

PFSense – MT ALTERNATIVE ADAPTATION

“Handy Guide”

CLASS OF DOCUMENT:	INSTALLATION & CONFIGURATION
RELATED PROJECTS:	N/A
DOCUMENT:	PFSense – MT ALTERNATIVE ADAPTATION “HANDY GUIDE”
LAST VERSION:	v0.1
LAST MODIFIED:	04/11/09
AUTHOR:	LAITH Z. (LZ)
FILENAME:	PFSense MT ALTERNATIVE ADAPTATION v0.1.ODT
REFERENCE:	N/A
DISTRIBUTION:	COPYRIGHT: NONE
STATUS:	DRAFT
KEYWORDS:	N/A
SKILLS REQUIRED	GENERAL NETWORKING, SHELL BASICS, GENERAL OS KNOWLEDGE

Version	Change LOG	Author
0.1	- Installation guide	LZ

السلام عليكم ورحمة الله

سوف أقوم كما وعدت سابقا بكتابة شرح لبديل للمايكروتك. أتمنى أن يكون نافعا للجميع.

بداية سوف أقوم بتقسيم العمل فيه على مراحل أبدأها بالتنصيب، ثم إعدادات بسيطة، وأخير أحاول أن اتعمق في الإعدادات قدر الإمكان، حيث إن التعمق في جميع النواحي لن يكون أمرا مجديا ومستنزفا للوقت كثيرا، أخيرا سوف أجعل بعد كل قسم مجالا واسعا للأسئلة.

سوف أعتمد على هذه الطريقة وهي كتابة المقال ووضعه في المنتدى بصيغة pdf وذلك كي يسهل على الأخوة قراءته بأي وقت منظمًا، وكذلك سوف اصنع له إصدار، فكلما أضفنا على الملف إضافة مهمة وكبيرة أو قسما كاملا مثلا، نقوم بزيادة رقم الإصدار. فائدة أخرى لهذه الطريقة هي النظام في وضع الصور.

ارتأيت أن يكون حديثنا ينقسم لثلاثة اقسام رئيسية يأتي بعدها الأسئلة، أو فنقل ثلاثة اقسام سأكتبها وباقي الأقسام سوف تسير وفق نسق الاخوة في المنتدى.

سيكون القسم الأول مختصا باختيار النظام وتنصيبه الذي سوف يكون بدلا للمايكروتك. القسم الثاني سيتحدث عن كيفية إعدادة ليوفر أهم خدمتين، الأولى هي الكابتف بورتال، والثانية هي pppoe server وهما الأهم لمستخدمي المايكروتك حسب اعتقادي. القسم الثالث سيكون مخصصا للغوص بعمق في أغلب مميزات النظام.

القسم الأول: اختيار النظام وتنصيبه

لقد بحثت مطولا عن نظام يعطيني كل المزايا التي يعطينها أي Routing/Firewalling platform، مثل دعم الـ RIP, OSPF, BGP وقد وُجِدت طالتي في نظام فياتا، والكابتف بورتال والـ PPPoE server ووجدتها ولكن تطبيقها صعب نوعا ما في نظام openWRT، إضافة إلى أنه لا يدعم بنية i386 بكفاءة.

لم أجد نظاما مبني على لينوكس-يونكس يوفر كل هذه المزايا، عجزت ولم أجد، وفجأة يأتي نظام مبني على freeBSD ليكون الحل الناجح والحاوي على كل شيء في ملف أيزو حجمه حوالي 60 ميكا بايت. نعم لقد كان لي بمثابة الحل المعجزة.

