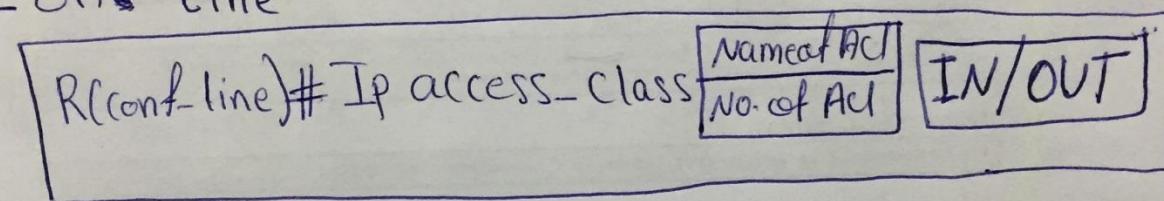


ACL JI mail ✘

- one interface

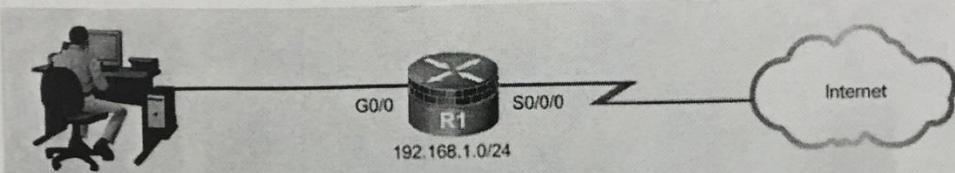


- one line



سوف نستخدم ACL في Security ومثال على ذلك يجب ان تتوفر هذه المجموعة من List على الراوتر المتصل بالانترنت لتجنب IP Spoofing كالتالي :

## Antispoofing with ACLs



Inbound on S0/0/0

```
R1(config)# access-list 150 deny ip 0.0.0.0 255.255.255.255 any
R1(config)# access-list 150 deny ip 10.0.0.0 0.255.255.255 any
R1(config)# access-list 150 deny ip 127.0.0.0 0.255.255.255 any
R1(config)# access-list 150 deny ip 172.16.0.0 0.15.255.255 any
R1(config)# access-list 150 deny ip 192.168.0.0 0.0.255.255 any
R1(config)# access-list 150 deny ip 224.0.0.0 15.255.255.255 any
R1(config)# access-list 150 deny ip host 255.255.255.255 any
```

Broadcast?

```
R1(config)# interface S0/0/0
R1(config-if)# ip access-group 150 IN
Inbound on G0/0
```

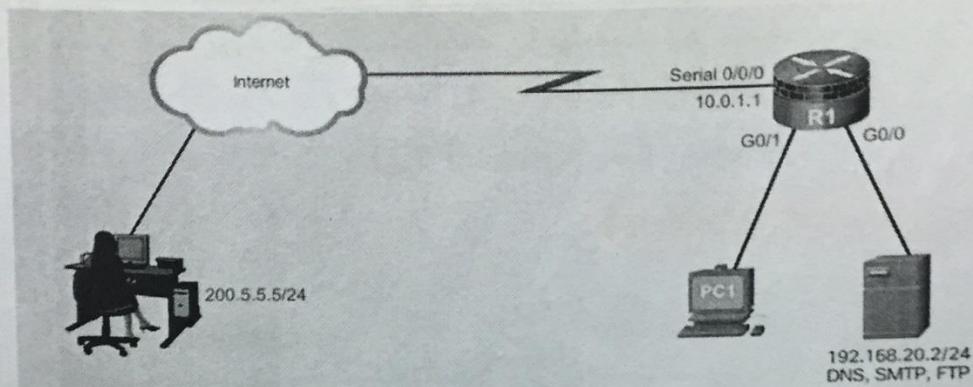
```
R1(config)# access-list 105 permit ip 192.168.1.0 0.0.0.255 any
```

```
R1(config)# interface G0/0
R1(config-if)# ip access-group 105
```

هذه الجمل تستفاد منها في منع اي IP ضمن الـ Private IP قادم من الـ WAN .

كمثال الجملة الأولى التي تمثل **0.0.0.0** تعني هنا اي احـ د قادم من **. Unspecified Address .**

## Permitting Necessary Traffic through a Firewall

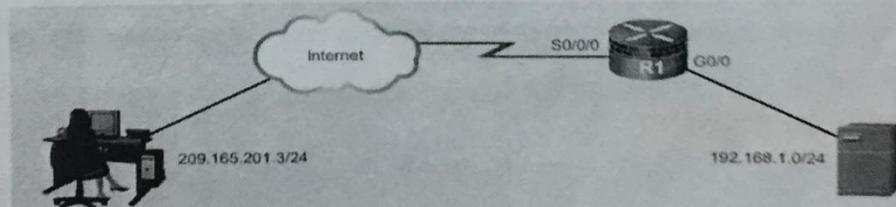


Inbound on Serial 0/0/0

```
R1(config)# access-list 180 permit udp any host 192.168.20.2 eq domain
R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq smtp
R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq ftp
R1(config)# access-list 180 permit tcp host 200.5.5.5 host 10.0.1.1 eq 22
R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq syslog
R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq snmptrap
```

في الصورة اعلاه يبين لنا اي الامور التي يفضل السماح لها بالمرور من خلال firewall

## Mitigating ICMP Abuse



Inbound on S0/0/0

```
R1(config)# access-list 112 permit icmp any any echo-reply
R1(config)# access-list 112 permit icmp any any source-quench
R1(config)# access-list 112 permit icmp any any unreachable
R1(config)# access-list 112 deny icmp any any
R1(config)# access-list 112 permit ip any any
```

Inbound on G0/0

```
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big
R1(config)# access-list 114 deny icmp any any
R1(config)# access-list 114 permit ip any any
```

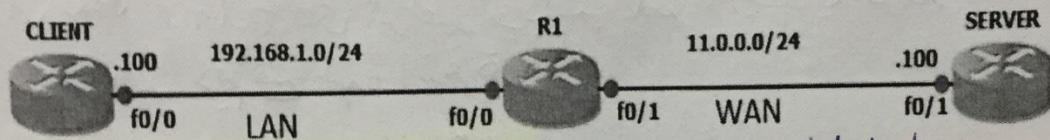
الصورة اعلاه في ما يخص عملية Ping .

في ما يخص ACL فإنها تعتبر كـ Firewall عند إنشائها على الراوتر وهناك أنواع عدّة هيكليات مستقلة لكل ACL لجعلها تعم كـ Firewall وهذه الأنواع أصبحت لا تستخدم في وقتنا الحاضر إلا ما ندر اي نقصد هنا نستعملها في حالة كانت الشركة لديها شبكة لا تحوي على أنواع جيدة وحديثة من الراوترات او السوچات. ولأنها لا تدعم Firewall

هذه الأنواع هي وبالإضافة لها نوع يسمى : TCP Intercept

: Established Keyword ACL - 1

فكرة



يوجة الكلمة established في نهاية كل قاعدة access-list

فكرة هذه الطريقة هي تطبيق ACL على الراوتر وان client يريد الذهاب الى السيرفر فستعمل هذه ACL على السماح بالمرور للاتصال القادم من الكلاينت الى السيرفر ولكن لا يرجع الاتصال من السيرفر الى الكلاينت الا اذا كان رجوع الاتصال مبني على ACK من الاتصال الرئيسي الذي عمله الكلاينت.

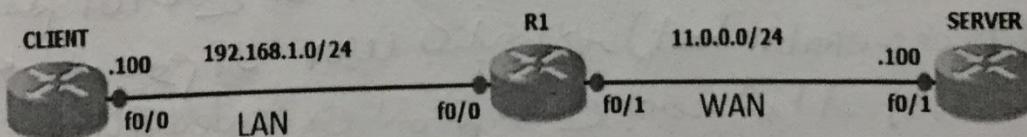
( اي يسمح فقط لـ Ack packet لـ client )

يعبر عن ال Router 1 از ال Client من خلال از Server (فقط)

حل هذه المسألة هي يسمح بمرور ال packet الذي انشأه من client و اي packet قادم من از Server ستفتح تم اعفافه عن از Ack Request .

: Time Range ACL - 2

فكرة



يعني ان تطبق از ACL باعتماد على الوقت.

