

تنظیم IPSec در لینوکس

پیش نیاز ها

این آموزش بر اساس توزیع CentOS 5.x و یا هر توزیع دیگر مبتنی بر RedHat است اما در تمامی توزیع های لینوکسی قابل استفاده است. برای پیاده سازی مفهوم IPSec نیاز به دو سیستم داریم که روی آنها لینوکس نصب شده باشد. دو ماشین مجازی را روی VMWare نصب کنید و برای هر کدام یک کارت شبکه تنظیم کنید و آدرس های IP را روی آنها تنظیم کنید.

مفهوم IPSec

IPSec مخفف IP Secure و به معنی امن کردن بسته های(Packet) انتقالی بین دو سیستم از طریق رمزنگاری(Encryption) است. ارتباط بین دو سیستم که از طریق اتصال IPSec امن شده اند را مانند یک تونل(Tunnel) فرض کنید که اطلاعات رد و بدل شده بین دو سیستم فقط و فقط برای این دو سیستم قابل فهم است و دیگران حتی با بدست آوردن این اطلاعات بخاطر رمزنگاری بودن اطلاعات، درکی از اطلاعات نخواهند داشت. اساس هر اتصال رمزنگاری شده وجود یک کلید یا Key است که برای رمزگشایی در سوی دیگر ارتباط استفاده خواهد شد.

در لینوکس دو نوع اتصال IPSec وجود دارد که در این آموزش نوع اول بررسی خواهد شد.

1. اتصال از نوع Host to Host

2. اتصال از نوع Network to Network

در نوع اول اتصال میان دو سیستم درون یک LAN برقرار می شود و هر host معرف یک ماشین است ولی اتصال نوع دوم میان دو شبکه مثلن بین دو LAN از طریق شبکه اینترنت مانند VPN استفاده خواهد شد.

فرض کنید دو ماشین دارید و می خواهید درون LAN یک ارتباط امن میان آنها ایجاد کنید. هر یک از این دو ماشین بعنوان یک host شناخته می شوند و نوع اتصال امن آنها host to host خواهد بود. مفهومی به نام Shared Key وجود دارد و به این معنی است که در این نوع اتصال حتمن و حتمن باید یک کلید مشترک بین دو host وجود داشته باشد تا هریک از دو host بتوانند عملیات رمزنگاری و رمز گشایی اطلاعات را انجام دهند.

نرم افزار های لازم

در توزیع های مبتنی بر RedHat بسته نرم افزاری ipsec-tools لازم برای پیاده سازی اتصال های IPSec می باشد و شامل دو بسته setkey و racoon است.

دستور زیر را برای بررسی نصب بودن ipsec-tools در توزیع های مبتنی بر Redhat اجرا کنید.

```
rpm -qa | grep ipsec-tools
```

اگر بسته نصب باشد باید خروجی زیر را ببینید.

```
ipsec-tools-0.6.5-13.el5_3.1
```

برای اطلاعات بیشتر از این نرم افزار و همچنین بسته هایی که با این بسته نصب می شوند دستور زیر را اجرا کنید. (خروجی در شکل زیر)

```
rpm -qi ipsec-tools
```

```
[root@localhost ~]# rpm -qi ipsec-tools
Name       : ipsec-tools                Relocations: (not relocatable)
Version    : 0.6.5                    Vendor: CentOS
Release    : 13.el5_3.1              Build Date: Tue 19 May 2009 06:54:35
          AM PDT
Install Date: Sun 07 Oct 2012 03:28:20 AM PDT    Build Host: builder16.centos.
org
Group      : System Environment/Base    Source RPM: ipsec-tools-0.6.5-13.el5
          _3.1.src.rpm
Size       : 883169                    License: BSD
Signature  : DSA/SHA1, Tue 19 May 2009 08:04:16 AM PDT, Key ID a8a447dce8562897
URL        : http://ipsec-tools.sourceforge.net/
Summary    : Tools for configuring and using IPSEC
Description:
This is the IPsec-Tools package. You need this package in order to
really use the IPsec functionality in the linux-2.5+ kernels. This
package builds:
- setkey, a program to directly manipulate policies and SAs
- racoon, an IKEv1 keying daemon
```

