



The way we work and handle data has changed with the emergence of cloud computing, mobile working and IP-based communication. Increasing complexity is creating brand new challenges for company networks and IT security.

Secure, flexible networking for SMEs

All communication and more and more software applications now depend on the IP network, sensitive company data is stored on central servers or in the cloud, and employees access it from various company locations, as well as home offices or on the move. The growing complexity of company networks is creating brand new challenges for our IT security. For the threat level has also changed: one in three Swiss SMEs have already fallen victim to cyber-attacks*.

What is Business Network Solutions?

Business Network Solutions offers you a fully managed company network. The different network services can be combined to provide comprehensive protection. The network solution is virtualised in the Swisscom cloud, while security and services are monitored round the clock. The high level of automation is unique in the market and offers you security with maximum flexibility.

Your benefits with Business Network Solutions:

- > **Managed network:** your network is always up to date as far as technology and firmware are concerned, without you having to do anything.
- > **Predictable costs:** the monthly fee covers operational and licensing costs, firmware updates and hardware exchange.
- > **Scalability:** however many locations, workspaces and connected devices you have, your network grows with you without the need for investment.
- > **High availability:** Network services are monitored around the clock by Swisscom.
- > **Data in Switzerland:** network data is stored in secure Swisscom Data Centers in Switzerland.
- > **Quick partner response:** all network services and hardware can be managed remotely in real time. On-site visits are rarely necessary.
- > **Perfectly coordinated:** get network solutions, Internet, telephony and cloud solutions from the same provider, all perfectly coordinated.

* Source: gfs-zürich (2017): [Cyberisiken in Schweizer KMU](#)