الوقت

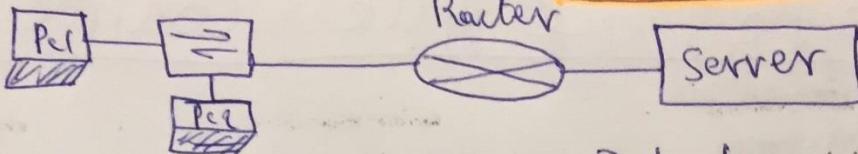
لو كان هناك صوره يعمل من 06:00AM الى 05:00PM يعني انه

يمكن از telnet من server الى client ولكن خارج از هذا الوقت غير

possible از از telnet . لذلك تطبق هذه الطريقة بواسطة (Time Range ACL)

الثانية topology يمكن إيجاده  $\therefore$  Dynamic ACL 

## lec 12



وهي أداة لـ PCI فقط لأنها تدخل إلى الـ Server

- Firewall & Dynamic Acl سے جگہ

لکی نہیں اور task ایسا ہے۔

ان تكون extended Acl و هي تمتع Dynamic Acl داخل او extended Acl  
نقرة في الـ Acl extended و توضح لهـ Acl المدخل الى الـ Server ومن ثم تـ  
ان ينبع الـ Acl منـ Server ولكن يجب ان يكونـ Acl لهـ  
قابلية ان يعاد telnet منـ الرافت ويكتب امرـ معيـ فيـ الرافت و بعـرةـ اـ  
يخرجـ منـ الرافت ويـمـ فتحـ فيهـ النـقرـةـ .

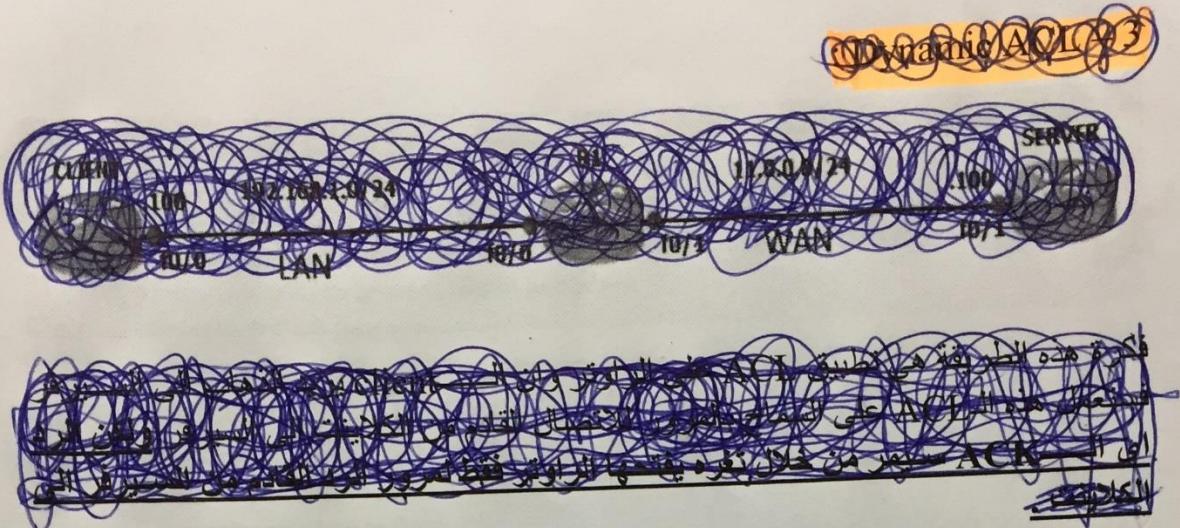
- Dynamic ACLs

نكون extended Acl لكي نسمح لـ Router A لـ Pcl باترر Acl لـ Router A لـ Pcl لـ telnet too لـ Router A لـ Pcl

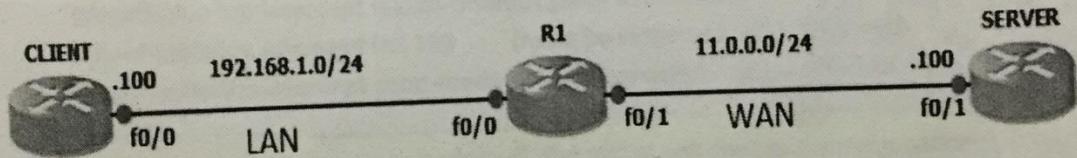
٢) تكون Dynamic Acl و static Acl هي اهمية بحث بعده او تجاهلها Extended Acl  
للحصول على سير Pcl الى Server . و يتم تحديد static Acl في حالة تم السماح للـ  
الدخول الى Router و كتابة her في المدخل enable mode  
٣) يكتب بحث امرئ تمنع اي Packet الى اي destination في او extended Acl

كما نعلم إن السلاحن للUser بالضول ك telnet لـ User بالضول او خطير و  
النبي لـ نوع او User بكتابه اخر (access-enable host) لـ كتابة  
نطري الـ ip السلاحن لـ extended Acl .  
User الـ ip السلاحن لـ extended Acl  
لـ اتم تحويل username & password لـ Router لـ telnet لـ User  
و ينزل الـ access-enable host لـ Router ie Pcl  
و اذا كانت مخطبة سفن يخون او  
بعدها او تعاينية وهذا يؤدي ان كتابة الـ extended Acl  
server الـ ip السلاحن لـ Router ie Pcl

يمكن أن يقدم الـ Router أو PC أو يسمى بالـ session في ACL. يمكن فتح النقرة وإغفالها أو يمكن لـ Router في أن يحددها بـ session (النقرة) وبعد ما تم إغفال النقرة.

Lee 13

: Reflexive ACL – 4



فكرة هذه الطريقة هي تطبيق ACL على الراوتر وان client يريد الذهاب الى السيرفر فستعمل هذه ACL على السماح بالمرور للاتصال القادم من الكلينت الى السيرفر وهذا سوف يعمل الراوتر على تكوين جدول يسمى State Table يستفاد من هذا الجدول لتسجيل الاتصال من الكلينت الى السيرفر والتحقق من ACK العائد من السيرفر الى الكلينت هل هي موجودة داخل الجدول ام لا.

## TCP Intercept - 5

هذا النوع لمنع احد اخطر الهجمات التي ذكرناها سابقاً وهي DOS ويحوي هذا النوع على Mode 2 وهي:

- Mitigation for half-open "embryonic" TCP sessions.
- TCP intercept tries to prevent this in two ways:

النقطة الأولى

- > Intercept mode (less common):
 

Proxy for all connections. Only connect to the server after the 3-way handshake completes.
- > Watch mode:
 

Passively monitors session establishment. Send TCP RST if the 3-way handshake doesn't complete in time.

النقطة الثانية

R(config)#ip tcp intercept mode <intercept|watch>

R(config)#ip tcp intercept watch-timeout [time in seconds]

R(config)#ip tcp intercept list 110 (must be extended ACL)

R(config)#ip tcp intercept drop-mode <oldest|random>

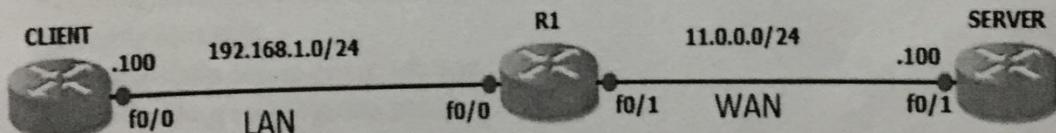
لتحذير المفهوم لـ session

بواسطة ACL نحدد معاصره (traffic) سعير لـ session list نفع (useful) لـ packets drop

For 1100 incomplete sessions by default, the router will start to drop the packets from that client

والنوع الاكثر شيوعاً هو Watch Mode

فكرة هذه التقنية هي لو كان لدينا الرابط التالي:



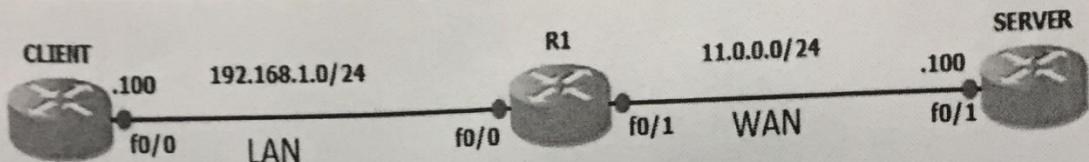
اراد الكلاينت الاتصال بالسيرفر فانه سوف يفتح Session مع السيرفر لاجل عملية الاتصال فسوف يعمل هنا الراوتر على مراقبة عدد Session التي سوف يستخدمها الكلاينت ولنفرض انه اتنا حددنا انه اذا فتح اكثرا من 1100 Session فسوف يجعل الراوتر على غلاق Session لم تكمل الاتصال لانه سوف يعتبر هذا الكلاينت كـ Attacker لكي يستنفذ كل Session الموجوده على السيرفر.

