WORTMANN AG
IT. MADE IN GERMANY.

terra CLOUD

Leistungsbeschreibung Firewall VM

Präambel

Um diese Leistungsbeschreibung vollständig verstehen zu können ist ein umfassendes Wissen im Bereich der Informationstechnologie notwendig. Das gleiche gilt für die dem Kunden übergebene Administration der Firewall VM.

Ist in diesem Dokument von IP-Adressen die Rede, so geht es ausschließlich um IPv4-Adressen nach RFC 791.

Produktbeschreibung

Die TERRA CLOUD GmbH stellt dem Kunden im Rahmen Ihrer Leistungen eine private Firewall VM zur Verfügung. Diese Firewall VM verbindet das öffentliche Internet mit dem privaten Netzwerk, das dem Kunden dediziert als eigener VLAN Abschnitt zur Verfügung gestellt wurde. Dabei verwendet der Kunde in seinem privaten Netzwerk ausschließlich private IP-Adressen nach RFC 1918. Die zentrale Aufgabe der Firewall VM ist der Schutz des Kundennetzwerkes mit verschiedenen Mechanismen:

Network Address Translation

Dieser Dienst dient zur Umsetzung der privaten IP-Adressen des Kundennetzwerkes in öffentliche IP-Adressen des Internets (Source NAT) und der Umsetzung von öffentlichen IP-Adressen, die am externen Interface der Firewall VM anliegen, auf private IP-Adressen im Kundennetzwerk (Destination NAT). Die Umsetzung basiert auf Teilen der RFCs 2663, 2766 und 3022.

Packetfilter (mit Stateful Packet Inspection)

Um steuern zu können, welche öffentlichen IP-Adressen mit welchen IP-Adressen des Kundennetzwerkes kommunizieren dürfen (IPv4-Pakete miteinander austauschen dürfen), ist der Packetfilter vorhanden. Dabei stehen folgende Entscheidungskriterien für die Auswahl einer Regel zur Verfügung. Quell-IPv4-Adresse einer Kommunikation. Ziel-IPv4-Adresse einer Kommunikation. Das verwendete Transportprotokoll (TCP, UDP, ESP und ICMP). Bei den Transportprotokollen TCP und UDP können zusätzlich die in diesen Protokollen verwendeten Quell und Zielports der Kommunikation ausgewertet werden. Die Firewall unterstützt bis zu 500 solcher Regeln je Firewall VM. Das Regelwerk wird von Zeile 1 abwärts abgearbeitet – sobald eine Regel zutrifft, wird deren Aktion durchgeführt und es werden keine weiteren Regeln mehr für dieses Paket berücksichtigt. Als Aktion steht dem Kunden zur Verfügung:

„Accept“ – das Paket und die damit zusammenhängende Kommunikation wird erlaubt.
„Drop“ – das Packet wird verworfen – es gibt keine Rückmeldung der Firewall an den Absender
„Reject“ – das Packet wird mit einem ICMP Paket „Destination Unkown“ beantwortet und verworfen.

Implizite Regeln

Innerhalb der Firewall VM gibt es so genannte implizite Regeln. Diese Regeln erlauben oder verbieten Netzwerktraffic. Diese impliziten Regeln können durch den Kunden nur eingeschränkt verändert werden und sind nur in einem gesonderten Dialog ersichtlich.

VPN Funktion - OpenVPN

Für den verschlüsselten Zugriff des Kunden auf Geräte in seinem Kundennetzwerk inklusive der Firewall VM stellt die Firewall eine sogenannte VPN-Verbindung zur Verfügung.

Diese VPN-Verbindung basiert auf der VPN-Software OpenVPN und nutzt in der Standardeinstellung zum Transport der gesamten Verbindung (Steuerung und Daten) UPD als Transportprotokoll.

Damit der Kunde eine VPN-Verbindung mit der Firewall VM aufbauen kann, muss er über einen passenden Client für sein Betriebssystem verfügen und sich aus dem TERRA CLOUD Portal die dazu gehörige Konfigurationsdatei sowie die Zugangsdaten (Benutzername und Passwort) besorgen. Außerdem muss der Kunde sicherstellen, dass dieser Rechner bis zur Firewall VM des Kundennetzwerkes uneingeschränkt das Transportprotokoll UDP von einem beliebigen Quellport auf den Zielport 1194 verwenden kann. Von einer Konfigurationsänderung des Transportprotokolles und des Zielports wird abgeraten.

