Leistungsbeschreibung

RIEDEL Managed MPLS VPN

Produktrelease 5.2

Riedel Networks GmbH & Co. KG

Datum: 23.05.2013

Dokumentenversion 1.05

Status: Freigegeben

1 Technische Realisierung des Riedel Managed MPLS VPN

1.1 MPLS

MPLS – der internationale Standard für virtuelle private IP-Netze

Die im Netzwerk der Riedel Networks eingesetzte Technologie heisst MPLS. MPLS steht für „Multi Protocol Label Switching“ und ermöglicht den Betrieb vieler paralleler und unabhängiger IP Netze auf derselbe Infrastruktur.

Die Produkte von Riedel Networks sind entsprechend den internationalen Standards der IETF implementiert, die Realisierung der VPN ist konform mit RFC 4364.

1.2 MPLS Layer 3 VPN

Sichere Netze durch private Verbindungen

Im Gegensatz zu den häufig eingesetzten IP VPNs und um für unsere Kunden ein Höchstmass an Sicherheit und Zuverlässigkeit zu erreichen, sind die Kommunikationswege und die Infrastruktur des Riedel Networks MPLS Netzes vollständig vom Internet getrennt, für Anschlüsse und Zugänge werden keine Internetanschlüsse mit öffentlichen IP-Adressen verwendet. Nur die Verwendung privater Kommunikationswege schützt Unternehmensstandorte, Home Offices und mobile Teilnehmer vollständig vor Angriffen aus dem Internet.

Eine Verbindung zum Internet wird in einem RIEDEL Managed VPN ausschliesslich für die externe Kommunikation hergestellt. Die Verknüpfung zum Internet erfolgt über zentrale Firewall Systeme, welche einen geschützten und kontrollierten Zugang aus den privaten Netzen in das Internet ermöglichen. Die Nutzung der zentralen Firewall Services ist optional.

1.3 IP Adressen im MPLS Layer 3 VPN

Ein wesentliches Merkmal eines MPLS Layer 3 VPN ist, dass es ein völlig autonomes IP-Netz darstellt.

Demzufolge gibt es im Wesentlichen keine Restriktionen für die Nutzung von IP-Adressen. Im Kundennetz können ohne Einschränkung private IP-Adressen gemäss RFC1918 verwendet werden. Die Verwendung (legaler oder „illegaler“) öffentlicher Adressen innerhalb eines VPN ist zwar nicht empfehlenswert, jedoch ebenfalls möglich.

Einzige Einschränkung für die freie Verwendbarkeit von IP-Adressen durch den Kunden ist ein Adressbereich, welcher von Riedel Networks für die virtuellen Router im MPLS-Netz sowie für die CN-Services (siehe Abschnitt 4) genutzt wird. Hierbei handelt es sich um den Adressraum des Class-A Netzes 2.0.0.0/8, welcher im Regelfall *innerhalb* der Kundennetze nicht verwendet wird.

Da Riedel Networks einen Ende-zu-Ende Service bis zur LAN-Schnittstelle liefert, müssen die vom Kunden verwendeten IP-Adressen Riedel Networks für die Einrichtung des VPN bekannt sein. Dies beschränkt sich jedoch auf die Kenntnis der jeweiligen Subnetze in den Kundenstandorten. Die entsprechenden Daten werden nach Vertragsabschluss erfasst und müssen vom Kunden zur Verfügung gestellt werden.

1.4 Bandbreitengarantie

Um eine Festlegung auf einzelne Punkt-zu-Punkt Verbindungen zu vermeiden, wurde im Riedel Networks Netz das Konzept der Committed Access Rate (CAR) umgesetzt. Ab dem Eintritt in das Riedel Networks MPLS-Netz ist der Weg von Datenpaketen nicht durch PVC’s oder Tunnel festgelegt, sondern wird dynamisch geroutet. Die Bandbreitengarantie der Committed Access Rate bedeutet, dass die Bandbreite einer Eingangsleitung nicht statisch auf festgelegte Ziele aufgeteilt wird, sondern dass diese Bandbreite sich dynamisch je nach Verkehrsaufkommen des Kunden auf verschiedene Ziele im VPN verteilt. Die Summe der Bandbreiten der Verkehrsströme wird unabhängig von den jeweiligen Zielen bis zur Höhe der für die Anschlussleitung garantierten Gesamtbandbreite innerhalb des MPLS-Netzes garantiert.

1.5 Kapazitätsmanagement

Um Engpässe im Kernnetz der Riedel Networks zu vermeiden, wird die Auslastung aller Verbindungen im Netz ständig überwacht. Bei Überschreitung eines Schwellwertes von 60% werden automatisch Erweiterungsmassnahmen initiiert.

1.6 Redundanz

Die Verfügbarkeit des Riedel Networks MPLS-Netzes wird im Kernnetz, dem Backbone, bestimmt durch ein konsequent redundantes Netzdesign, alle Komponenten im Riedel Networks Netz sind doppelt ausgelegt. Einzelheiten zur Verfügbarkeit des Kernnetzes können Abschnitt 6.2 entnommen werden. Für die Kundenanschlüsse und Netzzugänge der einzelnen Produktgruppen gelten unterschiedliche Einzelverfügbarkeiten, siehe ebenfalls Abschnitt 6.2.

1.7 Automatisierung / Überwachung

Eine wesentliche Voraussetzung für eine gleichbleibend hohe Service Qualität ist die weitgehende Automatisierung aller Funktionen im Riedel Networks Netz. Ein Kunden-MPLS VPN kann vollständig aus den Produkt- und Anschlussinformationen in der Kundendatenbank reproduziert werden.

Dies bedeutet, dass sich die Inbetriebnahme, Änderung oder Umschaltung von Anschlüssen, aber auch die Überwachung und die Behebung von Störungen im Netz wesentlich vereinfachen, da Fehler durch manuelle Einstellungen vermieden werden.

