Setting the firewall for LAN and DMZ

Router Version	Centro Business 1.0 Centro Business 2.0 Centro Business 3.0
Doc. Version	3.0
Status	Final
update	01.2023

Centro Business
Configuration instructions

Swisscom (Schweiz) AG
3050 Bern

swisscom

Contents

Setting the firewall for LAN and DMZ

1.1 Need

You wish to restrict Internet traffic to and from your customers' LAN / DMZ to protect your infrastructure and data.

1.2 Description

In the Centro Business Router, there are two independent firewalls available for customers' LAN and DMZ. For each firewall, you can choose between two predefined filter sets, and you have the option to set up your own filters or to disable the firewall. Different filter sets can be created for inbound and outbound traffic.

1.3 Requirements/limitations

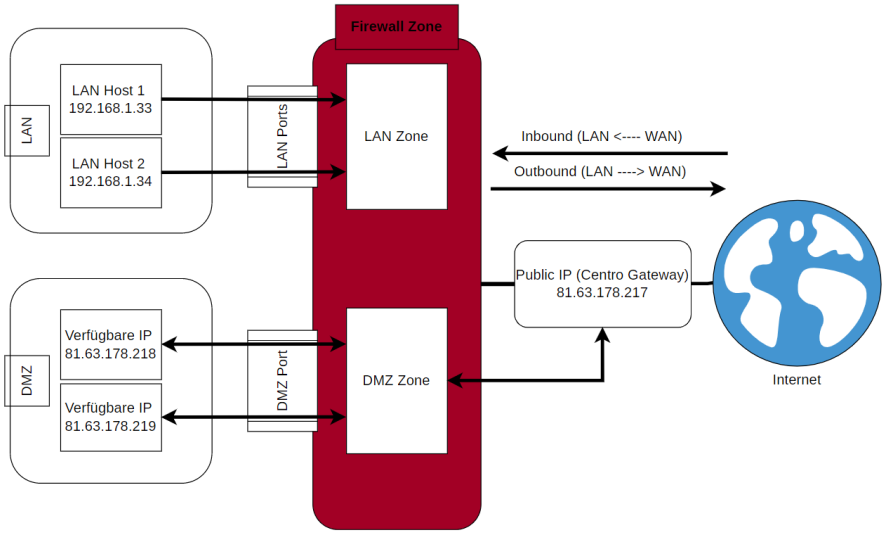
Requirements:

- Swisscom Contract: My SME Office, Business Internet Services, Business Internet Light, Enterprise Connect XS or Internet for private customers
- Centro Business with current firmware version. You can find the firmware on the official Centro Business help page under Update Firmware
- Access to the router portal is established

Limitations:

- If the customer does not use fixed IP addresses or has not enabled DMZ, only the LAN firewall will be displayed.
- BNS Service is enabled in the bundle.

1.4 Illustration



1.5 Basic settings (LAN and DMZ packet filter)

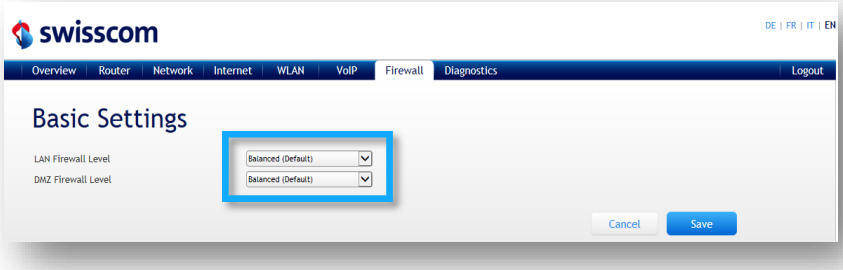
The firewall settings shown in **Settings, Firewall, Basic Settings** will depend on the connection or the use of any fixed IP addresses. If no fixed public IP addresses have been subscribed to or DMZ is not enabled, only the LAN firewall will be displayed. When DMZ is enabled, both the LAN and DMZ firewall is displayed.

The following filter sets can be selected for each firewall.

