

Leistungsbeschreibung Managed Firewall

Stand: 11/2010

1	Anwendungsbereich	3
2	Leistungsumfang Tele2 Managed Firewall für TopNet	3
2.1	Management.....	3
2.2	Hardware	3
2.3	Access	4
2.3.1	Internetanbindung	4
2.3.2	Anbindung der Kundenstandorte	4
3	Leistungsumfang Tele2 Managed Firewall für TopInternet.....	4
3.1	Management.....	4
3.2	Hardware	4
3.3	Access	5
3.3.1	Internetanbindung	5
3.3.2	Anbindung an das Kunden-LAN.....	5
3.4	Netzabschlusspunkt.....	5
4	Leistungsbestandteil Management	5
4.1	Management.....	5
4.2	Konfiguration.....	6
4.2.1	Sicherung von Änderungsanforderungen am Regelwerk.....	6
5	Serviceübergabe	7
6	Wartung und Support.....	7
7	Service Level Agreements (SLA).....	7

1 Anwendungsbereich

Gegenstand dieser Leistungsbeschreibung ist die Dienstleistung von Tele2 Telecommunication GmbH im Rahmen des Services Tele2 Managed Firewall.

Voraussetzung für den Bezug des Service Tele2 Managed Firewall ist ein Basisservice in Form eines Tele2 Business Internet Anschluss (TopInternet) bzw. einer Tele2 Unternehmensvernetzung (TopNet). Das jeweilige Basisservice ist nicht Bestandteil des Leistungsumfanges von Tele2 Managed Firewall, Details zum jeweiligen Basisservice siehe Leistungsbeschreibung TopInternet bzw. Leistungsbeschreibung TopNet.

Der Leistungsumfang des Services Tele2 Managed Firewall unterscheidet sich in

- Tele2 Managed Firewall für TopNet (Punkt 2) und
- Tele2 Managed Firewall für TopInternet (Punkt 3)

2 Leistungsumfang Tele2 Managed Firewall für TopNet

2.1 Management

Die allgemeine Erläuterung der Management-Features ist unter Punkt 4 dieser Leistungsbeschreibung aufgeführt.

2.2 Hardware und Realisierungsvarianten

Als Realisierungsvariante kann je nach Kundenwunsch und Leistungsbedarf eine der folgenden Möglichkeiten gewählt werden:

- CISCO™ ASA redundant ausgeführter Firewall Hardwarecluster, von Tele2 als Service betrieben
- CISCO™ ASA dedizierte Firewall: individuelle FW-Lösung als Service von Tele2 für den Kunden
- CISCO™ ASA dedizierte Kunden-Firewall am Tele2 Housing-Standort

Die Features sind abhängig von der jeweils eingesetzten Hardware.

Die Firewall Variante „CISCO™ ASA Hardwarecluster“ bietet dem Kunden den Vorteil eines hochperformanten Systems, das an zwei unterschiedlichen Standorten untergebracht ist, um maximale Ausfallsicherheit zu gewährleisten.

Vorteile im Detail

- Hardwareredundanz, d.h. Sicherheit gegen Ausfall einer Firewall
- Standortredundanz, d.h. Sicherheit gegen Ausfall eines Standortes
- Gespiegelte Sessions, d.h. Internet Sessions gehen bei Ausfall eines Standortes nicht verloren, sondern werden vom zweiten Standort weitergeführt.
- Stromversorgung, Klimatisierung und Zugangsschutz gemäß höchsten Rechenzentrumsstandards
- Direkte Internetanbindung an den Tele2 Backbone
- 7x24 Betreuung und Überwachung der Hardware
- Hochleistungs-Hardware-Cluster, d.h. keine Performance- und Durchsatzprobleme

Features

- Stateful Inspection Firewall
- NAT / PAT
- Einfache und schnelle Bandbreitenerhöhung möglich
- Durchsatz direkt nach Bedarf skalierbar
- Alle Kundenstandorte gleichzeitig geschützt

Die Variante „dedizierte Firewall als Service“ bietet dem Kunden den Vorteil maximaler Flexibilität bei der Auslegung und Konfiguration der Firewall Lösung, bei gleichzeitiger Überwachung der Hardware durch Tele2 Spezialisten, und direkter Internetanbindung an den Tele2 Backbone. Im Unterschied zur Variante „Hardwarecluster“ bietet die Variante „dedizierte Firewall als Service“ keine Redundanz.

Die Variante „dedizierte Kunden-Firewall“ bietet dem Kunden den Vorteil maximaler Flexibilität bei der Auslegung und Konfiguration der Firewall Lösung, bei gleichzeitiger aktiver Überwachung der Hardware durch Tele2 Spezialisten, und direkter Internetanbindung an den Tele2 Backbone. Bei dieser Variante befindet sich die Firewall Hardware im Kundenrack am Tele2 Housing Standort. Im Unterschied zur Variante „Hardwarecluster“ bietet die Variante „dedizierte Kunden-Firewall“ im Standard keine Redundanz, eine redundante Auslegung der Firewall Hardware ist jedoch auf Kundenwunsch optional möglich.

