Leistungsbeschreibung
enSecure Net

1 Standardleistungen

Die envia TEL GmbH (im Folgenden envia TEL genannt) überlässt dem Kunden eine Sicherheits- und Vernetzungslösung, die einen oder mehrere Internetanschlüsse absichern und optional miteinander vernetzen kann. Dazu werden dem Kunden ein oder mehrere Next Generation Firewall-Systeme (Firewalls) der Firma Fortinet zur Verfügung gestellt, welche zwischen WAN-Anschluss und lokalem Netzwerk geschaltet werden. Sofern die Vernetzungsfunktion genutzt wird, wird ein softwaredefiniertes Wide-Area Networking (SD-WAN) auf Basis von IPSec VPN-Tunnel bereitgestellt, in welches die Firewalls automatisch integriert werden. Für die Verwaltung der Firewalls steht ein zentrales Management-System zur Verfügung.

Darüber hinaus können weitere Sicherheits- und Vernetzungsleistungen sowie Management- und Analysefunktionen zur Verfügung gestellt werden.

Die zum Betrieb des Produktes notwendige WAN-Anbindung (i. d. R. ein oder mehrere Internetanschlüsse) ist nicht Bestandteil des Produktes und muss separat beauftragt werden.

1.1 Lokale Firewall-Systeme

envia TEL stellt dem Kunden Next Generation Firewall-Systeme (Firewalls) für die lokale Installation zur Verfügung. Diese schützt das lokale Netzwerk oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen aus dem Internet und bietet darüber hinaus weitere Funktionen, u. a. auch vor Sicherheitsrisiken innerhalb des Netzwerks. Alle Firewalls werden zentral administriert. envia TEL stellt den Systembetrieb der Firewall sicher. Dazu zählen Betrieb und die Überwachung (24x7) der zentralen Management-Plattform und die Installation von Updates, Patches und Fixes (siehe auch1.8) beinhaltet. Der Kunde erhält Zugriff auf die Firewall über die zentrale Management-Plattform. Er kann die für ihn im Kundenkontext erforderlichen Einstellungen der Firewall(s) konfigurieren. Auf systemseitige Einstellungen hat der Kunde keinen Zugriff.

Sofern mehrere Standorte vernetzt werden sollen, wird dies ebenfalls zentral administriert. Gleichartige Firewallkonfigurationen können mittels Templates zusammengefasst werden, um den Konfigurationsaufwand zu minimieren. Der verwendete Port für die WAN-Verbindung und die WAN-Konfiguration wird durch envia TEL verwaltet. Die Anzahl und Bandbreite der WAN-Verbindungen je Standort ist durch die Leistungsfähigkeit der gebuchten Firewall limitiert. Änderungen an den Ports der WAN-Verbindung(en) können über das Kundenportal der envia TEL beauftragt werden. Die für die Nutzung von **enSecure Net** notwendigen Internetanschlüsse müssen für eine Vernetzung nicht notwendigerweise über feste IP-Adressen/IP-Netze verfügen, da die Verbindungen zwischen den Standorten über die Netzbasierte Firewall (siehe 1.7.2) vermittelt werden.
Alle Firewalls werden mit Standardregeln vorkonfiguriert (alle Zugriffe von intern erlaubt, alle Zugriffe von extern verboten - gilt für IPv4 und IPv6) und NAT (Network Address Translation) für ausgehenden Verkehr aktiviert (gilt nur für IPv4).

Weiterhin ist DHCP (IPv4) auf dem LAN-Interface vorkonfiguriert. Die Konfiguration auf LAN Seite kann durch den Kunden geändert werden.

Es kommen verschiedene Firewall-Systeme des Herstellers Fortinet zum Einsatz. Die Firewalls werden dem Kunden für die Dauer der Produktnutzung zur Verfügung gestellt und verbleiben im Besitz der envia TEL. Die Firewall-Systeme sind für unterschiedliche Maximalbandbreiten/Maximalbelastungen vorgesehen und werden im Folgenden vorgestellt.

