1 Einleitung

Die ecotel communication ag (im Folgenden ecotel genannt) bietet dem Auftraggeber im Rahmen der technischen und betrieblichen Möglichkeiten optional zum VPN (»Virtual Private Network«) einen gesicherten Zugang aus Fremdnetzen zum *ethernet.VPN* des Auftraggebers als Zusatzleistung *ethernet.VPN Secure Access* an.

ecotel entwickelt zusammen mit dem Auftraggeber ein bedarfsgerechtes Konzept und stimmt den Kundenbedarf und die technischen Möglichkeiten ab.

Der Umfang der insgesamt vertraglich vereinbarten Leistungen ergibt sich aus dieser Leistungsbeschreibung und den einzelnen Leistungsbeschreibungen der vom Auftraggeber bestellten Leistungen sowie aus den Allgemeinen Geschäftsbedingungen und den besonderen Geschäftsbedingungen (»ecotel Besondere Geschäftsbedingungen Standortvernetzung«) der ecotel.

2 Standardleistungen

ethernet.VPN Secure Access ist eine Option von *ethernet.VPN* und bietet den gesicherten Zugang einzelner, gegebenenfalls mobiler Rechner (VPN-Clients) aus Fremdnetzen zum *ethernet.VPN* des Auftraggebers. Fremdnetze können dabei insbesondere auch das öffentliche Internet sein. Die Übergabe der Daten an das *ethernet.VPN* erfolgt an einer vorhandenen oder an einer im Rahmen von *ethernet.VPN Secure Access* optional bereit zu stellenden Firewall (VPN-Gateway).

Die Absicherung der Kommunikation zwischen VPN-Client und VPN-Gateway erfolgt dabei wahlweise durch Verschlüsselung (z.B. Secure IPSec) und / oder durch geeignete Trennung der privaten Datenkommunikation des *ethernet.VPN* von der Kommunikation der Fremdnetze durch logische Trennung (Tunneling). Optional ist auch der Zugang ganzer lokaler Netzwerke möglich, die über Fremdnetze mit dem *ethernet.VPN* des Auftraggebers direkt oder indirekt verbunden sind.

3 Verschlüsselung

Die Art der Verschlüsselung und die verwendete Schlüssellänge, welche zur Verschlüsselung der IP-Datenpakete verwendet wird, ist von der eingesetzten Hard-und Software abhängig. Es werden Schlüssel mit einer Mindestlänge von 256 Bit eingesetzt.

Soweit eine Verschlüsselung eingesetzt wird, findet diese zwischen VPN-Client und VPN-Gateway statt. Eine Verschlüsselung des Datenverkehrs innerhalb des *ethernet.VPN* ist nicht Bestandteil der Leistung *ethernet.VPN Secure Access*. Beim Einsatz einer Verschlüsselung im Ausland ist der Auftraggeber verpflichtet, die dort jeweils geltenden gesetzlichen Bestimmungen zu beachten

4 VPN-Gateway

Die Standardleistung von *ethernet.VPN Secure Access* umfasst die Konfiguration und die Verwaltung einer im Rahmen von *ethernet.VPN* vorhandenen Firewall (*ethernet.VPN Internet Access oder Internet Access DC),* die für die Zuführung der Secure Access Verbindungen zum VPN zuständig ist. Die vorhandene Firewall muss für Secure Access technisch nutzbar sein und sie muss eine Verbindung zum jeweiligen Fremdnetz (z.B. öffentliches Internet) haben. Die Firewall und der Zugang zum Internet sind nicht Bestandteil der Standardleistung von ethernet.VPN Secure Access.

Ist keine geeignete Firewall vorhanden wird im Rahmen von Secure Access für das VPN-Gateway eine Firewall sowie der Zugang zum Internet angeboten werden. Der Zugang zum Internet und dessen Absicherung erfolgt dabei in der Regel in einem der ecotel Datacenter (*ethernet.VPN Secure Access Gateway DC*). Alternativ dazu kann der Zugang auch an einem der Kundenstandorte erfolgen, wobei hier die Firewall ebenfalls am Kundenstandort steht (*ethernet.VPN Secure Access Gateway*). Beide Optionen sind im Absatz »Firewall« und »Internetzugang« dieser Leistungsbeschreibung definiert.

Die Anzahl der Secure Access Verbindungen die gleichzeitig konfiguriert werden können sowie die Verschlüsselungs-Performance ist vom Typ der Firewall und der eingesetzten Lizenzen (IPSec DC) abhängig. Diese Parameter und mögliche Einschränkungen sind im Absatz »Firewall-Typen« dieser Leistungsbeschreibung spezifiziert.

5 VPN-Client

Der VPN-Client von Secure Access (*ethernet.VPN Secure Access IPSec*) ist als Software ausgelegt, die auf den Rechnern des Auftraggebers installiert werden muss. ecotel verkauft die Anzahl der bestellten Lizenzen und stellt diese dem Auftraggeber zur Verfügung. Soweit nichts anderes vereinbart, ist der Auftraggeber für die Installation verantwortlich.

Der VPN-Client ist nicht für alle Betriebssysteme und Versionen von Betriebssystemen jederzeit verfügbar. Eine Liste der aktuell freigegebenen Betriebssysteme und Versionen ist auf Anfrage erhältlich. ecotel hat keinen Einfluss darauf, dass neue Betriebssysteme oder neue Betriebssystemversionen zukünftig vom Hersteller der Software unterstützt werden.

ecotel unterstützt den Auftraggeber bei Fragen zur Erstinstallation der VPN-Clients und konfiguriert das VPN-Gateway. Der Hersteller der Software ist für den Service und den weitergehenden Support des VPN-Client mit dem Auftraggeber gemeinsam verantwortlich.

Die Performance des VPN-Clients ist insbesondere bei Einsatz einer Verschlüsselung von der Performance des eingesetzten Rechners abhängig. ecotel hat auf die Performance wie auch auf die Stabilität des Rechners keinerlei Einfluss.

Die Autorisierung der VPN-Clients erfolgt auf Benutzer- oder Systemebene über Passwörter. Andere Autorisierungsmethoden (z.B. Tokenautorisierung, SecurID) sind optional erhältlich.

6 Internetdienst im Rahmen von *ethernet.VPN Secure Access*

6.1 IP-Router und Anschlussleitungen

Der Internetzugang erfolgt auf gemeinsamer Infrastruktur (z.B. Leitung, IP-Router) von *ecotel ethernet.VPN*. Die maximale Bandbreite des Internetdienstes ist abhängig von der zur Verfügung stehenden Infrastruktur (z.B. der Anschlussleitungen *ethernet.VPN line* / *ethernet.VPN gigabit line*, *ethernet.VPN vdsl*, *ethernet.VPN adsl* oder *ethernet.VPN LTE* sowie der IP-Router).

Im Einzelfall, insbesondere bei dem dezentralen Internetzugang, ist die Nutzung dieser Infrastruktur nicht an allen Standorten möglich, so dass ergänzend Leitungswege und gegebenenfalls IP-Router erforderlich sein können. Diese sind nicht Bestandteil von *ethernet.VPN Secure Access*.

6.2 IP-Adressen

Der Auftraggeber erhält für die Dauer der Inanspruchnahme des Internetzugangs von ecotel eine öffentliche, statische IP-Adresse zugewiesen. Unter Berücksichtigung der von der Réseaux IP Européens (RIPE) vorgegebenen Regeln (siehe Dokument ID: ripe-381) kann der Auftraggeber einen offiziell registrierten IP-Adressraum aus dem PA-Adressraum (Provider Aggregatable) der ecotel erhalten. Nach Vertragsbeendigung ist der Auftraggeber verpflichtet, diese von ecotel zugewiesenen IP-Adressen zurück zu geben und nicht mehr zu nutzen. Eine Nutzung von zuvor über andere Internet-Provider zugewiesene IP-Adressbereiche ist nicht möglich, die Nutzung eigener IP-Adressbereiche des Auftraggebers (PI-Adressraum) ist nach Rücksprache möglich.

6.3 Datentarif

Zur Ermittlung des Verbrauchs wird generell alle fünf Minuten der Absolutwert von ein- und von ausgehendem Datenverkehr in Byte gemessen, der über die Zugangsverbindung (Port) zum Internet fließt. Zur weiteren Berechnung werden die Differenzwerte zwischen jeweils zwei, zeitlich unmittelbar aufeinander folgenden Messintervallen gebildet, so dass das Übertragungsvolumen eines jeden Intervalls vorliegt.

Mit Ablauf eines Kalendermonats wird ein Kumulationsprozess gestartet, der die einzelnen im Abrechnungsmonat angefallenen Messwerte (Transportvolumina pro Port, jeweils ein- und ausgehender Verkehr getrennt) aggregiert:

6.3.1 Datenvolumen

Es werden alle Messwerte (Transportvolumina pro Port für ein- als auch für ausgehenden Verkehr) eines abgeschlossenen Kalendermonats summiert. Das Resultat ist das Transfervolumen des Kalendermonats. Das im monatlichen Entgelt der Option *ethernet.VPN Secure Access Gateway / Secure Access Gateway DC* vereinbarte inkludierte Transfervolumen wird mit dem Transfervolumen verrechnet. Darüber hinausgehendes Transfervolumen wir gemäß der Vereinbarung mit dem Auftraggeber zusätzlich in Rechnung gestellt.

7 Firewall im Rahmen von ethernet.VPN Secure Access

7.1 Funktion und Regelwerk

Die Firewall bei *ethernet.VPN Secure Access Gateway / Secure Access Gateway DC* filtert den Verkehr zwischen unterschiedlichen Netzen, in erster Linie zwischen dem öffentlichen Internet und dem *ethernet.VPN* des Auftraggebers. Es regelt damit die Zugriffsmöglichkeiten auf Ressourcen des *ecotel ethernet.VPN* zum Internet und vom Internet auf Ressourcen des *ecotel ethernet.VPN*.

Die Basisfunktionen der Firewall umfassen:

- IP-Paketfilter
- Port forwarding
- Network Adress Translation (NAT)
- Port+Network Adress Translation
- DoS und DDos Detection

Die Firewall gewährleistet den ausschließlichen Transport von IP-Datenpaketen. Das Regelwerk und der Transport der Daten beziehen sich daher ausschließlich auf die Netzwerkschichten drei und vier (Networklayer mit IP/ICMP und Transportlayer mit TCP/UDP). Zum Transport anderer Protokolle muss eine IP-Encapsuation eingesetzt werden, die nicht Bestandteil der Leistung *ethernet.VPN Secure Access Gateway / Secure Access Gateway DC* ist.

Mögliche Angriffe, welche sich auf IP/ICMP (Networklayer) oder TCP/UDP (Transportlayer) beziehen, werden innerhalb der Firewall erkannt und abgewehrt. Dies gilt für Angriffe auf die Firewall und die zu schützenden Netzwerke. Angriffe aus dem *ethernet.VPN* auf die Firewall, sowie Angriffe aus dem *ethernet.VPN* auf andere Netzwerke, welche über die Firewall erreicht werden, werden ebenso erkannt und abgewehrt.

Die Firewall bietet keinen Schutz vor Viren oder anderem schädlichem Code (Malicious Code), welche auf den ISO/OSI Schichten fünf, sechs oder höher verbreitet werden (Applikationsschichten).

Daten, welche nicht durch die Firewall transportiert werden, entziehen sich der Kontrolle durch die Firewall und können der Integrität der Firewall schaden. Der Auftraggeber muss daher insbesondere sicherstellen, dass keine andere ungesicherte Internetverbindung verwendet wird, welche die Firewall umgeht. Dies kann zum Beispiel bei Modems mit Anbindung an andere Netzwerke oder bei Wireless-LANs der Fall sein.

7.2 Schnittstellen

Die Firewall verfügt über mindestens zwei physikalische Layer-2-Schnittstellen, die als Gigabit Ethernet RJ45 ausgeführt sind. Schnittstellen mit höheren Geschwindigkeiten sind über einen Hardwarewechsel optional erhältlich.

Neben Ethernet werden keine anderen Layer-2 Protokolle direkt unterstützt. Die Anbindung von Netzen, welche über andere LAN-Protokolle eingebunden werden sollen, erfolgt über Medienkonverter oder IP-Router. Diese Geräte sind nicht Bestandteil von *ethernet.VPN Secure Access Gateway* / *Secure Access Gateway DC* und müssen separat beauftragt werden.

Folgende Tabelle gibt Aufschluss über die maximal zur Verfügung stehenden physikalischen und logischen Schnittstellen und die daraus resultierenden Sicherheitszonen der Firewall.

Firewall professional	
Phys. Schnittstellen / Zonen	5
Virtuelle LANs	5
Virtuelle Router	5
Firewall premium	
Phys. Schnittstellen / Zonen	10
Virtuelle LANs	10
Virtuelle Router	10

Beim Einsatz anderer Firewall-Typen als den hier aufgeführten, gelten die entsprechenden Schnittstellenparameter des jeweils eingesetzten Systems. Hierzu wird bei Bedarf eine gesonderte Vereinbarung zwischen ecotel und dem Auftraggeber geschlossen.

7.3 Firewall-Typ

Dem Auftraggeber stehen mit der Firewall professional und der Firewall premium zwei verschiedene Firewall-Typen zur Auswahl. Anhand der vom Auftraggeber übermittelten Anforderungen (z.B. gewünschte Transportleitung) wird ecotel eine Empfehlung aussprechen welcher Firewall-Typ der geeignete ist. Dennoch bleibt der Auftraggeber für die richtige Dimensionierung der Firewall und somit für die wahlweise Beauftragung der Firewall professional oder Firewall premium verantwortlich. Insbesondere sollten hier zukünftig höhere Anforderungen an die Firewall bereits Berücksichtigung finden (z.B. steigender IP-Verkehr oder steigende Anzahl VPN-Tunnel). Ein späterer Tausch der Firewall aufgrund gestiegener Anforderungen erzeugt Kosten und kann gemäß individuellem Angebot beauftragt werden.

Firewall professional	
Transportleistung *(gesamte Firewall)*	950 Mbit/s
Transportleistung *(Internet)*	Bis zu 950 Mbit/s
Routingleistung *(IP-Pakete / Sekunde)*	180 Kpps
Anzahl paralleler Sessions	900.000
Anzahl Security-Policies	Max. 5.000
Verschlüsselungs-Performance	IPSec: 75 Mbit/s SSL: 35 Mbit/s
Anzahl gleichzeitiger VPN-Tunnel	IPSec: 200 SSL: 100
Firewall premium	
Transportleistung *(gesamte Firewall)*	3 Gbit/s
Transportleistung *(Internet)*	Bis zu 1 Gbit/s
Routingleistung *(IP-Pakete / Sekunde)*	4,5 Mpps
Anzahl paralleler Sessions	1,3 Millionen
Anzahl Security-Policies	Max. 5.000
Verschlüsselungs-Performance	IPSec: 2 Gbit/s SSL: 150 Mbit/s
Anzahl gleichzeitiger VPN-Tunnel	IPSec: 500 SSL: 200

Die Daten basieren auf Herstellerangaben und geben die jeweils maximalen Werte wieder. Aus Performancegründen und zur Abpufferung von Verkehrsspitzen sollten die Auslastungen im Regelfall erheblich (≤ 80%) unter diesen maximalen Werten liegen.

7.4 Regelwerk und Änderungen

Der Auftraggeber legt eine Security-Policy fest. Gemäß dieser Policy wird von ecotel ein Regelwerk für die von ecotel bereitgestellte und gemanagten Firewall konfiguriert. Dieser Filtermechanismus arbeitet dabei auf der Ebene von IP-Netzen, IP-Nummern, ICMP Typen, TCP/UDP Ports und TCP/UDP Port Bereichen.
Das Regelwerk ist so aufgebaut, dass ein Datenpaket von einer Startadresse zu einer Zieladresse abgelehnt oder durchgelassen werden kann. Eine Ablehnung erfolgt explizit (*Reject*), indem ein ICMP-Reject an den Absender gesendet wird, oder ohne Rückmeldung an den Absender (*Silent Deny*).
Die Regeln können für eingehende und ausgehende Datenpakete definiert werden und können von der Tageszeit abhängig gemacht werden. Darüber hinaus kann auch eine Bandbreitenbegrenzung für den Datenverkehr (*Traffic-Shaping*) eingerichtet werden.
Änderungen am Regelwerk der Firewall werden von ecotel im Auftrag des Auftraggebers durchgeführt. Eine Änderung darf nur von autorisierten Personen, welche der ecotel bekannt sein müssen, beauftragt werden. Die Änderungsanfrage bedarf der Schriftform.
ecotel behält sich vor - ist jedoch nicht verpflichtet - die Änderungen auf Sinnhaftigkeit und Sicherheitsrelevanz zu überprüfen und gegebenenfalls weitere Änderungsberechtigte des Auftraggebers über die Änderung in Kenntnis zu

setzen und um Bestätigung der Änderung zu ersuchen. Der Auftraggeber ist jedoch alleine für die Auswirkungen der autorisierten Änderung in Bezug auf die Netzsicherheit verantwortlich.
Die Änderungen beziehen sich ausschließlich auf bestehende Netze und Systeme des Auftraggebers zum Zeitpunkt der Inbetriebnahme. Weitere, während der Betriebsphase, hinzugefügte Komponenten oder Netze sind nicht durch die Änderung abgedeckt und werden nach Aufwand in Rechnung gestellt. Alle weiteren Änderungen die sich auf die hinzugefügten Komponenten beziehen, werden in den Betrieb übernommen und gelten bzgl. der Änderungen dann wie bei Inbetriebnahme als Bestandssysteme und -netze.
Das Hinzufügen von VPN-Verbindungen, Änderungen der bestehenden Verbindungen oder weitere hier nicht erwähnte Änderungen sind gesondert zu beauftragen und werden nach Aufwand abgerechnet.

7.5 Betrieb und Überwachung

Der Betrieb *ethernet.VPN Secure Access* ist ein managed Service. Kosten für Hardwareaustausch bei Defekt, Software-Upgrades, Security-Patches sowie 24 x 7 Überwachung sind in den monatlichen Entgelt der Option enthalten.