2021-2022

جامعة البعث

الكلية التطبيقية – السنة الرابعة – تقنيات الحاسوب

الفصل الثاني 2021-2022

Networks Security

Lecture 4

:SUPERVISED BY

ENG. ALI MUSTAFA

Academic Year 2021-2022

قوائم التحكّم بالوصول

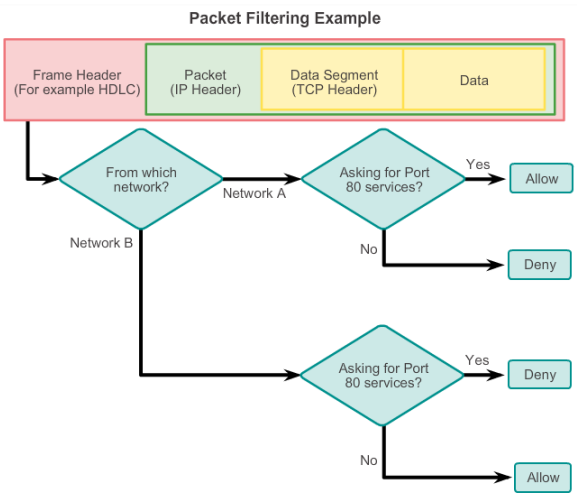
Access Control Lists (ACLs)

فلترة الرُزم (Packet filtering)

تتحكم تصفية الرُزم، التي تسمى أحيانًا تصفية الرُزمة الثابتة، في الوصول إلى الشبكة عن طريق تحليل الرُزم الواردة والصادرة وتمريرها أو إهمالها بناءً على معايير معينة، مثل عنوان IP المصدر، وعناوين IP الوجهة، والبروتوكول المنقول داخل الرُزمة.

يعمل جهاز التوجيه كمُصفّي للرُزم عندما يقوم بإعادة توجيه الرُزم أو رفضها وفقًا لقواعد التصفية (الفلترة).

قائمة التحكم بالوصول ACL هي قائمة متسلسلة من عبارات السماح أو الرفض، والمعروفة باسم access control entries (ACEs).



إرشادات عامة لإنشاء قوائم التحكم في الوصول

- ✓ استخدم قوائم ACL في موجهات جدار الحماية (firewall routers) الموضوعة بين شبكتك الداخلية والشبكة خارجية مثل الإنترنت.
- ✓ استخدم قوائم التحكم في الوصول (ACLs) على جهاز توجيه يقع بين جزأين من شبكتك للتحكّم في حركة المرور التي تدخل أو تخرج من جزء معين من شبكتك الداخلية.
- ✓ قم بإعداد قوائم التحكم في الوصول (ACLs) على أجهزة التوجيه الحدودية، وهي أجهزة التوجيه الموجودة على حواف الشبكات الخاصة بك.

- ✓ قم بإعداد قوائم التحكم في الوصول (ACL) لكل بروتوكول شبكة تم إعداده على منافذ الموجّه الحدوديّ.
- ✓ يتم وضع ACL واحدة لكل بروتوكول -للتحكّم في تدفّق حركة المرور على منفذ ما، ويجب تحديد ACL لكل بروتوكول مُفعّل على المنفذ.
- ✓ يتم وضع ACL واحدة لكل اتجاه -تتحكّم قوائم التحكم في الوصول (ACL) في حركة المرور في اتجاه واحد في كل مرة على المنفذ. يجب إنشاء اثنين من قوائم التحكم في الوصول (ACL) منفصلة للتحكّم في حركة المرور الواردة (Inbound) والصادرة (Outbound).
- ✓ يتم وضع ACL واحدة لكل واجهة -تتحكّم قوائم التحكّم في الوصول (ACL) في حركة المرور لمنفذ ما، على سبيل المثال، GigabitEthernet 0/0.

Guideline	Benefit
Base your ACLs on the security policy of the organization.	This will ensure you implement organizational security guidelines.
Prepare a description of what you want your ACLs to do.	This will help you avoid inadvertently creating potential access problems.
Use a text editor to create, edit and save ACLs.	This will help you create a library of reusable ACLs.
Test your ACLs on a development network before implementing them on a production network.	This will help you avoid costly errors.

أنواع قوائم التحكّم بالوصول (Types of Cisco ACLs)

لدينا نوعان:

1) **Standard ACLs:** تسمح لك قوائم ACLs القياسية بالسماح بحركة المرور أو رفضها بناءً على عناوين IP المصدر فقط.

لا يهم وجهة الرُزمة والمنافذ (TCP ports) المعنية.

مثال توضيحيّ:

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

هنا سيتم السماح لجميع حركات المرور من الشبكة / 24192.168.30.0.

ويتم حظر جميع حركات المرور الأخرى باستخدام قائمة التحكم بالوصول هذه بسبب وجود عبارة "deny any" ضِمنيًا في نهاية أي قائمة ACL.

2) **Extended ACLs:** تقوم قوائم ACL المُوسعة بتصفية رُزم البيانات IP بناءً على العديد من السمات ؛مثل **نوع البروتوكول وعنوان IP للمصدر أو/و للوجهة ومنافذ TCP أو UDP للمصدر و / أو للوجهة**.

مثال توضيحيّ:

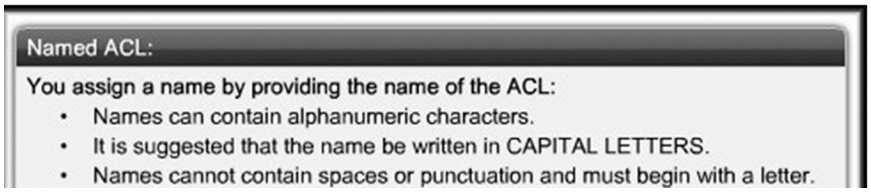
```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

يتم هنا السماح بحركة المرور التي تنشأ من أي عنوان على شبكة / 24192.168.30.0 إلى أي مضيف (جهاز) وجهة على المنفذ 80 (وهو منفذ البروتوكول HTTP).

➢ مجالات ترقيم قوائم التحكّم بالوصول

➢ قوائم التحكّم بالوصول المُسمّاة

يتم فيها استخدام اسم محرفيّ من أجل تسمية القائمة:



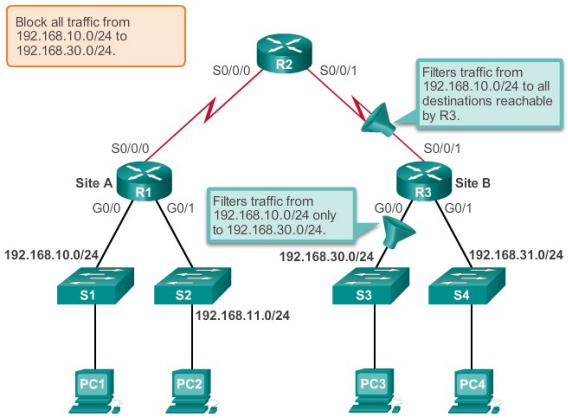
لا تخبرك قائمة التحكم في الوصول المرقّمة بالغرض أو الهدف من القائمة لكن يمكننا باستخدام قوائم ACL المسماة تسمية القائمة باسم ما يدل على عملها.

➢ مكان تموضع قوائم التحكّم بالوصول (Where to Place ACLs)

يجب وضع كل ACL بمكان يكون لها فيه أكبر تأثير على الكفاءة.

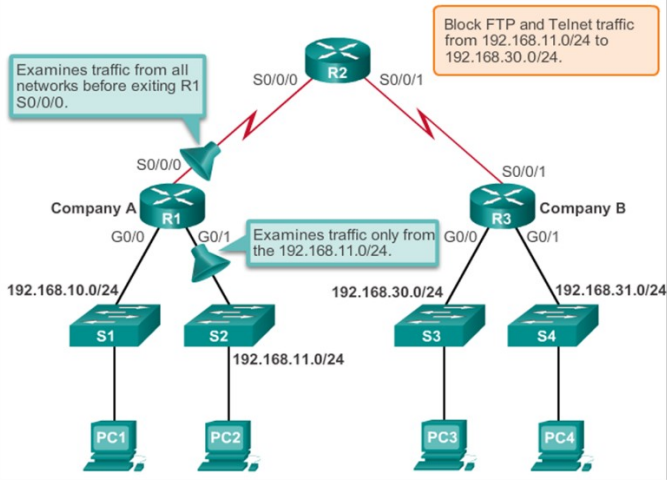
القواعد الأساسية هي:

Standard ACLs: يتم وضعها بالقرب من الوجهة قدر الإمكان نظرًا لأن قوائم ACL القياسية لا تُحدد عناوين الوجهة.



Standard ACL Placement

Extended ACLs: يتم وضع قوائم ACLs المُوسّعة في أقرب مكان ممكن من مصدر حركة المرور المُراد تصفيتها.



Extended ACL Placement

ACL Wildcard Masking ➢

- Wildcard Mask Examples: Hosts / Subnets (مطابقة جهاز معين أو شبكة كاملة):

Example 1

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.0.	00000000.00000000.00000000.00000000
Result	192.168.1.1	11000000.10101000.00000001.00000001

Example 2

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	255.255.255.255	11111111.11111111.11111111.11111111
Result	0.0.0.0	00000000.00000000.00000000.00000000

Example 3

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.255	00000000.00000000.00000000.11111111
Result	192.168.1.0	11000000.10101000.00000001.00000000

- Wildcard Mask Examples: Match Ranges (مُطابقة مجال من العناوين):

Example 1

	Decimal	Binary
IP Address	192.168.16.0	11000000.10101000.00010000.00000000
Wildcard Mask	0.0.15.255	00000000.00000000.00001111.11111111
Result Range	192.168.16.0 to 192.168.31.255	11000000.10101000.00010000.00000000 to 11000000.10101000.00011111.11111111

Example 2

	Decimal	Binary
IP Address	192.168.1.0	11000000.10101000.00000001.00000000
Wildcard Mask	0.0.254.255	00000000.00000000.11111110.11111111
Result	192.168.1.0	11000000.10101000.00000001.00000000
	All odd numbered subnets in the 192.168.0.0 major network	

- Calculating the Wildcard Mask:

Example 1

	255.255.255.255
–	255.255.255.000
	000.000.000.255

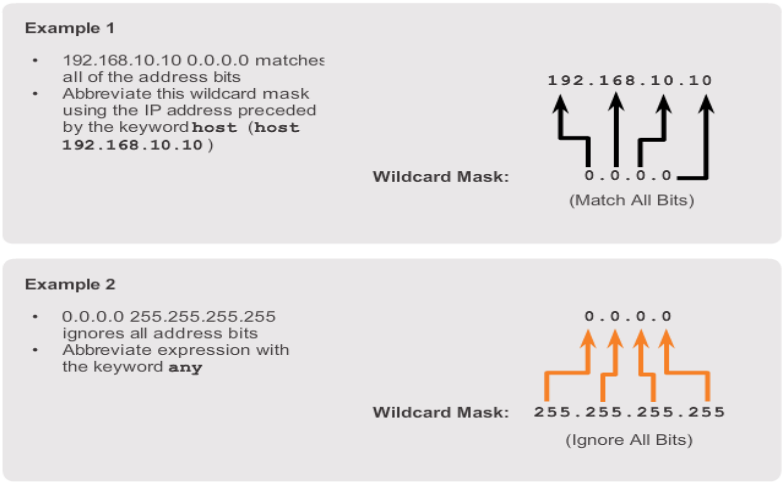
Example 2

	255.255.255.255
–	255.255.255.240
	000.000.000.015

Example 3

	255.255.255.255
–	255.255.252.000
	000.000.003.255

- كلمات مفتاحية بديلة عن ال (Wildcard Mask **Keywords**) Wildcard Mask



- <u>Examples</u> Wildcard Mask Keywords:

Example 1:

```
R1(config)#access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)#access-list 1 permit any
```

Example 2:

```
R1(config)#access-list 1 permit 192.168.10.10 0.0.0.0
R1(config)#access-list 1 permit host 192.168.10.10
```

➢ إعداد ال Standard ACL

- إنشاء Numbered Standard **ACL**

الصيغة الكاملة لتعليمة انشاء standard ACL كما يلي:

Router (config) # access-list *access-list-number* ***deny or permit*** **remark** *IP source Address [source-wildcard*]

لإزالة ACL، يتم استخدام أمر التكوين العام access-list **no**.

ملاحظة: يُستخدم الأمر remark للتوثيق وتجعل فهم قوائم الوصول أسهل كثيرًا.

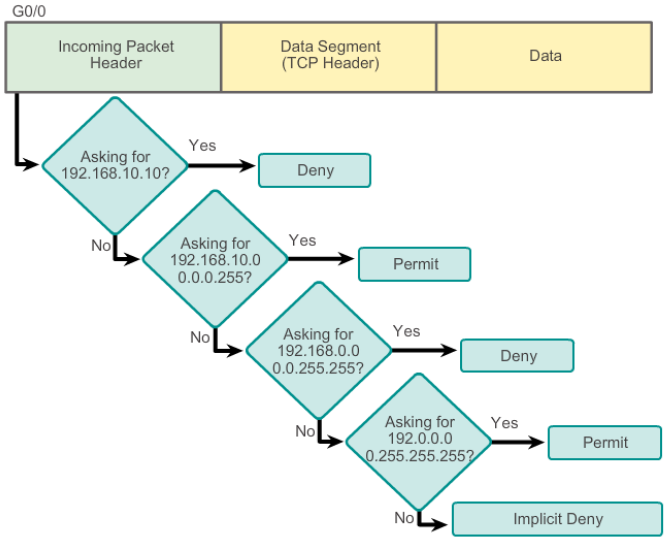
مثال:

access-list 2 deny host 192.168.10.10

access-list 2 permit 192.168.10.0 0.0.0.255

access-list 2 deny 192.168.0.0 0.0.255.255

access-list 2 permit 192.0.0.0 0.255.255.255



ملاحظة هامة:

ترتيب كتابة العبارات ضمن قائمة ما مُهم جداً.

تتم معالجة بيانات قائمة الوصول بالتتابع. لذلك، يعد الترتيب الذي يتم إدخال البيانات به أمرًا مهمًا.