Der maximal mögliche Datendurchsatz der Firewall hängt von den zu übertragenden Daten (Art, Anzahl und Größe der Datenpakete) sowie den genutzten Firewallfeatures ab (z. B. SSL-Inspection). Um Überlastungen der Firewall zu vermeiden, wird dem Kunden empfohlen das Datenblatt der jeweiligen FortiGate (siehe Downloadbereich unter www.enviatel.de) mit dem geplanten Einsatzszenario zu vergleichen.

Benötigte Patchkabel für die LAN- und WAN-Anbindung müssen durch den Kunden bereitgestellt werden. Optional bietet envia TEL auch diverse Patchkabel an (siehe 2.1).

1.1.1 Fortinet FortiGate 40F

Die FortiGate 40F unterstützt maximal zwei WAN-Verbindungen mit Schnittstellen des Typs 1000BaseT RJ45. Sie ist für die Nutzung an einem Internetanschluss mit Bandbreiten von max. 1 Gbit/s (symmetrisch) zzgl. einer Backupverbindung von max. 1 Gbit/s (symmetrisch) vorgesehen. Ein WAN-Port (auf dem Gerät mit „WAN“ bezeichnet) ist dabei fest auf DHCP/DHCPv6 eingestellt. Für den zweiten WAN-Port (auf dem Gerät mit „3“ bezeichnet) kann auch statische IP-Adressierung konfiguriert werden.

Die Firewall besitzt weiterhin 2 Ports (Gigabit-Ethernet/RJ45), die für LAN-Verbindungen genutzt werden.

1.1.2 Fortinet FortiGate 100F

Die FortiGate 100F unterstützt maximal eine WAN-Verbindung mit einer Schnittstelle vom Typ 10G SFP+ (auf dem Gerät mit „X1“ bezeichnet; verschiedene SFP+-Module stehen zur Auswahl) sowie zwei WAN-Verbindungen (auf dem Gerät mit „WAN1 “ und „WAN2“ bezeichnet) mit jeweils einer Schnittstelle vom Typ 1000BaseT RJ45. Die FortiGate 100F ist für die Nutzung an einem Internetanschluss mit Bandbreiten von max. 10 Gbit/s (symmetrisch) zzgl. max. zwei Backupverbindungen mit jeweils max. 1 Gbit/s (symmetrisch) vorgesehen. Ein WAN-Port (auf dem Gerät mit „WAN1“ bezeichnet) ist dabei fest auf DHCP/DHCPv6 eingestellt. Für die beiden anderen WAN-Ports

envia TEL GmbH
Geschäftsanschrift Friedrich-Ebert-Straße 26 · 04416 Markkleeberg · T 0800 0101600 · F 0800 3684283
www.enviaTEL.de · info@enviaTEL.de · **Geschäftsführung** Stephan Drescher · **Sitz der Gesellschaft** Markkleeberg
Registergericht Amtsgericht Leipzig · HRB 24812 · **USt-ID-Nr.** DE183563546

(„WAN2“ und „X1“) kann auch statische IP-Adressierung konfiguriert werden.

Die Firewall besitzt weiterhin 20 Ports (auf dem Gerät mit „1“ bis „20“ bezeichnet) mit Gigabit-Ethernet (12xRJ45, 4xSFP, 4xCombo Ports RJ45/SFP) und einen Port mit 10-Gigabit-Ethernet SFP+ (auf dem Gerät mit „X2“ bezeichnet), welche dem Kunden als LAN-Ports zur Verfügung stehen. Das Netzteil der FortiGate 100F ist redundant ausgeführt.

1.2 Hardwareredundanz

Bei Buchung der entsprechenden Option werden jeweils zwei Firewalls des entsprechenden Typs redundant als Firewall-Cluster betrieben. Bei Ausfall einer Firewall springt automatisch die zweite Firewall ein.

Beide Firewalls müssen WAN- und LAN-seitig über Switches miteinander verbunden sein und alle zugeführten Verbindungen müssen über diese Layer2-Struktur an beide Firewalls herangeführt werden.

