



1. Champ d'application

Les présentes conditions de l'offre s'appliquent à Business Network Solutions de Swisscom (Suisse) SA (ci-après «Swisscom»). Les conditions de l'offre «Business Network Solutions» s'appliquent en complément des «Conditions générales pour les prestations de service» («CG»), des «Conditions particulières» pour Internet et Service et des conditions de l'offre «Smart Business Connect» et priment en cas de contradictions.

2. Généralités

2.1 Conditions

Pour que Business Network Solutions fonctionne, une connexion active de Business Internet Services s'impose.

Business Network Solutions se compose d'une partie fixe «Managed Networks» en tant que base permettant l'accès au dashboard de Business Network Solutions dans lequel il est possible de configurer les options et d'en commander d'autres.

Pour Business Network Solutions, il s'impose d'utiliser exclusivement le matériel prescrit par Swisscom.

Un groupement Business Network Solutions peut se composer de plusieurs sites «Smart Business Connect» en Suisse. Le propriétaire du raccordement sur le site principal est considéré comme le client. Il est le titulaire du contrat pour tous les sites. Le premier site pour lequel Managed Networks est acquis est automatiquement le site principal. Il est possible de changer de site principal ultérieurement.

2.2 Commande, installation, configuration et assistance

L'achat de Managed Networks doit se produire dans le cadre de la commande de Business Internet Services.

Les autres options doivent être achetées indépendamment dans le dashboard. En acceptant l'offre, le client accepte que le partenaire obtienne immédiatement le statut de «Technical Admin» et que le partenaire puisse commander, résilier et configurer des options dans le dashboard pour tous les sites du groupement.

L'installation des options est effectuée sous sa propre responsabilité ou bien à titre onéreux par un partenaire. Il peut être engagé par Swisscom. L'installation des options conduit à une interruption notable des services actuels. Cette interruption peut prendre du temps. Aucune action en réparation ou dommages et intérêts ne pourra être intentée vis-à-vis de Swisscom.

La configuration en bonne et due forme de Business Network Solutions incombe au client et au partenaire. Le client est responsable des modifications techniques de l'infrastructure qui sont nécessaires pour le changement de solution. Il incombe au client de contrôler à quel point ce changement se répercute sur les prestations actuellement fournies, également de fournisseurs tiers.

Les prestations de service pour la configuration et l'intégration sur la base d'exigences individuelles des clients sont fournies en commun par Swisscom et des parties tierces (partenaires), c'est pourquoi le client déclare être d'accord pour que Swisscom mette les données et accès au système nécessaires à la disposition du partenaire que le client doit désigner. Au départ, le partenaire est identifié par le client. Pour un groupement Business Network Solutions, le client ne peut engager qu'un seul partenaire et obtient le statut de «Technical Admin». Si le client engage plusieurs partenaires, il est responsable du triage et de l'attribution des droits d'accès nécessaires.

L'obligation d'assistance de niveau 1 incombe au partenaire procédant à l'installation. Pour l'assistance, le client doit s'adresser au partenaire. Si Swisscom est mis à contribution pour un dérangement dû à une configuration défectueuse de Business Network Solutions, il se peut que les coûts soient facturés au client.

2.3 Restrictions

Une fois que Managed Networks/Business Network Solutions est activé, il n'est plus possible de garantir les débits promis pour Business Internet Services.

Les adresses IP fixes qui existent déjà pour Business Internet Services doivent être de nouveau commandées lors de la commande de Business Network Solutions. Le client ou le partenaire peut commander les adresses IP identiques dans le dashboard pendant un délai précis. Une fois le délai passé, le droit à des adresses IP identiques s'éteint. Le délai est indiqué pendant la commande. Pour le reste, les dispositions du chiffre 3.1.4. s'appliquent.

Une fois que Managed Networks est activé, il n'est plus possible d'utiliser les possibilités de configuration sur le routeur Centro Business. Les configurations existantes sont supprimées. Il incombe au client de les enregistrer avant l'activation des options et le cas échéant de les reconfigurer dans le dashboard de Business Network Solutions.

Pour garantir que les services Swisscom aient la meilleure qualité qui soit, Swisscom attribue à ces services



une configuration QoS statique qui ne peut pas être modifiée.

3. Options pour Business Network Solutions

Les options sont décrites en gros ci-après. De plus amples informations et les prix figurent dans les spécifications des services et sur le site Web. Sauf description contraire, les options sont facturées au site où elles sont utilisées.

3.1 Managed Networks

Managed Networks permet, grâce à l'accès au dashboard, de mettre en réseau des sites de client, de gérer les options DHCP et d'exploiter une zone démilitarisée (DMZ). Il est par ailleurs possible de définir des règles «Network Address Translation» (NAT) et des règles «Port Access Translation» (PAT). Les adresses IP nécessaires doivent être achetées séparément.

