

# بجمل Cisco VPN 3000 زكرم نيوكت RADIUS حشرم نيوعت و تاحشرم لادختساب

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الرسم التخطيطي للشبكة](#)
- [الاصطلاحات](#)
- [تكوين VPN 3000](#)
- [عوامل تصفية نفق VPN من LAN إلى LAN](#)
- [تكوين VPN 3000 - تعيين مرشح RADIUS](#)
- [تكوين خادم CSNT - تعيين مرشح RADIUS](#)
- [تصحيح الأخطاء - تعيين مرشح RADIUS](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

## المقدمة

في نموذج التكوين هذا، نريد استخدام عوامل التصفية للسماح للمستخدم بالوصول إلى خادم واحد فقط (10.1.1.2) داخل الشبكة ومنع الوصول إلى جميع الموارد الأخرى. يمكن إعداد مركز Cisco VPN 3000 للتحكم في بروتوكول IPsec، وبروتوكول الاتصال النفقي من نقطة إلى نقطة (PPTP)، ووصول عميل L2TP إلى موارد الشبكة باستخدام عوامل التصفية. تتكون عوامل التصفية من القواعد، والتي تكون مماثلة لقوائم الوصول على الموجه. إذا تم تكوين موجه ل:

```
access-list 101 permit ip any host 10.1.1.2  
access-list 101 deny ip any any
```

سيكون مكافئ مركز الشبكة الخاصة الظاهرية (VPN) هو إعداد مرشح باستخدام القواعد.

القاعدة الأولى لترخيص الشبكة الخاصة الظاهرية (VPN) هي `allowed_server_rule`، والتي تعادل الأمر `allowed ip 10.1.1.2 any host` الخاص بالموجه. تمثل قاعدة مركز الشبكة الخاصة الظاهرية (VPN) الثانية لدينا في `deny_server_rule` وهو ما يعادل أمر `deny ip any` للموجه.

إن عامل تصفية مركز VPN الخاص بنا هو `filter_with_2_rules`، وهو ما يعادل قائمة وصول الموجه 101، إنه يستخدم `allow_server_rule` و `deny_server_rule` (بهذا الترتيب). يفترض أنه يمكن للعملاء الاتصال بشكل صحيح قبل إضافة عوامل التصفية؛ فهم يتلقون عناوين IP الخاصة بهم من تجمع على مركز الشبكة الخاصة الظاهرية (VPN).

ارجع إلى [PIX/ASA 7.x ASDM: تقييد الوصول إلى الشبكة الخاصة بمستخدمي VPN للوصول عن بعد](#) لمعرفة المزيد حول السيناريو الذي يقوم فيه PIX/ASA 7.x بحظر الوصول من مستخدمي VPN.