إن نظام البي أس سنس هو نظام مبني على الفري بي أس دي، ولكي نعرف مدى قوة الأنظمة المبنية على الفري بي أس دي نذكر عدة منها:

الماك MAC لقد بني الماك OSX على الفري بي أس دي حيث إنه مبني على كيرنل دارون وهو بدوره شق من الفري بي أس دي. ويعتبر نظام الماك من أقوى أنظمة سطح المكتب، بل لعله الأقوى من وجهة نظري حيث إنني لم أجد نظاما يوفر كل الإمكانيات المدمجة مع بعضها البعض كحزمة واحدة مثل نظام الماك، مع قوة اليونكس، حيث الإصدار العاشر منه صنف على أنه نظام يونكس كامل وليس نظاما شبيها باليونكس Unix Like. الماك هو أحد الأنظمة التي أعتمد عليها، ولكنه للاستخدام المنزلي فقط، فأنا أستخدم الأوبونتو كنظام رئيسي في العمل.

مصادر:

[/http://www.apple.com/macosx](http://www.apple.com/macosx)

http://en.wikipedia.org/wiki/Mac_osx

PC-BSD نظام البي سي بي أس دي هو نظام مبني على الـ freeBSD مع الأخذ بعين الاعتبار المستخدم النهائي أو مستخدم سطح المكتب، يوفر هذا النظام إمكانيات في سهولة العمل للمستخدم النهائي تشابه لحد كبير الماك، حيث إنه يوفر إمكانيات تنصيب برامج بسهولة الوندوز، مع إنه نظام يونكس بكامل إمكانياته وقوته، ويدعم كما الماك freeBSD ports أي إنك تستطيع أن تقوم بتنصيب البرامج بطريقتين، الأولى برامج من الملفات الذاتية التنصيب مثل الوندوز، والأخرى كما في الفري بي أس دي من البورتات. طبعا النظام يوفر واجهة KDE 4.2.2 في آخر إصدار له، نظام رائع وجميل، قمت بتجربته وأعطاني الشعور بأنني أستخدم نظام ماك بواجهة مختلفة.

جون أو أس JunOS هو نظام تشغيل من جونيبر، يناظر سيسكو IOS Internetwork Operating System، نظام تشغيل مستقر جدا، وهو منصة فايرول وراوتر وسويج في نفس الوقت بتغيير الترخيص فقط، أي إنك تستطيع استخدام النظام كراوتر وسويج وفايرول بنفس الوقت إذا قمت بشراء الترخيص لجميعها، خلافا لنظام سيسكو الذي لا بد أن تشتري إصدارات مختلفة لكل منصة، لعله يظاهي نظام سيسكو في المميزات، إضافة إلى إنه يقدم ميزة لا يقدمها أي أو أس من سيسكو وهي الـ Modularity. وهذه الميزة هي إمكانية تشغيل أو إطفاء Modular واحد فقط في حال عطله أو عدم استقراره دون التأثير على النظام ككل، والموجيولر ممكن أن يكون هاردوير ككارت شبكة أو E1 أو T1 أو حتى Switch Modular أي سويج مضمن داخل الفايرول أو الراوتر. ومن الممكن أن يكون سوفتوير حيث بإمكانك تحديث جزء من النظام على عكس سيسكو حيث إنك لا بد أن تقوم بتحديث النظام ككل وإعادة تشغيله، أو إطفائه وتطوير الهاردوير، يشبه نظام لينوكس، حيث إن الـ Kernel Space تكون منفصلة ومستقرة وثابتة

جدا، وظيفتها فقط تقديم الخدمات لباقي السيرفيسس، وأما الـ User Space فإن كل الوظائف تكون في هذه المنطقة، بالتالي فإن تعطل أي سيرفيس لا يؤثر على الكيرنل إطلاقا، حيث إن الكيرنل هو كما الرفوف التي تحمل الكتب، بكل سهولة نستطيع التحكم في السيرفيس المتعطلة وإعادة تشغيلها بدون التأثير على باقي النظام.

استقرار النظام وثباته تجعله من أغلى الأنظمة على الإطلاق، وهذا لعله عامل يحد من انتشاره، ولكنه بدأ يأكل من سوق سيسكو في الـ Edge routers.