```
R1(config)#access-list 3 deny 192.168.10.0 0.0.0.255
R1(config)#access-list 3 permit host 192.168.10.10
% Access rule can't be configured at higher sequence num as
it is part of the existing rule at sequence num 10
R1(config)#
```

ACL 3: Host statement conflicts with previous range statement.

- إنشاء **ACL** Standard Named

```
Router (config) # ip access-list access-list-name
Router (config) # [deny or permit or] ip-source-address wildcard-mask
Router (config) # remark some-description (خطوة اختيارية)
```

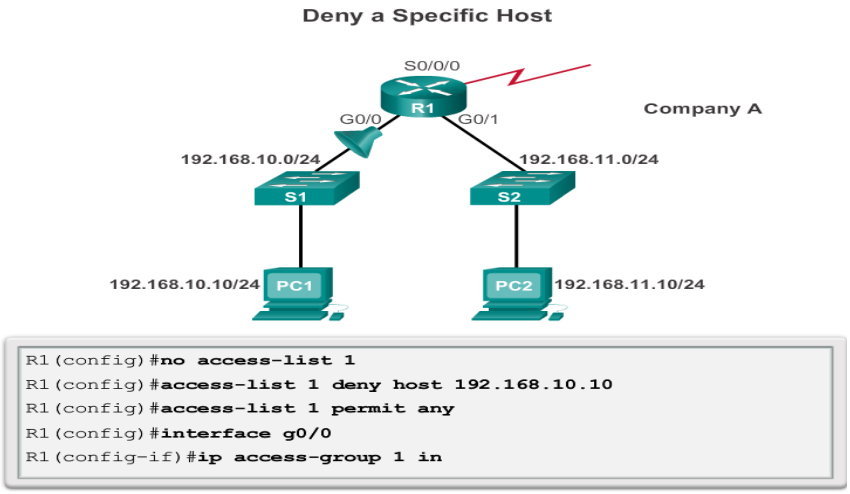
➢ تطبيق ال Standard ACLs على المنافذ

بعد إعداد ال standard ACL، يتم ربطها بمنفذ ما باستخدام التعليمة ip access-group:

```
Router (config-if) # ip access-group {access-list-number | access-list-name} { in | out }
```

لإزالة ACL من منفذ، أدخل أولاً الأمر no ip access-group ضمن المنفذ، ثم أدخل الأمر no access-list إذا أردت إزالة القائمة ACL بالكامل من وضع الإعدادات (Configuration Mode).

مثال: منع جهاز محدد من الخروج عبر الراوتر




```
R1(config)#no access-list 1
R1(config)#access-list 1 deny host 192.168.10.10
R1(config)#access-list 1 permit any
R1(config)#interface g0/0
R1(config-if)#ip access-group 1 in
```

- نعرض فيما يلي مثالين توضيحيين عن Numbered and Named Standard ACLs:

Example 1: Commenting a numbered ACL

```
R1(config)#access-list 1 remark Do not allow Guest workstation
through
R1(config)#access-list 1 deny host 192.168.10.10
R1(config)#access-list 1 remark Allow devices from all other
192.168.x.x subnets
R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 1 out
R1(config-if)#
```

Example 2: Commenting a named ACL

```
R1(config)#ip access-list standard NO_ACCESS
R1(config-std-nacl)#remark Do not allow access from Lab
workstation
R1(config-std-nacl)#deny host 192.168.11.10
R1(config-std-nacl)#remark Allow access from all other networks
R1(config-std-nacl)#permit any
R1(config-std-nacl)#interface G0/0
R1(config-if)#ip access-group NO_ACCESS out
R1(config-if)#
```

➢ Editing Standard Numbered ACLs

1- باستخدام مُحرر النصوص:

نستخدم محرر النصوص حتى ننسخ إليه عبارات القائمة ACL المُراد تعديلها ونعدّلها ونستخدم بعدها الأمر no لحذف القائمة القديمة وبعدها ننشئ أخرى جديدة وننسخ ضمنها العبارات الجديدة.

Editing Numbered ACLs Using a Text Editor

Configuration

```
R1(config)#access-list 1 deny host 192.168.10.99
R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
```

Step 1

```
R1#show running-config | include access-list 1
access-list 1 deny host 192.168.10.99
access-list 1 permit 192.168.0.0 0.0.255.255
```

Step 2

```
<Text editor>
access-list 1 deny host 192.168.10.10
access-list 1 permit 192.168.0.0 0.0.255.255
```

Step 3

```
R1#config t
Enter configuration commands, one per line.  End with
CNTL/Z.
R1(config)#no access-list 1
R1(config)#access-list 1 deny host 192.168.10.10
R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
```

Step 4

```
R1#show running-config | include access-list 1
access-list 1 deny host 192.168.10.10
access-list 1 permit 192.168.0.0 0.0.255.255
```

2- باستخدام الأرقام التسلسلية:

Editing Numbered ACLs Using Sequence Numbers

Configuration

```
R1(config)#access-list 1 deny host 192.168.10.99
R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
```

Step 1

```
R1#show access-lists 1
Standard IP access list 1
    10 deny   192.168.10.99
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
R1#
```

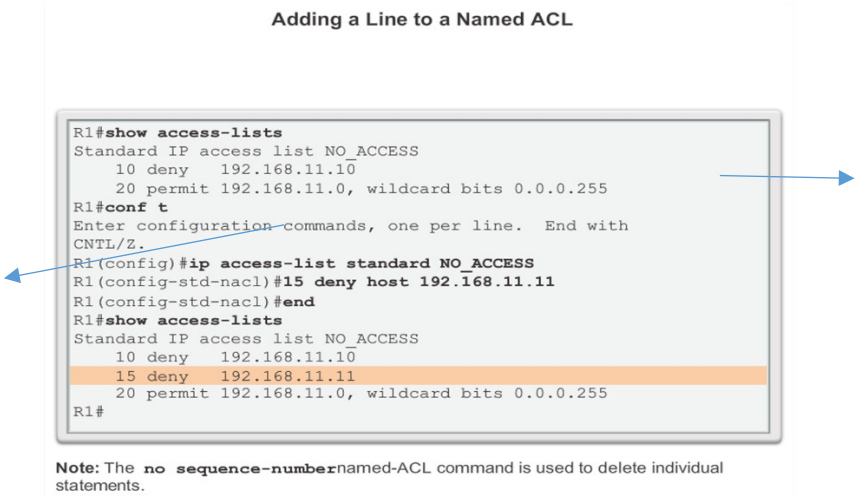
Step 2

```
R1#conf t
R1(config)#ip access-list standard 1
R1(config-std-nacl)#no 10
R1(config-std-nacl)#10 deny host 192.168.10.10
R1(config-std-nacl)#end
R1#
```

Step 3

```
R1#show access-lists
Standard IP access list 1
    10 deny   192.168.10.10
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
R1#
```

3- إضافة وحشر سطر جديد ضمن قائمة:



➢ التحقّق من ال ACLs

يتم ذلك باستخدام التعليمات التالية:

```
R1# show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30
<output omitted>
  Outgoing access list is 1
  Inbound  access list is not set
<output omitted>

R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted>
  Outgoing access list is NO_ACCESS
  Inbound  access list is not set
<output omitted>
```

```
R1# show access-lists
Standard IP access list 1
    10 deny   192.168.10.10
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny   192.168.11.11
    10 deny   192.168.11.10
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

➢ عرض بعض الاحصائيات (ACL Statistics)

لدينا ضمن هذه الاحصائيات عدد التطابقات (matches) التي مرّت على كل عبارة ضمن القوائم:

```
R1#show access-lists
Standard IP access list 1
    10 deny   192.168.10.10 (4 match(es))
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny   192.168.11.11
    10 deny   192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Output after pinging PC3 from PC1.

Matches have been incremented.

