2021-2022

جامعة البعث

الكلية التطبيقية – السنة الرابعة – تقنيات الحاسوب

الفصل الثاني 2021-2022

Networks Security

Lecture 6

SUPERVISED BY

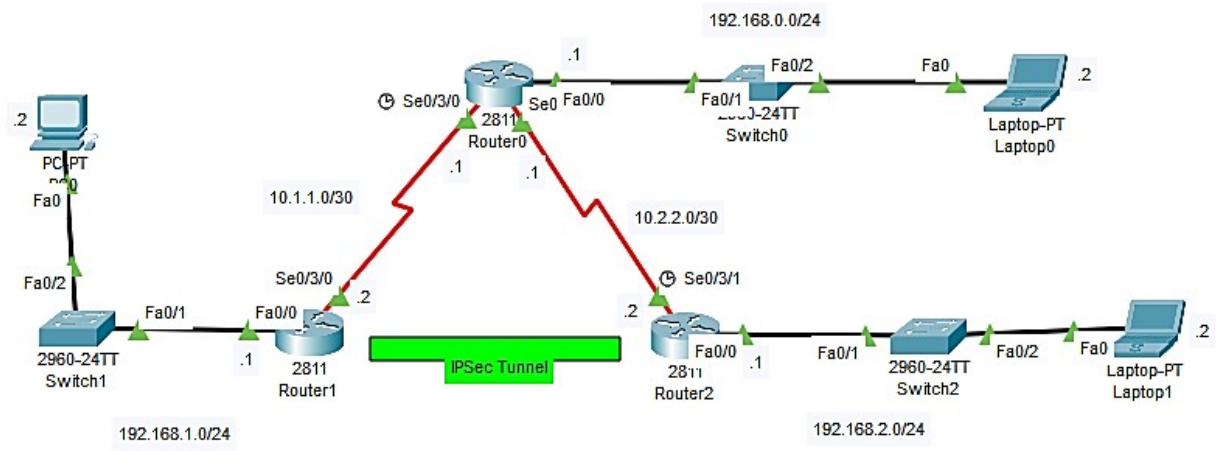
ENG. ALI MUSTAFA

Academic Year 2021-2022

IP Security (IPSec)

حماية الشبكات الافتراضية (VPN – Virtual Private Network) باستخدام IPSec

الطوبولوجيا المستخدمة:



سنقوم بإنشاء وصلة افتراضية بين الشبكتين 192.168.1.0 / 24 و 192.168.2.0 / 24 وحمايتها باستخدام IPSec.

لا ننسى أولاً إعطاء العناوين المناسبة كما هو موضّح بالشكل السابق وكذلك تطبيق توجيه معين (وليكن توجيه Static مثلاً) كالتالي:

على المُوجّه Router 0:

```
ip route 192.168.1.0 255.255.255.0 10.1.1.2
ip route 192.168.2.0 255.255.255.0 10.2.2.2
```

على المُوجّه Router 1:

```
ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

على المُوجّه Router 2:

```
ip route 0.0.0.0 0.0.0.0 10.2.2.1
```

الخطوات لإعداد IPSec:

تتم الخطوات على كل من طرفي الاتصال وهما المُوجّهين Router1 وRouter2.

- ✓ **الخطوات على طرف الاتصال الأول (Router1):**

الخطوة الأولى:

بالبداية سنقوم بتعريف قائمة وصول ACL تعرف لنا الرزم التي نريد حمايتها باستخدام IPSec عِلماً أنّ أيّة رُزم لا يتم تصنيفها ضمن القائمة لن يتم حمايتها:

```
access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
// أنشأنا Numbered Extended ACL للسماح بالاتصال ومرور البيانات بين الشبكتين 192.168.1.0 / 24 و 192.168.2.0 / 24
```

الخطوة الثانية:

تعريف وسطاء المرحلة الأولى لبروتوكول IKE (Internet Key Exchange) والتي يتم من خلالها **تأسيس رابطة حماية** ISAKMP SA (Internet Security Association and Key Management Protocol) والتي سنُحدد فيها خوارزميات التوثّق والتشفير وغيرها من **الوسطاء** كما يلي:

```
// 1-أنشأنا سياسة أو رابطة حماية isakmp برقم 10
crypto isakmp policy 10
//2-بعدها نُحدّد خوارزمية التشفير ولتكن AES وتحديد طريقة التوثّق من بين الطرفين المتصلين ولتكن باستخدام مفتاح مُشترك (Pre-Shared Key)
encryption aes
authentication pre-share
//3- نعطي رقم للمجموعة التي ستحوي طرفي الاتصال السابقين وليكن 2وهو نفسه سنستخدمه ضمن الطرف الثاني وهو المُوجّه Router2.
group 2
exit
//4- نُحدّد الان المفتاح المُشترك المُستخدم للتوثّق بين الطرفين وليكن vpnpa55 ونحدّد معهُ عنوان الطرف الثاني (عنوان المُوجّه Router2) وهو 10.2.2.2
crypto isakmp key vpnpa55 address 10.2.2.2
```

الخطوة الثالثة:

تعريف وسطاء <u>المرحلة الثانية</u> لبروتوكول ISAKMP وذلك عن طريق إنشاء مجموعة Transform Set نجمع من خلالها وسطاء المرحلة الثانية وهي التي ستستخدم في **<u>حماية الرُزم</u>** كما يلي:

```
// 1-ننشئ Transform set باسم VPN-SET ونحدد فيها الخوارزميات المُستخدمة فعلياً في تشفير الرُزم ولتكن 3DES والخوارزميات المُستخدمة للتوثّق من صحة هذه الرُزم ولتكن SHA-HMAC:
crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
//2-ننشئ بعدها map وليكن باسم VPN-MAP لربط هذه ال Transform set مع رابطة الحماية التي أنشأناها ضمن الخطوة الثانية وكنا قد أعطيناها الرقم 10
crypto map VPN-MAP 10 ipsec-isakmp
//3- نحدد الطرف الثاني من الاتصال وهو Router2 عن طريق عنوانه 10.2.2.2
set peer 10.2.2.2
//4- نكتب التعليمة التالية من أجل وضع واعتماد هذه الTransform set:
set transform-set VPN-SET
//5- تحديد البيانات التي سيتم حمايتها وهي البيانات بين طرفي الاتصال التي حددناها ضمن قائمة التحكّم بالوصول التي أنشأناها في الخطوة الأولى ذات الرقم 110
match address 110
exit
```

الخطوة الرابعة:

ربط بيانات المرحلة الثانية التي حصلنا عليها من خلال map (والتي أسميناها *VPN-MAP*) مع الواجهة الخارجية s0/3/0 للمُوجّه Router1 وذلك لتطبيق الحماية باستخدام IPSec كما يلي:

```
interface s0/3/0
crypto map VPN-MAP
```

- ✓ **الخطوات على طرف الاتصال الثاني (Router2):**

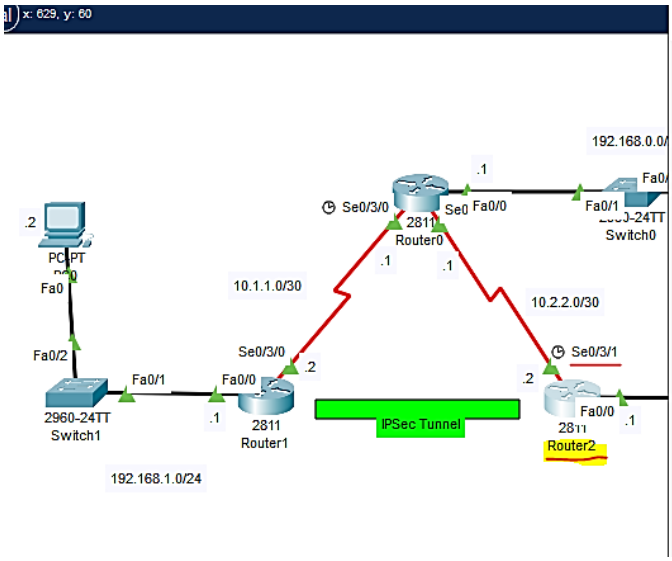
الآن سنقوم بتطبيق الخطوات ذاتها مع بعض التغيرات على طرف الاتصال الثاني وهو المُوجّه **Router2** كما يلي:

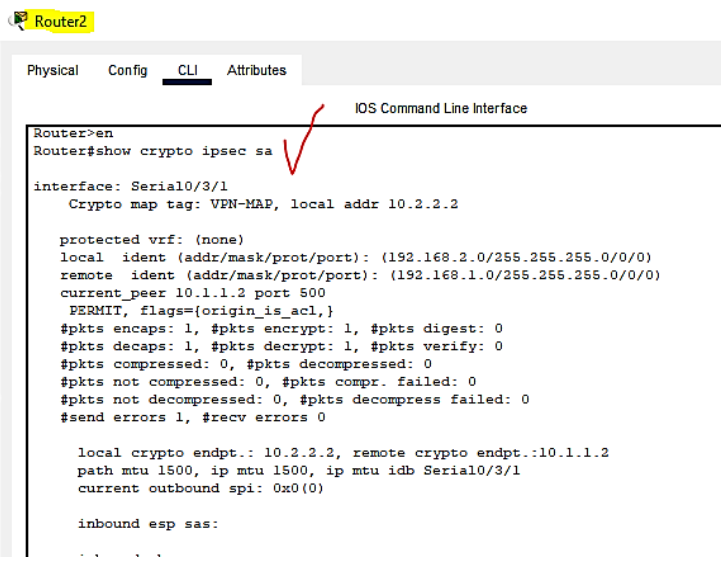
(طبعاً يجب مراعاة استخدام نفس الخوارزميات والمفاتيح التي تم إعداداها في الطرف الأول حتى يتمكنا من الاتصال)

```
access-list 110 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
#####################################################
crypto isakmp policy 10
encryption aes
authentication pre-share
group 2
exit
                                    //طبعاً هنا سنُحدّد عنوان الطرف الأول وهو عنوان المُوجّه Router1
crypto isakmp key vpnpa55 address 10.1.1.2
#####################################################
crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
set peer 10.1.1.2
set transform-set VPN-SET
match address 110
exit
#####################################################
interface s0/3/1
crypto map VPN-MAP
```

- للتحقّق يمكننا كتابة الأمر التالي:

```
Show crypto ipsec sa
```


x: 629, y: 60
192.168.0.0/
.1
Fa0/
Se0/3/0
Se0
Fa0/0
Fa0/1
2811
Router0
Switch0
.2
PC-PT
Fa0
.1
.1
10.1.1.0/30
10.2.2.0/30
Fa0/2
Se0/3/0
.2
Se0/3/1
Fa0/1
Fa0/0
.2
Fa0/0
2960-24TT
Switch1
.1
2811
Router1
IPSec Tunnel
2811
Router2
.1
192.168.1.0/24


Router2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>en
Router#show crypto ipsec sa
interface: Serial0/3/1
Crypto map tag: VPN-MAP, local addr 10.2.2.2
protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 10.1.1.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0
#pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0
local crypto endpt.: 10.2.2.2, remote crypto endpt.:10.1.1.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/3/1
current outbound spi: 0x0(0)
inbound esp sas:

Done

المراجع

- جامعة البعث -كلية الهندسة المعلوماتيّة -السنة الخامسة / مُقرّر أمن الشبكات الحاسوبيّة / **الدُكتورة زينب خَلوف.**

???Any Questions

أطيب الأُمنيات بالنجاح والتوفيق

مُدرّس المُقرر: م. علي مصطفى