Setting up an IPsec tunnel between RUT and Cisco device

□

Contents

Introduction

In computing, Internet Protocol Security (IPsec) is a secure network protocol suite of IPv4 that authenticates and encrypts the packets of data sent over an IPv4 network. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection.

This article provides an extensive configuration example with details on how to create a tunnel connection between two IPsec instances, one of which is configured on RUTxxx router and the other one on Cisco device.

Prerequisites

- One RUTxxx router of any type
- One Cisco router (this configuration example was created using Cisco RV340W)
- At least one router must have a Public Static or Public Dynamic IP address
- At least one end device (PC, Laptop, Tablet, Smartphone) to configure the routers
- (Optional) A second end device to configure and test remote LAN access

Configuration scheme

RUT configuration

Connect to router's **WebUI**, go to **Services > VPN > IPsec**. Enter a name for your IPsec instance, click **ADD** and when it appears in **IPsec Configuration** field, click **Edit**.

Then apply the configuration presented below.

1. **Enable** instance.
2. Set **My identifier** (device identifier for IPsec tunnel).
3. Write **Local IP address/Subnet mask** (an IP address/Subnet mask of the router on which the IPsec instance is configured).
4. Add **Remote VPN endpoint** (the Public IP address of the Cisco router).
5. Set **Remote identifier** (remote address of the remote peer).
6. Write **Remote IP address/Subnet mask** (LAN IP address/Subnet mask of the Cisco router).

Next step in configuring IPsec instance is **Phase** settings. For this example we left the default RUT **Phase 1** and **Phase 2** settings.

When you're finished with the configuration, click **Save** button and then you will be prompted back to IPsec window where you will need to configure **Pre-shared key**.

1. Press **Add** button.
2. Write **Pre-shared key** (a shared password used for authentication between the peers. The value of this field must match on both instances).
3. Add **Secret's ID selector** (Cisco LAN IP).
4. Press **Save**.

Cisco configuration

Connect to router's WebUI, go to **VPN > IPsec Profiles** and apply the following configuration.

1. Add **Profile Name** (anything you want).
2. Choose **Keying Mode** (Auto).
3. Choose **IKE version** (IKEv1).
4. Select **DH Group** (Group 5).
5. Select **Encryption** (3DES).
6. Choose **Authentication** (SHA1).
7. Set **SA Lifetime** (28800).
8. Choose protocol in **Protocol Selection** (ESP).

9. Select **Encryption** (3DES).
10. Select **Authentication** (SHA1).
11. Set **SA Lifetime** (28800).
12. Enable **Perfect Forward Secrecy**.
13. Select **Group: Group** (5).

When you are done with **IPsec Profiles**, save settings, go to **Site-to-Site** settings and apply the following configuration:

1. **Enable** it.
2. Select **IPsec Profile** (RUT).
3. Set **Interface** (your internet source).
4. Select **Remote Endpoint** (static IP).
5. Write **RUT Public IP**.
6. Add **Pre Shared Key** (a shared password used for authentication between the peers. The value of this field must match on both instances).
7. Disable **Minimum Key complexity**.
8. Select **Local Identifier Type** (IP Address).
9. Write **Local Identifier** (Cisco LAN IP address).
10. Select **Local IP Type** (Subnet).
11. Write **IP Address** (Cisco local network).
12. Add **Subnet Mask** (network mask).
13. Select **Remote Identifier Type** (Remote WAN IP).
14. Write **Remote Identifier** (RUT LAN IP).
15. Select **Remote IP Type** (Subnet).
16. Add **IP Address** (RUT local network).
17. Add **Subnet Mask** (RUT local network mask).

Testing the setup

If you've followed all the steps presented above, your configuration should be finished. But as with any other configuration, it is always wise to test the setup in order to make sure that it works properly. In order to test an IPsec connection, login to the RUT WebUI and go to **Services → CLI**. Login with user name: **root** and the router's admin password. From there you should then be able to **ping** the opposite instance's LAN IP address. To use a ping command, type **ping <ip_address>** and press the "Enter" key on your keyboard:

You can also test if LAN access is working the same way. Instead of pinging the opposite instance's LAN IP address, ping one of the end device's IPs. One common issue that can be encountered here is that the end devices **might need their DHCP leases renewed**. There are many methods of accomplishing this, but the easiest and most accessible way is to simply disconnect and reconnect the LAN cable to device or the router that it's connected to.

If the ping requests are successful, congratulations, your setup works! If not, we suggest that you review all steps once more.