```
R1#show access-lists
Standard IP access list 1
    10 deny   192.168.10.10 (8 match(es))
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny   192.168.11.11
    10 deny   192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

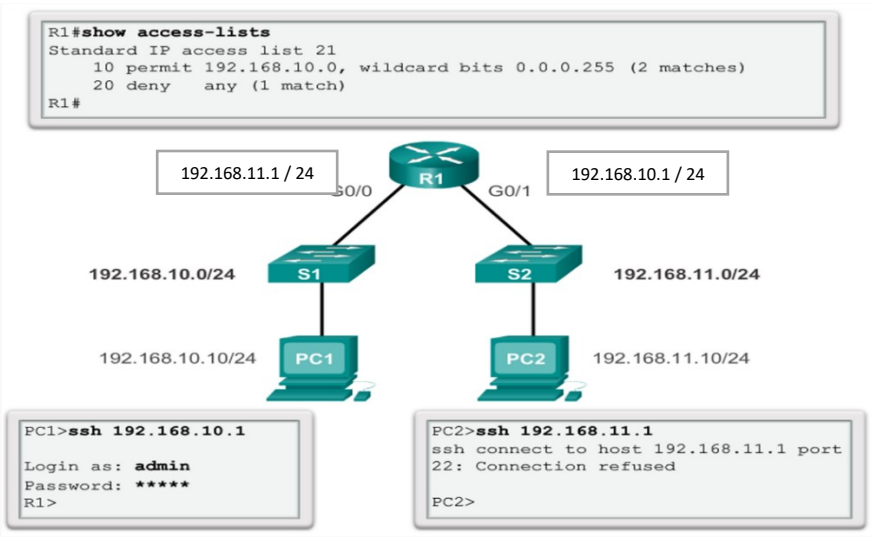
➢ إعداد Standard ACL لتأمين المنفذ VTY (securing Telnet & SSH)

تعتبر فلترة حركة مرور Telnet أو SSH عادةً من وظيفة ال ACL المُوسّعة لأنه بإمكانها الفلترة حسب بروتوكول ما.

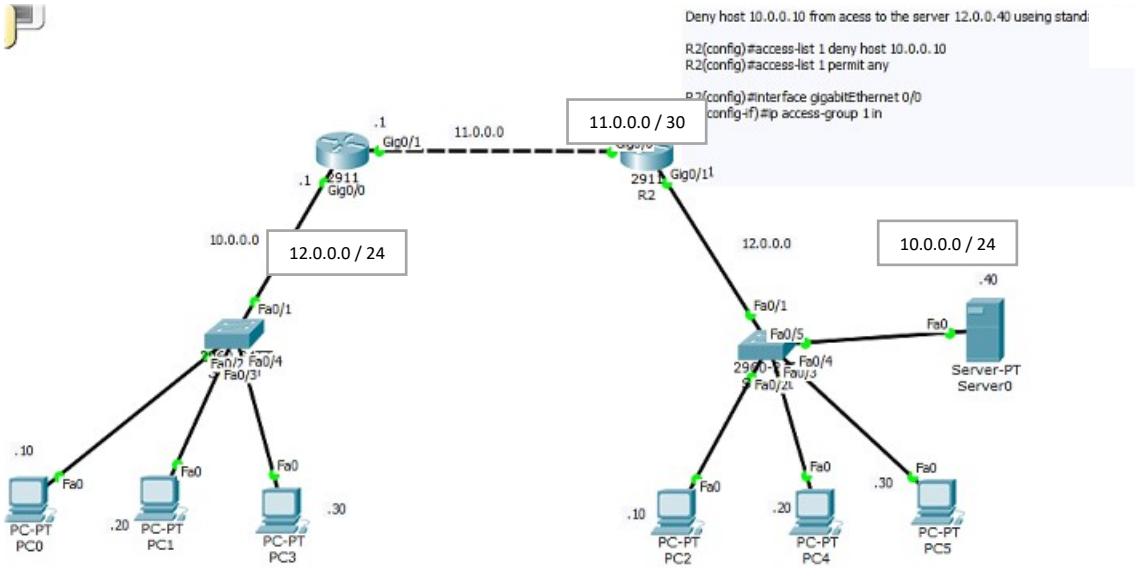
ومع ذلك، نظرًا لاستخدام التعليمة **access-class** لفلترة جلسات Telnet / SSH الواردة أو الصادرة حسب عنوان المصدر، يمكن استخدام قائمة ACL قياسية (Standard ACL).

```
Router (config) # line vty 0 4
Router (config-line) # access-class access-list-number {in [ vrf-also ] | out }
```

```
R1#show access-lists
Standard IP access list 21
    10 permit 192.168.10.0, wildcard bits 0.0.0.255 (2 matches)
    20 deny   any (1 match)
R1#
```



مثال (simple-ACL-standard):



➢ قوائم التحكّم بالوصول المُوسّعة (Extended ACLs)

قلنا إنه يمكننا هنا فلترة حركة البيانات بتحديد عنوان المصدر والهدف وتحديد البروتوكول ورقم المنفذ أو اسمه كالتالي:

Using Port Numbers

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

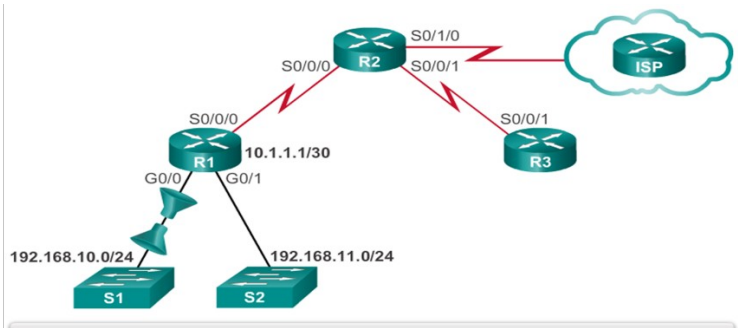
Using Keywords

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

الخطوات المُتبعة لإعداد قوائم التحكم في الوصول الموسّعة هي نفسها الخاصة بقوائم التحكم في الوصول القياسية حيث يتم إعداد قائمة التحكم بالوصول الموسّعة أولاً، ثم يتم تنشيطها على منفذ ما.

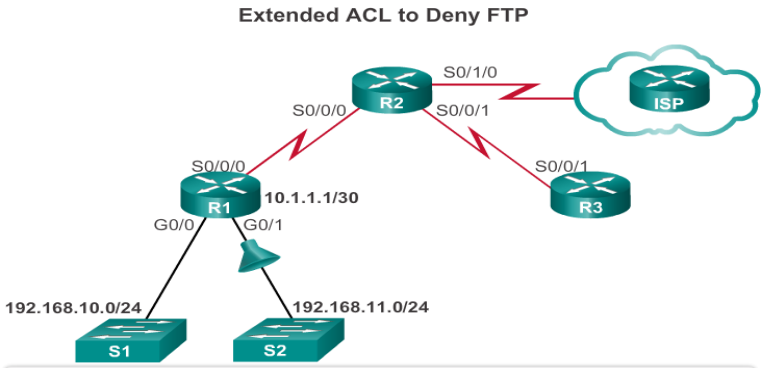
➢ تطبيق ال Extended ACLs على المنافذ

نُوضّح ذلك كالتالي:




```
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)#access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)#interface g0/0
R1(config-if)#ip access-group 103 in
R1(config-if)#ip access-group 104 out
```

مثال 1 (منع بيانات ال FTP):




```
R1(config)#access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0
0.0.0.255 eq ftp
R1(config)#access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0
0.0.0.255 eq ftp-data
R1(config)#access-list 101 permit ip any any
R1(config)#interface g0/1
R1(config-if)#ip access-group 101 in
```

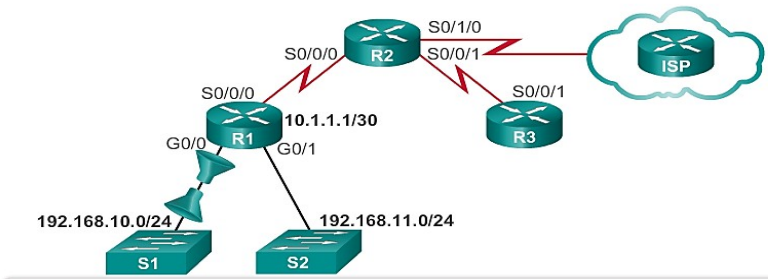
مثال 2 (إنشاء Named Extended ACLs):

نرى في المثال أدناه قائمتين الأولى باسم SURFING للسماح للشبكة الداخلية بالخروج إلى الانترنت (Surfing the net) والثانية باسم BROWSING للسماح لها باستعراض محتوى الويب الذي يتم طلبه فقط (**established**).

