

FIREWALL AS A SERVICE IN DER RHEIN-NECKAR CLOUD

Leistungsbeschreibung der PFALZKOM GmbH

Dieses Dokument enthält die Leistungsbeschreibung für das Produkt Firewall as a Service der PFALZKOM GmbH, nachfolgend die Gesellschaft genannt. Neben dieser Leistungsbeschreibung gelten die Allgemeinen Geschäftsbedingungen der Gesellschaft.

1. VERFÜGBARKEIT

Die Verfügbarkeit wird durch ein Cluster im Rechenzentrum der Gesellschaft sichergestellt. Der Service der Gesellschaft steht dem Kunden mit 99 % im Jahresmittel zur Verfügung.

2. NUTZUNG UND ANSCHLUSS DER ZENTRALEN FIREWALL

2.1 ZENTRALE (SHARED) FIREWALL

Das Produkt wird standardmäßig als zentrale ASP Lösung auf einer redundant ausgelegten virtualisierten Serverplattform angeboten.

ASP = Application Service Provider („Anwendungsdienstleister“).

2.2 ANBINDUNG

Das Produkt ist nur in Verbindung mit einem Internetanschluss HighP oder HighP-DSL der Gesellschaft buchbar. Zum Schutz dieses Anschlusses wird das Firewall-Produkt vorgeschaltet.

2.3 ADMINISTRATION

Die Administration der Zentralen Firewall und Veränderungen am Regelwerk erfolgen ausschließlich durch von der Gesellschaft autorisiertes Personal.

2.4 DEDIZIERTE LÖSUNG

Die Gesellschaft bietet den Firewall-Dienst optional auch als „Stand Alone“ Lösung an. In diesem Fall stellt die Gesellschaft dem Kunden ein dediziertes System in seinen Räumen oder im Rechenzentrum zur Verfügung.

3. FIREWALL-FUNKTIONALITÄT

Mehrstufiges Firewall-System mit Paketfilter, Application Layer Gateway und DMZ. Viruswall für HTTP und FTP- Verkehr.

3.1 FILTERTECHNIK

Direkter Datenverkehr (TCP / UDP und ICMP) vom LAN ins Internet und umgekehrt wird durch ein Regelwerk in den Paketfilterstufen (vor und hinter der DMZ) reglementiert (Statefull Paket Inspection).

3.2 PROXYDIENSTE / APPLICATION LAYER GATEWAY / VIRENSCHUTZ

Der HTTP- und FTP-Datenverkehr wird zusätzlich über einen Proxyserver geleitet. Ein direkter Kontakt zwischen LAN und Internet findet nicht statt. Somit können bestimmte Webseiten gesperrt werden. HTTP- und FTP-Verbindungen werden dadurch mit einer Antimalware-Lösung abgesichert. Ausnutzung von Protokollschwächen wird mittels Proxy-Server verhindert.

3.3 NAT

Vorhandene LAN-IP Adressen werden durch Network Address Translation (NAT) mit dem Internet verbunden.

3.4 DMZ

Durch ein erweitertes Regelwerk kann ein Netzbereich als demilitarisierte Zone (DMZ) konfiguriert werden. Die Konfiguration einer demilitarisierten Zone (DMZ) ist optional möglich.

3.5 PROTOKOLLE

Über die Zentrale Firewall können prinzipiell alle Internet-Protokolle geschaltet werden.

4. KONFIGURATION

4.1 REGELWERK-ERSTELLUNG

Für die Grundkonfiguration sind folgende Dienste standardmäßig erlaubt:

- E-Mail Versand und Empfang
- Keine direkten Internetzugriffe
- HTTP(S) / FTP via Proxy
- Standard-Virenschutz-Stufe
- Protokollierung

In Absprache mit dem Nutzer wird festgelegt, welche Protokolle und Ports freigeschaltet werden sollen. Das Setup wird schriftlich dokumentiert.