- **Balanced** (Default): In this operating mode, the firewall forwards all outgoing and incoming data traffic from and to LAN or DMZ except for a defined set of protocols.
- **Strict**: The firewall blocks incoming traffic to LAN or DMZ except for a few ports used for router management. With regard to outgoing traffic from the customer's LAN or DMZ, only a small set of ports is blocked.
- **Custom**: All incoming traffic for both IPv4 and IPv6 addresses to the customer's LAN is blocked. All outgoing traffic from the customer's LAN is allowed through.
- **Off**: The firewall is turned off. Both incoming and outgoing connections to and from the customer's LAN or DMZ are being allowed through.

Generally:
Avoid that your firewall is/will be set to "OFF" on the Centro Business. In this case, unnoticed connections or attacks can overload your system.

Under the tabs "**LAN firewall rules**" and "**DMZ firewall rules**" you can see the actual blocks for each service or port.



Q1.2023 NEW:

The HTTPS Port TCP:443 is dropped (Drop) inbound for the Firewall Level "Balanced (Default)"

Rule setting for LAN and DMZ Firewall					
Service	Destination Port	Inbound Rule	Outbound Rule	Balanced (Default)	Strict
Kerberos TCP	TCP:88	drop	reject	✓	✓
Kerberos UDP	UDP:88	drop	reject	✓	✓
Internet Printing Protocol	TCP:631	drop	reject	✓	✓
Simple Service Discovery Protocol TCP	TCP:2869	drop	reject	✓	✓
Simple Service Discovery Protocol UDP	UDP:1900	drop	reject	✓	✓
UPnP	UDP:3702	drop	reject	✓	✓
Sun RPC	TCP:111	drop	reject	✓	✓
Microsoft RPC	TCP:135	drop	reject	✓	✓
mDNS	UDP:5353	drop	reject	✓	✓
NetBIOS	TCP:139	drop	reject	✓	✓
Microsoft SMB	TCP:445	drop	reject	✓	✓
Remote Login	TCP:513	drop	reject	✓	✓
Remote Shell	TCP:514	drop	reject	✓	✓
Apple Filing Protocol	TCP:548	drop	reject	✓	✓
Link-Local Multicast Name Resolution	UDP:5355	drop	reject	✓	✓
Secure Shell (SSH)	TCP:22	drop	accept	✓	
Telnet	TCP:23	drop	accept	✓	
HTTP	TCP:80	drop	accept	✓	
HTTPS	TCP:443	drop	accept	✓	
Microsoft RDP	TCP:3389	drop	accept	✓	
VNC	TCP:5900	drop	accept	✓	
Default Policy	all packets	accept	accept	✓	
Default Policy	all packets	drop	accept		✓