ملاحظة:

تمنع الكلمة **established** كل حركة البيانات التي تم إنشاؤها بواسطة TCP القادمة من الإنترنت باستثناء أي رد على حركة مرور (TCP reply) مُرتبطة بحركة مرور TCP مُؤسّسة وتم البدء بها من داخل الشبكة.

Creating Named Extended ACLs

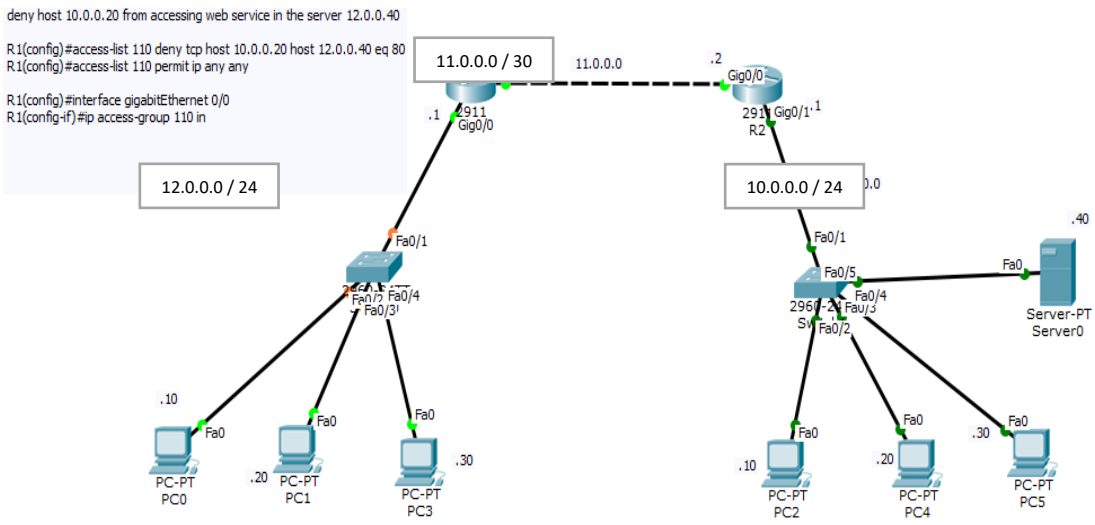



```
R1(config)#ip access-list extended SURFING
R1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)#exit
R1(config)#ip access-list extended BROWSING
R1(config-ext-nacl)#permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)#exit
R1(config)#interface g0/0
R1(config-if)#ip access-group SURFING in
R1(config-if)#ip access-group BROWSING out
```

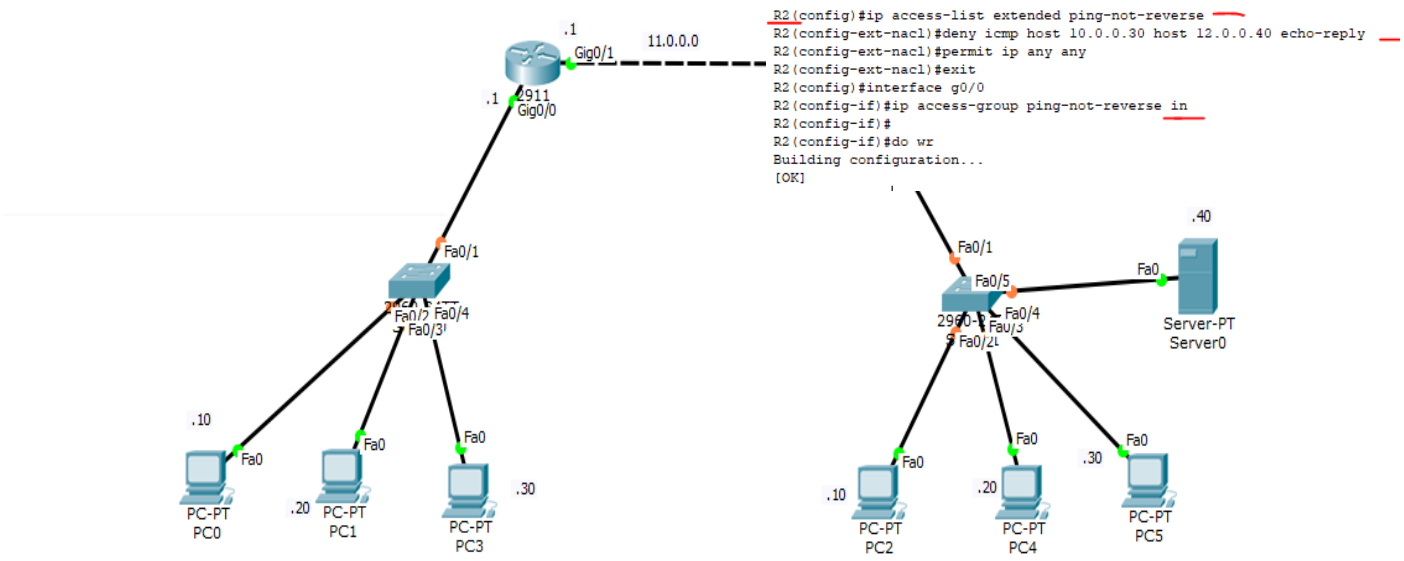
ويتم التحقّق أيضاً كالتالي:

```
R1#show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
R1#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted for brevity>
  Outgoing access list is BROWSING
  Inbound  access list is SURFING
<output omitted for brevity>
```

مثال 3:



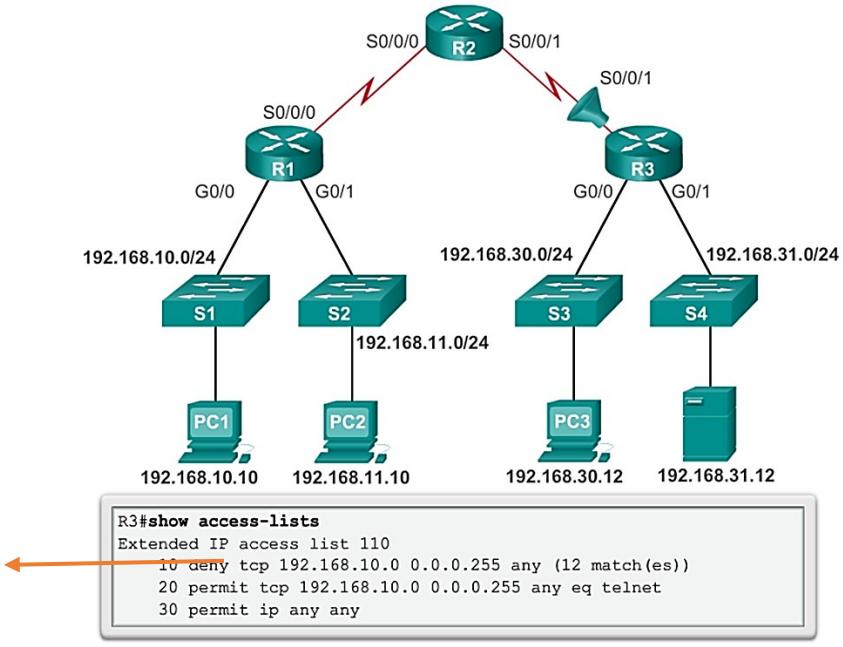
مثال 4:



- **بعض الأمثلة عن استكشاف أخطاء ال ACLs**

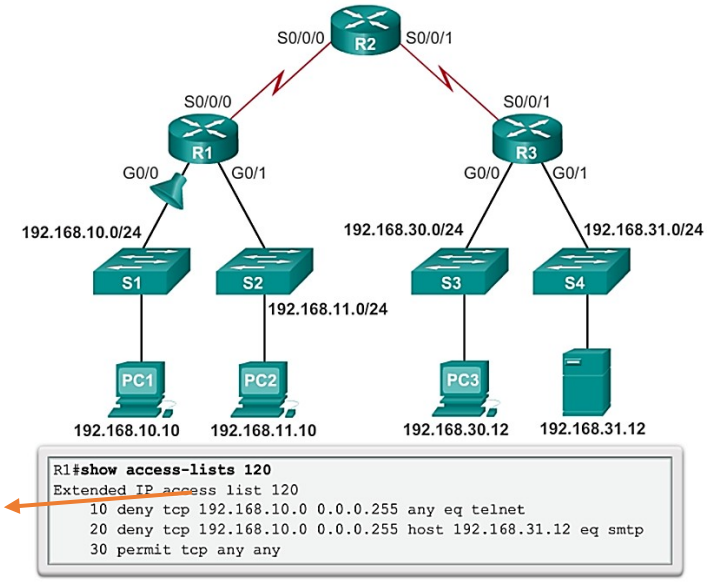
✓ Troubleshooting Common ACL Errors - Example 1

Host 192.168.10.10 has no connectivity with 192.168.30.12.



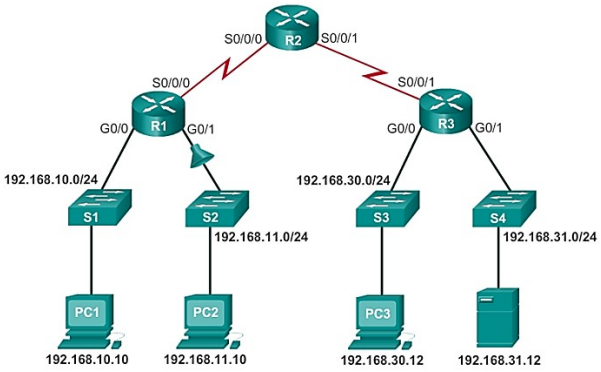
✓ Troubleshooting Common ACL Errors - Example 2

The 192.168.10.0 /24 network cannot use TFTP to connect to the 192.168.30.0 /24 network.



✓ Troubleshooting Common ACL Errors - Example 3

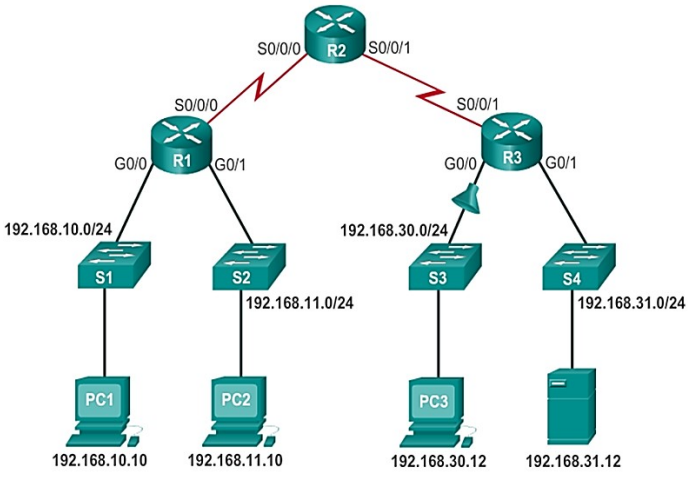
The 192.168.11.0 /24 network can use Telnet to connect to 192.168.30.0 /24, but according to company policy, this connection should not be allowed.




```
R1#show access-lists 130
Extended IP access list 130
    10 deny tcp any eq telnet any
    20 deny tcp 192.168.11.0 0.0.0.255 host 192.168.31.12 eq smtp
    30 permit tcp any any (12 match(es))
```

✓ Troubleshooting Common ACL Errors - Example 4

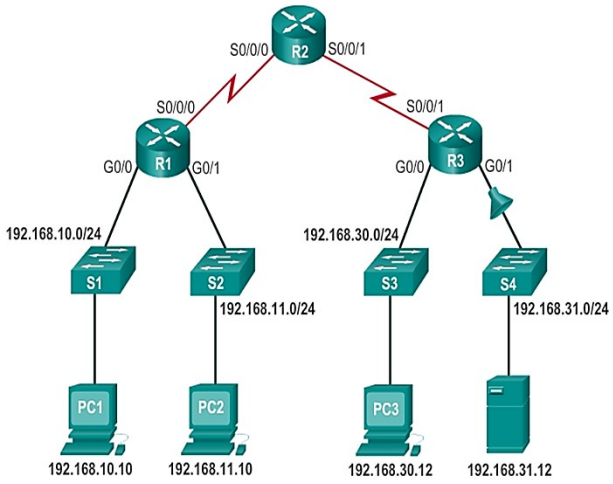
Host 192.168.30.12 is able to Telnet to connect to 192.168.31.12, but company policy states that this connection should not be allowed.




```
R3#show access-lists 140
Extended IP access list 140
    10 deny tcp host 192.168.30.1 any eq telnet
    20 permit ip any any (5 match(es))
```

✓ Troubleshooting Common ACL Errors - Example 5

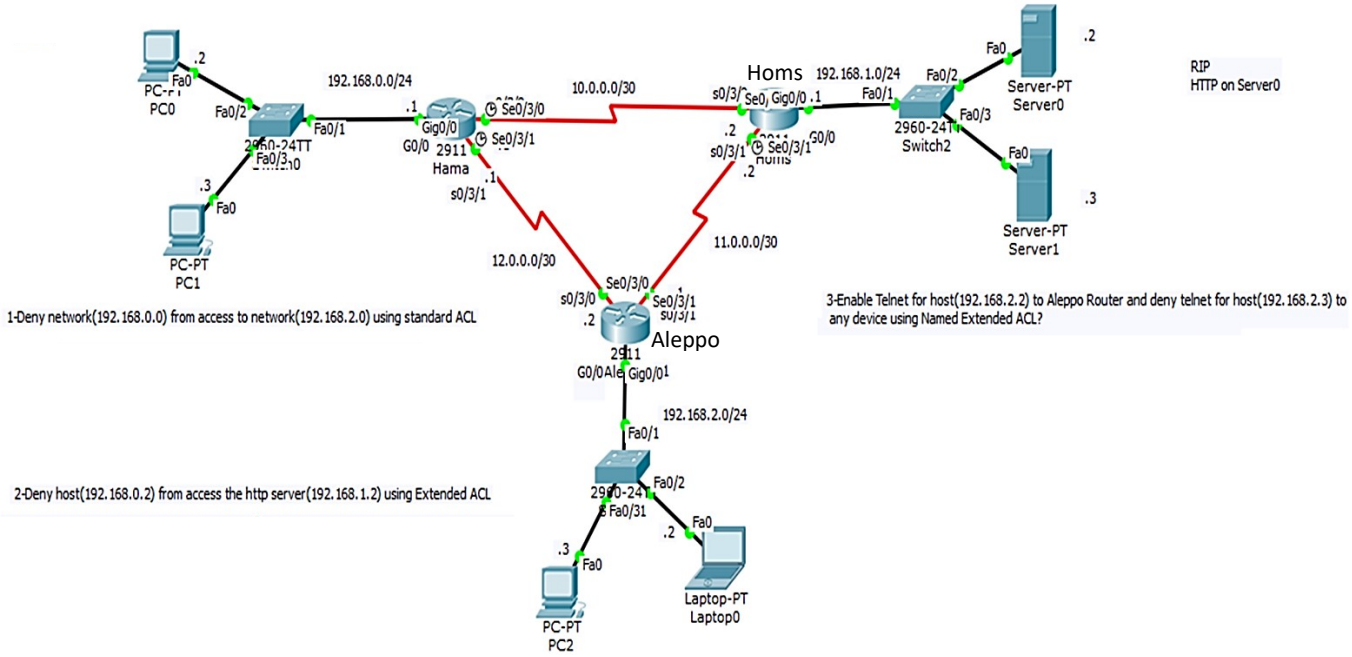
Host 192.168.30.12 can use Telnet to connect to 192.168.31.12, but according to the security policy, this connection should not be allowed.



