## Hirschmann Address Mapping

Hirschmann Address Mapping allows you to establish an unlimited number of networks with identical IP address ranges which are connected via VPN with a public network and clearly distinguishable from the public network.

- The individual networks' identical address ranges simplify the porting of their configuration.
- Their distinguishability from the common network facilitates the unambiguous administration.

You can use the Hirschmann Address Mapping, for example, to centrally administer multiple production cells.
The Firewall with Hirschmann Address Mapping allows you to replace the internal IP addresses with external valid and distinct IP addresses for the VPN connection. Hirschmann Address Mapping works like a 1:1 NAT router integrated in the VPN connection. The Firewall provides outgoing data packets from a definable address range with a new return address - the Firewall thus maps the internal return address to an valid external address. The Firewall automatically supplies incoming data packets with the valid internal destination address. This assignment is reversibly unique.

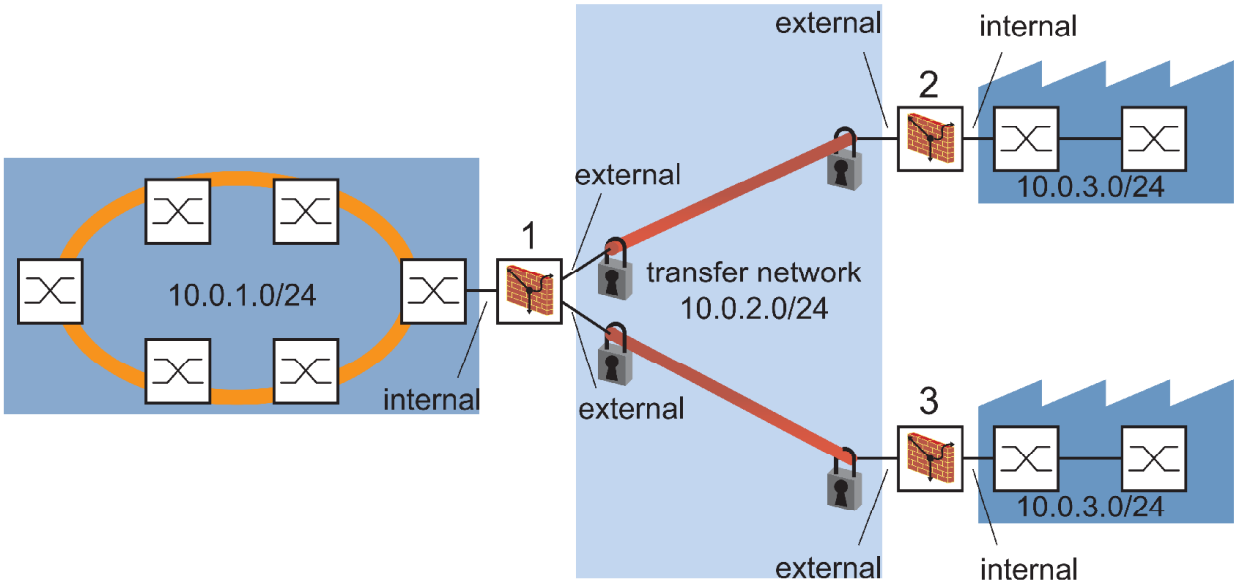


*Figure 40: Addressing several identical subnetworks from a public network (Hirschmann Address Mapping)*

The following is known:

| Parameter | Firewall 1 | Firewall 2 | Firewall 3 |
|---|---|---|---|
| IP address of internal port | 10.0.1.201 | 10.0.3.201 | 10.0.3.201 |
| IP address of external port | 10.0.2.1 | 10.0.2.2 | 10.0.2.3 |
| Pre-shared key | 456789defghi | 456789defghi | 456789defghi |
| Start IKE mode as | Initiator | Responder | Responder |
| IP parameters of the networks to be connected | 10.0.1.0/24 | 10.0.3.0/24 | 10.0.3.0/24 |
| Mapped IP parameter from the network | - | 10.0.4.0/24 | 10.0.5.0/24 |

*Table 14: Interface settings for Hirschmann Address Mapping on the participating firewalls*

For the routing of the firewall 1 set the IP networks for every VPN connection in the dialog `VPN:Connections` and in the tab page `IP Networks` according to the following table:

| VPN-name | Index | Source Address (CIDR) | Destination Adress (CIDR) | Description |
|---|---|---|---|---|
| Production control-production hall 1 | 1 | 10.0.1.0/24 | 10.0.4.0/24 | FW 1 to FW 2 |
| Production control-production hall 2 | 1 | 10.0.1.0/24 | 10.0.5.0/24 | FW 1 to FW 3 |