Die Standardisierung und Automatisierung bedeuten jedoch auch Sicherheit. Die Reproduzierbarkeit der VPN-Konfiguration ermöglicht einen Soll-Ist-Vergleich aller VPN-Komponenten. So werden Fehler oder Manipulationen schnell und sicher entdeckt.

1.8 Routing

Ein wesentlicher Unterschied eines MPLS-VPN im Vergleich zu einfachen IP-VPNs ist die Verlagerung der Routing Funktionen von den CE-Routern (Customer Edge) auf die PE-Router (Provider Edge).

Entsprechend der Physik gibt es vom Standort des Kunden nur eine Richtung zum Netz. Die Intelligenz der Routing-Entscheidung ist dort realisiert, wo tatsächlich die Entscheidung zwischen verschiedenen physikalischen Wegen zu treffen ist, nämlich im Netz des Providers.

Da aber viele unterschiedliche Kunden-IP-Netze, welche im MPLS-Netz zusammentreffen, häufig dieselben IP-Adressen verwenden und als völlig separate IP-Netze realisiert werden müssen, benötigt jedes VPN im Prinzip eigene Router. Diese sind als „virtuelle Router“ pro VPN in der Software des MPLS Netzes umgesetzt.

Transitverkehr

Da einfache IP-VPNs in der Regel nicht any-to-any vernetzt sind, werden IP Pakete dort oft nicht direkt zum Zielort transportiert, sondern passieren auf dem Weg mehrere Kundenstandorte, abhängig von der Topologie der logischen Verbindungen, also der PVC’s oder Tunnel. Diesen Effekt nennt man Transitverkehr.

Anders als in diesen Punkt-zu-Punkt Netzen, wo Routing Entscheidungen am Netzrand (Customer Edge) getroffen werden, gibt es in einem MPLS Layer 3 VPN keinen Transitverkehr. Da die Routing-Funktionen des MPLS VPN im Netz realisiert sind (Provider Edge), werden IP Pakete immer auf dem direkten Weg zum Zielort transportiert. Dies erhöht die Effizienz der Bandbreitennutzung der Zugangsleitungen erheblich und ermöglicht die Einhaltung von Service Levels auf IP Ebene anstelle der Transportebene.

1.9 Schnittstellen

Die Terminierung der VPN-Anschlüsse in den Standorten des Kunden geschieht durch einen CE-Router, welcher sich im Eigentum der Riedel Networks befindet und im Auftrag von Riedel Networks vor Ort installiert wird.

Die Übergabepunkte der VPN-Anschlüsse beim Kunden sind eine oder mehrere LAN Schnittstellen der CE-Router. Für alle Anschlussbandbreiten werden 100BaseT FastEthernet Schnittstellen bzw. 1000BaseT und 1000Base-LX GigabitEthernet Schnittstellen zur Verfügung gestellt. Für Anschlüsse auf Kupfer-Basis ist die Steckverbindung vom Typ RJ45/Cat5, bei Glasfaser-Anschlüssen vom Typ SC/PC oder LC/PC.

Die Anzahl der Schnittstellen pro Standort und ggf. die Zuordnung zu mehreren VPNs wird vom Kunden im Rahmen der Erfassung der technischen Parameter nach Auftragserteilung festgelegt. In der Regel wird genau eine LAN Schnittstelle pro Standort zur Verfügung gestellt.

Die Riedel Networks CE-Router, welche in den Kundenstandorten mit Anschluss zum Kunden LAN installiert werden, benötigen IP-Adressen im Adressraum des Kunden. Hierzu sollten vom Kunden drei nutzbare IP-Adressen jedes Subnetzes freigehalten werden.

Eine der drei reservierten IP-Adressen fungiert als sogenanntes „Default Gateway“ für die Endgeräte im LAN des Kunden. Die beiden übrigen Adressen werden gegebenenfalls für die Realisierung von Backup Optionen benötigt (siehe auch Abschnitt 3).

2 Access Optionen

2.1 Leased Line Access

Standortanbindung über Festverbindungen

Leased Line Access ist geeignet für zentrale Standorte und Rechenzentren, aber auch für mittlere Standorte mit hohem Brandbreitenbedarf und sehr hohen Qualitätsanforderungen. Der Kundenstandort wird über eine Festverbindung mit dem nächsten MPLS-Knoten der Riedel Networks verbunden.

Leased Line Access wird mit einer Bandbreite von 2 Mbit/s – 155 Mbit/s angeboten. Die möglichen Bandbreitenabstufungen hängen von der technischen Verfügbarkeit vor Ort ab.

Für die Realisierung der 4 -10 Mbit/s Anschlüße werden n x 2 Mbit/s Leitungen zu einer transparenten Verbindung gebündelt. Anschlüsse, Router und vor Ort Inbetriebnahme sind Bestandteil der Riedel Networks Dienstleistung. Dieser Anschlusstyp ist international verfügbar.

Für hochverfügbare Anwendungen bietet Riedel Networks optional eine doppelte Anbindung von Standorten an das Netz (HA Option siehe Abschnitt 0). Alternativ kann zwischen verschiedenen Backup Optionen gewählt werden (Einzelheiten hierzu finden sich in Kapitel 3)

2.2 Ethernet Access

Standortanbindung über Ethernet

Ethernet Access ist geeignet für zentrale Standorte und Rechenzentren, aber auch für mittlere Standorte. Der Kundenstandort wird über eine Ethernet-Verbindung mit dem nächsten MPLS-Knoten der Riedel Networks verbunden.

Ethernet Access wird mit einer Bandbreite von 2 Mbit/s – 1.000 Mbit/s angeboten. Die möglichen Bandbreitenabstufungen hängen von der technischen Verfügbarkeit vor Ort ab.