## المتطلبات الأساسية

### المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

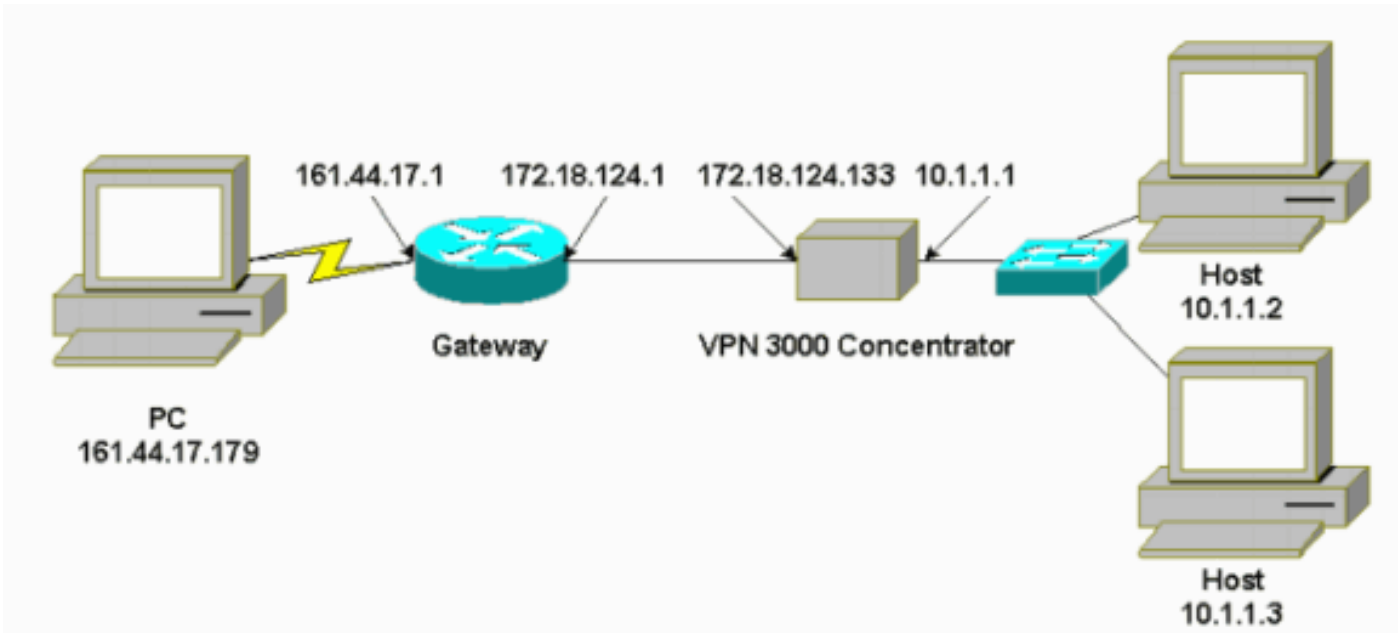
### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار D.2.5.2 من Cisco VPN 3000 Concentrator.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

### الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



### الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

## تكوين VPN 3000

أتمت هذا steps in order to شكلت ال VPN 3000 مركز.

1. أخترت تشكيل <إدارة سياسة> حركة مرور إدارة <قاعدة> إضافة وتحديد أول قاعدة مركز VPN يدعو enable\_server\_rule مع هذه الإعدادات: الإتياء - الوارد العمل — إلى الأمام عنوان المصدر - 255.255.255.255 عنوان الوجهة- 10.1.1.2 قناع حرف البدل- 0.0.0.0

Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-30608] - Microsoft Internet Explorer

File Edit View Go Favorites Help

Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print

Address http://172.18.124.133/access.html

VPN 3000 Concentrator Series Manager Main Help Support Logout

Logged in: admin Configuration Administration Monitoring

Configuration | Policy Management | Traffic Management | Rules | Add

Configure and add a new filter rule.

Rule Name  Name of this filter rule. The name must be unique.

Direction  Select the data direction to which this rule applies.

Action  Specify the action to take when this filter rule applies.

Protocol  Select the protocol to which this rule applies. For Other protocols, enter the protocol number.

or Other  Select whether this rule should apply to an established TCP connection.

TCP Connection

Source Address

Network List  Specify the source network address list or the IP address and wildcard mask that this rule checks.

IP Address  Note: Enter a **wildcard mask**, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

Wildcard-mask

Destination Address

Network List  Specify the destination network address list or the IP address and wildcard mask that this rule checks.

IP Address  Note: Enter a **wildcard mask**, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

Wildcard-mask

TCP/UDP Source Port

Port  For TCP/UDP, specify the source port ranges that this rule checks. For a single port number, use the same number for the start and end.

or Range  to

Configuration Administration Monitoring Refresh

CISCO SYSTEMS

Internet zone

2. في نفس المنطقة، قم بتعريف القاعدة الثانية لتركيز شبكات VPN التي تسمى `deny_server_rule` باستخدام الإعدادات الافتراضية التالية: الإتجاه - الواردالإجراء - الإسقاطعناوين المصدر والوجهة لأي شيء (255.255.255.255):

Configuration | Policy Management | Traffic Management | Rules | Modify

Modify a filter rule.

Rule Name  Name of this filter rule. The name must be unique.

Direction  Select the data direction to which this rule applies.

Action  Specify the action to take when this filter rule applies.

3. أختار تكوين < إدارة السياسة > إدارة حركة مرور البيانات < عوامل التصفية وأضف عامل تصفية filter\_with\_2\_rules الخاص بك.

Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-30608] - Microsoft Internet Explorer

File Edit View Go Favorites Help

Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print

Address http://172.18.124.133/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Log

Configuration | Administration | Monitor

Configuration | Policy Management | Traffic Management | Filters | Add

Configure and add a new filter.

**Filter Name**  Name of the filter you are adding. The name must be unique.

**Default Action**  Select the default action to take when no rules on this filter apply.

**Source Routing**  Check to have this filter allow IP source routed packets to pass.

**Fragments**  Check to have this filter allow fragmented IP packets to pass.

**Description**

CISCO SYSTEMS

Internet zone

4. قم بإضافة القاعدتين ل  
:filter\_with\_2\_rules

Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-30608] - Microsoft Internet Explorer

File Edit View Go Favorites Help

Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print

Address http://172.18.124.133/access.html Links

VPN 3000 Concentrator Series Manager Main Help Support Logout

Logged in: admin Configuration Administration Monitoring

Save Needed

Configuration
 

- Interfaces
- System
- User Management
- Policy Management
  - Access Hours
  - Traffic Management
    - Network Lists
    - Rules
    - SA's
    - Filters
  - NAT

Administration

Monitoring

Add, remove, prioritize, and configure rules that apply to a filter.

**Filter Name:** filter\_with\_2\_rules

Select an **Available Rule** and click **Add** to apply it to this filter.

Select a **Current Rule in Filter** and click **Remove**, **Move Up**, **Move Down**, or **Assign SA to Rule** as appropriate.

Select an **Available Rule**, then select a **Current Rule in Filter**, and click **Insert Above** to add the available rule above the current rule.

Current Rules in Filter	Actions	Available Rules
permit_server_rule (forward/in) deny_server_rule (drop/in)	<< Add << Insert Above Remove >> Move Up Move Down Assign SA to Rule Done	GRE In (forward/in) GRE Out (forward/out) IPSEC-ESP In (forward/in) IKE In (forward/in) IKE Out (forward/out) PPTP In (forward/in) PPTP Out (forward/out) L2TP In (forward/in) L2TP Out (forward/out) ICMP In (forward/in) ICMP Out (forward/out) RIP In (forward/in)

CISCO SYSTEMS

5. أختار تكوين < إدارة المستخدم > مجموعات وطبق المرشح على المجموعة:

Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-3060B] - Microsoft Internet Explorer

File Edit View Go Favorites Help

Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print

Address http://172.18.124.133/access.html

VPN 3000 Concentrator Series Manager Main | Help | Support | Logout

Logged in: admin Configuration | Administration | Monitoring

Configuration | User Management | Groups | Modify servergroup

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

General Parameters			
Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this group.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whether to allow alphabetic-only passwords.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this group.
Filter	filter_with_2_rules	<input type="checkbox"/>	Enter the filter assigned to this group.
Primary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the primary DNS server.
		<input type="checkbox"/>	Enter the IP address of the

## عوامل تصفية نفق VPN من LAN إلى LAN

من رمز مركز VPN 3.6 والإصدارات الأحدث، يمكنك تصفية حركة مرور البيانات لكل نفق من شبكة LAN إلى شبكة IPsec لشبكة VPN. على سبيل المثال، إذا قمت بإنشاء نفق من شبكة LAN إلى مركز VPN آخر بعنوان 172.16.1.1، وتريد السماح للمضيف بوصول 10.1.1.2 إلى النفق أثناء رفض جميع حركات المرور الأخرى، فيمكنك تطبيق filter\_with\_2\_rules عند إختيار التكوين < النظام > بروتوكولات أنفاق < IPsec > إلى شبكة VPN < تعديل وتحديد عامل التصفية with\_2\_rules تحت عاملالتصفية.



## VPN 3000 Concentrator Series Manager

### Configuration

- Interfaces
- System
  - Servers
  - Address Management
  - Tunneling Protocols
    - PPTP
    - L2TP
    - IPSec
      - LAN-to-LAN
      - IKE Proposals
      - NAT Transparency
  - IP Routing
  - Management Protocols
  - Events
  - General
  - Client Update
  - Load Balancing
- User Management
- Policy Management
- Administration
- Monitoring

### Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN | Modify

Modify an IPSec LAN-to-LAN connection.

