redIT

REDIT FIREWALL S, M, L

Leistungsbeschreibung / Nutzungsbedingung

Inhaltsverzeichnis

1 SERVICE LEVELS

- Die jährliche garantierte Verfügbarkeit der Services beträgt 99.5%. redIT stellt während dieser Zeit den reibungslosen Betrieb der gesamten Umgebung sicher und nimmt Anpassungen und Fehlerbehebungen vor, die nötig sind, um den Betrieb sicherzustellen.
- 7 X 24h Störungsannahme (E-Mail und *Telefon)
  (*nur für Kunden mit separaten Wartungsverträgen! Ansonsten gilt Mo - Fr 07.00 17.00)
- Maximal 2h Reaktionszeit (Mo - Fr von 07:00 - 17.00)

2 EINLEITUNG

Unsere redIT Firewall basiert auf einer mehrfach ausgezeichneten Next Generation Firewall, welche eine neue Generation von Real-Time Security Gateways definiert. Die redIT Firewall ist mehr als nur eine einfache Managed Firewall.
Die redIT Firewall ist eine ASIC beschleunigte Security Appliance, die alle wichtigsten Security- und Netzwerk-Funktionalitäten vereint, einschliesslich Firewall, SSL- und IP-Sec-VPN, Anti Virus, Intrusion Prevention, Web Filtering, Anti Spam, Application Control, Data Loss Prevention, SSL Traffic Inspection und WAN-Optimierung. Die UTM (Unified Threat Management; auf Deutsch sinngemäss in etwa: Zentrales Bedrohungsmanagement). Signaturen der redIT Firewall-Systeme werden weltweit automatisch und rund um die Uhr aktualisiert. Dies stellt den Real-Time Schutz vor Content-basierten E-Mail und Internetbedrohungen wie Viren, Würmern, Intrusions, ungewolltem Netzwerkverkehr und mehr sicher.
Eine redIT Firewall arbeitet als Filter zwischen dem Internet und dem Netzwerk des Kunden. Sie verfügt über ein Regelwerk, welches die Filtereigenschaften gemäss den Security Policies, dem Netz und den Systemvoraussetzungen des Kunden abbildet. Mögliche Angriffe, welche sich auf IP/ICMP [Netzwerk-Layer] oder TCP/UDP [Transport-Layer] beziehen, werden innerhalb der redIT Firewall erkannt und abgewehrt. Dies gilt für Angriffe auf die redIT Firewall und die zu schützenden Netzwerke.

3 PRODUKTSPEZIFIKATIONEN

Die redIT Firewall gibt es in 3 verschiedenen Ausprägungen:

redIT Firewall S (ungefähr 20 Benutzer)
redIT Firewall M (ungefähr 40 Benutzer)
redIT Firewall L (ungefähr 80 Benutzer)

Die redIT Firewall besteht aus technischen Einrichtungen, die eine abgesicherte Verbindung mit dem Internet ermöglichen. Diese Einrichtungen werden dem Kunden für die Dauer des Vertragsverhältnisses bereitgestellt:

- Hardwarekonfiguration (Anzahl Anschlüsse variiert je nach Modell):
  - GE RJ45 Anschlüsse 100/1000 Mbps Switch-Ports, welche zu DMZ-Ports um konfiguriert werden können
  - GE RJ45 Anschlüsse 100/1000 Mbps WAN-Ports
  - Konsole Anschluss
  - USB-Anschluss
  - Netzadapter inkl. Stromkabel
- Firewall mit UTM-Signaturen
- Sicherung der aktuellen redIT Firewall Konfiguration
- Permanente Überwachung Ihrer redIT Firewall
- Hardware-Austausch bei Defekt (Next Business Day)
- VPN-Verbindungen für den sicheren Datenverkehr zwischen mehreren Standorten
- Periodisches Update der Firewall-Firmware
- Zentralisiertes Log
- Next Generation Firewall Throughput
- Thread Protection Throughput
- IPsec Throughput
- SSL Inspection
- Application Control
- IPS (Intrusion Prevention System)

Die vorgeschlagene Benutzeranzahl ist nur ein Richtwert und kann nach Unternehmen und deren Anforderung variieren.

3.1 Grundkonfiguration (nach Aufwand)

Die Grundkonfiguration der redIT Firewall erfolgt auf Basis der mit dem Kunden abgestimmten Security Policies. Diese Security Policies werden mittels Formularvorlage der redIT, vom Kunden definiert und der redIT vor der Inbetriebnahme mitgeteilt. Der Kunde hat keine Möglichkeit die Konfiguration der redIT Firewall zu verändern. Dem Kunden wird ein Read-Only-User zur Verfügung gestellt. Mit diesem User hat er Einsicht in die Konfigurationseinstellung und Logs der Firewall.

3.2 Konfigurationsänderungen

Eine Änderung an der Konfiguration kann nur schriftlich per Support-Ticket beantragt werden. Für die Bestätigung wird redIT den Kunden telefonisch kontaktieren und den Änderungszeitpunkt mit ihm vereinbaren. Konfigurationsänderungen werden immer nach Aufwand verrechnet.

