Leistungsbeschreibung Secure-maxX

1 Geltungsbereich

Die LB enthält ergänzende Bestimmungen im Zusammenhang mit der Bestellung und Überlassung von Secure-maxX – Branch Firewalls durch TelemaxX.

Zusätzlich gilt die entsprechende SLA.

2 Leistungsbeschreibung

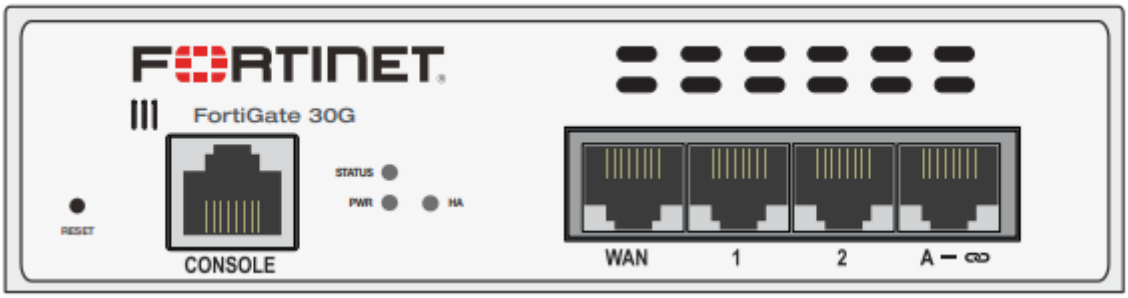
2.1 Servicevarianten

Jeder Standort hat eine dedizierte Standort ID, die bei der Bestellung automatisch vergeben wird.

Nach Absprache mit dem Kunden und im Rahmen der technischen und betrieblichen Möglichkeiten können Secure-maxX – Branch Firewalls mit folgenden Bandbreiten realisiert werden:

2.1.1 Secure-maxX – Branch 30G

Im Standard konfiguriert:



WAN (port3)

- DHCP, statisch

LAN (port1)

- Das LAN-Interface ist mit einem festen Netz konfiguriert welches Standortspezifisch einen anderen Netzbereich hat. Auf dem LAN-Interface ist ein DCHP-Server aktiv, welcher von .10-.200 IPs verteilt.
    - Bspw. Standort 1 = 10.10.**1**.0/24, Standort 2 = 10.10.**2**.0/24

DMZ/WAN2 (port2)

- Es gibt ein vorkonfiguriertes DMZ-Netz, in welchem kein DHCP vorhanden ist. Hier können Maschinen, die in ein DMZ-Netz gehören angeschlossen werden.

- In einer Dual-WAN Konfiguration ist dieser Port ein WAN-Port. Das vorkonfigurierte DMZ-Netz fällt dann weg

FortiLink (Port a)

- Der FortiLink Port ist für die Anbindung von FortiSwitchen reserviert. Über diesen wird das Protokoll FortiLink gesprochen, um FortiSwitche zu managen.

Werden Ports außerhalb ihrer vorkonfigurierten Funktion konfiguriert, ist diese Standardfunktion nicht nutzbar.
Genaue Technische Daten entnehmen sie den Datasheets von der Fortigate Webseite.

2.1.2 Secure-maxX – Branch 50G

Im Standard konfiguriert:

WAN (port4)

- DHCP, statisch

LAN (port1)

- Das LAN-Interface ist mit einem festen Netz konfiguriert welches Standortspezifisch einen anderen Netzbereich hat. Auf dem LAN-Interface ist ein DCHP-Server aktiv, welcher von .10-.200 IPs verteilt.
    - Bspw. Standort 1 = 10.10.**1**.0/24, Standort 2 = 10.10.**2**.0/24

DMZ/WAN2 (port2)

- Es gibt ein vorkonfiguriertes DMZ-Netz, in welchem kein DHCP vorhanden ist. Hier können Maschinen, die in ein DMZ-Netz gehören angeschlossen werden.
- In einer Dual-WAN Konfiguration ist dieser Port ein WAN-Port. Das vorkonfigurierte DMZ-Netz fällt dann weg

HA (port3)

- Der HA-Port ist für High Availability reserviert, über diesen wird der Konfigurationssync und der Heartbeat geschickt.

