Tech Note 6  How to setup and test a IPSEC VPN tunnel using two RAM or SN devices

Abstract:
This document provides a step-by-step procedure for setting up a LAN-to-LAN tunnel using IPSEC between two SN/RAM units and how to test end-to-end communication.

Product:
Any SN/RAM product

Use Case/ Problem Solved:
In many Machine-to-Machine (M2M) applications sensitive data needs to be secured when traversing a public medium. This can be accomplished using a VPN Tunnel using IPSec. IPSec uses encryption and authentication to secure potentially sensitive data across a public medium. Host to host communication can be encrypted using IPsec as well.

Key points to consider:
- It is critical that subnets for the Client and Server are not the same
- In this case the client is 192.168.0.x and the Server is 192.168.1.x
- Also, ensure the Gateway addresses are configured correctly
- Beside the addresses in the IPSEC configuration, almost all other parameters should be the same for both client and server (beside
being client and server)

- Multiple clients can be added to the system
- Other VPN tunnel types are available

**Required Software:**
Web Browser

**Required Firmware:**
3.20/4.20

**Procedure:**

**Part 1 – IPSEC Server Setup**

1. Log into the SN/RAM Web Browser
   - Type the device’s LAN/WAN IP, port 10000 into a web browser
   - **User Name**: admin
   - **Password**: Last six digits of the device’s serial number

2. Navigate to Networking → Tunneling (VPN) Settings → IPSEC → Configuration

3. Enable IPSEC by selecting **Yes** from the drop-down list

4. Click Add
5. Add a name for the Tunnel (must be alphanumeric)
6. Select Server from the Tunnel Type drop-down list
7. Select Hold from the Dead Peer Detection Action drop-down list
8. Click Next
9. Choose desired **Encryption** and **Authentication** settings for **Phase 1** and **Phase 2**
10. Add text into the **Pre-Shared Key** (should be non-dictionary word)
11. Click **Next**
12. Enter IP address of **Eth0** of **IPSec Server** in **Local Source IP**
13. Enter IP address of **subnet** of **Eth0** in **Local Private Subnet**
14. Enter IP address of **subnet** of **Eth0** of **Client** (must be in CIDR Notation)
15. Click **Finish**
16. Click **Apply**

**Part 2 – IPSEC Client Setup**
1. Log into the SN/RAM Web Browser
   a. Type the device’s LAN/WAN IP, port 10000 into a web browser
   b. **User Name:** admin
   c. **Password:** Last six digits of the device’s serial number
2. Navigate to **Networking → Tunneling (VPN) Settings → IPSEC → Configuration**
3. **Enable IPSEC** by selecting **Yes** from the drop-down list
4. Click Add

5. Add a name for the Tunnel (must be alphanumeric)
6. Select Client from the Tunnel Type drop-down list
7. Select Restart from the Dead Peer Detection Action drop-down list
8. Click Next
9. Choose desired **Encryption** and **Authentication** settings for **Phase 1** and **Phase 2**
10. Add text into the **Pre-Shared Key** (should be non-dictionary word and must match Server Key)
11. Click **Next**
12. Enter IP address of Eth0 of IPSec Client in Local Source IP
13. Enter subnet of Eth0 in Local Private Subnet (must be in CIDR Notation)
14. Enter Public IP address of Server
15. Enter subnet of Eth0 of Server (must be in CIDR Notation)
16. Click Finish
17. Click Apply

IPSEC is now configured
Verify that IPSec Tunnel Status displays UP (can take up to 60 seconds to connect, may need to click Refresh)
Part 3 – Testing IPSEC tunnel
Verify the IPSec tunnel is “alive”

1. Using a browser, connect to the IPSEC Server (192.168.1.10)
2. Navigate to Status → Diagnostic Tools → Ping.
   
   **Note:** Using this method (IP Addresses selected) will ensure your testing the VPN Tunnel.

   **Note:** Pinging the WAN address will simply verify that the Cellular device is online (and not actually check the VPN tunnel).
Topology:

![IPSec Tunnel Diagram]

Server Side
1a. Public IP Address
2a. Eth0 IP Address
3a. Eth0 Subnet Mask
4a. Controller 2 IP
5a. Controller 2 Subnet Mask
6a. Controller 2 Gateway

Client Side
1b. Public IP Address
2b. Eth0 IP Address
3b. Eth0 Subnet Mask
4b. Controller 1 IP
5b. Controller 1 Subnet Mask
6b. Controller 1 Gateway

Disclaimer:
It is the customer's responsibility to review the advice provided herein and its applicability to the system. Red Lion Controls makes no representation about specific knowledge of the customer's system or the specific performance of the system. Red Lion is not responsible for any damage to equipment or connected systems. The use of this document is at your own risk. Red Lion standard product warranty applies.

For more information: [http://www.redlion.net/support/policies-statements/warranty-statement](http://www.redlion.net/support/policies-statements/warranty-statement)