4.2 REGELWERK-ÄNDERUNGEN

In der Standardeinstellung ist der höchstmögliche Schutz eingestellt. Regelwerksänderungen sind Arbeiten, bei denen auf eine vorhandene Konfiguration der Firewall-Einstellungen zurückgegriffen werden kann. Dies können z.B. Freigaben von IP-Verbindungen im Paketfilter, Änderung von SMTP-Serveradressen, Konfiguration für den Zugriff von vorhandenen VPN Accounts oder Site-to-Site VPN oder die Anpassung eines bestehenden Kommunikationsweges (z.B. Reverseproxy für Outlook) sein.

Einführung neuer komplexer Regelwerksänderungen sind nicht im monatlichen Kontingent beinhaltet. Dies können z.B. VPNs, größere Umstellungen in Ihrer Netzwerk-Topologie oder die Einrichtung neuer Kommunikationswege sein.

Änderungen des firmeneigenen Regelwerkes können nur durch ein schriftliches Dokument erfolgen und werden, durch von der Gesellschaft autorisierte Mitarbeiter, im Zeitraum zwischen montags bis freitags von 8.00 bis 18.00 Uhr, sofern diese Tage keine gesetzlichen Feiertage in Rheinland-Pfalz sind, bearbeitet.

Änderungen am Regelwerk und andere Serviceanfragen werden über die Rufnummer: 0621 / 585-3285 oder per E-Mail: firewall@pfalzkommanet.de an die Gesellschaft gemeldet. Die Anzahl der enthaltenen Regelwerksänderungen pro Monat ist Einzelvertraglich nach dem jeweiligen Kundenbedarf vereinbart. Die Kontingente sind nicht auf Folgemonate übertragbar. Sämtliche Änderungen werden schriftlich dokumentiert.

4.3 VPN-KONZENTRATOR

VPNs können optional eingerichtet werden. Standardmäßig wird hierfür eine OpenVPN (TLS) Lösung eingesetzt. Andere Protokolle wie z. B. IPSEC oder L2TP sind nach Absprache möglich.

4.4 IP ADRESSEN IM LAN

Im Intranet werden die privaten IP-Adressen des Nutzers verwendet. Mit dem HighP- oder HighP-DSL-Anschluss stellt die Gesellschaft eine feste, öffentliche IP-Adresse aus dem Adressraum der Gesellschaft zur Verfügung. Die Rechte an den IP-Adressen verbleiben bei Auslaufen des Vertrages bei der Gesellschaft. siehe Leistungsbeschreibung:

- HighP

4.5 SMARTPHONE-ANBINDUNG

Optional kann ein weiteres Sicherheitsmodul für mobile Anwendungen dediziert eingerichtet werden.

5. ADMINISTRATION UND MONITORING

5.1 MONITORING

Die Anlage ist in das Netzwerkmanagementsystem integriert und wird aktiv überwacht.

Überwacht werden:

- Erreichbarkeit von primären und sekundären Systemen
- Funktionalität von Diensten
- NTP: Richtigkeit der Zeit für Protokollierung
- SSL: Gültigkeit von Zertifikaten
- POP3 / IMAP Frontsideproxy-Funktion
- HTTP(S) Frontsideproxy-Funktion
- Viruswall: Patternfile

5.2 ROUTINEMÄßIGE SYSTEM-UPDATES

Die auf den Systemen eingesetzten Software-Images werden nach dem Ermessen der Gesellschaft regelmäßig aktualisiert und auf dem neuesten Stand der Technik gehalten.

Innerhalb der Revision werden diese Software-Images auf die Produktivsysteme installiert. Kritische Modul-Updates werden mit den Nutzern abgesprochen.

5.3 REVISION

Standardmäßig wird einmal jährlich eine Revision der Anlage durchgeführt. Diese Wartung wird rechtzeitig im Voraus von der Gesellschaft angekündigt. Es kann unter Umständen zu einem kurzen Dienstausfall führen. Die Revision gilt nicht als Störung.

Bestandteile der Revision:

- Pflege und ggf. Backup der Protokolldateien
- Funktionalitätstests der Systeme
- Neuinstallation sicherheitsrelevanter Server auf Basis der aktuellen Softwareversionen
- Überprüfung des Netzwerkmanagements
- Überprüfung des Virenschutzes
- Überprüfung von Backup-Anbindungen

5.4 WARTUNG

Wartungsarbeiten an den Systemen werden im Regelfall mindestens 24 Stunden im Voraus angekündigt. Hierbei wird die voraussichtliche Länge der Wartungsarbeiten in Form eines Wartungsfensters mitgeteilt.

