Firewalls für Institute und zentrale Einrichtungen

Das Gauß-IT-Zentrum stellt allen Instituten und zentralen Einrichtungen im Rahmen der technischen Realisierungsmöglichkeiten eigene Firewalls innerhalb der zentralen Firewall-Infrastruktur bereit. Diese Firewalls bieten nicht nur Schutz vor dem Internet sondern trennen auch die Netze einzelner Einrichtungen innerhalb des Netzes der TU Braunschweig voneinander. Sollte Ihre Einrichtung über mehr als ein Netz verfügen, kontrolliert die Firewall auch den Verkehr zwischen diesen Netzen.

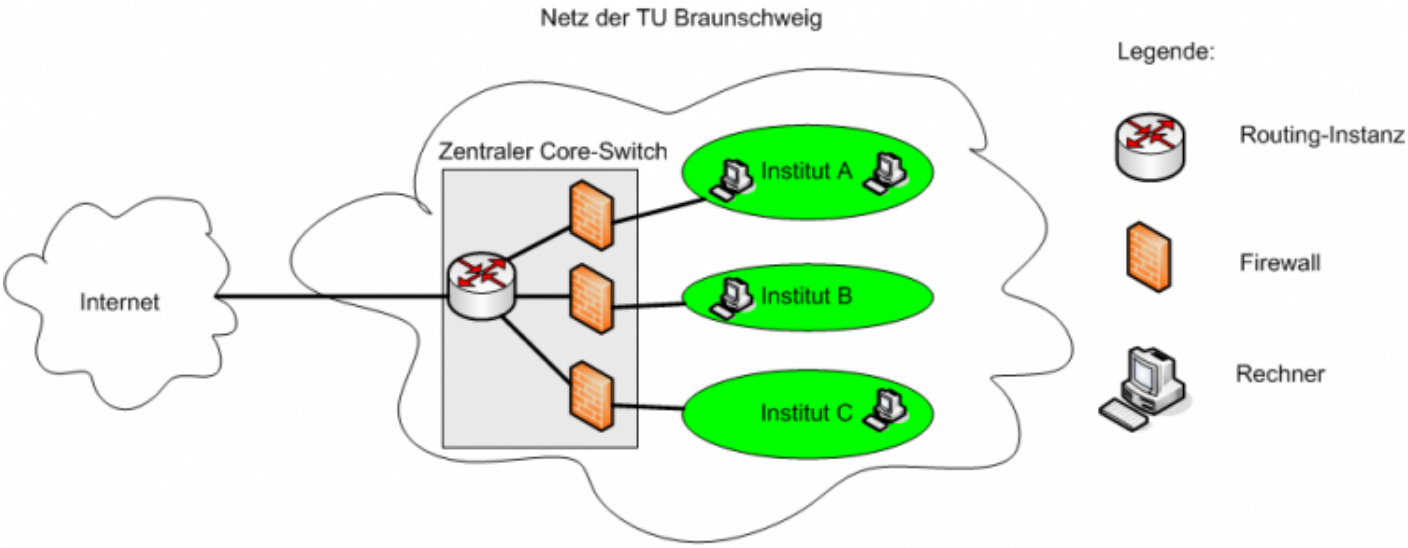


Abb. 1: Zentral bereitgestellte Firewall zum Schutz der Netze von Instituten innerhalb der Netzinfrastruktur der TU Braunschweig

Als Managed Firewall wird Ihre Instituts-Firewall von uns betreut. Änderungen werden von Ihnen als DV-Koordinator beauftragt und nach Rücksprache mit Ihnen auf der Firewall aktiviert. Den jeweils aktuellen Satz der Firewall-Regeln können Sie im KDD einsehen. In der Regel werden wir Ihre Anfragen nach Regeländerungen spätestens innerhalb von 48h an Arbeitstagen bearbeiten, meistens sogar innerhalb weniger Stunden.

Technische Realisierung

Die Firewalls sind an den Core-Routing-Standorten im Backbone-Netz der TU integriert. Es handelt sich jeweils um Firewall-Cluster, die aus zwei Geräten bestehen, über die die Institute redundant angebunden sind, was ein großes Maß an Ausfallsicherheit garantiert. Sollte ein Gerät oder die Anbindung eines Geräts ausfallen, so übernimmt das andere Gerät den Betrieb in Sekunden. Da die

