Frequently Asked Questions (FAQ)

F: Wie flexibel ist die Firewall und kann sie unsere Anforderungen überhaupt erfüllen?	**A**: Eine vollständige Liste sämtlicher Features der NGFW Firewall entnehmen Sie bitte den von der Firma ForcePoint zur Verfügung gestellten Dokumentation. Grundsätzlich handelt es sich um eine sogenannte „Next Generation Firewall“, die technologisch dem aktuellen Stand entspricht. Sie können damit also von Regeln für beispielsweise GRE-Tunnelling über einfache Regeln, die sämtlichen Verkehr zwischen bestimmten IP-Adressen auf Layer 3 regeln bis hin zu solchen Konfigurationen, die bestimmte HTTP- oder FTP-Direktiven prüfen und einschränken, alles konfigurieren was Sie als notwendig erachten. Selbstverständlich ist die Firewall so auch in der Lage nicht nur bei TCP, sondern auch bei UDP-Protokollen oder FTP den Verbindungsaufbau komplett zu verfolgen, sodass Kommunikationspartner, die eine Verbindung in einer Richtung aufgebaut haben, (temporär für die Dauer der Session) auch in umgekehrter Richtung Daten austauschen können, ohne dass spezielle Regeln in Rückrichtung nötig wären („stateful firewalling“).
F: Wir haben eine DMZ, wie können wir zukünftig eine DMZ abgrenzen?	**A:** Prinzipiell ist das Einrichten einer DMZ möglich. Dies geschieht in der Regel durch die Aufteilung Ihres Adressbereichs in zwei oder mehr Teile, die an der Firewall in verschiedene sogenannte VLANs aufgeteilt und getrennt durch die Firewall geführt werden. Zusätzlich zu unterschiedlichen Regelwerken, die die beiden Netzbereiche zum „Internet hin“ abgrenzen, geht dann auch der Verkehr zwischen den beiden Netzbereichen stets durch die Firewall und kann/muss ebenfalls mit speziellen Regeln versehen werden.
F: Wir haben einen bestehenden Regelsatz an unserer Firewall konfiguriert und würden gerne wissen, ob sich ein bestimmter Teil des Regelsatzes auch auf der vom Gauß-IT-Zentrum angebotenen Firewall umsetzen lässt.	**A:** Wir klären gerne in einem persönlichen Gespräch, wie sich Ihr konkretes Konfigurationsanliegen mit der von uns angebotenen Firewall umsetzen lässt.

F: Vor Generationen hat eine studentische Hilfskraft für uns einen Regelsatz entworfen. Da wir selbst die Regeln und deren Auswirkungen nicht verstehen: Können Sie den Regelsatz auf der zentralen Firewall einspielen?	**A**: Nein. Zum einen ist die Syntax der Konfiguration mit an Sicherheit grenzender Wahrscheinlichkeit nicht kompatibel, und zum anderen hat es sich als sinnvoll erwiesen, wenn zunächst der heute tatsächliche Bedarf festgestellt wird. Es ist für Sie nicht hilfreich, wenn Sie uns bei Problemen fragen: „Warum geht x und y nicht, wo doch z auch funktioniert“ und wir Ihnen nur antworten können: „Keine Ahnung, das haben Sie uns so konfigurieren lassen, das sollten Sie selbst wissen.“ In Sachen Konfiguration erleichtert die Firewall die Verwaltung im Übrigen natürlich durch gängige Methoden wie die Möglichkeit zur Anlegung von Service Groups und Network-Object Groups, die für verschiedene Regeln wieder verwendet werden können, bzw. in den meisten Fällen mehrere Regeln zu einer oder einigen wenigen Regeln zusammenfassbar machen. Es ergibt Sinn, bei einer Neukonfiguration mit Systematik genau diese Hilfsmittel zu nutzen, um die Übersichtlichkeit und damit auch die Wartbarkeit der zum Teil komplexen Regelwerke zu verbessern.
F: Wir betreiben einen eigenen DHCP-Server. Müssen wir dafür Regeln vorsehen?	**A:** Nein. Sollten Sie den gleichen DHCP-Server jedoch in mehreren Netzen nutzen wollen, müssen wir das DHCP-Relaying-Feature auf den Interfaces zu den Netzen konfigurieren, in denen der DHCP-Server nicht steht. D.h. in diesem Fall müssen Sie uns (z.B. per kurzer Mail) bescheid geben und die IP-Adresse des DHCP-Servers benennen. Darüber hinausgehende Firewall-Regeln werden aber auch dann nicht benötigt.
F: Sind die zentralen Firewalls auch VPN-Server?	**A:** Nein. Einen alternativen Dienst stellen wir jedoch unter dem Namen „Instituts-VPN“ über die zentrale VPN-Infrastruktur zur Verfügung. Näheres dazu finden Sie hier.
F: Das klingt alles ganz toll, nur wo ist der Haken?	**A:** Sie erhalten eine redundante (praktisch vollständig ausfallsichere) Firewall, basierend auf ausbaufähiger Firewall-Infrastruktur, die allen derzeit gängigen Anforderungen gerecht wird. Darüber hinaus müssen sie sich lediglich darum kümmern, welche Regeln für Ihre Anwendungszwecke notwendig sind und uns diese mitteilen. Auch wir können keinen Haken finden.

