



Unsere Arbeitsweise und unser Umgang mit Daten haben sich verändert durch Cloud Computing, mobiles Arbeiten und IP-basierte Kommunikation. Die zunehmende Komplexität stellt Firmennetzwerke und IT-Sicherheit vor ganz neue Herausforderungen.

Die sichere und flexible Netzwerklösung für KMU

Die gesamte Kommunikation und immer mehr Software-anwendungen laufen heute über das IP-Netz, sensitive Geschäftsdaten lagern auf zentralen Servern oder in der Cloud und Mitarbeitende greifen von verschiedenen Standorten sowie aus dem Homeoffice oder von unterwegs darauf zu. Die zunehmende Komplexität der Firmennetzwerke stellt unsere IT-Sicherheit vor ganz neue Herausforderungen. Denn auch die Bedrohungslage hat sich verändert: Ein Drittel der Schweizer KMU wurden bereits Opfer von Cyberattacken.*

Was ist Business Network Solutions?

Business Network Solutions bietet Ihnen ein voll betreutes Firmennetzwerk. Die verschiedenen Netzwerkservices können zu einem gesamtheitlichen Schutz kombiniert werden. Die Netzwerklösung ist virtualisiert in der Swisscom Cloud, Sicherheit und Services werden rund um die Uhr überwacht. Der hohe Automatisierungsgrad ist einzigartig auf dem Markt und bietet Ihnen Sicherheit bei maximaler Flexibilität.

* Quelle: gfs-zürich (2017): [Cyberrisiken in Schweizer KMU](#).

Ihre Vorteile mit Business Network Solutions

- > **Betreutes Netzwerk:** Ihr Netzwerk ist stets auf dem aktuellen Stand, was Technologie und Firmware angeht. Sie müssen sich um nichts kümmern.
- > **Planbare Kosten:** Die monatlichen Kosten beinhalten Betrieb, Lizenzkosten, Firmware-Updates sowie Hardwareaustausch.
- > **Skalierbarkeit:** Egal wie viele Standorte, Arbeitsplätze oder angeschlossene Geräte – Ihr Netzwerk wächst mit, ohne dass Investitionen fällig werden.
- > **Hohe Verfügbarkeit:** Die Netzwerkservices werden rund um die Uhr durch Swisscom überwacht.
- > **Daten in der Schweiz:** Die Netzwerkdaten sind in geschützten Swisscom Rechenzentren in der Schweiz gespeichert.
- > **Schnelles Eingreifen Ihres Partners:** Alle Netzwerkservices und die Hardware können in Echtzeit remote gemanagt werden. Dazu ist ein Einsatz vor Ort meist nicht nötig.
- > **Alles aufeinander abgestimmt:** Sie beziehen Netzwerklösungen, Internet, Telefonie und Cloudlösungen aus einer Hand und perfekt aufeinander abgestimmt.