DOS (Denial of service attack) attack  
 الـ DOS يقوم به اجهزة اخرين او Sessions attack  
 الـ DOS يهدى الى Server ولهذا يُؤدي الى ان جهاز او Server الذي لا يقدر عن اتمام Sessions ويركتب attack  
 انما Server down

lecture

## :CBAC (Context Based Access Control) – 6

هذا النوع من Firewall هو من اهم الانواع ويسمى ايضا بالStatefull Firewall.



بالنسبة لهذا النوع فانه ايضا يعتمد على انشاء ACL ول يكن السيناريو التالي :

الكلاينت يريد الدخول الى السيرفر فسوف تكون ACL على الراوتر وكما نعلم انه عند فتح اتصال بين الكلاينت والسيرفر فيكون هنالك رد من جهة السيرفر والذي سوف يفحصه الراوتر اذا كان الرد على طلب من قبل الكلاينت فان الراوتر سوف يسمح للTraffic بالدخول اذا لم يكن الرد على طلب من قبل الكلاينت فان الراوتر سوف يمنع هذا Traffic من الدخول وذلك بتكونين Role يطلق عليها Inspect, Inspection تعنى يتم فحص Packet من قبل الراوتر للتتأكد هل هذا Packet رد على اتصال تم انشائه من قبل الكلاينت ام لا.

وتكون الاوامر كالتالي :

```

R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 any
R1(config)#access-list 101 deny tcp any any
R1(config)#access-list 101 deny udp any any
R1(config)#access-list 101 deny icmp any any
R1(config)#int f1/0
R1(config-if)#ip access-group 100 out
R1(config-if)#ip access-group 101 in
  
```

هنا سمحنا بالاتصال بكل انواعه من الكلاينت الى اي Destination والذي هنا يكون السيرفر ومنعنا اي Traffic قادم من WAN اي نقصد السيرفر من الدخول الى الراوتر اي الشبكة الداخلية.

ملحوظه : ACL التي تكون من LAN to WAN لا يهم اي نوع من انواع Standard/Extended ACL.

اما ACL من WAN to LAN يجب ان تكون Extended

\* عملنا على ACL الان سوف تكون الـ Role اي Inspection كال التالي :

```
R1(config)#ip inspect ?
  alert-off      Disable alert
  audit-trail    Enable the logging of session information (addresses and
                  bytes)
  dns-timeout    Specify timeout for DNS
  hashtable-size Specify size of hashtable
  log            Inspect packet logging
  max-incomplete Specify maximum number of incomplete connections before
                  clamping
  name           Specify an inspection rule
  one-minute     Specify one-minute-sample watermarks for clamping
  redundancy     Redundancy settings for firewall sessions
  tcp            Config timeout values for tcp connections
  udp            Config timeout values for udp flows
<cr>

R1(config)#ip inspect name ?
  WORD  Name of inspection defined (16 characters max)
```

كماموضح في الصورة اعلاه نكون Inspect ونعطي له اسم (مثلا PERMIT) بعدها نحدد نوع الـ Traffic (اي الـ Traffic الذي سوف يدخل للراوتر القادم من الـ WAN) ول يكن مثلا : TCP,UDP,ICMP

```
R1(config)#ip inspect name PERMIT tcp ?
  alert          Turn on/off alert
  audit-trail   Turn on/off audit trail
  router-traffic Enable inspection of sessions to/from the router
  timeout        Specify the inactivity timeout time
<cr>

R1(config)#ip inspect name PERMIT tcp
R1(config)#ip inspect name PERMIT udp
R1(config)#ip inspect name PERMIT icmp
```

الآن تم اعداد الـ Inspection والخطوه الاخيره هو وضعها على الـ Interface المقابل للـ WAN والتي في حالتنا سوف تكون OUT :

```
R1(config)#int f1/0
R1(config-if)#ip ins
R1(config-if)#ip inspect ?
  WORD  Name of inspection defined
R1(config-if)#ip inspect PERMIT out
```

Server will pc we packet ديلوكس يتم فحص او

## CCNA - Security

ملاحظه : لو اردنا ان نعمل اتصال من الراوتر الى السيرفر سوف لن نستطيع لو كانت الاوامر  
اعلاه على حالها ألا لو دخلنا الامر التالي :

```
R1(config)#ip inspect name PERMIT tcp ?  
alert           Turn on/off alert  
audit-trail     Turn on/off audit trail  
router-traffic  Enable inspection of sessions to/from the router  
timeout         Specify the inactivity timeout time  
<cr>  
  
R1(config)#ip inspect name PERMIT tcp router-traffic  
R1(config)#ip inspect name PERMIT udp router-traffic  
R1(config)#ip inspect name PERMIT icmp router-traffic
```

والذي سوف نسمح من خلاله بالاتصال ان يتم من الراوتر الى السيرفر . اي ايها " سعر في مراقبة  
ار Router traffic الذي تم توليه عن ار traffic \* بالنسبة لأوامر Show الخاصة بالـ Inspect هي :

```
R1#show ip inspect ?  
all            Inspection all available information  
config        Inspection configuration  
ha             Show commands for IOS firewall High Availability  
interfaces    Inspection interfaces  
mib           FW MIB specific show commands  
name          Inspection name  
sessions      Inspection sessions  
sis            Inspection sessions (debug version)  
statistics    Inspection statistics  
tech-support  Inspection technical support
```

# نحوحة فقط هنا النوع من المنهج

## ZBFW

: ZBFW (Zone Based Policy Firewall) - 7

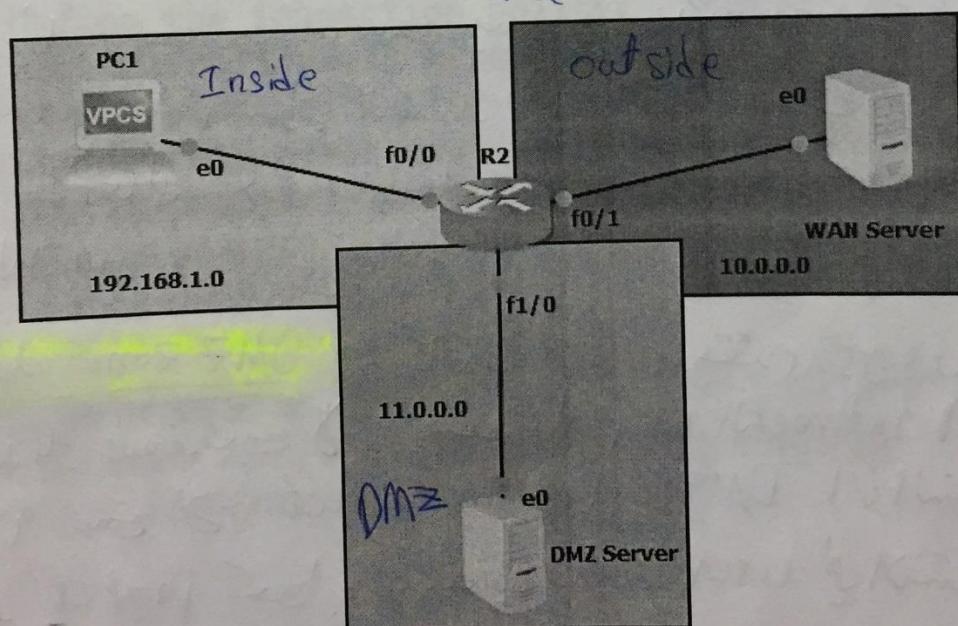
وهو من انواع Statefull Firewall وفكرة تكوين مناطق تسمى Zone في مثالنا التالي  
سيكون هناك 3 Zone وهي :

inside-  
outside-  
DMZ-

وبالاضافه الى ذلك هناك Zone مكونه تلقائيا تسمى Self Zone والفائده منها هي تجاوز المشكله التي كانت موجوده في CBAC والتي تمثل بان الراوتر الذي سوف يعمل كـ Firewall لا يتمكن من الاتصال بالشبكة الخارجيه الا بعد تطبيق امر Router Traffic Traffic كما ذكرنا سابقا والجدير باللاحظه ان كل Zone يتم احتسابها على عدد Interface التي تكون داخلها.