Bei Bandbreiten bis zu 10 Mbit/s wird in der Regel eine Kupfer-basierte Leitung benötigt, somit ist die Realisierung in der Regel unproblematisch. Bei Bandbreiten grösser 10 Mbit/s wird ein Anschluss mittels Glasfaser notwendig, hier können Baukosten in unbestimmter Höhe anfallen. Dieser Anschlusstyp ist international verfügbar.

Für hochverfügbare Anwendungen bietet Riedel Networks optional eine doppelte Anbindung von Standorten an das Netz (HA Option siehe Abschnitt 0). Alternativ kann zwischen verschiedenen Backup Optionen gewählt werden (Einzelheiten hierzu finden sich in Kapitel 3)

2.3 SDSL Access

Standortanbindung über SDSL

Die Anbindung über SDSL eignet sich für die meisten mittelgrossen oder kleineren Standorte eines Unternehmens mit durchschnittlichen Verfügbarkeits-und Bandbreitenanforderungen. Der Kundenstandort wird über eine symmetrische DSL Verbindung (SDSL) mit nächsten MPLS-Knoten der Riedel Networks verbunden.

SDSL Access wird mit einer Bandbreite von 1 Mbit/s – 20 Mbit/s angeboten. Die möglichen Bandbreitenabstufungen hängen von der technischen Verfügbarkeit vor Ort ab.

Für die Realisierung von Bandbreiten > 2 Mbit/s werden in der Regel mehrere SDSL Verbindungen gebündelt. Anschlüsse, Router und vor Ort Inbetriebnahme sind Bestandteil der Riedel Networks Dienstleistung.

2.4 ADSL Access

Standortanbindung über ADSL

Die ADSL Anschlüsse sind auf Grund der asymmetrischen Bandbreiten der Anbindung typischerweise nur für kleinere Firmenstandorte mit wenigen Benutzern und ggf. überwiegendem Internet Verkehr geeignet. Die möglichen Bandbreitenabstufungen für ADSL Access sind in Deutschland:

1 Mbit/s / 128 kbit/s , 2 Mbit/s / 384 kbit/s , 6 Mbit/s / 576 kbit/s und 16 Mbit/s / 1024 kbit/s *(Downstream / Upstream)*

In anderen europäischen Ländern werden hiervon abweichende Downstream und Upstream Bandbreiten angeboten. Die erforderlichen ADSL-Anschlüsse im Kundenstandort sind innerhalb Deutschlands und in mehreren Ländern sind Bestandteil der Riedel Networks Dienstleistung. In einigen Ländern müssen die ADSL-Anschlüsse jedoch vom Kunden bereitgestellt werden.

2.5 UMTS Remote Access

UMTS Access bietet einen geschützten Zugang über GPRS bzw. UMTS. Die UMTS/GPRS-Anschlüsse terminieren wie bei den übrigen Access Varianten in einem Riedel Networks CE-Router mit einer kundenseitigen LAN Schnittstelle. Die Übergabe erfolgt auf einem Fast Ethernet-Port. Verlängerungskabel für den Anschluss der UMTS Antenne an einen gegebenenfalls besseren Empfangsstandort sind nicht im Lieferumfang enthalten, können aber optional bis zu einer Länge von ca. 10 Metern angeboten werden.

2.5.1 UMTS national

Voraussetzung für die Nutzung des Dienstes ist ein Standard UTMS Kartenvertrag von T-Mobile. Der UMTS Kartenvertrag und die Datenkarte sind nicht Bestandteil der Dienstleistung der Riedel Networks. Die Berechnung des UMTS/GPRS Zuganges erfolgt über eine pauschale Monatsgebühr pro Datenkarte.

Die T-Mobile SIM Karte muss im Vorfeld zum Einbau in den Router der Riedel Networks zur Verfügung gestellt werden.

2.5.2 UMTS international

Über den Partner Hutchinson 3G kann eine SIM Karte zur Verfügung gestellt werden, die in nachfolgenden Ländern roamingfrei genutzt werden kann: Österreich, Italien, Grossbritannien, Irland, Schweden, Dänemark und Hongkong.

Es besteht die Möglichkeit der Abrechnung per Datenvolumen oder per „Flat“-Abrechnung. Bei den eingesetzten SIM-Karten handelt es sich um reine Datenkarten, die nicht für Telefonie freigeschaltet sind.

2.6 IPsec Remote Access

Riedel Networks ermöglicht es den Mitarbeitern seiner Kunden, sich mit Hilfe eines Cisco® VPN-Remote-Client über das öffentliche Internet und einen IPSec-Tunnel mit dem MPLS VPN zu verbinden. Dabei erfolgt die Authentisierung der Benutzer mit erhöhter Sicherheit, indem ein doppelter Sicherheitsmechanismus über Passwort kombiniert mit Security Token (One-Time-Password Generator) eingesetzt wird.

Die maximale nutzbare Bandbreite aller IPsec User in einem MPLS VPN wird in Absprache mit dem Kunden definiert.

Riedel Networks stellt den Benutzern des Kunden den Security Token (One-Time-Password Generator) zur Verfügung. Es können ggf. auch bereits seitens des Kunden angeschaffte Security Token genutzt werden, soweit diese den OATH Standard unterstützen.

So ist – ob von zu Hause oder von einem Wireless Hotspot aus – immer eine sichere Verbindung zum Unternehmensnetzwerk möglich.

3 Backup Optionen

Die verschiedenen Optionen funktionieren als Backup für Leitungsausfälle der Primärleitung. Die Backupverbindungen arbeiten grundsätzlich mit einem zusätzlichen CE Router. Auf der LAN Seite muss HSRP (Hot Standby Routing Protocol) verwendet werden, um eine Umschaltung des aktiven Routers für die Endgeräte im LAN transparent zu machen. Das Backup wird automatisch aufgebaut. Der Anschluss verhält sich im Wesentlichen wie im Normalbetrieb, gegebenenfalls mit reduzierter Bandbreite.

