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

بداية سوف أقوم بتقسيم العمل فيه على مراحل أبدؤها 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 منظما، وكذلك سوف اضع 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 فلنقل ثلاثة اقسام سأكتبها وباقي الأقسام سوف تسير وفق نسق الاخوة في المنتدى.

سيكون القسم الأول مختصا باختيار النظام وبتنصيبه الذي سوف يكون بديلا للمايكروتك.
القسم الثاني سيتحدث عن كيفية إعداده 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 يعطينيها أي Routing/Firewalling platform، مثل دعم الـ RIP, OSPF, BGP وقد وجت ظالتي في نظام فياتا، والكابتف بورتال والـ PPPoE server وجدتها 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 اف سنس هو نظام مبني على الفري بي اس دي، ولكي نعرف مدى قوة الأنظمة المبنية على الفري بي اس دي نذكر عدة منها:

الماك MAC لقد بني الماك OSX على الفري بي اس 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 إني لم اجد نظاما يوفر كل الإمكانيات المدمجة مع بعضها البعض كحزمة واحدة مثل نظام الماك، مع قوة اليونكس، حيث الإصدار العاشر منه صنف على إنه نظام يونكس كامل وليس نظاما شبيها باليونكس Unix Like. الماك هو أحد الأنظمة التي أعتمد عليها، ولكنه للاستخدام المنزلي فقط، فأنا استخدم الأوبونتو كنظام رئيسي في العمل.

مصادر:

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 الإعتبار 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 بأني أستخدم نظام ماك بواجهة مختلفة.

جون أو أس JunOS هو نظام تشغيل من جونيبر، يناظر سسكو IOS Internetwork Operating System، نظام تشغيل مستقر جدا، وهو منصة فايروول وراوتر وسويج في نفس الوقت بتغيير الترخيص فقط، إي إنك تستطيع استخدام النظام كراوتر وسويج وفايروول بنفس الوقت إذا قمت بشراء الترخيص لجميعها، خلافا لنظام سسكو الأي او اس الذي لابد أن تشتري إصدارات مختلفة لكل منصة، لعله يظاهي نظام سسكو في المميزات، إضافة إلى إنه يقدم ميزة لا يقدمها الأي او اس من سسكو 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 الفايروول أو الراوتر. ومن الممكن أن يكون سوفتوير حيث بإمكانك تحديث جزء من النظام على عكس سسكو حيث إنك لابد أن تقوم بتحديث النظام ككل وإعادة تشغيلة، 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 سيرفس لا يؤثر على الكيرنل إطلاقا، حيث إن الكيرنل هو كما الرفوف التي تحمل الكتب، بكل سهولة نستطيع التحكم في السيرفس 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 سسكو في الـ Edge routers.

مصادر:

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 أف 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/

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 اللنكين 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.

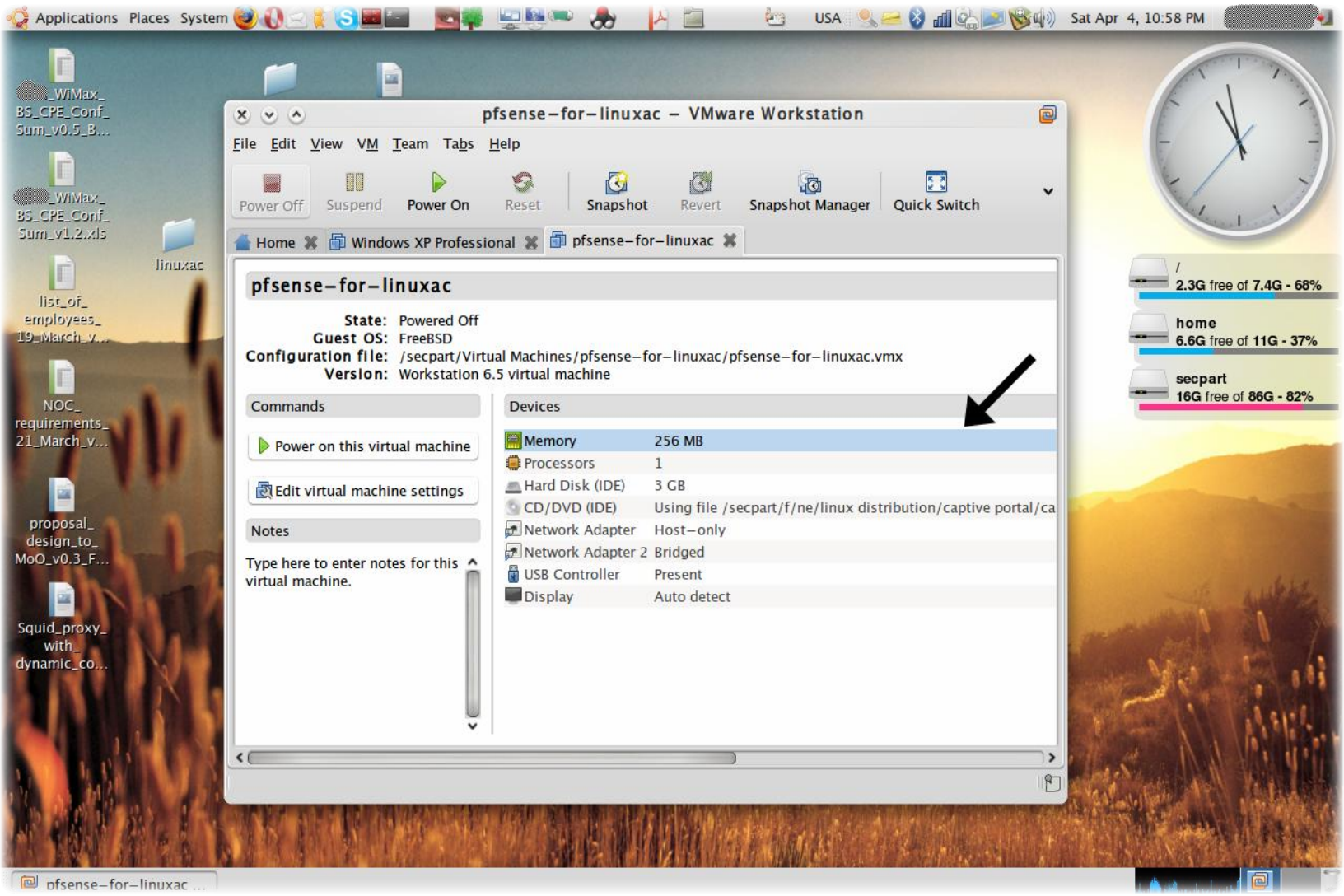
ننتقل الآن للمرحلة الأهم، وهي عملية التنصيب:

