

redNET Secure Gateway

Leistungsbeschreibung

1. Einleitung

Unsere redNET Secure Gateways basieren auf den mehrfach ausgezeichneten Antivirus-Firewalls von FortiGate, welche eine neue Generation von Real-Time Security Gateways definieren. Ein redNET Secure Gateway ist mehr als einfach nur eine Managed Firewall. FortiGate Systeme sind weltweit die einzigen, die von der ICSA (International Computer Security Association) für Antivirus, Anti-Spyware, IPSec, Firewall und Intrusion Detection zertifiziert sind und bieten so den höchsten Grad an verfügbarer Sicherheit. Die Geräte erkennen und entfernen schädliche Inhalte wie Viren, Würmer, Angriffe, unerwünschte Internet-Inhalte und mehr aus dem E-Mail- und Internet-Verkehr ohne die Netzwerk-Performance zu verringern.

Ein redNET Secure Gateway arbeitet als Filter zwischen dem Internet und dem Netzwerk des Kunden. Sie verfügt über ein Regelwerk, welches die Filtereigenschaften gemäss der Security Policy und 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 des Secure Gateway erkannt und abgewehrt. Dies gilt für Angriffe auf den Secure Gateway und die zu schützenden Netzwerke.

2. Leistungsumfang

redNET Secure Gateway besteht aus technischen Einrichtungen, die eine abgesicherte Verbindung mit dem Internet ermöglichen. Diese Einrichtungen werden dem Kunden für die Dauer des Vertragsverhältnisses bereitgestellt.

- Grundkonfiguration und Nutzung des Secure Gateways
- Automatische Updates der Secure Gateway Software
- Automatisches Update der Secure Gateway Signaturen
- Sicherung der aktuellen Secure Gateway Konfiguration
- Permanente Überwachung Ihres Secure Gateways
- Monatliche Reports über Firewall-Aktivitäten (falls als Option bestellt)
- HW-Replacement (Austausch bei Ausfall Ihres redNET Secure Gateways)
- Betrieb von VPN-Verbindungen für den sicheren Datenverkehr zwischen Hauptsitz, Filialen und Home Office Arbeitsplätzen

2.1 Herstellung

2.1.1 Grundkonfiguration

Die Grundkonfiguration des Secure Gateways erfolgt auf Basis der mit dem Kunden abgestimmten Security Policy. Falls der Kunde einen statischen IP-Adressen-Block besitzt brauchen wir 1 IP-Adresse aus seinen IP-Adressen-Pool für den Secure Gateway.

2.1.2 Automatische Update der Software

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.

2.1.3 Automatisches Update der Signaturen

redIT verwendet die offiziell zur Verfügung gestellten Signaturen des Herstellers und stellt den Secure Gateway auf ein automatisches Update ein. Für die Funktionsweise und Tüchtigkeit der Signaturen des Herstellers, kann redIT keine Haftung übernehmen.

2.2 Leistungen im Detail

2.2.1 Auswertungen

Eine Auswertung der aktuell stattgefundenen Aktivitäten auf dem redNET Secure Gateway, wird einmal im Kalendermonat (falls als Option bestellt) dem Kunden ausgehändigt.

2.2.2 Konfiguration

Der Kunde hat keine Möglichkeit die Konfiguration des Secure Gateways zu verändern.

2.2.3 Konfigurationsänderungen

Eine Änderung an der Konfiguration kann nur schriftlich per E-Mail an redNET.services@redIT.ch beantragt werden. Für die Bestätigung wird redIT den Kunden telefonisch kontaktieren. redIT wird Konfigurationsänderungen nur von den auf der Security Police aufgeführten Personen akzeptieren. Änderungen können nur innerhalb der Betriebszeiten durchgeführt werden.

2.2.4 Haftung

Datentransfers, welche nicht den Secure Gateway durchlaufen, entziehen sich der Kontrolle durch den Secure Gateway. Ebenso kann der Secure Gateway keine verschlüsselten oder mehrfach komprimierten Inhalte nach schadhafte Bedrohungen untersuchen. Der Service gewährleistet nicht die Sicherheit des Kundennetzwerkes sondern stellt einen Sicherheitsmechanismus zur Verfügung. Ein Secure Gateway kann keinen Schutz vor unbekanntem Angriffen geben.

3 Konfiguration

3.1 redNET Secure Gateway

Ein redNET Secure Gateway kann in folgenden Konfigurationsvarianten ausgeliefert werden:

3.2 Secure Gateway im Routing Modus (NAT)

Ermöglicht Aufbau und Betrieb eines DMZ [demilitarisierte Zone]. Weitere Details zu den Konfigurationen werden mit dem Kunden nach dessen Bedürfnissen und vorhandene Infrastruktur abgeklärt.

3.3 Secure Gateway im Bridge Modus (Transparent)

Die bestehende Infrastruktur des Kunden wird nicht verändert; der redNET Secure Gateway wird transparent in das Netzwerk des Kunden integriert. Weitere Details zu den Konfigurationen werden mit dem Kunden nach dessen Bedürfnissen und vorhandene Infrastruktur abgeklärt.

4 Service Levels

Garantierte Verfügbarkeit	99.5%
Monitoring/Alarmierung	7x24h (falls Option Monitoring/Alarmierung)
Störungsannahme	7x24h
Reaktionszeiten (Mo – Fr von 08.00 – 12.00 und 13.00 – 17.00)	Max. 2h
Reaktionszeiten (Mo – Fr von 17.00 – 08.00, Sa, So, Feiertage)	Max. 4h (falls Option Pikettbereitschaft)

Im Störfall ist der Helpdesk von Montag bis Freitag von 08.00 – 12.00 und 13.00 – 17.00 Uhr (ausgenommen gesamtschweizerische und lokale Feiertage) unter Telefon 0848 000 801 erreichbar. Ausserhalb dieser Zeiten können Sie jederzeit eine E-Mail an: redNET.services@redIT.ch absetzen.

4.1 Reaktionszeit

Die Reaktionszeit ist der Zeitraum zwischen der Störungsmeldung durch den Kunden und der Bestätigung der Störungsannahme durch das für die Störungsbehebung verantwortliche Team.

4.2 Wartungsarbeiten an den redIT Anlagen

Die periodische Wartung an den Support- und Überwachungseinrichtungen der redIT kann eine geplante Unterbrechung dieser Services bewirken. Die Wartungen werden während einem definierten Zeitraum, dem so genannten Wartungsfenster durchgeführt und mindestens 2 Tage im Voraus angekündigt. Die Wartungsfenster sind auf den ersten und dritten Mittwoch des Monats von 18.00 bis 06.00 Uhr festgelegt.

In dringenden Fällen kann eine ungeplante Wartung ausserhalb des offiziellen Wartungsfensters notwendig sein. In solchen Fällen werden die Kunden über den Beginn und das voraussichtliche Ende der Wartung sofort informiert.