How to Activate Forward Error Correction

https://campus.barracuda.com/doc/96026172/

Before You Begin

- Ensure you have understood the concept of FEC on a CGF/CGW. For more information, see Forward Error Correction (FEC) in TINA Tunnels.

Basic Requirements for Using FEC on a CGF/CGW

- Both peers must operate firewall firmware version 8.2.0 or higher.
- FEC is only available for TINA/UDP tunnels.
- FEC can be configured on both peers of a TINA transport.
- Dynamic Bandwidth Detection must be enabled on the transport.
- The FEC level stands for a certain number of repair packets that are added to the UDP data stream. The error correction level must be configured on both peers, but each peer can have a different level.

  When changing the FEC level, you must restart the transport.
- The maximum size of repair packets is limited and depends on the MTU of the VPN device.

  Do not change the MTU for the VPN unless you know exactly what you are doing!
  If the MTU of the VPN device is increased, the FEC will not work for packets larger than the hard-coded MTU.

How to Configure Forward Error Correction

The following example describes a scenario with the settings for 2 peers.

Replace these IP addresses so that they match your requirements.

- 1st peer: Public IP: 123.234.0.1
  - LAN IP: 192.168.0.0/24
  - Shared IP for LAN: 192.168.0.1
- 2nd peer: Public IP: 123.234.1.1
  - LAN IP: 192.168.1.0/24
  - Shared IP for LAN: 192.168.1.1

Step 1. Configure FEC on the Transport Level

Complete the following steps for both peers!

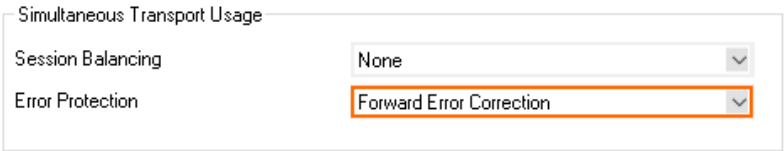
1. Configure Shared Networks and IPs.
    1. Go to **CONFIGURATION -> Configuration Tree -> Box -> Network -> IP Configuration**, section **Shared Networks and IPs**.
    2. Add the local network from the first peer to the list.
2. Configure the TINA tunnel.
    1. Go to **CONFIGURATION -> Configuration Tree -> Box -> Assigned Services -> VPN -> Site-to-Site**.
    2. Right-click the main view area.
    3. Select **New TINA tunnel...** from the list.
    4. In the **Basics** tab, configure the TINA tunnel according to your requirements.
    5. In the **SD-WAN - Bandwidth Protection** tab, set **Dynamic Bandwidth Detection** to **Active Probing and Passive Monitoring**.
    6. For **FEC level**, the recommended standard setting is **Medium**. Adjust this value to your requirements.
3. In the **Local Networks** tab:
    1. Set **Call Direction**. At least one of the firewalls must be active. In this example, select **Active**.
    2. Add the IP address of the local network interface: 192.168.0.1.
4. In the **Local** tab, configure the public IP address: 123.234.0.1
5. In the **Remote Networks** tab, add the network address of the remote LAN: 192.168.1.0/24
6. In the **Remote** tab, enter `123.234.1.1`
7. In the **Identity** tab, ensure that there is a public key present.
    1. Export the public key to a file.
8. Ensure that you have exported the public key from the complementary peer into a file.
    1. In the **Peer Identification** tab, import the public key from a file exported on the complementary peer.

Step 2a. (optional) Configure FEC on a Session Level for an Access Rule

On a session level for an access rule, you must either configure a **Connection Object** for FEC or create a new one. In both cases, the value for **Error Correction** must be configured with the same value.

This example assumes that an appropriate connection object is already present.

1. Go to **CONFIGURATION -> Configuration Tree -> Box -> Assigned Services -> Firewall -> Forwarding Rules -> Connections**.
2. Click **Lock**.
3. In the main view area, double-click the corresponding connection object.
4. The **Edit / Create a Connection Object** window is displayed.
5. In the section **SD-WAN VPN Settings**, click **Edit/Show...** .
6. In the section **Simultaneous Transport Usage**, select **Forward Error Correction** for **Error Protection**.