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

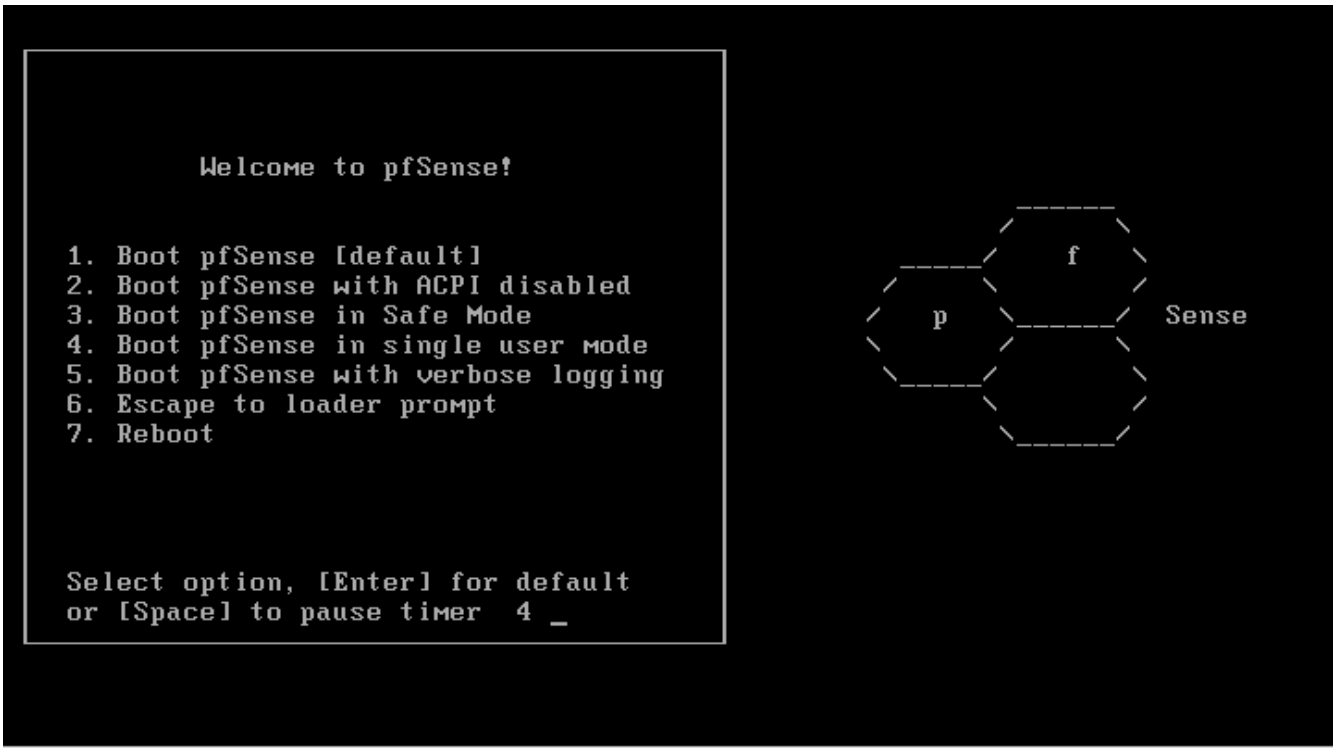
يمكنكم استخدام أي برنامج حوسبة افتراضية، أو حاسبة حقيقية تستخدمها كسيرفر، أو 1U server أو حتى Blade server.

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.

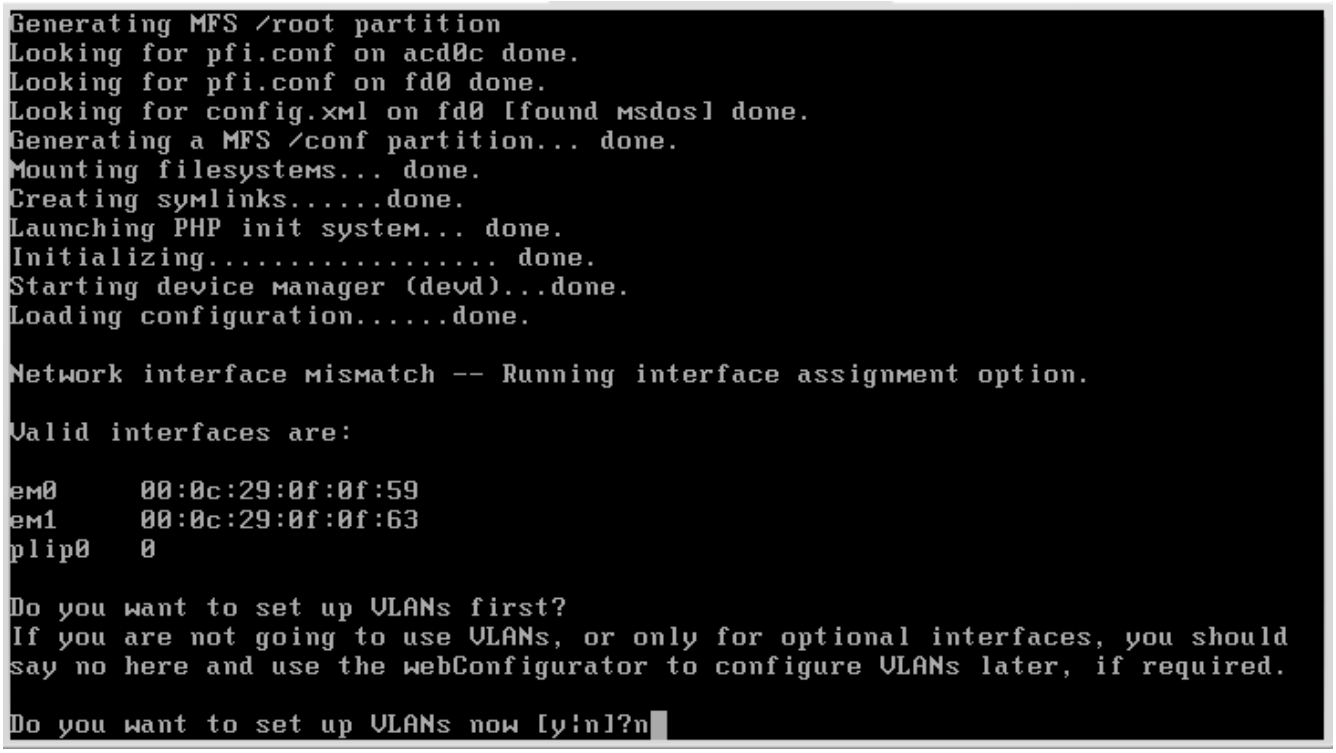
لقد استخدمت المواصفات التالية والتي تكفي حتى لسيرفر حقيقي:



عندما نبدأ بعملية الإقلاع، تظهر لنا الواجهة الأولى وهي:



ببساطة نترك الواجهة لتختار الخيار الإفتراضي، لننتقل للواجهة الثانية:



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

أريد أن اوضح بعض الأمور هنا: في التصميم الناجح والمحترف للشبكات، عادة ما يكون كل قسم من الشبكة في VLAN خاصة به، والفي لان هي ببساطة عبارة عن Subnet مستقلة مع رينج عناوين مختلف عن غيرها IP range. من فوائد هذه الطريقة هي، التخصص في كل شبكة فرعية، والأمن حيث إنك تقوم بمنع أعضاء شبكات معينة من دخول شبكات ثانية، فلو كان عندنا خدمتا 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 سيقلل 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 وأيهما 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 للبث باستخدامه أو كارت رابع للـ DMZ. بعض المعلومات الإضافية حول الـ DMZ.