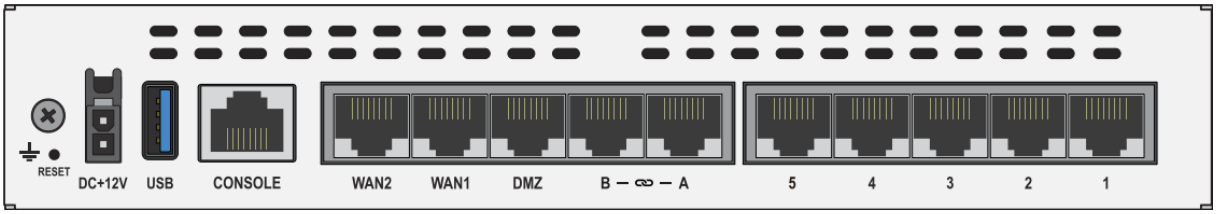
FortiLink (Port a)

- Der FortiLink Port ist für die Anbindung von FortiSwitchen reserviert. Über diesen wird das Protokoll FortiLink gesprochen, um FortiSwitche zu managen.

Werden Ports außerhalb ihrer vorkonfigurierten Funktion konfiguriert, ist diese Standardfunktion nicht nutzbar.

Genaue Technische Daten entnehmen sie den Datasheets von der Fortigate Webseite.

2.1.3 Secure-maxX – Branch 70F



WAN1 (port9)

- DHCP, statisch

WAN2 (port10)

- DHCP, statisch

LAN (port1)

- Das LAN-Interface ist mit einem festen Netz konfiguriert welches Standortspezifisch einen anderen Netzbereich hat. Auf dem LAN-Interface ist ein DCHP-Server aktiv, welcher von .10-.200 IPs verteilt.
    - Bspw. Standort 1 = 10.10.**1**.0/24, Standort 2 = 10.10.**2**.0/24

DMZ (port2)

- Es gibt ein vorkonfiguriertes DMZ-Netz, in welchem kein DHCP vorhanden ist. Hier können Maschinen, die in ein DMZ-Netz gehören angeschlossen werden.

HA (port3)

- Der HA-Port ist für High Availability reserviert, über diesen wird der Konfigurationssync und der Heartbeat geschickt.

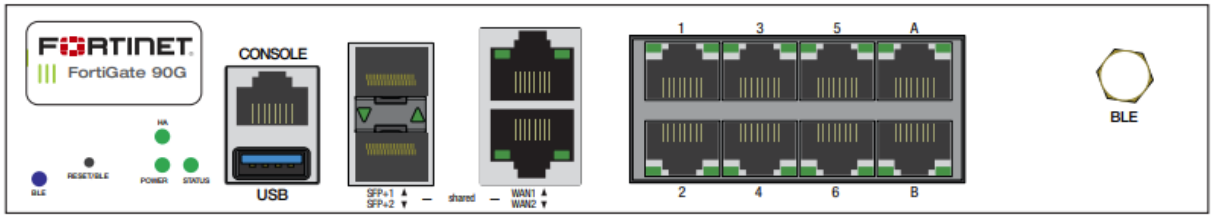
FortiLink (port a)

- Der Fortilink Port ist für die Anbindung von FortiSwitchen reserviert. Über diesen wird das Protokoll FortiLink gesprochen, um FortiSwitche zu managen.

Werden Ports außerhalb ihrer vorkonfigurierten Funktion konfiguriert, ist diese Standardfunktion nicht nutzbar.

Genaue Technische Daten entnehmen sie den Datasheets von der Fortigate Webseite.

2.1.4 Secure-maxX – Branch 90G



WAN1/SFP+1

- DHCP, statisch

WAN2/SFP+2

- DHCP, statisch

LAN (port1)

- Das LAN-Interface ist mit einem festen Netz konfiguriert welches Standortspezifisch einen anderen Netzbereich hat. Auf dem LAN-Interface ist ein DCHP-Server aktiv, welcher von .10-.200 IPs verteilt.
    - Bspw. Standort 1 = 10.10.**1**.0/24, Standort 2 = 10.10.**2**.0/24

DMZ (port2)

- Es gibt ein vorkonfguriertes DMZ-Netz, in welchem kein DHCP vorhanden ist. Hier können Maschinen, die in ein DMZ-Netz gehören angeschlossen werden.
- In einer Dual-WAN Konfiguration ist dieser Port ein WAN-Port. Das Standard DMZ-Netz fällt dann weg

HA (port3)

- Der HA-Port ist für High Availability reserviert, über diesen wird der Konfigurationssync und der Heartbeat geschickt.

FortiLink (Port a)

- Der Fortilink Port ist für die Anbindung von FortiSwitchen reserviert. Über diesen wird das Protokoll FortiLink gesprochen, um FortiSwitche zu managen.

Werden Ports außerhalb ihrer vorkonfigurierten Funktion konfiguriert, ist diese Standardfunktion nicht nutzbar.

Genaue Technische Daten entnehmen sie den Datasheets von der Fortigate Webseite.

2.2 Secure-maxX – Hardwareredundanz

Ein Firewall-Cluster besteht aus mehreren Firewalls, die zusammenarbeiten, um eine höhere Verfügbarkeit, Lastverteilung und Redundanz sicherzustellen.