3.1 High Availability (HA)

Für hochverfügbare Anwendungen bietet die HA-Option eine doppelte Standortanbindung über zwei Anschlussleitungen an zwei unterschiedliche MPLS Switches im Netz der Riedel Networks. Für die Verbindungen wird ein dynamisches Routing implementiert.

Beide Leitungen werden im Normalbetrieb soweit möglich im Load Sharing genutzt. Auf Grund der Terminierung der Leitungen auf verschiedenen MPLS Switches im Netz kann jedoch eine 1:1 Lastverteilung nicht realisiert werden, so dass nur die Bandbreite einer Leitung als CAR garantiert werden kann. Eine Schaltung der Hauseinführung über verschiedene Kabel kann nicht gewährleistet werden.

3.2 Leased Line Backup

Die Leased Line Backup Option wird mit einer Bandbreite von 2 Mbit/s – 155 Mbit/s angeboten. Die möglichen Bandbreitenabstufungen hängen von der technischen Verfügbarkeit vor Ort ab.

Für die Realisierung der 4 -10 Mbit/s Anschlüße werden n x 2 Mbit/s Leitungen zu einer transparenten Verbindung gebündelt. Anschlüsse, Router und vor Ort Inbetriebnahme sind Bestandteil der Riedel Networks Dienstleistung. Dieser Backuptyp ist international verfügbar.

3.3 Ethernet Backup

Die Ethernet Backup Option wird mit einer Bandbreite von 2 Mbit/s – 1.000 Mbit/s angeboten. Die möglichen Bandbreitenabstufungen hängen von der technischen Verfügbarkeit vor Ort ab.

Bei Bandbreiten bis zu 10 Mbit/s wird in der Regel eine Kupfer-basierte Leitung benötigt, somit ist die Realisierung in der Regel unproblematisch. Bei Bandbreiten grösser 10 Mbit/s wird ein Anschluss mittels Glasfaser notwendig, hier können Baukosten in unbestimmter Höhe anfallen. Anschlüsse, Router und vor Ort Inbetriebnahme sind Bestandteil der Riedel Networks Dienstleistung. Dieser Backuptyp ist international verfügbar.

3.4 SDSL Backup

Die SDSL Backup Option wird mit einer Bandbreite von 1 Mbit/s – 20 Mbit/s angeboten. Die möglichen Bandbreitenabstufungen hängen von der technischen Verfügbarkeit vor Ort ab.

Für die Realisierung von Bandbreiten > 2 Mbit/s werden in der Regel mehrere SDSL Verbindungen gebündelt. Anschlüsse, Router und vor Ort Inbetriebnahme sind Bestandteil der Riedel Networks Dienstleistung. Dieser Backuptyp ist international verfügbar.

3.5 ADSL Backup

Das ADSL Backup funktioniert als Backup für Leitungsausfälle. Die ADSL Backup Verbindungen arbeiten mit einem zusätzlichen CE Router.

Die möglichen Bandbreitenabstufungen hängen vom Angebot der örtlichen Telekommunikations-unternehmen und von der technischen Verfügbarkeit vor Ort ab. Anschlüsse, Router und vor Ort Inbetriebnahme sind Bestandteil der Riedel Networks Dienstleistung. In einigen Ländern müssen die ADSL-Anschlüsse jedoch vom Kunden bereitgestellt werden.

3.6 UMTS Backup

Die UMTS Backup Option wird über das UMTS Mobilfunknetz als Backup für Leitungsausfälle realisiert. Die UMTS Backup Option wird in einem einfachen (nicht gedoppelten) CE-Router realisiert, der sowohl die jeweilige Anschlussleitung terminiert als auch ein UMTS Modul enthält und die Umschaltung im Backup Fall steuert.

Im Backup Fall wird über das UMTS Mobilfunknetz eine Einwahlverbindung aufgebaut, wenn Datenpakete vom Kundenstandort in das MPLS VPN des Kunden geschickt werden. Der Wählvorgang ist für die Endgeräte im LAN des Kunden transparent, für diese verhält sich der Anschluss im Wesentlichen wie im Normalbetrieb, gegebenenfalls mit reduzierter Bandbreite. Abweichend vom Normalbetrieb kann es kurzzeitig zu Verzögerungen beim Transport der Pakete oder zu Paketverlusten kommen, was von der Auslastung der Mobilfunkzelle und den dort verfügbaren Kapazitäten abhängt.

3.7 IPsec Backup

IPsec Backup verbindet fest angebundene Standorte über einen zusätzlichen CE-Router und IPSec-Tunnel über einen Internetanschluss eines anderen Anbieters mit dem Riedel Networks MPLS VPN. Dabei stellt der Kunde den vor Ort erforderlichen Internet-Anschluss zur Verfügung, wobei eine **statische**, **öffentliche IP Adresse** exklusiv für das IPSec Backup bereitgestellt werden muss. Bereitstellung und Entstörung des Internet Anschlusses liegen im Verantwortungsbereich des Kunden.

3.8 Hardware-Redundanz CE Router

Um die Wiederherstellungszeit bei Ausfall eines CE Routers zu reduzieren, wird mit dieser Option ein zweiter, identischer CE Router installiert, der im „Warm-Standby“ mitläuft. Bei Konfigurationsänderungen des Haupt-Router wird der Standby-Router entsprechend aktualisiert, so dass der Kunde bei Ausfall des Haupt-Router die Anschlussleitung und die LAN Verbindungen auf den Backup-Router umstecken kann.

4 Service Optionen

4.1 Multi-CN – mehrere logische Netze pro Anschluss

Um komplexe Sicherheitskonzepte und Netzarchitekturen für Unternehmen und Unternehmens-gruppen zu realisieren, können pro physikalischem Standortanschluss eines Kunden auch mehrere logisch getrennte VPNs geschaltet werden, indem die Multi-CN-fähige MPLS-Plattform der Riedel Networks bis zum Kundenrouter erweitert wird.