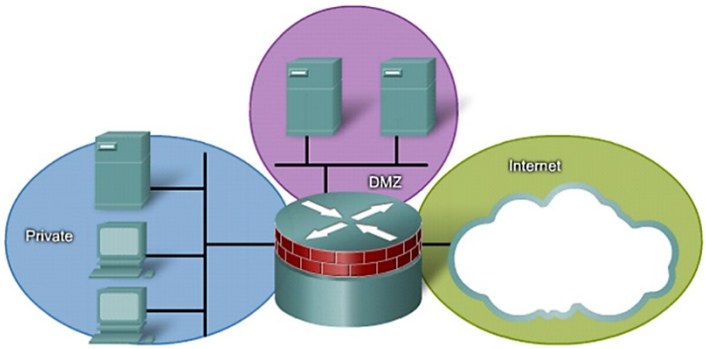

```
R2#show access-lists 150
Extended IP access list 150
    10 deny tcp any host 192.168.31.12 eq telnet
    20 permit ip any any
```

Homework: ☺

Implementing and configuring the following lab…



Zone-Based Policy Firewall (ZPF)



تستخدم قوائم التحكم بالوصول (ACL) التقليدية نموذج إعداد قائم على الواجهة، حيث سيتم تطبيق سياسة فحص الحالة على الواجهة. تتلقى جميع حركات المرور التي تمر عبر تلك الواجهة نفس سياسة الفحص.

بينما في جدار حماية السياسة المُعتمد على المنطقة (المعروف أيضًا باسم Zone-Policy Firewall، أو **ZFW**)، يتم تعيين الواجهات التي يُراد معاملتها بطريقة أمنية مماثلة إلى مناطق ثم يتم تطبيق سياسة الفحص على حركة المرور التي تنتقل بين هذه المناطق.

يمكننا إسناد واجهة ما لمنطقة أمان **واحدة فقط**.

➢ الأفعال الأساسية ضمن ZPF (إجراءات الفحص ضمن ZPF)

توجد ثلاثة أفعال أساسية:

1. **Inspect:** يسمح تلقائيًا بحركة العودة بين منطقتين (ذهاب وإياب).
2. **Pass:** مشابه لعبارة السماح permit الموجودة في قائمة التحكم بالوصول (ACL).
   لا يتتبع حالة الاتصالات أو الجلسات داخل حركة المرور.
   يسمح التمرير لحركة المرور في اتجاه واحد فقط (من منطقة إلى أُخرى باتجاه واحد).
   هنا يجب تطبيق سياسة مقابلة (تحوي فعل Pass اخر) للسماح بحركة العودة بالمرور في الاتجاه المعاكس.
3. **Drop:** مماثل لعبارة الرفض deny الموجودة في قائمة التحكم بالوصول (ACL).
   كما يتوفّر خيار التسجيل Log لتسجيل الرُزم المرفوضة.

➢ بعض القواعد لتطبيق Zone-Based Policy Firewall

1. يجب تعريف المنطقة zone قبل أن يتم إسناد الواجهات إليها.
2. يمكن إسناد أي واجهة (منفذ) إلى منطقة واحدة فقط.
3. يتم بشكل ضمني السماح بالمرور بين الواجهات الواقعة في نفس المنطقة.
4. حتى يتم السماح للمرور من وإلى واجهة من منطقة ما يجب تعريف سياسة تسمح أو تفحص المرور بين هذه المنطقة أو أي منطقة أخرى.

5. لا يمكن أن تمر الرزم بين اي واجهة من منطقة وواجهة اخرى لا تنتمي الى منطقة.

Note: Pass, inspect, and drop actions can only be applied between two zones.

➢ خطوات إعداد ال ZPF

1. تعريف المناطق.

2. تحديد class-maps التي تصف حركة المرور التي يجب أن يتم تطبيق سياسة عليها أثناء عبورها بين منطقتين ضمن zone-pair معيّنة.

3. تعريف policy-maps لتطبيق فعل على حركة المرور المُحددة ضمن ال class-maps السابق ذكرها.

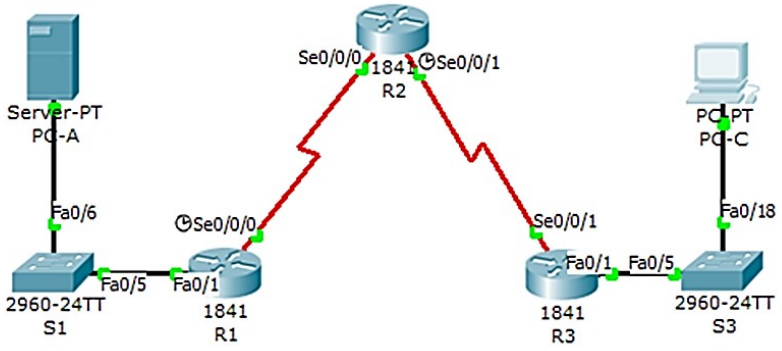
4. تحديد zone-pairs يحوي كل منطقتين مُراد تطبيق حماية بينهما.

5. تطبيق policy-maps على ال zone-pairs.

6. إسناد المنافذ للمناطق.

➢ ZPF Example 1

قم بإعداد ZPF أساسي على جهاز توجيه الحافة R3 الذي يسمح للمضيفين (الأجهزة) الداخليين بالوصول إلى الموارد الخارجية ويمنع المضيفين الخارجيين من الوصول إلى الموارد الداخلية.



وهنا جدول يُوضّح العناوين المستخدمة ضمن الطوبولوجيا السابقة:

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

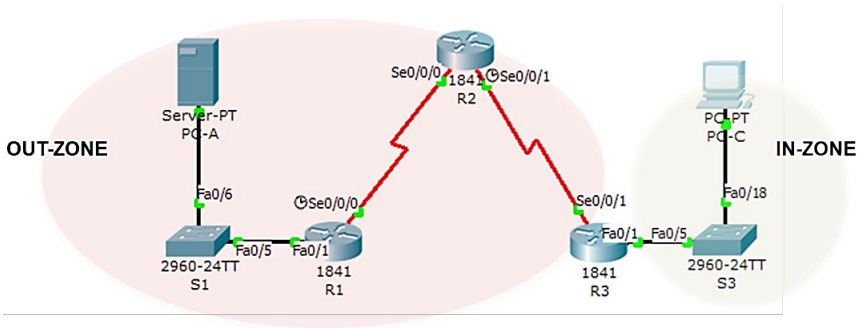
الحل:

Task 1: إنشاء المناطق Firewall Zones على جهاز التوجيه R3

الخطوة 1:

استخدم التعليمة zone security لإنشاء منطقة ولتكن باسم منطقة *IN-ZONE* ومنطقة باسم *OUT-ZONE*.

```
R3 (config) # zone security IN-ZONE
R3 (config-sec-zone) # zone security OUT-ZONE
R3 (config-sec-zone) # exit
```



Task 2:

تحديد فئة لحركة المرور وقائمة الوصول ACL:

أي إنشاء class map لمطابقة كل حركة المرور التي نريد السماح بها من المنطقة الموثوق بها إلى المنطقة الخارجية.