Name	<input type="text" value="Test Lan to Lan"/>
Interface	<input type="text" value="Ethernet 2 (Public) (172.18.124.133)"/>
Peer	<input type="text" value="172.16.1.1"/>
Digital Certificate	<input type="text" value="None (Use Preshared Keys)"/>
Certificate	<input type="radio"/> Entire certificate chain
Transmission	<input checked="" type="radio"/> Identity certificate only
Preshared Key	<input type="text" value="cisco123"/>
Authentication	<input type="text" value="ESP/MD5/HMAC-128"/>
Encryption	<input type="text" value="3DES-168"/>
IKE Proposal	<input type="text" value="IKE-3DES-MD5"/>
Filter	<input type="text" value="filter_with_2_rules"/>
IPSec NAT-T	<input type="checkbox"/>

## [تكوين VPN 3000 - تعيين مرشح RADIUS](#)

كما من الممكن تعريف عامل تصفية في مركز الشبكة الخاصة الظاهرية (VPN) ثم تمرير رقم عامل التصفية من خادم RADIUS (في شروط RADIUS، تكون السمة 11 هي معرف عامل التصفية)، حتى عندما تتم مصادقة المستخدم على خادم RADIUS، يكون معرف عامل التصفية مقترنا بذلك الاتصال. في هذا المثال، يفترض أن مصادقة RADIUS الخاصة بمستخدمي مركز VPN تكون قيد التشغيل بالفعل ولا يمكن إضافة إلا معرف التصفية.

قم بتعريف عامل التصفية على مركز VPN كما هو الحال في المثال السابق:



## Configuration | Policy Management | Traffic Management | Filters | Modify

Modify a configured filter.

**Filter Name**

Name of the filter to be modified. The name must be unique.

**Default Action**

Select the default action to be applied to traffic when no rules are found.

**Source Routing**

Check to allow the filter to apply to traffic that has been source routed.

