# Leistungsbeschreibung
# enSecure Cloud

## 1 Standardleistungen

Die envia TEL GmbH (im Folgenden envia TEL genannt) überlässt dem Kunden ein hochverfügbares und netzbasiertes Firewallsystem.

Das netzbasierte Firewallsystem kann auf verschiedenen Wegen zum Schutz kundeneigener Infrastruktur eingesetzt werden:

- über dedizierte Festverbindungen zu einem oder mehreren Kundenstandorten oder zum Datacenter Leipzig,
- über VPN-Einwahlzugänge,
- über IPsec-Tunnel,
- über eine Kombination aus obigen Möglichkeiten.

### 1.1 Netzbasierte Firewall

#### 1.1.1 Bereitstellung und Grundleistungen

Das Produkt **enSecure Cloud** beinhaltet ein leistungsfähiges, zentral gehostetes und redundantes Firewallsystem des Herstellers Fortinet. Mit der Bereitstellung des Produktes wird auf eine für den Kunden separierte Firewallinstanz eingerichtet (VDOM/Virtual Domain).

Die Firewallinstanz wird mit Standardregeln vorkonfiguriert (alle Zugriffe von intern erlaubt, alle Zugriffe von extern verboten - gilt für IPv4 und IPv6), bestellte öffentliche IP-Adressen (siehe 1.1.6) werden eingerichtet und NAT (Network Address Translation) für ein- und ausgehenden Verkehr aktiviert (gilt nur für IPv4).

Weiterhin kann DHCP (IPv4) auf Wunsch des Kunden aktiviert werden. Das LAN-Interface auf Kundenseite wird mit dem Netz 192.168.178.0/24 mit Gatewayadresse 192.168.178.1 vorkonfiguriert. Eine nachträgliche Anpassung auf einen anderen Adressbereich ist möglich. Weiterhin stellt envia TEL den Systembetrieb sicher, welcher die die Installation von Updates, Patches und Fixes sowie die Betriebsüberwachung (24x7) beinhaltet.

#### 1.1.2 Leistungsmerkmale

Die netzbasierte Firewall verfügt 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 1.1.1) | 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 2.1.3 |
| Logging und Standardreporting | Aktiviert | Siehe 1.1.4 |
| Konfigurationsbackup | Aktiviert | Siehe 1.1.5 |
| 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 |
| Sandbox Cloud Service | Inaktiv | Nutzt den FortiCloud Sandbox-Service, um neue Bedrohungen zu erkennen und zu deaktivieren |

#### 1.1.3 Zugriff
Sofern der Kunde seine netzbasierte Firewall selbst betreibt, kann er sich über das Serviceportal der envia TEL (siehe 1.4) Administratoren einrichten. Bei Beauftragung des Managed Service (siehe 2.5) besitzt der Benutzer nur lesende Berechtigungen für die netzbasierte Firewall, da in dem Fall sämtliche Änderungen an der netzbasierten Firewall durch envia TEL vorgenommen werden.

#### 1.1.4 Analysefunktion
Mit der Analysefunktionen besteht die Möglichkeit Logfiles und Events 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 Fortinet-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 2.1.4).

#### 1.1.5 Konfiguartionsbackup
envia TEL erstellt automatisch Backups der Firewallkonfiguration des Kunden bei jeder Änderung (Revision). Dieses Backup umfasst Konfigurationsdaten und dient der optionalen Wiederherstellung durch den Kunden. envia TEL hält die letzten 100 Backups vor. Ältere Backupversionen werden verworfen.

#### 1.1.6 IP-Adressen
Als Mitglied von RIPE (Réseaux Internet Protocol Européens) kann envia TEL seinen Kunden öffentliche IP-Adressen nach den von RIPE vorgegebenen Regeln zuteilen. envia TEL ist an diese Regeln strikt gebunden. Ausführliche Hinweise zu den Vergaberichtlinien finden Sie unter www.ripe.net. Die Zuteilung des als erforderlich dokumentierten Adressraumes erfolgt aus dem Provider Aggregatable Address Space (PA-Adressraum) der envia TEL GmbH. Sofern der Kunde öffentliche IP-Adressen aus dem PA-Adressraum der envia TEL GmbH bestellt, werden IP-Adressen der Version 4 (IPv4) und IPv6-Adressen (Dualstack) bereitgestellt. Bei der Vergabe von IPv4-Adressen vergibt envia TEL im Regelfall 2 IP-Adressen (für die Zuteilung weiterer IPv4-Adressen siehe 2.3 und 2.4). 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 SSL-VPN-Gateway für VPN-Einwahlzugänge (Homeoffice etc., siehe 2.1.3) reserviert ist.

### 1.2 Weitergabe von Leistungen
Der Weiterverkauf von Leistungen, die envia TEL im Rahmen dieses Vertrages gegenüber dem Kunden erbringt, ist unter Hinweis auf § 7 der Allgemeinen Geschäftsbedingungen für Geschäftskunden gestattet.

