# Servicebeschreibung S2004 Firewall + VPN für Einrichtungen der TU

**Version 1.1**
**Datum: 21.04.2021**

TECHNISCHE UNIVERSITÄT DARMSTADT

HRZ Hochschulrechenzentrum

Technische Universität Darmstadt
Hochschulrechenzentrum
Alexanderstraße 2
64283 Darmstadt

http://www.hrz.tu-darmstadt.de
service@hrz.tu-darmstadt.de

## Inhaltsverzeichnis

## Änderungshistorie

| Datum | Version | Änderung |
|---|---|---|
| 23.10.2017 | 1.0 | Initialversion |
| 21.04.2021 | 1.1 | Layout Anpassungen |
| | | |

## 1. Kurzbeschreibung des Service

Das HRZ betreibt die zentrale Firewall für die TU Darmstadt und stellt an dieser die Einhaltung der zentralen Policies der TU sicher.

Das HRZ bietet den Instituten die Installation einer nach ihren Vorgaben eingerichteten Firewall am Zugang zum Institutsnetz an. Das HRZ übernimmt dabei die Konfiguration, die Inbetriebnahme und den Betrieb der Firewall auf Basis der Kundenvorgaben. Im Rahmen dieses Angebots besteht auch die Möglichkeit, sich einen VPN-Zugang in das Institutsnetz einrichten zu lassen.

## 2. Zielgruppen

### 2.1. Kundengruppen

Beauftragt werden kann der Service von:

- Einrichtungen der TU (Fachbereiche, zentrale Einrichtungen)
- Zentralverwaltung
- Hochschulgruppen
- Studentische Gremien (ASTA, Fachschaften)

### 2.2. Anwendergruppen

Der Service kann von folgenden Anwendergruppen genutzt werden:

- Beschäftigte der TU
- Studierende
- Gäste und Partner (mit TU-ID)
- Lehrbeauftragte
- Studentische Hilfskräfte
- Externe/Gäste (ohne TU-ID)

## 3. Rahmenbedingungen (Technische Voraussetzungen)

Voraussetzung für die Installation einer Firewall sind ein oder mehrere Subnetze (IPv4/IPv6) an der TU Darmstadt. Diese können vom HRZ oder vom Auftraggeber betrieben sein, müssen sich aber an der TU Darmstadt befinden und eine Verbindung zum Netz der TU haben.
Der VPN-Client unterstützt Windows/MacOS/Linux-Klienten sowie iOS und Android.

## 4. Servicemerkmale

### 4.1. Zusammenfassung Funktionsumfang

- Firewall - Absicherung des Kundennetzwerkes gegen unerwünschte Zugriffe von außen
- Optional: Bereitstellen eines VPN-Zugangs ins Kundennetz
- Optional: Absichern des Netzes gegen Zugriffe aus dem Kundennetz heraus
- Optional: Absicherung mehrerer Netze, z.B. Servernetz, DMZ

### 4.2. Funktionsumfang des Service im Detail

Der Service Firewall dient zur Absicherung des oder der Kundennetze gegen ungewollte Verbindungen aus dem TU Netz und dem Internet. Auch eine Einschränkung von Zugriffen aus dem Netz heraus ist möglich. Hierfür wird gemeinsam mit den technischen Ansprechpartnern des Kunden ein Regelsatz erarbeitet und auf der Firewall implementiert.

Optional kann ein Regelsatz für Zugriffe aus dem Kundennetz installiert werden, der z.B. für bestimmte IP-Adressen nur Zugriffe auf einzelne Server im Netz der TU erlaubt.

Der Zugriff auf das Netz des Kunden kann optional über einen VPN-Service auf der Firewall erfolgen. Die berechtigten Nutzer_innen authentifizieren sich mit ihrer TU-ID und werden von den technischen Ansprechpartnern des Kunden über eine Webschnittstelle verwaltet. Die dazu nötige Software steht für die üblichen Betriebssysteme bereit.

Die zur Serviceerbringung nötigen Geräte, Software und entsprechende Lizenzen sind vom HRZ mit einem Wartungsvertrag abgesichert. Fallen einzelne Geräte aus dem Herstellersupport, so werden diese im Rahmen der abgeschlossenen Vereinbarung gegen gleichwertige Geräte ersetzt.

### 4.3. Betrieb und Sicherheit

Die Hardware ist bei einem externen Partner unter Wartung und kann innerhalb eines Arbeitstages ersetzt werden. In der Regel sind Geräte im Bestand vorhanden, so dass im Fehlerfall normalerweise deutlich schneller reagiert werden kann.

Durch proaktives Monitoring werden Fehler zum Teil im Vorfeld abgefangen.

Die Konfiguration der Geräte wird automatisch zentral gesichert. Administrativen Zugang haben nur Mitarbeitende der Abteilung Infrastruktur des HRZ. Alle Zugriffe werden protokolliert.

## 5. Funktionalitätsabgrenzungen

Der Service eignet sich nur bedingt für Anwendungen mit hohem Datendurchsatz. Die meisten Firewallmodelle (Beschreibung s. https://www.hrz.tu-darmstadt.de/services/it_services/firewall_vpn/preise_firewall_vpn/index.de.jsp) werden die Geschwindigkeit der Übertragung mindern.

## 6. Lizenzen und Kosten

Die Servicekosten enthalten die Aufwendungen für Hardware, notwendige Lizenzen und die Personalressourcen des HRZ. Bei Konfigurationsanpassungen wird in der Regel kein Entgelt erhoben. In seltenen Fällen, sollte der Konfigurationsaufwand sehr hoch sein (Beispiel: Komplette Umstrukturierung des Kundennetzes), wird der Aufwand nach Rücksprache stundenweise abgerechnet.