R2 is firewall device

المثال كالتالي :



## طريقة عمل ZBF

الخطوة الـ 1: ZBF هو برنامج ي Intercept (抓取) Packets (packets) من Internet و يقوم بـ Sniffing (抓取) Packets (packets) من Webserver (webserver) و يقوم بـ Sniffing (抓取) Packets (packets) من Webserver (webserver).

الخطوة الـ 2: يوجه أن تستمع لـ PC بال逎رو ان انت (webserver) و تستمع لـ PC بال逎رو ان انت (webserver).

عندما يجيء Packets (packets) من Webserver (webserver) فـ ZBF ي intercept (抓取) Packets (packets) من Webserver (webserver) و يـ Sniff (抓取) Packets (packets) من Webserver (webserver).

الخطوة الـ 3: يـ Sniff (抓取) Packets (packets) من Webserver (webserver) فـ ZBF يـ Sniff (抓取) Packets (packets) من Webserver (webserver) و يـ Sniff (抓取) Packets (packets) من Webserver (webserver).

الخطوة الـ 4: يـ Sniff (抓取) Packets (packets) من Webserver (webserver) فـ ZBF يـ Sniff (抓取) Packets (packets) من Webserver (webserver).

الخطوة الـ 5: يـ Sniff (抓取) Packets (packets) من Webserver (webserver) فـ ZBF يـ Sniff (抓取) Packets (packets) من Webserver (webserver).

الخطوة الـ 6: يـ Sniff (抓取) Packets (packets) من Webserver (webserver) فـ ZBF يـ Sniff (抓取) Packets (packets) من Webserver (webserver).

الخطوة الـ 7: يـ Sniff (抓取) Packets (packets) من Webserver (webserver) فـ ZBF يـ Sniff (抓取) Packets (packets) من Webserver (webserver).

الخطوة الـ 8: يـ Sniff (抓取) Packets (packets) من Webserver (webserver) فـ ZBF يـ Sniff (抓取) Packets (packets) من Webserver (webserver).

الخطوة الـ 9: يـ Sniff (抓取) Packets (packets) من Webserver (webserver) فـ ZBF يـ Sniff (抓取) Packets (packets) من Webserver (webserver).

الخطوة الـ 10: يـ Sniff (抓取) Packets (packets) من Webserver (webserver) فـ ZBF يـ Sniff (抓取) Packets (packets) من Webserver (webserver).

الخطوة الـ 11: يـ Sniff (抓取) Packets (packets) من Webserver (webserver) فـ ZBF يـ Sniff (抓取) Packets (packets) من Webserver (webserver).

Inspect → packets تفتيش فحص اطارات

## CCNA - Security

والاوامر ستكون :

### 1- Define the zones:

```
R1(config)#zone security INSIDE  
R1(config)#zone security OUTSIDE  
R1(config)#zone security DMZ
```

### 2- Classify the traffic:

```
R1(config)#class-map type inspect TCP → class map  
R1(config-cmap)#match protocol tcp ←TCP traffic  
R1(config)#class-map type inspect UDP → class map  
R1(config-cmap)#match protocol udp ← UDP traffic  
R1(config)#class-map type inspect ICMP → class map  
R1(config-cmap)#match protocol icmp ← ICMP traffic
```

### 3- Define the inspection policy:

```
R1(config)#policy-map type inspect IN_TO_OUT  
R1(config-pmap)#class TCP ← class  
R1(config-pmap-c)#inspect  
R1(config-pmap)#class UDP ← class  
R1(config-pmap-c)#inspect  
R1(config-pmap)#class ICMP ← class  
R1(config-pmap-c)#inspect
```

### 4- Associate the zone and apply the policy:

```
← Zones go policy here  
R1(config)#zone-pair security IN_TO_OUT_PAIR source INSIDE destination OUTSIDE  
R1(config-sec-zone-pair)#service-policy type inspect IN_TO_OUT
```

5- Apply the zone to the interface:

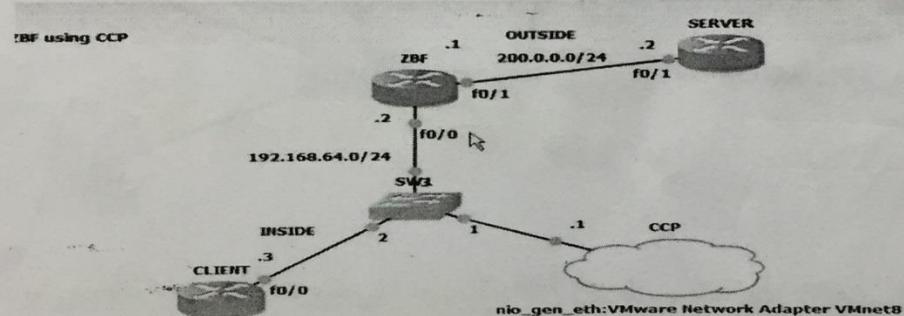
```
R1(config)#int s1/0  
R1(config-if)#zone-member security OUTSIDE  
R1(config)#int f0/0  
R1(config-if)#zone-member security INSIDE
```

6- Verify:

```
R1#show policy-map type inspect zone-pair sessions
```

\* استخدام ZPF مع CCP

المثال كالتالي :



## ZPF Configuration Considerations

- No filtering is applied for intra-zone traffic.
- Only one zone is allowed per interface.
- No Classic Firewall and ZPF configuration on same interface.
- If only one zone member is assigned, all traffic is dropped.
- Only explicitly allowed traffic is forwarded between zones.
- Traffic to the self zone is not filtered.

filtering only Self Zone

ملخص - في انتهاء الـ Acl التي تم دراستها لمحاباة الـ attack تتم بواسطة ان نفتح بفتح بورت محدد وآخر اخر portno . امر . لكن عادة ما كان الـ port الذي فتحناه لا يمر data محددة من خلال الـ port وتحوي على فايروسات محددة . لذلك سنتعرف ندراً سنتعرف كيف تتحقق او data التي نحن سمعنا لها باطرور .

CCNA - Security

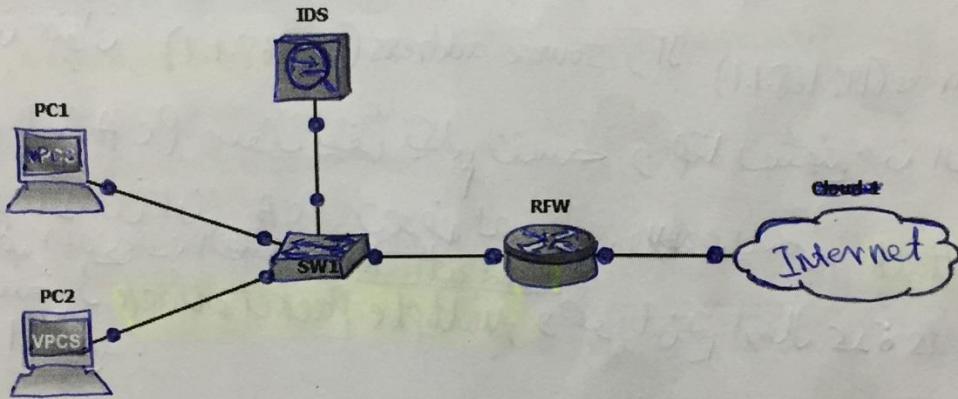
Lee 17

## Implementing Intrusion Prevention

في هذا الجزء سوف نتكلم عن نوعين من اجهزة الحماية والتي يمكن ايضا ان تكون برنامج يكون على نوعين هما IDS والـ IPS وفكرة لكل واحد منها تلخص كالتالي :

### IDS (Intrusion Detection System) - 1

فكرة IDS هي (IDS اما ان يكون Hardware او Software) لوكان لدينا الرابط التالي :



سوف يعمل IDS على اخذ نسخة من الداتا (النسخة التي سوف يأخذها بفعل تطبيق امر SPAN على البورت الذي يقابل IDS في السوق) القادمه من الانترنت والتي دخلت للشبكة عن طريق Firewall والتي دخلت بالفعل من خلال البورت الذي نحن فتحناه في FW لكي تمر الداتا اذا كان مصدرها طلب من خلال الشبكة الداخلية .