Die Layer2-Struktur ist durch den Kunden sicherzustellen. Zusätzlich ist für die Hardwareredundanz eine Querverkabelung zwischen den Firewalls (HA-Kabel) vorzunehmen (siehe Bild 1). WAN-seitig liefert i.d.R. der Internet-Service-Provider im Endgerät mehrere Switch-Ports mit.

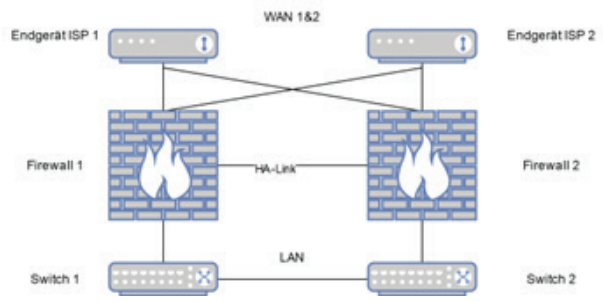

Bild 1: Layer2-Struktur zur Herstellung einer Hochverfügbarkeit durch Hardwareredundanz

1.3 Inbetriebnahme

envia TEL sendet dem Kunden die vorkonfigurierten Firewalls per Post zu. Der Kunde verbindet die WAN-Ports der Firewall mit den Ports des Endgeräts des Internet-Anschlusses/der Internetanschlüsse. Bei Hardwareredundanzen muss zusätzlich der HA-Link gesteckt werden. Die zu verwendenden Ports der Firewall werden dem Kunden vorab mitgeteilt. Nach dem Anschluss wird die Firewall abschließend automatisch konfiguriert (Zero Touch Provisioning). Dafür muss der Firewall automatisch eine IP-Adresse auf den WAN-Interfaces per DHCP zugewiesen werden. Dies ist durch den Kunden sicherzustellen. Sofern der Internetanschluss durch envia TEL bereitgestellt wird, ist ein DHCP-Server auf dem Endgerät verfügbar oder, bei statischen IP-Adressen, sorgt envia TEL für die entsprechende Vorkonfiguration der WAN-Ports der Firewall. Die IP-Netze der WAN-Verbindungen dürfen sich nicht überlappen (z. B. verwenden alle Router eines Herstellers dieselbe IP-Adresskonfiguration). Die Autokonfiguration benötigt einige Minuten. In dieser Zeit sollte die Firewall nicht vom Stromnetz oder dem WAN-Anschluss getrennt werden. Anschließend kann über die Firewall mit einer Basiskonfiguration aufs Internet und, sofern vorhanden, auf andere Standorte des SD-WAN zugegriffen werden. Die weitere Anpassung der Konfiguration muss über die zentrale Management-Plattform (siehe 1.7.1) vorgenommen werden.

1.4 Vernetzung und Verkehrssteuerung (SD-WAN)

Die im Produkt **enSecure Net** verwendeten Firewalls unterstützen die VPN-Vernetzung mittels IPSec und die Verkehrssteuerung mittels SD-WAN. Die Firewalls werden vor Auslieferung an den Kunden dem für den Kunden angelegten Netzwerk hinzugefügt. Die Netzbasierte Firewall fungiert dabei als zentrales VPN-Gateway, zu dem sich alle Standorte standardmäßig über Internet verbinden. Die Netzbasierte Firewall steuert die VPN-Verbindungen der einzelnen Standorte.

1.5 WAN-Redundanz

Die lokalen Firewalls können wie beschrieben (s. 1.1.1 und 1.1.2) mit mehreren Internetanschlüssen verbunden werden. Damit wird die Verfügbarkeit der Internetkonnektivität wesentlich erhöht. Auch die Erreichbarkeit innerhalb des SD-WAN wird so wesentlich verbessert. Änderungen der WAN-Konfiguration liegt im Bereich der Systemkonfiguration der Firewall und sind über das Kundenportal der envia TEL zu beauftragen.