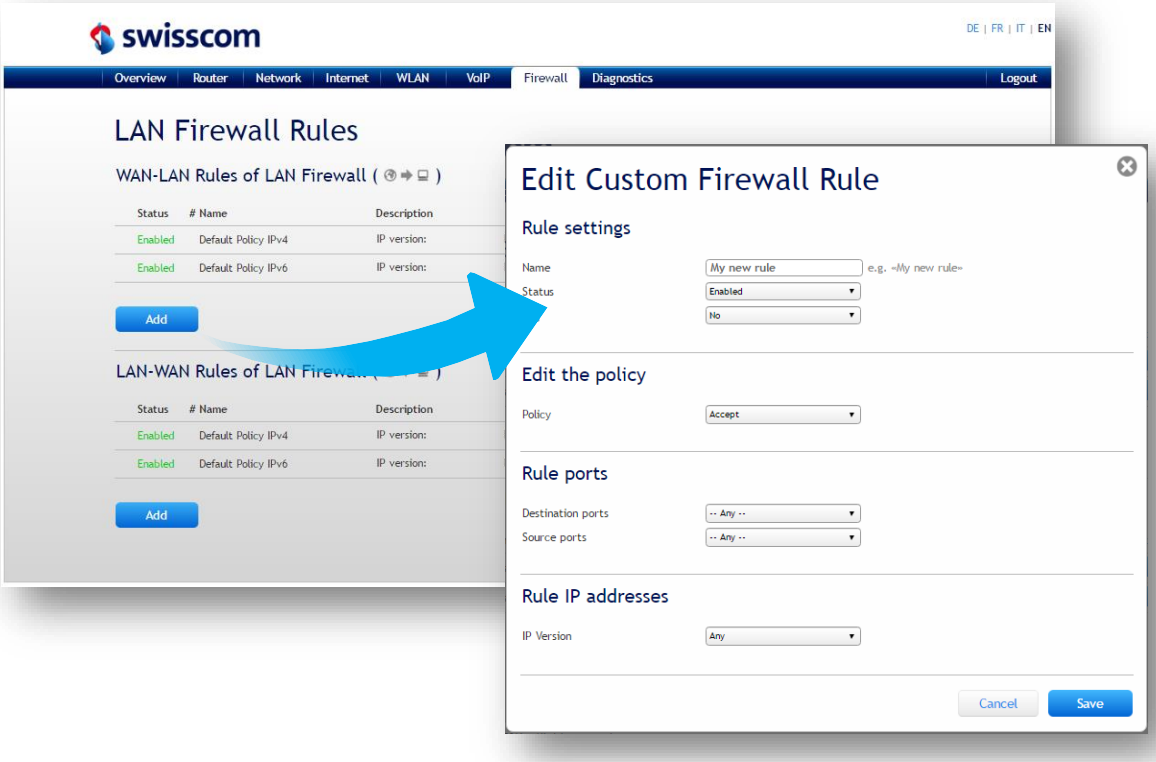
Rule setting for DMZ Firewall only					
Block List "Balanced" Setting	Destination Port	Inbound Rule	Outbound Rule	Balanced (Default)	Strict
TO LAN	all packets	drop	drop	✓	✓

1.6 Add / edit filter rules

When the basic setting for the LAN or DMZ firewall level is set to "**Custom**", you can create and edit your own rules for the relevant firewall. Here, you can select either incoming Internet traffic to the customer's LAN or DMZ or outgoing Internet traffic from the customer's LAN or DMZ. Select the **Add** button under **LAN firewall rules** or **DMZ firewall rules**, WAN-LAN rules or LAN-WAN to define the relevant rule.

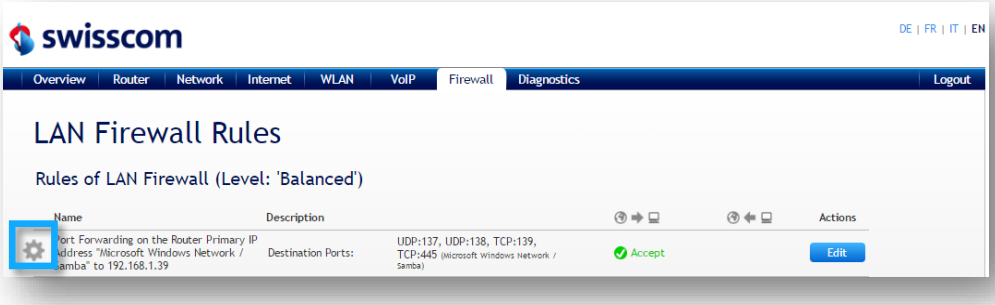
Each filter rule consists of the following data elements.

- Name (can be individually chosen)
- Status (enabled/disabled)
- Logs (yes/no)
- Policies (accept or reject)
- Destination ports (single port or port range, or several ports or ranges)
- Source ports (single port or port range, or several ports or ranges)
- IP Version (any, IPv4 or IPv6)
- Destination criterion type (IPv4 or IPv6) any address/single address, subnet, address range
- Source criterion type (IPv4 or IPv6) any address/single address, subnet, address range
- Exclusive flag (exclusion)



1.7 Automatically generated filter rules

If port forwarding is set up on the router's IP address or a fixed public IPv4 address, a filter rule is entered in the LAN firewall automatically. Once set, this rule cannot be edited or deleted. The adjustments can be performed: IP Version, source address and exclusive flag (exclusion). An automatically generated rule will be specially marked.



1.8 Content filters

Specific keywords can be entered in the content filter for filtering. Please note that content set up using an encrypted connection cannot be filtered.