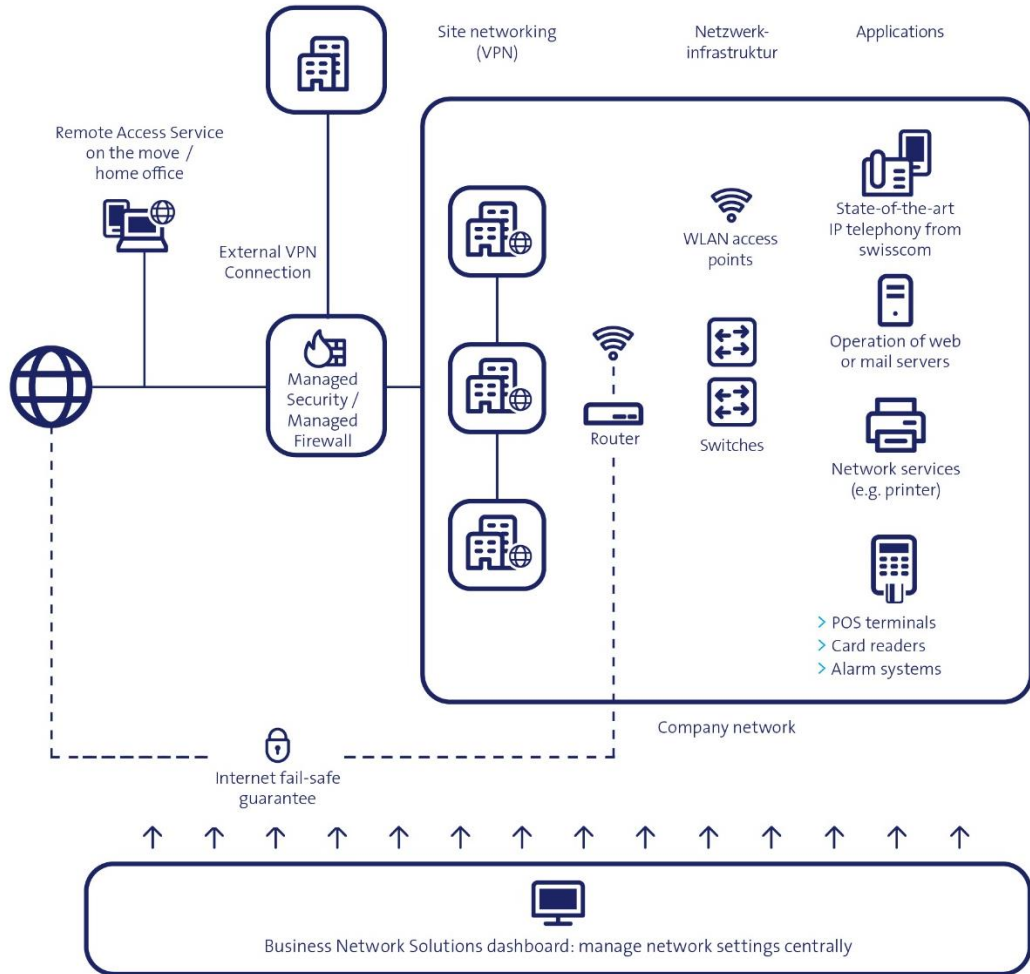


The information in this document does not constitute a binding offer. It is subject to revision at any time.

Swisscom (Switzerland) Ltd, SME, P.O. Box, CH-3050 Berne, SME Hotline 0800 055 055, www.swisscom.ch/sme

swisscom

The solution at a glance



Facts & Figures



Secure company network (VPN)

You can link different company locations together in a VPN (Virtual Private Network) separate from the Internet, which you can access securely away from the office.



Protection from outside attacks (firewall)

A powerful firewall with web filters and antivirus efficiently protects you against cyber threats, viruses and trojans.



Work worry-free via LAN and Wi-Fi

Separate user groups and guest Wi-Fi make your company network more secure.



Data never leaves the Swisscom network

Whether you access it in the Swisscom cloud or share it between locations, your data never leaves the secure Swisscom network.



The information in this document does not constitute a binding offer. It is subject to revision at any time.

Swisscom (Switzerland) Ltd, SME, P.O. Box,
CH-3050 Berne, SME Hotline 0800 055 055,
www.swisscom.ch/sme

swisscom

Secure data exchange in a company network and remote access

Managed Networks and Remote Access Service

The standards that VPNs* are expected to meet are growing in terms of security, reliability and data transfer speeds: with the move towards cloud computing, more and more data and software applications are being sent in real time via the public Internet and mobile working is becoming more widespread, with employees often using unprotected Wi-Fi networks away from the office.

Swisscom offers you a VPN solution in keeping with these rising demands. Unlike other providers, Swisscom ensures that your internal company data never leaves the Swisscom network, which, along with the VPN technology, makes it even more secure. Applications and data from the Swisscom cloud can be fully integrated into the network, enabling you to benefit from their high availability.

The Swisscom solution also enables staff to securely access their familiar work environment on the move or from their home office via an encrypted connection (central company server, cloud services). This prevents attackers from reading data communications even if they are accessed via an unsecured Wi-Fi network. And if login data is stolen (e.g. through phishing attacks), access remains secure thanks to two-factor authentication.

* Virtual Private Network (VPN): data traffic between company sites is transmitted via a secure VPN tunnel.

Added value with Managed Networks and Remote Access Service



Securely collaborate across company sites

Connect company locations via VPN in order to access shared data, servers, programs or network devices.



Protect data traffic between company locations

Data traffic between company locations is separate from the public Internet and cannot be accessed without authorisation. Your data never leaves the secure Swisscom network.



Securely access cloud services

Swisscom cloud services can be seamlessly integrated into the company network via a stable and fast connection (1 GB).



Work securely anywhere as if you were in the office

You can securely access the company network via an encrypted, stable VPN connection, even from outside company premises. Access is protected with two-factor authentication, which helps to limit the damage if login data is lost or stolen.



Automatically prioritise IP services

Thanks to Quality of Service (QoS), business-critical IP applications (e.g. real-time) always get the necessary bandwidth within the company network.



Scalable locations and remote access

It is very easy to add new locations to the company network without the need for a hardware firewall. An unlimited number of users can access the network remotely.