بسته setkey برای دست کاری کردن مدیریت کلید و صفت های امنیتی IPsec درون کرنل لینوکس استفاده می شود. دو پایگاه داده Security Association Database (SAD) و Security Policy Database (SPD) در کرنل وجود دارند که ورودی های آنها توسط دستور setkey افزوده و بروز می شوند و توسط racoon کنترل می شوند. اطلاعات بیشتر در صفحه راهنمای دستور setkey با دستور زیر ببینید.

```
man 8 setkey
```

بسته racoon که برای اختصاص Security Association بین اتصال های IPsec استفاده می شوند. در ایجاد یک اتصال IPsec برای ایجاد کلید می توانید هم بصورت دستی و هم بصورت خودکار انجام دهید و برای آنکه بصورت خودکار انجام شود باید بسته racoon روی سیستم نصب باشد.

racoon یک فایل به نام racoon.conf در مسیر /etc/racoon دارد که تنظیماتی مانند نوع یا متد authentication و تعیین نوع الگوریتم رمزنگاری در آن ذخیره می شوند. صفحه ی راهنمای آن با دستور زیر ببینید.

```
man 5 racoon.conf
```

برای ایجاد اتصال های IPSec هم می توانید بصورت دستی و با تغییر در فایل ها و همچنین بصورت گرافیکی و استفاده از ابزار **Network Administration Tool** استفاده کنید.

تنظیم IPSec Host to Host

این نوع اتصال میان دو ماشین درون یک LAN برای امن کردن ارتباط آنها استفاده می شود و نکته مهم این است که کلید استفاده شده برای اتصال های IPSec در هر دو host باید یکسان باشد. در هر صورت باید هر یک از نوع گرافیکی و دستی ایجاد اتصال ها را باید روی هر دو ماشین انجام دهید. فرض بر این است که روی ماشین A یک کارت شبکه با آدرس 192.168.149.132 و روی ماشین B یک کارت شبکه به آدرس 192.168.149.133 وجود دارد.

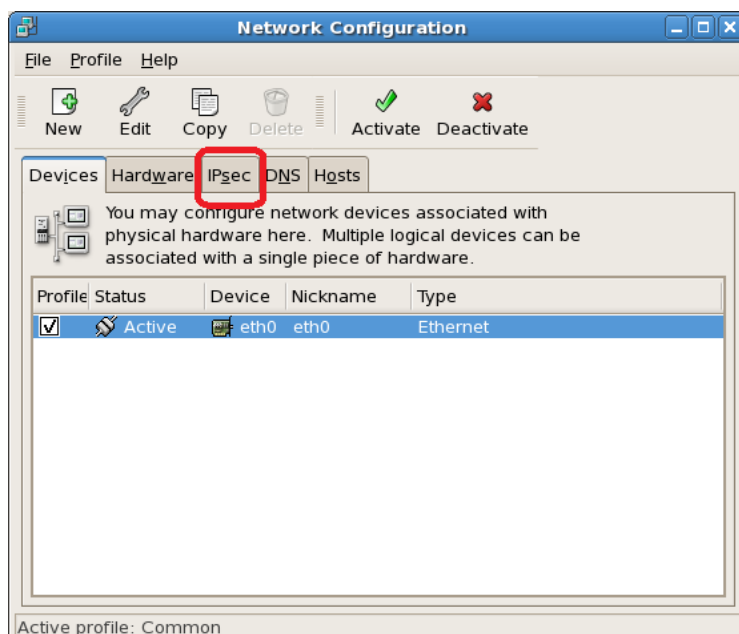
بطور کلی برای ایجاد یک اتصال IPSec Host to Host نیاز به موارد زیر داریم :

- آدرس IP ماشین دیگر که قصد اتصال امن با آن ماشین را داریم
- انتخاب یک متد رمزنگاری بصورت دستی یا خودکار با ابزار racoon
- انتخاب یک کلید مشترک میان هر دو ماشین
- انتخاب یک نام منحصر به فرد برای هر اتصال