Die Firewalls unterstützen eine feinstufige Konfiguration der Verwendung der WAN-Anbindungen. So kann der Datenverkehr je Applikation über Paramater wie Laufzeit, Jitter und Paket-Verlust z.B. automatisch der besten Internetanbindung oder statisch einer Internetverbindung fest zugewiesen werden. Um die Erreichbarkeit des Standortes aus dem Internet auch bei Ausfall einer der Internetanbindungen mit immer denselben festen IP-Adressen zu gewährleisten, kann dies über die Einbindung der Netzbasierten Firewall (siehe 2.1) erreicht werden. Diese stellt den Mittler zwischen lokaler Firewall und Internet dar.

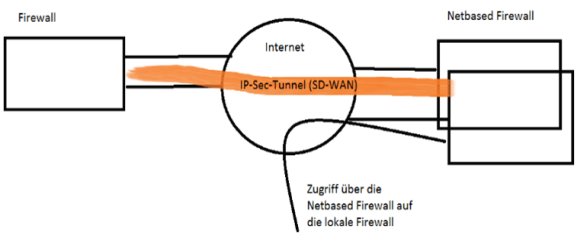

Bild 2: WAN-Redundanz

Leistungsbeschreibung
enSecure Net

1.6 Leistungsmerkmale

Die Firewalls verfügen über umfangreiche UTM-Leistungsmerkmale (Unified Threat Management), die durch den Kunden genutzt werden können.
Die folgende Übersicht zeigt die möglichen Dienste und ob diese mit Bereitstellung des Produkts aktiviert sind oder ob der Kunde sich diese selbst aktivieren muss (siehe Spalte Standardeinstellung).

Dienst	Standard-einstellung	Beschreibung
Statefull Firewall	Aktiviert (siehe 1.1)	Klassischer Firewall-Dienst mit Unterstützung des Signatur-DB-Service
Signature-DB-Service	Aktiviert	Bereitstellung verschiedener regelmäßig aktualisierter Datenbanken zur Verwendung in eigenen Filtern. Beinhaltet: Internet Service DB, Client ID DB, IP Geography DB, Malicious URL DB, URL Whitelist DB
Zertifikat-Prüfung	Aktiviert	Prüft die Gültigkeit und Vertrauenswürdigkeit von Serverzertifikaten
Web-Filter	Aktiviert	URL-Scan/Filter auf Basis von White-/Blacklists
Anti-Virus	Aktiviert	Schutz vor den neuesten Viren, Spyware und anderen Bedrohungen auf Inhaltsebene
SSL-VPN	Aktiviert	Siehe 1.8
Logging und Standardreporting	Aktiviert	Siehe 1.5.3
Konfigurationsbackup	Aktiviert	Siehe 1.5.4
Anti-Spam	Inaktiv	Der Antispam-Dienst verwendet eine Absender-IP-Reputationsdatenbank und eine Spam-Signaturdatenbank, um eine Vielzahl von Spam-Nachrichten zu erkennen und zu blockieren.
DNS-Filter	Inaktiv	Ermöglicht DNS-Black-/-Whitelists basierend auf dem Signature-DB-Service.
Applikationskontrolle	Inaktiv	Ermöglicht mittels Richtlinien den Zugriff auf Anwendungen oder ganzer Kategorien von Anwendungen zuzulassen, zu verweigern oder einzuschränken.
Mobiler Sicherheitsdienst	Inaktiv	Bietet wirksamen Schutz vor den neuesten Bedrohungen für mobile Android-Geräte
IPS mit Botnet-Filter	Inaktiv	Verhindert, dass Botnets und andere Bedrohungen mit Command & Control-Servern kommunizieren, um Daten zu filtern oder Malware herunterzuladen, blockiert groß angelegte DDoS-Angriffe von bekannten infizierten Quellen, schützt vor böswilligen Quellen im Zusammenhang mit Webangriffen, Phishing-Aktivitäten, Web-Scannen, Scraping und mehr
SSL Inspection	Inaktiv	Ermöglicht das Aufbrechen von verschlüsselten Verbindungen. Erfordert den unternehmensinternen Rollout von Zertifikaten
Content Disarm & Reconstruction (CDR)	Inaktiv	Entfernt alle aktiven Inhalte in Echtzeit aus Dateien, die nicht mit den Firewall-Richtlinien übereinstimmen
Virus Outbreak Protection	Inaktiv	Erkennung von Malware-Bedrohungen, die zwischen Signatur-Updates entdeckt wurden
Applikationskontrolle	Aktiviert	Ermöglicht die Erkennung von Anwendungen durch Analyse des Netzwerkverkehrs. Über eine Anwendungsdatenbank können betreffende Datenverkehre kontrolliert und priorisiert werden.
Verkehrssteuerung und Quality of Service	Inaktiv	Über verschiedene Qualitätsparameter wie Laufzeit, Jitter und Paket-Verluste können Anwendungen gezielt gesteuert werden.
Sicherheit und Segmentierung (z. B. IoT)	Inaktiv	Die Netzwerksegmentierung ermöglicht die physikalische Trennung unterschiedlicher Netzwerkegeräte in eigene Netze umso eine verbesserte Kontrolle über den Datenverkehr zu ermöglichen und unbefugte Zugriffe über Segmentgrenzen hinweg zu verhindern.
Transportverschlüsselung	Aktiviert	Zwischen den Standorten werden die Verbindungen mittels IPSec verschlüsselt.