مصادر:

[/http://www.juniper.net/us/en/products-services/nos/junos](http://www.juniper.net/us/en/products-services/nos/junos)

<http://en.wikipedia.org/wiki/JUNOS>

نظاما Monowall & pfSense

إن نظامي المونوول والبي اف سنس نظامان مبنيان على فري بي اس دي، ولكن بتغيير عملية البوت وإعادة بنائها على PHP كليا بدلا من الشل سكربت. البي اف سنس حقيقة هو شق من المونوول أعيد بناؤه ليستهدف البنية i396-x86-64 حيث إن المونوول مصمم أصلا ليكون على الأجهزة الصغيرة والمضمنة.

يمكنكم الإطلاع أكثر على النظامين من خلال موقعهما الرسمي، ، <http://m0n0.ch/wall/> ، <http://www.pfsense.org>.

وبإمكانكم البحث في الإنترنت عن الفارق أو بعض الفروق والاختلاف في المميزات وعيوب كل من هذين الفايروولين وباقي الفايروولات المبنية على اللينوكس. سأقوب بإدراج مصدر واحد لأحد المقالات التي كتبت كدراسة مختصرة لمميزات مجموعة فايروولات مختلفة والتي أجدها وافية إلى حد ما:

[/http://www.fsckin.com/2007/11/14/7-different-linuxbsd-firewalls-reviewed](http://www.fsckin.com/2007/11/14/7-different-linuxbsd-firewalls-reviewed)

تحميل البي اف سنس وتنصيبه

سوف نقوم أولا بتحميل البي اف سنس من الإنترنت ومن ثم تنصيبه على حاسبة افتراضية، بإمكانك تنصيبه على حاسبة حقيقية أو حتى 1U server أو حتى Blade server إذا كنت تنوي أن تضع النظام في الشبكة Production network الخاصة بك، أي إنك تريده أن يكون الفايروول والبروكسي الرئيسي لك في الشبكة.

نقوم بتحميل النظام من الإنترنت من الموقع الرسمي للفايروول، بإمكانكم مراجعة الموقع لمعلومات أكثر. يمكنكم تحميل الإصدار لتنصيب جديد من أحد اللينكين التاليين:

<http://pfsense.bol2riz.com/downloads/pfSense-1.2.2-LiveCD-Installer.iso>

<http://files.pfsense.org/mirror/downloads/pfSense-1.2.2-LiveCD-Installer.iso>

أو تحميل نسخة التحديث، أي أنك تملك نظاما قديما وتريد تحديثه لإصدار أحدث:

<http://files.pfsense.org/mirror/updates/pfSense-Full-Update-1.2.2.tgz>

<ftp://reflection.ncsa.uiuc.edu/pub/pfSense/updates/pfSense-Full-Update-1.2.2.tgz>

لن نناقش كيفية القيام بتحديث من إصدار قديم حيث إننا نفترض بأننا جميعا جدد وليس لدينا نظام قد حمل مسبقا به، سوف أقوم بوضع ملحق للأسئلة والأجوبة وأضع فيه قسما كاملا لكيفية التحديث.