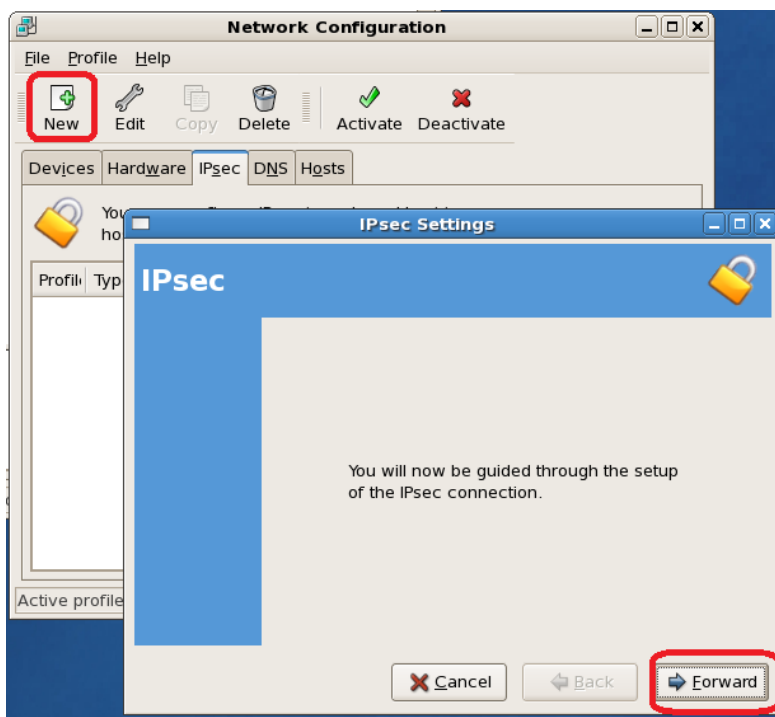
تنظیم گرافیکی با ابزار Network Administrator Tools

ابتدا دستور زیر را برای اجرای Network Administrator Tools در خط فرمان اجرا کنید و از پنجره باز شده IPsec Tab را انتخاب کنید.

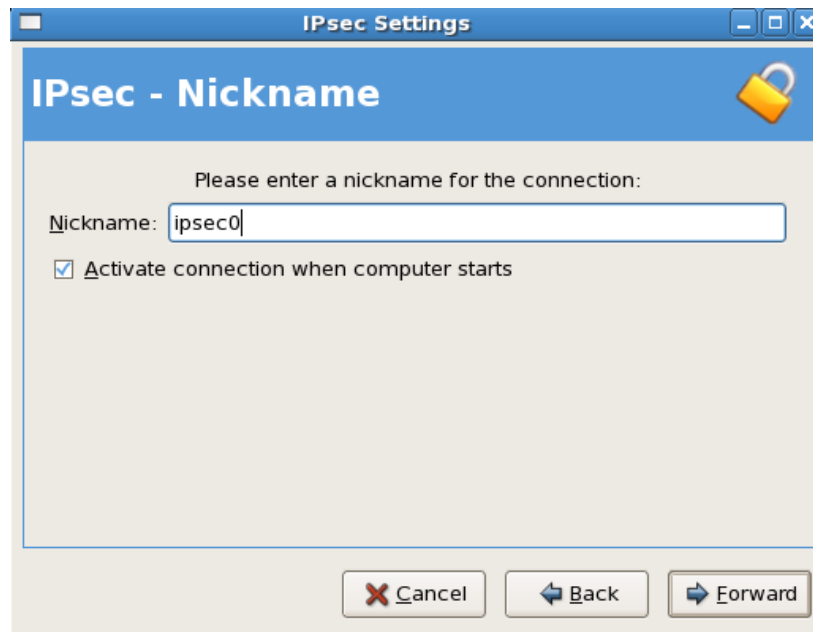
system-config-network



در پنجره روی New کلیک کنید تا ویزارد IPsec Setting باز شود و سپس روی Forward کلیک کنید.



در پنجره IPsec – Nickname یک نام منحصر به فرد برای اتصال انتخاب کنید و Active Connection when computer Start را می توانید انتخاب کنید. البته می توانید پس از اتمام تنظیمات بصورت دستی با کلیک روی Active اتصال را فعال کنید.