1.7 enSecure Net (Basis)

Jedem Kunden werden mit **enSecure Net (Basis)** verschiedene zentrale Komponenten zur Verfügung gestellt, die die Administration insbesondere größerer Netzwerke enorm vereinfachen. **enSecure Net (Basis)** bietet verschiedene Zusatzleistungen (siehe 2) und eine Reihe von Standardleistungen, die im Folgenden vorgestellt werden.

1.7.1 FortiManager

Mit dem FortiManager stellt envia TEL ein zentrales und hochverfügbar ausgeführtes Management-System über eine einzige, gemeinsame Konsole bereit, die für den Kunden aus dem Internet erreichbar ist.

Standardleistungen des FortiManagers:

- Eine zentrale Sicht auf alle Konfigurationen („Single Pane of Glass“),
- Unterstützung verschiedener Firewallprofile („Policy-Packages“) zur vereinfachten Standortkonfiguration,

- Gemeinsame Objektdefinitionen (z. B. Adressobjekte, Priorisierung, Sicherheitsprofile),
- Automatische Konfigurationsbackups mit Rollback-Funktionen (siehe 1.7.5),
- Automatisches Change-Log zur Nachvollziehbarkeit von Änderungen,
- Zentrale Konfiguration und Überwachung des SD-WAN.

1.7.2 Netzbasierte Firewall

Mit der Netzbasierten Firewall bietet envia TEL ein leistungsfähiges, zentral gehostetes und redundantes Firewallsystem des Herstellers Fortinet. Mit der Bereitstellung wird eine für den Kunden separierte Firewallinstanz eingerichtet und in das Netzwerk des Kunden integriert (VDOM/Virtual Domain). Die Netzbasierte Firewall bietet folgende Leistungen:

- Bereitstellung eines zentralen VPN-Gateways zur Anbindung der einzelnen Standorte über IPSec und zur Steuerung der dynamischen Shortcut-IPSec-Tunnel zwischen den Standorten
- Bereitstellung von VPN-Einwahlzugängen über ein zentrales VPN-Gateway inkl. Benutzerverwaltung (siehe 2.2)
- Zuweisung fester IP-Adressen
- Bereitstellung externe Erreichbarkeit bei Mehrwegeredundanz über feste IP-Adressen
- Verwendung für Anschlüsse im Datacenter Leipzig

envia TEL vergibt im Regelfall 2 IPv4-Adressen (für die Zuteilung weiterer IPv4-Adressen siehe 2.3). IPv6-Adressen werden, sofern nicht anders angegeben, mit einem Präfix der Größe /56 bereitgestellt. Optional können auch Netze mit einem Präfix von /52 oder /48 vergeben werden. Es ist zu beachten, dass je eine IPv4- und IPv6-Adresse aus den Adressbereichen des Kunden für das VPN-Gateway reserviert ist (SSL-VPN und IPSec-VPN).

