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 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 dezentral ein gesicherter oder wahlweise auch ungesicherter Zugang zum Internet an einem Kundenstandort eingerichtet werden.

ecotel entwickelt zusammen mit dem Auftraggeber dabei ein bedarfsgerechtes Konzept und stimmt die technischen Möglichkeiten auf die Kundenbedürfnisse ab.

2 Standardleistungen

ethernet.VPN Internet Access DC und ethernet.VPN Internet Access beinhalten den über eine dedizierte Firewall gesicherten Zugang zum öffentlichen Internet (Internetdienst) für Standorte eines ecotel ethernet.VPN.

Der Zugang zum Internet und dessen Absicherung erfolgt dabei in der Regel in einem der ecotel Datacenter („Internet Access DC“). Alternativ dazu kann der Zugang auch an einem der Kundenstandorte erfolgen, wobei hier die Firewall dann ebenfalls am Kundenstandort steht („Internet Access“).

Wird die Absicherung über eine Firewall der ecotel nicht gewünscht, kann auch ein ungesicherter Zugang zum Internet erfolgen. In diesem Fall ist der Auftraggeber für die Firewall und deren Betrieb verantwortlich.

Für den dezentralen Zugang steht dabei Internet Access ohne Firewall zur Verfügung, der zentrale Zugang mit kundeneigener Firewall ist nicht Bestandteil der Leistung ethernet.VPN Internet Access, kann jedoch auf Basis der Housing Produkte der ecotel realisiert werden.

3 Internetdienst

Jeder einzelne Standort innerhalb des ethernet.VPN wird entsprechend dem Bedarf mit einer individuellen Bandbreite beauftragt.

3.1 IP-Router und Leitung

Der Internetzugang erfolgt auf gemeinsamer Infrastruktur (z.B. Leitung, IP-Router) von ecotel ethernet.VPN. Die maximale Bandbreite des Internetdienstes ist dabei abhängig von der zur Verfügung stehenden Infrastruktur und kann gegebenenfalls individuell auf eine kleinere maximale Bandbreite (Peak-Bandbreite) begrenzt werden.

Im Einzelfall, insbesondere beim dezentralen Internetzugang, ist die Nutzung dieser Infrastruktur nicht an allen Standorten möglich, so dass ergänzend Leitungswege und gegebenenfalls IP-Router notwendig werden. Diese sind nicht Bestandteil von ethernet.VPN Internet Access.

3.2 IP-Adressen

Der Auftraggeber erhält für den Internetdienst eine öffentliche, statische IP-Adresse aus dem PA-Adressraum (Provider Aggregatable) der ecotel zugewiesen.

Als optionale Leistung erhält der Auftraggeber unter Berücksichtigung der von der Réseaux IP Européens (RIPE) vorgegebenen Regeln (siehe Dokument ID: ripe-381) einen offiziell registrierten IP-Adressraum zugewiesen. Eine Nutzung von zuvor über andere Internet-Provider zugewiesene IP-Adressbereiche ist nicht, die Nutzung eigener IP-Adressbereiche des Auftraggebers (PI-Adressraum) nur nach Rücksprache möglich.

3.3 Datentarif

Der entstehende Datenverkehr beim Zugang zum öffentlichen Internet kann mittels verschiedener Tarifmodelle abgerechnet werden.

Zur Ermittlung des Verbrauchs wird generell alle fünf Minuten (bei Bandbreiten größer 100 MBit/s abweichend) 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) je nach Tarifmodell wie folgt aggregiert:

3.3.1 Tarifmodell Volumen

Es werden alle Messwerte (Transportvolumina pro Port für ein- als auch für ausgehenden Verkehr) eines abgeschlossenen Monates summiert. Das Resultat ist das Übertragungsvolumen des Kalendermonats. Die gegebenenfalls im Grundbetrag enthaltene Datenmenge wird mit dem Übertragungsvolumen verrechnet, das Mehrvolumen in Rechnung gestellt.

Falls mit dem Auftraggeber sowohl eine Mindestabnahme als auch ein im Grundbetrag enthaltene Datenmenge vereinbart wurde, ist die enthaltene Datenmenge nicht von der Mindestabnahme abzuziehen.

3.3.2 Tarifmodell Flat

Bei der Flat–Abrechnung wird der entstehende Datenverkehr durch ein festes, wiederkehrendes Entgelt je Monat abgegolten. Dieses Entgelt ist dabei abhängig von der beauftragten Übertragungsbandbreite die maximal zur Verfügung steht (Peak-Bandbreite).

