Firewall für LAN und DMZ einstellen

Dokument-ID	Firewall für LAN und DMZ einstellen
Version	2.0
Status	Final
Ausgabedatum	04.2017

Centro Business
Konfigurationsanleitung

Swisscom (Schweiz) AG
3050 Bern

swisscom

Inhalt

Swisscom (Schweiz) AG
3050 Bern

Firewall für LAN und DMZ einstellen

1.1 Bedürfnis

Sie möchten den Internet-Traffic vom Internet in Ihr Kunden-LAN / DMZ oder vom Kunden-LAN / DMZ ins Internet einschränken um Ihre Infrastruktur und die Daten zu schützen.

1.2 Beschreibung

Im Centro Business Router stehen Ihnen zwei unabhängige Firewall für das Kunden-LAN und die DMZ zur Verfügung. Je Firewall können Sie zwischen zwei vordefinierten Filterset und den Möglichkeiten, eigene Filter zu erstellen oder die Firewall zu deaktivieren, wählen. Filterset können für Inbound-Traffic und Outbound-Traffic separat erstellt werden.

1.3 Voraussetzung/Einschränkungen

Voraussetzungen:

- Swisscom Vertrag: Business Internet Services, My KMU Office, inOne KMU office, Business Internet Light, Enterprise Connect XS oder Internet für Privatkunden
- Centro Business 2.0 mit aktueller Firmware Version. Die Firmware finden Sie auf der offiziellen Centro Business Hilfeseite unter Firmware aktualisieren
- Der Zugriff auf das Routerportal ist hergestellt

Einschränkungen:

- Wenn der Kunde keine fixen IP-Adressen nutzt oder keine DMZ aktiviert hat, wird nur die LAN-Firewall angezeigt.
- BNS Service ist auf dem Bundle aktiviert

1.4 Abbildung

Keine

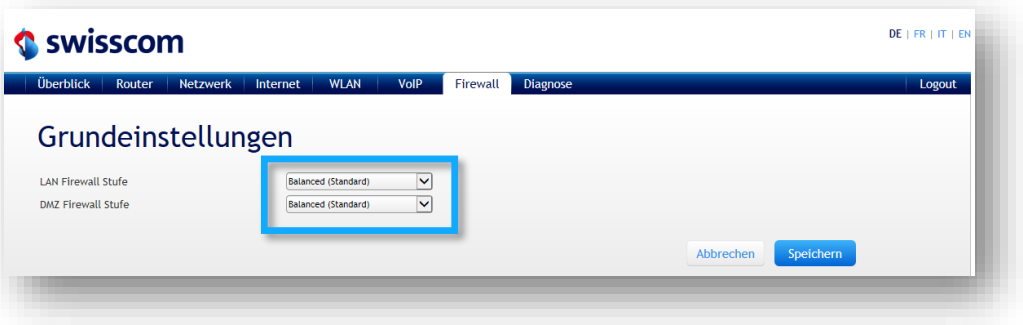
1.5 Grundeinstellungen (Paketfilter LAN und DMZ)

Je nach Anschluss oder der Nutzung allfälliger fixen IP-Adressen, werden im Menü **Firewall, Grundeinstellungen,** die Firewall Settings angezeigt. Wenn keine fixen Public-IP-Adressen abonniert sind oder wenn die DMZ nicht aktiviert ist, wird nur die LAN-Firewall angezeigt. Bei aktivierter DMZ werden sowohl die LAN- wie auch die DMZ-Firewall angezeigt.

Unter folgenden Filtersets kann je Firewall gewählt werden.

- **Balanced** (Default): In dieser Betriebsart leitet die Firewall den gesamten Datenverkehr mit Ausnahme eines definierten Satz von Protokollen aus dem LAN oder DMZ ins Internet und vom Internet ins LAN weiter.
- **Strict**: Die Firewall blockiert den Traffic vom Internet ins LAN oder DMZ bis auf wenige Ports, die für das Routermanagement genutzt werden. Vom Kunden-LAN oder der DMZ ins Internet ist nur ein kleines Set von Ports blockiert.
- **Custom**: Der gesamte Traffic für IPv4- und IPv6-Adressen werden vom Internet ins Kunden-LAN blockiert. Vom Kunden-LAN ins Internet gibt es keine Sperren.
- **Off**: Die Firewall ist ausgeschalten. Weder Verbindungen vom Internet ins Kunden-LAN oder DMZ noch Verbindungen von Kunden-LAN oder DMZ ins Internet werden geblockt.

In den Registern „**LAN-Firewall Regeln**“ und „**DMZ Firewall Regeln**“ sind die aktuellen Sperren je Service oder Port ersichtlich.

