

# Leistungsbeschreibung *envia TEL ip firewall*

## 1. Standardleistungen

Die **envia TEL GmbH** (im folgenden **envia TEL** genannt) stellt dem Kunden mit *envia tel ip firewall* ein leistungsfähiges Produkt zum Schutz eines an das Internet angeschlossenen Netzwerkes zur Verfügung. Zudem besteht die Möglichkeit mehrere Standorte per VPN miteinander zu verbinden bzw. einen Zugriff auf das geschützte Netzwerk per VPN-Client zu ermöglichen.

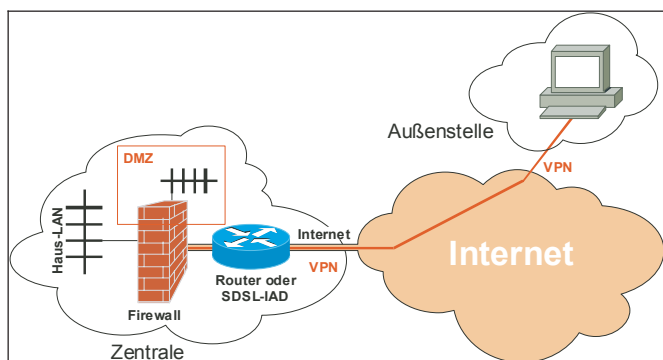


Bild: Beispiel für den Einsatz einer Firewall mit DMZ (Demilitarisierte Zone) und VPN-Option

### 1.1 Produktvarianten

Für eine optimale Anpassung an die Bedürfnisse des Kunden steht das Produkt **envia TEL ip firewall** in verschiedenen Produktvarianten zur Verfügung. Die Produktvariante legt die verfügbaren Leistungsmerkmale des Produktes fest:

#### 1.1.1 firewall basic

Diese, speziell für kleine Büros oder Heimarbeitsplätze geeignete Produktvariante, basiert auf einer CISCO PIX 501. Es besteht die Möglichkeit maximal 50 gleichzeitige Verbindungen über die Firewall aufzubauen und das geschützte Netz über ein VPN mit einem anderen Standort zu verbinden. Zudem beinhaltet die PIX 501 einen integrierten Switch mit 4 Fast-Ethernet-Ports.

#### 1.1.2 firewall standard

Die hier verwendete PIX 506 eignet sich besonders für den Einsatz in kleineren bis mittleren Unternehmen. Das Produkt hebt die Beschränkung auf maximal 50 gleichzeitige Verbindungen auf und erlaubt einen Firewalldurchsatz von maximal 100 Mbps.

#### 1.1.3 firewall profi

Die Lösung für mittlere Unternehmen erlaubt den Betrieb einer DMZ (Demilitarized Zone) zur sicheren Anbindung eigener Server an das Internet bzw. zu deren sicheren Integration in ein VPN. Zudem eignet sich die eingesetzte PIX 515 für sehr schnelle VPN. Über ein VPN lassen sich die verschiedenen Produktvarianten sehr gut kombinieren und mehrere Filialen eines Unternehmens unter Berücksichtigung unterschiedlicher Anforderungen miteinander verbinden.

### 1.2 Kundenbetreuung

**envia TEL** gewährt dem Kunden durch seine Security-Spezialisten Service und Support zur Anpassung von Firewall-Regeln an sich geänderte Bedürfnisse, Hilfeleistungen bei Problemen, Softwareupdates und Security-Patches. Dafür steht dem Kunden maximal eine Arbeitsstunde pro Monat während der regulären Arbeitszeit der **envia TEL** zur Verfügung. Darüber hinausgehende Leistungen werden separat abgerechnet.

#### 1.2.1 Updates

Updates werden, wenn dies aus Sicherheitsgründen oder zum Bereitstellen neuer Funktionen nötig ist, zeitnah eingespielt, sobald der Hersteller der eingesetzten Komponente solche zur Verfügung stellt. Die **envia TEL** hat keinerlei Einfluss auf die Bereitstellung von Updates durch einen Hersteller.