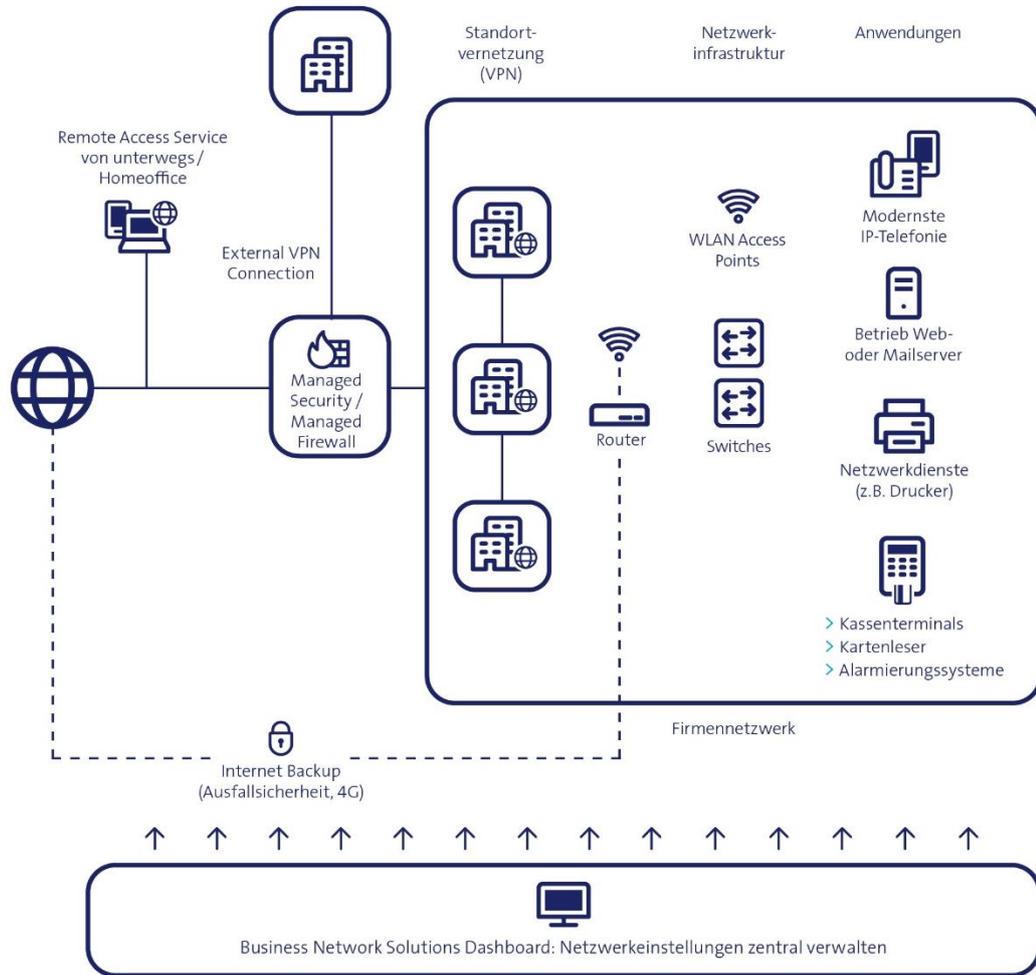


Die Informationen in diesem Dokument stellen kein verbindliches Angebot dar. Änderungen sind jederzeit vorbehalten.

Swisscom (Schweiz) AG KMU, Postfach, CH-3050 Bern, Tel. 0800 055 055, www.swisscom.ch/kmu

swisscom

Die Lösung auf einen Blick



Facts & Figures



Sicheres Firmennetzwerk (VPN)

Sie vernetzen Firmenstandorte in einem vom Internet getrennten VPN (Virtual Private Network) und greifen auch von ausserhalb des Büros geschützt darauf zu.



Schutz gegen Angriffe von aussen (Firewall)

Eine leistungsfähige Firewall mit Webfilter und Antivirus schützt effizient gegen Cyberbedrohungen, Viren und Trojaner.



Unbesorgt arbeiten im LAN und WiFi

Getrennte Nutzergruppen und separate Gäste-WiFis erhöhen die Sicherheit Ihres Firmennetzwerks.



Die Daten verlassen das Swisscom Netz nie

Ob Sie auf Daten in der Swisscom Cloud zugreifen oder diese zwischen Standorten austauschen: Ihre Daten verlassen das sichere Swisscom Netz nie.



Die Informationen in diesem Dokument stellen kein verbindliches Angebot dar. Änderungen sind jederzeit vorbehalten.

Swisscom (Schweiz) AG KMU, Postfach,
CH-3050 Bern, Tel. 0800 055 055, www.swisscom.ch/kmu

swisscom

Geschützter Datenaustausch im Firmennetzwerk und im Fernzugriff *Managed Networks & Remote Access Service*

Die Ansprüche an VPN* wachsen punkto Sicherheit, Zuverlässigkeit und Geschwindigkeit der Datenübertragung: Mit dem Trend zur Cloud werden immer mehr Daten und Softwareanwendungen in Echtzeit über das öffentliche Internet übertragen und Mitarbeitende arbeiten zunehmend mobil und nutzen dafür oft ungesicherte WiFi-Netzwerke.