Der Administrator kann weitere OpenVPN-Konten konfigurieren und verwenden. Diese Anbindung ist sowohl für einzelne Arbeitsplätze als auch für eine so genannte LAN-LAN-Kopplung geeignet. Als Gegenstellen für eine LAN-LAN-Kopplung sind Firewalls von Wortmann und Securepoint freigegeben. Firewalls weiterer Hersteller müssen vom Kunden auf ihre Kompatibilität mit der Firewall VM des Kundennetzwerkes auf eigene Kosten und Risiko getestet werden.

VPN-Funktion – IPSec VPN

Für die Anbindung von Endgeräten und für die LAN-LAN Kopplung steht auch das VPN-Protokoll IPSec zur Verfügung.

Für die Anbindung von Endgeräten empfehlen wir die Verwendung von OpenVPN.

Als Gegenstellen für eine LAN-LAN Kopplung mit IPSec sind Firewalls von Wortmann und Securepoint freigegeben. Firewalls weiterer Hersteller müssen vom Kunden auf ihre Kompatibilität mit der Firewall VM des Kundennetzwerkes auf eigene Kosten und Risiko getestet werden.

Administration / Administrationsverantwortung

Sobald dem Kunden die Administration der Firewall übergeben wurde, ist er auch für verschiedene vorkonfigurierte Dienste selber verantwortlich. Eine Fehlkonfiguration kann ihn z.B. auch von der Administration seines Netzwerkes abschneiden.

Optionale Sicherheitsfunktionen

Contentfilter-Paket

Das optional zu buchende Contentfilter-Paket dient zur Analyse und Kontrolle von HTTP- und HTTPS-Datenströmen aus dem Kundennetzwerk ins öffentliche Internet. Dabei kann HTTP und HTTPS automa-

tisch (transparent) aus dem Netzwerkverkehr herausgefiltert oder der HTTP-Proxy fest in der Software innerhalb des Kundennetzwerks hinterlegt werden.

Das Contentfilter-Paket bietet folgende Funktionen:

- Zugriffssteuerung anhand von Benutzern (nur bei aktiver Authentifizierung), Netzwerkobjekten und Netzwerkgruppen
- Freigabe/Sperrung einzelner Webseiten
- Freigabe/Sperrung von Website-Kategorien
- Freigaben gelten immer vor Sperrungen

Zur Analyse der Zugehörigkeit einer URL zu einer Kategoriewird diese zum Hersteller der Firewall VM Software übertragen.

Bei aktiviertem Antivirus-Paket prüft der HTTP-Proxy bei umgeleitetem Traffic diesen auch auf Viren, dabei kann zwischen zwei Virenscannern gewählt werden.

Eine userbasierte Steuerung des Zugriffs ist nicht im transparenten Modus möglich.

Es wird empfohlen, zum Contentfilter-Paket immer auch das Antivirus-Paket zu buchen.

Spamfilter-Paket

Mit dem optional zu buchenden Spamfilter-Paket kann der Kunde SMTP-Datenströme von unerwünschten Emails befreien. Dafür ist es notwendig, dass der Kunde zu filternde Email-Daten mittels des SMTP-Protokolles über das Mailrelay der Firewall routet. Hier kann der Kunde definieren für welche Domains er Emails entgegen nimmt und wohin diese nach der Prüfung weitergeleitet werden sollen. Dafür ist es notwendig, dass der Kunde in seinem Kundennetzwerk einen Mailserver mit SMTP-Schnittstelle betreibt.

Zur Spamabwehr verfügt die Firewall VM über folgende Mechanismen:

Greeting Pause

Beim Beginn der Kommunikation legt die Firewall VM eine Pause in der von SMTP vorgesehenen Begrüßung (Greeting) ein – wenn die Gegenstelle in dieser Zeit weitere Daten schickt, wird die Verbindung unterbrochen. Diese Funktion kann an- und abgeschaltet werden.