## 7. Bestell- und Änderungsverfahren

### 7.1. Bestellung des Service

Der Erstkontakt erfolgt typischerweise über den HRZ-Service (siehe 8.1).

Um die Konfiguration auf die Bedürfnisse des Kunden abzustimmen wird ausgehend von einer Basiskonfiguration gemeinsam mit dem Kunden die Erstkonfiguration erarbeitet und das passende Firewall-Modell herausgesucht. Es stehen ein Basis-Modell und ein schnelleres Modell zur Verfügung.
In dieser Phase wird normalerweise auch die Vereinbarung zwischen dem Kunden und dem HRZ abgeschlossen.

Der Service steht zum in der Vereinbarung festgehaltenen Datum zur Verfügung, eine Vorlaufzeit von einer Arbeitswoche ist zu beachten.

Mit Bestätigung der Bestellung geht dem Kunden die Vereinbarungsnummer zu, unter der Anfragen beim HRZ-Service getätigt werden können.
Ist der VPN-Service mitbeauftragt, erhält der Kunde einen Link zu dem webbasierten Managementsystem für die VPN-Zugänge.

### 7.2. Änderung der Servicemerkmale

#### 7.2.1. Änderungen der Konfiguration

Die Änderung der Firewall-Regeln kann direkt über eine Anfrage beim HRZ-Service (8.1) beauftragt werden.
Einfache Regeländerungen erfolgen kostenfrei, komplette Umkonfigurationen werden auf Stundenbasis abgerechnet.

Änderungen der berechtigten VPN-User können über eine Webschnittstelle selbst vorgenommen werden.

#### 7.2.2. Änderung der technischen Ansprechpersonen

Die Löschung oder Ergänzung technischer Ansprechpersonen kann von einer der bestehenden technischen Ansprechpersonen über eine Anfrage beim HRZ-Service (8.1) vorgenommen werden. Es ist ratsam, mindestens immer zwei Ansprechpersonen aufzuführen.

#### 7.2.3. Änderungen der Abrechnungsdaten

Die Änderung der Abrechnungsdaten kann direkt mit dem Stab Verwaltung des HRZ erfolgen:
(vertragsmanagement@hrz.tu-darmstadt.de )

#### 7.2.4. Änderung des Firewallmodells

Eine Änderung des Firewall-Modells kann beim HRZ-Service (8.1.) beauftragt werden. Die Mindestvertragslaufzeit verlängert sich dadurch wieder auf 3 Jahre.

### 7.3. Kündigung des Service

Die Vereinbarung wird über einen Zeitraum von 3 Jahren geschlossen und verlängert sich jeweils um ein weiteres Jahr, wenn die Vereinbarung nicht 3 Monate vor Vereinbarungsende gekündigt wird.

Ein Sonderkündigungsrecht wird dem Kunden eingeräumt, falls sich die Organisationseinheit auflöst oder die Räumlichkeiten verliert, in denen der Service angeboten wird.
Hier ist eine Kündigungszeit von 2 Monaten zu beachten.

## 8. Support

### 8.1. Standardwege für Supportanfragen

Supportanfragen sind zu richten an:

HRZ-Service
Webformular: http://www.hrz.tu-darmstadt.de/kontaktformular
E-Mail: service@hrz.tu-darmstadt.de
Hotline: +49 6151 16-71 112

Supportberechtigt sind die in der Vereinbarung aufgeführten technischen Ansprechpersonen.
Änderungen der technischen Ansprechpersonen können ebenfalls über das Webformular veranlasst werden.

Reaktionszeit für Anfragen ist ein Arbeitstag.

### 8.2. Supportumfang

| Support | Verfügbarkeit | Bearbeitungszeit |
|---|---|---|
| Informationen, Anleitungen, FAQs online unter www.hrz.tu-darmstadt.de/institutsfirewall | 24/7 | n.a. |
| Supportanfragen per Webformular oder E-Mail | 24/7 | Während der üblichen Arbeitszeiten[1)] |
| Hotline | Hotline-Zeiten siehe online unter: http://www.hrz.tu-darmstadt.de/service | Während der Verfügbarkeitszeiten, sofern das Anliegen von den Mitarbeiter_innen an der Hotline sofort bearbeitet werden kann. Für Anliegen, die nicht sofort bearbeitbar sind, wird ein Support-Ticket erstellt, das während der üblichen Arbeitszeiten[1)] bearbeitet wird |

[1)] Es gelten die Allgemeinen Betriebs- und Servicezeiten des HRZ

## 9. Systemzeiten

Notwendige Systemzeiten werden per E-Mail mit einem Vorlauf von mindestens einer Woche an die technischen Ansprechpartner geschickt.

Bei sicherheitskritischen Updates kann die Ankündigungszeit verkürzt werden

## 10. Anhang

Nachfolgend eine Übersicht wichtiger Dokumente und Weblinks:

**Informationen, Anleitungen, FAQs**

- https://www.hrz.tu-darmstadt.de/institutsfirewall

**Entgeltliste**

- Entgeltliste unter: https://www.hrz.tu-darmstadt.de/services/it_services/firewall_vpn/preise_firewall_vpn/index.de.jsp

**Nutzungsbedingungen**

---

**Allgemeine Service- und Betriebszeiten**

- https://www.hrz.tu-darmstadt.de/betrieb-servicezeiten

**Benutzungsordnung für IT-Systeme der Technischen Universität Darmstadt**

- https://www.hrz.tu-darmstadt.de/it-benutzungsordnung

**Leitlinie zur Informationssicherheit der TU Darmstadt**

- http://www.hrz.tu-darmstadt.de/itsecurity_policy