6. ENTSTÖRUNG

Die Gesellschaft beseitigt Störungen eigener technischer Einrichtungen im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten. Hierbei werden Leistungen in Abhängigkeit des vom Kunden gewählten Servicelevels erbracht.

6.1 SERVICELEVEL

Die Leistung Standard Service ist mit dem Grundpreis abgegolten.

6.2 ANNAHME DER STÖRUNGSMELDUNG

Die Gesellschaft nimmt Störungsmeldungen innerhalb der Servicebereitschaftszeit telefonisch unter der Rufnummer **0800-6883633** entgegen.

6.3 SERVICEBEREITSCHAFT

Standard Service: Montags bis freitags von 8.00 bis 18.00 Uhr, sofern diese Tage keine gesetzlichen Feiertage in Rheinland-Pfalz sind.

Premium Service: Montags bis sonntags sowie an gesetzlichen Feiertagen von 0.00 bis 24.00 Uhr.

6.4 REAKTIONSZEIT

Standard Service: In der Regel innerhalb von einer (1) Stunde während der in 6.3 definierten Servicebereitschaft.

Premium Service: In der Regel innerhalb von einer (1) Stunde während der in 6.3. definierten Servicebereitschaft.

6.5 ENTSTÖRUNGSFRIST FIREWALL

Bei Störungsmeldungen, die innerhalb der unter 6.3 definierten Servicebereitschaftszeit eingehen, wird nach folgenden Störungsklassen kategorisiert:

SK1:

Fehler, durch die die zweckmäßige Nutzung des Dienstes nicht möglich oder unzumutbar eingeschränkt ist. (System arbeitet nicht.)

SK2:

Fehler, durch die die zweckmäßige Nutzung des Dienstes zwar beeinträchtigt ist, der produktive Betrieb jedoch fortgeführt werden kann. (System arbeitet eingeschränkt.)

SK3:

Fehler, durch die die zweckmäßige Nutzung nicht oder nur unwesentlich eingeschränkt ist.

Die Störungen werden in der Regel innerhalb folgender Zeiten (abhängig vom Servicelevel) beseitigt:

SK1: innerhalb von acht Stunden

SK2: am darauffolgenden Arbeitstag

SK3: keine garantierte Zeit

Die Störungsdauer errechnet sich aus der Zeitdifferenz zwischen dem Eingang der Störungsmeldung bei der zuständigen Ansprechstelle der Gesellschaft und dem Zeitpunkt der Störungsbeseitigung. Bei Störungsmeldungen, die außerhalb der definierten Servicebereitschaft eingehen, beginnt die Entstörungsfrist am folgenden Werktag (Montag bis Freitag) um 08.00 Uhr.

Fällt das Ende der Entstörungsfrist auf einen gesetzlichen Feiertag, Samstag oder Sonntag, wird die Entstörungsfrist ausgesetzt und am folgenden Werktag (Montag bis Freitag) fortgesetzt. Verspä-

tungen, die vom Kunden zu vertreten sind, vermindern die errechnete Störungsdauer entsprechend.

Die Gesellschaft beseitigt eine Störung während der Servicebereitschaftszeit innerhalb der angegebenen Entstörungsfristen und abhängig von der Serviceklasse.

6.6 RÜCKMELDUNG

Die Gesellschaft teilt dem Kunden die erfolgreiche Beseitigung der Störung unverzüglich telefonisch, per Fax oder E-Mail mit. Ist der Kunde am Tag der Entstörung in der Zeit der Servicebereitschaft nicht erreichbar, erfolgt die Benachrichtigung erst am Folgetag.

7. VERTRAGSBEENDIGUNG

Bei Vertragsbeendigung (Kündigung / Ablauf / Aufhebung / etc.) wird die Gesellschaft die Zugänge unverzüglich sperren; das Regelwerk und die Logfiles werden gelöscht. Das Wiederherstellen der Daten ist nicht möglich.