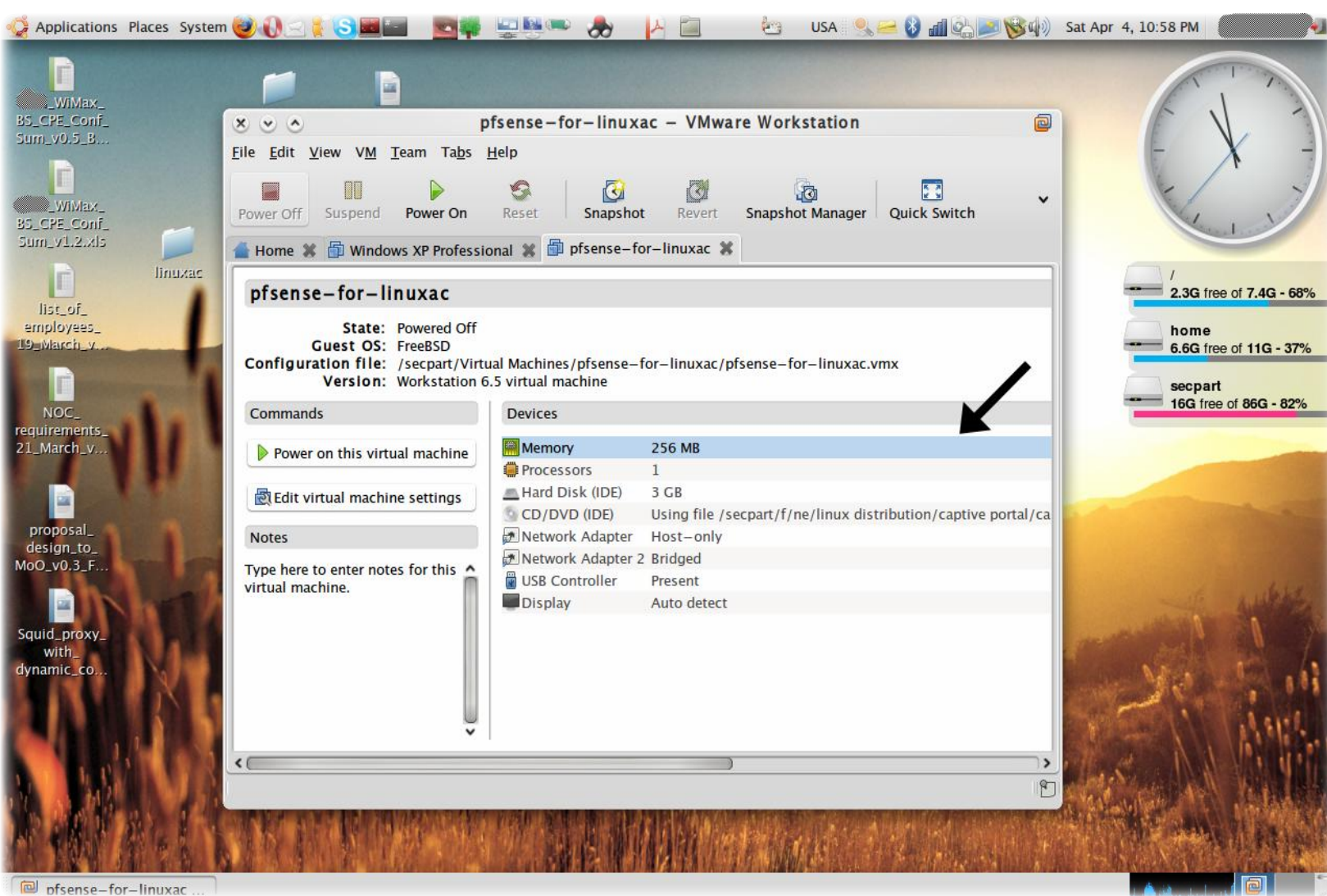
نتقل الآن للمرحلة الأهم، وهي عملية التنصيب:

لقد قمت حقيقة بعملية التنصيب والإعداد على حاسبة افتراضية، وقد استخدمت البرنامج VMware Workstation 6.5 for Linux.

