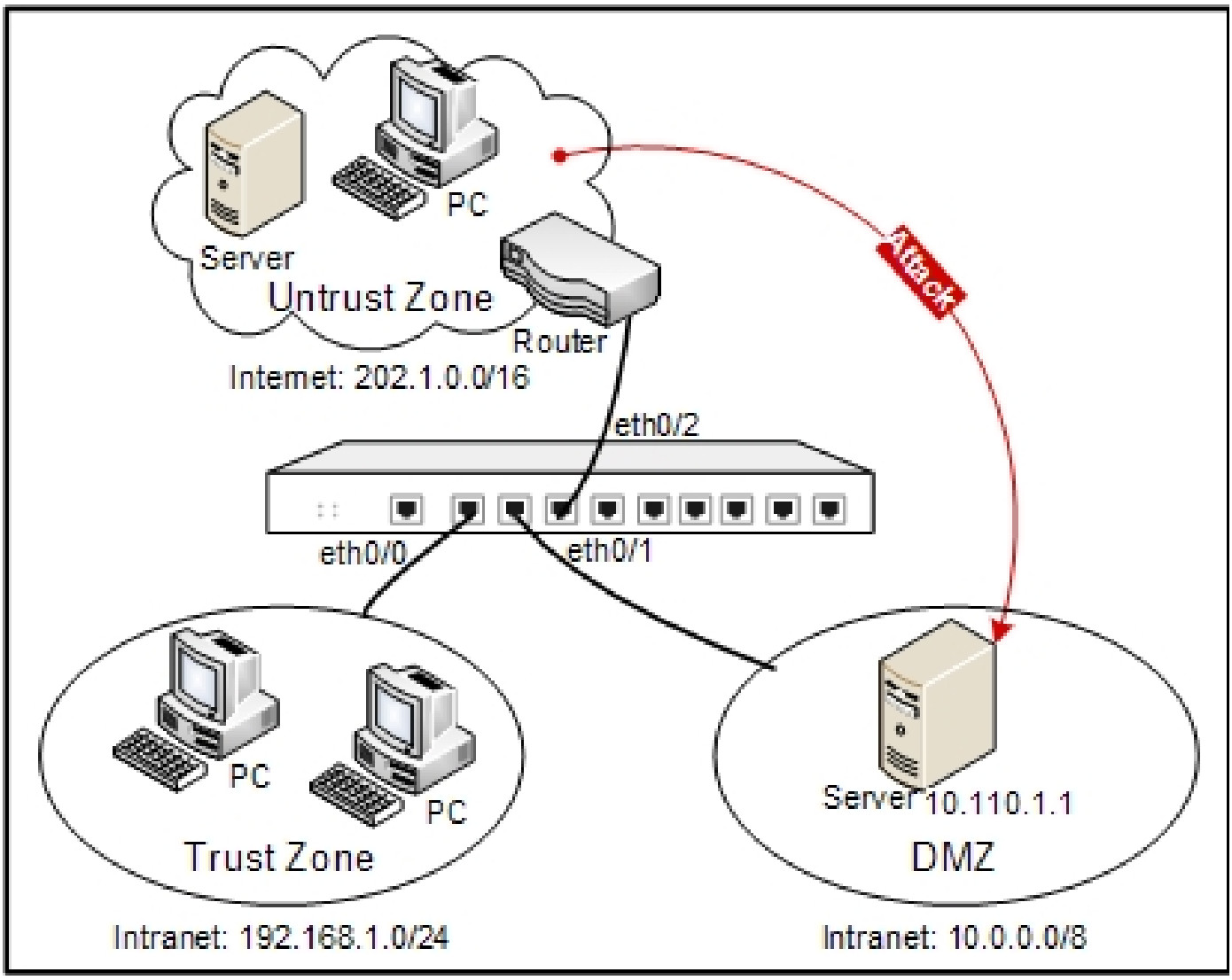
Land Attack Defense Configuration Example

This section describes a Land attack defense configuration example.

Ethernet 0/0 is bound to the trust zone, ethernet 0/2 is bound to the untrust zone, and ethernet 0/1 is bound to the DMZ zone. Protect the server in the DMZ zone against Land attacks.

The defense networking topology is shown as follows:



Take the following steps:

Step 1: Configure ethernet0/0, ethernet0/2 and ethernet0/1.

1. On the Navigation pane, click **Configure** > **Network** > **Network** to visit the Network page.
2. Select **ethernet0/0** from the interface list, and click **Edit**. In the Interface Configuration dialog, configure the options as below:
    - **Name**: ethernet0/0
    - **Binding zone**: Layer 3 zone
    - **Zone**: Select **trust** from the **Zone** list.

3. Click **OK** to save the changes and return to the main page.
4. Select **ethernet0/2** from the interface list, and click **Edit**. In the Interface Configuration dialog, configure the options as below:
    - **Name**: ethernet0/2
    - **Binding zone**: Layer 3 zone
    - **Zone**: Select **untrust** from the drop-down list.
    - **Type**: Static IP
    - **IP address**: 202.1.0.1
    - **Netmask**: 24
6. Click **OK** to save the changes and return to the main page.
7. Select **ethernet0/1** from the interface list, and click **Edit**. In the Interface Configuration dialog, configure the options as below:
    - **Name**: ethernet0/1
    - **Binding zone**: Layer 3 zone
    - **Zone**: Select **dmz** from the drop-down list.
    - **Type**: Static IP
    - **IP**: 10.0.0.1
    - **Netmask**: 8
6. Click **OK** to save the changes and return to the main page.

Step 2: Configure a policy rule.

1. On the Navigation pane, click **Configure** > **Security** > **Policy** to visit the Policy page.
2. Click **New**. On the **Basic** tab in the Policy Configuration dialog, configure the options as below:
    - **Src zone**: untrust
    - **Dst zone**: dmz
    - **Src address**: Any
    - **Dst address**: Any
    - **Service**: Any
    - **Action**: Permit
3. Click **OK** to save the settings and return to the main page.

Step 3: Enable Land attack defense for the untrust zone.

1. On the Navigation pane, click **Configure** >**Security** > **Attack Defense** to visit the Attack Defense page.
2. Select **untrus**t from the **Zone** drop-down list.
3. In the Denial of service defense section, select the **Land attack** check box to enable Land attack defense, and select **Drop** from the **Action** drop-down list.
4. Click **OK** to save the changes and return to the main page.

Step 4: Test the Land attack defense configured for the server. Craft a packet with identical source and destination IP address, and send it to 10.110.1.1. The device will detect a Land attack, and then give an alarm and drop the packet.