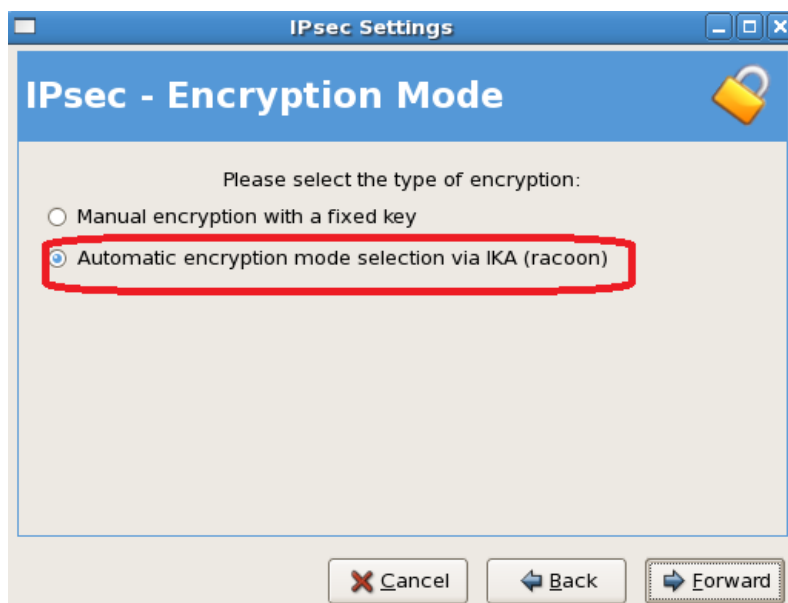
The image shows a Windows-style dialog box titled "IPsec Settings" with a subtitle "IPsec - Nickname". It contains a text input field labeled "Nickname:" with the text "ipsec0" entered. Below the input field is a checked checkbox labeled "Activate connection when computer starts". At the bottom, there are three buttons: "Cancel", "Back", and "Forward".

در پنجره IPsec – Connection Type نوع Host to Host Encryption را انتخاب کنید.



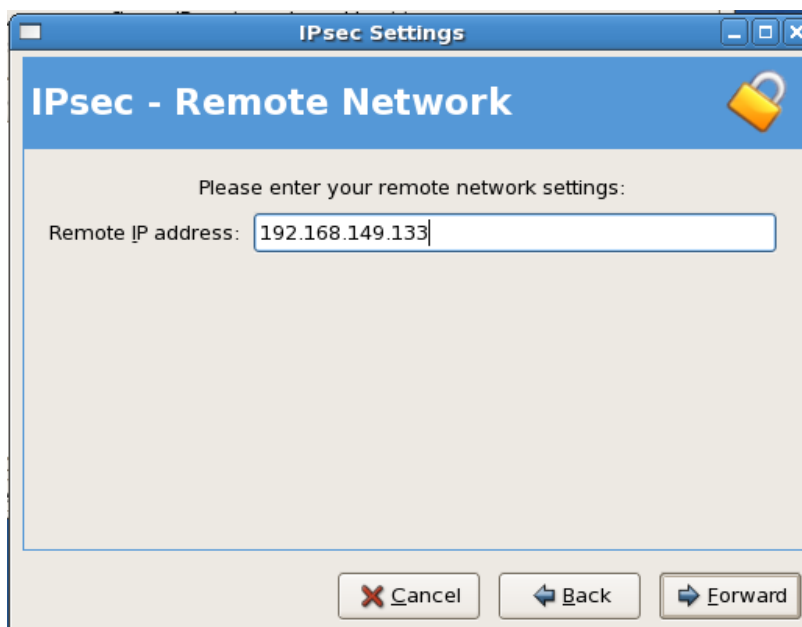
The image shows a Windows-style dialog box titled "IPsec Settings" with a subtitle "IPsec - Connection Type". It contains two radio button options: "Host to Host encryption" (which is selected and highlighted with a red rectangle) and "Network to Network encryption (VPN)". At the bottom, there are three buttons: "Cancel", "Back", and "Forward".