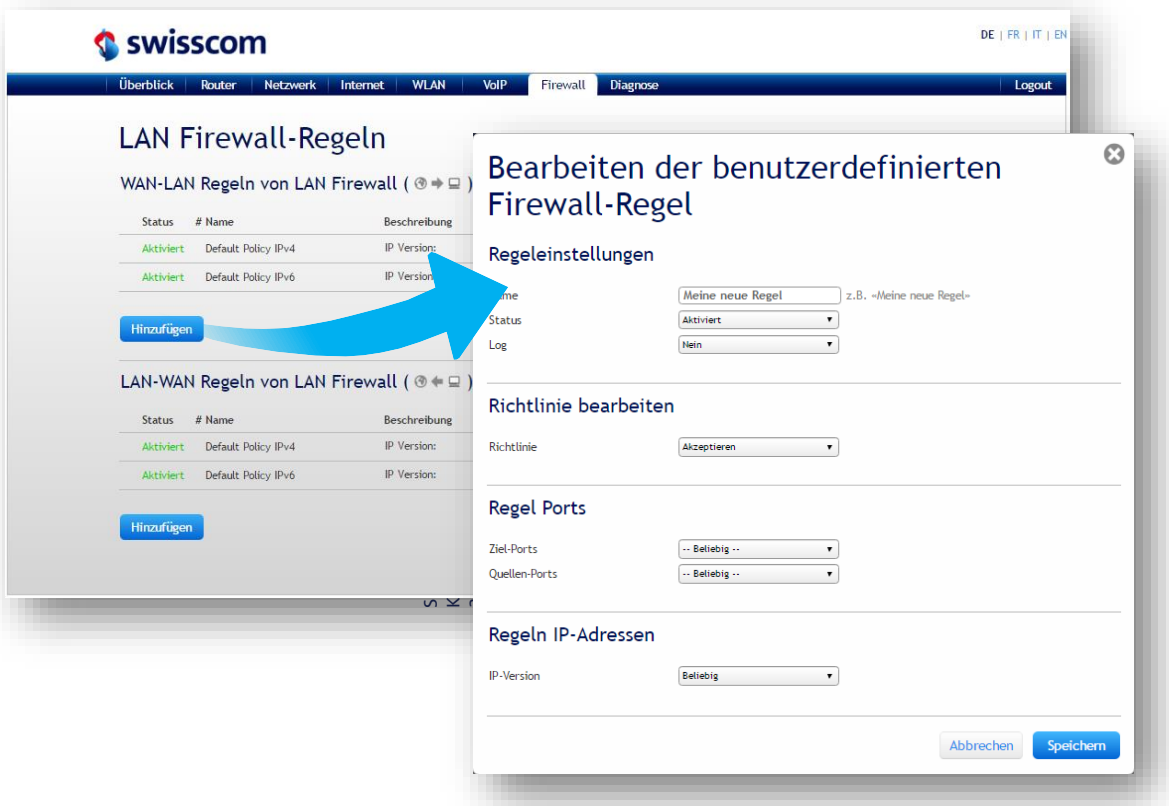


1.6 Filterregeln eintragen / anpassen

Wenn in der Firewall-Grundeinstellung für die LAN- oder DMZ-Firewall Level **„Custom“** eingestellt ist, können Sie in der entsprechenden Firewall eigene Regeln erstellen oder anpassen. Dabei können Sie zwischen Traffic vom Internet ins Kunden-LAN oder in die DMZ und vom Kunden-LAN oder aus der DMZ ins Internet unterscheiden. Wählen Sie unter **LAN Firewall Regeln** oder **DMZ Firewall Regeln**, WAN-LAN Regeln oder LAN-WAN Regeln den Button **Hinzufügen** und definieren Sie die entsprechende Regel.

Jede Filterregel besteht dabei aus folgenden Datenelementen.

- Namen (kann selber bestimmt werden)
- Status (Aktiviert/Deaktiviert)
- Logs (ja/nein)
- Richtlinien (akzeptieren oder ablehnen)
- Ziel-Ports (einzelner Port oder Port Range, oder mehrere Port oder Range)
- Quellen-Port (einzelner Port oder Port Range, oder mehrere Port oder Range)
- IP-Version (beliebig, IPv4 oder IPv6)
- Ziel Kriterium Typ (IPv4 oder IPv6) beliebige Adresse/einzelne Adresse, Subnetz, Adressbereich
- Quelle Kriterium Typ (IPv4 oder IPv6) beliebige Adresse/einzelne Adresse, Subnetz, Adressbereich
- Exclusiv-Flag (Ausschliessen)



1.7 Automatisch generierte Filterregeln

Wenn eine Port-Weiterleitung auf der Router-IP-Adresse oder einer fixen Public-IPv4-Adresse eingerichtet ist, wird automatisch eine Filterregel in die LAN-Firewall eingetragen. Die Regel kann nachträglich bearbeitet aber nicht gelöscht werden. Folgende Anpassungen sind möglich: IP-Version, Quellen-Adresse und Exclusiv-Flag (Ausschliessen) und Eine automatisch generierte Regel wird speziell gekennzeichnet.

1.8 Inhaltsfilter

Im Inhaltsfilter könne bestimmte Schlüsselwörter für eine Filterung eingetragen werden. Bitte beachte Sie, dass Inhalte, die mit einer verschlüsselten Verbindung aufgebaut werden, nicht gefiltert werden können.