هذه النسخة التي سوف يأخذها IDS سوف يعمل على فحصها Deep Inspection للتأكد من خلوها من اي فايروسات وفي حال وجد ان هذه النسخة تحوي على فايروس فسوف يرسل تبليغ الى Router Firewall يبلغه ان مصدر هذه الداتا هو Attacker فسوف يعمل FW على عمل Block لهذا المصدر اي IP (عملية التبليغ هذه فقط في الاصدارات الاحدث من IDS).

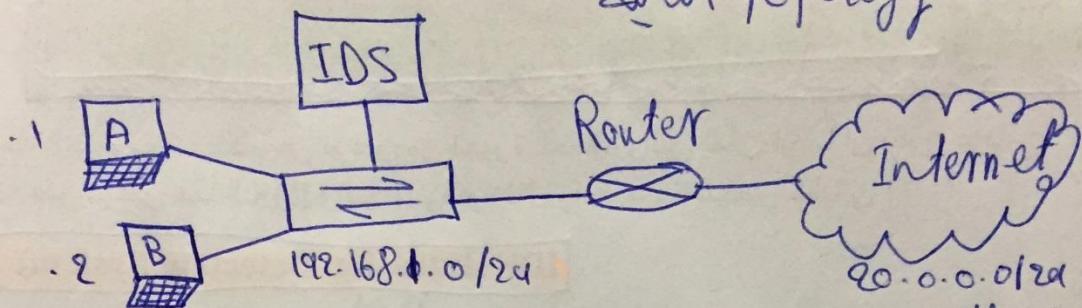
من الرابط اعلاه نفهم ان الداتا التي تحوي الفايروس قد دخلت بالفعل الى الشبكة الداخلية ويسمي IDS Work Passively Mode وهذا هي احد اشكالات IDS .

## مادحةIDS

- one packet attack
  - multiple packet attacks

- attack II in class

لوكان لينار الملة



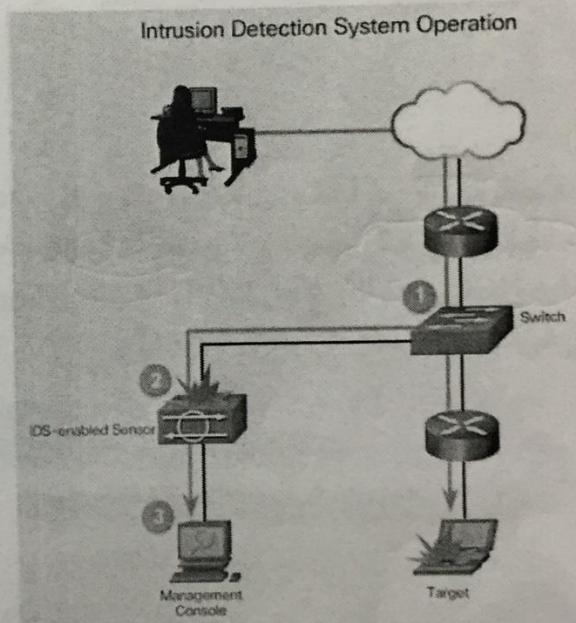
لأنه إذا تم إدخال بروتوكول ARP في الشبكة، فإنه سيقوم بـ  
استهداف عنوان destination address (192.168.1.1) للـ source address (192.168.1.1)

وبالتالي إنIDS ستفيق بكل نسخة وليست منIDS  
لأن يبلغ الأدوات أن PCA لم يتم لفهمه .  
ويمكن له أن يستخدم **Land attack** أو **Multiple packet attack** لـ-  
النهاية الرابعة .

## Monitor for Attacks

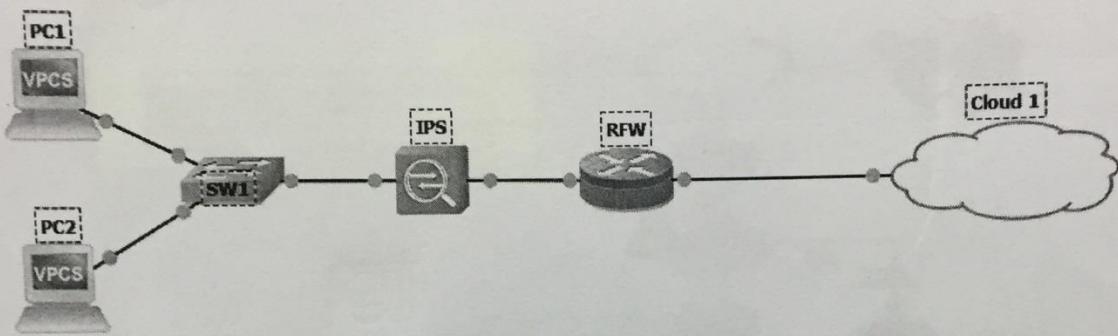
### Advantages of an IDS:

- attack N, this is just like attack because of 1
- Works passively
  - Requires traffic to be mirrored in order to reach it
  - Network traffic does not pass through the IDS unless it is mirrored



**IPS (Intrusion Prevention System) – 2**

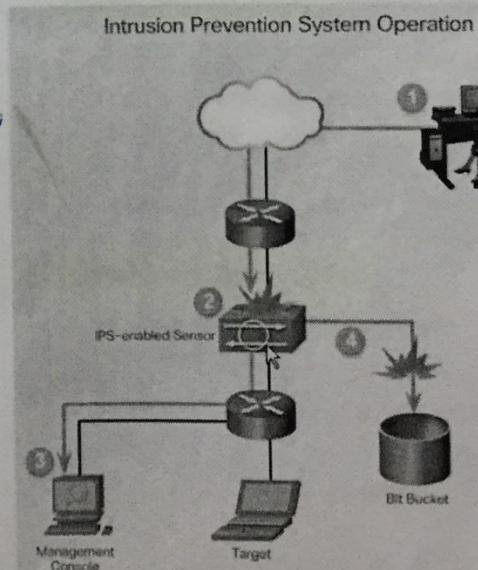
هذا النوع فكرته كالتالي :



كما نلاحظ من الرابط اعلاه ان IPS يكون في مسار الـ Attacker ان وجد اي يعمل على وقف الهجوم في حال حدوثه ولا يسمح للبيانات المصابة بفايروس مثلا من الدخول الى الشبكة الداخلية ويسمى هذا النوع من IPS بالـ **inline Mode** ومن مشاكل هذا النوع هو عمل لود عالي في الشبكة وممكن ان يعمل **Delay**.

**Detect and Stop Attacks****IPS:**

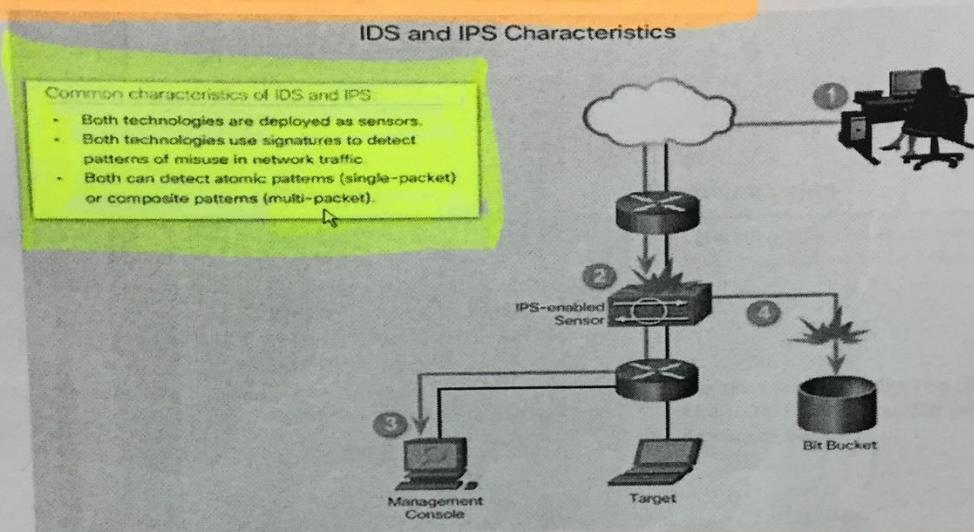
- Implemented in an inline mode *attack ينبعي المعا*
- Monitors Layer 3 and Layer 4 traffic
- Can stop single packet attacks from reaching target
- Responds immediately, not allowing any malicious traffic to pass