Swisscom bietet Ihnen eine VPN-Lösung, die diesen steigenden Ansprüchen gerecht wird. Anders als bei anderen Anbietern verlässt Ihr firmeninterner Datenverkehr das Swisscom Netz nie, was neben der VPN-Technologie die Sicherheit zusätzlich erhöht. Anwendungen und Daten aus der Swisscom Cloud können vollumfänglich in das Netzwerk integriert werden. Dadurch profitieren Sie von einer sehr hohen Verfügbarkeit dieser Dienste.

Mit der Lösung von Swisscom greifen Mitarbeitende auch von unterwegs oder aus dem Homeoffice über eine verschlüsselte Verbindung sicher auf ihre gewohnte Arbeitsumgebung zu (zentrale Firmenserver, Clouddienste). Somit können Angreifer die Datenkommunikation nicht mitlesen, selbst wenn der Zugriff über ein ungesichertes WiFi erfolgt. Und falls Zugangsdaten gestohlen werden (z.B. durch Phishing-Attacken) bleibt der Zugriff dank Zwei-Faktor-Authentifizierung sicher.

* Virtual Private Network (VPN): Der Datenverkehr zwischen Firmenstandorten wird über einen gesicherten VPN-Tunnel übertragen.

Ihre Mehrwerte mit Managed Networks und Remote Access Service



Standortübergreifend sicher zusammenarbeiten

Firmenstandorte via VPN vernetzen, um auf gemeinsame Daten, Server, Programme oder Netzwerkgeräte zuzugreifen.



Geschützter Datenverkehr zwischen Firmenstandorten

Der Datenverkehr zwischen Firmenstandorten ist vom öffentlichen Internet getrennt. Unbefugte haben keinen Zugriff. Ihre Daten verlassen das sichere Swisscom Netz nie.



Sicher auf Cloud Services zugreifen

Swisscom Cloud Services können über eine stabile und performante Verbindung (1 GB) nahtlos in das Firmennetzwerk eingebunden werden.



Überall sicher arbeiten, als wäre man im Büro

Über eine verschlüsselte und stabile VPN-Verbindung greifen Sie auch ausserhalb der Firma sicher auf das Firmennetzwerk zu. Der Zugriff ist mit Zwei-Faktor-Authentifizierung geschützt. Das hilft, den Schaden zu begrenzen, falls Login-Daten verloren oder gestohlen werden.



Automatische Priorisierung von IP-Diensten

Dank Quality of Service (QoS) erhalten geschäftskritische IP-Anwendungen (z.B. Realtime) stets die notwendige Bandbreite im Firmennetzwerk.



Skalierbarkeit der Standorte und Anzahl Remote-Zugriffe

Die Integration zusätzlicher Standorte im Firmennetzwerk ist sehr einfach möglich und setzt keine Hardware-Firewall voraus. Die Anzahl der Nutzer, die von ausserhalb auf das Netzwerk zugreifen, ist nicht begrenzt.



Effizienter Schutz gegen Angriffe auf das Firmennetzwerk

Managed Security

Sie möchten Ihren Internetzugang mit einer Firewall schützen?

Mit Managed Security verfügen Sie über eine performante Sicherheitslösung, die Ihr Firmennetzwerk effizient gegen Cyberbedrohungen schützt. Das alles zu kalkulierbaren Kosten. Die Firewall ist in der Swisscom Cloud virtualisiert, was entscheidende Vorteile gegenüber Hardware-Firewall-Lösungen vor Ort mit sich bringt (z.B. Skalierbarkeit, hohe Verfügbarkeit und Performanz).

Einzigartig auf dem Markt: Mit Managed Security integriert Swisscom die virtualisierte Firewall des renommierten Security-Anbieters Fortinet mit dem Internetservice sowie den Netzwerkservices von Swisscom. Durch den hohen Automatisierungsgrad profitieren Sie von mehr Sicherheit und einer schnellen Inbetriebnahme bei maximaler Flexibilität.

Swisscom überwacht die Lösung rund um die Uhr und übernimmt für Sie das Software-Patches-Management inkl. Lizenz-Management. Ein Rundum-Sorglos-Paket!