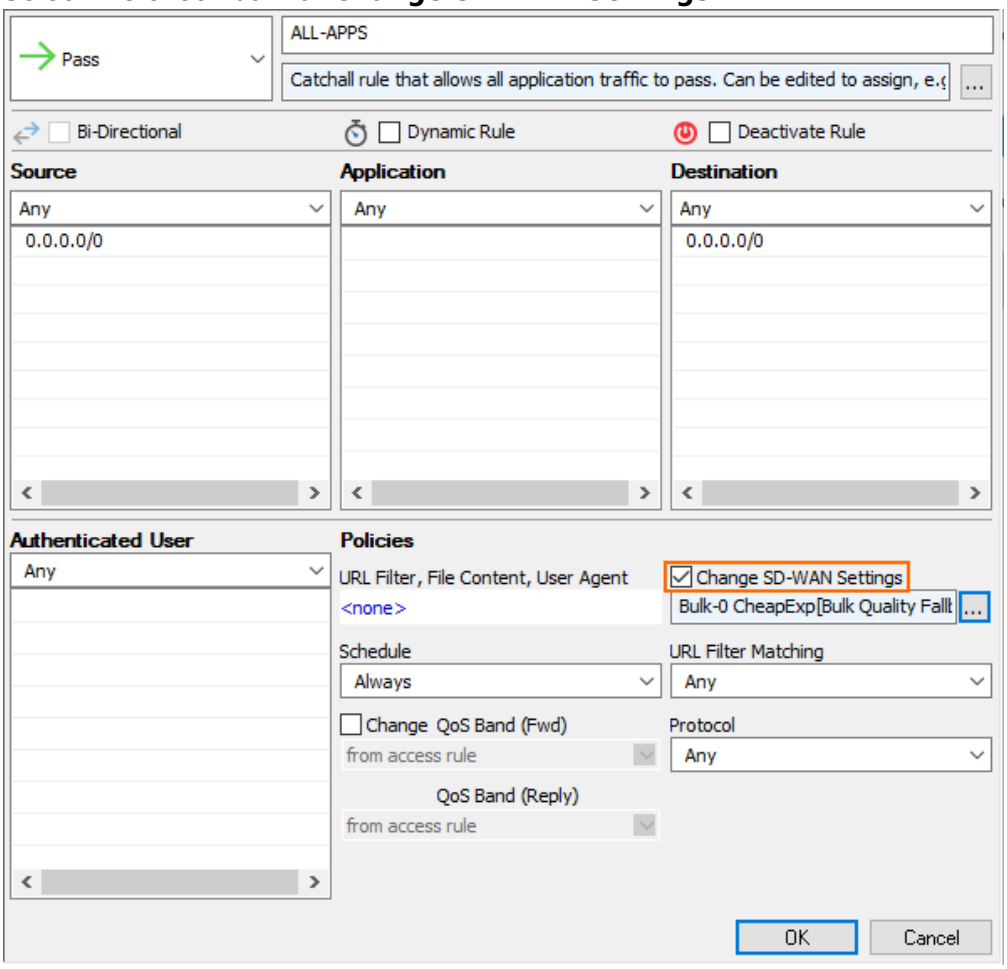


7. Click **OK**.
8. Click **OK**.
9. Click **Send Changes / Activate**.

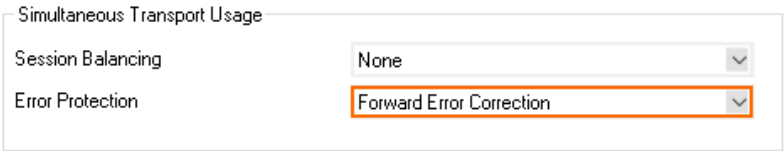
Step 2b. (optional) Configure FEC on a Session Level for an Application Rule

You can override the settings for an application rule by performing the following steps:

1. Go to **CONFIGURATION -> Configuration Tree -> Box -> Assigned Services -> Firewall -> Forwarding Rules -> Application Rules**.
2. In the main view area, double-click the application rule that you want to override.
3. The window **Edit Rule** is displayed.
4. Select the check box for **Change SD-WAN Settings**.