### 1.3 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 2.2).

### 1.4 Serviceportal
envia TEL stellt ihren Kunden im Serviceportal unter der Internetadresse www.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 Firewall

#### 2.1.1 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 und beinhaltet Themen wie Konfiguration, Analyse, Reporting und kann auf die Erfordernisse des Kunden angepasst werden. Die Abrechnung erfolgt nach Zeit analog 2.1.2.

#### 2.1.2 Telefonische Beratung
Das Cybersecurity-Team der envia TEL steht dem Kunden für Fragen zur Verfügung. Die Beauftragung erfolgt über das Serviceportal (siehe 1.4), 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 Service nutzt (siehe 2.5), wird die Abrechnung über diesen Service vorgenommen. Telefonische Beratungen werden an Werktagen zwischen 8 und 17 Uhr bearbeitet.

#### 2.1.3 VPN-Einwahlzugänge
Mittels VPN ist die Verbindung eines Gerätes (PC, Smartphones, Tables etc.) mit dem internen Netz des Kunden über das Internet und ein VPN-Gateway möglich. VPN-Einwahlzugänge sind für Kunden verfügbar und vorkonfiguriert. Dazu ist

eine IPv4-Adresse aus den Adressbereich des Kunden für das VPN-Gateway reserviert. Das Gateway wird dem Kunden bei der Produktbereitstellung mitgeteilt und ist im Serviceportal der envia TEL einsehbar. Die einzelnen VPN können durch den Kunden im Serviceportal der envia TEL verwaltet werden. VPN können optional mit einem 2. Faktor abgesichert werden. Als 2. Faktor stehen SMS und E-Mail zur Verfügung (der SMS-Versand ist auf deutsche Mobilfunkanbieter beschränkt). Abgerechnet wird tagesaktuell nach der Anzahl der jeweils aktiven VPN mit und ohne 2. Faktor. Das VPN wird mittels SSL aufgebaut. Als VPN-Client (Zugangssoftware) 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.

**2.1.4 Erweiterte Analysefunktion**
Optional bietet envia TEL dem Kunden zusätzlichen Logspeicher, mehr Events oder einen längeren Zeitraum auswerten zu können.

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

**2.1.5.1 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 Netbased Firewall hergestellt. Für die Bereitstellung der Ethernet Line ist eine zusätzliche Bestellung des Produkts enGiga Line cloud connect notwendig.

**2.1.5.2 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 Netbased 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.

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

### 2.3. Zuteilung zusätzlicher öffentlicher IPv4-Adressen
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. Zuteilung von öffentlicher IPv4/v6-Netzen
Auf Wunsch des Kunden ist es möglich größere IPv4/v6-Netze zuzuteilen. Der Bedarf dafür muss gerechtfertigt sein und vom Kunden schriftlich begründet werden. Die Zuteilung erfolgt gegen einen einmaligen Preis für die Zuteilung und, bei IPv4-Netzen, einen monatlichen Grundpreis, der sich nach der Größe des gewünschten IPv4-Netzes richtet.

### 2.5. Managed Security & Network Service
envia TEL bietet dem Kunden auf Wunsch einen Managed Security & Network Service, in welchem der Betrieb der Netbased Firewall 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 Security & Network**“.

### 2.6 Telefonie/Sprache
envia TEL bietet optional verschiedene Sprachdienste als Ergänzung zum Produkt **enSecure Cloud** an. Diese können über das Produkt **enVoice IP** gebucht werden. Die technische Lösung ist detailliert im Dokument „Technische Richtlinie enVoice IP an enSecure“ beschrieben.

## 3 Wahl des Abrechnungsmodells

Bei der Abrechnung von Datenvolumen erfolgt die Messung des ein- und ausgehenden Datenvolumens auf Basis von Layer 2 (lt. OSI-Schichtenmodell) am LAN-Datenport der Firewallinstanz des Kunden. Die Abrechnung des übertragenen Datenvolumens kann nach verschiedenen Verfahren erfolgen:

### 3.1 Bandbreitenabhängige Abrechnung nach Burst-Methode
Für die Abrechnung nach der Burstmethode wird das ein- und ausgehende Datenvolumen in 5-Minuten-Intervallen ermittelt und aus dem gemessenen Volumen die durchschnittliche Bandbreite der 5-Minuten-Intervalle errechnet. Dabei werden ein- und ausgehendes Verkehrsvolumen eines 5-Minuten-Intervalls nicht summiert. Ausschlaggebend für die Abrechnung ist der Datenverkehr mit der jeweils höheren Bandbreite. Am Monatsende werden die Bandbreitendaten der Größe nach sortiert und 5 % der größten Werte verworfen. Der nach Abzug größte verbleibende Wert wird als die zu berechnende Bandbreite genommen. Die Abrechnung erfolgt nach angefangenen Mbit/s.

### 3.2 Abrechnung mit Mindestabnahmemenge (Commitment)
Die Zählung des Datenverkehrs erfolgt analog zu 3.1, wobei mindestens eine vertraglich vereinbarte Mindestabnahmemenge in Rechnung gestellt wird.

### 3.3 Pauschale Abrechnung (Flatrate)
Dem Kunden wird ein fester monatlicher Grundpreis unabhängig von der tatsächlichen Nutzung pauschal in Rechnung gestellt.