Ihr Nutzen mit Managed Security



Firewall mit Certificate & Deep Packet Inspection

Eine in der Swisscom Cloud virtualisierte port- und IP-basierte Firewall kontrolliert Ihren gesamten Netzwerkverkehr (inkl. https-Verkehr). Mit Antispoofing wird der Zugriff auf Ihr Netzwerk mit gefälschtem Absender verhindert.



Webfilter

Ein Webfilter bietet Ihnen die Möglichkeit, basierend auf URL-Kategorien, die Webzugriffe zu kontrollieren (Black/White-Listen) und unsichere Seiten zu blockieren. Sie können aus vordefinierten Sicherheitsstufen auswählen und/oder diese individuell anpassen.



Antivirus (Zusatzoption)

Der Web-Verkehr wird untersucht und bekannte Viren werden erkannt und blockiert. Die Signaturen des Virenschanners werden stündlich aktualisiert, um auch die neusten Viren und Trojaner zu identifizieren und zu entfernen.



Logging und Reporting

Der Netzwerkverkehr wird protokolliert. Dies ermöglicht Ihnen eine einfache Analyse der Nutzung und die Fehlersuche. Zudem erhalten Sie ein monatliches Reporting mit den wichtigsten Eckdaten.



External VPN Connection (Site to Site IPSec VPN)

Einbinden von Firmenstandorten mit Connectivity anderer Provider (z.B. von Kabelanbietern oder im Ausland) oder von Partnerfirmen in das Business Network Solutions Firmennetzwerk.



Ihre Mehrwerte mit Managed Security



Hohe Verfügbarkeit und Sicherheit

Die Firewall wird rund um die Uhr proaktiv überwacht, der Virenschutz wird stündlich aktualisiert und die Firmware ist stets auf dem neuesten Stand. Die cloudbasierte Lösung bietet zudem eine hohe Verfügbarkeit (Redundanz) der Firewall.



Starke Performance

Keine Begrenzung der verfügbaren Bandbreite durch Hardwareperformance oder Datendurchsatz der Firewall.



Investitionsschutz und Flexibilität

Egal, wie sich Ihre Firma in Zukunft entwickelt: Bei einer Skalierung der Benutzer und/oder der Bandbreite passt sich Managed Security an.



Mehrere Standorte schützen

Sie nutzen eine zentrale Firewall für mehrere Firmenstandorte. Für zusätzliche Standorte kann der Firewallschutz innert Minuten aufgeschaltet werden.



Von Branchenexperten empfohlen

Lieferant der Security-Lösung ist die Firma Fortinet, die von unabhängigen Branchenexperten empfohlen wird (Gartner, NSS Labs).

Die Informationen in diesem Dokument stellen kein verbindliches Angebot dar. Änderungen sind jederzeit vorbehalten.

Swisscom (Schweiz) AG KMU, Postfach,
CH-3050 Bern, Tel. 0800 055 055, www.swisscom.ch/kmu



Unbesorgt und sicher arbeiten im LAN und WiFi

Managed LAN

Immer mehr Arbeitsprozesse basieren auf dem IP-Netz: Telefonie, Datenaustausch, Softwareanwendungen, Cloud Services oder Maschinen und Netzwerkgeräte wie z.B. Drucker.

Stabilität und Performanz dieser Anwendungen sind abhängig vom LAN – also von der Verkabelung im Firmengebäude und den verbauten Hardwarekomponenten. Wenn das LAN ausfällt, funktioniert in der Firma nichts mehr. Oft sind die firmeneigenen LAN-Strukturen über die Zeit gewachsen und stossen mit den wachsenden Anforderungen an ihre Grenzen hinsichtlich Sicherheit, Leistungs- und Innovationsfähigkeit.

Mit Managed LAN können Sie eine LAN- und WiFi-Vernetzung aufbauen, ohne in Hardware zu investieren, und müssen sich um nichts kümmern. Denn Sie beziehen Netzwerkhardware (Switches und Access Points) im Servicemodell. Für den Betrieb und Unterhalt ist Swisscom verantwortlich. Sie profitieren von einem abgestimmten und betreuten LAN und sind technologisch stets auf dem aktuellen Stand.