### 1.3 SLA

#### 1.3.1 Entstörung

**envia TEL** beseitigt Störungen ihrer technischen Einrichtungen im Rahmen der technischen und betrieblichen Möglichkeiten. Sofern nicht einzelvertraglich anders geregelt, erbringt sie hierbei insbesondere folgende Leistungen:

- Störungen nimmt **envia TEL** täglich von 0.00 bis 24.00 Uhr per Fax (0800 2728666) oder telefonisch (0800 0101600) entgegen
- Störungsbehebungen erfolgen außerhalb gesetzlicher Feiertage von Montag bis Freitag von 8.00-17.00 Uhr
- Beginn der Störungsbearbeitung (Reaktionszeit) erfolgt innerhalb von 2 Stunden
- Die maximale Entstörzeit beträgt 24 Stunden ab Störungsmeldungseingang (abzüglich Samstag, Sonn- und Feiertage)

#### 1.3.2 Vertragsstrafen

Bei Überschreitung der Entstörzeit erhält der Kunde eine Gutschrift über 15 % der monatlichen Grundgebühr pro 24 Stunden Ausfall, wobei der Begriff Entstörzeit die Zeitspanne zwischen der Meldung der Störung durch den Kunden und der Wiederherstellung der Verfügbarkeit bezeichnet. Es erfolgt nur eine Anrechnung der unter Entstörzeit (siehe 1.3.1) angegebenen Zeiten. Die Gutschrift ist pro Monat auf maximal 100 % der monatlichen Grundgebühr begrenzt.

## 2. Firewall

Die Firewall arbeitet als Filter zwischen Internet und dem Organisationsnetzwerk des Kunden. Die Firewall verfügt über ein Regelwerk, welches die Filtereigenschaften gemäß der Security-Policy und den Netz- und Systemvoraussetzungen des Kunden abbildet (siehe 2.3). Mögliche Angriffe, welche sich auf IP/ICMP (Netzwerklayer) oder TCP/UDP (Transportlayer) beziehen, werden innerhalb der Firewall erkannt und abgewehrt. Dies gilt für Angriffe auf die Firewall und die zu schützenden Netzwerke.

Der IP-Router, welcher der Verbindung zum Internet dient, befindet sich aus Sicht des Organisationsnetzes im Internet und vor der Firewall. Somit ist ein Schutz des Routers vor Angriffen nicht gegeben.

### 2.1 Limitierung

Die Firewall bietet keinen Schutz vor Viren oder anderem schädlichem Code (z. B. Trojanern). Dazu muss ein separater Content-Filter betrieben werden (siehe 4).

Datentransfers, welche nicht durch die Firewall transportiert werden, entziehen sich der Kontrolle durch die Firewall. Der Kunde muss sicherstellen, dass keine anderen Internetverbindungen existieren, welche die Firewall umgehen, wie z. B. Modems mit Anbindung an andere Netzwerke oder Wireless-LANs.

### 2.2 Schnittstellen

Die Firewall verfügt über mindestens 2 physikalische Layer-2-Schnittstellen, welche als Fast-Ethernet (10/100baseTx) ausgeführt sind. Die Anbindung von Netzen, welche über andere Netzzugangsprotokolle eingebunden werden sollen, erfolgt über Medienkonverter oder Router. Diese Geräte sind nicht Bestandteil der Firewall und müssen separat beauftragt werden.

### 2.3 Filterregeln

Gemäß der Security-Policy des Vertragspartners werden Filterregeln für die Firewall konfiguriert. Durch die Firewall werden die IP-Netze kontrolliert, welche über die Layer-2-Schnittstellen der Firewall IP-Pakete transportieren.

Das Regelwerk des Filtermechanismus arbeitet auf der Ebene von IP-Adressbereichen, IPPortbereichen und IP-Protokollen. Zum Transport anderer Protokolle muss eine IP-Encapsulation eingesetzt werden. Die Regeln können für eingehende und ausgehende Datenpakete definiert werden. Das Regelwerk ist so aufgebaut, dass ein Datenpaket von einer Startadresse zu einer Zieladresse abgelehnt oder durchgelassen wird.