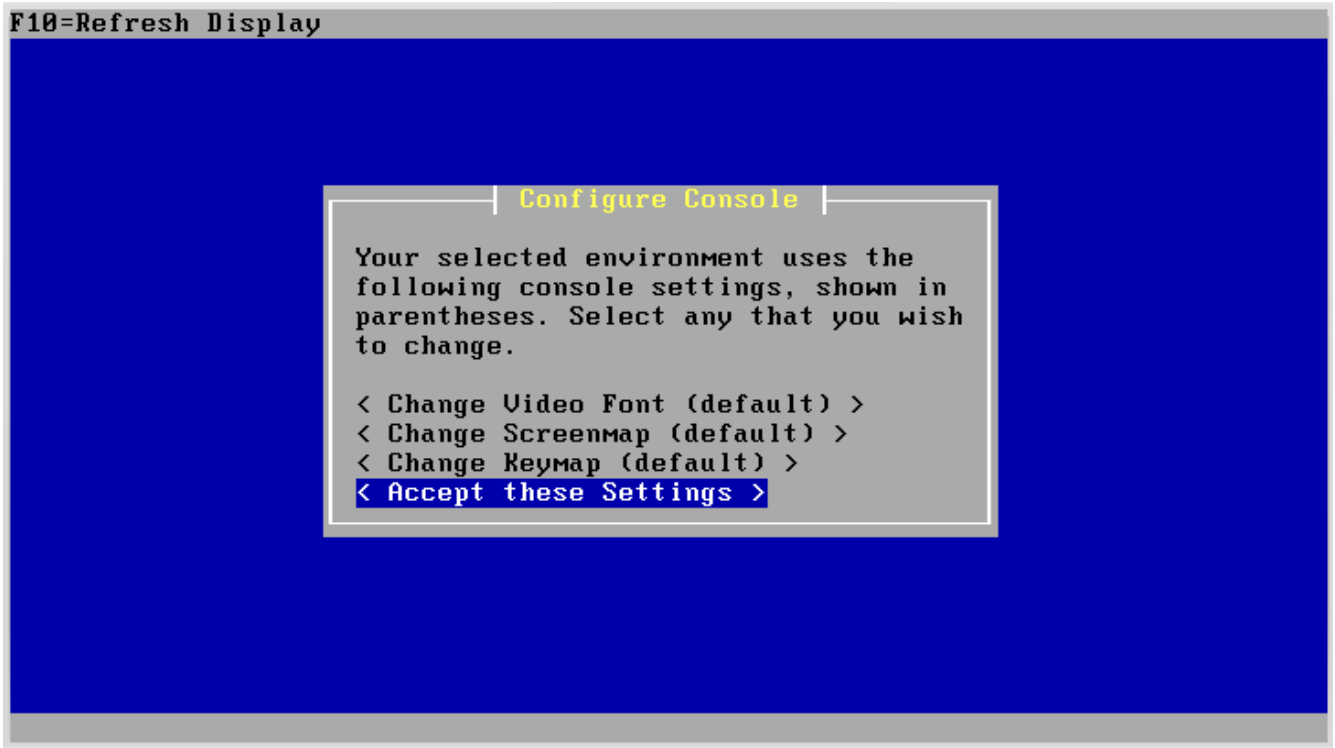
(http://en.wikipedia.org/wiki/DMZ_(computing

```
*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.

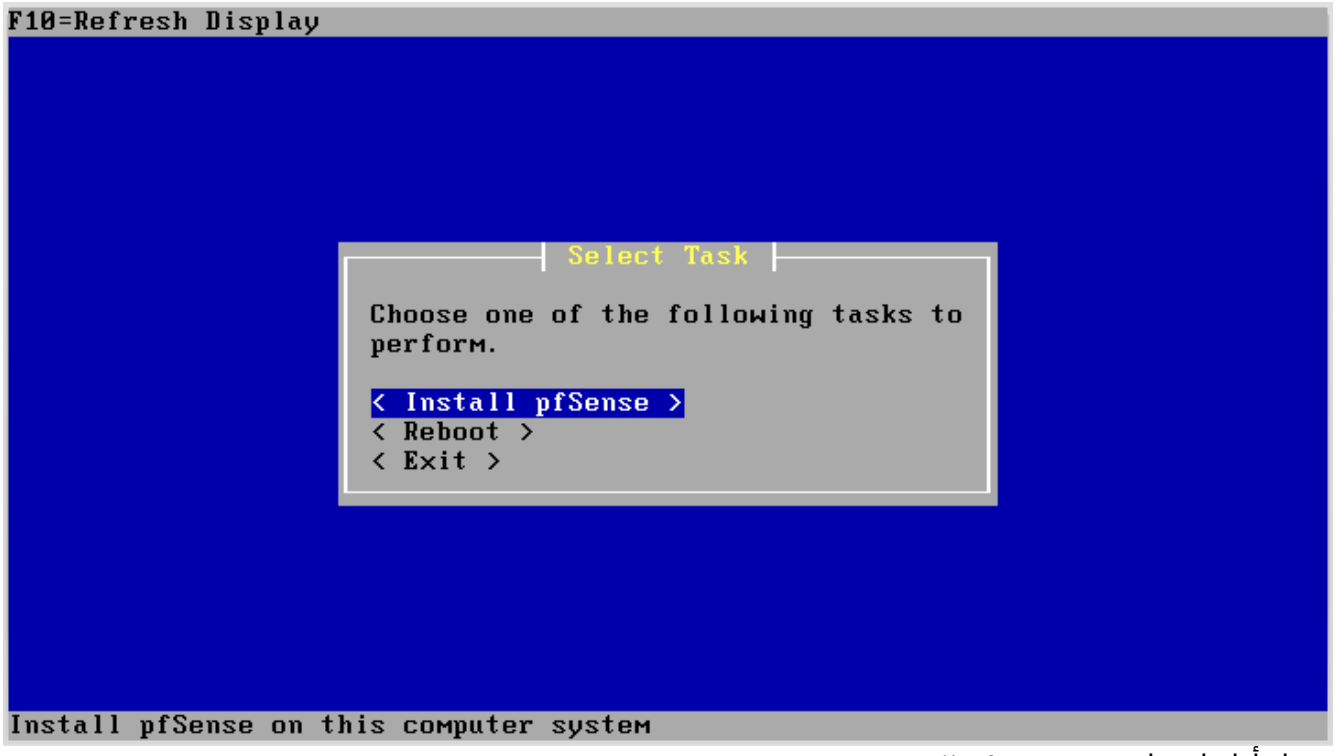
في الواجهة التالية سوف تظهر لنا الـ shell الخاصة بالـ pfSense. وهي مبرمجة بلغة الـ PHP.

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