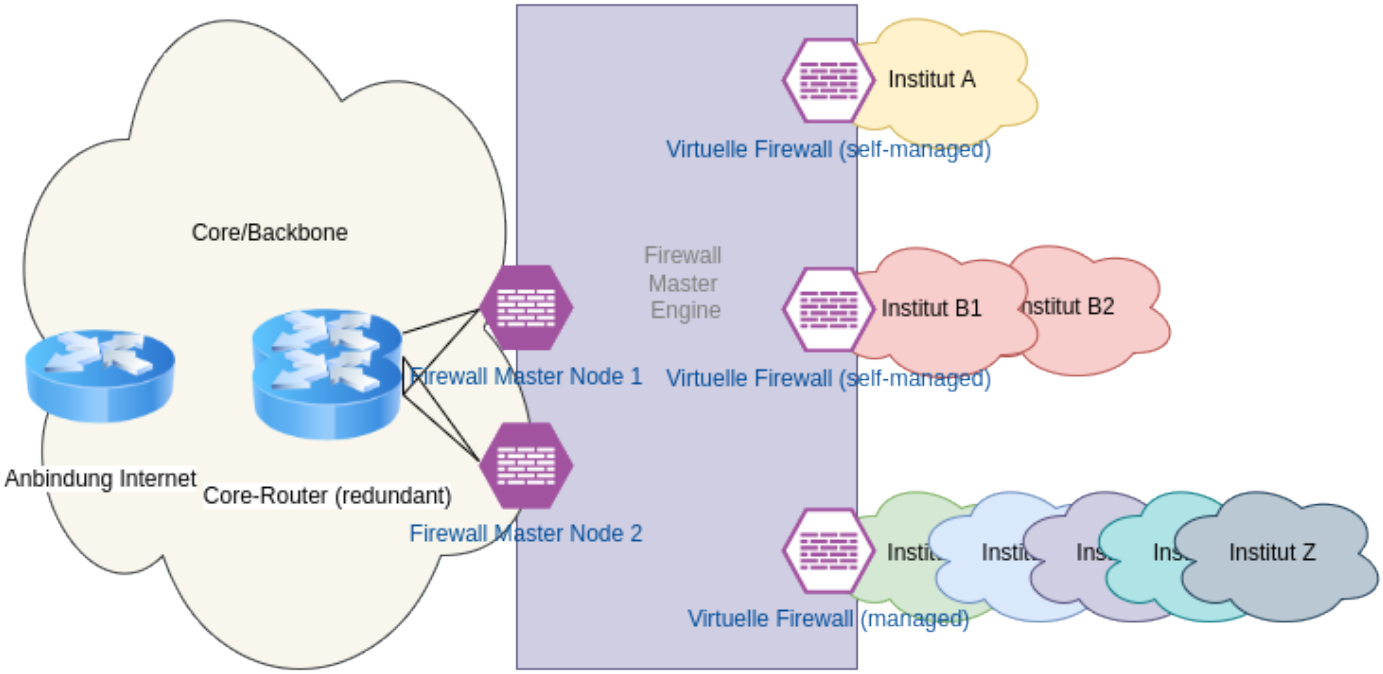
Statusinformationen jeder Verbindung vorliegen, geschieht dies im Allgemeinen sogar ohne Verbindungsabbruch.

Die Instituts-Firewalls werden auf den Firewall-Clustern als sogenannte virtuelle Firewalls realisiert. Für den Firewall-Administrator verhalten sich diese Kontexte genauso wie eine Firewall mit eigenständiger Hardware.

Die von uns angebotenen Firewalls werden über das Routing-Protokoll OSPF(v2/v3) in das IP-Netz der TU eingebunden. Auf den Firewalls selbst liegt jeweils das Gateway der einzelnen Institutsnetze. Auch das DHCP-Relaying wird ggf. von den Firewalls übernommen. Jedes Netz, egal ob auf unterschiedlichen oder der gleichen Firewall wie andere Netze, ist von allen anderen Netzen Firewall-technisch getrennt. D. h. Zugriff von einem Netz auf Rechner/Services in einem anderen Netz muss immer per Firewall-Regeln eingehend und ggf. ausgehend freigeschaltet werden.

Das Management/die Konfiguration der Firewalls erfolgt über ein Webinterface, das über einen von der Firewall selbst getrennten Server zur Verfügung gestellt wird. Es kann in jedem Browser verwendet werden und erfordert keine zusätzlichen Programme (z.B. Java). Änderungen (z.B. am Regelwerk) werden dort zunächst eingetragen, gespeichert und dann auf die Firewall übertragen. Spätestens in der Nacht werden alle gespeicherten Änderungen automatisch auf die Firewalls übertragen, um auch Updates zu Malware-Erkennungen, die regelmäßig und automatisch vom Hersteller übermittelt werden, auf allen Firewalls zeitnah (ohne manuelles Zutun) zu aktivieren.

Wartungen an den Firewalls oder dem Management-Server werden in der Regel in den Wartungsfenstern Mittwochs zwischen 6:00 und 7:00 Uhr durchgeführt. In dieser Zeit kann es sein, dass der Management-Server nicht zur Verfügung steht. Sollten wir erwarten, dass es durch Wartungsarbeiten an den Firewalls zu einem vorübergehenden Ausfall der Netzanbindung kommt, kündigen wir dies separat an. In der Regel sind jedoch auch Updates der Firewall und sogar Hardware-Arbeiten im Betrieb und ohne Ausfall möglich.



Revision #1
Created 2024-05-15 13:19:14 UTC by Tina Strauf
Updated 2024-05-15 13:31:34 UTC by Tina Strauf