Effective protection against attacks on the company network

Managed Security

Do you want to protect your Internet access with a firewall?

Managed Security provides you with a high-performance security solution that effectively protects your company network against cyber threats, all at a calculable cost. The firewall is virtualised in the Swisscom cloud, which has crucial advantages over on-premise hardware firewall solutions (e.g. scalability, high availability and performance).

Unique in the market: with Managed Security, Swisscom integrates the virtualised firewall of the renowned security provider Fortinet with its own Internet and network services. The high level of automation guarantees greater security, fast set-up and maximum flexibility.

Swisscom monitors the solution round the clock and looks after software patch management, including licence management, for you. A complete, worry-free package!



Your benefits with Managed Security



Firewall with deep packet inspection

A virtualised port- and IP-based firewall in the Swisscom cloud controls all your network traffic (including https traffic). Anti-spoofing prevents fake senders accessing your network.



Web filter

A web filter based on URL categories enables you to control web access (black/white lists) and block unsafe sites. You can select from and/or individually adapt predefined security levels.



Antivirus (additional option)

Web traffic is analysed and known viruses are identified and blocked. Virus scanner signatures are updated hourly in order to identify and remove the latest viruses and trojans.



Logging and reporting

Network traffic is logged, enabling you to easily analyse usage and troubleshoot. You also receive a monthly report containing key data.



External VPN Connection (Site to Site IPSec VPN)

Integration of company locations with connectivity from other providers (e.g. cable providers or foreign providers) or partner companies into the Business Network Solutions company network.



Added value with Managed Security



High availability and security

The firewall is proactively monitored round the clock, virus protection is updated hourly and firmware is always up to date. The cloud-based solution also offers high firewall availability (redundancy).



Strong performance

Available bandwidth is not limited by hardware performance or firewall throughput.



Investment protection and flexibility

Regardless of how your company develops in the future, Managed Security can be adapted to changing user numbers and/or bandwidths.



Protect multiple sites

You use a central firewall for multiple company sites. Firewall protection can be switched on within minutes for additional locations.



Recommended by industry experts

The security solution is provided by Fortinet, a company recommended by independent industry experts (Gartner, NSS Labs).

The information in this document does not constitute a binding offer. It is subject to revision at any time.

Swisscom (Switzerland) Ltd, SME, P.O. Box,
CH-3050 Berne, SME Hotline 0800.055.055,
www.swisscom.ch/sme

swisscom



Worry-free, secure working via LAN and Wi-Fi

Managed LAN

An increasing number of work processes are based on the IP network: telephony, data exchange, software applications, cloud services, or machines and network devices such as printers.

The stability and performance of these applications depend on the LAN, i.e. the cabling inside the company building and the built-in hardware components. If the LAN fails, nothing in the company will work anymore. Many companies' own LAN structures have grown over time and, in face of rising demands, are reaching their limits in terms of security, performance and capacity for innovation.

With Managed LAN, you can create a LAN and Wi-Fi network without investing in hardware or worrying about anything because the network hardware (switches and access points) is included as part of the service model, while Swisscom is responsible for operational and maintenance issues. You benefit from a coordinated, managed LAN and state-of-the-art technology at all times.

Added value with Managed LAN



Managed hardware without investment costs

You'll get managed LAN and Wi-Fi hardware components as part of the service model and don't have to worry about firmware updates, licence renewals and hardware exchange. There are no investment costs – you only pay for what you need at the time.



Fast connections and maximum availability

High-quality hardware from the Aruba company enables you to set up stable, fast LAN and Wi-Fi networks that provide maximum availability of business-critical IP services.



State-of-the-art technology at all times

Swisscom ensures that your hardware is always state of the art and replaces it if it stops working or if functions are no longer supported.



Work securely via LAN and Wi-Fi

Your Wi-Fi is encrypted (WPA2). Separate networks (e.g. for local servers or departments) make the network more secure and limit access to sensitive data.