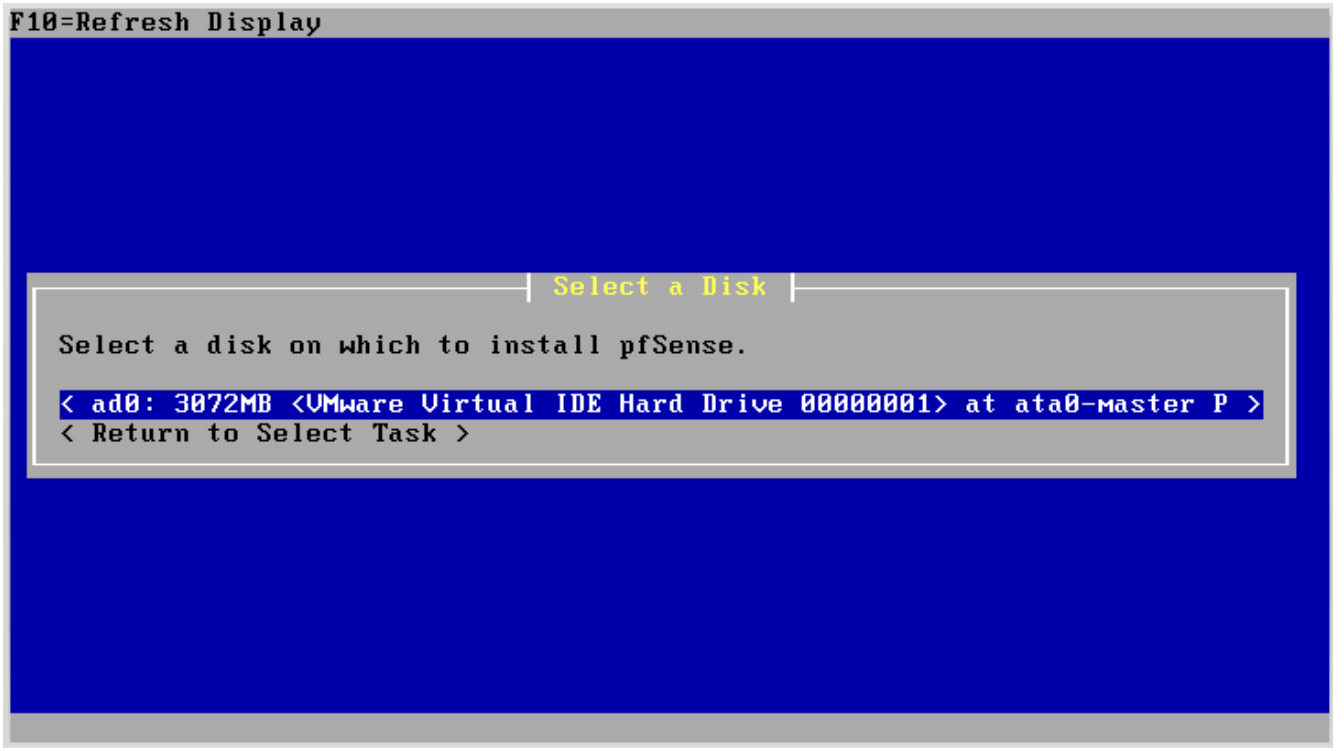


في الصفحات التالية سوف أقوم باختيار الخيارات الإفتراضية حيث إن شرح تنصيب freeBSD هو خارج عن نطاق بحثنا.

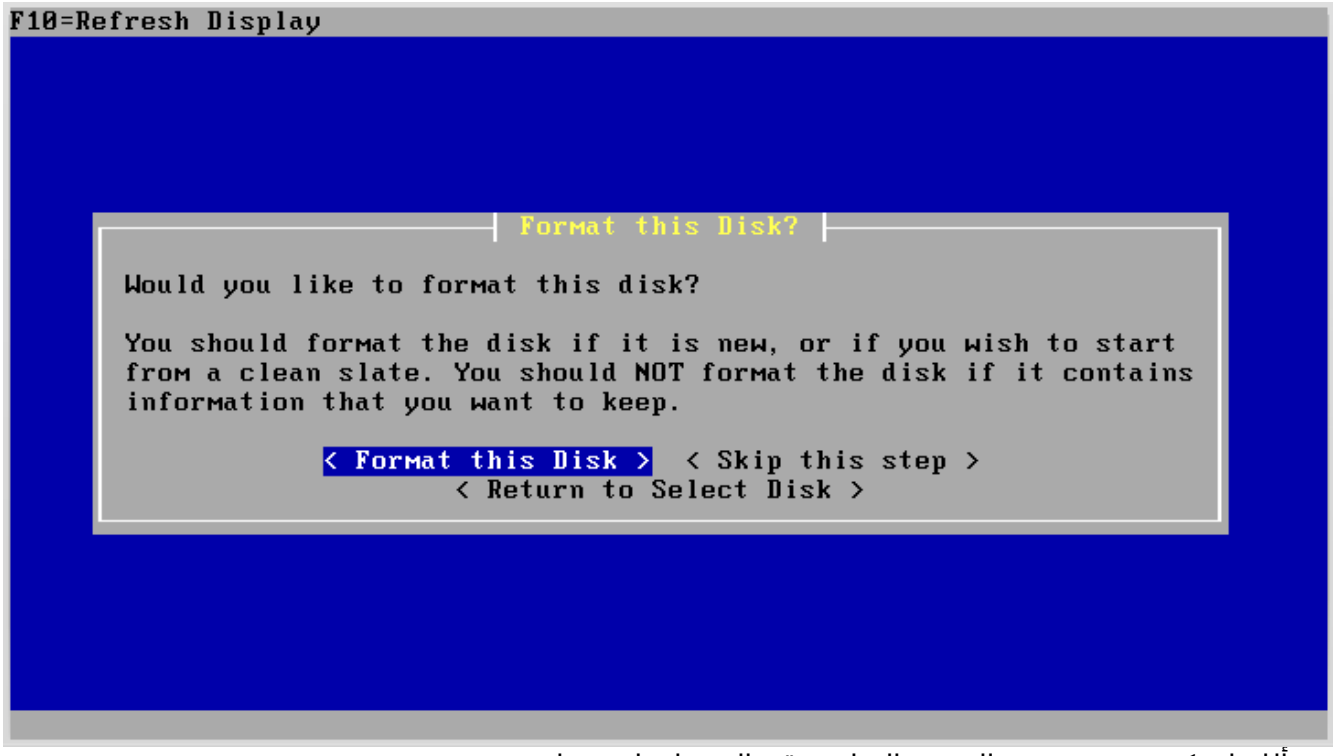
نختار في الصفحة الأولى للتنصيب Accept these Settings وننتقل للصفحة الثانية:



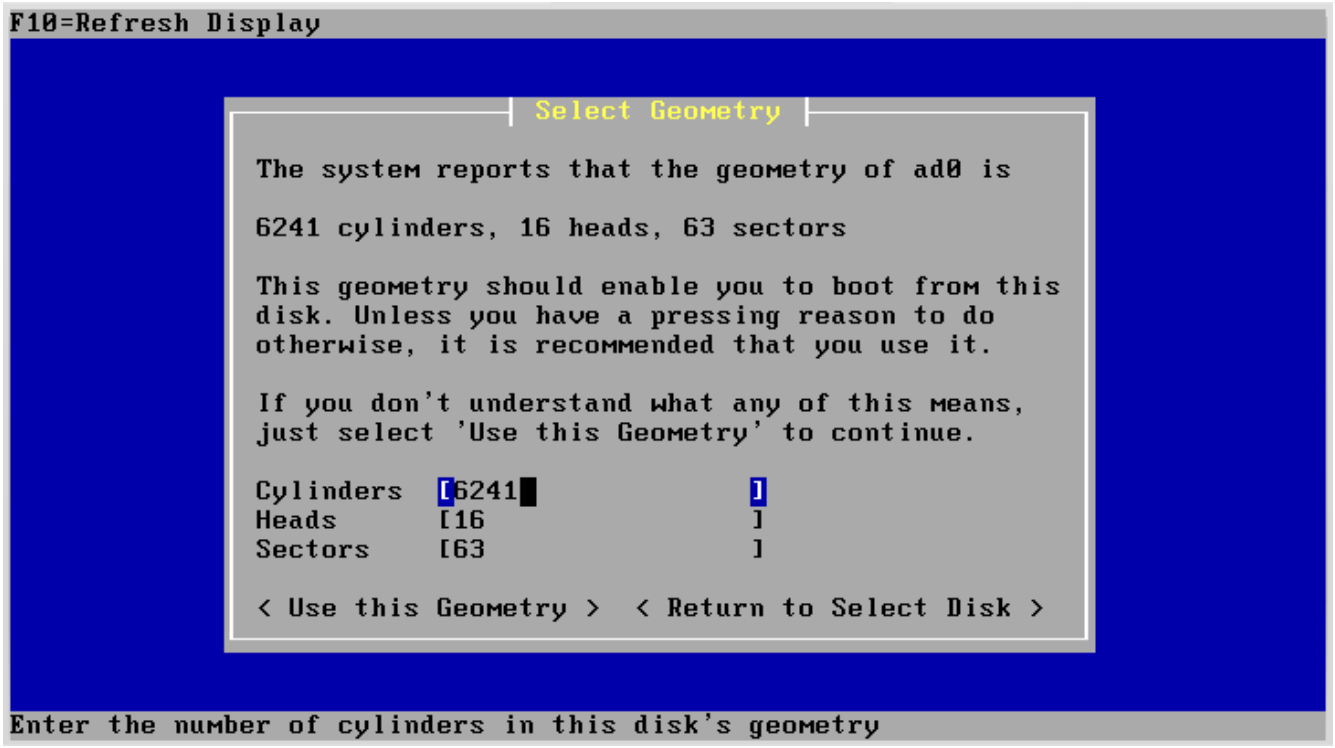