Mit der Multi-CN Funktion werden am CE-Router im Kundenstandort separate LAN-Schnittstellen oder VLANs pro logischem Netz zur Verfügung gestellt. Es gibt keine Restriktionen hinsichtlich der Verwendung überlappender IP-Adressen in den verschiedenen CNs.

Die Multi-CN Funktion erlaubt eine flexible Trennung von Diensten und Benutzergruppen auf einer physikalischen Anschlussleitung. Anstelle von mehreren privaten Netzen kann mit der Multi-CN Funktion auch ein transparenter Internetzugang parallel zu einem privaten IP-Netz geschaltet werden.

4.2 Riedel Extranet – die Business-to-Business Lösung

Ein Managed VPN der Riedel Networks bietet standardmässig über die Any-to-Any Kommunikation zwischen den Teilnehmern ein hohes Mass an Flexibilität. Für Anwendungsbereiche im B2B Bereich werden allerdings dedizierte Kommunikationsverbindungen benötigt.

Verschiedene Geschäftspartner sollen zentrale Anwendungen im Kunden-VPN nutzen, ohne dass das hohe Sicherheitsniveau eingeschränkt wird.

Hierfür bietet die Riedel Networks eine Extranet-Lösung mit einer sternförmigen Netztopologie an. Diese Variante bietet alle Leistungsmerkmale eines Riedel Networks Managed VPN mit der Ausnahme, dass die Kommunikationsverbindungen nur Punkt-zu-Punkt möglich sind. Der Sternmittelpunkt wird von dem zentralen Serverbereich gebildet, auf den die Geschäftspartner Zugriff haben sollen.

Die Riedel Networks stellt mit dem Riedel Extranet eine leistungsfähige B2B Plattform zur Verfügung mit der der Kunde seine Geschäftspartner sicher und zuverlässig in seine Kommunikationsstruktur einbinden kann. In Kombination mit der Multi-CN Funktion kann der Kunde somit das VPN für sein Intranet um eine homogene Lösung für das Extranet erweitern.

4.3 SNMP Readonly

Auf Wunsch richtet Riedel Networks dem Kunden SNMP-Lesezugriff auf die CE Router ein. Dieser Zugriff gibt dem Kunden die Möglichkeit, Serviceparameter der CE Router für eigene Auswertungen hinsichtlich Verfügbarkeit und Auslastungsstatistiken abzurufen.

Auf den CE Routern wird das SNMP Protokoll in der Version 2c bereitgestellt.

Der Kunde nennt Riedel Networks die IP-Adresse(n) von maximal 4 Systemen innerhalb seines VPN , die für SNMP-Readonly Anfragen auf die CE Routern freigeschaltet werden. Als Zieladresse für SNMP Anfragen steht dem Kunden die LAN IP des/der CE Router zur Verfügung. Der Kunde legt den community-string fest, der für die Anfragen verwendet werden soll und teilt diesen Riedel Networks mit. Um eine Überlastung der CE Router (und damit ggf. Beeinträchtigung der Anbindung) bei zyklischen Abfragen zu vermeiden, sollten Abfragen nicht öfter als alle 5 Minuten durchgeführt werden.

4.4 Internetzugang über zentrale Firewall Systeme

Jedes Unternehmen benötigt neben der internen Connectivity auch eine Verbindung zum Internet für die externe Kommunikation des Unternehmens. Optional stellt Riedel Networks einen geschützten Zugang zum Internet zur Verfügung, welcher das VPN über zentrale Firewall Systeme mit dem Internet verbindet.

Die Firewall Systeme für den zentralen Firewall Service sind ebenso wie die Upstream Verbindungen zum Internet redundant ausgelegt. Funktional handelt es sich um sogenannte Application Layer Firewalls, welche den höchsten technisch möglichen Schutz-Level darstellen. Das heisst, dass es keine direkten IP-Verbindungen aus einem Riedel Networks Managed VPN in das Internet gibt, direkte Verbindungen (auch über Paketfilter oder NAT) werden vollständig unterbunden. Auf diese Weise werden alle Angriffe auf Port- oder IP-Ebene vollständig und sicher von allen Systemen innerhalb eines VPN ferngehalten.

Statt dessen geschieht die Kommunikation indirekt über sogenannte Application Layer Proxies, welche die internen und die externen IP-Verbindungen terminieren und auf Anwendungsebene getrennte Verbindungen nach innen und aussen aufbauen. Hierdurch können nur Verbindungen hergestellt werden, für die explizit ein Application Proxy auf den Firewall Systemen zur Verfügung steht.

Riedel Networks garaniert die vertraglich vereinbarten Internet Bandbreiten bis zu einem Tier-1 oder Tier-2 Upstream Provider. Der Internetzugang kann in Bandbreitenstufen von 1 Mbit/s bereitgestellt werden. Die Bandbreitengarantien enden an der Schnittstelle von Riedel Networks zu anderen Internet Service Providern auf der Internetseite der Firewall Systeme.

Die folgenden Kommunikationsfunktionen bietet der Application Layer Firewall Service:

Webzugang von innen nach aussen

Ein http/https/ftp Proxy stellt für die Teilnehme im Managed VPN den gewohnten Internet Zugang zur Verfügung. Die heruntergeladenen Inhalte order die URL's werden nicht protokolliert oder gefiltert.

Die Freigabe dieser Firewall Funktion kann entweder für das gesamte VPN, für einzelne Subnetze oder dediziert für einzelne IP-Adressen erfolgen. Standardkonfiguration ist die Freigabe für das gesamte Managed VPN.

Mail Transport bidirektional

Die Firewall Systeme stellen eine SMTP Proxy Funktion für den Mailtransport aus den VPN's ins Interne und umgekehrt zur Verfügung. Die Steuerung des Mail Routings geschieht sowohl intern als auch extern über DNS. Hierzu nutzen die Firewall Systeme einen speziellen internen DNS Service der Riedel Networks.