### 2.4 NAT/PAT

An der Netzwerkschnittstelle, welche die Verbindung zum Internet darstellt, wird bei Bedarf eine IP-Network-Address Translation (NAT) durchgeführt. Die Address Translation kann für eingehende und ausgehende Verbindungen konfiguriert werden. Es stehen statische und dynamische NAT zur Verfügung. Die dynamische NAT wird durchgeführt, wenn es sich bei den IP-Nummern im Organisationsnetz des Kunden um private IP-Netze nach RFC-1918 handelt oder die IPNetze aus dem offiziellen Adressraum des Internets stammen aber einem AS (Autonomen System) zugeordnet sind, welches nicht dem Vertragspartner gehört und kein AS der **envia TEL** ist.

Die statische NAT wird verwendet, wenn externe IPAdressen auf interne IP-Adressen abgebildet werden müssen, um einen Zugriff auf organisationsinterne Ressourcen zu ermöglichen. Bei statischer NAT ist eine Abbildung von externer Adresse mit beliebigem Port auf eine interne Adresse mit definiertem Port möglich (Port Address Translation).

### 2.5 DMZ

Die demilitarisierte Zone (DMZ) wird zum Betrieb von Diensten verwendet, welche sowohl aus dem Organisationsnetz als auch aus dem Internet erreichbar sein sollen. Durch das Auslagern von Diensten in die DMZ werden diese Dienste außerhalb des Netzwerkes der Organisation betrieben und somit von den internen Netzen des Vertragspartners physikalisch und logisch getrennt, befinden sich aber weiterhin im Schutzbereich der Firewall. Typische Dienste, welche in einer DMZ platziert werden, sind E-Mail-Server, Webserver, Nameserver, Proxy-Server und Fileserver für die Nutzung über ein VPN.

## 3. IP VPN

Das Virtual Private Network (VPN) verbindet private IP-basierte Netzwerke über öffentliche IP-Netzwerke mit Hilfe von VPN-Gateways, welche in der Firewall implementiert sind. Die Daten werden vor dem Verlassen des Netzwerkes des Kunden im VPN-Gateway verschlüsselt und dem adressierten VPN-Gateway übergeben. Das VPN-Gateway stellt sicher, dass die Daten nur an autorisierte Knoten des VPN zugestellt werden. Das adressierte VPN Gateway entschlüsselt die Datenpakete und sendet diese an den Empfänger in den adressierten Teil des VPN.

Für den Aufbau der Verbindungen wird IPsec verwendet. Es findet keine End-to-End Verschlüsselung statt. Die Daten werden im Netzwerk des Vertragspartners weiterhin unverschlüsselt übertragen. Zu beachten ist, dass die über ein VPN zugreifenden PCs in einem ähnlich hohen Sicherheitskontext laufen sollten, wie das durch das Produkt ip firewall geschützte Netz, da sonst ein z. B. durch einen Trojaner befallener Heim-PC das Firmennetz infizieren könnte.

### 3.1 VPN Clients

VPN Clients sind ausschließlich als Software ausgelegt, welche vom Anbieter der Firewall bereitgestellt werden. Die VPN Software wird auf einem Client installiert. Die installierte Clientsoftware ist nicht für alle Betriebssysteme und Versionen von Betriebssystemen verfügbar. Die benötigten Versionen für die zum Einsatz kommenden Betriebssysteme sind mit **envia TEL** abzustimmen. **envia TEL** hat keinerlei Einfluss auf die Verfügbarkeit der Software für Betriebssysteme und deren Versionsstände. Die Authentifikation der Benutzer kann auf Benutzer- oder Systemebene erfolgen. Die Authentifikation wird von der Firewall durchgeführt.

## 4. Zusatzleistungen

**envia TEL** erbringt auf Wunsch des Kunden im Rahmen der technischen und betrieblichen Möglichkeiten sowie gegen gesondertes Entgelt zusätzliche Leistungen:

- Workshops zur Festlegung einer Security- Policy
- Erarbeitung eines detaillierten Firewallkonzepts
- Regelmäßiges Backup der PIX/Router-Konfigurationen
- Hochverfügbarkeitslösung mit zusätzlicher Firewall im Hot-stand-by-Betrieb
- Content-Filter zum Schutz vor Viren und anderem schädlichem Code (z. B. Trojanern)
- Filterung von E-Mail-Viren