Replacing openswan ipsec with strongswan ipsec

- Introduction
- Motivation
- Ticket
- Use cases:
  - Strongswan ipsec vpn configurations
- Template changes:
  - Installing the StrongSwan
  - Upgrade:
    - Bring up pre upgrade vpn tunnels with strongswan
- UI
- API
- Configuration examples
  - Remote access VPN:
  - S2S VPN ipsec.conf:

Introduction

Currently VR is using openSwan ipsec vpn. This is an opensource ipsec vpn package that provides the Site-to-Site as well as Remote Access VPN in cloudstack VR.

This feature will replace OpenSwan ipsec with the StrongSwan ipsec vpn.

Motivation

Features of strongswan over openswan is:

1. Openswan is currently not maintained. Strongswan project is maintained by debian.
2. Strongswan ipsec supports the latest version of OS X clients.

Ticket

[CLOUDSTACK-8682 - Getting issue details...](#) STATUS

Use cases:

There are no use case changes w.r.t openswan ipsec.

Strongswan ipsec vpn configurations

Strongswan supports below vpn models as openswan.

1. Remote access VPN (isolated network and VPC)
2. Site to Site VPN (VPC).

Template changes:

Installing the StrongSwan

VR template is installed with the StrongSwan U4.5.2 package.

1. VRs deployed in cloudstack version will be come with the new template which is having strongswan.
2. If there are already VRs running, on reboot from cloudstack will pick up the new template.

Upgrade:

After upgrade if there existing vpn tunnels then these tunnels works with opnswan ipsec until the VR is upgraded.

Once the VR is upgraded existing/new vpn tunnel will use the strongswan ipsec tunnel.
Bring up pre upgrade vpn tunnels with strongswan

For existing tunnels to come up strongswan ipsec daemon, VR needs to be upgraded.

CS will apply new vpn (strongswan) configuration on VR.

For end user perspective there is no change in configuration. Only the changes are in VR ipsec configuration.

The below the configuration files get updated in the VR.

1. /etc/ipsec.conf
2. /var/lib/strongswan/ipsec.secrets.inc

Once the VRs are restarted, previously existing VPN connections will be broken. Once the VR rebooted successfully then VPN clients can re-establish the tunnels strongswan ipsec.

UI

N/A

API

N/A

Configuration examples

Remote access VPN:

ipsec.conf:

# ipsec.conf - strongSwan IPsec configuration file
# basic configuration
config setup

#nat_traversal=yes
# charonstart=yes
# plutostart=yes
#virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12
# Add connections here.
conn %default

keyingtries=1
authby=psk

conn L2TP_PSK

#left
left=10.147.52.223
leftprotoport=17/1701

#right
right=%any
rightprotoport=17/%any
rightsubnetwithin=10.1.2.0/8

leftnexthop=%defaultroute

#ipsec
pfs=no
auto=add
keyexchange=ikev1
forceencaps=yes
#leftfirewall=yes
include /var/lib/strongswan/ipsec.conf.inc
#include /etc/ipsec.d/l2tp.conf
S2S VPN ipsec.conf:

Example configuration on VR
==============================strongswan s2s conf ===============

root@r-5-QA:/etc/ipsec.d# cat /etc/ipsec.conf

# Manual: ipsec.conf.5
version 2.0
config setup
plutodebug=control
charonstart=no
include /etc/ipsec.d/*.conf

root@r-5-QA:/etc/ipsec.d# cat ipsec.vpn-10.147.52.174.conf

#vpn
conn vpn-10.147.52.174
ike lifetime=60m
keylife=20m
rekeymargin=3m
keyingtries=1
keyexchange=ikev1
authby=secret
left=10.147.52.173
leftsubnet=10.10.0.0/16
#leftid=@10.147.52.173
leftid=@moon
leftfirewall=yes
right=10.147.52.174
rightsubnet=10.20.0.0/16
#rightid=@10.147.52.174
rightid=@sun
auto=add

root@r-5-QA:/etc/ipsec.d# cat /etc/ipsec.secrets

@include /var/lib/openswan/ipsec.secrets.inc
@include /etc/ipsec.d/ipsec.*.secrets
@moon @sun : PSK "123456789"