نختار أول اختيار وهو Install pfSense.



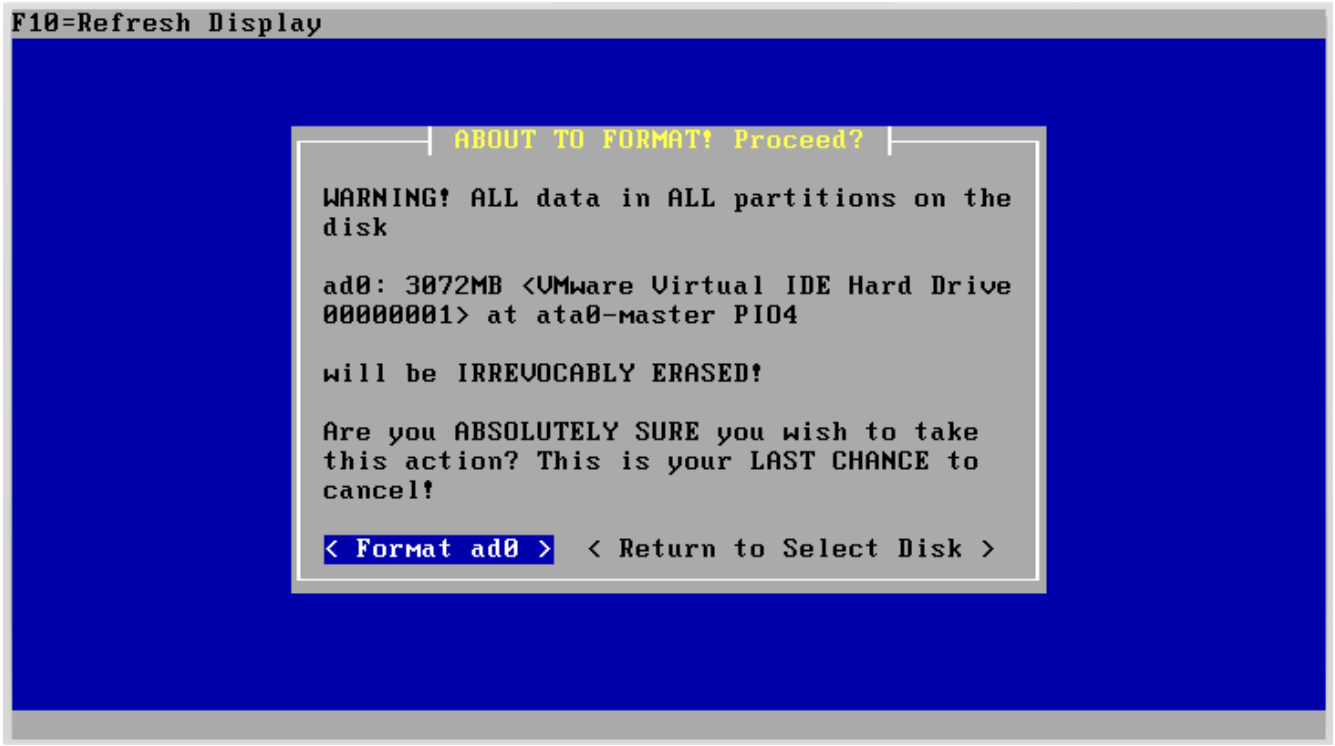
نختار القرص الصلب الموجود في السيرفر، أيا كان اسمه لا تهم للإسم المهم أن تختار القرص الصلب الموجود.



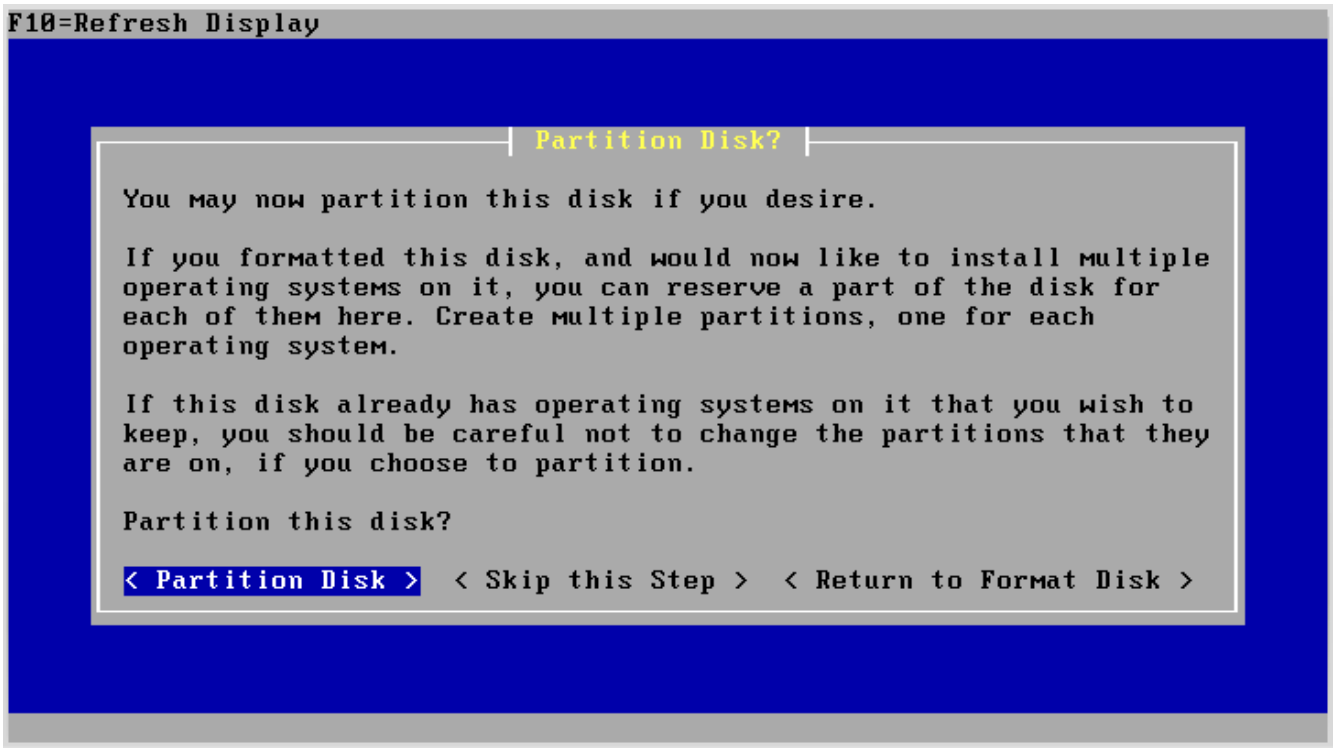
يسألك إن كنت تريد تهيئة القرص الصلب، قم الضغط عليه مباشرة دون تردد