3.3 UTM-Signaturen

Der Kunde hat die Möglichkeit Security Policies inklusive Application Control und IPS, Web Filtering, Anti Virus und Anti Spam zu aktivieren. Die redIT verwendet die offiziell vom Hersteller zur Verfügung gestellten UTM-Signaturen und stellt die redIT Firewall auf ein automatisches Update dieser ein. UTM-Signaturen sind Updates der Datenbank-basierten Services wie Antivirus, IDP, Webfilter, Anti Spam, etc. Für die Funktionsweise und Tüchtigkeit der Signaturen des Herstellers, kann redIT keine Haftung übernehmen.

3.4 Sicherung der aktuellen redIT Firewall Konfiguration

redIT erstellt bei der ersten Konfiguration sowie bei jeder weiteren Konfigurationsänderung automatisch eine Sicherung der Firewall-Konfiguration. Somit ist gewährleistet, dass zum Beispiel beim Austausch eines defekten Gerätes die letzte verfügbare Konfiguration verwendet werden kann und dieser möglichst rasch und unkompliziert durchgeführt werden kann.

3.5 Permanente Überwachung Ihrer redIT Firewall

Im Leistungsumfang ist die permanente Überwachung der Firewall im Preis enthalten (PING). Bei einer Störung des Gerätes während der Öffnungszeiten kontaktiert redIT den Kunden proaktiv und schlägt diesem Lösungsmassnahmen vor oder leitet je Störung entsprechende Massnahmen selbständig ein, um den Fehler möglichst rasch zu beheben.

3.6 Austauschservice NBD (Next Business Day)

Bei einem Defekt/Ausfall der Firewall ist redIT verpflichtet während den Bürozeiten (08:00 Uhr - 12:00 Uhr und 13:00 Uhr - 17:00 Uhr) dem Kunden bis zum nächsten Tag ein Gerät mit der letzten gesicherten Konfiguration zur Verfügung zu stellen. Das Gerät wird auf dem Postweg zugestellt oder kann vom Kunden bei redIT direkt abgeholt werden.

3.7 VPN-Verbindungen für den sicheren Datenverkehr zwischen mehreren Standorten

Für den Aufbau von VPN-Tunneln verlässt sich redIT auf die Angaben im Grundkonfigurationsformular.

3.8 Haftung

Datentransfers, welche nicht die redIT Firewall durchlaufen, entziehen sich der Kontrolle durch dieser. Ebenso kann die redIT Firewall keine verschlüsselten oder mehrfach komprimierten Inhalte nach schadhaften Bedrohungen untersuchen. Der Service gewährleistet nicht die Sicherheit des Kundennetzwerkes, sondern stellt einen Sicherheitsmechanismus zur Verfügung. Eine redIT Firewall kann keinen Schutz vor unbekannten Angriffen gewährleisten.

4 INBETRIEBNAHME

Nach Bestelleingang wird die Machbarkeit überprüft und mit dem Kunden kommuniziert. Der Kunde wird über den weiteren Ablauf informiert und das Installationsdatum bekannt gegeben.

5 VORAUSSETZUNGEN

Um redIT Firewall zu nutzen, sind folgende Voraussetzungen seitens des Kunden zu erfüllen, die nicht Produktbestandteile sind:

- Machbarkeit - Diese Prüfung wird bei Bestelleingang überprüft
- Stromanschluss für Firewall am Kundenstandort

6 NICHT ENTHALTENE LEISTUNGEN

- Konfiguration der redIT Firewall (nach Aufwand)
- Inbetriebnahme vor Ort (nach Aufwand)
- Netzwerkkabel (RJ45 min. CAT 5e)
- Verlängerungskabel und Steckdosenleisten für die Stromversorgung
- Rack Mount Kit (kann separat bestellt werden)

7 ALLGEMEINE BESTIMMUNGEN

redIT kann nicht für Konfigurations- oder Manipulationsfehler des Kunden oder Dritten haftbar gemacht werden. Für Services, bei welchen Systemressourcen geteilt verwendet werden (Shared Services), nimmt der Kunde Rücksicht und schränkt die übermässige Nutzung dieser Ressourcen ein, um eine Beeinträchtigung der Leistung anderer Kunden auf demselben System zu verhindern («Fair use»). Beansprucht der Kunde die Systemressourcen über Gebühr (Vergleich mit dem Durchschnitt der Systemnutzer plus Toleranz), unterbreitet redIT dem Kunden ein Angebot für eine höhere Leistungsklasse. Nimmt der Kunde dieses Angebot nicht an, behält sich redIT vor, fristlos vom Vertrag zurückzutreten.
Die Services werden «Best effort» gewährleistet. Es gibt, wo nicht anders vermerkt, keine Garantie für bestimmte zugewiesene Systemressourcen oder Leistungsmerkmale. Bestehen Anzeichen eines rechts- oder vertragswidrigen Verhaltens, insbesondere einer missbräuchlichen Nutzung eines Service, kann redIT den Zugriff auf den Service ohne Vorankündigung umgehend entschädigungslos sperren oder einschränken, den Kunden zur rechts- und vertragskonformen Benutzung anhalten, den Vertrag frist- und entschädigungslos auflösen und gegebenenfalls Schadenersatz sowie die Freistellung von Ansprüchen Dritter verlangen.
Sollten einzelne Bestimmungen dieser Leistungsbeschreibung/Nutzungsbedingung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der übrigen Bestimmungen des jeweiligen Vertrags nicht tangiert.