1.7.3 Nutzerverwaltung

Der Kunde kann sich beliebig viele Zugänge für den FortiManager über das Serviceportal der envia TEL einrichten (siehe 1.9). Die Zugänge sind zwingend über einen 2. Faktor geschützt (2FA per E-Mail oder SMS). Bei Beauftragung des Managed Service (siehe 2.9) besitzen die Zugänge nur lesende Berechtigungen, da in dem Fall sämtliche Konfigurationsänderungen durch envia TEL vorgenommen werden.

1.7.4 Analysefunktion

Mit der Analysefunktion (FortiAnalyzer) besteht die Möglichkeit Logfiles und Events der Firewalls zu durchsuchen und erweiterte Reportings zu erstellen bzw. fertige Reportings zu nutzen und sich diese auch automatisch zu festgelegten Zeitpunkten bzw. eventgesteuert zusenden zu lassen. Folgende FortiAnalyzer-Module sind nutzbar:

- FortiView,
- LogView,
- Incidents & Events,
- Reports.

Für die genannten Funktionalitäten werden für den Kunden fünf GByte Logspeicher reserviert. Weiterer Logspeicher kann optional bereitgestellt werden (siehe 2.8).

1.7.5 Konfigurationsbackups

Die zentrale Management-Plattform erstellt automatisch Backups der Konfiguration jeder Änderung (Revision). Diese Backups umfassen Konfigurationsdaten und dienen der optionalen Wiederherstellung durch den Kunden. envia TEL hält die letzten 100 Backups vor. Ältere Backupversionen werden verworfen.

1.8 Softwareupdates

envia TEL kümmert sich zentral um die regelmäßige Aktualisierung aller Hard- und Softwarekomponenten. Dazu gehören sämtliche Firewalls (FortiGate), FortiManager, FortiAnalyzer und weitere verwendete Komponenten (z. B. FortiAuthenticator). Dadurch werden die Softwarekomponenten auf einem aktuellen und sicheren Stand gehalten und neue Leistungsmerkmale verfügbar gemacht. Durch die Updates kann es in Einzelfällen auch zu Einschränkungen kommen, da z. B. bestimmte Funktionen nach einem Update nicht mehr verfügbar sind oder anders abgebildet wurden. Die Updates werden innerhalb des Wartungsfensters (siehe externes Dokument „Servicelevel Agreement“) vorgenommen. Betroffene Kunden werden vorab über Updates und damit verbundene Änderungen informiert.

1.9 Serviceportal

envia TEL stellt ihren Kunden im Serviceportal unter der Internetadresse portal.enviaTEL.de verschiedene Dienstleistungen zur Verfügung. So können Informationen zu Verträgen, Rechnungen und Verbrauchsdaten eingesehen werden. Zudem sind viele Leistungsmerkmale und Optionen zu bestehenden Verträgen änderbar. Der Zugang zum Serviceportal erfolgt per Kundennummer und Passwort. Beide Informationen werden dem Kunden zu Beginn eines Vertragsverhältnisses zugeschickt. Der Kunde hat sicherzustellen, dass die Zugangsdaten nicht missbräuchlich verwendet werden können.