Ihr Mehrwert mit Managed LAN



Gemanagte Hardware ohne Investitionskosten

Sie beziehen gemanagte LAN- und WiFi-Hardwarekomponenten im Servicemodell und müssen sich nicht um Firmware-Updates, Lizenzverlängerungen und Hardwareaustausch kümmern. Investitionskosten fallen nicht an – Sie zahlen nur für Leistungen, die Sie aktuell benötigen.



Schnelle Verbindungen und höchste Verfügbarkeit

Hochwertige Hardware der Firma Aruba ermöglicht die Einrichtung stabiler und leistungsfähiger LAN- und WiFi-Netzwerke für eine höchstmögliche Verfügbarkeit geschäftskritischer IP-Services.



Stets die aktuelle Technologie

Swisscom sorgt dafür, dass Ihre Hardware stets auf dem aktuellen Stand der Technik ist, und tauscht diese aus, wenn diese defekt ist oder Funktionen nicht mehr unterstützt werden.



Geschützt arbeiten in LAN und WiFi

Ihr WiFi ist verschlüsselt (WPA2). Getrennte Netzwerke (z.B. für lokale Server oder Abteilungen) erhöhen die Sicherheit des Netzwerks und schränken den Zugriff auf sensitive Daten ein.



Sicherer Netzwerkzugriff

Managed LAN bietet die Grundlage für personalisierte Logins (die Systemintegration zentraler Nutzerverzeichnisdienste wird unterstützt). Dies erhöht die Netzwerksicherheit.



Unterbrechungsfreies WiFi

Nutzer können sich ohne WiFi-Unterbrüche im ganzen Gebäude bewegen. Bei mangelhafter Mobilfunkabdeckung können die Nutzer so auch mobil über das WiFi telefonieren.



Sicherer Internetzugang für Gäste (Zusatzoption Public WLAN)

Sie bieten Ihren Gästen einen WiFi-Hotspot an und sind rechtlich abgesichert, falls der Internetzugang für illegale Aktivitäten genutzt wird. Der Service entspricht den aktuellen Datenschutzbestimmungen für Gäste-WiFis.



Pricing

| Ihre Internet- und Serviceleistungen ¹ | L | M | S | XS |
|--|--------------------------------|----------------------------------|-------------------|-------------------|
| Max. Down- und Upload ² | 10 Gbit/s ³ | 300 Mbit/s | 100 Mbit/s | 10 Mbit/s |
| Internet Backup ⁴ Ausfallsicherheit für Internet und Telefonie max. Down- und Upload, Mbit/s | inklusive 100/20 | inklusive 50/10 | – | – |
| Serviceleistungen | advanced | plus | standard | standard |
| > Service Desk und Störungsannahme ⁵ | 7×24 h | 7×24 h | 7×24 h | 7×24 h |
| > Supportzeiten | Mo–Sa 6–22 Uhr | Mo–Fr 8–19 Uhr Sa 8–17 Uhr | Mo–Fr 8–17 Uhr | Mo–Fr 8–17 Uhr |
| > Max. Störungsbehebungszeit ⁶ (während Supportzeiten) | 8 Std. | 10 Std. | – | – |
| > Entschädigung ⁷ bei Nichteinhaltung der Störungsbehebungszeit | Monatsgebühr inkl. Optionen | – | – | – |
| Router | | | | |
| Centro Business 2.0 (max. 1 GBit/s) ² 4-Port-Universal-WLAN-Router unterstützt ISDN (ITA) Einzelpreis 149.– statt 299.– | gratis | 99.– einmalig | 149.– einmalig | 149.– einmalig |
| Centro Business 3.0 (max. 10 GBit/s) ² 1 x 10GB-Port/ 4 x 1GB-Port Wi-Fi 6 Router kein Bridge-Modus ⁹ keine ITA (ISDN Schnittstelle) Einzelpreis 299.– | 49.– einmalig | 149.– einmalig | 199.– einmalig | 249.– einmalig |
| Option Top Speed³ | | | | |
| Monatstarif | inklusive | 40.- | 40.- | |
| Max. Down- und Upload ² | 10 Gbit/s | 10 Gbit/s | 10 Gbit/s | |
| Monatstarif pro Anschluss | 300.- | 125.– | 90.- | 55.- |

Ihre Netzwerklösung (Managed Networks)

| | | | | |
|--|--------------------|------|------|------|
| > Standortvernetzung (VPN) | ja | ja | ja | ja |
| > Quality of Service (QoS) | ja | ja | ja | ja |
| > DHCP-Optionen | ja | ja | ja | ja |
| > NAT/PAT-Regeln | ja | ja | ja | ja |
| > DMZ ⁸ | ja | ja | ja | ja |
| > LAN Routing | ja | ja | ja | ja |
| > DNS-Server-Einstellungen | ja | ja | ja | ja |
| Monatstarif pro Anschluss | Inkl. ⁹ | 60.– | 60.– | 60.– |
| Rabatt bei Einsatz an einem Firmenstandort | | 30.– | 30.– | – |

Die Informationen in diesem Dokument stellen kein verbindliches Angebot dar. Änderungen sind jederzeit vorbehalten.

Swisscom (Schweiz) AG KMU, Postfach,
CH-3050 Bern, Tel. 0800.055.055, www.swisscom.ch/kmu

swisscom



Die Informationen in diesem Dokument stellen kein verbindliches Angebot dar. Änderungen sind jederzeit vorbehalten.

Swisscom (Schweiz) AG KMU, Postfach,
CH-3050 Bern, Tel. 0800 055 055, www.swisscom.ch/kmu

swisscom

Optionen zu Ihrer Netzwerklösung

Managed Firewall

- > Port-basierte stateful Firewall
- Monatstarif pro Standort
(muss für alle Standorte aktiviert werden) 10.–
- Nicht kombinierbar mit Managed Security

Managed Security

- > Port- und IP-basierte Firewall
- > Deep Packet Inspection
- > Webfilter

| | | |
|---|-------------------------|---------------------------|
| Monatstarif pro Standort (muss für alle Standorte aktiviert werden) Nicht kombinierbar mit Managed Firewall | 60.– erster Standort | 30.– weitere Standorte |
|---|-------------------------|---------------------------|

Zusatzoptionen

- > Antivirus für das Netzwerk 10.– pro Standort
- > External VPN Connection (Site to Site VPN)
 - Bis zu 5 Verbindungspunkte CHF 20.–
 - Bis zu 10 Verbindungspunkte CHF 30.–
 - Bis zu 15 Verbindungspunkte CHF 50.–
 - Bis zu 20 Verbindungspunkte CHF 65.–
 - Bis zu 25 Verbindungspunkte CHF 80.–

Fixe IP-Adressen

| | | | | | | |
|-------------|------|------|------|------|------|------|
| Anzahl | 1 | 4 | 8 | 16 | 32 | 64 |
| Monatstarif | 12.– | 22.– | 33.– | 50.– | 70.– | 95.– |

Remote Access Service (RAS)

| | | | | | |
|-------------|--------|------|------|------|-------|
| Benutzer | Bis zu | 5 | 10 | 15 | 20 |
| Monatstarif | | 35.– | 65.– | 90.– | 110.– |

Managed LAN

- > Austauschservice für Hardware (Defekt/End of Life)
- > LAN Management

| | |
|---|------|
| Monatstarif pro Standort (zuzüglich Servicepauschale für Hardware) | 25.– |
|---|------|

| | |
|---|-------|
| Monatstarif für gemanagte Netzwerkhardware | |
| > Switch klein, Aruba JL258A (8 Ports, mit Power over Ethernet) | 25.– |
| > Switch mittel, Aruba JL259A (24 Ports) | 29.– |
| > Switch mittel, Aruba JL261A (24 Ports, mit Power over Ethernet) | 49.– |
| > Switch gross, Aruba JL262A (48 Ports, mit Power over Ethernet) | 79.– |
| > WLAN Access Point indoor ¹⁰ (Wi-Fi 5), Aruba JX954A (inkl. Wandmontagekit schwarz) | 15.– |
| > WLAN Access Point indoor ¹⁰ (Wi-Fi 6), Aruba R2H28A (inkl. Wandmontagekit schwarz) | 15.– |
| > WLAN Access Point outdoor ¹⁰ , Aruba JX966A | 49.– |
| > WLAN Hospitality Access Point ¹⁰ , Aruba JY678A (inkl. Tischmontagekit, weiss) | 19.– |
| > Distribution Switch, Aruba JL075A (16SFP+ 2-slot) | 250.– |



Die Informationen in diesem Dokument stellen kein verbindliches Angebot dar. Änderungen sind jederzeit vorbehalten.