در پنجره IPsec – Encryption Mode گزینه Automatic encryption mode selecting via IKA (racoon) را انتخاب کنید.

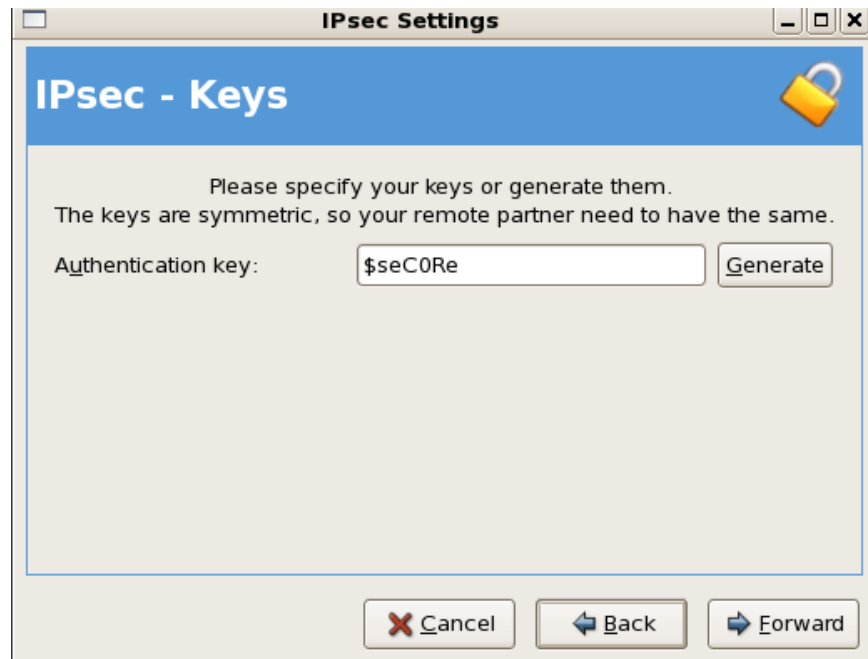


همانطور که گفته شد، برای ایجاد خودکار کلید باید ابزار racoon روی سیستم نصب شده باشد.

در پنجره IPsec – Remote Network باید آدرس IP ماشین B را انتخاب کنید. بطور مثال 192.168.149.133 را انتخاب کنید.



پس ارتباط امن باید بصورت دو طرفه بین ماشین A با آدرس 192.168.149.132 و ماشین B با آدرس 192.168.149.133 برقرار خواهد بود. در پنجره IPsec – Keys کلید را انتخاب کنید. این کلید حتمن و حتمن باید مشترک بین دو ماشین باشد. می توانید بصورت دستی کلید را وارد کنید یا اینکه از Generate استفاده کنید. کلید دلخواه را وارد کنید. سعی کنید کلید ترکیبی از حروف و اعداد باشد. بطور مثال \$seC0Re را وارد کنید.



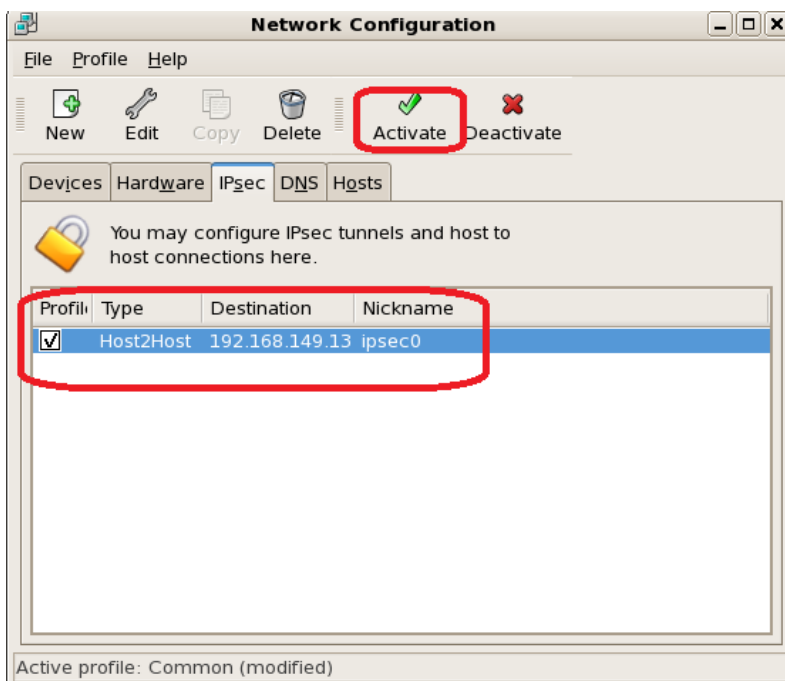
در پنجره IPsec – Summary خلاصه تنظیمات را می توانید مشاهده کنید. فیلد `ipsec.EncryptionMode=auto` یک سری از تنظیمات مانند نوع authentication و الگوریتم رمزنگاری را بصورت پیش فرض به اتصال توسط برنامه raccoon اختصاص می دهد. در پنجره زیر روی Apply کلیک کنید.