Sofern die Mail Server innerhalb des Kunden-VPN den internen DNS (Domain Name Service) der Riedel Networks nutzen, ist keine Änderung der Konfiguration der Mail Server erforderlich – diese „finden" die Firewall Systeme automatisch, deren Addresse sie über den internen DNS erhalten. Dies gilt auch in umgekehrter Richtung: die Firewall Systeme „finden" die Mail Server über deren Einträge im internen DNS.

Auf Grund der engen Verflechtung der Firewall Systeme mit dem DNS ist die Nutzung des VPN Firewall Service nur möglich in Verbindung mit der Nutzung des internen DNS der Riedel Networks sowie der Administration der Internet Domains des Kunden durch Riedel Networks (siehe Abschnitt 4.6).

Virencheck und Spamfilter

Die Funktion des Mail Gateways beinhaltet eine Basis-Schutzfunktion gegen Viren und Spam. Eingehende Mails werden durch einen Viren-Filter auf Viren untersucht, infizierte Anhänge werden gelöscht. Ebenso findet eine Spam-Filterung statt. Abhängig von der Klassifizierung werden die Mails entweder gelöscht oder durch eine Header-Option als Spam gekennzeichnet bzw. an eine „spam-admin" Addresse beim Kunden zugestellt. Darüber hinaus findet keine Filterung von Inhalten statt, ein Logging von Absender- oder Empfängerinformationen von Emails findet ebenfalls nicht statt.

Reverse Proxy

Diese Funktion ermöglicht es, Webserver sicher innerhalb des VPN aufzustellen, und diese über die Firewall Systeme im Internet indirekt „sichtbar" zu machen. Diese Funktion ist Bestandteil des Web Mirror Service (Abschnitt 4.7), kann jedoch auch separat genutzt werden. Der Reverse Proxy unterstützt die Protokolle http/https/ftp.

4.5 Transparenter Internetzugang

Alternativ zu dem Internetzugang mit zentraler Firewall kann ein transparenter Internetzugang parallel zu einem Kunden-VPN bereitgestellt werden. In diesem Fall ist der Kunde selbst für die Absicherung durch Firewall Systeme verantwortlich. Der transparente Internetzugang ist ein qualitativ hochwertiger Internetanschluss, der innerhalb des Riedel Networks Netzes ohne Überbuchung bis zu einem Internet-Upstream-Provider durchgeschaltet wird.

Bestandteil des Dienstes ist standardmässig die Bereitstellung eines /29 Subnetzes mit 5 nutzbaren, statischen IP-Adressen pro Anschluss. Bei Bedarf können auch grössere Adressbereiche zur Verfügung gestellt werden.

Der Internetzugang kann in Bandbreitenstufen von 1 Mbit/s bereitgestellt werden. Voraussetzung für die Nutzung des transparenten Internetzuganges ist ein VPN-Anschluss mit Multi-CN Funktion, siehe Abschnitt 4.1.

4.6 Administration von Internet Domains

Ein ergänzender Service zum geschützten Internetzugang über Firewall ist die Administration der Internet Domains des VPN Kunden. Da die Funktion der Firewall Systeme z.B. für das Mail Routing eng mit der Administration von Domain Namen und Name Service verknüpft ist, ist dieser Service automatisch Bestandteil bzw. Voraussetzung des Firewall Service.

Enthalten in diesem Service sind alle Aktivitäten zur An- und Ummeldung und für Änderungen von Domain Namen. Riedel Networks übernimmt selbstverständlich auch technische Bereitstellung und Pflege der Domains im internationalen Name Service.

4.7 Web Mirror

Der Web Mirror Service ist eine elegante und vor allen Dingen sichere Alternative zum klassischen Web Hosting. Der Service wird realisiert durch redundante Web Mirror Systeme im Internet, welche über den Reverse Proxy (siehe Abschnitt 4.1) mit dedizierten Webservern innerhalb des Kunden-VPN kommunizieren können.

Dies bedeutet, dass ein VPN-Kunde seine Webserver geschützt innerhalb des VPN aufstellen kann. Dorthin gibt es jedoch keine direkte Verbindung aus dem Internet. Daher werden die Webseiten der im VPN befindlichen freigegebenen Webserver des Kunden vollautomatisch über die Reverse Proxy Funktion des Firewall Service auf den Riedel Networks Web Mirror im Internet gespiegelt. Der Spiegelserver bedient alle Anfragen von Kunden und Besuchern, auch wenn die internen Systeme kurzzeitig nicht erreichbar sind.

Zur Gewährleistung der Aktualität des Spiegelservers ist jedoch eine permanente Verbindung über den Reverse Proxy zu den Webservern des Kunden erforderlich. Dynamische Inhalte können nicht gespiegelt werden, in diesem Fall greift der Web Mirror Service in Echtzeit über den Reverse Proxy auf die Webserver des Kunden zu. Eine direkte Verbindung von Benutzern im Internet zu den Webservern des Kunden wird jedoch auch in diesem Fall nicht aufgebaut.

5 Quality of Service

5.1 Priorisierung von IP Traffic

Wenn auf den VPN-Anschlüssen zeitweise eine Auslastung der Anschlussbandbreite vom Kundenstandort zum VPN von 100% erreicht wird, so wird unspezifisch für alle Anwender und Anwendungen die Performance der Netznutzung deutlich reduziert. Um eine kostenoptimale Dimensionierung der Leitungen zu ermöglichen, können IP Pakete auf der Zugangsleitung zwischen CE (Customer Edge) und PE (Provider Edge) nach IP-Adressen oder Portnummern in Serviceklassen priorisiert werden. Da Riedel Networks keinen Einfluss auf den vom Kunden erzeugten Traffic hat, erfolgt die Steuerung über eine Priorisierung von IP Paketen. Die Priorisierung kann serverbezogen über die Absender oder Empfänger IP-Adressen erfolgen, oder anwendungsbezogen über die Portnummern der Datenpakete.