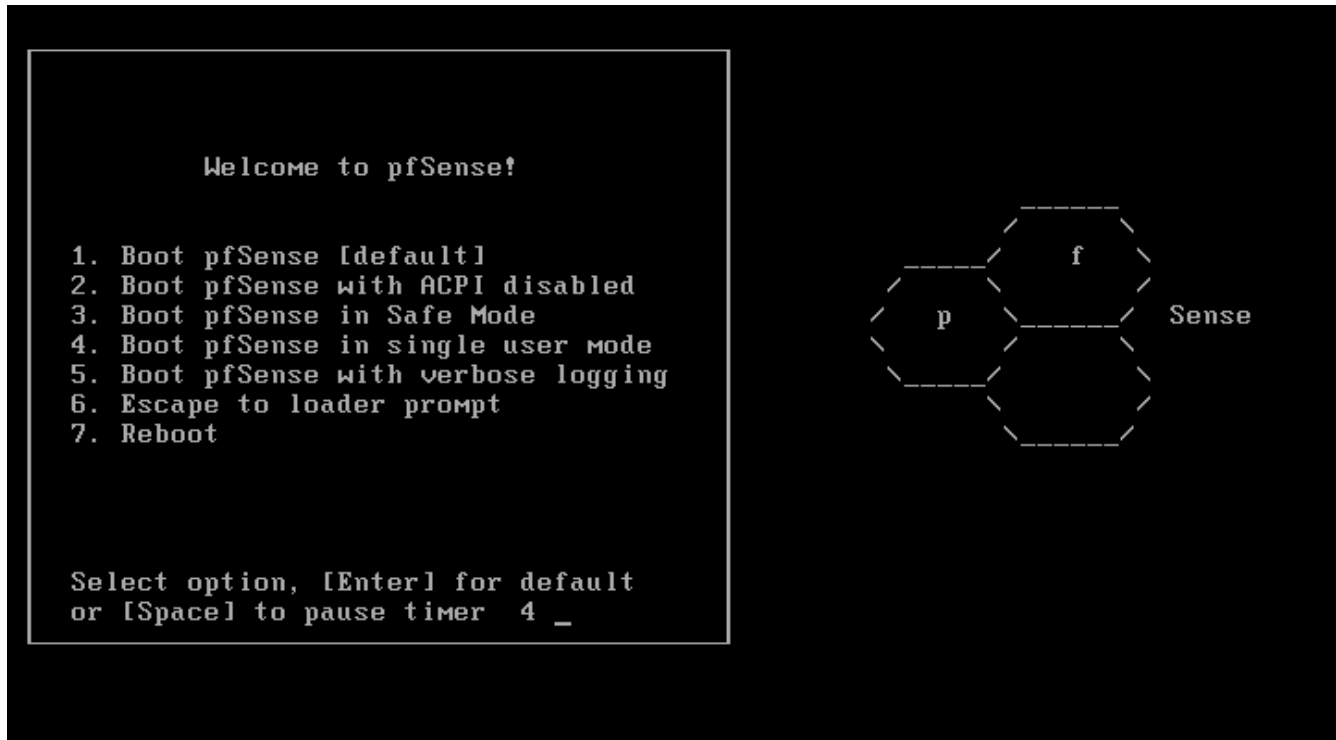
يمكنكم استخدام أي برنامج حوسبة افتراضية، أو حاسبة حقيقية تستخدمها كسيرفر، أو 1U server أو حتى Blade server.

كل ما تحتاجه هو كرتا شبكة، يكون الأول لان والثانية وان؛ حيث إن البي اف سنس لن يتم تنصيبه على سيرفر به كرت شبكة واحدة.

لقد استخدمت المواصفات التالية والتي تكفي حتى لسيرفر حقيقي:



عندما نبدأ بعملية الإقلاع، تظهر لنا الواجهة الأولى وهي:



ببساطة نترك الواجهة لتختار الخيار الافتراضي، لننتقل للواجهة الثانية:

```
Generating MFS /root partition
Looking for pfi.conf on acd0c done.
Looking for pfi.conf on fd0 done.
Looking for config.xml on fd0 [found msdos] done.
Generating a MFS /conf partition... done.
Mounting filesystems... done.
Creating symlinks.....done.
Launching PHP init system... done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

em0      00:0c:29:0f:0f:59
em1      00:0c:29:0f:0f:63
plip0    0

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.
Do you want to set up VLANs now [y;n]?n
```

هنا سوف نختار إذا ما كنا نريد وضع كل كارت شبكة في VLAN خاصة به.