از پنجره Network Configuration از منوی File روی Save کلیک کنید و سپس دستور زیر را اجرا کنید.

```
/etc/init.d/network restart
```

همانطور که می بینید یک خط در IPsec Tab اضافه شده است. برای فعال کردن آن بصورت آنی و دستی روی Activate کلیک کنید.



پس از ایجاد یک اتصال روی ماشین، فایل های زیر در ماشین ساخته می شوند.

- /etc/sysconfig/network-scripts/ifcfg-<nickname>
- /etc/sysconfig/network-scripts/keys-<nickname>
- /etc/racoon/<remote-ip>.conf
- /etc/racoon/psk.txt

و اگر نوع Encryption از نوع خودکار باشد فایل racoon.conf نیز ساخته خواهد شد

تنظیم دستی اتصال IPsec Host to Host

در این بخش اتصال IPsec Host to Host را بصورت خودکار و بوسیله racoon روی ماشین B ایجاد می کنیم و هیچ تفاوتی بین روش گرافیکی و دستی وجود ندارد. تنها مواردی که باید فراموش نشود این است که از ابزار racoon استفاده می کنیم که معادل Automatic Encryption است و همچنین از کلیدی که در ماشین A ساختیم (\$sec0Re) بعنوان کلید مشترک استفاده می کنیم.

نامی که برای اتصال ماشین B انتخاب می کنیم ipsec1 خواهد بود. باید فایلی به نام ifcfg-ipsec1 را در دایرکتوری /etc/sysconfig/network-scripts ایجاد کنیم و مقادیری را در آن وارد کنیم.

```
vi /etc/sysconfig/network-scripts/ifcfg-ipsec1
```

گام اول : ایجاد فایل ifcfg-name_connection_ipsec

شکل کلی نام فایل ifcfg-<name_connection_ipsec> است و درون آن اصلاحات زیر باید قرار گیرد.

1. DST=X.X.X.X
2. TYPE=IPSEC
3. ONBOOT=no/yes
4. IKE_METHOD=PSK

گزینه اول اشاره به آدرس ماشین مقصدی دارد که قصد ارتباط امن با آنرا دارید. در این مثال ماشین B قصد ارتباط امن با ماشین A با آدرس 192.168.149.132 را دارد. پس باید آدرس ماشین A جاگزین X.X.X.X شود.

گزینه دوم نوع اتصال یا Connection را یعنی IPsec تعیین می شود.

گزینه سوم اگر no باشد این اتصال پس از بوت شدن Active نمی شود ولی اگر yes باشد معادل Active Connection when computer Start است و هنگام بوت شدن این کانکشن فعال خواهد شد. مقدار این گزینه را نیز yes تعیین کنید و توجه کنید که no و yes هر دو باید با حروف کوچک باشند.

گزینه چهارم روش ایجاد کلید اشتراکی را تعیین می کند که روش PSK انتخاب شده است.