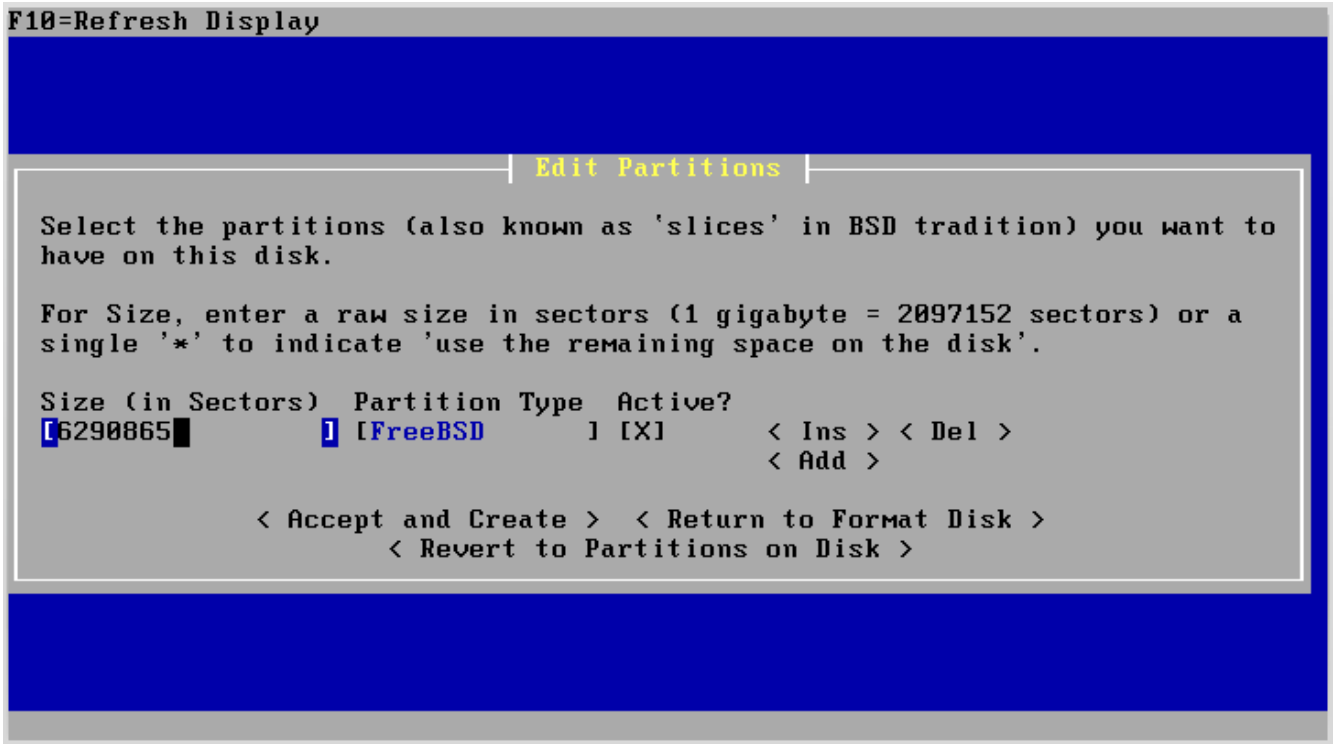
قم باختيار use this Geometry وقم بالضغط عليه مباشرة، حقيقة عملية التنصيب بالخيارات الافتراضية هو أمر ممل نوعا ما، ولكن نحن نحتاج لأن نستخدم الخيارات الغير افتراضية فقط حين نستخدم البي اف سنس استخدامات متقدمة جدا.



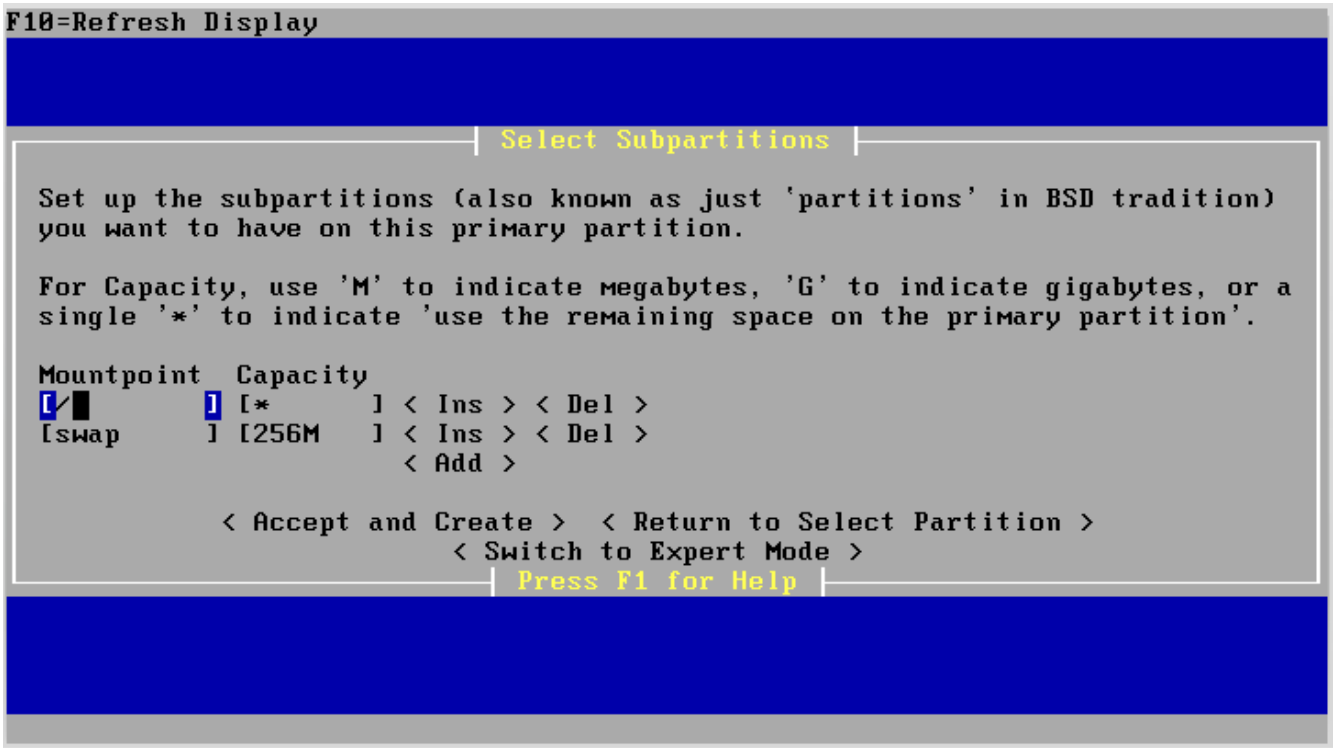
اضغط enter مباشرة بدون تردد