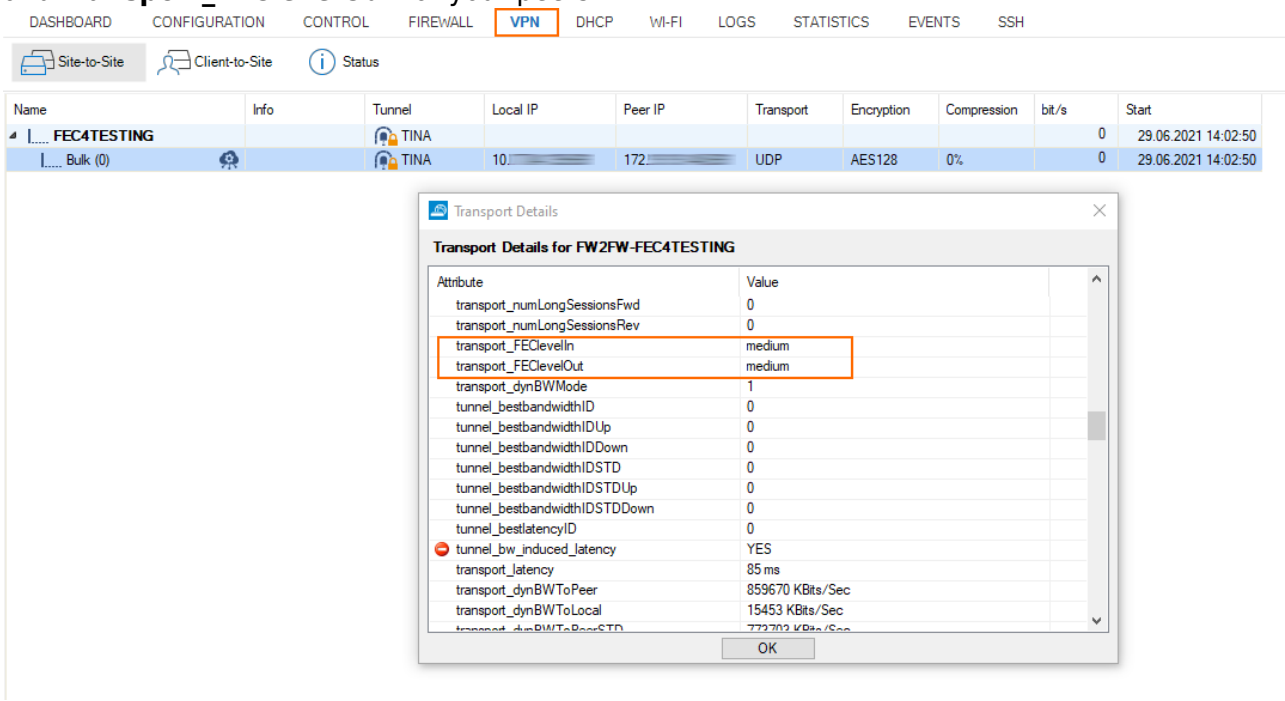
5. Click the **'...'** button.
6. The **SD-WAN Settings** window is displayed.
7. In the section **Simultaneous Transport Usage**, select **Forward Error Correction** for **Error Protection**.



8. Click **OK**.
9. Click **Send Changes / Activate**.

Step 3. Check the Transport Details for Your Configuration.

1. Go to **VPN -> Site-to-Site**.
2. Double-click the transport for which you have configured FEC.
3. The **Transport Details** window is displayed.
4. In the list, locate the two entries with the name **transport_FEClevelIn** and **transport_FEClevelOut** for your peers.



Figures