Secure network access

Managed LAN provides the basis for personalised logins (integration of central user directory services is supported), increasing network security.



Seamless Wi-Fi

Users can move around the whole building without Wi-Fi interruptions and make mobile phone calls via Wi-Fi if mobile coverage is poor.



Secure Internet access for guests (Public WLAN additional option)

You can offer your guests a Wi-Fi hotspot, safe in the knowledge that you are legally protected if it is used for illegal activities. The service meets current guest Wi-Fi data protection rules.



Pricing

Your Internet and services ¹	L	M	S	XS
Max. down-/upload speed ²	10 Gbit/s ³	200 Mbit/s	50 Mbit/s	10 Mbit/s
Internet Backup ⁴ Fail-safe guarantee for Internet and telephony Max. down- and upload, Mbit/s	included 100/20	included 50/10	–	–
Service level	advanced	plus	standard	standard
> Service desk and fault report hotline ⁵	7/24	7/24	7/24	7/24
> Support times	Mon–Sat 6 am–10 pm	Mon–Fri 8 am–7 pm Sat 8 am–5 pm	Mon–Fri 8 am–5 pm	Mon–Fri 8 am–5 pm
> Max. fault repair time ⁶ (during support times)	8 hrs	10 hrs	–	–
> Compensation Conditions under footnote 7	Monthly fee incl. options	–	–	–
Router				
Centro Business 2.0 (max. 1 GBit/s) ² 4-port universal WLAN router No bridge mode ⁹ Unit price 149.– instead of 299.–	free	99.– (one-off)	149.– (one-off)	149.– (one-off)
Centro Business 3.0 (max. 10 GBit/s) ² 1 x 10GB-Port/ 4 x 1GB-Port Wi-Fi 6 Router No bridge mode ⁹ No ITA (ISDN interface) Unit price 299.–	49.– (one-off)	149.– (one-off)	199.– (one-off)	249.– (one-off)
Top Speed Option³	L	M	S	
Monthly fee	included	40.-	40.-	
Max. down/upload speed ²	10 Gbit/s	10 Gbit/s	10 Gbit/s	
Monthly fee per connection	300.-	125.–	90.-	55.-

Your network solution (Managed Networks)

> Site networking (VPN)	yes	yes	yes	yes
> Quality of Service (QoS)	yes	yes	yes	yes
> DHCP options	yes	yes	yes	yes
> NAT/PAT rules	yes	yes	yes	yes
> DMZ ⁸	yes	yes	yes	yes
> LAN routing	yes	yes	yes	yes
> DNS server settings	yes	yes	yes	yes
Monthly fee per connection ⁹	Incl. ⁹	60.–	60.–	60.–
Discount if only used at one company site		30.–	30.–	–

The information in this document does not constitute a binding offer. It is subject to revision at any time.

Swisscom (Switzerland) Ltd, SME, P.O. Box,
CH-3050 Berne, SME Hotline 0800.055.055,
www.swisscom.ch/sme

swisscom



The information in this document does not constitute a binding offer. It is subject to revision at any time.

Swisscom (Switzerland) Ltd, SME, P.O. Box,
CH-3050 Berne, SME Hotline 0800 055 055,
www.swisscom.ch/sme

swisscom

Options for your network solution

Managed Firewall

> Port-based stateful firewall

Monthly fee per site 10.–

(must be activated at all sites)

Cannot be combined with Managed Security

Managed Security

> Port- und IP-based firewall

> Deep packet inspection

> Web filter

Monthly tariff per site 60.– 30.–
(must be activated at all sites) for the first site for each additional site

Cannot be combined with Managed Firewall

Additional options

> Antivirus for the Network 10.– for each site

> External VPN Connection (Site to Site VPN):