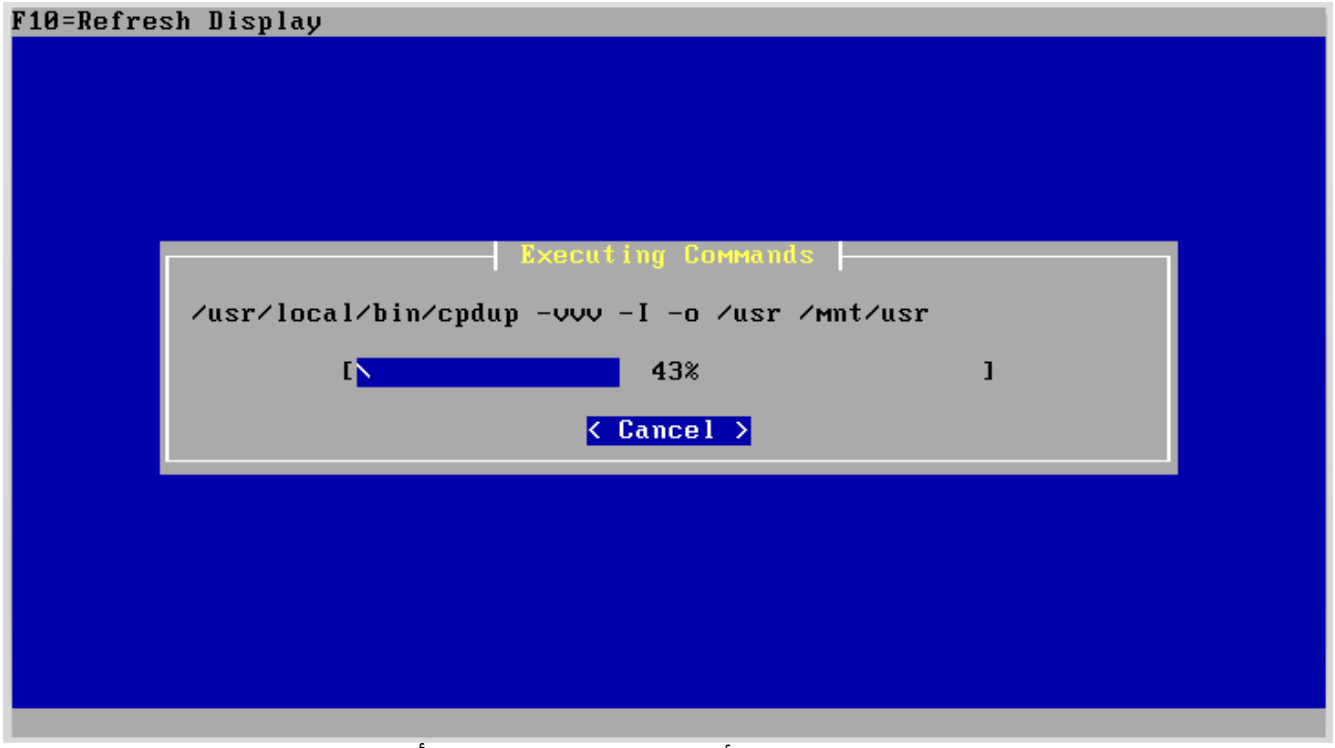
enter مرة أخرى، أمري إلى الله، نضل نعيدها لحد ما نكمل



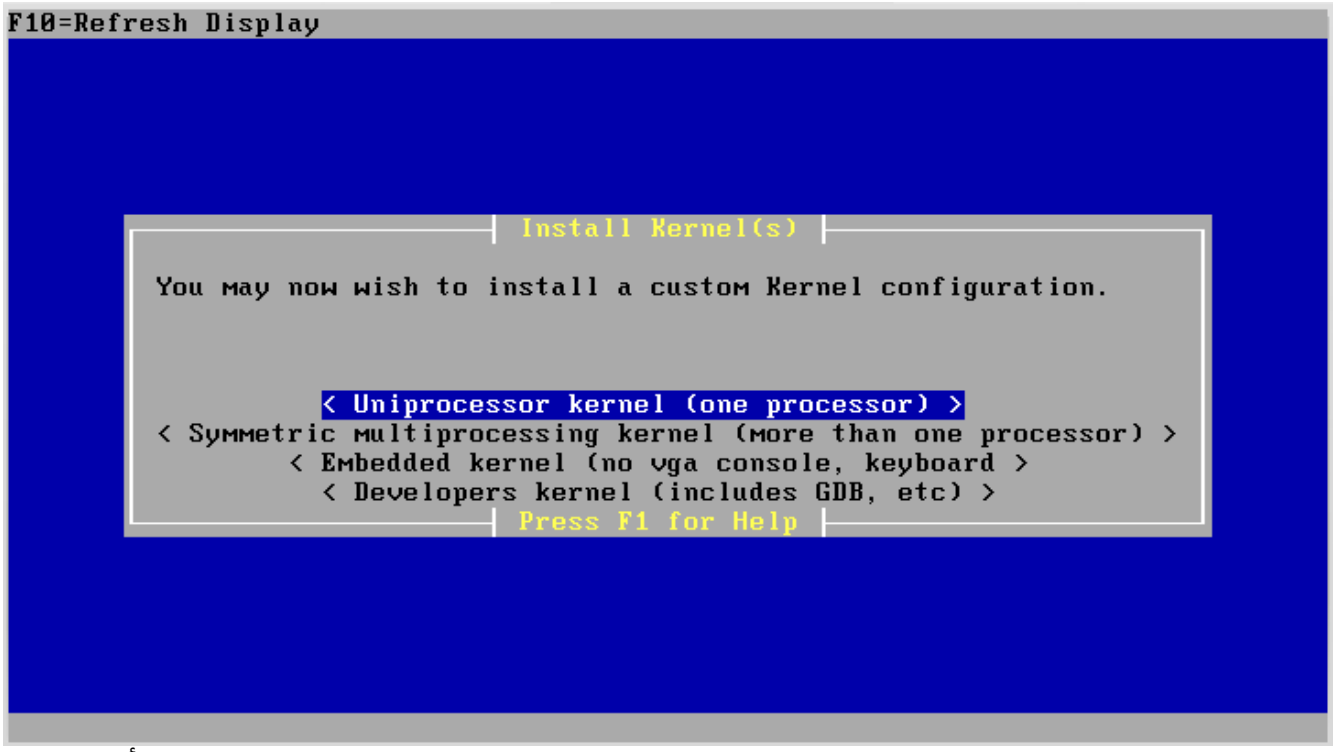
Accept and Create مباشرة، لا نحتاج إلى تفكير حاليا



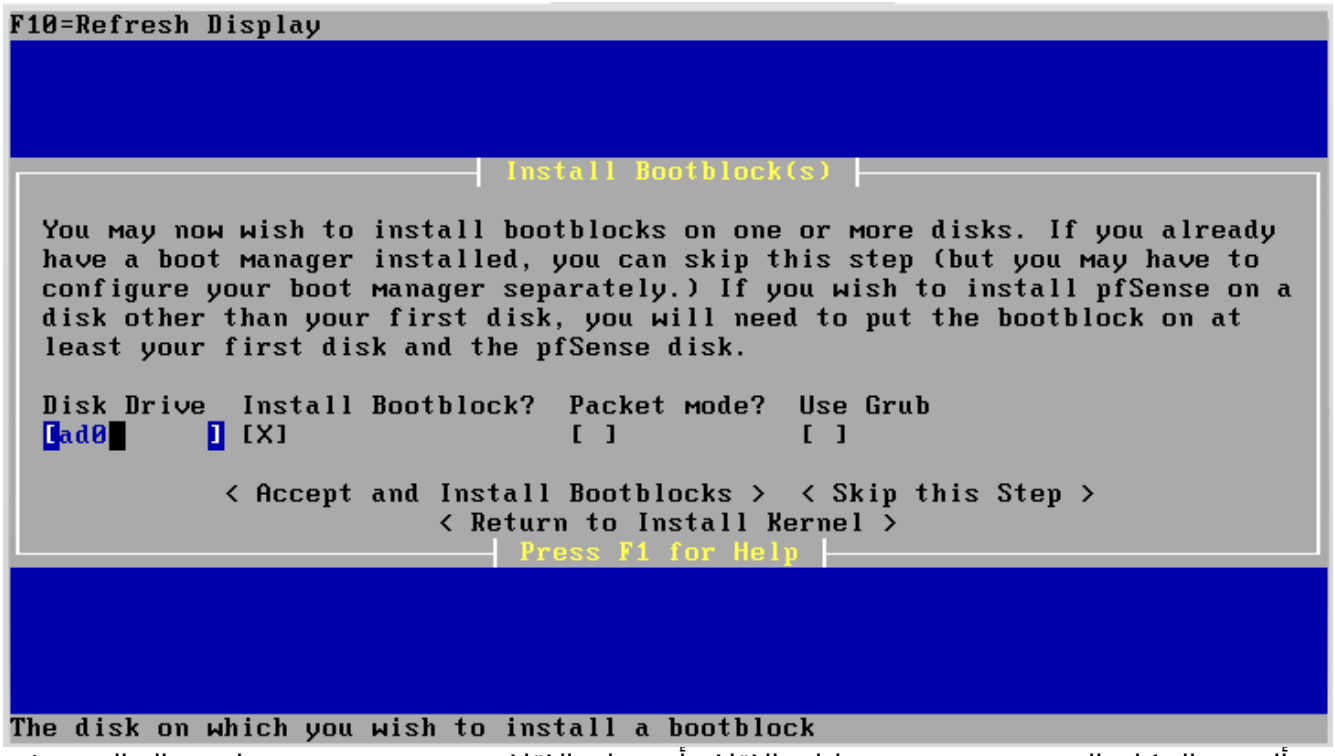
Accept and create، إلى الواجهة التالية



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



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.



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، طبعا لم نعرض لكثير من الأمور حتى الآن وسوف نعتمد كثيرا على الصور للتوضيح، بعض الآراء والاسئلة للإجابة عنها وتوضيح ما هو غير واضح.

تحياتي، وإلى اللقاء في القسم الثاني.