5.2 Diensteklassen (Classes of Service)

Riedel Networks unterstützt die speziellen Anforderungen für die Realisierung komplexer VPN Strukturen durch ein intelligentes Bandbreitenmanagement. Es werden die folgenden Diensteklassen unterstützt:

Realtime Voice

Für Telefonie, VoIP und Intercom Anwendungen geeignet. Die eingerichtete Bandbreite steht der Anwendung jederzeit zur Verfügung, Datenpakete dieser Klasse werden mit höchster Priorität transportiert. Die nicht genutzte Kapazität kann von Anwendungen anderer Klassen genutzt werden.

Realtime Video

Für HD / SD – SDI Signalübertragung mit Videokomprimierung dem MPEG 4 AVC H.264 Standard entsprechend bis zu einer Signalqualität HP@L4.1 / FullHDTV 1080p geeignet. Die eingerichtete Bandbreite steht der Anwendung jederzeit zur Verfügung, Datenpakete dieser Klasse werden mit höchster Priorität transportiert. Die nicht genutzte Kapazität kann von Anwendungen anderer Klassen genutzt werden.

Klasse Platin

Für Mission Critical Data wie zum Beispeil SAP® oder CITRIX® Anwendungen geeignet. Die eingerichtete Bandbreite steht der Anwendung jederzeit zur Verfügung, Datenpakete dieser Klasse werden mit entsprechend hoher Priorität transportiert. Die nicht genutzte Kapazität kann von Anwendungen anderer Klassen genutzt werden.

Klasse Gold

Für Bulk Data wie zum Beispiel Druckbefehle oder File Transfer geeignet. Die konfigurierte Bandbreite steht als Minimum jederzeit zur Verfügung. Von Anwendungen der Gold-Klasse nicht genutzte Kapazität kann von Anwendungen anderer Klassen genutzt werden.

Klasse Default

Für Anwendungen dieser Klasse ist die Bandbreite reserviert, die nach Abzug der Platin-und / oder Gold-Bandbreite auf der Anschlussleitung verfügbar ist. Alle Anwendungen in dieser Klasse teilen sich die hier verfügbare Bandbreite nach dem „best-effort“ Prinzip. Diese Klasse ist für Anwendungen ohne definierten Mindestbandbreitenbedarf geeignet. Es erfolgt keine Bandbreitenreservierung bezogen auf die Anwendung.

5.3 Performance Reporting

Optional bietet Riedel Networks ein Tool zur Überwachung der Netzwerkperformance mit intuitiver Web-Benutzeroberfläche bietet an. Über Smartphone Apps für iOS® und Android® kann das Netzwerk ebenfalls optional unterwegs überwacht werden.

Performance Monitoring

Das Performance Reporting liefert graphisch aufbereitete statistische Daten über die Traffic Entwicklung aller VPN Anschlüsse des Kunden. Für jeden Standort wird die Gesamtauslastung (bei Multi-CN die Auslastung der einzelnen logischen Verbindungen) dargestellt. Folgenden Werte werden minütlich aktualisiert angezeigt:

- Auslastung in %
- Latency in Millisekunden
- Jitter in Millisekunden
- Paket Loss in %

Fehlerbenachrichtigung

Das Riedel Networks Performace Reporting bietet eine automatische Benachrichtigung zu einem Fehler über E-Mail oder SMS an einen vom Kunden zu bestimmenden Empfänger. Gleichzeitig eröffnen wir ein Service Ticket und beginnen mit der Fehlerbehebung.

6 Service Level Agreements (SLAs)

6.1 Garantierte Netzlaufzeiten

Riedel Networks garantiert die Netzlaufzeiten der Datenpakete innerhalb des Kernnetzes von Provider Edge (PE) bis Provider Edge, das heisst vom Eintrittspunkt eines Datenpaketes in das MPLS-Netz bis zum Austrittspunkt des Paketes aus dem MPLS-Netz:

garantierte Netzlaufzeit PE–PE national	< 20 ms
garantierte Netzlaufzeit PE–PE Europa	< 40 ms
garantierte Netzlaufzeit PE–PE interkontinental	< 200 ms

Die angegebenen Werte sind Tagesdurchschnittswerte. Da Riedel Networks keinen Einfluss auf die vom Kunden produzierte Last auf den Zugangsleitungen von den Kundenstandorten zum MPLS-Netz hat, können die Laufzeiten der Pakete auf den Anschlussleitungen und Zuführungen nicht garantiert werden.

6.2 Verfügbarkeiten – Kernnetz, Access

Riedel Networks garantiert für das MPLS Kernnetz von Provider Edge (PE) bis Provider Edge eine Verfügbarkeit von **99,95%**, für die VPN Services wird eine Verfügbarkeit von 99,5% garantiert.

Für die einzelnen VPN-Anschlüsse werden je nach Access Option unterschiedliche Verfügbarkeiten garantiert:

Access Option	Ohne Backup	Mit Backup	Mit HA Option
Remote Access	97,5%	N/A	N/A
ADSL	98,5%	99,0%	N/A
SDSL	98,5%	99,0%	99,5%
Leased Line / Ethernet	99,0%	99,5%	99,8%

Die angegebenen Werte sind Jahresdurchschnittswerte. Bei der Berechnung der Verfügbarkeit der Plattform werden angekündigte Wartungen nicht berücksichtigt. Die Berechnung der Störungsdauer beginnt mit der Erkennung einer Störung durch das Riedel Networks NOC bzw. mit der Meldung einer Störung durch den Kunden an Riedel Networks NOC (Network Operation Center).

Sofern sich die Dauer einer Störung aus vom Kunden zu vertretenden Gründen (siehe Abschnitt 7.1) verlängert, wird diese Zeit bei der Berechnung der Verfügbarkeit nicht berücksichtigt.