أريد أن أوضح بعض الأمور هنا: في التصميم الناجح والمحترف للشبكات، عادة ما يكون كل قسم من الشبكة في VLAN خاصة به، والفني لان هي ببساطة عبارة عن Subnet مستقلة مع رينج عناوين مختلف عن غيرها IP range. من فوائد هذه الطريقة هي، التخصيص في كل شبكة فرعية، والأمن حيث إنك تقوم بمنع أعضاء شبكات معينة من دخول شبكات ثانية، فلو كان عندنا خدماتنا إنترنت منفصلة نقوم

بتقديمها لمجموعتي زبائن، لا يؤثر أي منهما على الآخر.

الفائدة الثانية هي تنظيم الشبكة، حيث إنك بمجرد أن ترى netID معين تعرف تماما أين يقع، وكل VLAN ID يختص بقسم من الشبكة وهذا سيسهل علينا حل المشاكل مستقبلا.

الفائدة الثالثة، تقليل عدد الأجهزة المستخدمة ما سيقفل كمية المال المنفق، حيث إنك تستطيع استخدام Cisco catalyst 4506 switch واحد وفيه 3-4 modules بدل أن تقوم بشراء 4 سويجات.

نحن لن نقوم بتغيير أي شيء الآن حيث إن هذا الخيار يعتبر خيار خاص، سوف نختار لا n.

إلى الواجهة التالية:

```
Valid interfaces are:
```

```
em0      00:0c:29:0f:0f:59
em1      00:0c:29:0f:0f:63
plip0    0
```

```
Do you want to set up VLANs first?
```

```
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.
```

```
Do you want to set up VLANs now [y!n]?n
```

```
*NOTE*  pfSense requires *AT LEAST* 2 assigned interfaces to function.
        If you do not have two interfaces you CANNOT continue.
```

```
        If you do not have at least two *REAL* network interface cards
        or one interface with multiple VLANs then pfSense *WILL NOT*
        function correctly.
```

```
If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.
```

```
Enter the LAN interface name or 'a' for auto-detection: em0
```

سوف نخصص كل كرت شبكة، أي نختار أي الكروت هو اللان وأيها الوان. التسميات تختلف قليلا في اليونكس أو البي اس دي عن اللينوكس، عموما em0 تعني eth0 ببساطة هنا وهكذا. قد تجد xpi0, xpi1 حسب نوع الدرايفر.

نسمي الكارت الذي سوف نستخدمه كلان هنا، ونسمي الكارت الذي سوف نستخدمه كوان في الواجهة التالية:

```
em0      00:0c:29:0f:0f:59
em1      00:0c:29:0f:0f:63
plip0    0
```

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y!n]?n

NOTE pfSense requires ***AT LEAST*** 2 assigned interfaces to function.
If you do not have two interfaces you **CANNOT** continue.

If you do not have at least two ***REAL*** network interface cards or one interface with multiple VLANs then pfSense ***WILL NOT*** function correctly.

If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: em0

Enter the WAN interface name or 'a' for auto-detection: em1

في الواجهة التالية، نستطيع تحديد ما إذا كان عندما كارت ثالث، من الممكن استخدام كارت وايرليس للبت باستخدامه أو كارت رابع لل DMZ. بعض المعلومات الإضافية حول ال DMZ.

([http://en.wikipedia.org/wiki/DMZ_\(computing\)](http://en.wikipedia.org/wiki/DMZ_(computing)))

NOTE pfSense requires ***AT LEAST*** 2 assigned interfaces to function.
If you do not have two interfaces you **CANNOT** continue.

If you do not have at least two ***REAL*** network interface cards or one interface with multiple VLANs then pfSense ***WILL NOT*** function correctly.

If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: em0

Enter the WAN interface name or 'a' for auto-detection: em1

Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

```
LAN  -> em0
WAN  -> em1
```

Do you want to proceed [y!n]?