Jede der vier Service Varianten ist mit Hardwareredundanz erhältlich. Dafür wird ein dedizierter Link zwischen den zwei Hardwaresystemen benötigt.

2.3 Synchronisation der Konfiguration und der aktiven Sessions

Mithilfe eines dedizierten HA-Ports wird die Konfiguration der Primären Firewall immer mit der Sekundären synchronisiert. Auch wird die Information über die aktiven Sessions synchronisiert, um bei einem Schwenk möglichst ausfallfrei auf die sekundäre Firewall zu wechseln.

2.4 Monitoring Ports

Ports, die bei Ausfall einen HA-Schwenk triggern sollen, müssen in der HA-Konfiguration bei Monitored-Interfaces eingetragen werden. Dadurch schwenkt die Firewall dann auf den anderen Member im Cluster, um den Interface-Hardware-Ausfall abzufangen.

2.5 Bestellung und Inbetriebnahme

Nach erster Bestellung wird der Zugang erstellt, eine VDOM zugewiesen und die Firewalls vorkonfiguriert. Dann werden die Firewalls verpackt und gehen in den Versand.

Der Versand erfolgt klimaneutral und ggf. in mehreren Päckchen. Wir nutzen als Versandpartner DHL oder UPS.

2.6 WAN-Redundanz

Bei den Servicevarianten, wie der 70F und der 90G gibt es zwei vorgefertigte WAN-Interfaces, die beide in der SD-WAN Zone liegen. Wenn ein zweites WAN-Interface über eine weitere Internetleitung angeschlossen wird, beeinträchtigt dies den Betrieb nicht. Die IPSec Tunnel und das Management funktionieren weiterhin.

- Bei kleineren Modellen ist dies eine standardisierte Sonderkonfiguration, die bei Bestellung mit angegeben werden kann. Dann wird ein zusätzliches Interface als WAN-Interface vorkonfiguriert und gekennzeichnet. Dieses Interface entfällt allerdings dann als nutzbares LAN-Interface

3 Leistungsmerkmale

In den folgenden Punkten wird beschrieben wie sie als Kunde den Service Secure-maxX nutzen und ihre Firewalls administrieren können.

3.1 Zentrale Administrationsplattform

Für die Administration der Sites nutzen sie einen unserer FortiManager. Der FortiManager ist eine Plattform für die Administration von Fortinet Firewalls, APs und Switches. Die Anmeldung am FortiManager funktioniert komfortabel über unser TelemaxX Kundencenter.

Zugehörig zu ihrem Secure-maxX Service im Kundencenter finden sie den Link zum FortiManager. Dort melden sie sich an und kommen in ihre ADOM, in der sich ihre VDOM und ihre Sites befinden.

Unter Policy und Objects befinden sich die Regeln und Firewall-Objekte. Hier können sie diverse Anpassungen vornehmen und auf die Sites oder die VDOM pushen. Durch das zentrale Management sind individuelle Objekte auf alle Sites und die VDOM anwendbar.

Der FortiManager hält für jedes Device 100 Revisionen vor, bei Fehlkonfigurationen können sie jederzeit zu einem vorherigen Status zurückkehren.

3.2 Secure-maxX SCC

Ein SCC (Security Control Center) ist eine Virtual Domain, oder eine virtuelle Instanz in einer physikalischen Firewall. Diesem SCC können virtuelle und physikalische Interfaces zugewiesen werden.

Das SCC ist die zentrale Schnittstelle aller Secure-maxX Services und Connect.

Das SCC wird im priorisierten Zyklus gepatcht. Das SCC ist immer Hardwareredundant. Softwareredundanz kann als Upgrade zusätzlich bestellt werden.

3.3 Secure-maxX WiFi

Bei Secure-maxX WiFi können FortiAPs zur Bereitstellung von Wireless Access Points bestellt werden. Diese erfüllen den WiFi 7 Standard und werden nach Absprache auf eine oder mehrere Fortigate als WLC (Wireless Controller) eingerichtet.

3.4 Zentrale Konfigurationssicherungen

Die Konfigurationen der Sites und des SCC werden täglich gesichert und 7 Tage vorgehalten. Danach gibt es einen Rollover und die älteste Konfiguration wird überschrieben.