Graylisting (oder Greylisting)

Mittels Graylisting erfolgt die Annahme einer Email per SMTP nur, wenn der Absender schon einmal eine Email an den Empfänger vom gleichen Absenderserver geschickt hat. Schickt ein Mailserver das erste Mal eine Email an einen Empfänger des Kunden, so wird diese Verbindung mit einem temporären Fehler abgelehnt. Die Firewall VM merkt sich nun die IP-Adresse des sendenden Servers, die Emailadresse des Absenders und die Emailadresse des Empfängers und setzt diese für eine eingestellte Zeit (z. B. 7 Tage) auf eine Whitelist. Beim nächsten Zustellungsversuch des gleichen Absender-Servers wird die Email dann angenommen. Diese Funktion kann an- und abgeschaltet werden.
Die Funktion Graylisting entspricht nicht dem RFC 2821 (SMTP) und kann bei eingehenden Emails zu Verzögerungen auch im gewünschten Mailverkehr führen.

Message Identifikation Verfahren

Aus dem Inhalt einer zu prüfenden Email wird ein Message ID generiert. Diese wird zur zentralen Datenbank des Herstellers übertragen und die Firewall VM erhält einen Status zu dieser Email zurück. Der Email-Inhalt wird dabei in keinem Fall an den Hersteller übertragen. Der Status dieser Email kann lauten
„Clean“ – Email ist unverdächtig
„Probably Spam“ – Email ist möglicherweise unerwünscht – hierunter fallen oft auch abonnierte Newsletter.
„Spam“ – Die Email ist eine Spam.
Eine SPAM-Email wird definiert als eine Email deren Zustellung der Kunde nicht angefordert hat. Ausdrücklich kein SPAM sind Newsletter, die der Kunde abonniert hat. Ausdrücklich keine SPAM sind Geschäfts-Emails oder private Emails von korrekt arbeitenden Unternehmen oder sich korrekt verhaltenden Privatpersonen.

Die Spamerkennungsquote liegt bei Aktivierung aller Funktionen mindestens bei 98% im Jahresmittel. Die Fehlerquote – also die Deklarierung erwünschter Emails als SPAM – liegt bei weniger als 1% im Jahresmittel.

Bei aktiviertem Antivirus-Paket prüft die Firewall VM die durchgeleiteten Emails auch auf Viren, dabei werden beide integrierten Virenscannern nacheinander verwendet.

Es wird empfohlen, zum Spamfilter-Paket immer auch das Antivirus-Paket zu buchen.

Antivirus-Paket

Das optional zu buchende Antivirus-Paket kann nicht einzeln gebucht werden, sondern ist immer eine empfohlene Erweiterung für das Contentfilter-Paket und / oder das Spamfilter-Paket. Die Funktion des Antivirus-Paketes wird in der Leistungsbeschreibung des Content-Filter-Paketes und des Spam-Filter-Paktes beschrieben.

Firewall Management

Die betriebsbereite Übergabe der Firewall ist immer Bestandteil der Leistung. Für die Installation und den Betrieb stehen nun mehrere Varianten zur Verfügung.

1. **Self Managed Firewall VM**
   Die Firewall VM wird mit einer vorkonfigurierten Konfiguration geliefert und zur eigenen Administration durch den Kunden an diesen übergeben. Ab dem Zeitpunkt der Übergabe an den Kunden ist dieser selber verantwortlich für den Betrieb der Firewall. Hierfür sind dedizierte technische Kenntnisse notwendig. Der Kunde sollte die Firewall VM ausschließlich durch ausreichend qualifiziertes Personal konfigurieren lassen.

2. **Erstinstallation**
   Die Firewall VM wird mit einer vorkonfigurierten Konfiguration geliefert und dann durch das NOC Team der TERRA Cloud GmbH auf eine mit dem Kunden abgestimmte Konfiguration gebracht. Dafür wird dem Kunden ein Fragebogen zur Verfügung gestellt, den dieser ausgefüllt zur Verfügung stellen muss. Die einstellbaren Konfigurationsteile der Firewall VM entsprechen den Möglichkeiten die aus dieser Leistungsbeschreibung ergehen. Nicht aufgeführte Dienste können nach Einzelüberprüfung entgeldlich zusätzlich konfiguriert werden. Ein Anrecht auf Konfigurationen außerhalb der Leistungs-