نختار y في حال أن الإعدادات التي قمنا بها كلها سليمة.

في الواجهة التالية سوف تظهر لنا ال shell الخاصة بال pfSense. وهي مبرمجة بلغة ال PHP.

```
LAN*          ->  em0      ->  192.168.1.1
WAN*          ->  em1      ->  192.168.20.104 (DHCP)

pfSense console setup
*****
0) Logout (SSH only)
1) Assign Interfaces
2) Set LAN IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) PFtop
10) Filter Logs
11) Restart webConfigurator
12) pfSense PHP shell
13) Upgrade from console
14) Enable Secure Shell (sshd)
98) Move configuration file to removable device
99) Install pfSense to a hard drive/memory drive, etc.

Enter an option: 99
```

نختار 99 ثم نضغط على Enter لقبول الاختيار لبدء التنصيب. سوف يبدأ التنصيب مباشرة وندخل والواجهة الأولى للتنصيب مباشرة:



في الصفحات التالية سوف أقوم باختيار الخيارات الافتراضية حيث إن شرح تنصيب freeBSD هو خارج عن نطاق بحثنا.

نختار في الصفحة الأولى للتنصيب Accept these Settings وننتقل للصفحة الثانية:

F10=Refresh Display

Select Task

Choose one of the following tasks to perform.

- < Install pfSense >
- < Reboot >
- < Exit >

Install pfSense on this computer system

نختار أول اختيار وهو Install pfSense.

F10=Refresh Display

Select a Disk

Select a disk on which to install pfSense.

- < ad0: 3072MB <VMware Virtual IDE Hard Drive 00000001> at ata0-master P >
- < Return to Select Task >

نختار القرص الصلب الموجود في السيرفر، أيا كان اسمه لا تهم للإسم المهم أن تختار القرص الصلب الموجود.

F10=Refresh Display

Format this Disk?

Would you like to format this disk?

You should format the disk if it is new, or if you wish to start from a clean slate. You should NOT format the disk if it contains information that you want to keep.

< Format this Disk > < Skip this step >
< Return to Select Disk >

يسألك إن كنت تريد تهيئة القرص الصلب، قم بالضغط عليه مباشرة دون تردد

F10=Refresh Display

Select Geometry

The system reports that the geometry of ad0 is
6241 cylinders, 16 heads, 63 sectors

This geometry should enable you to boot from this disk. Unless you have a pressing reason to do otherwise, it is recommended that you use it.

If you don't understand what any of this means, just select 'Use this Geometry' to continue.

Cylinders	[6241]	[]
Heads	[16]	[]
Sectors	[63]	[]

< Use this Geometry > < Return to Select Disk >

Enter the number of cylinders in this disk's geometry

قم باختيار use this Geometry و قم بالضغط عليه مباشرة، حقيقة عملية التنصيب بالخيارات الافتراضية هو أمر ممل نوعا ما، ولكن نحن نحتاج لأن نستخدم الخيارات الغير افتراضية فقط حين نستخدم البي اف سنس استخدامات متقدمة جدا.

F10=Refresh Display

ABOUT TO FORMAT! Proceed?

WARNING! ALL data in ALL partitions on the disk

ad0: 3072MB <VMware Virtual IDE Hard Drive 00000001> at ata0-master P104

will be IRREVOCABLY ERASED!

Are you ABSOLUTELY SURE you wish to take this action? This is your LAST CHANCE to cancel!

< Format ad0 > < Return to Select Disk >

اضغط enter مباشرة بدون تردد

F10=Refresh Display

Partition Disk?

You may now partition this disk if you desire.

If you formatted this disk, and would now like to install multiple operating systems on it, you can reserve a part of the disk for each of them here. Create multiple partitions, one for each operating system.

If this disk already has operating systems on it that you wish to keep, you should be careful not to change the partitions that they are on, if you choose to partition.

Partition this disk?