Up to 5 connection points: CHF 20.–

Up to 10 connection points: CHF 30.–

Up to 15 connection points: CHF 50.–

Up to 20 connection points: CHF 65.–

Up to 25 connection points: CHF 80.–

Fixed IP addresses

No.	1	4	8	16	32	64
Monthly fee	10.–	20.–	30.–	45.–	65.–	85.–

Remote Access Service (RAS)

User	Up to	5	10	15	20
Monthly fee		35.–	65.–	90.–	110.–

Managed LAN

> Hardware replacement service (defective, end-of-life)

> LAN Management

Monthly fee per location 25.–
(plus service fee for hardware)

Monthly fee for managed network hardware	
> Small switch, Aruba JL258A (8 ports, with power over Ethernet)	25.–
> Medium switch, Aruba JL259A (24 ports)	29.–
> Medium switch, Aruba JL261A (24 ports, with power over Ethernet)	49.–
> Large switch, Aruba JL262A (48 ports, with power over Ethernet)	79.–
> WLAN Access Point indoor* (Wi-Fi 5), Aruba JX954A (incl. wall mounting kit, black)	15.–
> WLAN Access Point indoor* (Wi-Fi 6), Aruba R2H28A (incl. wall mounting kit, black)	15.–
> WLAN access point outdoor ¹⁰ , Aruba JX966A	49.–
> WLAN hospitality access point ¹⁰ , Aruba JY678A (incl. table mounting kit, white)	19.–
> Distribution Switch, Aruba JL075A (16SFP+ 2-slot)	250.–



Hardware for sale	
> SFP module (10G SFP+ LC SR)	240.-
> SFP module (1G SFP LC SX)	80.-
> SFP module (1G SFP RJ45)	150.-
> PoE+ injector 802.3at (JW629A)	105.-
> Wall Mount Kit, Outdoor, rotatable, Aruba 11048903	65.-
> Wall Mount Kit, Outdoor, fix, Aruba 11048902	65.-

Public WLAN

Public WLAN basic

- > Possibility of assigning a name to the public WLAN (SSID)
- > Lawful interception
- > 24/7 support public WLAN users

Monthly fee per access point 6.-

Public WLAN advanced

- > Possibility of assigning a name to the public WLAN (SSID)
- > Lawful interception
- > 24/7 support public WLAN users
- > Customisable login page and SMS texts
- > Additional login options

Monthly fee per access point 12.-

Additional paid options per location

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

- ¹ Business Network Solutions is also available with Business Internet Services wireless (see document Business Internet Services wireless Facts & Pricing).
- ² The available speed depends on local optical fibre expansion and the router that is used. A Swisscom connection with an optical fibre line (FTTH max 1 GBit/s and XGS-PON max. 10 GBit/s) to the business premises is usually required for identical upload and download bandwidths. Check the maximum speed available for your business address at swisscom.ch/checker
- ³ Maximum speed is reduced to 700 Mbit/s with BNS, which requires more router processing power.
- ⁴ Internet Backup offers a fail-safe guarantee for Internet access and telephony (the number and quality of simultaneous calls depends on the available bandwidth of the mobile network). Internet Backup is available free (instead of CHF 50.-) with a 4G modem.
- ⁵ Faults can be reported to your Swisscom SME partner from 8 am to 12 noon and from 1 pm to 5 pm Monday to Friday, and to the Swisscom SME Hotline at other times.
- ⁶ The fault repair time is the period from the fault being reported to Swisscom until the full Swisscom service is restored. Details on calculation can be found in section 3 of the Service Level Agreement (SLA).
- ⁷ Cumulative conditions for compensation with SBC L are: A fault must occur in the sense of a serious drop in performance of a service that is caused by Swisscom (i.e. not by the customer or partner) (see section 2.3 of the SLA). The 8-hour fault rectification target is not met. The fault does not occur during the initial installation phase of the service concerned.
- ⁸ A DMZ requires at least 4 fixed IP addresses. Fixed IP addresses must be purchased separately as an option.
- ⁹ Managed Networks is included in the Business Internet Service L package.
- ¹⁰ Power supply units are not included with any of the access points.