6.3 Paketverluste (Packet Loss)

Riedel Networks garantiert eine maximale Verlustrate für den Transport der Datenpakete innerhalb des Kernnetzes von Provider Edge (PE) bis Provide Edge, das heisst vom Eintrittspunkt der Datenpakete in das MPLS-Netz bis zum Austrittspunkt der Pakete aus dem MPLS-Netz:

Maximale Paketverlustrate in % PE–PE national 10^{-2}

Maximale Paketverlustrate in % PE–PE Europa 10^{-2}

Maximale Paketverlustrate in % PE–PE interkontinental 10^{-2}

Die angegebenen Werte sind Tagesdurchschnittswerte. Da Riedel Networks keinen Einfluss auf die vom Kunden produzierte Last auf den Zugangsleitungen von den Kundenstandorten zum MPLS-Netz hat, können die Verlustraten der Pakete auf den Anschlussleitungen und Zuführungen nicht garantiert werden.

6.4 Wiederherstellungszeit

Im Fall von Störungen gelten je nach gewählter Access Option unterschiedliche Obergrenzen für die Wiederherstellungszeit eines gestörten Anschlusses:

Access Option	Ohne Backup	Mit Backup	Mit HA Option
Remote Access	Nächster Arbeitstag	N/A	N/A
ADSL	24 h	24 h	N/A
SDSL	24 h	12h	8h
Leased Line / Ethernet	12 h	8 h	4h

Im Falle höherer Gewalt oder nicht von Riedel Networks zu verantwortender Ereignisse kann die Wiederherstellungszeit im Einzelfall überschritten werden. Die Einhaltung der oben genannten Wiederherstellungszeiten wird für 95% aller gemeldeten Störungen garantiert.

Sofern sich die Dauer einer Störung aus vom Kunden zu vertretenden Gründen (siehe Abschnitt 7.1) verlängert, wird diese Zeit bei der Berechnung der maximalen Entstörungszeit nicht berücksichtigt.

7 Umsetzung der SLA's

7.1 Erreichbarkeit und Zugang zu Räumlichkeiten des Kunden

Bei der Meldung einer Störung ist vom Kunden eine Telefonnummer anzugeben, unter der das Riedel Networks NOC bis zur Behebung der Störung einen Ansprechpartner erreichen kann, der auf Anforderung den Zugang zum Riedel Networks Equipment in den Räumlichkeiten des Kunden ermöglichen kann.

Sofern ein Kundenanschluss oder ein Service komplett ausgefallen ist (Priorität 1 gemäss Abschnitt 7.2), muss der Ansprechpartner des Kunden rund um die Uhr erreichbar sein, andernfall während der Bürozeiten zwischen 9 und 17 Uhr.

Sofern der Kunde die Erreichbarkeit des Ansprechpartners oder die Zugangsmöglichkeit zum Equipment nicht gewährleisten kann, verlängert sich entsprechend die maximale Entstörungszeit. Die hierdurch entstehenden Verzögerungen werden bei der Berechnung der Verfügbarkeit nicht berücksichtigt.

7.2 Riedel Networks Ansprechpartner und Case Priority

Service Aktivierung

Für die Inbetriebnahme von Anschlüssen, für die Aktivierung oder Deaktivierung von Services und für Änderungen der genutzten Dienstleistungen ist das Riedel Networks Service Team der Ansprechpartner des Kunden. Das Service Team ist erreichbar werktags von 9 bis 17 Uhr GMT +1.

Das Service Team koordiniert alle Aktivitäten im Zusammenhang mit der Inbetriebnahme oder Änderungen von Anschlüssen und Services. Beim Service Team kann jederzeit der aktuelle Projektsstatus laufender Aktivitäten vom Kunden abgefragt werden. Alle Anliegen des Kunden, welche Auftragscharakter besitzen und zu Änderungen an der aktuellen Netz- oder Servicekonfiguration führen, müssen per Email oder Fax vom Kunden bestätigt werden.

Störungsbehandlung

Im Falle von Störungen oder technischen Problemen ist das Riedel Networks NOC (Network Operation Center) telefonisch oder per Email zu informieren. Das NOC vergibt eine Ticket-Nummer und eine Case Priority.

- **Prio 1:** Störungen, die zu einer gravierenden Nutzungseinschränkung führen:
  Komplettausfall eines Anschlusses oder eines Services, sowie schwerwiegende Leistungseinbußen oder Teilausfall >25% eines Anschlusses oder eines Services
- **Prio 2:** Störungen, welche die Nutzung einschränken:
  Teilausfall eines Anschlusses oder eines Services mit erheblichen Einschränkungen der Verfügbarkeit > 5%
- **Prio 3:** Störungen, die lediglich geringfügige Nutzungseinschränkungen nach sich ziehen:
  Ausfälle, Störungen oder Fehler bei einzelnen Anschlüssen oder Ausfälle und Fehler bei Services , die für den Kunden nicht geschäftskritisch sind, sowie Fehler, die zu einer eingeschränkten Verfügbarkeit führen (Übertragungsfehler, Störgeräusche, Abbrüche)
- **Prio 4:** Anfragen zu Konfigurationsänderungen, keine Nutzungeinschänkung:
  Änderungen von Konfigurationen wie z.B. das Hinzufügen einer Diensteklasse oder Routingänderungen

Das NOC bleibt in allen Fällen bis zur Behebung des Problems Ansprechpartner des Kunden. Der Kunde wird fortlaufend über die Aktivitäten informiert.

7.3 Rufnummern und eMail-Adressen

Service Team (8h/5d)

Tel.: +49 6033 92462-444

E-Mail: rn-service@riedel.net

Network Operation Center / NOC (24h/7d)

Tel.: +49 6033 92462-222

E-Mail: rn-noc@riedel.net