Access

2.2.1 Internetanbindung

Eine Tele2 Internet Anbindung ist Voraussetzung für das Service Tele2 Managed Firewall für TopNet.

2.2.2 Anbindung der Kundenstandorte

Die Anbindung der Kundenstandorte ist nicht Bestandteil dieses Services, sondern wird im Rahmen von **Tele2 TopNet** realisiert

Der oder die Standorte des Kunden mit TopNet Access können über das Service Tele2 Managed Firewall für TopNet unter Berücksichtigung des mit dem Kunden definierten Regelsets auf das Internet zugreifen.

3 Leistungsumfang Tele2 Managed Firewall für TopInternet

3.1 Management

Die allgemeine Erläuterung der Management-Features ist unter Punkt 4 dieser Leistungsbeschreibung aufgeführt.

3.2 Hardware

Als Firewall Hardware kann je nach Kundenwunsch und Leistungsbedarf eine der folgenden Möglichkeiten gewählt werden:

- Integrierte Firewall im CISCO™i TopInternet-Zugangsrouten, oder
- CISCO™ Firewall Hardware am Kundenstandort, oder
- CISCO™ Firewall Hardware am Tele2 Housing-Standort

Die Features sind abhängig von der jeweils eingesetzten Hardware.

3.3 Access

3.3.1 Internetanbindung

Die Internetanbindung ist nicht Bestandteil des Leistungsumfanges dieses Services, sondern als **Tele2 TopInternet** separat zu bestellen.

Wird ein separates Gerät als Firewall hinter dem Tele2 TopInternet Router eingesetzt, so dürfen allfällige freie Netzwerk-Ports am Router weder direkt, noch indirekt mit dem LAN verbunden werden, da diese Ports nicht von der Firewall gesichert werden. Alle Geräte, Netze, oder Netzwerkteile, die direkt am Tele2 TopInternet Router angeschlossen werden, befinden sich außerhalb des von Tele2 Managed Firewall für TopInternet gesicherten Bereiches des Internets und Tele2 lehnt jede Verantwortung für die Sicherheit dieser sowie aller netzwerkmäßig dahinter liegenden Komponenten ab.

3.3.2 Anbindung an das Kunden-LAN

Für die Anbindung an das Kunden-LAN steht je nach eingesetzter Firewall Hardware zumindest ein gesicherter Ethernet Port zu Verfügung. Die Einbindung in das LAN hat dann über eine vom Kunden beizustellende geeignete Hardware (z.B. Switch, Hub) zu erfolgen.

3.4 Netzabschlusspunkt

Der Netzabschlusspunkt legt die Grenze der Verantwortung zwischen Tele2 und dem Kunden fest. Beim Service Managed Firewall TopInternet ist der Netzabschlusspunkt das von Tele2 am Kundenstandort zur Verfügung gestellte Endgerät.

4 Leistungsbestandteil Management

Das Service Tele2 Managed Firewall sichert das Kundennetzwerk gemäß vereinbarter Regeln vor unerlaubtem Verkehr in das und aus dem Internet. Das Service stellt dem Kunden die Funktionalitäten einer Firewall im klassischen Sinne zu Verfügung. Weiterführende Schutzmechanismen, wie z.B. Spam- oder Virenfilter, die keine Firewall-Funktionalität darstellen, sind nicht Bestandteil dieses Service, können aber separat von Tele2 bezogen werden.

4.1 Management

Das Management der Firewall wird von Tele2 durchgeführt.

Im Rahmen der Management-Aufgaben übernimmt Tele2 folgende Tätigkeiten:

- Erstellen der Firewall Regeln gemäß der Kundenanforderung
- Einspielen des Regelwerkes in die Firewall
- Backup des Regelwerkes
- Änderungen des Regelwerkes nach Kundenanforderung
- Sicherstellung der Berechtigung von Änderungsanforderungen
- Überprüfung des Regelwerks auf Konsistenz
- Überwachung der Firewall auf Verfügbarkeit
- Sperre einzelner IP-Adressen oder ganzer IP-Bereiche bei Gefahr im Verzug
Verbindungsunterbrechungen die aufgrund von Sperrungen wegen Gefahr im Verzug resultieren, stellen keine Serviceunterbrechung dar, die den Kunden zu Ansprüchen gegenüber Tele2 ermächtigen.
- Sperre einzelner IP-Adressen oder ganzer IP-Bereiche, die allgemein als gefährlich bekannt sind (Black-Lists)

Auf Kundenwunsch können diese Bereiche auch wieder freigegeben werden, allerdings übernimmt Tele2 keinerlei Verantwortung für Schäden, die dem Kunden dadurch entstehen

- Aktualisierung der Firewall-Software zur Behebung erkannter Sicherheitsprobleme. Tele2 ist bemüht Aktualisierungen, die mit einer Serviceunterbrechung verbunden sind, im vereinbarten Servicefenster durchzuführen, behält sich jedoch das Recht vor, Aktualisierungen jederzeit vorzunehmen, wenn Dringlichkeit und Sicherheit dies erfordern. Dem Kunden erwachsen daraus keinerlei Ansprüche gegenüber Tele2 wegen Serviceausfalles, da die Sicherheit und Integrität des Netzwerkes gegenüber Verfügbarkeit Priorität besitzt.

4.2 Konfiguration

Im Rahmen der Einrichtung des Service Tele2 Managed Firewall unterstützt Tele2 den Kunden bei der Definition des Regelwerkes der Firewall. Konfigurationsanpassungen werden im ersten Monat nach Inbetriebnahme unlimitiert durchgeführt. Danach sind bis zu vier Änderungsanforderungen vom Kunden pro Monat im Entgelt enthalten. Änderungsanforderungen beinhalten übliche Konfigurationsänderungen im Rahmen des Netzwerkbetriebs. Grundlegende Netzwerkänderungen (z.B. Umstellung eines gesamten IP-Adress-Bereichs, Einrichten einer neuen DMZ, etc.) sind nicht davon umfasst.

Bei Tele2 Managed Firewall für TopNet sind Änderungen am Regelwerk, die durch neu hinzugekommene TopNet-Standorte notwendig werden, je einmal pro neuem Standort, zusätzlich enthalten.

Darüber hinausgehende Änderungswünsche des Kunden werden zum jeweilig gültigen Stundensatz von Tele2 abgerechnet, wobei angefangene Viertelstunden als volle Viertelstunden verrechnet werden.

Änderungen am Regelwerk werden von Tele2 Mo-Fr (werktags) zwischen 7:00-18:00 durchgeführt.

Die Durchführung von Änderungsanforderungen erfolgt möglichst umgehend, spätestens jedoch am nächsten Werktag.

4.2.1 Sicherung von Änderungsanforderungen am Regelwerk

Anforderungen zu Änderungen am Regelwerk werden nur entgegengenommen, wenn sie per Email von einer der vorab vereinbarten eindeutigen Email-Adressen (Ansprechperson) des Kunden stammen und an die Email-Adresse securebox@at.tele2.com gerichtet sind.

Alle Anforderungen, die der obigen Vorgehensweise nicht entsprechen werden nicht bearbeitet. Diese Vorgehensweise dient dem Schutz des Kunden vor unberechtigten Änderungsanforderungen.

Eine korrekte Anforderung wird dem Absender bestätigt. Hat der Kunde die Änderung nicht veranlasst, muss er der Bestätigung unverzüglich widersprechen, die Änderung wird in diesem Fall nicht durchgeführt beziehungsweise rückgängig gemacht. Es obliegt in diesem Fall dem Kunden geeignete Maßnahmen zur Identifizierung des unberechtigten Absenders zu veranlassen, wobei Tele2 den Kunden dabei im Rahmen der gesetzlichen Möglichkeiten über Anforderung unterstützt.

Widerspricht der Kunde der Bestätigung der Anforderung nicht oder verspätet, so gilt sie als vom Kunden autorisiert und Tele2 haftet für keinerlei Schäden, die dem Kunden aus dieser Änderung allfällig entstehen.

Tele2 kann nicht die Sicherheit des kompletten Kundennetzwerkes gewährleisten, sondern stellt den vom Kunden definierten Sicherheitsmechanismus (Firewall Regelwerk) zur Verfügung. Weiters übernimmt Tele2 nicht die Haftung für Datenverluste die durch Service-Unterbrechungen der Tele2 Managed Firewall verursacht wurden.

5 Serviceübergabe

Die Herstellungszeit ist abhängig vom jeweils gewählten Basisservice sowie der gewählten Firewall Hardware und wird individuell im konkreten Kundenangebot ausgewiesen.

Die Serviceübergabe erfolgt mit Übermittlung des Übergabeprotokolls (schriftlich oder mündlich) pro realisierter Managed Firewall.

Ab Serviceübergabe erfolgt die Verrechnung der von Tele2 erbrachten Leistung an den Kunden.

6 Wartung und Support

Zur Meldung von technischen Störungen stehen dem Kunden

- die technische Service-Hotline von Mo-So von 0-24:00 unter 050500 3333,
- sowie die Email-Adresse securebox@at.tele2.com zur Verfügung.

Fehler in den zentralen Komponenten im Tele2-Netzwerk und der Server-Hardware werden von Tele2 von Mo-So von 0-24:00 proaktiv überwacht und behoben.

Die Entstörung erfolgt gemäß dem Service Level Agreement des jeweiligen Basisservices.

7 Service Level Agreements (SLA)

Service Level Agreements richten sich immer nach dem SLA des jeweiligen Basisservices.

ⁱ Alle im vorliegenden Dokument verwendeten eingetragenen Warenzeichen sind im Eigentum der jeweiligen Firma.