گام دوم : ایجاد کلید مشترک

فایل keys-ipsec1 تعیین کننده کلیدی است که مشترک بین دو ماشین است. این فایل در ماشین A به نام keys-ipsec0 است و باید محتوای آنرا در فایل keys-ipsec1 کپی کنید. شکل کلی این فایل بصورت زیر و در مسیر زیر در هر ماشینی که در اتصال امن قرار دارد وجود دارد.

```
less /etc/sysconfig/network-scripts/keys-<name_connection_ipsec>
```

محتوای فایل keys-ipsec0 در ماشین A بصورت زیر است که باید آنرا در فایل keys-ipsec1 در ماشین B کپی کنید.

```
IKE_PSK="$seC0Re"
```

شکل کلی محتوای این فایل ها بصورت زیر است.

```
IKE_PSK="SHARED_KEY"
```

نکته بسیار مهمی که در ارتباط با فایل keys-name_connection_ipsec مجوز آنهاست که باید تنها مجوز read-only داشته باشند و تنها توسط کاربر root خوانده شوند پس لازم است مجوز آنها را به 600 با دستور زیر تغییر دهید.

```
chmod 600 /etc/sysconfig/network-scripts/keys-ipsec1
```

گام سوم : تعیین تنظیمات اتصال برای آدرس ماشین را دور

وقتی روی ماشین A در خواست ورود آدرس ماشین B داده شد پس از Forward کردن یک فایل به نام 192.168.149.133.conf در مسیر زیر ساخته شد که شامل تنظیماتی است و در شکل زیر قایل مشاهده است. مسیر فایل در ماشین A :

less /etc/racoon/192.168.149.133.conf

```
remote 192.168.149.131
{
    exchange_mode aggressive, main;
    my_identifier address;
    proposal {
        encryption_algorithm 3des;
        hash_algorithm sha1;
        authentication_method pre_shared_key;
        dh_group 2;
    }
}
```

پیش از هر چیز باید یک فایل در ماشین B با آدرس ماشین A بصورت 192.168.149.132.conf در زیر مسیر دایرکتوری /etc/racoon ایجاد کنید.

remote X.X.X.X تعیین کننده آدرس ماشین راه دور است که در اینجا باید با آدرس ماشین A جاگزین شود.

حالت یا مد authentication در توزیع های مبتنی بر Redhat ، حالت aggressive است و خط دوم در حالت کلی مد authentication را تعیین می کند. برای انتخاب حالت authentication دلخواه تان باید بجای گزینه Automatic Encryption حالت Manual را انتخاب می کردید.

my_identifier address روشی که با آن host راه دور تعیین هویت می شود را تعیین می کند که در اینجا با address ماشین راه دور اینکار انجام می شود.

encryption_algorithm الگوریتم انتخابی در هنگام عمل authentication را تعیین می کند که در اینجا از نوع 3des که مخفف Triple Data Encryption Standard است

hash_algorithm الگوریتمی که ارتباط امن میان دو host را با رمزنگاری داده های انتقالی میانشان تعیین میکند.

authentication_method تعیین کننده مدت ارتباطی میان دو host است که در اینجا چون از نوع IPsec Host to Host از نوع pre_shared_key است.

dh_group

گام چهارم : ایجاد فایل تنظیمات ابزار racoon

همانطور که گفته شد اگر می خواهید از روش ایجاد خود کار کلید استفاده کنید نیاز به ابزار racoon است و فایل racoon.conf تنظیمات آن است. مسیر این فایل در دایرکتوری /etc/racoon.conf است.

vi /etc/racoon/racoon.conf

و محتوای آن بصورت زیر است :

```
# Racoon IKE daemon configuration file.
# See 'man racoon.conf' for a description of the format and entries.

path include "/etc/racoon";
path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";

sainfo anonymous
{
    pfs_group 2;
    lifetime time 1 hour ;
    encryption_algorithm 3des, blowfish 448, rijndael ;
    authentication_algorithm hmac_shal, hmac_md5 ;
    compression_algorithm deflate ;
}
```

این فایل شامل مسیر های دایرکتوری های پیش فرض و همچنین مسیر فایل psk.txt (Pre Shared Key) است.

نوشته شده توسط : امیر احمدی نامی

سایت [آموزش های فارسی](#)