3.2 Managed Networks light

L'option Managed Networks light inclut les mêmes fonctions que Managed Networks, mais ne peut être utilisée que pour un seul site d'entreprise, sans mise en réseau avec d'autres sites.

Pour bénéficier de ce service sur plusieurs sites, il convient de souscrire autant d'abonnements Managed Networks light qu'il y a de sites concernés. Même dans ce cas, n'est possible qu'une utilisation isolée, c'est-à-dire sans mise en réseau des sites. Par conséquent, seule l'option Managed Networks peut être utilisée pour la mise en réseau des sites par VPN. Malgré cela - dans le cas des solutions PWLAN, Blue TV Host et DCS Trunk (téléphonie) - seule une utilisation isolée est autorisée, c'est-à-dire sans mise en réseau avec d'autres sites de l'entreprise.

En conséquence, l'option "Managed Networks" est utilisée uniquement pour la mise en réseau de sites VPN, en particulier dans le cas de Smart ICT et DCS ou d'autres solutions de mise en réseau de données telles que VPN RAS/S2S, etc.

Swisscom se réserve le droit de contrôler que l'option Managed Networks light est utilisée conformément au contrat et de facturer la différence par rapport à l'option Managed Networks en cas d'usage abusif. Les autres mesures prévues par les CGV demeurent réservées.

3.3 Managed Firewall Standard

Le service Managed Firewall Standard permet de fixer une réglementation pour le trafic de données sortant du LAN. Il est possible de choisir parmi différents niveaux de sécurité prédéfinis ou de définir une réglementation indépendante. La réglementation indépendante est effacée dès que le pare-feu est désactivé ou qu'une autre réglementation est sélectionnée. Afin de proposer la meilleure sécurité qui soit, l'option doit être absolument prise pour tous les sites du groupement lors de la commande. Si des sites sont ajoutés ultérieurement au groupement, l'option s'y applique automatiquement et est facturée en sus pour lesdits sites.

3.4 Remote Access Services

Avec Remote Access Services, Swisscom propose une solution permettant d'accéder au réseau de l'entreprise et ce indépendamment du lieu. Pour cela, différentes variantes d'authentification à deux facteurs (SMS et Mobile ID) sont proposées. Les détails et conditions d'utilisation de Mobile ID figurent sur <http://documents.swisscom.com>.

La configuration et l'installation des clients nécessaires ainsi que l'acquisition des terminaux sont entièrement sous la responsabilité du partenaire et du client. Si le client n'utilise pas la Mobile ID mise à disposition par Swisscom, le fonctionnement des services ne pourra être garanti.

L'utilisation du client RAS dans des réseaux publics, dans d'autres réseaux que Swisscom ou bien à l'étranger peut comporter des risques en matière d'écoute par des tiers non autorisés ayant manipulé le réseau. La connexion entre l'utilisateur et Internet ne fait pas partie du service RAS. Le client ou utilisateur doit s'en charger lui-même en s'adressant à un fournisseur d'accès à Internet (FAI). La qualité du service et la prestation du RAS dépendent de la qualité de la connexion mise à disposition par le FAI choisi.

Pour bénéficier de la sécurité de Business Network Solutions, les Swisscom Helpdesks ne sont pas autorisés à transmettre d'informations sur les profils de client (nom d'utilisateur, mots de passe etc.). Ils n'ont pas accès aux données qui sont enregistrées sur des serveurs sûrs. Si un utilisateur a besoin de telles informations, seul un représentant autorisé du client peut les consulter via le BNS dashboard.

Les conditions d'utilisation Mobile ID, disponibles sur le site Internet de Swisscom, s'appliquent en supplément au Remote Access Service, Mobile ID compris. Les options sont facturées au site principal.



3.5 Managed LAN

Managed LAN permet la mise en place et l'administration d'un WLAN (Wireless Local Area Network) au sein de réseaux d'entreprises avec différents groupes d'utilisateurs sur le dashboard. L'option doit être commandée si nécessaire pour chaque site de l'entreprise et la facturation se fait par site.

Il convient de se procurer le matériel nécessaire à cet effet (Access Points, Switches) auprès de Swisscom (service de modèle avec taxe mensuelle). Swisscom s'assure que les Access Points et Switches employés correspondent à la technologie la plus moderne pour les fonctionnalités fournies.

Les appareils mentionnés (Access Points, Switches) demeurent la propriété de Swisscom. Si le client résilie un appareil dans le cadre du modèle de service ou signale un défaut à Swisscom, Swisscom lui indique la date et l'adresse auxquelles il doit retourner l'appareil. Si le client ne renvoie pas l'appareil à cette adresse dans le délai imparti, Swisscom est en droit de lui facturer la valeur marchande de l'appareil en question (prix de vente actuel sur le marché moyennant l'application d'un amortissement sur cinq ans). A la fin du contrat, le client s'engage à restituer l'infrastructure à Swisscom dans l'état qui résulte d'une utilisation conforme au contrat.