3.5 Secure-maxX-Connect

Secure-maxX Connect sind standardisierte Anbindungen von internen und externen Services der TelemaxX und ihrer Partner. Diese können jederzeit im Kundencenter dazu gebucht werden. Das Dazubuchen erfolgt über einen kostenfreien Service-Request. Im Folgenden sind zur Bereitstellung notwendige Infos sowie die Bereitstellungszeit beschrieben:

Service	Vorrausichtliche Bereitstellungszeit	Besonderheiten
S3	1-3 Tage	L3-Anbindung nur zu Latenzverbesserung
Opencloud	1-3 Tage	Anbindung per L2-Customer Connect und VLANs in aus Opencloud in die VDOM möglich
Cloud	1-3 Tage	Anbindung per L2-Customer Connect und VLANs in aus VMware-Cloud in die VDOM möglich
VPC	3-5 Tage	L3-Anbindung nur zu Latenzverbesserung
Housing	3-5 Tage	Anbindung je nach Portverfügbarkeit mit 1-10G Vollständige L2 Verbindung in VDOM
Microsoft Azure Peering Service (MAPS)	24h	Enablement der Internetleitung an der VDOM für den Service MAPS
DDoS-AlwaysOn DDoS-OnDemand	24h Bei AlwaysOn Lernphase 7 Tage	Enablement der Internetleitung an der VDOM für den Service DDoS

3.6 Leistungsabgrenzung

Der Internetanschluss und die Datennutzung ist Fair-Use. Bei unsachgemäßer Verwendung behalten wir uns das Recht vor den Service, zu Zwecken der Sicherheit der TelemaxX und ihrer Kunden, einzuschränken.

3.7 Softwareupdates

Art des Patches	Beschreibung	Benachrichtigung
Signaturen	IPS-/ AV-Signaturen werden angepasst	Nein
Patches	Patches bspw. Von 7.2.8 auf 7.2.9 werden bis zu zwei Wochen getestet und dann gestaffelt ausgerollt.	Ja mit Patchzeitfenster
Minor Releases	Major Releases bspw. Von 7.2 auf 7.4 werden erst einige Monate getestet und dann in einem Mature Status gestaffelt ausgerollt.	Ja mit Patchzeitfenster und Patchnotereport
Major Releases	Major Releases bspw. Von 7.x auf 8.x werden erst einige Monate getestet und dann in einem Mature Status gestaffelt ausgerollt.	Ja mit Patchzeitfenster und Patchnotereport

3.8 Nutzerverwaltung und Kundencenter

Die Nutzerverwaltung erfolgt über das TelemaxX Kundencenter. Als zentrale Plattform für ihre Services bei der TelemaxX lassen sich weitere Sites und Zusatzoptionen buchen. Sie können über das Kundencenter als Landingpage auch diverse Services konfigurieren und administrieren.

Wenn sie einen Administrator zu ihrem FortiManager hinzufügen möchten, geschieht dies auch über das Kundencenter.

3.9 Knowledgebase

Die zentrale Knowledgebase der TelemaxX kb.telemaxx.de beinhaltet auch technische Dokumentation und Anleitungen für Secure-maxX. Hier finden sie für alle Komponenten detaillierte Anleitungen und Grafiken, die ihnen die Administration erleichtern.

Ein FAQ mit oft gestellten Fragen findet sich an derselben Stelle.

4 Zusatzleistungen

4.1 Patchkabel und SFP-Connect und Einbaurahmen

Patchkabel, SFP-Connect und Einbaurahmen von der Firma Rackmount-IT können zu den Services nach Bedarf dazu gebucht werden. Nach der Laufzeit müssen sie wieder mit der Hardware zurückgeschickt werden. Kabel sind vom Zurücksenden ausgenommen.

Custom Branding auf den Einbaurahmen sind möglich, bitte fragen sie unseren Vertrieb zeitnah vor Bestellung, da ansonsten die Einbaurahmen ohne Branding bestellt werden.

4.2 Zusätzliche öffentliche IPv4-Adressen zum SCC

Das SCC hat eine 100Mbit geteilte Internetleitung die auf bis zu 1Gbit hochgestuft werden kann. Bei Bedarf kann auch eine höhere Bandbreite zur Verfügung gestellt werden, dies bedarf jedoch einer gesonderten Prüfung und ist von der Verfügbarkeit der geteilten Infrastruktur des SCC abhängig. Eine Public IP hat das SCC bereitgestellt, bei Bedarf können weitere dazu bestellt werden. IPv6 Adressen sind auch dazu bestellbar.

4.3 Einweisung

Auf Anfrage können sie eine auf vier Wochen zeitlich begrenzte Demo (je nach Verfügbarkeit von Demo-Hardware) sowie eine Einweisung in das Produkt bekommen.

4.4 Internetanbindung

Um in den Secure-maxX Service zu nutzen müssen die Standorte eine Internetverbindung haben. DHCP, statisch und PPPoE sind möglich für die IP-Vergabe. PPPoE bedarf einer Remotekonfiguration durch einen Engineer und wird pro Standort mit 1h Secure-maxX Care OnDemand berechnet.

Ein TelemaxX Internetservice wird nicht benötigt um Secure-maxX zu nutzen.