2 Zusatzleistungen

2.1 Patchkabel und SFP-Module

envia TEL bietet dem Kunden optional die Bereitstellung verschiedener Patchkabel (auch LWL-Patchkabel) und SFP-Module im Rahmen der Produktbestellung zum Kauf an.

envia TEL GmbH
Geschäftsanschrift Friedrich-Ebert-Straße 26 · 04416 Markkleeberg · T 0800 0101600 · F 0800 3684283
www.enviaTEL.de · info@enviaTEL.de · **Geschäftsführung** Stephan Drescher · **Sitz der Gesellschaft** Markkleeberg
Registergericht Amtsgericht Leipzig · HRB 24812 · **USt-ID-Nr.** DE183563546

2.2 VPN-Einwahlzugänge

Mittels SSL-VPN ist die Verbindung eines Gerätes (PC, Smartphones, Tablets etc.) mit dem internen Netz des Kunden über das Internet auf das VPN-Gateway möglich. Das VPN-Gateway ist für den Kunden bei Bereitstellung der Netzbasierten Firewall (siehe 1.7.2) vorkonfiguriert. Die IP-Adresse und der Hostname des VPN-Gateways werden dem Kunden bei der Produktbereitstellung mitgeteilt. VPN-Benutzer können durch den Kunden im Serviceportal der envia TEL verwaltet werden. Die Zugänge können dabei optional mit einem zweiten Faktor abgesichert werden. Als zweiter Faktor stehen SMS und E-Mail zur Verfügung (der SMS-Versand ist auf in Deutschland tätige Mobilfunkanbieter beschränkt).

Abgerechnet wird tagesaktuell nach der Anzahl der jeweils aktiven VPN-Benutzer mit und ohne zweiten Faktor. Als Zugangssoftware (VPN-Client) wird der Fortinet-VPN-Client genutzt (Download https://www.forticlient.com/downloads bzw. aus dem Geräte-App-Store). Alternativ besteht die Möglichkeit über das kundenspezifische VPN-Gateway per Browser zuzugreifen

2.3 Zusätzliche öffentliche IPv4-Adressen zur Netzbasierten Firewall

Auf Wunsch des Kunden ist es möglich zusätzliche IPv4-Adressen einzeln zuzuteilen. Der Bedarf muss gerechtfertigt sein und vom Kunden schriftlich begründet werden. Die Zuteilung erfolgt gegen einen einmaligen Bereitstellungspreis und einen monatlichen Grundpreis, der sich nach der Anzahl der IPv4-Adressen richtet.

2.4 Support

Das Cybersecurity-Team der envia TEL steht dem Kunden für Fragen zur Verfügung. Die Beauftragung erfolgt über das Serviceportal (siehe 1.9), in welchem jeweils ein Service Request angelegt wird. Die weitere Kommunikation kann sowohl telefonisch als auch per E-Mail über den Service Request erfolgen. Die Abrechnung erfolgt im 15 Minuten-Takt (jeweils Aufrundung auf ein Vielfaches von 15 Minuten). Sofern der Kunde einen Managed Firewall & Network Service nutzt (siehe 2.9), wird die Abrechnung über diesen Service vorgenommen. Telefonische Beratungen werden von Montag bis Donnerstag zwischen 8 und 17 Uhr und freitags von 8 bis 14 Uhr angeboten.

2.5 Einweisung

Auf Wunsch des Kunden wird eine Einführung in die Nutzung des Firewall-Systems vorgenommen. Die Einweisung erfolgt in Form von Webkonferenzen und beinhaltet eine grundlegende Einführung in die Nutzung der netzbasierten Firewall als auch Themen wie Konfiguration, Analyse, Reporting und kann auf die Erfordernisse des Kunden angepasst werden. Die Abrechnung erfolgt nach Zeit analog 2.4.

2.6 Internetanbindung

envia TEL stellt verschiedene Produkte zur Bereitstellung von Internetanschlüssen zur Verfügung, die gemeinsam mit **enSecure Net** genutzt werden können. Dazu zählen die Produkte **enDSL**, **enGiga Flex** und **enGiga Flex+**.

2.7 Cloud Connect

Optional kann der Service eines Cloud-Service-Providers (Amazon AWS, Microsoft Azure etc.) an die Netzbasierte Firewall (siehe 1.7.2) über ein eigenes Interface eingebunden werden. Die Verbindung zum Cloud-Service-Provider kann in zwei Varianten umgesetzt werden.