Sensor *او IPS و او IDS* *ان* *ان*

\* أوجه التشابه بين النوعين تلخص بالنقاط التالية :

## Similarities Between IDS and IPS



مقارنه بين النوعين تلخص بالنقاط التالية :

## Advantages and Disadvantages of IDS and IPS

### Advantages IDS:

- No impact on network *(نـاـفـعـ لـأـرـجـاعـ)*
- No network impact if there is a sensor failure. *(فـيـ حـالـةـ فـشـلـ اـلـI~D~Sـ فـيـ هـذـهـ أـسـبـابـ)*
- No network impact if there is a sensor overload. *(فـيـ حـالـةـ اـتـهـمـ اـلـI~D~Sـ فـيـ هـذـهـ أـسـبـابـ)*

### Disadvantages IDS:

- Response action cannot stop trigger *(أـعـصـيـعـ إـعـكـافـ اـلـI~D~Sـ)*
- Correct tuning required for response actions
- More vulnerable to network security evasion techniques *(أـنـهـ لـأـرـجـاعـ الـI~D~Sـ فـيـ هـذـهـ أـسـبـابـ)*

*أـنـهـ لـأـرـجـاعـ الـI~D~Sـ فـيـ هـذـهـ أـسـبـابـ*

### Advantages IPS:

- Stops trigger packets *(يـعـقـدـ اـلـI~P~Sـ)*
- Can use stream normalization techniques *(يـعـيـسـكـ اـنـ لـقـلـ لـI~P~Sـ .ـ مـعـ مـاـهـ)*
- Response action *(أـعـصـيـعـ إـعـكـافـ اـلـI~P~Sـ)*
- Fast detection *(فـيـ قـيـفـةـ اـلـI~P~Sـ)*

### Disadvantages IPS:

- Sensor issues might affect network traffic *(يـعـكـفـ اـنـ اـلـI~P~Sـ يـعـكـفـ اـنـ فـيـ مـاـهـ اـلـI~P~Sـ)*
- Sensor overloading impacts the network *(أـنـهـ لـأـرـجـاعـ اـلـI~P~Sـ فـيـ هـذـهـ أـسـبـابـ)*
- Some impact on network *(لـوـحـدـهـ اـلـI~P~Sـ)*

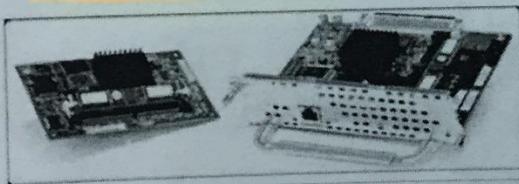
\*في ما يخص الـ IPS يوجد منه نوعان :

## Host-Based and Network-Based IPS

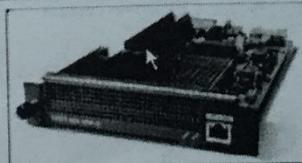
	Advantages	Disadvantages
Host-Based IPS (HIPS)	<ul style="list-style-type: none"> <li>Provides protection specific to a host operating system</li> <li>Provides operating system and application level protection</li> <li>Protects the host after the message is decrypted</li> </ul>	<ul style="list-style-type: none"> <li>Operating system dependent</li> <li>Must be installed on all hosts</li> </ul>
Network-Based IPS (NIPS)	<ul style="list-style-type: none"> <li>Cost effective <i>نافع و ملحوظ</i></li> <li>Operating system independent</li> </ul>	<ul style="list-style-type: none"> <li>Cannot examine encrypted traffic</li> <li>Must stop malicious traffic prior to arriving at host</li> </ul>

\*أنواع أجهزة الـ IDS والـ IPS لدى سيسكو :

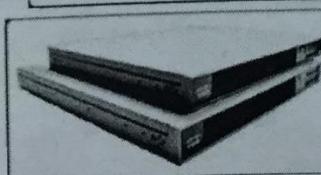
### Cisco's Modular and Appliance-Based IPS Solutions



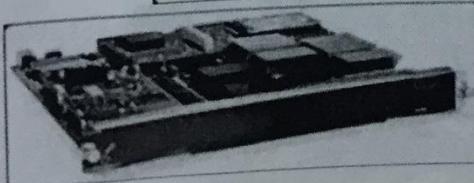
Cisco IPS AIM and Network Module Enhanced (IPS NME)



Cisco ASA AIP-SSM



Cisco IPS 4300 Series Sensors



Cisco Catalyst 6500 Series IDSM-2

\* عند عملية اختيار IPS يجب مراعات ما يلي :

## Choose an IPS Solution

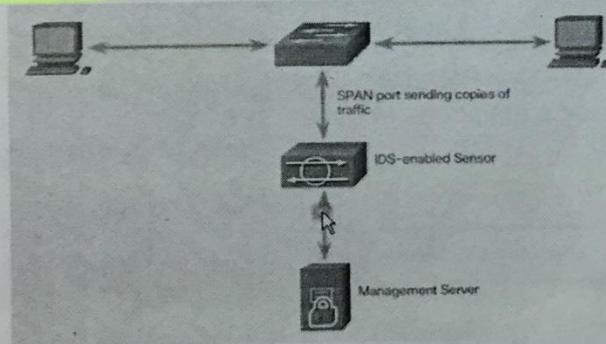
Factors affecting the IPS sensor selection and deployment:

- Amount of network traffic
- Network topology
- Security budget
- Available security staff to manage IPS

\* IPS يحوي على طريقتين للربط في الشبكة و تكو كال التالي :

## Modes of Deployment

### Promiscuous Mode



و هؤلاء يكونونIPS  
ليس بالمرأفة بين  
ال destination f source

### Inline Mode

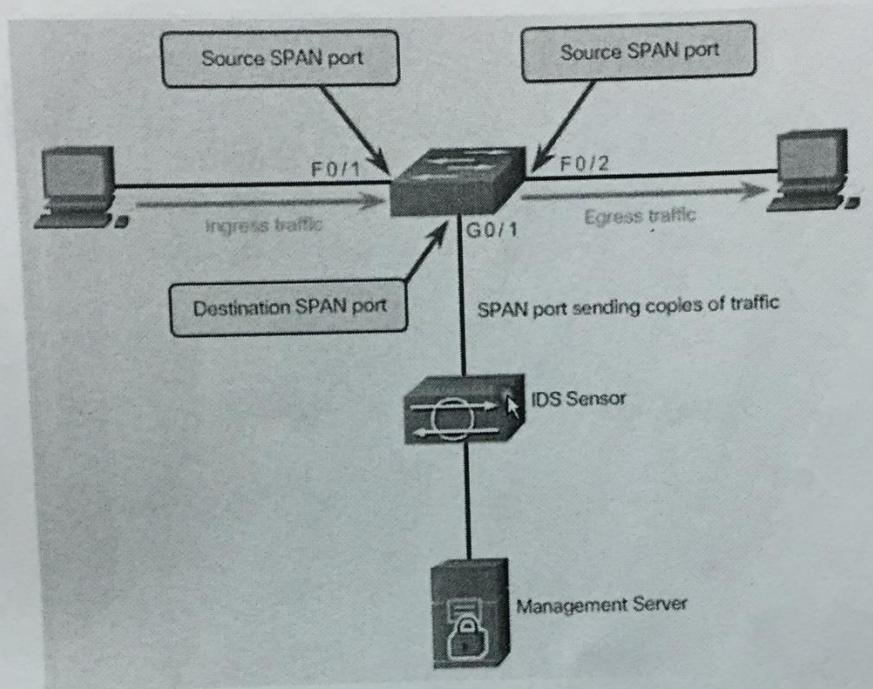


هؤلاء يكونونIPS  
يكون بين ال destination f source  
 IPS Sensor

أو IPS يكون بمقدار اثنين  
Inline mode وPromiscuous mode

\*في ما يخص البورت الذي سوف يحول نسخه الداتا الداخله الى IDS توضح بالشكل ادناه :

## Cisco SPAN



### Cisco SPAN Commands:

- Monitor session command – used to associate a source port and a destination port with a SPAN session.