F: Was hat das Gauß-IT-Zentrum davon?	**A:** Abgesehen davon, dass wir diesen Service schlicht für eine ziemlich gute Dienstleistung für die Institute und Einrichtungen halten, haben „wir“ davon, dass sich gegenüber von Ihnen betriebenen Firewalls für uns bei Störungen jedweder Art die Transparenz erhöht. Aktuell ist es ermüdend oft der Fall, dass Netze, die hinter eigenen Firewalls hängen, für uns „Blackboxes“ sind, in die wir keinen Einblick haben. Wenn dann ein Fehler auftritt, können wir in der Regel nicht annähernd so schnell die Ursache finden, wie es der Fall wäre, wenn wir auf Anhieb die Firewall oder auch nur Wechselwirkungen mit der Firewall (sie muss ja nicht immer „falsch“ konfiguriert sein) ausschließen können. Es ist mindestens hilfreich, wenn nicht sogar in den meisten Fällen unabdingbar, für eine schnelle und zielführende Fehlersuche zu wissen, was die Firewall macht und was sie nicht macht. Dazu kommt, dass unsere zentrale Firewall-Infrastruktur auch alle Verbindungsaufbauten etc. loggt. Diese Informationen können bei einem Sicherheitsvorfall dafür sorgen, dass ggf. schnell ausgeschlossen werden kann, ob sich eine Kompromittierung außerhalb des betroffenen Netzes ausgebreitet hat, was ggf. dafür sorgt, dass ein Institut nicht länger als nötig "vom Netz" getrennt ist
F: Die Firewall-Infrastruktur an sich finden wir sehr gut, jedoch möchten wir selbst die Regeln in der Firewall pflegen. Unser Institut hat hierzu ausreichend fest angestelltes und gut ausgebildetes Personal, sodass wir uns die Pflege selbst zutrauen.	**A:** In der Vergangenheit konnten wir diesen Service problemlos anbieten. Vorfälle haben jedoch dafür gesorgt, dass das Modell einer "self-managed" Firewall nur noch in Ausnahmefällen, und nur nach Rücksprache mit dem CISO-Team eingerichtet wird. Sprechen Sie uns dazu gern an.
F: Wir haben nur eine studentische Hilfskraft, die für uns die Firewall pflegt. Wie gestalten wir die Übergabe der Firewall?	**A:** Sprechen Sie uns einfach an: noc@tu-braunschweig.de. Zur Information: In der Regel sollten die Zeiträume, in denen Sie die Administration der Firewall übernehmen, und die potenzielle Rückgabe einer an Sie delegierten Firewall-Administration größer als ein Jahr sein. Auch die Rolle des DV-Koordinators ist vom Grundsatz her nur an fest angestelltes Personal Ihres Instituts zu übertragen. Dies sollte im Allgemeinen Konstanz und Qualität bei den entsprechenden Arbeiten erhöhen.