3.6 Public WLAN (PWLAN)

3.5.1 Généralités

Le PWLAN permet au client de mettre à la disposition de ses usagers un accès Internet avec une authentification utilisateur par SMS. Cette option payante doit être commandée par chaque site d'entreprise sur lequel le client désire avoir un PWLAN. Chaque licence PWLAN Accesspoint est facturée.

3.6.2 PWLAN basic

PWLAN basic permet de se connecter par authentification SMS et EAP-SIM.

3.6.3 PWLAN advanced

PWLAN advanced permet de personnaliser la présentation du WLAN.

En cas de connexion par numéro de bon, par un appareil et par PMS, le client procède à l'identification des utilisateurs conformément à la loi (obligation contractuelle essentielle du client). Le client garantit la mise à disposition des informations d'identification requises des personnes dans un format courant, défini par Swisscom et adapté au traitement automatisé, pen-

dant 6 mois minimum à compter du jour de la dernière utilisation du moyen d'accès par l'utilisateur concerné. En outre, il s'engage à transmettre immédiatement ces informations sur demande (de Swisscom ou de l'autorité compétente) en vue de l'identification immédiate ou ultérieure des utilisateurs dans le cadre de la procédure de surveillance selon la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT, RS 780.1).

Connexion par numéro de bon: en cas de connexion par numéro de bon, Swisscom ne dispose d'aucune information permettant d'identifier l'utilisateur. En offrant un moyen d'accès, le client est pleinement responsable de l'identification correcte et conforme des utilisateurs, y compris de la saisie, de la conservation, de la mise à disposition et de la transmission des données personnelles nécessaires au respect ou à l'application des obligations légales d'informer.

Connexion par PMS: connexion à l'aide des Credentials d'utilisateur saisis par le client via la connexion de la base de données du client par protocole SSH au système PWLAN de Swisscom. Le client est tenu de respecter les obligations suivantes:

- acquisition et implémentation de toutes les licences pour le(s) système(s) requis (SSH-Service, PMS, etc.);
- mise à disposition, lien et connexion physiques, exploitation, maintenance des systèmes client au niveau du «peering point» Swisscom;
- garantie du bon fonctionnement des services SSH (y compris localisation du dérangement et rétablissement du service normal);
- identification de tous les utilisateurs et saisie des données d'identification et personnelles dans le cadre de la mise à disposition de moyens d'accès (y compris informations de connexion SSH et PMS associées)

Connexion par un appareil: enregistrement des appareils client (adresse MAC) dans le Business Center de Swisscom. Le client s'engage en particulier à gérer immédiatement les adresses MAC dans le Business Center de Swisscom (y compris à les actualiser par des ajouts/suppressions). Le client s'assure que seuls figurent dans le Business Center de Swisscom des appareils pour une connexion de ce type qui sont sa propriété exclusive et sont utilisés principalement par lui-même ou en son nom, et dont il peut identifier à tout moment les utilisateurs.

3.7 Managed Security



3.7.1 Généralités

Managed Security permet de configurer et d'administrer des services de pare-feu et UTM (Unified Threat Management) au sein de réseaux d'entreprise via le tableau de bord BNS.

Si le client commande l'option, celle-ci sera automatiquement activée par le partenaire sur tous les sites du client, puis facturée par site.

La responsabilité de la sécurité des systèmes côté client incombe au client/partenaire. Swisscom ne peut être tenue responsable des paramètres de sécurité configurés par le partenaire/client via le tableau de bord BNS.

3.7.2 Composants optionnels importants

Les principaux composants de l'option sont décrits ci-dessous.

- **Reporting**
Swisscom met à la disposition du client/partenaire un module de reporting permettant au client/partenaire d'accéder aux rapports. Swisscom attire l'attention du client sur le fait qu'il doit informer ses utilisateurs du réseau (tels que les employés ou les invités) à l'avance de l'utilisation de ce module de reporting afin de ne pas porter atteinte à leur droit à la vie privée. Dans ce contexte, il est recommandé d'adopter un règlement de surveillance qui fournisse des informations sur les mesures de protection techniques et de compte-rendu utilisées, ainsi que sur les modalités d'utilisation et de surveillance. Swisscom se réserve le droit d'interrompre momentanément ou définitivement le module de reporting, que ce soit pour des raisons techniques ou autres.
- **Logging**
Les données de journalisation enregistrées par le pare-feu sont disponibles en téléchargement sur le tableau de bord BNS. Le client est lui-même responsable du respect de la législation sur la protection des données.
- **Filtre Web**
Le filtre Web est utilisé pour bloquer l'accès à certaines pages Web présentant des contenus indésirables. Ces filtres sont mis à jour périodiquement. Le client a la possibilité de bloquer différentes catégories de contenu indésirable. Swisscom décline toute responsabilité et garantie concernant les URL contenues et leur catégorisation, dans les limites de la loi.
- **External VPN Connection Point**

L'External VPN Connection Point permet au client d'intégrer un site non-BNS dans le réseau d'entreprise BNS. La responsabilité des sites, services et appareils connectés via la connexion VPN externe incombe exclusivement au client (ou au partenaire mandaté par ses soins). Swisscom n'assume aucune responsabilité quant à la sécurité des sites connectés via la connexion VPN externe ou pour les éventuels logiciels malveillants qui risqueraient d'infecter le réseau BNS via ces sites.

3.8 Particularités pour les adresses IP fixes dans le cadre de Business Network Solutions

Pour Business Network Solutions, il convient d'acheter des adresses IP fixes dans le dashboard. Aucun droit à des adresses IP précises n'existe. Les adresses IP commandées dans le dashboard ne peuvent pas être reprises pour Business Internet Services en cas de résiliation de l'option ou des options à la base comme Managed Networks.

Attention, pour les sous-réseaux de 4 à 64 adresses IP fixes, trois adresses IP sont respectivement utilisées pour la mise à disposition technique du service et ne peuvent donc plus être employées pour des services spécifiques du client. Les options sont facturées au site principal.

4. Prix, facturation et rabais

Les prix actuels, à savoir les coûts uniques et récurrents des options figurent sur le site Internet de Swisscom. Les rabais et promotions ne s'appliquent pas à Business Network Solutions. Lors de l'utilisation du client Remote Access Service, le trafic occasionné est facturé séparément.

L'obligation de payer Managed Networks commence au moment de l'activation du Business Internet Service à la base. Si Business Internet Services est déjà activé, l'obligation de payer commence au moment de la commande de Managed Networks. L'obligation de payer les autres options commence au moment de leur commande.

5. Confidentialité et protection des données

Dans les cas d'assurance ou pour des raisons de maintenance, Swisscom se réserve le droit d'accéder au dashboard et d'enregistrer et évaluer l'ensemble des données log pour améliorer la qualité.



Lors de l'activation de Business Network Solutions, le client cède l'ensemble du trafic réseau (également du réseau privé) à Swisscom. Swisscom se réserve le droit d'enregistrer les données de configuration afin d'améliorer les options.

En cas d'assistance, Swisscom peut accorder aux prestataires de services étrangers un accès temporaire à ce service et aux données associées telles que les identifiants WLAN, les configurations des commutateurs et les points d'accès des clients (mais pas l'identité respective des clients). Pour les prestataires de services d'un pays dont le niveau de protection est inférieur à celui de la Suisse (p. ex. USA, Inde), Swisscom assure une protection appropriée par une ou plusieurs mesures conformément à l'art. 6 al. 2 LPD.

6. Garantie légale

Swisscom s'assure que les points d'accès employés correspondent à la technologie la plus moderne pour les fonctionnalités fournies. Pour offrir ce standard de qualité élevée, Swisscom utilise les moyens de sécurité appropriés et les plus modernes. Le client prend acte de ce que, malgré tous les efforts de Swisscom et l'utilisation des normes de sécurité et des techniques les plus modernes, une sécurité et un fonctionnement sans faille des systèmes et des procédures utilisés ne peuvent être garantis. Swisscom prend par ailleurs les précautions nécessaires pour protéger l'infrastructure utilisée des interventions de tiers. La protection absolue du réseau de l'entreprise ne peut être absolument garantie.

7. Conclusion, durée minimale et résiliation

7.1 Conclusion, entrée en vigueur

La commande d'une option conduit à un complément du contrat existant. Vis-à-vis de Swisscom, le client est responsable de procéder lui-même aux commandes dans le dashboard ou d'autoriser quelqu'un à les passer.

7.2 Délais de résiliation et durée minimale

Les options Business Network Solutions n'ont pas de durée minimale. Les options commandées dans le dashboard doivent être résiliées par le client dans le dashboard. De son côté, Swisscom peut utiliser d'autres canaux pour procéder à d'éventuelles résiliations.

La résiliation du Business Internet Service de Smart Business Connect conduit automatiquement à la suppression de toutes les options associées.

La résiliation de Managed Networks conduit automatiquement à la suppression de toutes les options du site correspondant.

Il est seulement possible de résilier Managed Networks sur le site principal si toutes les options sur tous les autres sites du groupement ont été résiliées.

Dès qu'une option est résiliée, toutes les configurations associées sont automatiquement supprimées. Les configurations ne peuvent donc pas être enregistrées.

8. Modification et cessation

Les modifications et la cessation de Business Network Solutions ou d'options individuelles sont régies par les CG et les Conditions particulières.

Octobre 2022