Associate a SPAN session with a source port

```
Switch(config)# monitor session number source [ interface interface | vlan vlan ]
```

Associate a SPAN session with a destination port

```
Switch(config)# monitor session number destination [ interface interface | vlan vlan ]
```

- Show monitor command – used to verify the SPAN session.

# PART TWO

CCNA - Security

## IPS Signatures

اي Attacks في العالم يوجد له Signature تعرف هذا الـ Attack وبالتالي تبين لهذه العملية :

### Signature Attributes

A signature is a set of rules that an IDS and an IPS use to detect typical intrusion activity.

Signatures have three distinct attributes:

- Type
- Trigger(alarm)
- Action

الـ Signature هو مجموعه من القوانين التي سوف يستخدمهاIDS او IPS للكشف عن هذا Attack .

### Signature Types

Signatures are categorized as either:

- **Atomic** – this simplest type of signature consists of a single packet, activity, or event that is examined to determine if it matches a configured signature. If yes, an alarm is triggered and a signature action is performed.
- **Composite** – this type of signature identifies a sequence of operations distributed across multiple hosts over an arbitrary period of time.

: Composite يكون على نوعين هما Atomic والـ Signature

Atomic – 1 : وهو احد انواع Signature الذي يكون نوعه Single Packet اي بكت واحد يكون من خلاله Attack والنوع الذي يحمي من هذا Attack هو IDS .

Land attack هناك

2 - Composite Signature : هذا النوع من Signature يحوي على عدد من العمليات التي من خلالها يتم الـ Attack وال النوع الذي يحمي من هذا الـ Attack هو الـ IPS .

\* يتم التعرف على Signature مع كل تحديث حيث هذا التحديث يمكن الأجهزة من التعرف على الفايروسات الجديدة وطريقة الحماية منها ومن خلال موقع سسكون يمكن تحديث مثلاً IPS للتعرف على Signature الجديدة والحماية منها :

## Signature File

- As new threats are identified, new signatures must be created and uploaded to an IPS.
- A signature file contains a package of network signatures.

The screenshot shows the Cisco Download Software interface. At the top, there are navigation links for Products & Services, Support, How to Buy, Training & Events, and Partners. A search bar is also present. Below the header, the page title is "Download Software". Underneath, it says "Downloads Home > Products > Security > Network Security > Integrated Threat Control > IOS Intrusion Prevention System Feature Software > IOS IPS Signature Data File-S855". The main content area is titled "IOS Intrusion Prevention System Feature Software". On the left, there's a sidebar with a tree view showing "Latest S855" and "S351". The main panel shows "Release S855" with a "Signature Update S855 Readme" link. Below that is a table with one row: "IOS IPS Signature Update Package in 5x format for CLI users IOS-S855-CLI.pkg", with a "Release Date" of "03-MAR-2015", a "Size" of "21.52 MB", and "Download" and "Add to cart" buttons.

نستطيع فعل download لـ Signaturefile عن موقع Cisco كل خطة من الزمن . اي نعمل تحرير للـ IDS و/or IPS عن طريق تحرير او رادة عددar تنفيذar . Cisco موقع

⊗ نستطيع ان نقول ان الـ IDS و IPS الـ Signature

## Signature Micro-Engines

Cisco IOS defines five micro-engines:

- Atomic – Signatures that examine simple packets.
- Service – Signatures that examine the many services that are attacked.
- String - Signatures that use regular expression-based patterns to detect intrusions. *attack كل نوع من المهاجم*
- Multi-string – Supports flexible pattern matching and Trend Labs signatures. *attack كل نوع من المهاجم*
- Other – Internal engine that handles miscellaneous signatures. *attack كل نوع آخر من المهاجم*

الـIPS يكون مقسم على 5 اقسام كما مبين اعلاه لأجل الحمايه .

## Signature Alarm

Detection Type	Advantages
Pattern-based Detection	<ul style="list-style-type: none"> <li>Easy configuration</li> <li>Fewer false positives</li> <li>Good signature design</li> </ul>
Anomaly-based Detection	<ul style="list-style-type: none"> <li>Simple and reliable</li> <li>Customized policies</li> </ul>
Policy-based Detection	<ul style="list-style-type: none"> <li>Easy configuration</li> <li>Can detect unknown attacks</li> </ul>
Honey pot-based Detection	<ul style="list-style-type: none"> <li>Window to view attacks</li> <li>Distract and confuse attackers</li> <li>Slow down and avert attacks</li> <li>Collect information about attack</li> </ul>

attack signature *attack signature*  
 firewall *firewall*  
 traffic *traffic*  
 traffic *traffic*  
 traffic *traffic*  
*attack* *attack* *attack* *attack* *attack*

Detection Type	Disadvantages
Pattern-based Detection	<ul style="list-style-type: none"> <li>No detection of unknown signatures</li> <li>Initially a lot of false positives</li> <li>Signatures must be created, updated, and tuned</li> </ul>
Anomaly-based Detection	<ul style="list-style-type: none"> <li>Generic output</li> <li>Policy must be created</li> </ul>
Policy-based Detection	<ul style="list-style-type: none"> <li>Difficult to profile typical activity in large networks</li> <li>Traffic profile must be constant</li> <li>Dedicated honey pot server</li> <li>Hot pot server must not be trusted</li> </ul>
Honey pot-based Detection	

# Detection Types

CCNA - Security

## Pattern-Based Detection

	one Packet	Multiple Packet
	Signature Type	
	Atomic Signature	Composite Signature
Pattern-based Detection	No state required to examine pattern to determine if signature action should be applied.	Must contain state or examine multiple items to determine if signature action should be applied.
Example	Detecting an Address Resolution Protocol (ARP) request that has a source Ethernet address of FF:FF:FF:FF:FF:FF. because usually the destination ARP packet only has address as FF:FF:FF:FF:FF:FF	Searching for the string "confidential" across multiple packets in a TCP session.

## Anomaly-Based Detection

	one Packet	Multiple Packet
	Signature Type	
	Atomic Signature	Composite Signature
Anomaly-based Detection	No state required to identify activity that deviates from normal profile.	State required to identify activity that deviates from normal profile.
Example	Detecting traffic that is going to a destination port that is not in the normal profile.	Verifying protocol compliance for HTTP traffic.

port 21 telnet JI die  
 port 80 C19 JI die  
 port 23 telnet JI die  
 port 80 HTTP JI die

## Policy-Based and Honey Pot-Based Detection

	One Packet	Multiple Packet
	Signature Type	
	Atomic Signature	Composite Signature
Policy-based Detection	No state required to identify undesirable behavior.	Previous activity (state) required to identify undesirable behavior.
Example	Detecting abnormally large fragmented packets by examining only the last fragment. فی الحالات التي لا يتحقق فيها معايير التفتيش المطلوبة في كل بروتوكول اتصال (IP Packet)، فـ IPS يرسل تحذيرات يستفاد منها وتكون كالتالي:	A Sun Unix host sending RPC requests to remote hosts without initially consulting the Sun PortMapper program.

\*IPS ممكن ان يرسل تحذيرات يستفاد منها وتكون كالتالي :

## Alarm Triggering Mechanisms

### Understanding Alarm Types:

Alarm Type	Network Activity	IPS Activity	Outcome
False positive	Normal user traffic	Alarm generated	Tune alarm
False negative	Attack traffic	No alarm generated	Tune alarm
True positive	Attack traffic	Alarm generated	Ideal setting
True negative	Normal user traffic	No alarm generated	Ideal setting

admin will alarm if user IPs - بعثة - Positive -

admin will alarm if user IPs - لا يبعث - Negative -

attack - يبعث - true -

attack - لا يبعث - false -

so

alarm will attack if attack - يبعث - user IPs - attack - yes - false positive  
alarm if attack - لا يبعث - false negative

alarm will attack - yes - true positive

alarm if attack - لا يبعث - true negative

بالنسبة للتتبیه یکو نعلی نوعین :

## Manage Generated Alerts

Generating an Alert:

Specific Alert	Description
Produce alert	This action writes the event to the Event Store as an alert.
Produce verbose alert	This action includes an encoded dump of the offending packet in the alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected.

alarmdu bie ای  
attack) اسکرپت packet ۱۰۰> start ۰۰ alarm du ن

## Log Activities for Later Analysis

Logging the Activity:

Specific Alert	Description
Log attacker packets	This action starts IP logging on packets that contain the attacker address and sends an alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected.
Log pair packets	This action starts IP logging on packets that contain the attacker and victim address pair. An alert will be written to the Event Store, even if the Produce Alert action is not selected.
Log victim packets	This action starts IP logging on packets that contain the victim address and sends an alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected.