beschreibung besteht nicht.
Die Firewall VM wird inkl. Konfiguration an den Kunden übergeben und mit diesem zusammen ge testet. Nach erfolgreichem Test geht die Firewall in den Status „Self Managed“ über – somit gelten die Bedingungen von Absatz 1.
Die Erstkonfiguration ist beschränkt auf 40 Netzwerkobjekte und 40 Portfilterregeln, sowie die Einrichtung einer IPSEC LAN-LAN Kopplung und dem Anlegen von drei OpenVPN-Zugängen für Roadwarrior. Weitere Konfigurationen sind gegen Aufpreis verfügbar.

3. Full Managed

Die gesamte Konfiguration und Verwaltung der Firewall VM wird durch das NOC Team der TERRA CLOUD GmbH vorgenommen. Hierbei wird nach der Bereitstellung der Firewall VM diese entsprechend der mit dem Kunden abgestimmten Daten konfiguriert. Für die Konfiguration wird dem Kunden ein Fragebogen zur Verfügung gestellt, den dieser entsprechend ausgefüllt der TERRA CLOUD GmbH zur Verfügung stellen muss.
Die Erstkonfiguration ist beschränkt auf 40 Netzwerkobjekte und 40 Portfilterregeln, sowie die Einrichtung einer IPSEC LAN-LAN-Kopplung und das Anlegen von 3 OpenVPN-Zugängen für Roadwarrior. Weitere Konfigurationen sind gegen Aufpreis verfügbar.
Für Änderungen (Changes) im Betrieb steht dem Kunden ein Kontingent von einzelnen Aktionen zur Verfügung. Der Kunde kann 40 Netzwerkobjekte neu einrichten oder ändern lassen. Der Kunde kann 40 Portfilterregeln einrichten oder ändern lassen. Der Kunde kann eine IPSEC LAN-LAN-Kopplung einrichten oder ändern lassen. Der Kunde kann bis zu 3 OpenVPN Zugänge für Roadwarrior einrichten oder ändern lassen. Weitere Konfigurationen sind gegen Aufpreis verfügbar. Das Kontingent wird alle 12 Monate wieder auf die oben stehenden Werte aufgefüllt. Alte Kontingente sind dann damit verfallen.

Zugriff durch TERRA Cloud NOC-Mitarbeiter

Die Mitarbeiter des TERRA Cloud NOCs haben für Wartungszwecke einen Zugang auf die Firewall VM unabhängig vom Betriebsmodus. Die Wahrung des Datenschutzes ist sichergestellt.

Zugriff durch Lieferanten

Die TERRA Cloud GmbH ist berechtigt, für die Erfüllung der Leistungen Dritte Unternehmen mit heran zu ziehen.

SLA

Dienstleistungen, wie Bereitstellung einer Firewall VM, Erstkonfiguration oder Full Managed Firewall VMs unterliegen keinen vorher definierten Lieferzeiten. Für die Durchführung von Änderungen (Changes) bei einem Full Managed-Vertrag werden keine bestimmten Umsetzungszeiten garantiert.

Ansonsten gelten die SLAs der übergeordneten Dienste.

Weitere Funktionalitäten

Die zur Verfügung gestellte Firewall VM bietet einen weitaus größeren Funktionsumfang als in dieser Leistungsbeschreibung beschrieben. Die geschuldete Leistung ergibt sich ausschließlich über die in diesem Dokument beschriebenen Leistungen der Firewall VM.

Weitere Funktionen stehen dem Kunden zur Verfügung – deren Nutzung erfolgt aber auf eigenes Risiko und auf eigene Haftung des Kunden.

Begriffserklärung

RFC – Reqeusts for Comments

Die Requests for Comments sind eine Reihe von technischen und organisatorischen Dokumenten des RFC-Editors zum Internet. Wenn RFCs sich durch allgemeine Akzeptanz und Gebrauch zum Standard entwickelt haben, definieren diese Dokumente das allgemein anerkannte Vorgehen.
RFCs könne hier eingesehen werden: https://www.rfc-editor.org/

NOC – Network Operation Center

Ist die Abteilung der TERRA Cloud GmbH, die für den Betrieb des Rechenzentrums verantwortlich ist.