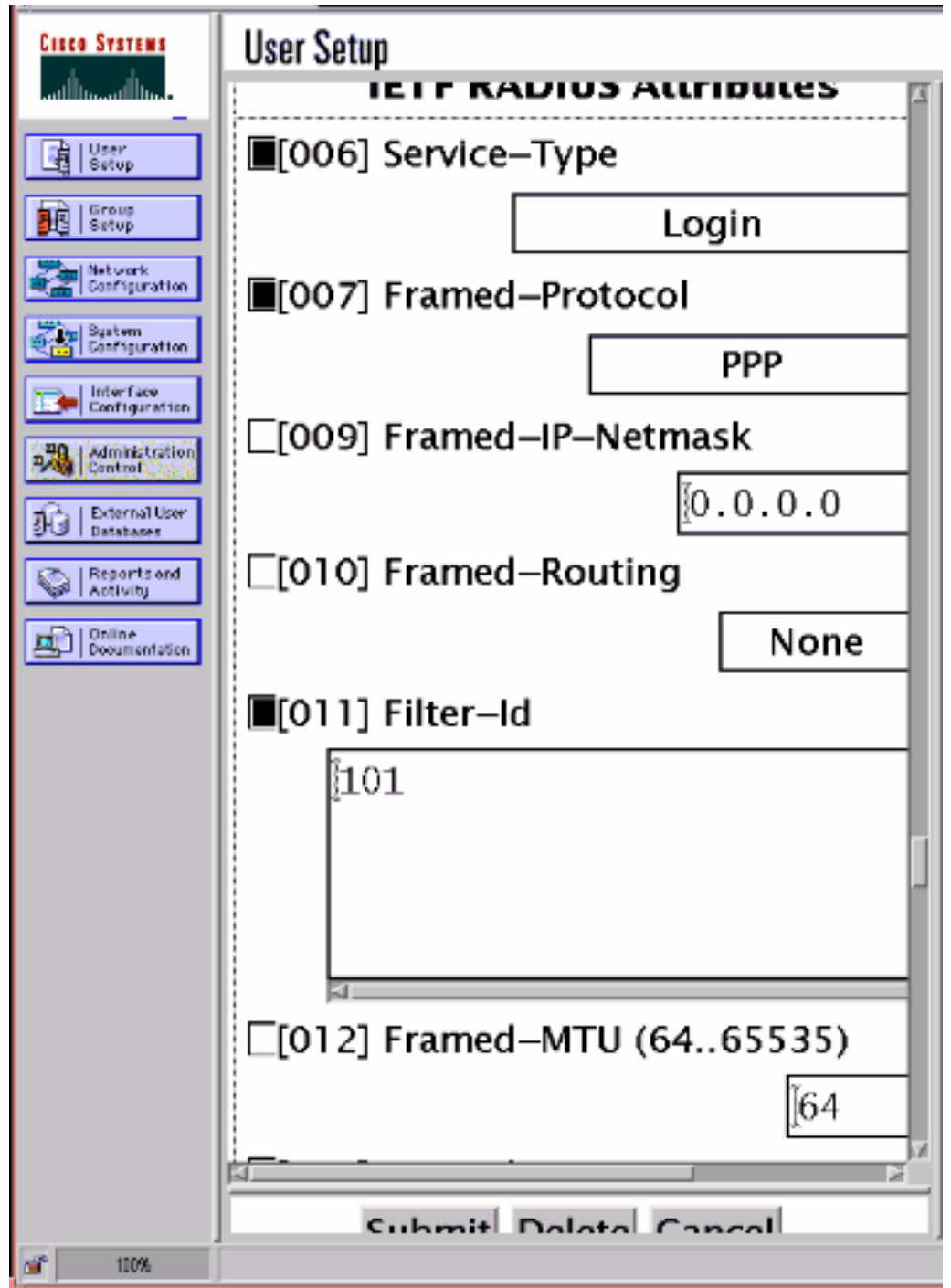
**Fragments**

Check to allow the filter to apply to fragmented IP packets.

**Description**

## [تكوين خادم CSNT - تعيين مرشح RADIUS](#)

قم بتكوين السمة 11، Filter-id على خادم Cisco Secure NT لتكون 101:



## [تصحيح الأخطاء - تعيين مرشح RADIUS](#)

إذا كان AUTHDECODE (مستوى الخطورة 1-13) قيد التشغيل في مركز VPN، يظهر السجل أن خادم Cisco Secure NT يرسل أسفل قائمة الوصول 101 في السمة 11 (0x0b):

```
SEV=13 AUTHDECODE/0 RPT=228 11:27:58.100 01/24/2001 207
020C002B 768825C5 C29E439F 4C8A727A ...+v.%...C.L.rz :0000
.....EA7606C5 06060000 00020706 00000001 .v :0010
.....0B053130 310806FF FFFFFFFF ..101 :0020
```

## [التحقق من الصحة](#)

لا يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

## استكشاف الأخطاء وإصلاحها

لأغراض استكشاف الأخطاء وإصلاحها فقط، يمكنك تشغيل تصحيح أخطاء المرشح عند إختيار التكوين < النظام > الأحداث < الفئات وإضافة الفئة Filterdbg التي تكون درجة الخطورة إلى السجل = 13. في القواعد، قم بتغيير الإجراء الافتراضي من إعادة التوجيه (أو الإسقاط) إلى إعادة التوجيه وتسجيل الدخول (أو إسقاط وتسجيل). عند إسترداد سجل الأحداث في المراقبة < سجل الأحداث، يجب أن يعرض إدخلات مثل:

```
SEV=9 FILTERDBG/1 RPT=62 14:20:17.190 12/21/2000 221  
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8
```

```
SEV=9 FILTERDBG/1 RPT=63 14:20:18.690 12/21/2000 222  
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8
```

## معلومات ذات صلة

- [مفاوضة IPsec/بروتوكولات IKE](#)
- [الأسئلة المتداولة حول VPN 3000 Concentrator](#)
- [دعم RADIUS](#)
- [دعم مركز Cisco VPN 3000](#)
- [دعم عمل VPN 3000 من Cisco](#)
- [مصدر المحتوى الإضافي الآمن من Cisco لدعم Windows](#)
- [طلب التعليقات \(RFCs\)](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوح

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انء مچي ف ني مدختسمل معد يوتحم مي دقتل ليرشبل او  
امك ةقيد نوك تن ل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تلبل  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىل إامئاد ةوچرلاب ي صؤت و تامچرتل هذه ةقد نع اهتيل وئس م Cisco  
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل