ethernet.VPN Internet Access / DC
Leistungsbeschreibung

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«) eine zentrale und gesicherte Anbindung an das öffentliche Internet über die Zusatzleistung *ethernet.VPN Internet Access DC (Datacenter)* an.
Alternativ kann über die Zusatzleistung *ethernet.VPN Internet Access* auch ein dezentraler Zugang zum öffentlichen Internet an einem VPN-Standort des Auftraggebers eingerichtet werden.

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 Internet Access DC und *ethernet.VPN Internet Access* beinhalten einen, über eine dedizierte Firewall gesicherten, Zugang zum öffentlichen Internet (Internetdienst) für Standorte des von ecotel bereitgestellten und gemanagten VPN des Auftraggebers.

Bei *ethernet.VPN Internet Access DC* erfolgt der Zugang zentral und gesichert an einem ecotel Datacenter (»DC«). Die durch ecotel bereitgestellte und gemanagte Firewall befindet sich im ecotel Datacenter.
Alternativ kann *ethernet.VPN Internet Access DC* mit einer kundeneigenen Firewall im ecotel Datacenter bereitstellt werden.
Bei *ethernet.VPN Internet Access* erfolgt der Zugang dezentral und gesichert an einem VPN-Standort des Auftraggebers. Die durch ecotel bereitgestellte und gemanagte Firewall befindet sich am Standort des Auftraggebers.
Auf Wunsch kann bei *ethernet.VPN Internet Access* der dezentrale Zugang ungesichert bereitgestellt werden. Der Auftraggeber erhält in diesem Fall keine von ecotel gemanagte Firewall.

3 Internetdienst

3.1 IP-Router und Anschlussleitungen

Der Zugang zum öffentlichen Internet erfolgt auf der Infrastruktur 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 (*ecotel ethernet.VPN Internet Access*), 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 Internet Access*.

3.2 IP-Adressen

Der Auftraggeber erhält für die Dauer der Inanspruchnahme des Internetzugangs von ecotel eine öffentliche, statische IP-Adresse. 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.

3.3 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:

3.3.1 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 Internet Access / ethernet.VPN Internet Access DC* vereinbarte inkludierte Transfervolumen wird mit dem Transfervolumen verrechnet. Darüber hinausgehendes Transfervolumen wird gemäß der Vereinbarung mit dem Auftraggeber zusätzlich in Rechnung gestellt.

3.4 DDoS Protection

Der Auftraggeber hat die Möglichkeit im Rahmen der Beauftragung von *ethernet.VPN Internet Access DC* oder *ethernet.VPN Internet Access* die Produktoption »ecotel DDoS Protection« zu beauftragen.
Durch die Beauftragung von »ecotel DDoS Protection« wird die ecotel Datenleitung des Auftraggebers gegen DDoS-Angriffe geschützt. Sollte der Auftraggeber zusätzliche Anbindungen an das Internet von anderen Anbietern nutzen, sind diese nicht durch den DDoS-Schutz von ecotel geschützt.
Ein DDoS-Angriff hat zum Beispiel zum Ziel, durch eine Vielzahl gleichzeitiger Anfragen an einen Server, eine Überlastung einer IT-Infrastruktur zu erzeugen und dadurch die Verfügbarkeit von Diensten einzuschränken oder vollständig zu blockieren. Hiervon können z.B. Web-Auftritte, Public-Cloud-Dienste oder E-Mail- Systeme des Auftraggebers betroffen sein. Mit der Produktoption »ecotel DDoS-Protection« bietet ecotel dem Auftraggeber eine automatisierte DDoS Mitigation, welche DDoS-Angriffe erkennt und abwehrt. Dies erfolgt im ecotel IP Backbone durch eine kontinuierliche Echtzeit-Analyse des Trafficverhaltens der IP-Adressen des Auftraggebers. Im Falle einer DDoS Attacke und der darauf folgenden Mitigation wird der betroffene Traffic »gereinigt« noch bevor er die IT-Infrastruktur des Auftraggebers erreicht. Die ecotel DDoS Mitigationsmechanismen unterscheiden hierbei zwischen validem (»Legitimate Traffic«) und auffälligem Datenverkehr (»Attack Traffic«). Auffälliger Datenverkehr wird durch die Mitigationsmechanismen automatisch in der Regel innerhalb weniger Minuten blockiert (»Time to Mitigation« kleiner 2 Minuten) und nur der »Legitimate Traffic« an die IT-Infrastruktur des Auftraggebers weitergeleitet.

DDoS Attacken verändern sich stetig. Die ecotel Mitigationsplattform passt sich den Veränderungen laufend an. Dennoch ist es möglich, dass es vereinzelt zu »False Positive« (Legimate Traffic wird als Attack Traffic bewertet und blockiert) oder »False Negative« Fällen (Attack Traffic wird als Legitimate Traffic bewertet und nicht blockiert) kommen kann.

Die folgenden Angriffstypen werden durch ecotel DDoS Protection erkannt und abgewehrt:

- Reflection Amplification Flood Attacks (TCP, UDP, ICMP, DNS, mDNS , SSDP, NTP, NetBIOS, rpcbind , SNMP, SQL RS, Chargen , L2TP, Microsoft SQL Resolution Service)
- Fragmentation Attacks (Teardrop, Targa3, Jolt2, Nestea)
- TCP Stack Attacks (SYN, FIN, RST, ACK, SYN ACK, URG PSH, other combinations of TCP Flags, slow TCP attacks)
- Application Attacks (HTTP GET/POST Floods, slow http Attacks, SIP Invite Floods, DNS Attacks, HTTPS Protocol Attacks)
- SSL/TLS Attacks (Malformed SSL Floods, SSL Renegotiation, SSL Session Floods)
- DNS Cache Poisoning
- Vulnerability Attacks
- Resource Exhaustion Attacks (Slowloris , Pyloris , LOIC, etc.)
- Flash Crowd Protection; Attacks on Gaming Protocols

Im Falle eines DDoS-Angriffs und dessen Abwehr durch ecotel wird der Auftraggeber schriftlich benachrichtigt (»ecotel DDoS Report«). Die Benachrichtigung erfolgt in Form einer E-Mail an den, mit dem Auftrag der ecotel Datenleitung oder nachträglich benannten, »Ansprechpartner für Telekommunikation« oder »Technischen Ansprechpartner« des Auftraggebers. Der Versand des ecotel DDoS Reports kann nur erfolgen, wenn zuvor ein Ansprechpartner mit E-Mail-Adresse hinterlegt wurde.

Der ecotel DDoS Report wird in der Regel innerhalb von 60 Minuten nach Beginn des DDoS-Angriffes versendet. Der Report informiert den Auftraggeber - neben der erfolgreichen Abwehr - über den Zeitraum der Attacke, die betroffene IP-Adresse sowie den jeweiligen Angriffstyp.

4 Firewall im ecotel Datacenter

Die durch ecotel bereitgestellte und gemanagte Firewall befindet sich in einem ecotel Datacenter.

4.1 Funktion und Regelwerk

Die von ecotel bereitgestellte und gemanagte Firewall filtert den Verkehr zwischen dem öffentlichen Internet und dem *ecotel ethernet.VPN* des Auftraggebers. Dadurch werden sowohl die Zugriffsmöglichkeiten von Ressourcen des *ecotel ethernet.VPN DC* zum Internet als auch vom öffentlichen Internet auf Ressourcen des *ecotel ethernet.VPN DC* gemanaged.

Die Basisfunktionen der Firewall umfassen:

- IP-Paketfilter
- Port forwarding
- Network Adress Translation (NAT)
- Port+Network Adress Translation

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 Internet Access 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.

4.2 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 Internet Access DC / ethernet.VPN Internet Access* 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 premium	
Phys. Schnittstellen / Zonen	10
Virtuelle LANs	10
Virtuelle Router	10

4.3 Firewall-Typ

Der Auftraggeber hat die Möglichkeit eine *Firewall premium* zu beauftragen. Anhand der vom Auftraggeber übermittelten Anforderungen (z.B. gewünschte Transportleitung) wird ecotel eine Empfehlung aussprechen ob diese Firewall geeignet ist. Sollten die Anforderungen des Auftraggebers die Firewall premium übersteigen, dann kann bei Bedarf eine gesonderte Vereinbarung zwischen ecotel und dem Auftraggeber geschlossen werden. Dennoch bleibt der Auftraggeber für die richtige Dimensionierung der Firewall und somit für die Beauftragung der Firewall verantwortlich. Insbesondere sollten hier zukünftig höhere Anforderungen
an die Firewall bereits Berücksichtigung finden (z.B. steigender IP-Verkehr und höhere Transportleistung). Ein späterer Tausch der Firewall aufgrund gestiegener Anforderungen erzeugt Kosten und kann gemäß individuellem Angebot beauftragt werden.

Firewall premium	
Transportleistung *(gesamte Firewall)*	10 Gbit/s
Transportleistung *(Internet)*	Bis zu 1 Gbit/s
Anzahl paralleler Sessions	700.000
Anzahl Security-Policies	Max. 5.000
Verschlüsselungs-Performance	IPSec: 6,5 Gbit/s SSL: 900 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.

Auf Wunsch des Auftraggebers kann die durch ecotel bereitgestellte und gemanagte Firewall sich am Standort des Auftraggebers befinden (*ecotel ethernet.VPN Internet Access*). Hierzu wird bei Bedarf eine gesonderte Vereinbarung zwischen ecotel und dem Auftraggeber geschlossen.

4.4 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.

4.5 Betrieb und Überwachung

Der Betrieb *ethernet.VPN Internet Access/ ethernet.VPN Internet Access DC* 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.