Swisscom (Schweiz) AG, KMU, Postfach,
CH-3050 Bern, Tel. 0800 055 055, www.swisscom.ch/kmu

swisscom

| | |
|--|-------|
| Hardwareangebot zum Kauf | |
| > SFP-Modul (10G SFP+ LC SR) | 240.– |
| > SFP-Modul (1G SFP LC SX) | 80.– |
| > SFP-Modul (1G SFP RJ45) | 150.– |
| > PoE+ Injector 802.3at (JW629A) | 105.– |
| > Montage-Kit, Outdoor, schwenkbar, Aruba 11048903 | 65.– |
| > Montage-Kit, Outdoor, fix, Aruba 11048902 | 65.– |

Public WLAN

- Public WLAN basic
- > Möglichkeit, dem Public WLAN einen Namen zuzuweisen (SSID)
 - > Lawful Interception
 - > 24/7 Support für Endnutzer des Public WLAN

Monatstarif pro Access Point 6.–

- Public WLAN advanced
- > Möglichkeit, dem Public WLAN einen Namen zuzuweisen (SSID)
 - > Lawful Interception
 - > 24/7 Support für Endnutzer des Public WLAN
 - > Personalisierbare Login Seite und SMS Texte
 - > Zusätzliche Login Möglichkeiten

Monatstarif pro Access Point 12.–

Zusätzliche kostenpflichtige Optionen pro Standort

- > Device Login 30.–
 - > PMS Login 200.–
 - > Content Filtering 50.–
-

¹ Business Network Solutions ist auch mit Business Internet Services wireless verfügbar (siehe Factsheet Business Internet Services wireless)

² Die verfügbare Geschwindigkeit ist abhängig vom örtlichen Glasfaserausbau und vom eingesetzten Router. Für identische Down- und Upload-Bandbreiten ist in der Regel ein Swisscom Anschluss mit einer Glasfaserleitung (FTTH max 1 GBit/s und XGS-PON max. 10 GBit/s) bis in die Geschäftsräumlichkeiten erforderlich. Verfügbare Maximalgeschwindigkeit an Ihrer Geschäftsadresse prüfen auf swisscom.ch/checker

³ Bei der Nutzung von Business Network Services (BNS) reduziert sich die Geschwindigkeit auf max. 700 Mbit/s, da dies mehr Rechenleistung vom Router erfordert.

⁴ Internet Backup bietet Ausfallsicherheit für Internet und Telefonie. (Die Anzahl und die Qualität gleichzeitig möglicher Gespräche hängen von der verfügbaren Bandbreite des Mobilfunknetzes ab.) Internet Backup wird mit einem 4G-Modem gratis (statt CHF 50.–) angeboten.

⁵ Die Störungsannahme erfolgt von Montag bis Freitag von 8.00 bis 12.00 Uhr und von 13.00 bis 17.00 Uhr durch Ihren Swisscom KMU-Partner, ausserhalb dieser Zeiten durch die Swisscom KMU-Hotline.

⁶ Die Störungsbehebungszeit beschreibt die Dauer vom Zeitpunkt der Störungsmeldung bei Swisscom bis zur Wiederherstellung der vollen Servicebereitschaft eines Swisscom Dienstes.

⁷ Bei Nichteinhaltung der Störungsbehebungszeit werden Ihnen die kompletten Monatsgebühren von Business Internet Services und Business Network Solutions inkl. Optionen erlassen.

⁸ Eine DMZ benötigt mindestens 4 fixe IP-Adressen. Die fixen IP-Adressen müssen als Option zusätzlich gekauft werden.

⁹ Managed Networks ist im Paket Business Internet Service L inbegriffen.

¹⁰ Bei sämtlichen Access Points sind keine Stromspeisungsnetzteile beigelegt.