How to Create a TINA VPN Tunnel between Barracuda NG Firewalls

https://campus.barracuda.com/doc/41116248/

Use the TINA protocol for VPN connections between two Barracuda NG Firewalls The TINA protocol offers many advantages:

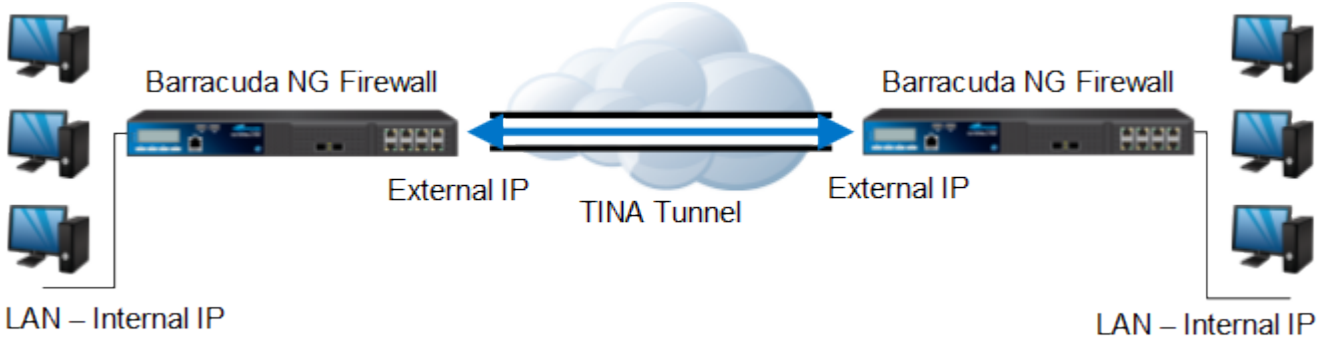
- Modified initial handshake with the intention to improve denial-of-service protection for x.509 digital certificate based authentication.
- Multiple encapsulation transports (ESP, UDP, TCP and TCP/UDP hybrid mode).
- Multiple transport paths for a logical tunnel for improved traffic distribution across multiple links and enhanced protection against line failure.
- Heartbeat monitoring of the tunnel status for failover action.
- Continual bandwidth and throughput evaluation.
- Immunity to intermittent NAT devices or proxies (HTTPS, SOCKS) on the way between two tunnel endpoints.

The following article provides you with instructions on how to create a TINA VPN tunnel between Barracuda NG Firewall:

In this article:

Example Environment

This example configuration uses default VPN settings and IP addresses for the networks that are illustrated in the following figure:



IP Address	Location 1	Location 2
Management IP	10.10.10.1	10.10.20.1
Local Area Network	10.10.10.0/24	10.10.20.0/24
External IP	212.86.0.253	213.47.0.253

Tunnel Setting	Location 1	Location 2
Transport	UDP	UDP
Encryption	AES	AES
Authentication	MD5	MD5

The following sections use the default transport, encryption, and authentication settings. For more detailed information, see TINA Tunnel Settings.

Configure the TINA Tunnel at Location 1

For the Barracuda NG Firewall at Location 1, configure the network settings and export the public key.

1. Log into the Barracuda NG Firewall at Location 1.
2. Open the **Site to Site** page (**Config > Full Config > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service**)
3. Click **Lock**.
4. Click the **TINA Tunnels** tab.
5. Right-click the table and select **New TINA tunnel**.
6. In the **Name** field, enter the name for the new VPN tunnel.
7. Configure the local and remote networks.
    1. Click the **Local Networks tab** and enter the network address of Location 1. For example, enter `10.10.10.0/24` into the **Network Address** field and then click **Add**.
    2. Click the **Remote Networks** tab and enter the network address of Location 2. For example, enter `10.10.20.0/24` into the **Remote Network** field and then click **Add**.
    3. Click the **Local** tab and enter the external IP address of Location 1. You can select **First Server IP**, **Second Server IP**, or **Dynamic**. You can also explicitly enter an IP address. For example, select **Explicit List** from the **IP Address or Interface used for Tunnel Address** list, enter `212.86.0.253`, and then click **Add**.
    4. Click the **Remote** tab and enter the external IP address or FQDN of Location 2 and then click **Add**. E.g., `213.47.0.253` or `vpnloc2.yourdomain.com`
8. Export the public key to the clipboard.
    1. Click the **Identify** tab.
    2. From the **Identification Type** list, select **Public Key**.
    3. Click **Ex/Import** and select **Export Public Key to Clipboard**.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Create the TINA Tunnel at Location 2

1. Log into the Barracuda NG Firewall at Location 2.
2. Open the **Site to Site** page (**Config > Full Config > Box > Virtual Servers > *your virtual server*** **> Assigned Services > VPN-Service**).
3. Click **Lock**.
4. Click the **TINA Tunnels** tab.
5. Right-click the table and select **New TINA tunnel**.
6. In the **Name** field, enter the name for the new VPN tunnel.
7. Configure the local and remote networks.
    1. Click the **Local Networks** tab and enter the network address of Location 2. For example, enter `10.10.20.0/24` into the **Network Address** field and then click **Add**.
    2. Click the **Remote Networks** tab and enter the network address of Location 1. For example, enter `10.10.10.0/24` into the **Remote Network** field and then click **Add**.
    3. Click the **Local** tab and enter the external IP address of Location 2. You can select **First Server IP**, **Second Server IP**, or **Dynamic**. You can also explicitly enter an IP address. For example, select **Explicit List** from the **IP Address or Interface used for Tunnel Address** list, enter `213.47.0.253`, and then click **Add**.
    4. Click the **Remote** tab and enter the external IP address or FQDN of Location 1 and then click **Add**.E.g., `212.86.0.253` or `vpnloc1.yourdomain.com`
8. Import the public key from Location 1.
    1. Click the **Peer Identification** tab.
    2. Click **Ex/Import** and select **Import from Clipboard**.
9. Export the public key for Location 2 to the clipboard.
    1. Click the **Identify** tab.
    2. From the **Identification Type** list, select **Public Key**.
    3. Click **Ex/Import** and select **Export Public Key to Clipboard**.
10. Click **OK**.
11. Click **Send Changes** and **Activate**.

Import the Public Key for Location 1

The TINA VPN tunnel is not activated until the public key of Location 2 is imported to Location 1.

1. Log into the Barracuda NG Firewall at Location 1.
2. Open the **Site to Site** page (**Config > Full Config > Box > Virtual Servers > *your virtual server*** **> Assigned Services > VPN-Service**).
3. Click **Lock**.
4. Open the configuration for Location 1.
5. Click the **Peer Identification** tab.
6. Click **Ex/Import** and select **Import from Clipboard**.
7. Click **OK**.
8. Click **Send Changes** and **Activate**.

After configuring the TINA VPN tunnel on both Barracuda NG Firewalls, you must also create a firewall rule

on both systems to allow access to their LANs.

Next Step

Create access rule to allow traffic in and out of your VPN tunnel: How to Create Access Rules for TINA Site-to-Site VPN Access.

Figures

1. tina_tunnel.png