## Deny the Activity

Dropping or Preventing the Activity:

Specific Alert	Description
<u>Deny attacker inline</u>	<ul style="list-style-type: none"> <li>This action terminates the current packet and future packets from this attacker address for a specified period of time.</li> <li>The sensor maintains a list of the attackers currently being denied by the system.</li> <li>Entries may be removed from the list manually or automatically based on a timer.</li> <li>The timer is a sliding timer for each entry. Therefore, if attacker A is currently being denied, but issues another attack, the timer for attacker A is reset and attacker A remains on the denied attacker list until the timer expires.</li> <li>If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.</li> </ul>
<u>Deny connection inline</u>	This action terminates the current packet and future packets on this TCP flow.
<u>Deny packet inline</u>	This action terminates the packet.

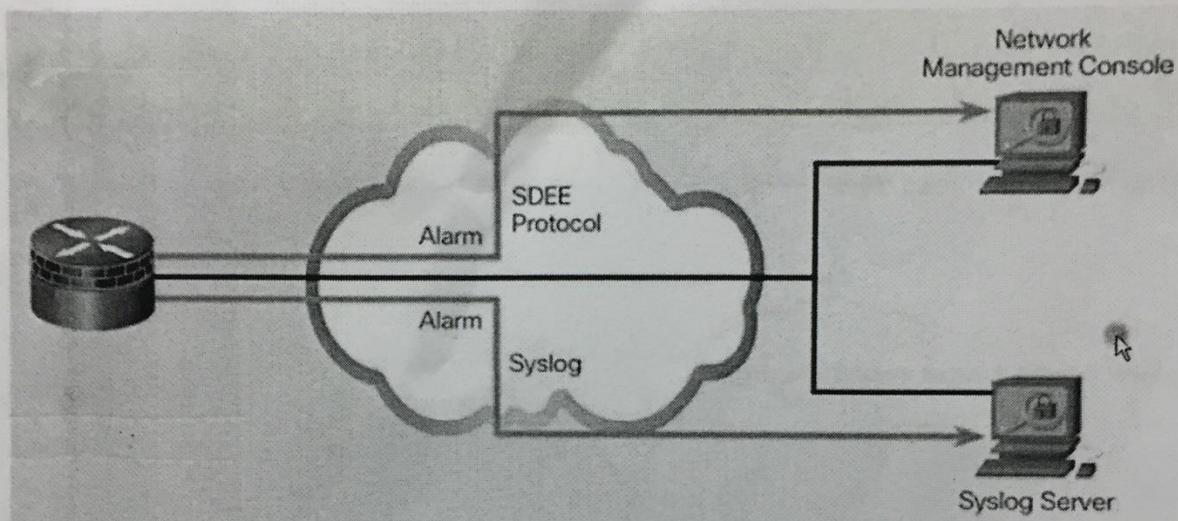
## Reset, Block, and Allow Traffic

Resetting the Connection and Blocking the Activity:

Specific Alert	Description
<u>Reset TCP connection</u>	This action sends TCP resets to hijack and terminate the TCP flow.
<u>Request block connection</u>	This action sends a request to a blocking device to block this connection.
<u>Request block host</u>	This action sends a request to a blocking device to block this attacker host.
<u>Request SNMP trap</u>	<ul style="list-style-type: none"> <li>This action sends a request to the notification application component of the sensor to perform Simple Network Management Protocol (SNMP) notification. An alert will be written to the Event Store, even if the Produce Alert action is not selected.</li> </ul>

\*يمكن ارسال logs الى IPS الى Logs Server بطريقتين هما :

## Secure Device Event Exchange



### SDEE ( Secure Device Event Exchange) – 1

هذا البروتوكول مخصص لأرسال logs الناتجه عن IPS .

### Syslog – 2

المعروف هذا البروتوكول وطريقة عمله .

# Lec 18

CCNA - Security

## : IPS Configuration\*

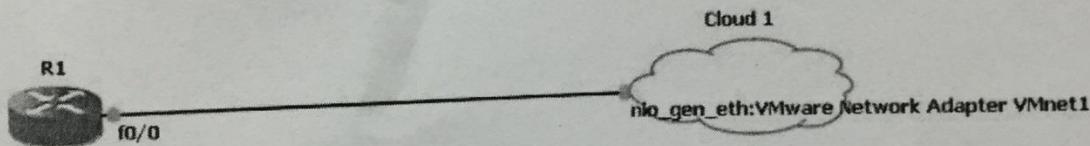
هناك طريقتين للـConfig بالنسبة للـIPS وهي :

1 - بواسطة الـCLI اي Config مباشر على الراوتر او جهاز الـIPS

2 - بواسطة الـCCP

ملاحظه (كما ذكرنا يمكن ان يكون الـIPS عباره عن كارت Module يربط داخل الراوتر او جهاز مستقل او يمكن تطبيقه على الراوتر مباشره ولكنه سوف ياثر على الـProcessor .)

المثال التالي سوف نبين عملية تطبيق الأوامر :



أولاً / نعمل للـFlash او الـDisk في الراوتر لتهيئته لاستقبال الـSignature : Signature Format

```
R1#format disk0:  
Format operation may take a while. Continue? [confirm]  
Format operation will destroy all data in "disk0:". Continue? [confirm]  
Writing Monlib sectors.....  
Monlib write complete
```

ثانياً / انشاء File بـاي اسم نختاره ولتكن الاسم IPS في داخل للـFlash او الـDisk:0 في داخله الـSignature : Signature

```
R1#mkdir ips  
Create directory filename [ips]?  
Created dir disk0:/ips
```

**ثالثاً/ نسخ الـ Signature الخاصه بالـ IPS الى الراوتر**

```
R1#copy tftp: disk0:/ips
Address or name of remote host [10.0.0.2]?
Source filename [IOS-S636-CLI.pkg]?
Destination filename [/ips/IOS-S636-CLI.pkg]?
Accessing tftp://10.0.0.1/IOS-S636-CLI.pkg...
Loading IOS-S636-CLI.pkg from 10.0.0.2 (via FastEthernet0/0): !!!!!!!!
!!!!!!![OK - 14685484 bytes]
14685484 bytes copied in 317.128 secs (46308 bytes/sec)
```

**رابعاً/ تنفيذ اوامر IPS لانشاء Rule الخاصه بنا كالتالي :**

R1(config)#ip ips ?	
auto-update	Auto Update
config	Location of IPS configuration files
deny-action	Specify Deny action
enable-clidelta	Enable the clidelta functionality
event-action-rules	Event Action Rules (SEAP)
fail	Specify what to do during any failures
inherit-obsolete-tunings	Transfer select tunings from obsolete signatures
memory	Memory settings for signature compilation
<b>name</b>	Specify an IPS rule
notify	Specify the notification mechanisms (SDEE or log) for the alarms
select-exploit	Select exploit or vulnerability signatures
signature-category	Signature Category
signature-definition	Signature Definition
tunables	Configure the tunable parameters for IPS

**. Rule 1 - تحديد اسم للـ Rule**

```
R1(config)#ip ips name ROUTER_IPS
```

**2 - تحديد مكان الـ Signature ومكان تجميع الـ IPS Logs**

```
R1(config)#ip ips config location disk0:/ips
R1(config)#ip ips no
R1(config)#ip ips notify s
R1(config)#ip ips notify SDEE
R1(config)#ip http server
```

**كما ذكرنا ان SDEE هو السيرفر المخصص اصلاً لتجميع الـ IPS Logs**