الخطوة 1:

إنشاء قائمة تحكم في الوصول (ACL) تُحدد حركة المرور الداخلية (*الشبكة الداخلية*).

```
R3 (config) # access-list 101 permit ip 192.168.3.0 0.0.0.255 any
```

الخطوة 2:

إنشاء class map تُشير إلى قائمة ال ACL الخاصة بحركة البيانات الداخلية.

نستخدم التعليمة class map type inspect مع الخيار match-all لإنشاء class map ولتكن باسم *IN-NET-CLASS-MAP*، وبعدها نستخدم التعليمة match access-group لمطابقة القائمة 101 التي أنشأناها في مثالنا.

```
R3 (config) # class-map type inspect match-all IN-NET-CLASS-MAP
R3 (config-cmap) # match access-group 101
R3 (config-cmap) # exit
```

Task 3: تحديد سياسات جدار الحماية (Specify Firewall Policies)

الخطوة 1:

إنشاء policy map لتحديد ما يجب فعله مع حركة البيانات المتطابقة، وهنا نستخدم التعليمة policy-map type inspect ونُنشئ policy map ولتكن باسم *IN-2-OUT-PMAP*.

```
R3 (config) # policy-map type inspect IN-2-OUT-PMAP
R3 (config-pmap) #
```

الخطوة 2:

تحديد نوع الفعل واسم ال class map التي تُشير إلى قائمة ال ACL الخاصة بحركة البيانات الداخلية:

```
R3 (config-pmap) # class type inspect IN-NET-CLASS-MAP
R3 (config-pmap-c) #
```

الخطوة 3:

تحديد إجراء الفحص (الفعل) لهذه ال policy map.

```
R3 (config-pmap-c) # inspect
% No specific protocol configured in class IN-NET-CLASS-MAP for
inspection. All protocols will be inspected.
R3 (config-pmap-c) # exit
R3 (config-pmap) # exit
```

Task 4: تطبيق سياسات الجدار الناري (Apply Firewall Policies)

الخطوة 1: إنشاء زوج من المناطق.

نستخدم التعليمة zone-pair security حتى نُنشئ زوج من المناطق وليكن باسم *IN-2-OUT-ZPAIR* ونحدّد المنطقتين المصدر والوجهة واللتين تم إنشاؤها في المهمة **Task 1**.

```
R3 (config) # zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
R3 (config-sec-zone-pair) #
```

الخطوة 2: تحديد خريطة السياسة (ال policy map) للتعامل مع حركة المرور بين المنطقتين.

نقوم بربط خريطة السياسة والإجراءات المرتبطة بها بزوج المنطقة باستخدام التعليمة service-policy type inspect وتحديد والإشارة إلى ال policy map التي تم إنشاؤها مسبقًا وهي *IN-2-OUT-PMAP*.

```
R3 (config-sec-zone-pair) # service-policy type inspect IN-2-OUT-PMAP
R3 (config-sec-zone-pair) # exit
R3 (config) #
```

وبعدها نقوم بإسناد الواجهات لمناطق الأمان المناسبة.

نستخدم التعليمة zone-member security في وضع إعداد الواجهة (interface config mode) لإسناد المنفذ (الواجهة) Fa0 / 1 إلى *IN-ZONE* والمنفذ S0 / 0/1 إلى *OUT-ZONE*.

```
R3 (config) # interface fa0/1
R3 (config-if) # zone-member security IN-ZONE
R3 (config-if) # exit
```

```
zone security IN-ZONE
zone security OUT-ZONE
exit
access-list 101 permit ip 192.168.3.0 0.0.0.255 any
class-map type inspect match-all IN-NET-CLASS-MAP
match access-group 101
exit
policy-map type inspect IN-2-OUT-PMAP
class type inspect IN-NET-CLASS-MAP
inspect
exit
exit
```

1

2

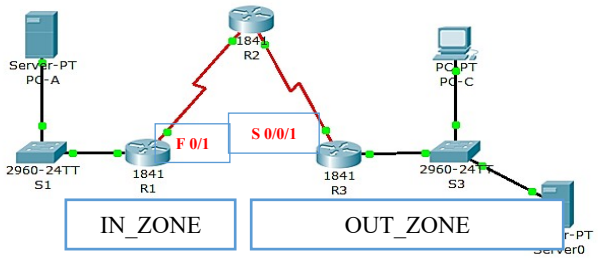
```
zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
service-policy type inspect IN-2-OUT-PMAP
exit
interface fa0/1
zone-member security IN-ZONE
exit
interface s0/0/1
zone-member security OUT-ZONE
exit
```

- نتحقق أخيراً (Test Firewall Functionality from *IN-ZONE* to *OUT-ZONE*):

يجب أن يكون الاتصال وطلب صفحات الويب مسموحاً من الشبكة الداخلية IN-ZONE إلى الخارجية وممنوعاً بالاتجاه المُعاكس.

➢ ZPF Example 2

قم بإعداد ZPF أساسي على جهاز توجيه الحافة R3 الذي يسمح للمضيفين الداخليين بالوصول عبر البروتوكولين ICMP و TCP إلى الموارد الخارجية ويمنع المضيفين الخارجيين من الوصول إلى الموارد الداخلية.



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

سنستعرض فيما يلي جميع خطوات الحل:

1

```
zone security IN-ZONE
zone security OUT-ZONE
exit
class-map type inspect match-any IN-NET-CLASS-MAP
match protocol icmp
match protocol tcp
exit
policy-map type inspect IN-2-OUT-PMAP
class type inspect IN-NET-CLASS-MAP
inspect
exit
exit
```

2

```
zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
service-policy type inspect IN-2-OUT-PMAP
exit
interface fa0/1
zone-member security IN-ZONE
exit
interface s0/0/1
zone-member security OUT-ZONE
exit
```

ملاحظة عن ال Class-maps:

يمكن أن تطبق عمليات **match-any** أو **match-all** لتحديد كيفية تطبيق معايير المطابقة. إذا تم تحديد match-any، يجب أن تفي حركة البيانات بمعيار واحد فقط من معايير المطابقة في ال class-map. إذا تم تحديد match-all، يجب أن تتطابق حركة البيانات مع جميع معايير ال class-map.

نعرض هنا أخيراً توضيح لطريقة كتابة هذه التعليمات ضمن موجّه الأوامر (CLI) على الراوتر R3:

```
Router(config)#zone security IN-ZONE
Router(config-sec-zone)#zone security OUT-ZONE
Router(config-sec-zone)#exit
Router(config)#class-map type inspect match-any IN-NET-CLASS-MAP
Router(config-cmap)#match protocol icmp
Router(config-cmap)#match protocol tcp
Router(config-cmap)#policy-map type inspect IN-2-OUT-PMAP
Router(config-pmap)#class type inspect IN-NET-CLASS-MAP
Router(config-pmap-c)#inspect
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-
ZONE
Router(config-sec-zone-pair)#service-policy type inspect IN-2-OUT-PMAP
Router(config-sec-zone-pair)#exit
Router(config)#interface fa0/1
Router(config-if)#zone-member security IN-ZONE
Router(config-if)#exit
Router(config)#interface s0/0/1
Router(config-if)#zone-member security OUT-ZONE
Router(config-if)#exit
Router(config)#
```

المراجع

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

???Any Questions