< Partition Disk > < Skip this Step > < Return to Format Disk >

enter مرة أخرى، أمري إلى الله، نضل نعيدها لحد ما نكمل

F10=Refresh Display

Edit Partitions

Select the partitions (also known as 'slices' in BSD tradition) you want to have on this disk.

For Size, enter a raw size in sectors (1 gigabyte = 2097152 sectors) or a single '*' to indicate 'use the remaining space on the disk'.

Size (in Sectors) Partition Type Active?

[6290865] [FreeBSD] [X] < Ins > < Del >
< Add >

< Accept and Create > < Return to Format Disk >
< Revert to Partitions on Disk >

Accept and Create مباشرة، لا نحتاج إلى تفكير حاليا

F10=Refresh Display

Select Subpartitions

Set up the subpartitions (also known as just 'partitions' in BSD tradition) you want to have on this primary partition.

For Capacity, use 'M' to indicate megabytes, 'G' to indicate gigabytes, or a single '*' to indicate 'use the remaining space on the primary partition'.

Mountpoint Capacity

[/] [*] < Ins > < Del >
[swap] [256M] < Ins > < Del >
< Add >

< Accept and Create > < Return to Select Partition >
< Switch to Expert Mode >

Press F1 for Help

Accept and create، إلى الواجهة التالية

F10=Refresh Display

Executing Commands

```
/usr/local/bin/cpdup -vvv -I -o /usr /mnt/usr
```

[

43%

]

< Cancel >

واو، بلشنة بالفرمته، حتى الآن كنا نضع حجر الأساس للتهيئة، والآن بدأت عملية التهيئة والتنصيب

F10=Refresh Display

Install Kernel(s)

You may now wish to install a custom Kernel configuration.

< Uniprocessor kernel (one processor) >

< Symmetric multiprocessing kernel (more than one processor) >

< Embedded kernel (no vga console, keyboard) >

< Developers kernel (includes GDB, etc) >

Press F1 for Help

قم بالإختيار حسب نوع الحاسبة التي عندك، فإن كانت بمعالج واحد قم بالضغط على الخيار الأول، إما إن كانت المعالج متعدد الأنوية أو كان لديك أكثر من معالج فقم باختيار الخيار الثاني، وإذا كان الجهاز مضمنا فقم بالخيار الثالث.

F10=Refresh Display

Install Bootblock(s)

You may now wish to install bootblocks on one or more disks. If you already have a boot manager installed, you can skip this step (but you may have to configure your boot manager separately.) If you wish to install pfSense on a disk other than your first disk, you will need to put the bootblock on at least your first disk and the pfSense disk.

Disk Drive	Install Bootblock?	Packet mode?	Use Grub
[ad0]	[X]	[]	[]

< Accept and Install Bootblocks > < Skip this Step >
< Return to Install Kernel >

Press F1 for Help

The disk on which you wish to install a bootblock

يسأل عن المكان الذي نريد تنصيب خيارات الإقلاع أو منظم الإقلاع Boot manager، وبطبيعة الحال سوف نختار الخيار الأول وهو: Accept and install bootblock.

تمت عملية التنصيب بنجاح، عند أول إقلاع سوف تظهر لك نفس الواجهة التي رأيتها سابقا بنفس الخيارات التي قمنا بعملها من تسمية كروت الشبكة وما إلى ذلك، ولكن بدون الخيار 99 أي خيار التنصيب.

في القسم التالي سوف نبدأ بعملية الإعداد. هذا ما سنقوم به بعد الإجابة عن الأسئلة وتقييم طريقة العرض.

أود من الأخوة إبداء آرائهم حول طريقة العرض، طبعاً لم نعرض لكثير من الأمور حتى الآن وسوف نعتمد كثيراً على الصور للتوضيح، بعض الآراء والأسئلة للإجابة عنها وتوضيح ما هو غير واضح.

تحياتي، وإلى اللقاء في القسم الثاني.