*Table 15: VPN routing settings for Hirschmann Adress Mapping on the firewall of the production control*

For the address mapping of firewalls 2 and 3, set the IP networks in the dialog `VPN:Connections` and in the tab page `IP Networks` according to the following table:

| Firewall | Index | Source address (CIDR) | Destination address (CIDR) | Mapped source address (CIDR) | Description |
|---|---|---|---|---|---|
| 2 | 1 | 10.0.3.0/24 | 10.0.1.0/24 | 10.0.4.0/24 | FW 2 to FW 1 |
| 3 | 1 | 10.0.3.0/24 | 10.0.1.0/24 | 10.0.5.0/24 | FW 3 to FW 1 |

*Table 16: VPN routing settings for Hirschmann Address Mapping on the firewall of the production networks*

**Note:** In the “Mapping destination address (CIDR)” column, no entry is required.

Prerequisites for further configuration:
- The VPN parameters are configured on the 3 devices.
- The IP parameters of the Firewall router interface are configured.
- The devices in the internal network have the IP address of the internal interface (port 1) of the respective Firewall as their gateway.

☐ Create the routing for Firewall 2 on Firewall 1.

☐ Select the dialog `Virtual Private Network:Connections`.
☐ Select the connection with the name “Production control production hall 1” and click on “Edit”.
☐ Select the IP “Networks” tab page. The device shows an empty table.
☐ Click on “Create entry” to create a new line.
☐ In the 1st line, enter:
- “Source address (CIDR)”, `10.0.1.0/24`
- “Destination address (CIDR)”, `10.0.4.0/24` (mapped network)
- “Description”, `FW 1 to FW 2`

☐ Click on “Write” to temporarily save the data.
☐ Click on “Back” to return to the `Virtual Private Network Connections` dialog.

☐ Create the routing for Firewall 3 on Firewall 1.

☐ Select the connection with the name “Production control production hall 2” and click on “Edit”.
☐ Select the IP “Networks” tab page. The device shows an empty table.
☐ Click on “Create entry” to create a new line.
☐ In the 1st line, enter:
- “Source address (CIDR)”, `10.0.1.0/24`
- “Destination address (CIDR)”, `10.0.5.0/24` (mapped network)
- “Description”, `FW 1 to FW 3`

☐ Click on “Write” to temporarily save the data.
☐ Click on “Back” to return to the `Virtual Private Network Connections` dialog.

☐ Save your settings.

☐ Click on “Write” to temporarily save the data.
☐ Open the `Basic Settings:Load/Save` dialog.
☐ Click on “Save to NVM + ACA” to permanently save the data.

☐ Create the address mapping for the Firewall 2.

☐ Select the dialog `Virtual Private Network:Connections`.
☐ Select the connection with the name “Production control production hall 1” and click on “Edit”.
☐ Select the IP “Networks” tab page. The device shows an empty table.
☐ Click on “Create entry” to create a new line.
☐ In the 2nd line, enter:
- “Source address (CIDR)”, `10.0.3.0/24`
- “Destination address (CIDR)”, `10.0.1.0/24`
- “Mapping source address (CIDR)”, `10.0.4.0/24`
- “Description”, `FW 2 to FW 1`

☐ Click on “Write” to temporarily save the data.
☐ Click on “Back” to return to the `Virtual Private Network Connections` dialog.
☐ Click on “Write” to temporarily save the data.
☐ Open the `Basic Settings:Load/Save` dialog.
☐ Click on “Save to NVM + ACA” to permanently save the data.

☐ Create the routing for Firewall 3.

☐ Select the dialog `Virtual Private Network:Connections`.
☐ Select the connection with the name “Production control production hall 2” and click on “Edit”.
☐ Select the IP “Networks” tab page. The device shows an empty table.
☐ Click on “Create entry” to create a new line.
☐ In the 2nd line, enter:
- “Source address (CIDR)”, `10.0.3.0/24`
- “Destination address (CIDR)”, `10.0.1.0/24`
- “Mapping source address (CIDR)”, `10.0.5.0/24`
- “Description”, `FW 3 to FW 1`

☐ Click on “Write” to temporarily save the data.
☐ Click on “Back” to return to the `Virtual Private Network Connections` dialog.
☐ Click on “Write” to temporarily save the data.
☐ Open the `Basic Settings:Load/Save` dialog.
☐ Click on “Save to NVM + ACA” to permanently save the data.