3.3.3 Tarifmodell Bandbreite

Beim Tarifmodell der durchschnittlich genutzten Bandbreite nach 95/5 Percentil-Methode, werden alle Messwerte in aufsteigender Reihenfolge sortiert, jedoch wird nur der jeweils höhere Messwert von ein- und ausgehendem Verkehr berücksichtigt. Von den größten (volumenstärksten) Messwerten werden die obersten 5% verworfen. Der dann verbleibende größte (volumenstärkste) Messwert wird für die Berechnung der genutzten Bandbreite herangezogen.

Eine Auflösung des Datenverkehrs nach IP-Adressen und/oder verwendeten Diensten pro Port oder Kunde sowie eine permanente Kontrolle über die jeweilige Höhe des geflossenen Datenverkehrs erfolgt bei der Abrechnung der Verbrauches nicht. Maßgeblich für die Messung des entstandenen Datenverkehrs sind einzig die Messergebnisse von ecotel, die dem Auftraggeber mit Rechnungsstellung übermittelt werden.

4 Firewall

4.1 Funktion und Regelwerk

Die Firewall bei ethernet.VPN Internet Access 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 ethernet.VPN zum Internet und vom Internet auf Ressourcen des 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 Internet Access 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 und Zonen

Die Firewall verfügt über mindestens zwei physikalische Layer-2-Schnittstellen, die als Ethernet (IEEE802.3, 10/100 BaseTX) ausgeführt sind. Schnittstellen mit höheren Geschwindigkeiten sind über einen Hardwarewechsel optional erhältlich.

Die physikalischen Schnittstellen werden dabei für die Anbindung zweier sogenannter Sicherheitszonen verwendet, je eine für die gesicherte Zone und eine für die ungesicherte Zone. Werden darüber hinaus weitere Sicherheitszonen benötigt, zum Beispiel für den Betrieb einer DMZ (Demilitarisierte Zone), können optional weitere Ethernet Schnittstellen zur Verfügung gestellt werden.

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 und müssen separat beauftragt werden.

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

	Firewall professional	Firewall premium
Zahl phys. Schnittstellen / Zonen	2 (optional bis 8)	2 (optional bis 40)
Zahl virtueller LANs	10 (optional bis 50)	100
Virtueller Router	3 (optional bis 4)	6

Beim Einsatz anderer Firewall-Typen als den hier aufgeführten, gelten die entsprechenden Schnittstellenparameter des jeweils eingesetzten Systems.

4.3 Firewall-Typen

Entsprechend den erforderlichen Übertragungsbandbreiten und weiterer Performancekriterien stehen dem Auftraggeber zwei Firewall-Typen zur Verfügung. ecotel stimmt dabei zusammen mit dem Auftraggeber die technischen Bedürfnisse ab und schlägt einen der beiden Firewall-Typen zur Nutzung vor. Der Auftraggeber bleibt aber verantwortlich für die korrekte Dimensionierung der Firewall auf Basis folgender Daten, insbesondere bei einem zukünftigen Wachstum der Anforderungen (z.B. steigender IP-Verkehr oder steigende Anzahl VPN-Tunnel):

	Firewall professional	Firewall premium
Transportleistung der gesamten Firewall	160 MBit/s	350 MBit/s
Routingleistung in IP-Paketen je Sekunde	30.000	100.000
Anzahl paralleler Sessions	8.000 (optional bis 16.000)	48.000
Anzahl Security-Policies	max. 200	max. 1.000
Verschlüsselungs-Performance (bei 3DES+SHA1)	40 MBit/s	100 MBit/s
Anzahl gleichzeitiger VPN-Tunnel	20 (optional bis 40)	500

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.

4.4 Regelwerk und Änderungen

Gemäß der Security-Policy des Auftraggebers wird ein Regelwerk für die 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 erfolgt 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 auf Bedarf 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 den Vertrag abgedeckt und werden nach Aufwand in Rechnung gestellt. Alle weiteren Änderungen die sich auf die hinzugefügten Komponenten beziehen, werden in den normalen 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 ist ein Full-Service. Kosten für Hardwareaustausch bei Defekt, Software-Upgrades, Security-Patches sowie 24 x 7 Überwachung sind in den monatlichen Betriebskosten enthalten.

ecotel communication ag, Prinzenallee 11, D-40549 Düsseldorf
Tel.: +49 (0) 211 55 007 0, Fax +49 (0) 211 55 007 222
www.ecotel.de