2.7.1 Anbindung mittels dedizierter Leitung

Die Verbindung wird mittels einer transparenten Layer 2-Punkt-zu-Punkt-Verbindung (Ethernet Line) vom Datacenter des Cloud-Service-Providers zu einem dedizierten Interface der Netzbasierten Firewall hergestellt. Für die Bereitstellung der dedizierten Leitung sind die Produkte **enGiga Secure** sowie **enGiga Line cloud connect** bzw. **enData LeipCIX** notwendig.

2.7.2 Anbindung mittels VPN-Tunnel

Die Verbindung wird über einen verschlüsselten IPSec-Tunnel aus einer Routing-Instanz des Cloud-Services zu einem VPN-Gateway auf der Netzbasierten Firewall hergestellt. Hierzu sind neben dem Cloud-Zugang eine FortiGate Cloud VM oder ein anderes IPSec-fähiges Gateway in der Cloud des Anbieters notwendig und durch den Kunden bereitzustellen.

2.8 Erweiterte Analysefunktion

envia TEL bietet dem Kunden zusätzlichen Logspeicher, um mehr Events oder einen längeren Zeitraum auswerten zu können.

2.9 Managed Firewall und Network Service

envia TEL bietet dem Kunden auf Wunsch einen Managed Firewall & Network Service, in welchem der Betrieb seiner Firewall bzw. seines WAN durch zertifizierte Cybersecurity-Spezialisten der envia TEL sichergestellt wird. Alle Änderungen an der Firewall, wie die Erstellung und Pflege des Firewall-Regelwerks, wird anhand von Kundenanforderungen durch envia TEL vorgenommen. Für eine detaillierte Beschreibung und die verschiedenen Abrechnungsmodelle siehe die separate Leistungsbeschreibung „enManaged Firewall & Network“.

2.10 Telefonie/Sprache

envia TEL bietet optional verschiedene Sprachdienste als Ergänzung zum Produkt **enSecure Net** an. Diese können über das Produkt **enVoice IP** gebucht werden.

envia TEL GmbH
Geschäftsanschrift Friedrich-Ebert-Straße 26 · 04416 Markkleeberg · T 0800 0101600 · F 0800 3684283
www.enviaTEL.de · info@enviaTEL.de · **Geschäftsführung** Stephan Drescher · **Sitz der Gesellschaft** Markkleeberg
Registergericht Amtsgericht Leipzig · HRB 24812 · **USt-ID-Nr.** DE183563546

2.11 Entstörung und Servicelevel Agreements (SLA)

envia TEL beseitigt Störungen ihrer technischen Einrichtungen im Rahmen der technischen und betrieblichen Möglichkeiten. Informationen über Störungen nimmt envia TEL täglich von 0:00 bis 24:00 Uhr über die kostenlose Rufnummer 0800 0101600 bzw. Fax 0800 2728666 entgegen. Sofern nicht einzelvertraglich anders geregelt, gelten die Angaben des Dokuments „Servicelevel-Agreement“. Der dort aufgeführte Servicelevel „Standard“ ist bereits kostenfrei in das Produkt integriert. Als kostenpflichtige Zusatzleistung für das vorliegende Produkt, werden die Servicelevel „Komfort“ und „Premium“ angeboten (siehe 2.12).

2.12 Servicelevel Komfort und Premium

Alternativ zum Servicelevel „Standard“ werden die Servicelevel „Komfort“ und „Premium“ angeboten, welche Verbesserungen hinsichtlich Verfügbarkeit, Wiederherstellung und Entstörung bieten (siehe Dokument „Servicelevel-Agreement“).

Die Buchung der Servicelevel „Komfort“ und „Premium“ ist nur bei Vorhandensein einer Hardwareredundanz möglich (siehe 1.2), da nur über eine Hardwareredundanz die Wiederherstellung innerhalb der vorgebenden Zeit bei einem Hardwareausfall sichergestellt werden kann.