3. Für und Wider

Wider: Wir haben schon eine Firewall. Mit Ihrer Lösung schwindet aus unserer Sicht die Transparenz.	**Für**: Inzwischen könnten Sie im KDD jederzeit Einblick in das für Ihr Netz/Ihre Netze geltende eingehende Regelwerk nehmen.

Wider: Mit der Firewall vom Gauß-IT-Zentrum sind wir abhängig vom GITZ.	**Für**: Ganz ehrlich? Nicht abhängiger als Sie es sowieso schon sind. Sollte eines schwarzen Tages das GITZ abbrennen und Corerouter, sowie die Firewalls in Rauch aufgehen, dann hätten wir aktuell alle auch so ein riesiges Problem, da dann eh kein Netzwerk mehr zur Verfügung steht. Was Wartungsarbeiten an den Firewalls (Software-Updates etc.) angeht, so werden wir diese in der Regel in den Wartungsfenstern Mittwochs morgens 6:00 - 7:00 Uhr und darüber hinaus in den allermeisten Fällen ohne Ausfall durchgeführt. Nicht zuletzt dafür haben wir ja in Redundanz investiert. Natürlich müssen Sie ggf. einen zeitlichen Versatz zwischen ihrem Auftrag für eine Änderung am Regelwerk und der Ausführung einplanen. Vergessen Sie dabei jedoch nicht, dass auch Instituts-eigene Administratoren gelegentlich nicht verfügbar/erreichbar sind, bzw. ggf. – auf Grund mangelnder Erfahrung/Routine – deutlich länger für die Umsetzung einer Änderung brauchen als Mitarbeiter am GITZ, die sich täglich mit der Firewall beschäftigen. Nicht zuletzt wird durch den Austausch zwischen Mitarbeitern des Instituts und dem GITZ über eine Regeländerung auch eine Art 4-Augen-Prinzip implementiert, die in der Vergangenheit immer wieder dafür gesorgt hat, das "Löcher in der Firewall" deutlich kleiner ausgefallen sind, als sie ggf. wären, hätte ein Mitarbeiter am Institut die Regel ohne Rücksprache eingetragen.

Wider: Unsere Firewall ist noch nie kaputt gegangen und einfach zu pflegen. Der Vorteil erhöhter Redundanz ist für uns daher nicht relevant.	**Für**: Mit Verlaub, diese Art der Betrachtung ist extrem kurzsichtig. Tatsächlich sollte *keine* Firewall, solange sie läuft und die Regeln entsprechend der eigenen Wünsche implementiert sind, irgendwelche „Probleme“ oder großartige Arbeit machen. Dies gilt aber nur bis zu dem Tag, an dem sie ausfällt; entweder weil die Hardware (oder ein Stück Hardware) oder die Software den Dienst quittiert. Wenn Sie dafür nicht einen extrem guten und kurzfristig implementierbaren Ausfallplan haben, ist Ihr Institut für die Zeit, in der Sie daran noch arbeiten, komplett vom Netz abgeschnitten; ganz abgesehen von der Zeit, die es u. U. braucht, bis qualifiziertes Personal vor Ort ist. Unserer Erfahrung nach wird ein Ausfall des „Internets“ in den allermeisten Fällen von den Mitarbeitern am Institut als Zeit betrachtet, in der faktisch so gut wie nicht gearbeitet werden kann. Bei uns ist alles redundant. Dies schließt nicht nur die Firewall selbst, sondern auch die Stromversorgung mit ein. Bei einem Ausfall einer Komponente eines Gerätes übernimmt das Andere die Arbeit ohne Verbindungsausfall. Noch dazu ist unsere Infrastruktur beim Hersteller „im Service“, und wenn eine Komponente ausfällt, haben wir innerhalb von etwa 24 – 48 Stunden Ersatz. → In unseren Augen erhöht das die Verfügbarkeit bzw. Ausfallsicherheit ganz erheblich.

Revision #3
Created 15 May 2024 13:31:39 by Tina Strauf
Updated 16 May 2024 10:37:51 by Tina Strauf